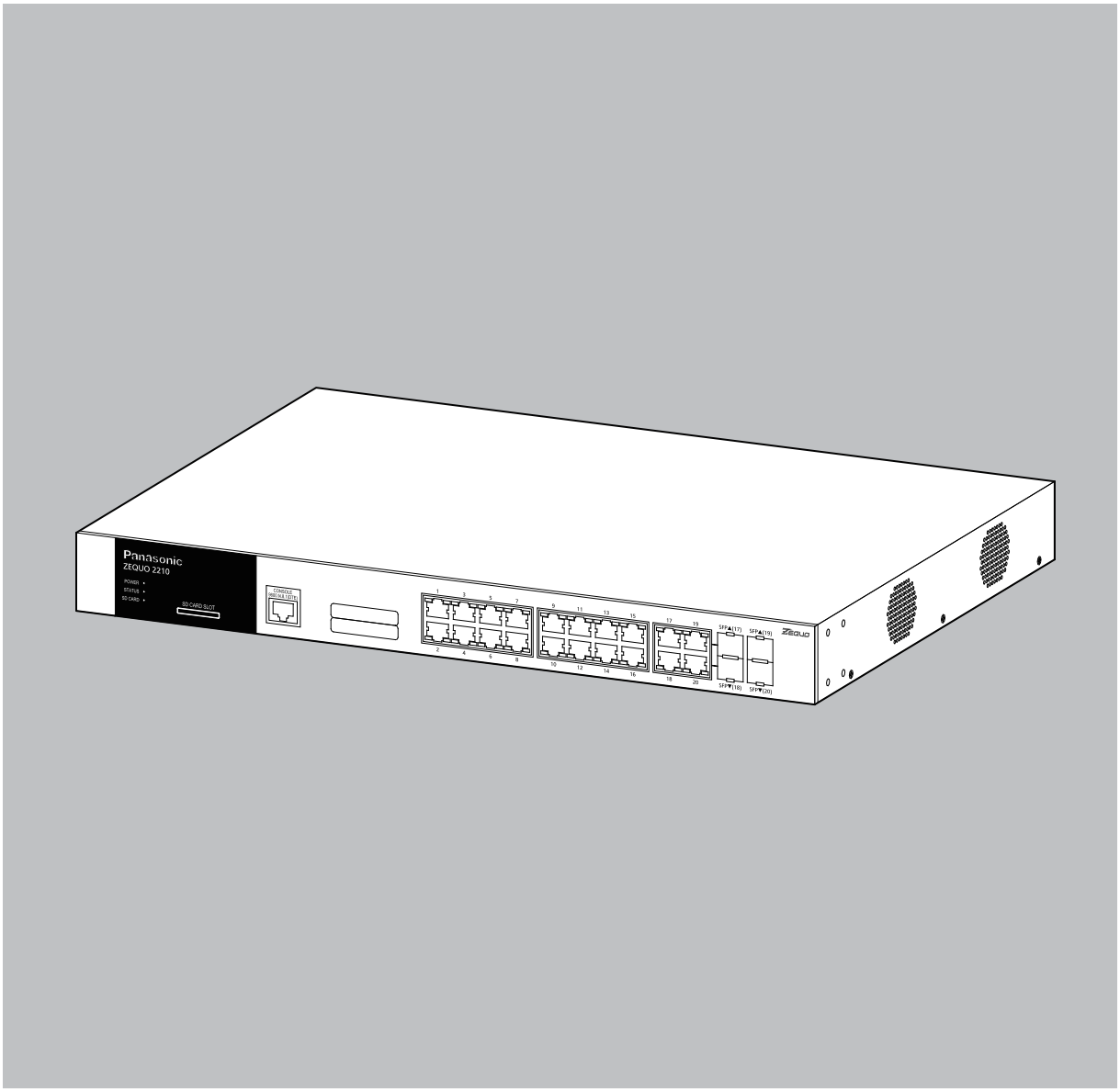
Panasonic

ZEQUO 2210

取扱説明書

品番 PN26161

- お買い上げいただき、まことにありがとうございます。
- 説明書をよくお読みのうえ、正しく安全にお使いください。
- **ご使用前に「安全上のご注意」（2 ～ 6 ページ）を必ずお読みください。**
- **いかなる場合でも、お客様で本体を分解した場合には、保証対象外となります。**



目次

安全上のご注意　必ずお守りください

人への危害、財産の損害を防止するため、必ずお守りいただくことを説明しています。

■誤った使い方をしたときに生じる危害や損害の程度を説明しています。

⚠注意「軽傷を負うことや、財産の損害が発生するおそれがある内容」です。

■お守りいただく内容を次の図記号で説明しています。

してはいけない内容です。	実行しなければならない内容です。

⚠注意

禁止

●**交流 100V 以外では使用しない**
火災・感電・故障の原因になります。

●**ぬれた手で電源プラグを抜き差ししない**
感電・故障の原因になります。

●**雷が発生したときは、この装置や接続ケーブルに触れない**
感電の原因になります。

●**この装置を分解・改造しない**
火災・感電・故障の原因になります。

●**電源コードを傷つけたり、無理に曲げたり、引っ張ったり、ねじったり、たばねたり、はさみ込んだり、重いものをのせたり、加熱したりしない**
電源コードが破損し、火災・感電の原因になります。

●**開口部やツイストペアポート、コンソールポート、SFP 拡張スロット、SD カードスロットから内部に金属や燃えやすいものなどの異物を差し込んだり、落とし込んだりしない**
火災・感電・故障の原因になります。

●**ツイストペアポートに 10BASE-T/100BASE-TX/1000BASE-T 以外の機器を接続しない**
火災・感電・故障の原因になります。

●**コンソールポートに別売のコンソールケーブル PN72001 RJ45-Dsub9 ピンコンソールケーブル以外を接続しない**
火災・感電・故障の原因になります。

●**水のある場所の近く、湿気やほこりの多い場所に設置しない**
火災・感電・故障の原因になります。

●**直射日光の当たる場所や温度の高い場所に設置しない**
内部温度が上がり、火災の原因になります。

⚠注意	
禁止	**●振動・衝撃の多い場所や不安定な場所に設置しない** 落下して、けが・故障の原因になります。 **●この装置を火に入れない** 爆発・火災の原因になります。 **●SFP 拡張ポートに別売の SFP モジュール (PN54021K/PN54023K) 以外実装しない** 火災・感電・故障の原因になります。 対応するSFP拡張モジュールの最新情報は、ホームページにてご確認ください。

⚠注意	
必ず守る	**●付属の電源コード（ 交流 100V 仕様 ）を使う** 感電・誤動作・故障の原因になります。 **●故障時は電源プラグを抜く** 電源を供給したまま長時間放置すると火災の原因になります。 **●必ずアース線を接続する** 感電・誤作動・故障の原因になります。 **●電源コードを電源ポートにゆるみなどがないよう、確実に接続する** 感電や誤動作の原因になります。 **●ステータス LED（ STATUS ）が橙点滅となった場合は、故障のため電源プラグを抜く** 電源を供給したまま長時間放置すると火災の原因になります。 **●ツイストペアポート、SFP 拡張ポート、コンソールポート、SD カードスロット、電源コード掛けブロックで手などを切らないよう注意の上取り扱う**

使用上のご注意

●内部の点検・修理は販売店にご依頼ください。

●商用電源は必ず本装置の近くで、取り扱いやすい場所からお取りください。

●この装置を設置・移動する際は、電源コードを外してください。

●この装置を清掃する際は、電源コードを外してください。

●仕様限界をこえると誤動作の原因となりますので、ご注意ください。

●RJ45 コネクタ（ ツイストペアポート、コンソールポート ）の金属端子やコネクタに接続されたツイストペアケーブルのモジュラプラグの金属端子に触れたり、帯電したものを近づけたりしないでください。静電気により故障の原因になります。

●コネクタに接続されたツイストペアケーブルのモジュラプラグをカーペットなどの帯電するものの上や近辺に放置しないでください。静電気により故障の原因になります。落下など強い衝撃を与えないでください。故障の原因になります。

●以下場所での保管・使用はしないでください。
（ 仕様の環境条件下にて保管・使用をしてください ）
- 水などの液体がかかるおそれのある場所、湿気が多い場所
- ほこりの多い場所、静電気障害のおそれのある場所（ じゅうたんの上など ）
- 直射日光が当たる場所
- 結露するような場所、仕様の環境条件を満たさない高温・低温の場所
- 振動・衝撃が強い場所

●この装置を上下に重ねて置かないでください。また、左右に並べておく場合はすき間を 20mm 以上設けてください。

●ラックマウントする場合は、上下の機器との間隔を 20mm 以上離してお使いください。

●SFP 拡張ポートに別売の SFP モジュール (PN54021K/PN54023K) 以外を実装した場合、動作保証はいたしませんのでご注意ください。対応する SFP 拡張モジュールの最新情報は、ホームページにてご確認ください。

●SD カードスロットに別売のパナソニック製 SD カード以外を実装した場合、動作保証はいたしませんのでご注意ください。また、フォーマットはこの装置で実施してください。

1. お客様の本取扱説明書に従わない操作に起因する損害および本製品の故障・誤動作などの要因によって通信の機会を逸したために生じた損害については、弊社はその責任を負いかねますのでご了承ください。
2. 本書に記載した内容は、予告なしに変更することがあります。
   最新版は弊社ホームページをご覧ください。
3. 万一ご不審な点がございましたら、販売店までご連絡ください。

※ 本文中の社名や商品名は、各社の登録商標または商標です。

この装置は，クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　　ＶＣＣＩ－Ａ

1. はじめに

ZEQUO 2210 は、16 個の 10/100/1000/BASE-T ポート、および 4 組の排他使用可能な 10/100/1000BASE-T ポートおよび SFP 拡張スロットを有する、管理機能付きレイヤ 2 オールギガイーサネットスイッチングハブです。

1.1. 製品の特徴

- ポート 1 ～ 20（ ツイストペアポート ）は、オートネゴシエーションに対応した 10BASE-T/100BASE-TX/1000BASE-T ポートです。設定による速度及び通信モードの切り替えが可能です。ただし、ポート 17 ～ 20 は、半二重モードをサポートしておりません。
  ポート 17 ～ 20 は、SFP 拡張スロットと排他利用にて使用可能です。
- すべてのツイストペアポートがストレート / クロスケーブル自動判別機能を搭載しています。
  端末、ネットワーク機器の区別を意識せず、ストレートケーブルを用いて相互接続できます。
  （ループ障害防止のため、工場出荷時に、ポート 1 ～ 16 は MDI-X 固定に設定されています。）
- SD カード上のファームウェア・設定情報を用いた起動、設定情報の変更・保存、およびファームウェアの変更・保存が可能です。
- 省電力モード (Power Saving Mode) の搭載により、接続状態を自動検知し、電力消費を必要量に抑制します。
- IEEE802.3az(LPI) に対応した省電力型イーサネット (Energy Efficient Ethernet) をサポートしており、リンクアップ時にデータ通信が行われていない場合に省電力状態に移行し、ポートごとに電力消費を抑えることが可能です。
- オートネゴシエーション機能に対応し、10BASE-T、100BASE-TX、1000BASE-T の混在環境に容易に対応できます。また、設定により速度・通信モードの固定が可能です。
- 通信確認のための Ping コマンドを実行することができます。
- 標準MIB (MIB II ,Bridge MIB,RMON 4グループ等)をサポートし、SNMPマネージャからスイッチの管理が行えます。（詳細は付録 A. を参照下さい。）
- ZEQUOASSIST による GUI ベースの簡易設定作業をサポートします。
- アクセスコントロール機能をサポートしており、IP アドレス、MAC アドレス、プロトコル番号、L4 ポート番号などでフィルタリングが可能です。
- スパニングツリープロトコルをサポートし、冗長性のあるシステム構築が可能です。
- IEEE802.1Q のタグ VLAN をサポートしており、最大 4K 個の VLAN が登録可能です。
- IEEE802.1p の QoS 機能をサポートしています。
- IEEE802.3ad のリンクアグリゲーション機能をサポートしており、最大 8 ポート 32 グループまでの構成が可能です。
- リングプロトコルをサポートし、リング構成による冗長化システムの構築が可能です。
- IEEE802.1X の認証機能をサポートし、未登録ユーザによるネットワークアクセスを防止します。
- IGMP Snooping 機能をサポートし、マルチキャストパケットによる帯域の占有を防ぎます。

1.2. 同梱品の確認

開封時に必ず内容物をご確認ください。不足があった場合は、販売店にご連絡ください。

- ZEQUO 2210 本体 1 台
- 取扱説明書 1 冊
- CD-ROM（本取扱説明書を含む）1 枚
- ゴム足 4 個
- 取付金具（1 9インチラックマウント用）2 個
- ねじ（1 9インチラックマウント用）4 本
- ねじ（取付金具と本体接続用）8 本
- ダミー SD カード 1 枚
- 電源コード 1 本

※ 付属の電源コードは AC100V 専用コードです。

1.3. 別売オプション

- PN54021K 1000BASE-SX SFP Module
- PN54023K 1000BASE-LX SFP Module
- PN72001 RJ45-DSub9 ピン コンソールケーブル

1.4. 各部の機能と名称

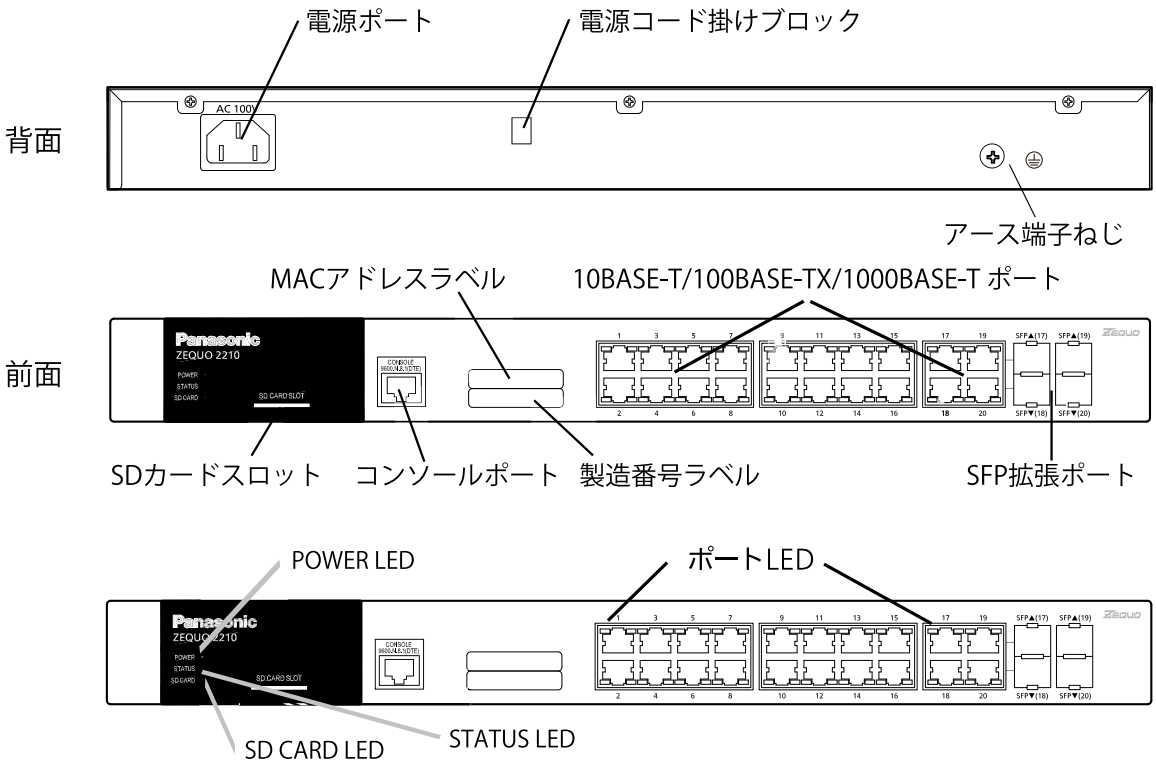


図 1-1 背面、前面、LED

●電源ポート

付属の電源コードを接続し、電源コンセントに接続します。

●電源コード掛けブロック

付属の電源コードを引っ掛けると、電源ポートから電源コードが抜けにくくなります。

●アース端子ねじ

アース線を使用して、アース端子ねじと接地面を接続します。

● SD カードスロット

SD カードを挿入し、設定情報の変更、ファームウェアの変更・保存が可能です。

● 10BASE-T/100BASE-TX/1000BASE-T ポート (ポート 1 ～ 16)

10BASE-T/100BASE-TX/1000BASE-T 端末ハブリピータスイッチングハブなどを接続します。
ツイストペアケーブル(CAT5e以上)のケーブル長は100m以内に収まるように設置してください。

● 10BASE-T/100BASE-TX/1000BASE-T ポート (ポート 17 ～ 20)

10BASE-T/100BASE-TX/1000BASE-T 端末ハブリピータスイッチングハブなどを接続します。
通信モードは全二重モードのみをサポートしており、半二重モードはサポートしていません。
ツイストペアケーブル(CAT5e以上)のケーブル長は100m以内に収まるように設置してください。

● SFP 拡張ポート (ポート 17 ～ 20)

SFP のモジュールを実装できます (ツイストペアポートとの排他利用になります)。
SFP 拡張ポートがリンクした際、自動的に切り替わります。

●コンソールポート

VT100 互換端末等と接続し、本機の設定および管理をします。

通信方式	:	RS-232C	エミュレーションモード	:	VT100
通信速度	:	9,600bps	データ長	:	8 ビット
ストップビット	:	1 ビット	パリティ制御	:	なし
フロー制御	:	なし	通信コネクタ	:	RJ45

コンソールケーブルは、別売オプションの RJ45-DSub9 ピンコンソールケーブル (PN72001) をご使用ください。

1.5. LED の動作

1.5.1. 起動時の LED の動作

本装置に電源を入れると LED が全点灯します。その後、POWER（電源）LED が緑色に点灯、STATUS (ステータス)LED が橙色に点灯しハードウェアの自己診断を実行します。完了すると POWER（電源）LED、STATUS（ステータス）LED ともに緑色に点灯し、スイッチングハブとして動作します。

1.5.2. 動作中の LED の動作

本装置はポート毎に配置されている LED により動作中の各ポートの状態を確認することが可能です。

●システム LED

LED	動作	内容
POWER（電源）LED	緑点灯	電源 ON
	消灯	電源 OFF
STATUS（ステータス）LED	緑点灯	システム正常稼動
	橙点灯	システム起動中
	橙点滅	システム障害
SD CARD LED	緑点灯	SD カード挿入中
	緑点滅	データ読込 / 書込中
	橙点灯	SD カード異常
	消灯	未挿入

● 10/100/1000BASE-T ポート LED(ポート 1 ～ 20)

LED	動作	内容
リンク / 送受信 LED(LINK/ACT.)	緑点灯	1000Mbps 全二重モードでリンクが確立
	緑点滅	1000Mbps 全二重モードでパケットを送受信中
	橙点灯	10/100Mbps でリンクが確立
	橙点滅	10/100Mbps でパケットが送受信中
	消灯	端末未接続

● 1000BASE-X ポート LED(ポート 17 ～ 20)

LED	動作	内容
リンク / 送受信 LED(LINK/ACT.)	緑点灯	1000Mbps 全二重モードでリンクが確立
	緑点滅	1000Mbps 全二重モードでパケットを送受信中
	消灯	端末未接続

2. 設置

2.1. １９インチラックへの設置

付属品の取付金具 2 個とねじ（取付金具と本体接続用 8 本）を取りだし、本装置の横にある 4 つの穴にねじで本機と取付金具を固定してください。
その後、付属品のねじ（19 インチラックマウント用）4 本、またはラックに用意されているねじで、しっかりと本装置をラックに固定してください。

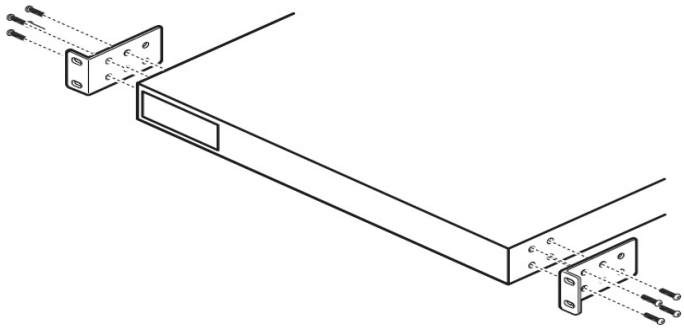


図 2-1　19 インチラックへの設置

また、取付金具へのねじ位置を下図のように変更することで、本装置の前面を 20mm 奥まらせることが可能です。

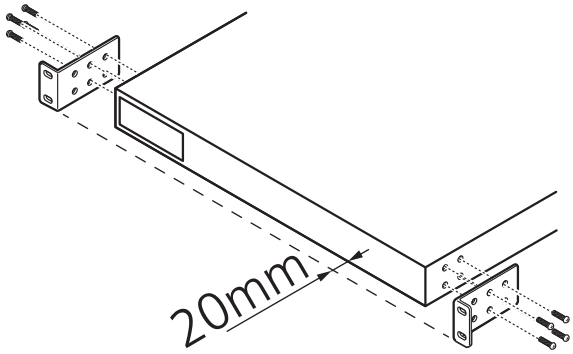


図 2-2　19 インチラックへの設置（20mm 奥）

3. 接続

3.1. ツイストペアポートを使用した接続

●接続ケーブル

接続には、8 極 8 心の RJ45 モジュラプラグ付き、CAT5e 以上に準拠したストレートケーブル（ツイストペアケーブル）をご使用ください。

●ネットワーク構成

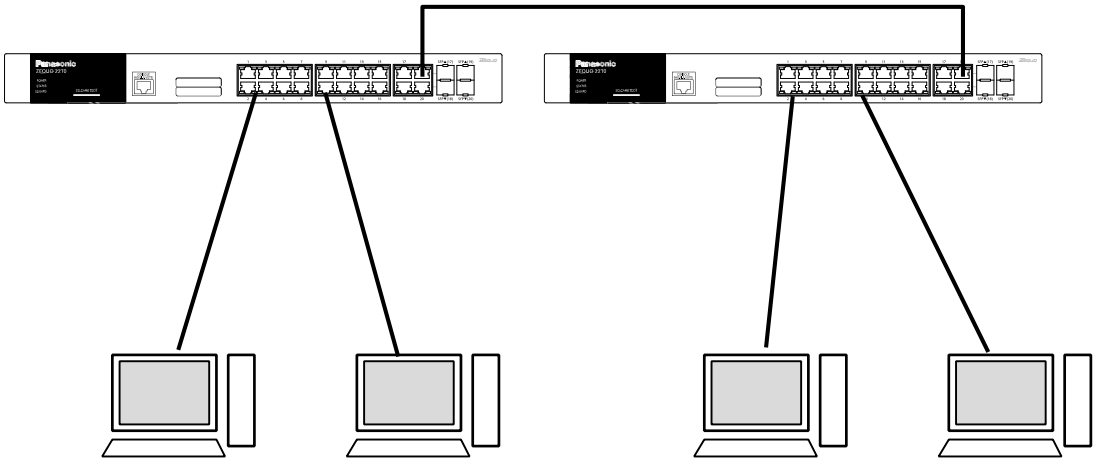


図 3-1　接続構成例

各端末と本装置との間のケーブル長が 100m 以内に収まるように設置してください。オートネゴシエーション機能をもった端末または LAN 機器を接続すると、各ポートは自動的に最適なモードに設定されます。オートネゴシエーション機能を持たない機器または端末を接続すると、本装置は通信速度を自動的に判断し、設定しますが、全 / 半二重は判断できないため、半二重に設定されます。オートネゴシエーション機能をもたない機器または端末を接続する際は、ポートの通信条件を固定するよう設定してください。

ご注意：通信条件を固定に設定した場合は、Auto-MDI/MDI-X 機能は動作しませんので、スイッチ間の接続はクロスケーブルを使用する必要があります。

3.2. SFP 拡張スロットを使用した接続

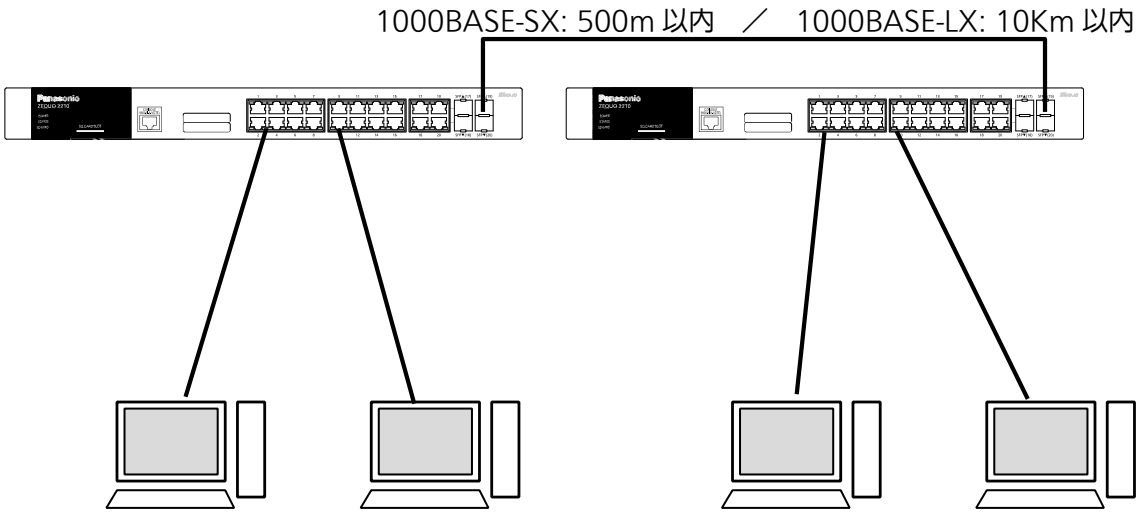


図 3-2 光ファイバケーブル接続例

SFP 拡張スロットへオプションの SFP モジュールを差し込むことにより、光ファイバでの接続が可能です。本製品の工場出荷時状態はツイストペアポートが有効ですが、リンクが確立した際に自動的に SFP 拡張ポートが有効となります。
それぞれ TX ポートは相手側機器の RX ポートへ、RX ポートは相手側機器の TX ポートへ接続してください。

弊社ではオプションとして下記の SFP モジュールを取り扱っています。

- 1000BASE-SX SFP Module (品番：PN54021K)
- 1000BASE-LX SFP Module (品番：PN54023K)

3.3. 電源の接続

添付の電源コードを本体の電源ポートに接続し、電源プラグをコンセントに接続します。100V（50/60Hz）で動作します。
電源スイッチはありません。電源コードを接続すると、電源が投入され、動作を開始します。電源を切る際には電源プラグをコンセントから抜いてください。

4. コマンドラインインターフェースの使用

コマンドラインインターフェース（CLI）とは、本装置の設定および管理をする操作画面です。
本装置のコンソールポートへの VT-100 互換端末等の接続、または telnet 等のリモート接続により CLI を利用できます。
ここでは、CLI の利用方法について以下の内容を説明しています。

- コンソールポートへの接続の概要
- 本装置の IP アドレスの設定方法
- コマンドの使用方法の概要
  - ・コマンドヘルプを表示する “?” コマンド
  - ・パラメータの省略時の動作
  - ・コマンド入力の補完機能、入力履歴の利用
  - ・タイプミス時の動作
- 構文表記のルール
- 利用できる入力編集キー、ページ操作キー

4.1. コンソールポートを介した本装置へのアクセス

本装置のコンソールポートのデフォルト設定は、以下のとおりです。

- 9600 ボー
- パリティなし
- データ長 8 ビット
- ストップビット 1 ビット

VT-100 端末をエミュレート可能なターミナルエミュレータプログラムが動作し、上記のコンソールポート設定を行ったコンピュータを、RJ-45 から RS-232 DB-9 の変換ケーブルで本装置のコンソールポートに接続します。
コンソールポートと管理コンピュータが正しく接続されると、以下の画面が表示されます。

```
                    Zxxx0 Gigabit Ethernet Switch
                      Command Line Interface

                      Firmware: Build 1.0.0.xx

UserName:
```

ユーザ名とパスワードの初期値は共に "manager" です。ログインが成功すると、CLI 入力カーソル **Zxxx0:admin#** が表示されます。これは、あらゆるコマンドを入力するコマンドラインです。

4.2. 本装置の IP アドレスの設定

各装置には、独自の IP アドレスを割り当てる必要があります。このアドレスを用いて、SNMP ネットワークマネージャまたは他の TCP/IP アプリケーション（BOOTP、TFTP など）と通信します。本装置のデフォルト IP アドレスは、0.0.0.0 です。このデフォルト IP アドレスは、ご使用のネットワークアドレス体系に合わせて変更できます。
本装置には、工場出荷時に固有の MAC アドレスが割り当てられています。この MAC アドレスは変更できません。以下に示す初期起動時のコンソール画面上に表示されます。

```
  Boot Procedure                                          V1.0.0.xx
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address    : 00-01-02-03-04-00
  H/W Version    : A1

  Please Wait, Loading V1.0.0.xx Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
  Device Discovery ..........................................  100 %
  Configuration init ........................................  100 %
```

本装置の IP アドレスは、BOOTP または DHCP プロトコルで自動的に設定できます。この場合、本装置に割り当てられたアドレスを把握しておくことが必要です。
コマンドラインプロンプトで、コマンド **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy** を入力します。ここで、一連の **x** は **System** という名前の IP インターフェースに割り当てられた IP アドレスで、一連の **y** は対応するサブネットマスクを表します。
あるいは、**config ipif System ipaddress xxx.xxx.xxx.xxx/z** と入力することもできます。ここで、一連の **x** は **System** という名前の IP インターフェースに割り当てられた IP アドレスで、**z** は対応するサブネット数を CIDR 表記で表したものです。
本装置上の **System** という名前の IP インターフェースに IP アドレスとサブネットマスクを割り当てて、それらを使用して管理端末から本装置の Telnet または Web ベース管理エージェントに接続することができます。

```
Zxxx0:admin# config ipif System ipaddress 10.24.22.100/255.0.0.0
Command: config ipif System ipaddress 10.24.22.100/8

Success.

Zxxx0:admin#
```

上記の実行例では、本装置に IP アドレスとして 10.24.22.100、サブネットマスクとして 255.0.0.0 を割り当てています。システムメッセージ **Success** は、コマンドが正しく実行されたことを示します。これで、Telnet、SNMP MIB ブラウザ、および CLI を介して本装置を設定および管理できるようになります。
CLI には、便利な機能が数多くあります。**?** コマンドを入力すると、トップレベルの全コマンドのリストが表示されます。

```
Zxxx0:admin#?
Command: ?

..
?
cable_diag ports
cd
change drive
clear
clear address_binding dhcp_snoop binding_entry ports
clear address_binding nd_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear dhcpv6 binding
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

コマンド入力時に必須パラメータを指定しなかった場合は、CLI は Next possible completions: というメッセージを表示します。

```
Zxxx0:admin#config account
Command: config account
Next possible completions:
<username>

Zxxx0:admin#
```

この実行例では、パラメータ <username> を指定せずにコマンド config account が入力されています。そのため、CLI はメッセージ Next possible completions: を表示して <username> を入力するよう促します。CLI のどのコマンドもこの機能を備えています。複雑なコマンドの場合は、パラメータプロンプト表示がいくつかの階層にわたって行われます。
また、任意コマンドと 1 つの空白文字を入力した後で、Tab キーを繰り返し押すことで、利用可能なすべてのサブコマンドが順番に表示されます。
コマンドプロンプトで前のコマンドを再入力するには、上矢印キーを押します。コマンドプロンプトに、前のコマンドが表示されます。

```
Zxxx0:admin# config account
Command: config account
Next possible completions:
<username>

Zxxx0:admin# config account
```

上記の実行例では、コマンド config account に必須パラメータ <username> を入力しませんでした。そのため、CLI では Next possible completions: <username> プロンプトを返しています。コマンドプロンプトで前のコマンド（config account）を再入力するために、上矢印キーを押しました。ここで、適切なユーザ名を入力して、config account コマンドを再実行できます。

CLI のすべてのコマンドが、このように動作します。さらに、ヘルププロンプトの構文も本書で示すものと同じです。山括弧 < > は数値または文字列、中括弧 { } はオプションのパラメータまたはパラメータの選択肢、角括弧 [ ] は必須パラメータをそれぞれ示します。
CLI で認識されないコマンドを入力すると、Available commands: プロンプトの下にトップレベルコマンドが表示されます。

```
Zxxx0:admin#the
Available commands:
..                  ?                   cable_diag          cd
                    change              clear               config
copy                create              debug               del
delete              dir                 disable             download
enable              erase               format              login
logout              md                  move                no
ping                ping6               rd                  reboot
reconfig            rename              reset               save
show                telnet              traceroute          traceroute6
upload

Zxxx0:admin#
```

トップレベルコマンドとしては、show または config などがあります。これらのコマンドの多くは、トップレベルコマンドを限定するために 1 つまたは複数のパラメータを要します。これは、show の対象または config の対象の指定に相当します。つまり、対象として指定するのが、後に続くパラメータです。
例えば、パラメータを追加せずに show コマンドを入力した場合、CLI には利用可能な後に続くパラメータがすべて表示されます。

```
Zxxx0:admin#show
Command: show
Next possible completions:
802.1p              802.1x              access_profile      account
accounting          acct_client         arpentry            asymmetric_vlan
attack_log          auth_client         auth_diagnostics
auth_session_statistics                 auth_statistics     authen
authen_enable       authen_login        authen_policy       authentication
authorization       autoconfig          bandwidth_control   boot_file
bpdu_protection     broadcast_ping_reply                    command
command_history     community_encryption                    config
current_config      ddm                 device_status       dhcp_snoop
dnsr                dot1v_protocol_group                    dscp
egress_access_profile                   egress_flow_meter   environment
error               fdb                 filter              flow_meter
gratuitous_arp      gvrp                hol_prevention      host_name
igmp_snooping       ip_source_binding   ip_verify_source    ipif
ipif_ipv6_link_local_auto               iproute             ipv6
ipv6route           jumbo_frame         l2protocol_tunnel   lacp_port
limited_multicast_addr                  link_aggregation    lldp
lldp_med            log                 log_save_timing
log_software_module                     loopback
mac_based_access_control                mac_based_access_control_local
mac_based_vlan      mac_notification    max_mcast_group
mcast_filter_profile                    mirror              mld_snooping
multicast           multicast_fdb       name_server         nlb
packet              per_queue           port                port_group
port_security       port_security_entry                     port_vlan
ports               power_saving        private_vlan        ptp
radius              rcp                 rmon                router_ports
rspan               scheduling          scheduling_mechanism
serial_port         session             snmp                sntp
ssh                 stack_device        stack_information   stacking_mode
storage_media_info                      stp                 subnet_vlan
switch              syslog              system_severity     tech_support
terminal            time                time_range          traffic
traffic_segmentation                    trap                trusted_host
utilization         vlan                vlan_precedence     vlan_trunk
voice_vlan          wac                 wred

Zxxx0:admin#
```

上記の実行例では、show コマンドに対する利用可能な後に続くパラメータがすべて表示されています。次のコマンドプロンプトで上矢印キーを使用して show コマンドに戻り、account パラメータを指定し直しました。それにより、CLI には、本装置で設定されているユーザアカウントが表示されます。

4.3. コマンド構文の記号

本書でのコマンドエントリの記述方法や値と引数の指定方法には、以下の記号を使用しています。コンソールインターフェースからアクセス可能な CLI のオンラインヘルプでも同じ構文を使用します。

NOTE すべてのコマンドで、大文字と小文字が区別されます。テキストの大文字 / 小文字を変更する Caps Lock やその他の不要な機能を無効化してください。

構文	概要
山括弧 < >	変数または値を囲みます。ユーザが変数または値を指定しなければなりません。例えば、構文 **create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}}** では、ユーザはコマンドを入力するときに、**<ipif_name 12>** に IP インターフェース名を、**<vlan_name 32>** に VLAN 名を指定する必要があります。山括弧は入力しないでください。
角括弧 [ ]	必須の値または必須の引数のリストを囲みます。値または引数を 1 つのみ指定する必要があります。例えば、構文 **create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}** では、ユーザはコマンドを入力するときに、admin、operator、power_user、または user のいずれかのレベルのアカウントを指定する必要があります。角括弧は入力しないでください。
垂直バー |	リスト内の複数の項目を区切るのに使用し、その中からいずれか 1 つの項目のみを選択する必要があることを示します。例えば、構文 **reset {[config |system]} {force_agree}** では、ユーザはこのコマンドに config または system のどちらかを選択します。垂直バーは入力しないでください。
中括弧 { }	オプションの値またはオプションの引数のリストを囲みます。1 つ、または、複数の値または引数を指定できます。例えば、構文 **reset {[config | system]} {force_agree}** では、ユーザはこのコマンドに config または system のどちらかを選択します。中括弧は入力しないでください。
括弧 ( )	先行する構文にて中括弧で囲まれた1つまたは複数の値または引数を指定する必要があることを示します。例えば、構文 **config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}(1)** では、ユーザは hops または time またはその両方を指定できます。中括弧に続く「(1)」は、中括弧内の引数または値を 1 つ以上指定する必要があることを示します。括弧は入力しないでください。
ipif <ipif_name 12> metric <value 1-31>	**12** は、IP インターフェース名の最大長を示します。 **1-31** は、メトリック値の有効な範囲を示します。

4.4. 行編集キー

キー	概要
Delete	カーソル下の文字を削除して、行の残りを左にシフトします。
Backspace	カーソルの左の文字を削除して、行の残りを左にシフトします。
Ctrl+R	オンとオフを切り替えます。オンの場合、テキストを挿入して、前のテキストを右にシフトします。
上矢印	前に入力したコマンドを繰り返します。上矢印キーを押すたびに、現在表示中のものより 1 つ前のコマンドが表示されます。これにより、現在のセッションのコマンド履歴をさかのぼって見直すことができます。下矢印キーを押すと、コマンド履歴リストの入力順の古いものから新しいものへ進むことができます。
下矢印	下矢印キーは、現在のセッションで入力したコマンド履歴の次のコマンドを表示します。各コマンドは、入力した順序で表示されます。前のコマンドを見直すには、上矢印キーを使用します。
左矢印	カーソルを左に移動します。
右矢印	カーソルを右に移動します。
Tab	適切なトークンの選択に役立ちます。

show コマンドの出力がページ末尾に到達すると、画面表示が一時停止します。

4.5. 複数ページ表示制御キー

キー	概要
スペース	次のページを表示します。
Ctrl+C	複数のページを表示する場合に、残りのページの表示を停止します。
Esc	複数のページを表示する場合に、残りのページの表示を停止します。
n	次のページを表示します。
p	前のページを表示します。
q	複数のページを表示する場合に、残りのページの表示を停止します。
r	現在表示中のページをリフレッシュします。
a	ページ間で一時停止せずに、残りのページを表示します。
Enter	次の行またはテーブルエントリを表示します。

5. 基本的な管理コマンド

ここでは、本装置の基本的な管理を行うコマンドについて説明しています。

- 本装置の管理を行うユーザのアカウントの作成、編集、表示、削除

  NOTE ユーザアカウントは、最大 8 つ作成できます。

- コンソールに現在ログインしているユーザの表示
- 本装置の電源、温度、ファンの状態の表示と管理
- コンソールポート（シリアルポート）の設定
- 画面のページ送りの一時停止、横幅の設定、画面の消去
- Telnet の利用
- 設定、ログファイルの NV-RAM への保存
- 設定の初期化、再起動
- ログイン、ログアウト

---

create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}
config account <username> {encrypt [plain_text | sha_1] <password>}
show account
delete account <username>
show session
show switch
show environment
config temperature [trap | log] state [enable | disable]
config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}(1)
show serial_port
config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}(1)
enable clipaging
disable clipaging
enable telnet {<tcp_port_number 1-65535>}
disable telnet
save {[config <pathname> | log | all]}
reboot {force_agree}
reset {[config | system]} {force_agree}
login
logout
clear
config terminal width [default | <value 80-200>]
show terminal width
show device_status

5.1. create account

● 概要

このコマンドは、ユーザアカウントを作成します。ユーザ名は 1 ～ 15 文字、パスワードは 0 ～ 15 文字で設定します。最大 8 つのアカウント（admin、operator、user を含む）を作成できます。

● 構文

create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}

● パラメータ

admin	管理者アカウントの名前を指定します。
operator	オペレータアカウントの名前を指定します。
power_user	パワーユーザレベルアカウントを指定します。パワーユーザレベルは、オペレータレベルよりも低く、ユーザレベルよりも高いレベルです。
user	ユーザアカウントの名前を指定します。
<username 15>	15 文字以内のユーザ名を指定します。
encrypt	（オプション）使用する暗号化を指定します。 plain_text パスワードをプレーンテキスト形式で指定します。 sha_1 パスワードを SHA-1 暗号化形式で指定します。 <password> ユーザアカウントのパスワードです。プレーンテキスト形式でのパスワードと暗号化形式でのパスワードは、長さが異なります。プレーンテキスト形式でのパスワードは、0 ～ 15 文字で設定しなければなりません。暗号化形式でのパスワードは、35 バイト長に固定されます。パスワードの大文字と小文字は区別されます。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

管理者レベルのユーザ manager を作成するには：

```
Zxxx0:admin#create account admin manager
Command: create account admin manager

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

Zxxx0:admin#
```

オペレータレベルのユーザ Sales を作成するには：

```
Zxxx0:admin##create account operator Sales
Command: create account operator Sales

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

Zxxx0:admin#
```

ユーザレベルのユーザ System を作成するには：

```
Zxxx0:admin##create account user System
Command: create account user System

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

Zxxx0:admin#
```

5.2. config account

● 概要

コマンドにパスワード情報を指定しなかった場合、ユーザに対してパスワードを対話形式で入力するようプロンプトが表示されます。このとき、ユーザはプレーンテキストパスワードのみ入力できます。コマンドにパスワードを指定した場合、ユーザはプレーンテキスト形式または暗号化形式のどちらでパスワードを入力するかを選択できます。暗号化アルゴリズムは、SHA-1 ベースです。

● 構文

config account <username> {encrypt [plain_text | sha_1] <password>}

● パラメータ

<username>	アカウントの名前を指定します。アカウントは、すでに定義されている必要があります。
encrypt	（オプション）暗号化タイプとして plain_text または sha_1 を指定します。 plain_text パスワードをプレーンテキスト形式で指定します。プレーンテキスト形式でのパスワードは、0 ～ 15 文字で設定しなければなりません。パスワードの大文字と小文字は区別されます。 sha_1 パスワードを SHA-1 暗号化形式で指定します。暗号化形式でのパスワードは、35 バイト長に固定されます。パスワードの大文字と小文字は区別されます。
<password>	パスワードを指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

manager アカウントのユーザパスワードを設定するには：

```
Zxxx0:admin#config account manager
Command: config account manager

Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

Zxxx0:admin#
```

administrator アカウントのユーザパスワードを設定するには：

```
Zxxx0:admin#config account administrator encrypt sha_1
*@&NWoZK3kTsExUV00Ywo1G5jlUKKv+toYg
Command: config account administrator encrypt sha_1
*@&NWoZK3kTsExUV00Ywo1G5jlUKKv+toYg
Success.

Zxxx0:admin#
```

5.3. show account

● 概要

このコマンドを用いて、作成したユーザアカウントを表示します。

● 構文

show account

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

作成したアカウントを表示するには：

```
Zxxx0:admin#show account
Command: show account

Current Accounts:
Username         Access Level
---------------  ------------
System           User
Sales            Operator
manager            Admin

Zxxx0:admin#
```

5.4. delete account

● 概要

このコマンドを用いて、既存のアカウントを削除します。

● 構文

delete account <username>

● パラメータ

<username> 削除するユーザの名前を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。アクティブな管理者ユーザが 1 人存在する必要があります。

● 実行例

ユーザアカウント System を削除するには：

```
Zxxx0:admin#delete account System
Command: delete account System

Success.

Zxxx0:admin#
```

5.5. show session

● 概要

このコマンドを用いて、CLI セッションにログイン中の現行ユーザリストを表示します。

● 構文

show session

● パラメータ

なし

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

現在ログイン中のユーザのアカウントリストを表示するには：

```
Zxxx0:admin#show session
Command: show session

ID  Live Time     From          Level   User
--  ------------  ------------  -----   --------------------
8   23:37:42.270  Serial Port   admin   Anonymous

Total Entries: 1

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

5.6. show switch

● 概要

このコマンドを用いて、スイッチ情報を表示します。

● 構文

show switch

● パラメータ

なし

● 制限

なし

● 実行例

スイッチ情報を表示するには：

```
Zxxx0:admin#show switch
Command: show switch

Product Name                : ZEQUO xxxx
Product Number              : PNxxxxxx
MAC Address                 : xx-xx-xx-xx-xx-xx
IP Address                  : 0.0.0.0 (Manual)
VLAN Name                   : default
Subnet Mask                 : 0.0.0.0
Default Gateway             : 0.0.0.0
Boot PROM Version           : Build V1.0.0.xx
Firmware Version            : Build V1.0.0.xx
Hardware Version            : xx
System Name                 :
System Location             :
System Uptime               : 0 days, 0 hours, 0 minutes, 0 seconds
System Contact              :
Spanning Tree               : Disabled
GVRP                        : Disabled
IGMP Snooping               : Disabled
MLD Snooping                : Disabled
VLAN Trunk                  : Disabled
Telnet                      : Enabled (TCP 23)
SNMP                        : Disabled
SSH Status                  : Disabled
802.1X                      : Disabled
Jumbo Frame                 : Off
CLI Paging                  : Enabled
MAC Notification            : Disabled
Port Mirror                 : Disabled
SNTP                        : Disabled
HOL Prevention State        : Enabled
Syslog Global State         : Disabled
Password Encryption Status  : Disabled
DNS Resolver                : Disabled

Zxxx0:admin#
```

5.7. show environment

● 概要

このコマンドを用いて、本装置の内部電源、外部電源、内部温度ステータスを表示します。

● 構文

show environment

● パラメータ

なし

● 制限

なし

● 実行例

スイッチのハードウェアステータスを表示するには：

```
Zxxx0:admin#show environment
Command: show environment

Internal Power      : Active
External Power      : Fail
Current Temperature(Celsius) :   56
High Warning Temperature Threshold(Celsius) :    79
Low Warning Temperature Threshold(Celsius)  :    11

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

5.8. config temperature

● 概要

このコマンドを用いて、システム内部温度の警告トラップまたはログの状態を設定します。

● 構文

config temperature [trap | log] state [enable | disable]

● パラメータ

trap	警告温度トラップを設定する場合に指定します。
log	警告温度ログを設定する場合に指定します。
state	警告温度イベントに対するトラップまたはログの状態を有効化または無効化します。デフォルトは enable です。 enable 警告温度イベントに対するトラップまたはログの状態を有効化します。 disable 警告温度イベントに対するトラップまたはログの状態を無効化します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

警告温度トラップ状態を有効化するには：

```
Zxxx0:admin#config temperature trap state enable
Command: config temperature trap state enable

Success.

Zxxx0:admin#
```

警告温度ログ状態を有効化するには：

```
Zxxx0:admin#config temperature log state enable
Command: config temperature log state enable

Success.

Zxxx0:admin#
```

5.9. config temperature threshold

● 概要

このコマンドを用いて、警告温度の上限しきい値または下限しきい値を設定します。温度が上限しきい値を超えたとき、または下限しきい値を下回ったときに、本装置でアラームトラップを送信するかログを記録します。

● 構文

config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}(1)

● パラメータ

high	上限しきい値を指定します。上限しきい値は、下限しきい値よりも高い値に設定する必要があります。 <temperature -500-500> 上限しきい値を指定します。この値は、-500 ～ 500 の範囲で指定します。
low	下限しきい値を指定します。 <temperature -500-500> 下限しきい値を指定します。この値は、-500 ～ 500 の範囲で指定します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

警告温度上限しきい値として 80 を設定するには：

```
Zxxx0:admin#config temperature threshold high 80
Command: config temperature threshold high 80

Success.

Zxxx0:admin#
```

5.10. show serial_port

● 概要

このコマンドを用いて、現在のコンソールポート設定を表示します。

● 構文

show serial_port

● パラメータ

なし

● 制限

なし

● 実行例

コンソールポート設定を表示するには：

```
Zxxx0:admin#show serial_port
Command: show serial_port

Baud Rate     : 9600
Data Bits     : 8
Parity Bits   : None
Stop Bits     : 1
Auto-Logout   : 10 mins

Zxxx0:admin#
```

5.11. config serial_port

● 概要

このコマンドを用いて、管理ホストとの通信で使用するシリアルビットレートと、アイドル接続の自動ログアウト時間を設定します。

● 構文

config serial_port {baud_rate [9600 | 19200 | 38400 | 9600] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}(1)

● パラメータ

baud_rate
ボーレート値を指定します。デフォルトのボーレート値は 9600 です。
9600 ボーレートとして 9600 を指定します。
19200
ボーレートとして 19200 を指定します。
38400
ボーレートとして 38400 を指定します。
115200
ボーレートとして 115200 を指定します。

auto_logout
タイムアウト値を指定します。デフォルトのタイムアウトは 10 分です。
never タイムアウトなしを指定します。
2_minutes
アイドル値が 2 分を超えたときに、本装置が自動ログアウトするよう指定します。
5_minutes
アイドル値が 5 分を超えたときに、本装置が自動ログアウトするよう指定します。
10_minutes
アイドル値が 10 分を超えたときに、本装置が自動ログアウトするよう指定します。
15_minutes
アイドル値が 15 分を超えたときに、本装置が自動ログアウトするよう指定します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

ボーレートを設定するには：

```
Zxxx0:admin# config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

Zxxx0:admin#
```

5.12. enable clipaging

● 概要

このコマンドを用いて、show コマンドの出力がページの末尾に到達したときに、画面表示の一時停止を有効化します。デフォルトでは有効に設定されます。

● 構文

enable clipaging

● パラメータ

なし

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

show コマンドの出力がページの末尾に到達したときに画面表示の一時停止を有効化するには：

```
Zxxx0:admin#enable clipaging
Command: enable clipaging

Success.

Zxxx0:admin#
```

5.13. disable clipaging

● 概要

このコマンドを用いて、show コマンドの出力がページの末尾に到達したときに、画面表示の一時停止を無効化します。デフォルトでは有効に設定されます。

● 構文

disable clipaging

● パラメータ

なし

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

show コマンドの出力がページの末尾に到達したときに画面表示の一時停止を無効化するには：

```
Zxxx0:admin#disable clipaging
Command: disable clipaging

Success.

Zxxx0:admin#
```

5.14. enable telnet

● 概要

このコマンドを用いて、Telnet を有効化し、ポート番号を設定します。デフォルトでは有効化され、ポート番号は 23 に設定されます。

● 構文

enable telnet {<tcp_port_number 1-65535>}

● パラメータ

<tcp_port_number 1-65535> （オプション）TCP ポート番号を指定します。TCP ポート番号は、1 ～ 65535 の範囲で指定します。 Telnet プロトコルで通常利用する TCP ポートは、23 です。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

Telnet を有効化してポート番号を設定するには：

```
Zxxx0:admin#enable telnet 23
Command: enable telnet 23

Success.

Zxxx0:admin#
```

5.15. disable telnet

● 概要

このコマンドを用いて、Telnet を無効化します。

● 構文

disable telnet

● パラメータ

なし

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

Telnet を無効化するには：

```
Zxxx0:admin#disable telnet
Command: disable telnet

Success.

Zxxx0:admin#
```

5.16. save

● 概要

このコマンドを用いて、現在の設定またはログを不揮発性 RAM に保存します。パラメータ無しの場合は、現在の設定のみが起動用設定ファイルに保存されます。

● 構文

save {[config <pathname> | log | all]}

● パラメータ

config	（オプション）設定を保存するために指定します。 <pathname> 指定した設定のパス名を指定します。
log	（オプション）ログを保存するために指定します。
all	（オプション）現在アクティブな設定への変更およびログを保存するために指定します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

現在の設定を起動設定ファイルに保存するには：

```
Zxxx0:admin#save
Command: save

Saving all configurations to NV-RAM.......... Done.

Zxxx0:admin#
```

現在の設定を 1 という名前のファイルに保存するには：

```
Zxxx0:admin#save config 1
Command: save config 1

Saving all configurations to NV-RAM.......... Done.

Zxxx0:admin#
```

ログを NV-RAM に保存するには：

```
Zxxx0:admin#save log
Command: save log

Saving all system logs to NV-RAM.............. Done.

Zxxx0:admin#
```

すべての設定およびログを NV-RAM に保存するには：

```
Zxxx0:admin#save all
Command: save all

Saving  configuration and logs to NV-RAM...... Done.

Zxxx0:admin#
```

5.17. reboot

● 概要

このコマンドを用いて、スイッチを再起動します。

● 構文

reboot {force_agree}

● パラメータ

force_agree	（オプション）確認なしに、ただちに reboot コマンドを実行する場合に指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

スイッチを再起動するには：

```
Zxxx0:admin#reboot
Command: reboot

Are you sure you want to proceed with the system reboot?(y/n)
Please wait, the switch is rebooting…
```

5.18. reset

● 概要

このコマンドを用いて、スイッチの設定を工場出荷状態に初期化します。パラメータなしの場合は、スタック、IP アドレス、ユーザアカウント、ログを除くすべての設定を初期化します。

● 構文

reset {[config | system]} {force_agree}

● パラメータ

config	（オプション）スタックの設定を除くすべての設定を初期値にリセットします。保存および再起動は実行されません。
system	（オプション）すべての設定を工場出荷状態に初期化し、再起動を実行します。
force_agree	（オプション）指定すると、確認なしに、ただちに reset コマンドを実行します。

NOTE パラメータを指定しなかった場合は、スタック、IP アドレス、ユーザアカウント、ログを除くすべての設定が初期化されますが、保存はされないため、適宜 save コマンドを実行してください。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

IP アドレスを除く、スイッチのすべてのパラメータをリセットするには：

```
Zxxx0:admin#reset
Command: reset

Are you sure to proceed with system reset except IP address?(y/n)
Success.

Zxxx0:admin#
```

システム構成設定をリセットするには：

```
Zxxx0:admin#reset config
Command: reset config

Are you sure to proceed with system reset?(y/n)
Success.

Zxxx0:admin#
```

すべてのシステムパラメータをリセットし、保存してスイッチを再起動するには：

```
Zxxx0:admin#reset system
Command: reset system

Are you sure to proceed with system reset, save and reboot?(y/n)
Loading factory default configuration… Done.
Saving all configuration to NV-RAM… Done.
Please wait, the switch is rebooting…
```

5.19. login

● 概要

このコマンドを用いて、スイッチにログインします。

● 構文

login

● パラメータ

なし

● 制限

なし

● 実行例

スイッチにログインするには：

```
Zxxx0:admin#login
Command: login

UserName:
```

5.20. logout

● 概要

このコマンドを用いて、スイッチからログアウトします。

● 構文

logout

● パラメータ

なし

● 制限

なし

● 実行例

スイッチからログアウトするには：

```
Zxxx0:admin#logout
Command: logout

***********
* Logout *
***********


                          Zxxx0 Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 1.0.0.xx

UserName:
```

5.21. clear

● 概要

このコマンドを用いて、端末画面をクリアします。

● 構文

clear

● パラメータ

なし

● 制限

なし

● 実行例

端末画面をクリアするには：

```
Zxxx0:admin#clear
Command: clear
```

5.22. config terminal width

● 概要

このコマンドを用いて、端末画面幅を設定します。

● 構文

config terminal width [default | <value 80-200>]

● パラメータ

default	デフォルトの端末画面幅値を指定します。
<value 80-200>	端末画面幅の値として 80 ～ 200 文字を指定します。初期値は 80 です。

● 制限

なし

● 実行例

端末幅を設定するには：

```
Zxxx0:admin#config terminal width 90
Command: config terminal width 90

Success.

Zxxx0:admin#
```

5.23. show terminal width

● 概要

このコマンドを用いて、端末画面幅の現在の設定を表示します。

● 構文

show terminal width

● パラメータ

なし

● 制限

なし

● 実行例

端末幅の現在の設定を表示するには：

```
Zxxx0:admin#show terminal width
Command: show terminal width

Global terminal width     : 80
Current terminal width    : 80

Zxxx0:admin#
```

5.24. show device_status

● 概要

このコマンドは、システムの電源およびファンの現在のステータスを表示します。

● 構文

show device_status

● パラメータ

なし

● 制限

なし

● 実行例

装置のステータスを表示するには：

```
Zxxx0:admin# show device_status
Command: show device_status

Unit 1:
    Internal Power: Active
    Right Fan     : OK

Zxxx0:admin#
```

6. アクセス認証コントロールコマンド

ここでは、設定や管理の際に本装置へアクセスするための認証設定を行うコマンドについて説明しています。

enable password encryption
disable password encryption
enable authen_policy
disable authen_policy
show authen_policy
create authen_login method_list_name <string 15>
config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}
delete authen_login method_list_name <string 15>
show authen_login [default | method_list_name <string 15> | all]
create authen_enable method_list_name <string 15>
config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local _enable | none}
delete authen_enable method_list_name <string 15>
show authen_enable [default | method_list_name <string 15> | all]
config authen application [console | telnet | ssh | all] [login | enable] [default| method_list_name <string 15>]
show authen application
create authen server_group <string 15>
config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group <string 15>
show authen server_group {<string 15>}
create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}
config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}
delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
show authen server_host
config authen parameter response_timeout <int 0-255>
config authen parameter attempt <int 1-255>
show authen parameter
enable admin
config admin local_enable
config accounting service [network | shell | system] state [enable {[radius_only | method_list_name <string 15> | default_method_list]} | disable]
show accounting service

6.1. enable password encryption

● 概要

ユーザアカウント設定情報は設定ファイルに格納されます。本コマンドによりパスワードの暗号化を有効にした場合はパスワードが暗号化された上で保存され、無効の場合はプレーンテキストで保存されます。
パスワードの暗号化を有効にする前にアカウントが作成されている場合は、全てのアカウントのパスワードが自動的に暗号化されます。

NOTE 暗号化されたパスワードは、プレーンテキストに復号することはできません。

● 構文

enable password encryption

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

パスワードの暗号化を有効にするには：

```
Zxxx0:admin#enable password encryption
Command: enable password encryption

Success.

Zxxx0:admin#
```

6.2. disable password encryption

● 概要

ユーザアカウント設定情報は設定ファイルに格納されます。本コマンドによりパスワードの暗号化を無効にした場合はパスワードがプレーンテキストで保存され、有効の場合は暗号化された上で保存されます。

NOTE 一度暗号化されたパスワードは、本コマンドで暗号化を無効にしても元のプレーンテキストへ復号することはできません。

● 構文

disable password encryption

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

パスワードの暗号化を無効にするには：

```
Zxxx0:admin#disable password encryption
Command: disable password encryption

Success.

Zxxx0:admin#
```

6.3. enable authen_policy

● 概要

システムのアクセス認証ポリシーを有効にします。認証が有効な場合は、ユーザログインや管理者レベル昇格のための認証方式リストが選択されます。

● 構文

enable authen_policy

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

システムアクセス認証ポリシーを有効にするには：

```
Zxxx0:admin#enable authen_policy
Command: enable authen_policy

Success.

Zxxx0:admin#
```

6.4. disable authen_policy

● 概要

システムのアクセス認証ポリシーを無効にします。

● 構文

disable authen_policy

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

システムアクセス認証ポリシーを無効にするには：

```
Zxxx0:admin#disable authen_policy
Command: disable authen_policy

Success.

Zxxx0:admin#
```

6.5. show authen_policy

● 概要

このコマンドを用いて、アクセス認証ポリシーの状態を表示します。

● 構文

show authen_policy

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

システムアクセス認証ポリシーの状態を表示するには：

```
Zxxx0:admin#show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

Zxxx0:admin#
```

6.6. create authen_login method_list_name

● 概要

このコマンドを用いて、ユーザログイン用の認証方式リストを作成します。認証方式リストは最大 8 個まで作成することができます。

● 構文

create authen_login method_list_name <string 15>

● パラメータ

<string 15> リスト名を 15 文字以内で指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

認証方式リスト login_list_1 を作成するには：

```
Zxxx0:admin#create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

Zxxx0:admin#
```

6.7. config authen_login

● 概要

このコマンドを用いて、ユーザログインのための認証方式リストの設定を行います。
認証方式リストが TACACS+、TACACS、ローカルの順番で登録されている場合、ログイン時の認証要求はまずはじめに TACACS+ サーバグループ内の最初の登録ホストへ送信され、このホストからの応答がない場合は次のホストへ送信されます。全ての TACACS+ サーバグループのホストから応答がない場合は TACACS グループへ遷移し、同様に全ての TACACS グループ内のホストから応答がない場合はローカルへ、と認証要求先が遷移します。
TACACS/XTACACS/TACACS+/RADIUS などの遠隔認証を用いて本装置にログインした場合は、ユーザレベル権限のみ割り当てられます。管理者レベルに昇格するには、enable admin コマンドを実行してください。ローカルアカウントにてログインした場合は、アカウント作成時の権限に依存します。

● 構文

config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}

● パラメータ

default	工場出荷時の認証方式を設定します。
method_list_name	ユーザ定義の認証方式リスト名を指定します。 <string 15> 認証方式名を 15 文字以内で入力します。
method	認証方式を指定します。 tacacs （オプション）ビルトイングループ ”tacacs” を指定します。 xtacacs （オプション）ビルトイングループ ”xtacacs” を指定します。 tacacs+ （オプション）ビルトイングループ ”tacacs+” を指定します。 radius （オプション）ビルトイングループ ”radius” を指定します。 server_group （オプション）ユーザ定義のグループ名を指定します。 <string 15> サーバグループリスト名を 15 文字以内で入力します。 local （オプション）ローカルアカウントデータベースを指定します。 none （オプション）認証なしに指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

ユーザ定義のサーバグループに対する認証方式リストを設定するには：

```
Zxxx0:admin#config authen_login method_list_name login_list_1 method tacacs+
tacacs local
Command: config authen_login method_list_name login_list_1 method tacacs+ tacacs
local

Success.

Zxxx0:admin#
```

6.8. delete authen_login method_list_name

● 概要

このコマンドを用いて、ユーザ定義の認証方式リストの削除をします。

● 構文

delete authen_login method_list_name <string 15>

● パラメータ

<string 15> ユーザ定義の認証方式リスト名を 15 文字以内で入力します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

ユーザ定義の認証方式リスト名を削除するには：

```
Zxxx0:admin#delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

Zxxx0:admin#
```

6.9. show authen_login

● 概要

このコマンドを用いて、ユーザの認証方式の設定を表示します。

● 構文

show authen_login [default | method_list_name <string 15> | all]

● パラメータ

default	認証方式リスト名を 15 文字以内で入力します。
method_list_name ユーザ定義の認証方式リスト名を指定します。 <string 15> 認証方式リスト名を 15 文字以内で入力します。	
all	全てのログイン認証方式を表示します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

ユーザ定義の認証方式リストを表示するには：

```
Zxxx0:admin#show authen_login method_list_name login_list_1
Command: show authen_login method_list_name login_list_1

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
login_list_1      1         tacacs+          Built-in Group
                  2         tacacs           Built-in Group
                  3         mix_1            User-defined Group
                  4         local            Keyword

Zxxx0:admin#
```

6.10. create authen_enable method_list_name

● 概要

このコマンドを用いて、管理者レベル昇格用認証方式リストを作成します。

● 構文

create authen_enable method_list_name <string 15>

● パラメータ

<string 15> ユーザ認証方式リスト名を 15 文字以内で入力します。

● 制限

このコマンドは、管理者レベルのみ実行できます。

● 実行例

管理者レベル昇格用のユーザ定義認証方式リストを作成するには：

```
Zxxx0:admin# create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1

Success.

Zxxx0:admin#
```

6.11. config authen_enable

● 概要

このコマンドを用いて、管理者レベル昇格用認証方式リストの設定を行います。

● 構文

config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local _enable | none}

● パラメータ

default	工場出荷時の認証方式を設定します。
method_list_name	ユーザ定義の認証方式リスト名を指定します。 <string 15> 認証方式リスト名を 15 文字以内で入力します。
method	認証方式を指定します。 tacacs （オプション）ビルトイングループ ”tacacs” を指定します。 xtacacs （オプション）ビルトイングループ ”xtacacs” を指定します。 tacacs+ （オプション）ビルトイングループ ”tacacs+” を指定します。 radius （オプション）ビルトイングループ ”radius” を指定します。 server_group （オプション）ユーザ定義のサーバグループリスト名を指定します。 <string 15> サーバグループリスト名を 15 文字以内で入力します。 local_enable （オプション）ローカルアカウントデータベースを指定します。 none （オプション）認証なしに指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

ユーザ定義のサーバグループに対する認証方式リストを設定するには：

```
Zxxx0:admin#config authen_enable method_list_name enable_list_1 method tacacs+
tacacs local
Command: config authen_enable method_list_name enable_list_1 method tacacs+ tacacs
local

Success.

Zxxx0:admin#
```

6.12. delete authen_enable method_list_name

● 概要

このコマンドを用いて、管理者レベル昇格用認証方式リストを削除します。

● 構文

delete authen_enable method_list_name <string 15>

● パラメータ

<string 15> ユーザ認証方式リスト名を 15 文字以内で入力します。

● 制限

このコマンドは、管理者レベルのみ実行できます。

● 実行例

管理者レベル昇格用のユーザ定義認証方式リストを削除するには：

```
Zxxx0:admin# delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

Zxxx0:admin#
```

6.13. show authen_enable

● 概要

このコマンドを用いて、管理者レベル昇格用認証方式の設定を表示します。

● 構文

show authen_login [default | method_list_name <string 15> | all]

● パラメータ

default	認証方式リスト名を 15 文字以内で入力します。
method_list_name ユーザ定義の認証方式リスト名を指定します。 <string 15> 認証方式リスト名を 15 文字以内で入力します。	
all	全てのログイン認証方式を表示します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

管理者レベル昇格用認証方式リストを表示するには：

```
Zxxx0:admin#show authen_enable method_list_name enable_list_1
Command: show authen_enable method_list_name enable_list_1

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
enable_list_1     1         local_enable     Keyword

Zxxx0:admin#
```

6.14. config authen application

● 概要

このコマンドを用いて、ログイン方法ごとの認証方式の設定を行います。

● 構文

config authen application [console | telnet | ssh | all] [login | enable] [default | method_list_name <string 15>]

● パラメータ

console	コンソールを指定します。
telnet	Telnet を指定します。
ssh	SSH を指定します。
all	コンソール、Telnet、SSH 全てを指定します。
login	ユーザレベルの認証方式を指定します。
enable	管理者レベルの認証方式を指定します。
default	工場出荷時設定を指定します。
method_list_name ユーザ定義の認証方式リスト名を指定します。 <string> ユーザ定義の認証方式リスト名を 15 文字以内で入力します。	

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

Telnet のログイン方式を設定するには：

```
Zxxx0:admin#config authen application telnet login method_list_name login_list_1
Command: config authen application telnet login method_list_name login_list_1

Success.

Zxxx0:admin#
```

6.15. show authen application

● 概要

このコマンドを用いて、ユーザレベルおよび管理者レベルのログイン方式一覧を表示します。

● 構文

show authen application

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

ログイン方式一覧を表示するには：

```
Zxxx0:admin#sshow authen application
Command: show authen application

Application  Login Method List  Enable Method List
-----------  -----------------  ------------------
Console      default            default
Telnet       default            default
SSH          default            default

Zxxx0:admin#
```

6.16. create authen server_group

● 概要

このコマンドを用いて、ユーザ定義のサーバーグループを作成します。ビルトインのサーバーグループを含め最大 8 グループまで作成でき、1 グループあたり最大 8 ホストまで登録が可能です。

● 構文

create authen server_group <string 15>

● パラメータ

<string 15> サーバーグループ名を 15 文字以内で入力します。

● 制限

このコマンドは、管理者レベルのみ実行できます。

● 実行例

管理者レベル昇格用のユーザ定義認証方式リストを削除するには：

```
Zxxx0:admin# create authen server_group mix_1
Command: create authen server_group mix_1

Success.

Zxxx0:admin#
```

6.17. config authen server_group

● 概要

このコマンドを用いて、認証サーバグループ内の認証サーバの追加と削除を行います。

● 構文

config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

● パラメータ

server_group	
	認証方式を指定します。
	tacacs
	ビルトイングループ ”tacacs” を指定します。
	xtacacs
	ビルトイングループ ”xtacacs” を指定します。
	tacacs+
	ビルトイングループ ”tacacs+” を指定します。
	radius
	ビルトイングループ ”radius” を指定します。
	<string 15>
	サーバグループリスト名を 15 文字以内で入力します。
add	サーバーグループへサーバホストを追加します。
delete	サーバーグループからサーバホストを削除します。
server_host	
	サーバホストの IP アドレスを指定します。
	<ipaddr>
	サーバホストの IP アドレスを入力します。
protocol	認証プロトコルを指定します。
	tacacs
	TACACS 認証を指定します。
	xtacacs
	XTACACS 認証を指定します。
	tacacs+
	TACACS+ 認証を指定します。
	radius
	RADIUS 認証を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

サーバグループに認証サーバホストを追加するには：

```
Zxxx0:admin#config authen server_group mix_1 add server_host 10.1.1.222 protocol
tacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol
tacacs+

Success.

Zxxx0:admin#
```

6.18. delete authen server_group

● 概要

このコマンドを用いて、ユーザ定義の認証サーバグループを削除します。

● 構文

delete authen server_group <string 15>

● パラメータ

<string 15> サーバグループ名を 15 文字以内で入力します。

● 制限

このコマンドは、管理者レベルのみ実行できます。

● 実行例

管理者レベル昇格用のユーザ定義認証方式リストを削除するには：

```
Zxxx0:admin# delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

Zxxx0:admin#
```

6.19. show authen server_group

● 概要

このコマンドを用いて、認証サーバグループの設定を表示します。

● 構文

show authen server_group {<string 15>}

● パラメータ

<string 15> 認証方式リスト名を 15 文字以内で入力します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

認証サーバグループの設定を表示するには：

```
Zxxx0:admin#show authen server_group
Command: show authen server_group

Group Name       IP Address       Protocol
---------------  ---------------  --------
mix_1            10.1.1.222       TACACS+
                 10.1.1.223       TACACS
radius           10.1.1.224       RADIUS
tacacs           10.1.1.225       TACACS
tacacs+          10.1.1.226       TACACS+
xtacacs          10.1.1.227       XTACACS

Total Entries : 5

Zxxx0:admin#
```

6.20. create authen server_host

● 概要

このコマンドを用いて、認証サーバホストの作成を行います。サーバホストは最大 16 個まで登録が可能です。

● 構文

create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

● パラメータ

<ipaddr>	IP アドレスを指定します。
protocol	認証プロトコルを指定します。 tacacs TACACS 認証を指定します。 xtacacs XTACACS 認証を指定します。 tacacs+ TACACS+ 認証を指定します。 radius RADIUS 認証を指定します。
port	（オプション）認証プロトコル用のポート番号を指定します。 初期値は TACACS/XTACACS/TACACS+ が 49、RADIUS が 1812 です。 <int 1-65535> 認証プロトコル用のポート番号を 1-65535 の値で指定します。
key	（オプション）TACACS+ および RADIUS 認証のキーを指定します。入力がない場合は暗号化はされません。TACACS および XTACACS では使用されません。 <key_string 254> 認証キーを英数字 254 文字以内で指定します。 none 暗号化を行わないよう指定します。
timeout	（オプション）サーバ応答の待ち時間を指定します。初期値は 5 秒です。 <int 1-255> タイムアウトを 1-255 秒の間で指定します。
retransmit	（オプション）再送信回数を指定します。初期値は 2 回です。TACACS+ では使用されません。 <int 1-20> 再送信回数を 1-20 回の間で指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

TACACS+ の認証サーバを追加し、ポート番号を 15555、タイムアウトを 10 秒に設定するには：

```
Zxxx0:admin#create authen server_host 10.1.1.222 protocol tacacs+ port 15555
timeout 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555 timeout
10

Key is empty for TACACS+ or RADIUS.
Success.

Zxxx0:admin#
```

6.21. config authen server_host

● 概要

このコマンドを用いて、認証サーバホストの設定を行います。

● 構文

config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

● パラメータ

<ipaddr>	IP アドレスを指定します。
protocol	認証プロトコルを指定します。 tacacs TACACS 認証を指定します。 xtacacs XTACACS 認証を指定します。 tacacs+ TACACS+ 認証を指定します。 radius RADIUS 認証を指定します。
port	（オプション）認証プロトコル用のポート番号を指定します。 初期値は TACACS/XTACACS/TACACS+ が 49、RADIUS が 1812 です。 <int 1-65535> 認証プロトコル用のポート番号を 1-65535 の値で指定します。
key	（オプション）TACACS+ および RADIUS 認証のキーを指定します。入力がない場合は暗号化はされません。TACACS および XTACACS では使用されません。 <key_string 254> 認証キーを英数字 254 文字以内で指定します。 none 暗号化を行わないよう指定します。
timeout	（オプション）サーバ応答の待ち時間を指定します。初期値は 5 秒です。 <int 1-255> タイムアウトを 1-255 秒の間で指定します。
retransmit	（オプション）再送信回数を指定します。初期値は 2 回です。TACACS+ では使用されません。 <int 1-20> 再送信回数を 1-20 回の間で指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

TACACS+ 認証サーバの認証キーを設定するには：

```
Zxxx0:admin#config authen server_host 10.1.1.222 protocol tacacs+ key "This is a
secret."
Command: config authen server_host 10.1.1.222 protocol tacacs+ key "This is a
secret."

Key is empty for TACACS+ or RADIUS.
Success.

Zxxx0:admin#
```

6.22. delete authen server_host

● 概要

このコマンドを用いて、認証サーバホストの削除を行います。

● 構文

delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

● パラメータ

<ipaddr>	IP アドレスを指定します。
protocol	認証プロトコルを指定します。 tacacs TACACS 認証を指定します。 xtacacs XTACACS 認証を指定します。 tacacs+ TACACS+ 認証を指定します。 radius RADIUS 認証を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

認証サーバホストを削除するには：

```
Zxxx0:admin#delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

Zxxx0:admin#
```

6.23. show authen server_host

● 概要

このコマンドを用いて、認証サーバホストの設定を表示します。

● 構文

show authen server_host

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

認証サーバホストの設定を表示するには：

```
Zxxx0:admin#show authen server_host
Command: show authen server_host

IP Address       Protocol  Port   Timeout  Retransmit  Key
---------------  --------  -----  -------  ----------  -------------------------
10.1.1.222       TACACS+   15555  10       ------      This is a secret.

Total Entries : 1

Zxxx0:admin#
```

6.24. config authen parameter response_timeout

● 概要

このコマンドを用いて、コンソール /Telnet/SSH からの入力待ち時間の設定を行います。

● 構文

config authen parameter response_timeout <int 0-255>

● パラメータ

<iint 0-255> コンソール /Telnet/SSH からの入力待ち時間を 0-255 秒の間で指定します。0 はタイムアウトなしを表します。初期値は 30 秒です。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

入力待ち時間を 60 秒に設定するには：

```
Zxxx0:admin#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

Zxxx0:admin#
```

6.25. config authen parameter attempt

● 概要

このコマンドを用いて、コンソール /Telnet/SSH からのログインまたは管理者レベル昇格の際のログイン失敗許容回数の設定を行います。

● 構文

config authen parameter attempt <int 1-255>

● パラメータ

<iint 1-255>
コンソール/Telnet/SSHからのログインまたは管理者レベル昇格の際のログイン失敗許容回数を 1-255 の間で指定します。初期値は 3 回です。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

ログイン失敗許容回数を 9 回に設定するには：

```
Zxxx0:admin#config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

Zxxx0:admin#
```

6.26. show authen parameter

● 概要

このコマンドを用いて、認証のパラメータを表示します。

● 構文

show authen parameter

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

認証のパラメータを表示するには：

```
Zxxx0:admin#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

Zxxx0:admin#
```

6.27. enable admin

● 概要

このコマンドを用いて、認証サーバを利用した管理者レベルへの昇格を行います。管理者レベル未満のユーザが本コマンドを実行することにより、TACACS、XTACACS、TACACS+、ユーザ定義のサーバーグループ、local_enable, none によるユーザ認証が行われます。
TACACS、XTACACS、RADIUS を使用する場合は、事前に認証サーバへユーザー名を「enable」としたアカウントの作成が必要です。
本コマンドはアクセス認証ポリシーが無効の場合は実行できません。

● 構文

enable admin

● パラメータ

なし

● 制限

なし

● 実行例

管理者レベルに昇格するには：

```
Zxxx0:oper#enable admin
Command: enable admin

PassWord:*****
Success.

Zxxx0:admin#
```

6.28. config admin local_enable

● 概要

このコマンドを用いて、管理者レベルへの昇格に必要な local enable パスワードの設定を行います。管理者レベル昇格方法を ”local_enable” に指定した場合に必要です。
このコマンドで local enable パスワードを設定しない場合は、管理者レベル昇格を行うごとにプレーンテキストでのパスワード入力が必要です。

● 構文

config admin local_enable

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

local enable パスワードを設定するには：

```
Zxxx0:oper#config admin local_enable
Command: config admin local_enable

Enter the old password:
Enter the case-sensitive new password:*****
Enter the new password again for confirmation:*****
Success.

Zxxx0:oper#
```

6.29. config accounting service

● 概要

このコマンドを用いて、RADIUS アカウンティングサービスの設定を行います。

● 構文

config accounting service [network | shell | system] state [enable | disable]

● パラメータ

network	802.1XおよびWACでのRADIUSアカウンティングサービスを指定します。工場出荷時は無効です。
shell	コンソール、Telnet、SSH によるこの装置へのログインの際の RADIUS アカウンティングサービスを指定します。初期値は無効です。
system	設定初期化及び再起動実行時の RADIUS アカウンティングサービスを指定します。初期時は無効です。
state	enable RADIUS アカウンティングサービスを有効に指定します。 disable RADIUS アカウンティングサービスを無効に指定します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

ログイン用の RADIUS アカウンティングサービスを有効にするには：

```
Zxxx0:admin#config accounting service shell state enable
Command: config accounting service shell state enable

Success.

Zxxx0:admin#
```

6.30. show accounting service

● 概要

このコマンドを用いて、RADIUS アカウンティングサービスの状態を表示します。

● 構文

show accounting service

● パラメータ

なし

● 制限

なし

● 実行例

RADIUS アカウンティングサービスの設定を表示するには：

```
Zxxx0:admin#show accounting service
Command: show accounting service

Accounting State
-------------------
Network : Disabled
Shell   : Disabled
System  : Disabled

Zxxx0:admin#
```

7. 802.1X コマンド

IEEE 802.1X とは、クライアントがネットワークに接続する際にユーザ認証を行い、登録されていないクライアントのネットワークへの接続を遮断するしくみです。不正なユーザや機器の接続を防止し、情報資産のセキュリティを保護します。

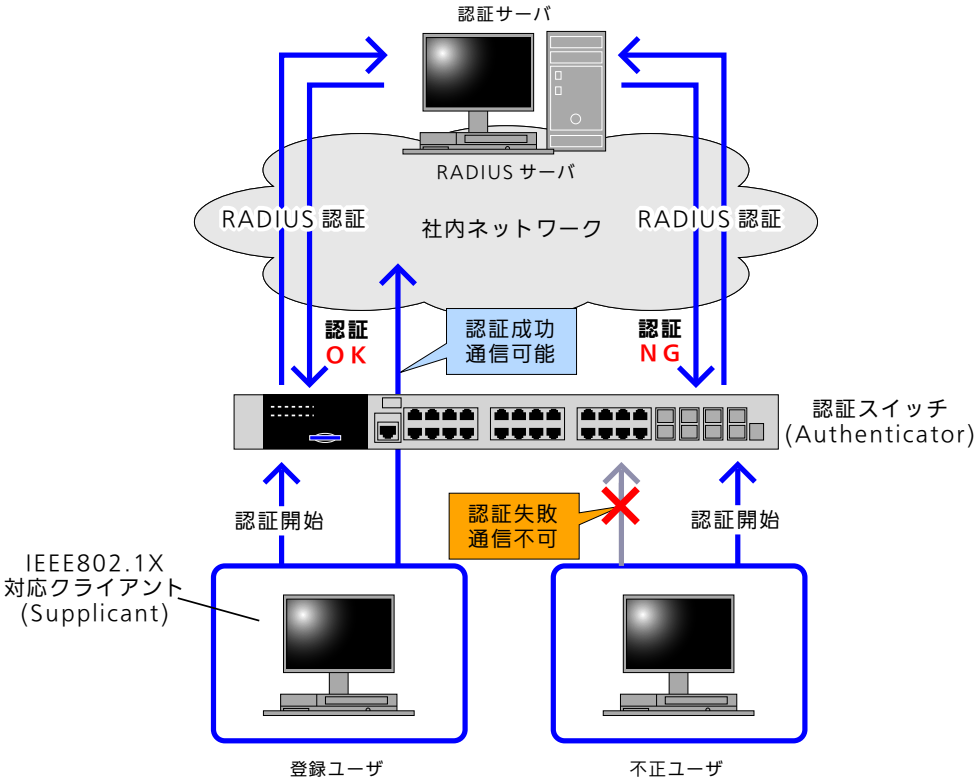


図 7-1　IEEE 802.1X の概略

IEEE 802.1X の認証を利用するには、上図のように、クライアント、認証スイッチ、認証サーバが必要となります。

- クライアントには、IEEE 802.1X 準拠のソフトウェアが必要です（IEEE 802.1X 対応のクライアントは Supplicant と呼ばれます）。クライアントは、ネットワークへの接続時に認証要求を行い、承認されると、ネットワークに接続できるようになります。
- 認証スイッチは、クライアントと認証サーバの認証プロセスの仲介を行います。未承認のクライアントに対してはネットワークへの接続を遮断します（認証スイッチは Authenticator とも呼ばれます）。本製品では、ポート毎に認証の有効／無効、認証に関する設定を行えます。
- 認証サーバには、通常 RADIUS サーバを使用します。登録されているユーザからの認証要求に対してのみ承認を与えます。認証サーバは認証スイッチに 3 台まで登録できます。

NOTE　認証スイッチ内のローカルデータベースにユーザを登録し、RADIUS サーバの代わりに、または RADIUS サーバのフェイルオーバ対応として利用することもできます。

● ポートベース認証と MAC ベース認証

認証スイッチのポートにクライアントをどのように接続するかにより、認証方法を変える必要があります。本装置では、ポートベース認証と MAC ベースの認証のいずれかを選択できます。

- **ポートベース認証**：クライアントが接続されたポートに対して認証します。
- **MAC ベース認証**：接続したクライアントの MAC アドレスに基づいて認証します。認証スイッチの 1 つのポートで複数のクライアントが通信する環境（例：島ハブを利用している場合など）でも認証できます。1 ポートにつき 448 個までの MAC アドレスを登録できます。

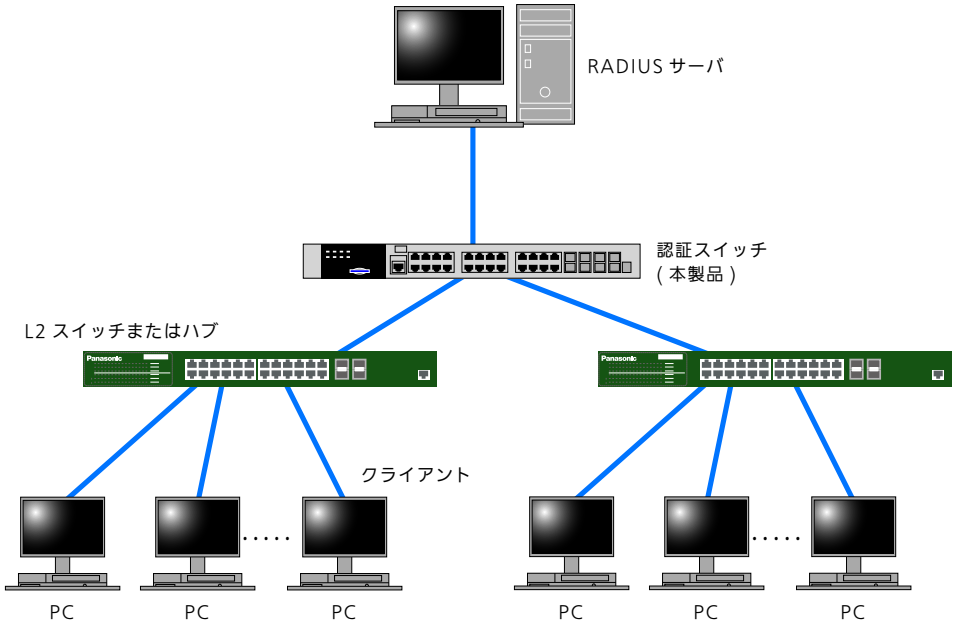


図 7-2　島ハブでの認証

NOTE　島ハブでの認証を行うには、島ハブにあたるスイッチに EAP フレーム透過機能が必要となります。EAP フレームとは認証プロセスで使用される通信データのことです。EAP フレーム透過機能に未対応のスイッチを経由して接続している場合、EAP フレームが破棄され、認証が行われません（本製品は、EAP フレーム透過機能に対応しています）。

● ゲスト VLAN

IEEE 802.1X とゲスト VLAN の機能を組み合わせれば、未認証のクライアントに対して、通信を完全に遮断するのではなく、インターネットへの接続のみを認証するなど、制限された接続を提供することができます。

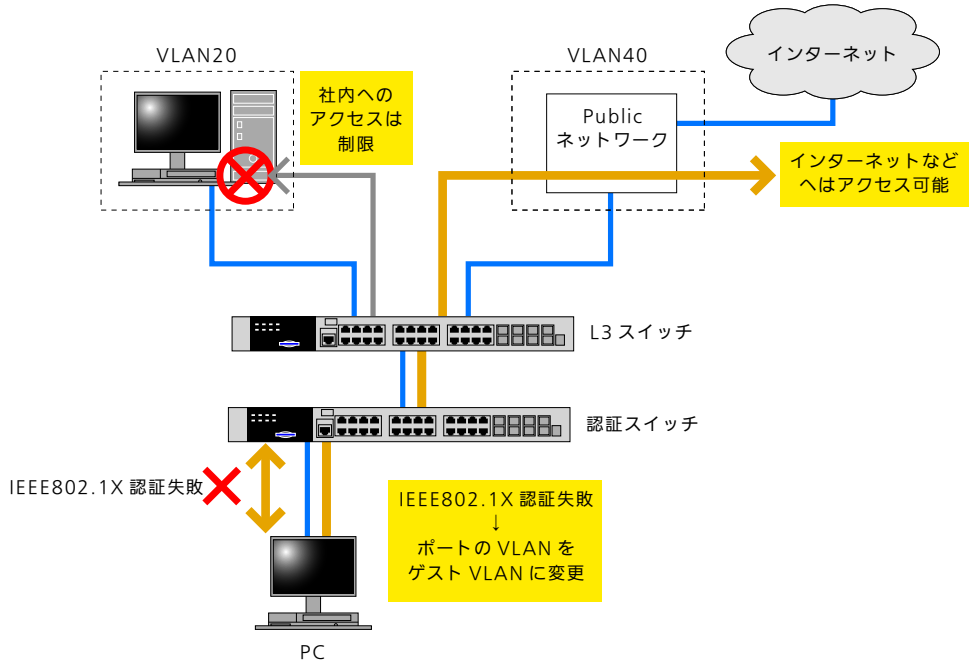


図 7-3　ゲスト VLAN での接続

NOTE　ゲスト VLAN に割り当てられる VLAN は 1 つのみです。

● IEEE 802.1X を利用したダイナミック VLAN

静的 VLAN では、ポート毎に接続先の VLAN が固定となります。これに対し、ダイナミック VLAN では、接続するポートによらず、クライアントの MAC アドレス等の情報に基づき、接続先の VLAN を決定します。

ダイナミック VLAN を実現するにはいくつかの方式がありますが、IEEE802.1X の RADIUS サーバの情報を利用してダイナミック VLAN を構築することができます。RADIUS サーバにクライアントの VLAN 情報を登録していると、認証の際、VLAN の情報も取得し、どのポートからの接続でもクライアントの所属する VLAN へ接続できるようになります。

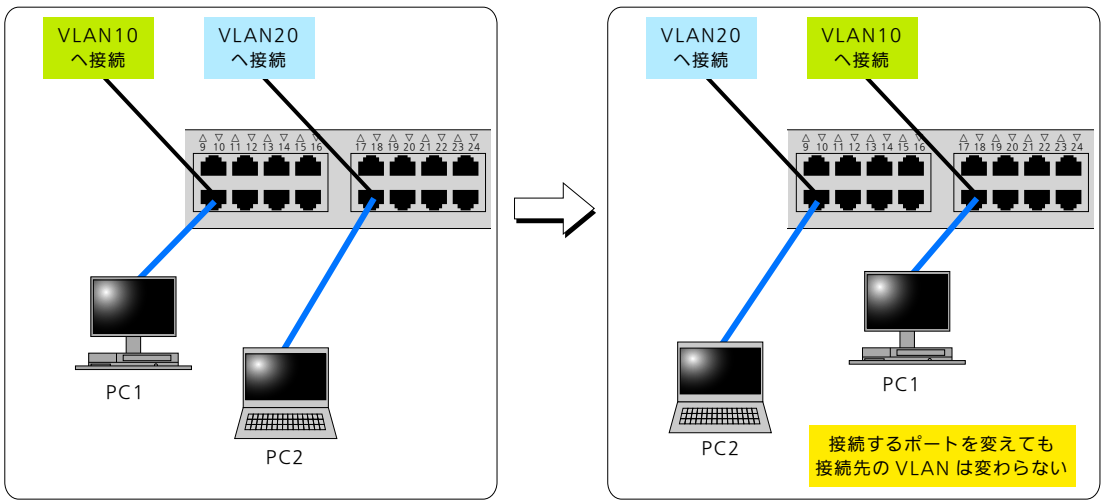


図 7-4　ダイナミック VLAN

---

enable 802.1x
disable 802.1x
create 802.1x user <username 15>
delete 802.1x user <username 15>
show 802.1x user
config 802.1x auth_protocol [local | radius_eap]
show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}
config 802.1x capability ports [<portlist> | all] [authenticator | none]
config 802.1x fwd_pdu ports [<portlist> | all] [enable | disable]
config 802.1x fwd_pdu system [enable | disable]
config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}(1)]
config 802.1x authorization attributes radius [enable | disable]
config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]
config 802.1x max_users [<value 1-448> | no_limit]
config 802.1x reauth [port_based ports [<portlist> | all] |mac_based ports [<portlist> | all] {mac_address <macaddr>}]
create 802.1x guest_vlan <vlan_name 32>
delete 802.1x guest_vlan <vlan_name 32>
config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]

---

show 802.1x guest_vlan
config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <sec 1-255> | retransmit <int 1-20>}(1)]
config radius delete <server_index 1-3>
config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <password 32> | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}(1)
show radius
show auth_statistics {ports <portlist>}
show auth_diagnostics {ports <portlist>}
show auth_session_statistics {ports <portlist>}
show auth_client
show acct_client
config accounting service [network | shell | system] state [enable | disable]
show accounting service

7.1. enable 802.1x

● 概要

このコマンドを用いて、802.1X 機能を有効にします。

● 構文

enable 802.1x

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

802.1X 機能を有効にするには：

```
Zxxx0:admin#enable 802.1x
Command: enable 802.1x

Success.

Zxxx0:admin#
```

7.2. disable 802.1x

● 概要

このコマンドを用いて、802.1X 機能を無効にします。

● 構文

disable 802.1x

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

802.1X 機能を無効にするには：

```
Zxxx0:admin#disable 802.1x
Command: disable 802.1x

Success.

Zxxx0:admin#
```

7.3. create 802.1x user

● 概要

このコマンドを用いて、802.1X ユーザを作成します。

● 構文

create 802.1x user <username 15>

● パラメータ

<username 15> ユーザ名を追加します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ctsnow という名前のユーザを作成するには：

```
Zxxx0:admin#create 802.1x user ctsnow
Command: create 802.1x user ctsnow

Enter a case-sensitive new password:
Enter the new password again for confirmation:

Success.

Zxxx0:admin#
```

7.4. delete 802.1x user

● 概要

このコマンドを用いて、指定したユーザを削除します。

● 構文

delete 802.1x user <username 15>

● パラメータ

<username 15> ユーザ名を削除します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

Tiberius という名前のユーザを削除するには：

```
Zxxx0:admin#delete 802.1x user Tiberius
Command: delete 802.1x user Tiberius

Success.

Zxxx0:admin#
```

7.5. show 802.1x user

● 概要

このコマンドを用いて、802.1X ローカルユーザアカウント情報を表示します。

● 構文

show 802.1x user

● パラメータ

なし

● 制限

なし

● 実行例

802.1X ユーザ情報を表示するには：

```
Zxxx0:admin#show 802.1x user
Command: show 802.1x user

Current Accounts:
Username         Password
---------------  ------------
ctsnow           gallinari

Total Entries : 1

Zxxx0:admin#
```

7.6. config 802.1x auth_protocol

● 概要

このコマンドを用いて、802.1X 認証プロトコルを設定します。

● 構文

config 802.1x auth_protocol [local | radius_eap]

● パラメータ

local	認証プロトコルとしてローカルを指定します。
radius_eap	認証プロトコルとして RADIUS EAP を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

802.1X RADIUS 認証を設定するには：

```
Zxxx0:admin#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

Zxxx0:admin#
```

7.7. show 802.1x

● 概要

このコマンドを用いて、802.1X の状態または設定を表示します。

● 構文

show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}

● パラメータ

auth_state	（オプション）一部またはすべてのポートの 802.1X 認証を表示します。
auth_configuration	（オプション）一部またはすべてのポートの 802.1X 設定を表示します。
ports	（オプション）表示するポートの範囲を指定します。 <portlist> 表示するポートの範囲を指定します。

● 制限

なし

● 実行例

802.1X 情報を表示するには：

```
Zxxx0:admin#show 802.1x
Command: show 802.1x

802.1X                   : Disabled
Authentication Protocol  : RADIUS_EAP
Forward EAPOL PDU        : Disabled
Max User                 : 448
RADIUS Authorization     : Enabled

Zxxx0:admin#
```

ポート 1 ～ 4 の 802.1X 状態を表示するには：

```
Zxxx0:admin# show 802.1x auth_state ports 1-4
Command: show 802.1x auth_state ports 1-4

Status:  A - Authorized; U - Unauthorized; (P): Port-Based 802.1X Pri: Priority
Port  MAC Address          Auth    PAE State      Backend    Status VID   Pri
                           VID                    State
----- -------------------- ------- -------------- ---------- ------ ----- -----
1     00-00-00-00-00-01    10      Authenticated  Idle       A      4004  3
1     00-00-00-00-00-02    10      Authenticated  Idle       A      1234  -
1     00-00-00-00-00-04    30      Authenticating Response   U       -    -
2     -                    (P)  -  Authenticating Request    U       -    -
3     -                    (P)  -  Connecting     Idle       U       -    -
4     -                    (P)  -  Held           Fail       U       -    -

Total Authenticating Hosts: 3
Total Authenticated Hosts : 2

Zxxx0:admin#
```

ポート 1 の 802.1X 設定を表示するには：

```
Zxxx0:admin# show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

Port number                      : 1
Capability                       : None
AdminCrlDir                      : Both
OpenCrlDir                       : Both
Port Control                     : Auto
QuietPeriod                      : 60 Seconds
TxPeriod                         : 30 Seconds
SuppTimeout                      : 30 Seconds
ServerTimeout                    : 30 Seconds
MaxReq                           : 2 Times
ReAuthPeriod                     : 3600 Seconds
ReAuthenticate                   : Disabled
Forward EAPOL PDU On Port        : Disabled
Max User On Port                 : 16

Zxxx0:admin#
```

7.8. config 802.1x capability ports

● 概要

このコマンドを用いて、ポート機能を設定します。

● 構文

config 802.1x capability ports [<portlist> | all] [authenticator | none]

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを設定します。
authenticator	アクセスを認証するためにポートに認証の役割を与えます。認証されたサービスは、そのポートを介してアクセスが認証されます。
none	指定したポートでの認証を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 10 にポート機能を設定するには：

```
Zxxx0:admin#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

Zxxx0:admin#
```

7.9. config 802.1x fwd_pdu ports

● 概要

このコマンドを用いて、スイッチの指定ポートで802.1X PDUの転送を制御するポートを設定します。

● 構文

config 802.1x fwd_pdu ports [<portlist> | all] [enable | disable]

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを指定します。
enable	802.1X PDU フォワーディング状態を有効にします。
disable	802.1X PDU フォワーディング状態を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 2 で 802.1X PDU フォワーディング状態を設定するには：

```
Zxxx0:admin#config 802.1x fwd_pdu ports 1-2 enable
Command: config 802.1x fwd_pdu ports 1-2 enable

Success.

Zxxx0:admin#
```

7.10. config 802.1x fwd_pdu system

● 概要

このコマンドを用いて、802.1X PDU 転送制御設定をします。

● 構文

config 802.1x fwd_pdu system [enable | disable]

● パラメータ

enable	802.1X PDU 転送制御設定を有効にします。
disable	802.1X PDU 転送制御設定を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

802.1X PDU 転送制御状態を設定するには：

```
Zxxx0:admin#config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

Zxxx0:admin#
```

7.11. config 802.1x auth_parameter ports

● 概要

このコマンドを用いて、ポートに関連付けられた認証動作を制御するパラメータを設定します。

● 構文

config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}(1)]

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを設定します。
default	すべてのパラメータを初期値に設定します。
direction	（オプション）アクセスコントロールの方向を設定します。 both 双方向アクセスコントロールを指定します。 in 入口アクセスコントロールを指定します。
port_control	（オプション）パラメータ port_control を force_authorized または force_unauthorized に設定することで、特定のポートを無条件に承認または未承認に設定します。port_control を auto に設定した場合、制御されるポートは認証の結果を反映します。 force_authorized ポートはクライアントに対する 802.1X ベース認証なしに、通常のトラフィックを送受信します。 auto ポートは未承認状態で開始し、クライアントと認証サーバの間でやりとりする認証メッセージを中継します。 force_unauthorized ポートは未承認状態を維持して、クライアントが認証を試みても、それらすべてを無視します。
quiet_period	（オプション）quietWhile タイマーの初期化値です。初期値は 60 秒です。値は 0 ～ 65535 の範囲で指定できます。 <sec 0-65535> 認証失敗後の非認証期間の値は、0 ～ 65535 秒で指定します。

tx_period	（オプション）txWhen タイマーの初期化値です。初期値は 30 秒です。値は 1 ～ 65535 の範囲で指定できます。 <sec 1-65535> 送信期間の値は、1 ～ 65535 秒で指定します。
supp_timeout	（オプション）サプリカントをタイムアウトさせる aWhile タイマーの初期化値です。初期値は 30 秒です。値は 1 ～ 65535 の範囲で指定できます。 <sec 1-65535> タイムアウト値は、1 ～ 65535 秒で指定します。
server_timeout	（オプション）認証サーバをタイムアウトさせる aWhile タイマーの初期化値です。初期値は 30 秒です。値は 1 ～ 65535 の範囲で指定できます。 <sec 1-65535> サーバタイムアウト値は、1 ～ 65535 秒で指定します。
max_req	（オプション）認証 PAE ステートマシンがサプリカントに EAP Request パケットを再送する最大回数です。初期値は 2 です。値は 1 ～ 10 の範囲で指定できます。 <value 1-10> 必要な最大回数は、1 ～ 10 で指定します。
reauth_period	（オプション）再認証タイマーとして使用します。0 以外の秒数を指定します。初期値は 3600 です。 <sec 1-65535> 再認証期間の値は、1 ～ 65535 秒で指定します。
max_users	（オプション）最大ユーザ数は、1 ～ 448 で指定します。 <value 1-448> 最大ユーザ数の値は、1 ～ 448 で指定します。 no_limit ユーザ数を無制限に設定します。
enable_reauth	（オプション）特定のポートでの再認証メカニズムを有効または無効にします。 enable 特定のポートでの再認証メカニズムを有効にします。 disable 特定のポートでの再認証メカニズムを無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポートに関連付けられた認証動作を制御するパラメータを設定するには：

```
Zxxx0:admin# config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

Zxxx0:admin#
```

7.12. config 802.1x authorization attributes radius

● 概要

このコマンドを用いて、承認された設定の受け入れを有効または無効にします（VLAN、802.1p、ACL、入力 / 出力帯域幅などに関する属性の設定方法については、本書の付録セクションを参照）。

● 構文

config 802.1x authorization attributes radius [enable | disable]

● パラメータ

enable	グローバル承認ステータスを有効にした場合、RADIUS　サーバによって割り当てられた　VLAN、802.1p、デフォルトプライオリティ、ACL などの承認属性を受け入れます。デフォルトの状態は enable です。
disable	RADIUS サーバによって割り当てられた承認属性を受け入れません。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

承認された設定の 802.1X 受け入れ状態を設定するには：

```
Zxxx0:admin#config 802.1x authorization attributes radius enable
Command: config 802.1x authorization attributes radius enable

Success.

Zxxx0:admin#
```

7.13. config 802.1x init

● 概要

このコマンドを用いて、一部またはすべての認証ステートマシンを初期化します。

● 構文

config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

● パラメータ

port_based ports	ポートベースモードでの認証を設定します。
<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを設定します。
mac_based ports	ホストベース 802.1X モードでの認証を設定します。
<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを設定します。
mac_address	（オプション）ホストの MAC アドレスを指定します。
<macaddr>	MAC アドレスを入力します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

一部またはすべての認証ステートマシンを初期化するには：

```
Zxxx0:admin# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

Zxxx0:admin#
```

7.14. config 802.1x max_users

● 概要

このコマンドを用いて、802.1X 最大システムユーザ数を設定します。

● 構文

config 802.1x max_users [<value 1-448> | no_limit]

● パラメータ

<value 1-448>	最大ユーザ数を指定します。
no_limit	ユーザ数を無制限に指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

802.1X 最大システムユーザ数を設定するには：

```
Zxxx0:admin# config 802.1x max_users 2
Command: config 802.1x max_users 2

Success.

Zxxx0:admin#
```

7.15. config 802.1x reauth

● 概要

このコマンドを用いて、ポートに接続された装置を再認証します。再認証期間中、ポートステータスは再認証に失敗するまで承認状態を維持します。

● 構文

config 802.1x reauth [port_based ports [<portlist> | all] |mac_based ports [<portlist> | all] {mac_address <macaddr>}]

● パラメータ

port_based ports スイッチは認証されたポートに基づいてデータを通過させます。 <portlist> 設定するポートの範囲を指定します。 all すべてのポートを設定します。
mac_based ports スイッチは認証された RADIUS クライアントの MAC アドレスに基づいてデータを通過させます。 <portlist> 設定するポートの範囲を指定します。 all すべてのポートを設定します。
mac_address （オプション）認証された RADIUS クライアントの MAC アドレスを指定します。 <macaddr> MAC アドレスを入力します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポートに接続された装置を再認証するには：

```
Zxxx0:admin# config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

Zxxx0:admin#
```

7.16. create 802.1x guest_vlan

● 概要

このコマンドを用いて、スタティック VLAN をゲスト VLAN として割り当てます。ゲスト VLAN として割り当てる具体的な VLAN は、すでに存在している必要があります。ゲスト VLAN として割り当てる具体的な VLAN は、削除できません。

● 構文

create 802.1x guest_vlan <vlan_name 32>

● パラメータ

<vlan_name 32> ゲスト VLAN として割り当てるスタティック VLAN を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スタティック VLAN をゲスト VLAN として割り当てるには：

```
Zxxx0:admin# create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

Zxxx0:admin#
```

7.17. delete 802.1x guest_vlan

● 概要

このコマンドを用いて、ゲスト VLAN 設定を削除します。ただし、スタティック VLAN 自体は削除しません。

● 構文

delete 802.1x guest_vlan <vlan_name 32>

● パラメータ

<vlan_name 32> ゲスト VLAN 名を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ゲスト VLAN 設定を削除するには：

```
Zxxx0:admin# delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

Zxxx0:admin#
```

7.18. config 802.1x guest_vlan ports

● 概要

このコマンドを用いて、ゲスト VLAN を設定します。

● 構文

config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]

● パラメータ

<portlist>設定するポートの範囲を指定します。	
all	すべてのポートを設定します。
state	設定したポートのゲスト VLAN ポート状態を指定します。 enable ゲスト VLAN を参加させます。 disable ゲスト VLAN の参加を解除します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 8 にゲスト VLAN を設定するには：

```
Zxxx0:admin# config 802.1x guest_vlan ports 1-8 state enable
Command: config 802.1x guest_vlan ports 1-8 state enable

Warning, The ports are moved to Guest VLAN.

Success.

Zxxx0:admin#
```

7.19. show 802.1x guest_vlan

● 概要

このコマンドを用いて、ゲスト VLAN 情報を表示します。

● 構文

show 802.1x guest_vlan

● パラメータ

なし

● 制限

なし

● 実行例

ゲスト VLAN 情報を表示するには：

```
Zxxx0:admin#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest Vlan Setting
-----------------------------------------------------------
Guest vlan : guest
Enable guest vlan ports : 1-10

Zxxx0:admin#
```

7.20. config radius add

● 概要

このコマンドを用いて、新しい RADIUS サーバを追加します。サーバのインデックス番号が小さいほど、認証プライオリティは高くなります。

● 構文

config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <sec 1-255> | retransmit <int 1-20>}(1)]

● パラメータ

<server_index 1-3>	RADIUS サーバインデックスを指定します。
<server_ip>	RADIUS サーバの IP アドレスを指定します。
<ipv6add>	使用する IPv6 アドレスを指定します。
key	スイッチと RADIUS サーバの間の共有キーを指定します。これを用いてユーザの認証データを暗号化してから、インターネット上に送り出します。最大キー長は、32 です。 <passwd 32> 最大パスワード長は、32 文字です。
default	auth_port を 1812、acct_port を 1813 にそれぞれ設定します。

auth_port	スイッチと RADIUS サーバの間で RADIUS 認証データをやりとりするために使用する UDP ポート番号を指定します。範囲は 1 ～ 65535 です。 <udp_port_number 1-65535> 認証ポート値は、1 ～ 65535 の範囲で指定します。
acct_port	スイッチと RADIUS サーバの間で RADIUS アカウンティング統計をやりとりするために使用する UDP ポート番号を指定します。範囲は 1 ～ 65535 です。 <udp_port_number 1-65535> アカウンティング統計値は、1 ～ 65535 の範囲で指定します。
timeout	サーバ応答を待つ時間を秒で指定します。初期値は 5 秒です。 <int 1-255> タイムアウト値は、1 ～ 255 の範囲で指定します。
retransmit	再送回数を指定します。初期値は 2 です。 <int 1-20> 再送値は、1 ～ 20 の範囲で指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

新しい RADIUS サーバを追加するには：

```
Zxxx0:admin#config radius add 1 10.48.74.121 key manager default
Command: config radius add 1 10.48.74.121 key manager default

Success.

Zxxx0:admin#
```

7.21. config radius delete

● 概要

このコマンドを用いて、RADIUS サーバを削除します。

● 構文

config radius delete <server_index 1-3>

● パラメータ

<server_index 1-3>	RADIUS サーバインデックスを指定します。範囲は 1 ～ 3 です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

RADIUS サーバを削除するには：

```
Zxxx0:admin#config radius delete 1
Command: config radius delete 1

Success.

Zxxx0:admin#
```

7.22. config radius

● 概要

このコマンドを用いて、RADIUS サーバを設定します。

● 構文

config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <password 32> | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}(1)

● パラメータ

<server_index 1-3>	RADIUS サーバインデックスを指定します。
ipaddress	RADIUS サーバの IP アドレスを指定します。 <server_ip> RADIUS サーバの IP アドレスを入力します。 <ipv6addr> IPv6 アドレスを入力します。
key	スイッチと RADIUS サーバの間の共有キーを指定します。これを用いてユーザの認証データを暗号化してから、インターネット上に送り出します。最大キー長は、32 です。 <passwd 32> スイッチと RADIUS サーバの間の共有キーを指定します。これを用いてユーザの認証データを暗号化してから、インターネット上に送り出します。最大キー長は、32 です。
auth_port	スイッチと RADIUS サーバの間で RADIUS 認証データをやりとりするために使用する UDP ポート番号を指定します。デフォルトは 1812 です。 <udp_port_number 1-65535> 認証ポート値は、1 ～ 65535 の範囲で指定します。 default 初期値を使用します。

acct_port	スイッチと RADIUS サーバの間で RADIUS アカウンティング統計をやりとりするために使用する UDP ポート番号を指定します。デフォルトは 1813 です。 **<udp_port_number 1-65535>** アカウンティング統計値は、1 ～ 65535 の範囲で指定します。 **default** 初期値を使用します。
timeout	サーバ応答を待つ時間を秒で指定します。初期値は 5 秒です。 **<int 1-255>** サーバ応答を待つ時間を秒で指定します。タイムアウト値は、1 ～ 255 の範囲で指定します。初期値は 5 秒です。 **default** 初期値を使用します。
retransmit	再送回数を指定します。初期値は 2 です。 **<int 1-20>** 再送値は、1 ～ 20 の範囲で指定します。 **default** 初期値を使用します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

RADIUS サーバを設定するには：

```
Zxxx0:admin#config radius 1 ipaddress 10.48.74.121 key manager
Command: config radius 1 ipaddress 10.48.74.121 key manager

Success.

Zxxx0:admin#
```

7.23. show radius

● 概要

このコマンドを用いて、RADIUS サーバ設定を表示します。

● 構文

show radius

● パラメータ

なし

● 制限

なし

● 実行例

RADIUS サーバ設定を表示するには：

```
Zxxx0:admin#show radius
Command: show radius

Index 1
    IP Address      : 192.168.69.1
    Auth-Port       : 1812
    Acct-Port       : 1813
    Timeout         : 5
    Retransmit      : 2
    Key             : 123456

Total Entries : 1

Zxxx0:admin#
```

7.24. show auth_statistics

● 概要

このコマンドを用いて、認証統計情報を表示します。

● 構文

show auth_statistics {ports <portlist>}

● パラメータ

ports	（オプション）表示するポートを指定します。 <portlist> 表示するポートの範囲を指定します。

● 制限

なし

● 実行例

ポート 3 の認証統計情報を表示するには：

```
Zxxx0:admin# show auth_statistics ports 3
Command: show auth_statistics ports 3

Auth VID    :100
MAC Address :00-00-00-00-00-03
Port number : 3

EapolFramesRx                       0
EapolFramesTx                       6
EapolStartFramesRx                  0
EapolReqIdFramesTx                  6
EapolLogoffFramesRx                 0
EapolReqFramesTx                    0
EapolRespIdFramesRx                 0
EapolRespFramesRx                   0
InvalidEapolFramesRx                0
EapLengthErrorFramesRx              0
LastEapolFrameVersion               0
LastEapolFrameSource                00-00-00-00-00-03

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

7.25. show auth_diagnostics

● 概要

このコマンドを用いて、認証診断情報を表示します。

● 構文

show auth_diagnostics {ports <portlist>}

● パラメータ

ports	（オプション）表示するポートを指定します。 <portlist> 表示するポートの範囲を指定します。

● 制限

なし

● 実行例

ポート 3 の認証診断情報を表示するには：

```
Zxxx0:admin# show auth_diagnostics ports 3
Command: show auth_diagnostics ports 3

Auth VID                                100
MAC Address                             00-00-00-00-00-03
Port number : 1

EntersConnecting                        20
EapLogoffsWhileConnecting               0
EntersAuthenticating                    0
SuccessWhileAuthenticating              0
TimeoutsWhileAuthenticating             0
FailWhileAuthenticating                 0
ReauthsWhileAuthenticating              0
EapStartsWhileAuthenticating            0
EapLogoffWhileAuthenticating            0
ReauthsWhileAuthenticated               0
EapStartsWhileAuthenticated             0
EapLogoffWhileAuthenticated             0
BackendResponses                        0
BackendAccessChallenges                 0
BackendOtherRequestsToSupplicant        0
BackendNonNakResponsesFromSupplicant    0
BackendAuthSuccesses                    0
BackendAuthFails                        0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

7.26. show auth_session_statistics

● 概要

このコマンドを用いて、認証セッション統計情報を表示します。

● 構文

show auth_session_statistics {ports <portlist>}

● パラメータ

ports	（オプション）表示するポートを指定します。 <portlist> 表示するポートの範囲を指定します。

● 制限

なし

● 実行例

ポート 1 の認証セッション統計情報を表示するには：

```
Zxxx0:admin# show auth_session_statistics ports 3
Command: show auth_session_statistics ports 3

Auth VID     : 100
MAC Address : 00-00-00-00-00-03
Port number : 3

SessionOctetsRx                         0
SessionOctetsTx                         0
SessionFramesRx                         0
SessionFramesTx                         0
SessionId
SessionAuthenticMethod                  Remote Authentication Server
SessionTime                             0
SessionTerminateCause                   SupplicantLogoff
SessionUserName

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

7.27. show auth_client

● 概要

このコマンドを用いて、認証クライアント情報を表示します。

● 構文

show auth_client

● パラメータ

なし

● 制限

なし

● 実行例

認証クライアント情報を表示するには：

```
Zxxx0:admin# show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               Manager


radiusAuthServerEntry ==>
radiusAuthServerIndex :1

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         X
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               MANAGER


radiusAuthServerEntry ==>
radiusAuthServerIndex :2

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         X
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0
```

```
radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               MANAGER


radiusAuthServerEntry ==>
radiusAuthServerIndex :3

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         X
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0

Zxxx0:admin#
```

7.28. show acct_client

● 概要

このコマンドを用いて、アカウントクライアント情報を表示します。

● 構文

show acct_client

● パラメータ

なし

● 制限

なし

● 実行例

アカウントクライアント情報を表示するには：

```
Zxxx0:admin# show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier               MANAGER


radiusAuthServerEntry ==>
radiusAccServerIndex : 1

radiusAccServerAddress                   0.0.0.0
radiusAccClientServerPortNumber          X
radiusAccClientRoundTripTime             0
radiusAccClientRequests                  0
radiusAccClientRetransmissions           0
radiusAccClientResponses                 0
radiusAccClientMalformedResponses        0
radiusAccClientBadAuthenticators         0
radiusAccClientPendingRequests           0
radiusAccClientTimeouts                  0
radiusAccClientUnknownTypes              0
radiusAccClientPacketsDropped            0

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier               MANAGER


radiusAuthServerEntry ==>
radiusAccServerIndex : 2

radiusAccServerAddress                   0.0.0.0
radiusAccClientServerPortNumber          X
radiusAccClientRoundTripTime             0
radiusAccClientRequests                  0
radiusAccClientRetransmissions           0
radiusAccClientResponses                 0
radiusAccClientMalformedResponses        0
radiusAccClientBadAuthenticators         0
radiusAccClientPendingRequests           0
radiusAccClientTimeouts                  0
radiusAccClientUnknownTypes              0
radiusAccClientPacketsDropped            0

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier               MANAGER
```

```
radiusAuthServerEntry ==>
radiusAccServerIndex : 3

radiusAccServerAddress                    0.0.0.0
radiusAccClientServerPortNumber           X
radiusAccClientRoundTripTime              0
radiusAccClientRequests                   0
radiusAccClientRetransmissions            0
radiusAccClientResponses                  0
radiusAccClientMalformedResponses         0
radiusAccClientBadAuthenticators          0
radiusAccClientPendingRequests            0
radiusAccClientTimeouts                   0
radiusAccClientUnknownTypes               0
radiusAccClientPacketsDropped             0

Zxxx0:admin#
```

7.29. config accounting service

● 概要

このコマンドを用いて、指定した RADIUS アカウンティングサービスの状態を設定します。

● 構文

config accounting service [network | shell | system] state [enable | disable]

● パラメータ

network	802.1X ポートアクセスコントロールのアカウンティングサービスを指定します。工場出荷時ではこのサービスは無効です。
shell	シェルイベントのアカウンティングサービスを指定します。ユーザが（コンソール、Telnet、または SSH を介して）スイッチにログインまたはログアウトし、タイムアウトが発生すると、アカウンティング情報を収集して RADIUS サーバに送信します。工場出荷時ではこのサービスは無効です。
system	リセットおよび再起動などのシステムイベントのアカウンティングサービスを指定します。工場出荷時ではこのサービスは無効です。
state	アカウンティングサービスの状態を指定します。 enable 指定したアカウンティングサービスを有効にします。 disable 指定したアカウンティングサービスを無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

RADIUS アカウンティングサービスシェルの状態を有効に設定するには：

```
Zxxx0:admin# config accounting service shell state enable
Command: config accounting service shell state enable

Success

Zxxx0:admin#
```

7.30. show accounting service

● 概要

このコマンドを用いて、RADIUS アカウンティングサービス情報を表示します。

● 構文

show accounting service

● パラメータ

なし

● 制限

なし

● 実行例

アカウンティングサービス情報を表示するには：

```
Zxxx0:admin#show accounting service
Command: show accounting service

Accounting State
-------------------
Network : Disabled
Shell   : Disabled
System  : Disabled

Zxxx0:admin#
```

8. ACL(Access Control List) コマンド

ネットワークのセキュリティを守るためには、内部、外部からの不正な通信を遮断することが重要です。
Access Control とは、スイッチに到達したパケットのヘッダ内の情報を調べ、ルールを設定してパケットの転送をフィルタリングする機能です。Access Control 機能を利用するには、フィルタリングする対象、条件、動作を定義した Access Control List（ACL）を作成し、適用するポートや VLAN を設定します。

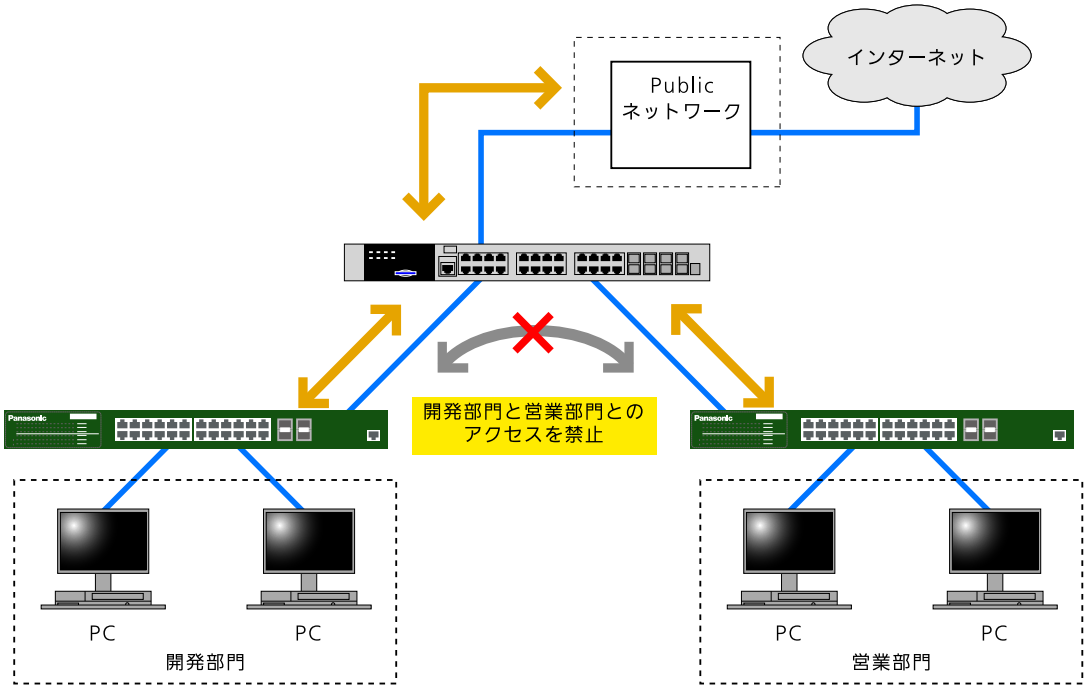


図 8-1　Access Control の概略

● アクセスリストプロファイル（access list profile）

本装置では、ACL を「アクセスリストプロファイル」という名称で、ID 1 ～ 6 まで作成できます。
プロファイルでは、以下のような多様なカテゴリからフィルタリングの対象を設定できます。

- IEEE 802.1p プライオリティ
- VLAN 名、VLAN 番号
- MAC アドレス
- Ether タイプ
- IP アドレス
- DSCP（優先制御情報）
- プロトコルタイプ
- TCP/UDP ポート番号

- IPv6 トラフィッククラス、フローラベル
- 任意のパケットコンテンツ（パケットバイトオフセット、マスクで指定し、4 個まで定義可能）

さらに、各プロファイルではパケットの詳細の情報とフィルタリング動作を定義したルールを ID 1 ～ 256 まで作成できます。

NOTE プロファイルおよびルールは、id が小さい番号の順に適用されます。

また、タイムレンジを設定し、日時や曜日に応じて適用するルールを変更することもできます。

NOTE タイムレンジを利用する場合、スイッチの内蔵時計を正確に調整しておくことが必要です。設定については「時刻および SNTP コマンド」の項を参照してください。

● 適用できる動作

ルールに一致したパケットには、以下の動作を適用できます。

- Permit：転送します。

NOTE IEEE 802.1p プライオリティ、DSCP、出力パケット IP 優先度もあわせて変更できます。

- Deny：転送せずに破棄します。
- Mirror：別途設定したミラーリングポートにパケットをコピーして転送します。

NOTE ミラーリングの設定については、「Mirror Commands」の項を参照してください。

- Counter：一致したパケット数を記録します。

● フローメータ（Flow Meter）

対象とするパケットのバイト数に応じてフィルタリングを行います。帯域、バイト数のしきい値を設定し、パケットのバイト数がしきい値内であるかどうかで、転送や破棄の動作を適用できます。

create access_profile profile_id <value 1-6> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}(1) | ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}(1) | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1) | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}(1)]
delete access_profile [profile_id <value 1-6> | profile_name <name 1-32> | all]

config access_profile [profile_id <value 1-6> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>}(1) | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]}(1) | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}(1) | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}(1)] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror {group_id <value 1-4>} | deny] {time_range <range_name 32>} | delete access_id <value 1-256>]
show access_profile {[profile_id <value 1-6> | profile_name <name 1-32>]}
config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]
show time_range
show current_config access_profile
config flow_meter [profile_id <value 1-6> | profile_name <name 1-32>] access_id <value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]
show flow_meter {[profile_id <value 1-6> | profile_name <name 1-32>] {access_id <value 1-256>}}

8.1. create access_profile profile_id

● 概要

このコマンドを用いて、アクセスリストプロファイルを作成します。

● 構文

create access_profile profile_id <value 1-6> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}(1) | ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}(1) | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1) | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}(1)]

● パラメータ

<value 1-6>
プロファイル ID として 1 ～ 6 を指定します。プロファイル ID 番号が小さいほど、プライオリティは高くなります。

profile_name
プロファイル名を指定します。
<name 1-32>
32 文字以内で設定します。

ethernet イーサネット ACL ルールを指定します。
vlan VLAN マスクを指定します。マスクの末尾 12 ビットのみ考慮されます。
<hex 0x0-0x0fff>
（オプション）VLAN マスクを指定します。
source_mac
送信元 MAC マスクを指定します。
<macmask 000000000000-ffffffffffff>
送信元 MAC マスクを指定します。
destination_mac
宛先 MAC マスクを指定します。
<macmask 000000000000-ffffffffffff>
宛先 MAC マスクを指定します。
802.1p
802.1p プライオリティタグマスクを指定します。
ethernet_type
イーサネットタイプを指定します。

ip IP ACL ルールを指定します。
vlan VLAN マスクを指定します。マスクの末尾 12 ビットのみ考慮されます。
<hex 0x0-0x0fff> - （オプション）VLAN マスクを指定します。
source_ip_mask
IP 送信元サブマスクを指定します。
<netmask>
IP 送信元サブマスクを指定します。
destination_ip_mask
IP 宛先サブマスクを指定します。
<netmask>
IP 宛先サブマスクを指定します。
dscp DSCP マスクを指定します。
icmp ルールが ICMP トラフィックに適用されます。
type （オプション）ICMP パケットタイプを指定します。
code （オプション）ICMP コードを指定します。
igmp ルールが IGMP トラフィックに適用されます。
type （オプション）IGMP パケットタイプを指定します。
tcp ルールが TCP トラフィックに適用されます。
src_port_mask
（オプション）TCP 送信元ポートマスクを指定します。
<hex 0x0-0xffff>
TCP 送信元ポートマスクを指定します。
dst_port_mask
（オプション）TCP 宛先ポートマスクを指定します。
<hex 0x0-0xffff>
TCP 宛先ポートマスクを指定します。
flag_mask
（オプション）TCP フラグフィールドマスクを指定します。
all 以下のすべてのパラメータを確認する場合に指定します。
urg （オプション）緊急ポインタフィールドを有効にするために指定します。
ack （オプション）確認応答フィールドを有効にするために指定します。
psh （オプション）プッシュ機能を指定します。
rst （オプション）接続をリセットするために指定します。
syn （オプション）シーケンス番号を同期するために指定します。
fin （オプション）送信元からのデータ送信を終了します。
udp ルールが UDP トラフィックに適用されます。
src_port_mask
（オプション）TCP 送信元ポートマスクを指定します。
<hex 0x0-0xffff>
TCP 送信元ポートマスクを指定します。
dst_port_mask
（オプション）TCP 宛先ポートマスクを指定します。
<hex 0x0-0xffff>
TCP 宛先ポートマスクを指定します。
protocol_id_mask
ルールが IP プロトコル ID トラフィックに適用されます。
<hex 0x0-0xff>
ルールが IP プロトコル ID トラフィックに適用されます。
user_define_mask
（オプション）L4 部分マスクを指定します。
<hex 0x0-0xffffffff>
L4 部分マスクを指定します。

packet_content_mask

最大 6 つのオフセットを指定できます。各オフセットは、単一の UDF フィールドとして認識される 1 バイトのデータを定義します。オフセット参照も設定できます。タグの末尾、イーサネットタイプの末尾、または IP ヘッダの末尾で開始するよう定義できます。

offset_chunk_1

オフセットチャンク 1 を指定して、ユーザが 1 つのパケット内の指定された offset_chunk を一度に調べることができるようにし、フレームコンテンツオフセットおよびマスクを指定します。

<value 0-31>

オフセットチャンク 1 の値を入力します。値は 0 ～ 31 で指定します。

<hex 0x0-0xffffffff>

オフセットチャンク 1 マスク値を入力します。

offset_chunk_2

オフセットチャンク 2 を指定して、ユーザが 1 つのパケット内の指定された offset_chunk を一度に調べることができるようにし、フレームコンテンツオフセットおよびマスクを指定します。

<value 0-31>

オフセットチャンク 2 の値を入力します。値は 0 ～ 31 で指定します。

<hex 0x0-0xffffffff>

オフセットチャンク 2 マスク値を入力します。

offset_chunk_3

オフセットチャンク 3 を指定して、ユーザが 1 つのパケット内の指定された offset_chunk を一度に調べることができるようにし、フレームコンテンツオフセットおよびマスクを指定します。

<value 0-31>

オフセットチャンク 3 の値を入力します。値は 0 ～ 31 で指定します。

<hex 0x0-0xffffffff>

オフセットチャンク 3 マスク値を入力します。

offset_chunk_4

オフセットチャンク 4 を指定して、ユーザが 1 つのパケット内の指定された offset_chunk を一度に調べることができるようにし、フレームコンテンツオフセットおよびマスクを指定します。

<value 0-31>

オフセットチャンク 4 の値を入力します。値は 0 ～ 31 で指定します。

<hex 0x0-0xffffffff>

オフセットチャンク 4 マスク値を入力します。

ipv6	**IPv6 フィルタリングマスクを指定します。** class IPv6 クラスマスクを指定します。 flowlabel IPv6 フローラベルマスクを指定します。 source_ipv6_mask IPv6 送信元 IP マスクを指定します。 <ipv6mask> IPv6 送信元 IP マスクを指定します。 destination_ipv6_mask IPv6 宛先 IP マスクを指定します。 <ipv6mask> IPv6 宛先 IP マスクを指定します。 tcp ルールが TCP トラフィックに適用されます。 src_port_mask （オプション）TCP 送信元ポートマスクを指定します。 <hex 0x0-0xffff> TCP 送信元ポートマスクを指定します。 dst_port_mask （オプション）TCP 宛先ポートマスクを指定します。 <hex 0x0-0xffff> TCP 宛先ポートマスクを指定します。 udp - ルールが UDP トラフィックに適用されます。 src_port_mask （オプション）TCP 送信元ポートマスクを指定します。 <hex 0x0-0xffff> TCP 送信元ポートマスクを指定します。 dst_port_mask （オプション）TCP 宛先ポートマスクを指定します。 <hex 0x0-0xffff> TCP 宛先ポートマスクを指定します。 icmp ルールが ICMP トラフィックに適用されます。 type （オプション）ICMP パケットタイプを指定します。 code （オプション）ICMP コードを指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

アクセスリストプロファイルを作成するには：

```
Zxxx0:admin#create access_profile profile_id 1 profile_name 1 ethernet vlan
source_mac FF-FF-FF-FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p
ethernet_type
Command: create access_profile profile_id 1 profile_name 1 ethernet vlan source_mac
FF-FF-FF-FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p ethernet_type


Success.


Zxxx0:admin#


Zxxx0:admin#create access_profile profile_id 2 profile_name 2 ip vlan
source_ip_mask 255.255.255.255 destination_ip_mask 255.255.255.0 dscp icmp
Command: create access_profile profile_id 2 profile_name 2 ip vlan source_ip_mask
255.255.255.255 destination_ip_mask 255.255.255.0 dscp icmp


Success.


Zxxx0:admin#
```

8.2. delete access_profile

● 概要

このコマンドを用いて、アクセスリストプロファイルを削除します。

● 構文

delete access_profile [profile_id <value 1-6> | profile_name <name 1-32> | all]

● パラメータ

profile_id	アクセスリストプロファイルのインデックスを指定します。 <value 1-6> アクセスリストプロファイルのインデックスを指定します。値として 1 ～ 6 を入力します。
profile_name	プロファイル名を指定します。 <name 1-32> プロファイル名を指定します。32 文字以内で設定します。
all	アクセスリストプロファイル全体を削除するよう指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

アクセスリストプロファイルを削除するには：

```
Zxxx0:admin#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

Zxxx0:admin#
```

8.3. config access_profile

● 概要

このコマンドを用いて、アクセスリストエントリを設定します。

● 構文

config access_profile [profile_id <value 1-6> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>}(1) | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]}(1) | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}(1) | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}(1)] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror {group_id <value 1-4>} | deny] {time_range <range_name 32>} | delete access_id <value 1-256>]

● パラメータ

profile_id
　　アクセスリストプロファイルのインデックスを指定します。
　　<value 1-6>
　　　　アクセスリストプロファイルリストの ID を入力します。入力値として 1 ～ 6 を指定します。

profile_name
プロファイル名を指定します。
<name 1-32>
プロファイル名を指定します。32 文字以内で設定します。

add access_id
アクセスリストエントリのインデックスを指定します。アクセス ID 番号が小さいほど、プライオリティは高くなります。
auto_assign
アクセス ID を自動的に割り当てる場合に指定します。
<value 1-256>
アクセス ID の入力値として 1 ～ 256 を指定します。

ethernet イーサネット ACL ルールを指定します。
vlan VLAN 名を指定します。
<vlan_name 32>
VLAN 名を指定します。32 文字以内で設定します。
vlanid VLAN ID を指定します。
<vlanid 1-4094>
VLAN ID として 1 ～ 4094 を指定します。
mask（オプション）マスクを指定します。
<hex 0x0-0x0fff>
マスクを指定します。
source_mac
送信元 MAC アドレスを指定します。
<macaddr>
送信元 MAC アドレスを指定します。
mask（オプション）マスクを指定します。
<macmask>
マスクを指定します。
destination_mac
宛先 MAC アドレスを指定します。
<macaddr>
宛先 MAC アドレスを指定します。
mask（オプション）マスクを指定します。
<macmask>
マスクを指定します。
802.1p
802.1p プライオリティタグ値を指定します。
<value 0-7>
802.1p プライオリティタグ値を指定します。プライオリティタグ値の範囲は 1 ～ 7 です。
ethernet_type
イーサネットタイプを指定します。
<hex 0x0-0xffff>
イーサネットタイプを指定します。

ip IP ACL ルールを指定します。
vlan VLAN 名を指定します。
<vlan_name 32>
VLAN 名を指定します。32 文字以内で設定します。
vlanid
VLAN ID を指定します。
<vlanid 1-4094>
VLAN ID として 1 ～ 4094 を指定します。
mask
（オプション）マスクを指定します。
<hex 0x0-0x0fff>
マスクを指定します。
source_ip
IP 送信元アドレスを指定します。
<ipaddr>
IP 送信元アドレスを指定します。
mask（オプション）マスクを指定します。
<netmask>
マスクを指定します。
destination_ip
IP 宛先アドレスを指定します。
<ipaddr>
IP 宛先アドレスを指定します。
mask（オプション）マスクを指定します。
<netmask>
マスクを指定します。
dscp DSCP の値を指定します。
<value 0-63>
DSCP の値を指定します。DSCP 値の範囲は 0 ～ 63 です。
icmp ICMP を指定します。
type
（オプション）ルールが ICMP タイプトラフィック値に適用されます。
<value 0-255>
タイプトラフィック値として 0 ～ 255 を指定します。
code （オプション）ルールが ICMP コードトラフィック値に適用されます。
<value 0-255>
コードトラフィック値として 0 ～ 255 を指定します。
igmp IGMP を指定します。
type （オプション）ルールが IGMP タイプトラフィック値に適用されます。
<value 0-255>
IGMP タイプトラフィック値として 0 ～ 255 を指定します。
tcp TCP を指定します。

src_port
（オプション）ルールが TCP 送信元ポート範囲に適用されます。
<value 0-65535>
値として 0 ～ 65535 を指定します。
mask（オプション）マスクを指定します。
<hex 0x0-0xffff>
マスクを指定します。
dst_port
（オプション）ルールが TCP 宛先ポート範囲に適用されます。
<value 0-65535>
値として 0 ～ 65535 を指定します。
mask（オプション）マスクを指定します。
<hex 0x0-0xffff>
マスクを指定します。
flag TCP フラグフィールド値を指定します。
all 以下のすべてのパラメータを確認する場合に指定します。
urg （オプション）緊急ポインタフィールドを有効にするために指定します。
ack （オプション）確認応答フィールドを有効にするために指定します。
psh （オプション）プッシュ機能を指定します。
rst （オプション）接続をリセットするために指定します。
syn （オプション）シーケンス番号を同期するために指定します。
fin （オプション）送信元からのデータ送信を終了します。
udp UDP を指定します。
src_port
（オプション）UDP 送信元ポート範囲を指定します。
<value 0-65535>
値として 0 ～ 65535 を指定します。
mask（オプション）マスクを指定します。
<hex 0x0-0xffff>
マスクを指定します。
dst_port
（オプション）UDP 宛先ポート範囲を指定します。
<value 0-65535>
値として 0 ～ 65535 を指定します。
mask（オプション）マスクを指定します。
<hex 0x0-0xffff>
マスクを指定します。
protocol_id
ルールが IP プロトコル ID トラフィックの値に適用されます。
<value 0-255>
値として 0 ～ 255 を指定します。
user_define
（オプション）ルールが IP プロトコル ID および 4 バイト長の IP ヘッダの後ろのマスクオプションに適用されます。
<hex 0x0-0xffffffff>
ルールが IP プロトコル ID および 4 バイト長の IP ヘッダの後ろのマスクオプションに適用されます。
mask（オプション）マスクを指定します。
<hex 0x0-0xffffffff>
マスクを指定します。

packet_content
ユーザ定義マスクに対するパケットコンテンツを指定します。
offset_chunk_1
監視するオフセットトランク 1 のコンテンツを指定します。
<hex 0x0-0xffffffff>
監視するオフセットトランク 1 のコンテンツを入力します。
mask 各フィールドに追加マスクを指定します。
<hex 0x0-0xffffffff>
使用する追加マスク値を入力します。
offset_chunk_2
監視するオフセットトランク 2 のコンテンツを指定します。
<hex 0x0-0xffffffff>
監視するオフセットトランク 2 のコンテンツを入力します。
mask 各フィールドに追加マスクを指定します。
<hex 0x0-0xffffffff>
使用する追加マスク値を入力します。
offset_chunk_3
監視するオフセットトランク 3 のコンテンツを指定します。
<hex 0x0-0xffffffff>
監視するオフセットトランク 3 のコンテンツを入力します。
mask 各フィールドに追加マスクを指定します。
<hex 0x0-0xffffffff>
使用する追加マスク値を入力します。
offset_chunk_4
監視するオフセットトランク 4 のコンテンツを指定します。
<hex 0x0-0xffffffff>
監視するオフセットトランク 4 のコンテンツを入力します。
mask 各フィールドに追加マスクを指定します。
<hex 0x0-0xffffffff>
使用する追加マスク値を入力します。

ipv6 ルールが IPv6 フィールドに適用されます。
class IPv6 クラスの値を指定します。
<value 0-255>
値として 0 ～ 255 を指定します。
flowlabel
IPv6 フローラベルの値を指定します。
<hex 0x0-0xfffff>
IPv6 フローラベルの値を指定します。
source_ipv6
IPv6 送信元アドレスの値を指定します。
<ipv6addr>
IPv6 接続元アドレスの値を指定します。
mask（オプション）マスクを指定します。
<ipv6mask>
マスクを指定します。
destination_ipv6
IPv6 宛先アドレスの値を指定します。
<ipv6addr>
IPv6 接続先アドレスの値を指定します。
mask（オプション）マスクを指定します。
<ipv6mask>
マスクを指定します。

tcp TCP を指定します。
src_port
（オプション）TCP 送信元ポート範囲を指定します。
<value 0-65535>
値として 0 ～ 65535 を指定します。
mask（オプション）マスクを指定します。
<hex 0x0-0xffff>
マスクを指定します。
dst_port
（オプション）TCP 宛先ポート範囲を指定します。
<value 0-65535>
値として 0 ～ 65535 を指定します。
mask（オプション）マスクを指定します。
<hex 0x0-0xffff>
マスクを指定します。
udp UDP を指定します。
src_port
（オプション）UDP 送信元ポート範囲を指定します。
<value 0-65535>
値として 0 ～ 65535 を指定します。
mask（オプション）マスクを指定します。
<hex 0x0-0xffff>
マスクを指定します。
dst_port
（オプション）UDP 宛先ポート範囲を指定します。
<value 0-65535>
値として 0 ～ 65535 を指定します。
mask マスクを指定します。
<hex 0x0-0xffff>
マスクを指定します。
icmp ルールが ICMP トラフィックの値に適用されます。
type ルールが ICMP タイプトラフィックの値に適用されます。
<value 0-255>
使用する ICMP タイプ値を入力します。値は 0 ～ 255 で指定します。
code ルールが ICMP コードトラフィックの値に適用されます。
<value 0-255>
使用する ICMP コード値を入力します。値は 0 ～ 255 で指定します。

port スイッチの各ポートに対してアクセスプロファイルルールを定義できます。ポートリストは、最も小さいスイッチ番号と、そのスイッチの開始ポート番号をコロンで区切って指定します。
<portlist>
ポートのリストを指定します。
all アクセスルールがすべてのポートに適用されます。

vlan_based
VLAN ベースの ACL ルールを指定します。このルールはすべてのポートに適用されること、およびパケットは設定した VLAN に属することの 2 つの条件を満たす必要があります。VLAN 名または VLAN ID で指定できます。
vlan VLAN 名を指定します。
<vlan_name 32>
VLAN 名を指定します。32 文字以内で設定します。
vlan_id
VLAN ID を指定します。
<vlanid 1-4094>
VLAN ID として 1 ～ 4094 を指定します。

permit アクセスプロファイルに一致するパケットが、スイッチで認証されます。

priority （オプション）アクセスプロファイルに一致するパケットが、スイッチで設定した 802.1p プライオリティタグフィールドに再マッピングされます。
<value 0-7>
値として 0 ～ 7 を指定します。

replace_priority
（オプション）アクセスプロファイルに一致するパケットが、スイッチで設定した 802.1p プライオリティタグフィールドを書き換えることを指定します。

replace_dscp_with
（オプション）アクセスプロファイルに一致するパケットの DSCP が、値に基づいて変更されます。
<value 0-63>
値として 0 ～ 63 を指定します。

replace_tos_precedence_with
（オプション）出力パケットの IP 優先度が、新しい値に変更されます。動作プライオリティを指定せずに使用した場合、パケットはデフォルト TC に送信されます。
<value 0-7>
値として 0 ～ 7 を指定します。

counter （オプション）ACL カウンタ機能の有効 / 無効を指定します。
enable
ACL カウンタ機能を有効化にします。ルールがフローメータと連動していない場合は、すべての一致パケットがカウントされます。ルールがフローメータと連動している場合は、カウンタがオーバーライドされます。
disable
ACL カウンタ機能を無効化にします。デフォルトのオプションは disable です。

mirror アクセスプロファイルに一致するパケットが、ミラーポートにコピーされます。

group_id
使用するグループ ID を指定します。
<value 1-4>
使用するグループ ID を入力します。値は 1 ～ 4 で指定します。

deny アクセスプロファイルに一致するパケットが、スイッチによってフィルタリングされます。

time_range
（オプション）このタイムレンジエントリ名を指定します。
<range_name 32>
このタイムレンジエントリ名を指定します。32 文字以内で設定します。

delete access_id
アクセス ID を削除する場合に指定します。
<value 1-256>
値として 1 ～ 256 を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

アクセスリストエントリを設定するには：

```
Zxxx0:admin#config access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp port 1 permit
Command: config access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp port 1 permit

Success.

Zxxx0:admin#
```

8.4. show access_profile

● 概要

このコマンドを用いて、現在のアクセスリストテーブルを表示します。

● 構文

show access_profile {[profile_id <value 1-6> | profile_name <name 1-32>]}

● パラメータ

profile_id	（オプション）アクセスリストプロファイルのインデックスを指定します。 <value 1-6> プロファイル ID として 1 ～ 6 を指定します。
profile_name	（オプション）アクセスリストプロファイル名を指定します。 <name 1-32> プロファイル名として 1 ～ 32 を指定します。

● 制限

なし

● 実行例

現在のアクセスリストテーブルを表示するには：

```
Zxxx0:admin#show access_profile
Command: show access_profile

Access Profile Table

Total User Set Rule Entries : 3
Total Used HW Entries       : 19
Total Available HW Entries  : 1005
================================================================================
Profile ID: 1      Profile Name: 1                     Type: Ethernet
Mask on
    VLAN ID   : 0xFF
    Source MAC: FF-FF-FF-FF-FF-00
    802.1p
Available HW Entries: 254
--------------------------------------------------------------------------------
Rule ID : 1       Ports: 1-10
Match on:
   VLAN ID    : 2    Mask : 0xFFF
   Source MAC : 00-01-02-03-04-00
Action:
   Permit
   Replaced Priority to 2
   Replace DSCP to 33

Matched Count: 0 packets
--------------------------------------------------------------------------------
Rule ID : 256 (auto assign) Ports: -
Match on:
   VLAN ID    : 8
   Source MAC : 00-01-02-03-04-00
   802.1p
Action:
   Deny
================================================================================
Profile ID: 3      Profile Name: 3                     Type: IPv4
Mask on
    Source IP : 255.255.255.0
    TCP
    Source Port : 0x00FF
Available HW Entries: 254
--------------------------------------------------------------------------------
Rule ID : 4      Ports: 1-28
Match on:
   Source IP : 192.168.1.0
   TCP
Source Port: 210   Mask : 0x0FFF
Action:
   Mirror
================================================================================
```

```
Profile ID: 2  Profile Name: IMPBv4

Mask
   Source MAC : FF-FF-FF-FF-FF-FF
   Source IP : 255.255.255.255
Consumed HW Entries: 2
-------------------------------------------------------------------------------
Rule ID : 1      Ports: 1
 Match on
    Source MAC : 00-05-04-03-02-01    Mask : FF-FF-FF-FF-FF-FF
    Source Ip : 10.10.10.1            Mask : 255.255.255.255
 Action:
    Permit
-------------------------------------------------------------------------------
-
Rule ID : 2    Ports: 1
Match on
   Any
Action:
   Deny

===============================================================================
Profile ID: 3    Profile Name: VLAN Counter
Consumed HW Entries: 9

Profile ID: 4    Profile Name: System
Consumed HW Entries: 4

Zxxx0:admin#
```

NOTE Total User Set Entries は、ユーザが作成した ACL ルール総数を示します。Total Used HW Entries は、装置内で使用されているハードウェアエントリ総数を示します。Available HW Entries は、装置内で利用可能なハードウェアエントリ総数を示します。

各ルールに対してエントリマスクをサポートするアクセスプロファイルを表示するには：

```
Zxxx0:admin#show access_profile profile_id 2
Command: show access_profile profile_id 2

Access Profile Table

Profile ID: 2     Profile Name: 2         Type: Ethernet
Mask on
    VLAN            : 0xF
    Source MAC      : FF-FF-FF-00-00-00
    Destination MAC : 00-00-00-FF-FF-FF
Available HW Entries: 255
-------------------------------------------------------------------------------
Rule ID : 22      Ports: 1-7
Match on:
   VLAN ID          : 8                  Mask : 0xFFF
   Source MAC       : 00-01-02-03-04-05  Mask : FF-FF-FF-FF-FF-FF
   Destination MAC  : 00-05-04-03-02-00  Mask : FF-FF-FF-FF-FF-00
Action:
   Deny

Zxxx0:admin#
```

ID が 5 であるプロファイルに対するパケットコンテンツマスクプロファイルを表示するには：

```
Zxxx0:admin#show access_profile profile_id 5
Command: show access_profile profile_id 5

Access Profile Table

================================================================================
Profile ID: 5     Profile name: 5  Type: User Defined

MASK on
    offset_chunk_1 : 0      value : 0x0000FFFF

Available HW Entries : 256
================================================================================

Zxxx0:admin#
```

8.5. config time_range

● 概要

このコマンドを用いて、本装置の機能を有効にする特定のタイムレンジを定義します。タイムレンジは、曜日と時間で指定します。指定したタイムレンジは、SNTP 時刻または設定時刻に基づくことに注意してください。これらの時刻が設定されていない場合、タイムレンジは正しく機能しません。

● 構文

config time_range <range_name 32> [hours start_time < hh:mm:ss> end_time< hh:mm:ss> weekdays <daylist> | delete]

● パラメータ

<range_name 32>	タイムレンジ設定名を指定します。
hours start_time	開始時刻を指定します（24 時間形式）。例えば、19:00 は午後 7 時を意味します。単に 19 と指定することもできます。start_time は、end_time よりも小さい値になるように設定してください。 < hh:mm:ss> 時刻を指定します。
end_time	終了時刻を指定します（24 時間形式）。 < hh:mm:ss> 時刻を指定します。
weekdays	タイムレンジに含める曜日のリストを指定します。何曜日から何曜日までという範囲を定義するには、ダッシュを使用します。個々の曜日を指定するには、カンマで区切ります。mon-fri（月曜から金曜まで）や sun, mon, fri（日曜、月曜、および金曜）のように指定します。 <daylist> 曜日のリストを指定します。
delete	タイムレンジプロファイルを削除します。タイムレンジプロファイルが ACL エントリと関連付けられている場合には、このタイムレンジプロファイルの削除に失敗します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチの任意の機能を有効にするタイムレンジを設定するには：

```
Zxxx0:admin#config time_range testdaily hours start_time 12:0:0 end_time 13:0:0
weekdays mon,fri
Command: config time_range testdaily hours start_time 12:0:0 end_time 13:0:0
weekdays mon,fri


Success.


Zxxx0:admin#
```

8.6. show time_range

● 概要

このコマンドを用いて、現在のタイムレンジ設定を表示します。

● 構文

show time_range

● パラメータ

なし

● 制限

なし

● 実行例

現在のタイムレンジ設定を表示するには：

```
Zxxx0:admin#show time_range
Command: show time_range

Time Range Information
-------------------------
Range Name    :  testdaily
Weekdays      :  Mon,Fri
Start Time    :  12:00:00
End Time      :  13:00:00

Total Entries :1

Zxxx0:admin#
```

8.7. show current_config access_profile

● 概要

このコマンドを用いて、ユーザレベル権限でログインした場合には、現在の設定の ACL 部分を表示します。現在の設定全体を表示するには、管理者レベル権限でアクセスできる show config コマンドを使用します。

● 構文

show current_config access_profile

● パラメータ

なし

● 制限

なし

● 実行例

現在の設定の ACL 部分を表示するには：

```
Zxxx0:admin#show current_config access_profile
Command: show current_config access_profile

#------------------------------------------------------------------------------
# ACL
create access_profile Ethernet vlan profile_id 1
config access_profile profile_id 1 add access_id 1 ethernet vlan default port 1
permit

create access_profile ip source_ip_mask 255.255.255 profile_id 2
config access_profile profile_id 2 add access_id 1 ip source_ip 10.10.10.10 port 2
deny

#------------------------------------------------------------------------------

Zxxx0:admin#
```

8.8. config flow_meter

● 概要

このコマンドを用いて、フローベースのメータリング機能を設定します。メータリング機能では、シングルレート 2 カラー、シングルレート 3 カラー、およびツーレート 3 カラーの 3 つのモードがサポートされます。この機能のパラメータを適用する前に、アクセスルールを作成しておく必要があります。シングルレート 2 カラーモードについては、ユーザがこのルールに対する優先帯域幅を Kbps 単位で設定できます。この帯域幅超過が生じた場合、超過したパケットは、ユーザ設定に基づいて破棄されるか DSCP が書き換えられます。シングルレート 3 カラーモードについては、ユーザはコミットレート（単位 Kbps）、コミットバーストサイズ、およびピークバーストサイズを指定する必要があります。ツーレート 3 カラーモードについては、ユーザはコミットレート（単位 Kbps）、コミットバーストサイズ、ピークレート、およびピークバーストサイズを指定する必要があります。グリーンのパケットは適合動作、イエローのパケットは超過動作、レッドのパケットは違反動作としてそれぞれ扱われます。
DSCP 書き換え動作は、適合する（グリーン）パケットおよび適合しない（イエローおよびレッド）パケットに対して実行できます。ただし、イエロー/ レッドパケットの破棄を選択している場合は、DSCP 書き換え動作は実際には無効となります。シングルレート 3 カラーモードおよびツーレート 3 カラーモードのカラーマッピングは、RFC 2697 および RFC 2698 で規定されるカラーブラインド状況に従います。

● 構文

config flow_meter [profile_id <value 1-6> | profile_name <name 1-32>] access_id <value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]

● パラメータ

profile_id	
	アクセスリストプロファイルのインデックスを指定します。
	<value 1-6>
	値として 1 ～ 6 を指定します。
profile_name	
	プロファイル名を指定します。
	<name 1-32>
	プロファイル名を指定します。32 文字以内で設定します。

access_id	アクセスリストエントリのインデックスを指定します。 **<value 1-256>** 値として 1 ～ 256 を指定します。
rate	シングルレート 2 カラーモードのレートを指定します。フローに対するコミット帯域幅を Kbps 単位で指定します。 **<value 0-1048576>** 値として 0 ～ 1048576 を指定します。
burst_size	（オプション）シングルレート 2 カラーモードのバーストサイズを指定します。単位はキロバイトです。 **<value 0-131072>** 値として 0 ～ 131072 を指定します。
rate_exceed	シングルレート 2 カラーモードのコミットレートを超過したパケットの動作を指定します。動作として、以下のいずれかを指定できます。 **drop_packet** ただちにパケットを破棄します。 **remark_dscp** 指定した DSCP をパケットにマーク付けします。より高い優先度を持つパケットに対してパケットを破棄するよう設定します。 **<value 0-63>** 値として 0 ～ 63 を指定します。
tr_tcm	ツーレート 3 カラーモードを指定します。 **cir** CIR（Committed Information Rate）を指定します。単位は Kbps です。CIR は、必ず PIR（Peak Information Rate）以下に設定します。 **<value 0-1048576>** 値として 0 ～ 1048576 を指定します。 **cbs** （オプション）コミットバーストサイズを指定します。単位はキロバイトです。 **<value 0-131072>** 値として 0 ～ 131072 を指定します。 **pir** PIR を指定します。単位は Kbps です。PIR は、必ず CIR 以上に設定します。 **<value 0-1048576>** 値として 0 ～ 1048576 を指定します。 **pbs** （オプション）ピークバーストサイズを指定します。単位はキロバイトです。 **<value 0-131072>** 値として 0 ～ 131072 を指定します。
color_blind	メータモードをカラーブラインドとして指定します。デフォルトは、カラーブラインドモードです。
color_aware	メータモードをカラーアウェアとして指定します。パケットの最終カラーは、パケットの初期カラーおよびメータリング結果によって決まります。

conform	（オプション）このフィールドは、グリーンのパケットフローを示します。グリーンのパケットフローについては、このフィールドに示した値で DSCP フィールドを書き換えることができます。ユーザは、counter パラメータを使用してグリーンのパケットをカウントするよう選択することもできます。 permit グリーンのパケットフローを認証する場合に、このパラメータを指定します。 replace_dscp このパラメータに変更後の DSCP 値を入力することで、グリーンのフローにあるパケットの DSCP フィールドを書き換えることができます。 <value 0-63> 値として 0 ～ 63 を指定します。 counter （オプション）このパラメータを使用して、グリーンのフローにある指定した ACL エントリに対してパケットカウンタを有効化 / 無効化します。 enable グリーンのフローにある指定したACLエントリに対してパケットカウンタを有効化します。 disable グリーンのフローにある指定したACLエントリに対してパケットカウンタを無効化します。
exceed	（オプション）このフィールドは、イエローのパケットフローを示します。イエローのパケットフローでは、超過パケットを認証または破棄できます。ユーザは、これらのパケットの DSCP フィールドを書き換えることができます。その場合、ラジオボタンをチェックして、該当フィールドに新しい DSCP 値を入力します。 permit イエローのパケットフローを認証する場合に、このパラメータを指定します。 replace_dscp パケットの DSCP を変更するよう指定します。 <value 0-63> パケットの変更後の DSCP を入力します。値は 0 ～ 63 で指定します。 drop イエローのフローにあるパケットを破棄する場合に、このパラメータを指定します。 counter （オプション）このパラメータを使用して、グリーンのフローにある指定した ACL エントリに対してパケットカウンタを有効化 / 無効化します。 enable グリーンのフローにある指定したACLエントリに対してパケットカウンタを有効化します。 disable グリーンのフローにある指定したACLエントリに対してパケットカウンタを無効化します。

violate	このフィールドは、レッドのパケットフローを示します。レッドのパケットフローでは、超過パケットを認証または破棄できます。ユーザは、これらのパケットの DSCP フィールドを書き換えることができます。その場合、ラジオボタンをチェックして、該当フィールドに新しい DSCP 値を入力します。 permit レッドのパケットフローを認証する場合に、このパラメータを指定します。 replace_dscp パケットの DSCP を変更します。 <value 0-63> パケットの変更後の DSCP を入力します。値は 0 ～ 63 で指定します。 drop レッドのフローにあるパケットを破棄する場合に、このパラメータを指定します。 counter （オプション）このパラメータを使用して、グリーンのフローにある指定した ACL エントリに対してパケットカウンタを有効化 / 無効化します。 enable グリーンのフローにある指定したACLエントリに対してパケットカウンタを有効化します。 disable グリーンのフローにある指定したACLエントリに対してパケットカウンタを無効化します。
sr_tcm	シングルレート 3 カラーモードを指定します。 cir CIR（Committed Information Rate）を指定します。単位は Kbps です。 <value 0-1048576> 値として 0 ～ 1048576 を指定します。 cbs コミットバーストサイズを指定します。単位はキロバイトです。 <value 0-131072> 値として 0 ～ 131072 を指定します。 ebs 超過バーストサイズを指定します。単位はキロバイトです。 <value 0-131072> 値として 0 ～ 131072 を指定します。
color_blind	メータモードをカラーブラインドとして指定します。デフォルトは、カラーブラインドモードです。
color_aware	メータモードをカラーアウェアとして指定します。パケットの最終カラーは、パケットの初期カラーおよびメータリング結果によって決まります。

conform	（オプション）このフィールドは、グリーンのパケットフローを示します。グリーンのパケットフローについては、このフィールドに示した値で DSCP フィールドを書き換えることができます。ユーザは、counter パラメータを使用してグリーンのパケットをカウントするよう選択することもできます。 permit グリーンのパケットフローを認証する場合に、このパラメータを指定します。 replace_dscp このパラメータに変更後の DSCP 値を入力することで、グリーンのフローにあるパケットの DSCP フィールドを書き換えることができます。 <value 0-63> 値として 0 ～ 63 を指定します。 counter （オプション）このパラメータを使用して、グリーンのフローにある指定した ACL エントリに対してパケットカウンタを有効化 / 無効化します。 enable グリーンのフローにある指定したACLエントリに対してパケットカウンタを有効化します。 disable グリーンのフローにある指定したACLエントリに対してパケットカウンタを無効化します。
exceed	（オプション）このフィールドは、イエローのパケットフローを示します。イエローのパケットフローでは、超過パケットを認証または破棄できます。ユーザは、これらのパケットの DSCP フィールドを書き換えることができます。その場合、ラジオボタンをチェックして、該当フィールドに新しい DSCP 値を入力します。 permit イエローのパケットフローを認証する場合に、このパラメータを指定します。 replace_dscp パケットの DSCP を変更します。 <value 0-63> パケットの変更後の DSCP を入力します。値は 0 ～ 63 で指定します。 drop イエローのフローにあるパケットを破棄する場合に、このパラメータを指定します。 counter （オプション）このパラメータを使用して、グリーンのフローにある指定した ACL エントリに対してパケットカウンタを有効化 / 無効化します。 enable グリーンのフローにある指定したACLエントリに対してパケットカウンタを有効化します。 disable グリーンのフローにある指定したACLエントリに対してパケットカウンタを無効化します。

violate	このフィールドは、レッドのパケットフローを示します。レッドのパケットフローでは、超過パケットを認証または破棄できます。ユーザは、これらのパケットの DSCP フィールドを書き換えることができます。その場合、ラジオボタンをチェックして、該当フィールドに新しい DSCP 値を入力します。 permit レッドのパケットフローを認証する場合に、このパラメータを指定します。 replace_dscp パケットの DSCP を変更します。 <value 0-63> パケットの変更後の DSCP を入力します。値は 0 ～ 63 で指定します。 drop レッドのフローにあるパケットを破棄する場合に、このパラメータを指定します。 counter （オプション）このパラメータを使用して、グリーンのフローにある指定した ACL エントリに対してパケットカウンタを有効化 / 無効化します。 enable グリーンのフローにある指定したACLエントリに対してパケットカウンタを有効化します。 disable グリーンのフローにある指定したACLエントリに対してパケットカウンタを無効化します。 deleteこのパラメータを使用して、指定したフローメータを削除します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ツーレート 3 カラーのフローメータを設定するには：

```
Zxxx0:admin#config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 conform replace_dscp 21 exceed drop violate permit
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 conform replace_dscp 21 exceed drop violate permit

Success.

Zxxx0:admin#
```

適合する（グリーン）および適合しない（イエローおよびレッド）パケットに対して実行する DSCP 書き換え動作を変更するには：

```
Zxxx0:admin# config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 exceed permit replace_dscp 21 violate permit replace_dscp 21
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 exceed permit replace_dscp 21 violate permit replace_dscp 21

Success.

Zxxx0:admin#
```

8.9. show flow_meter

● 概要

このコマンドを用いて、フローメータテーブルを表示します。

● 構文

show flow_meter {[profile_id <value 1-6> | profile_name <name 1-32>] {access_id <value 1-256>}}

● パラメータ

profile_id（オプション）プロファイル ID を指定します。 <value 1-6> プロファイル ID を指定します。値として 1 ～ 6 を入力します。
profile_name （オプション）プロファイル名を指定します。 <name 1-32> プロファイル名を指定します。32 文字以内で設定します。
access_id（オプション）アクセス ID を指定します。 <value 1-256> アクセス ID を指定します。値として 1 ～ 256 を入力します。

● 制限

なし

● 実行例

フローメータ設定を表示するには：

```
Zxxx0:admin#show flow_meter
Command: show flow_meter

Flow Meter Information
------------------------------------------------------------------------------
Profile ID:1     Aceess ID:1     Mode : trTCM / ColorBlind
CIR(Kbps):1000     CBS(Kbyte):200      PIR(Kbps):2000     PBS(Kbyte):200
Action:
      Conform : Permit                        Counter: Disabled
       Exceed : Permit     Replace DSCP: 21   Counter: Disabled
      Violate : Permit     Replace DSCP: 21   Counter: Disabled
------------------------------------------------------------------------------

Total Entries: 1

Zxxx0:admin#
```

9. ARP コマンド

ARP（Address Resolution Protocol）は、IP アドレスから MAC アドレスを求めるプロトコルです。
スイッチは、同一ネットワーク上の機器に ARP 要求を送信し、機器からの返信に基づき IP アドレスと MAC アドレスの対応を ARP テーブルと呼ばれる表データで管理します。

```
Interface       IP Address       MAC Address       Type
--------------- ---------------  ----------------- ---------------
System          10.0.0.0         FF-FF-FF-FF-FF-FF Local/Broadcast
System          10.90.90.90      00-01-02-03-04-00 Local
System          10.255.255.255   FF-FF-FF-FF-FF-FF Local/Broadcast
```

ARP テーブルは、通常自動的に作成されます（ダイナミックエントリ）が、手動で書き込むこともできます（スタティックエントリ）。ダイナミックエントリは、参照されない状態が指定の時間（エージングタイム）を過ぎると消去されますが、スタティックエントリは意図的に削除しない限り保持されます。

create arpentry <ipaddr> <macaddr>
delete arpentry [<ipaddr> | all]
config arpentry <ipaddr> <macaddr>
config arp_aging time <min 0-65535>
show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static | mac_address <macaddr>}
clear arptable
show ipfdb {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}

9.1. create arpentry

● 概要

このコマンドを用いて、スイッチの ARP テーブルに IP アドレスおよび対応する MAC アドレスを書き込みます。

● 構文

create arpentry <ipaddr> <macaddr>

● パラメータ

<ipaddr> エンドノードまたはステーションの IP アドレスです。
<macaddr> 上記の IP アドレスに対応する MAC アドレスです。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP アドレス 10.48.74.121 および MAC アドレス 00:50:BA:00:07:36 のスタティック ARP エントリを作成するには：

```
Zxxx0:admin#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

Zxxx0:admin#
```

9.2. delete arpentry

● 概要

このコマンドを用いて、前述の create arpentry コマンドで作成したスタティック ARP エントリを削除します。削除するには、エントリの IP アドレスを指定するか all（すべて）を指定します。all を指定すると、スイッチの ARP テーブルを削除します。

● 構文

delete arpentry [<ipaddr> | all]

● パラメータ

<ipaddr>	エンドノードまたはステーションの IP アドレスです。
all	すべての ARP エントリを削除します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ARP テーブルから IP アドレス 10.48.74.121 のエントリを削除するには：

```
Zxxx0:admin#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

Zxxx0:admin#
```

9.3. config arpentry

● 概要

このコマンドを用いて、ARP テーブルにスタティックエントリを設定します。エントリの IP アドレスと MAC アドレスを指定します。

● 構文

config arpentry <ipaddr> <macaddr>

● パラメータ

<ipaddr> エンドノードまたはステーションの IP アドレスです。
<macaddr> 上記の IP アドレスに対応する MAC アドレスです。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP アドレス 10.48.74.121 および MAC アドレス 00:50:BA:00:07:36 のスタティック ARP エントリを作成するには：

```
Zxxx0:admin#config arpentry 10.48.74.121 00-50-BA-00-07-36
Command: config arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

Zxxx0:admin#
```

9.4. config arp_aging time

● 概要

このコマンドを用いて、ある ARP エントリがスイッチの ARP テーブルから破棄されるまでに、アクセスされることなく ARP テーブル内に保持される最大時間（分）を設定します。

● 構文

config arp_aging time <min 0-65535>

● パラメータ

<min 0-65535> ARP エージアウトタイムを分で指定します。デフォルトは、20 分です。範囲は、0 ～ 65535 分です。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ARP エージングタイムを設定するには：

```
Zxxx0:admin#config arp_aging time 30
Command: config arp_aging time 30

Success.

Zxxx0:admin#
```

9.5. show arpentry

● 概要

このコマンドを用いて、ARP（Address Resolution Protocol）テーブルを表示します。IP アドレス、インターフェース名、またはスタティックエントリに基づいて表示をフィルタリングします。

● 構文

show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static | mac_address <macaddr>}

● パラメータ

ipif	ARP テーブルエントリが作成されたエンドノードまたはステーションが存在する IP インターフェース名です。 <ipif_name 12> IP インターフェース名を指定します。12 文字以内で設定します。
ipaddress	エンドノードまたはステーションの IP アドレスです。 <ipaddr> IP アドレスを指定します。
static	ARP テーブルへのスタティックエントリを表示します。
mac_address	MAC アドレスに基づいて ARP エントリを表示します。 <macaddr> MAC アドレスを指定します。

NOTE パラメータを指定しなかった場合、すべての ARP エントリを表示します。

● 制限

なし

● 実行例

ARP テーブルを表示するには：

```
Zxxx0:admin# show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface       IP Address        MAC Address         Type
--------------  ----------------  ------------------  ---------------
System          10.0.0.0          FF-FF-FF-FF-FF-FF   Local/Broadcast
System          10.90.90.90       00-01-02-03-04-00   Local
System          10.255.255.255    FF-FF-FF-FF-FF-FF   Local/Broadcast

Total Entries: 3

Zxxx0:admin#
```

9.6. clear arptable

● 概要

このコマンドを用いて、ARP テーブルからダイナミックエントリを削除します。スタティック ARP エントリは影響を受けません。

● 構文

clear arptable

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ARP テーブルからダイナミックエントリを削除するには：

```
Zxxx0:admin#clear arptable
Command: clear arptable

Success.

Zxxx0:admin#
```

9.7. show ipfdb

● 概要

このコマンドを用いて、本装置の IP アドレスフォワーディングテーブルを表示します。

● 構文

show ipfdb {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}

● パラメータ

ip_address	（オプション）フォワーディングテーブルの IP アドレスを指定します。 <ipaddr> 表示する IP アドレスを入力します。
interface	（オプション）フォワーディングテーブルのインターフェース名を指定します。 <ipif_name 12> インターフェース名を入力します。名前は 12 文字以内で設定できます。
port	（オプション）表示するポートを指定します。 <port> 表示するポート番号を入力します。

● 制限

なし

● 実行例

本装置の IP アドレスフォワーディングテーブルを表示するには：

```
Zxxx0:admin# show ipfdb
Command: show ipfdb

Interface     IP Address       Port      Learned
------------  ---------------- --------- ---------

Total Entries: 0

Zxxx0:admin#
```

10. Asymmetric VLAN コマンド

Asymmetric VLAN とは、VLAN 同士の通信を遮断しつつ、複数の VLAN からインターネットや社内サーバ等の共有リソースにアクセスしたい場合に利用するしくみの 1 つです。特定のポートを複数の VLAN に所属させます。タグ付き VLAN が利用できない場合などに利用します。

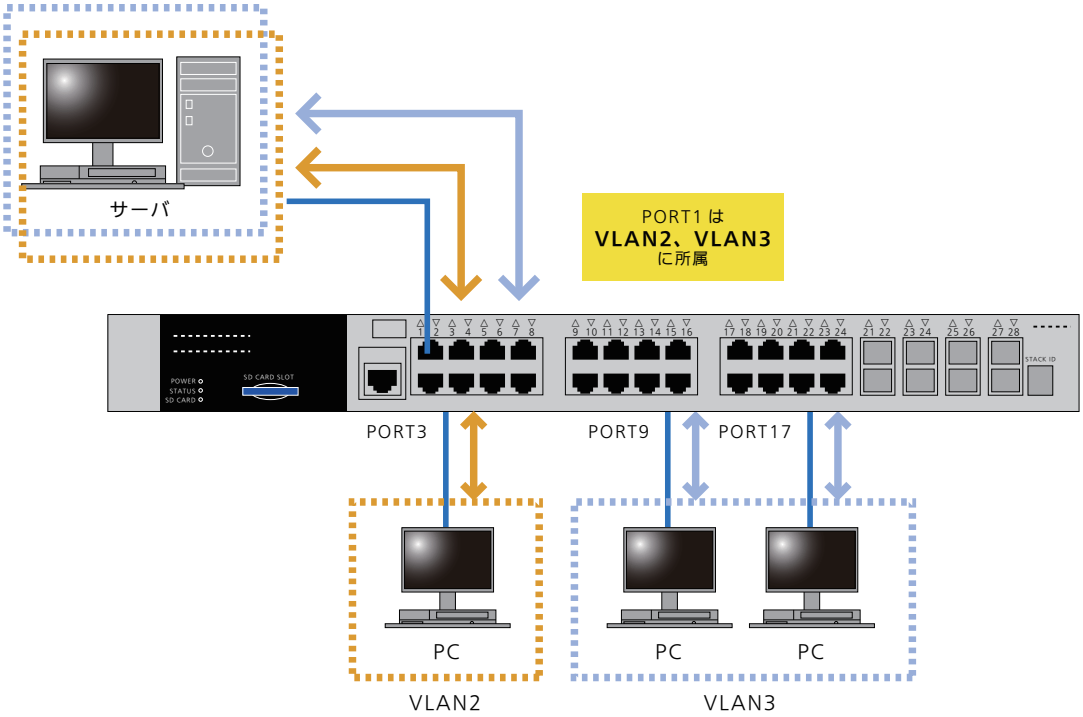


図 10-1　Asymmetric VLAN の概略

Port1：VLAN2、VLAN3 に所属
Port3：VLAN2 に所属
Port9、17：VLAN3 に所属

上記の例では、サーバ以外の VLAN2、VLAN3 相互の通信は遮断されますが、VLAN2、VLAN3 の各端末からのサーバの利用は可能です。

enable asymmetric_vlan disable asymmetric_vlan show asymmetric_vlan

10.1. enable asymmetric_vlan

● 概要

このコマンドを用いて、Asymmetric VLAN 機能を有効にします。

● 構文

enable asymmetric_vlan

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

Asymmetric VLAN 設定を有効にするには：

```
Zxxx0:admin# enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

Zxxx0:admin#
```

10.2. disable asymmetric_vlan

● 概要

このコマンドを用いて、Asymmetric VLAN 機能を無効にします。

● 構文

disable asymmetric_vlan

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

Asymmetric VLAN 設定を無効にするには：

```
Zxxx0:admin# disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

Zxxx0:admin#
```

10.3. show asymmetric_vlan

● 概要

このコマンドを用いて、Asymmetric VLAN 機能を表示します。

● 構文

show asymmetric_vlan

● パラメータ

なし

● 制限

なし

● 実行例

Asymmetric VLAN を表示するには：

```
Zxxx0:admin# show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric Vlan : Disabled

Zxxx0:admin#
```

11.Auto Configuration コマンド

Auto Configuration 機能を有効にすると、本製品は起動の際、あらかじめ設置しておいた TFTP サーバから本製品の設定ファイルを読み込むようになります。

show autoconfig enable autoconfig disable autoconfig

11.1. show autoconfig

● 概要

このコマンドを用いて、TFTP サーバから自動的に設定を取得する機能の状態を表示します。

● 構文

show autoconfig

● パラメータ

なし

● 制限

なし

● 実行例

Auto Configuration 機能の状態を表示するには：

```
Zxxx0:admin#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled

Zxxx0:admin#
```

11.2. enable autoconfig

● 概要

このコマンドを用いて、DHCP 応答パケットのオプションに基づいて、TFTP サーバから設定を自動的に取得する機能を有効にします。この方法を用いるには、TFTP サーバ IP アドレスおよび設定ファイル名情報を配信できるよう、あらかじめ DHCP サーバに設定しておく必要があります。

● 構文

enable autoconfig

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

DHCP Auto Configuration 機能を有効にするには：

```
Zxxx0:admin#enable autoconfig
Command: enable autoconfig

Success.

Zxxx0:admin#
```

11.3. disable autoconfig

● 概要

このコマンドを用いて、TFTP サーバから自動的に設定を取得する機能を無効にします。

● 構文

disable autoconfig

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

Auto Configuration 機能を無効にするには：

```
Zxxx0:admin#disable autoconfig
Command: disable autoconfig

Success.

Zxxx0:admin#
```

12. 基本的な IP コマンド

ここでは本装置の IP アドレス設定を行います。

● IPv6 Link-Local アドレス

通常 IPv6 アドレスが設定されていない状態では、Link-Local アドレスも未設定となります。Link-Local アドレスの自動設定を有効にすると、IPv6 アドレスを設定していない状態でも Link-Local アドレスが自動的に設定され、ローカルネットワーク内での通信が可能になります。

> **NOTE** デフォルトゲートウェイの設定は「IPルーティングコマンド」章を参照してください。

● IP アドレス簡単設定 (IP setup interface)

弊社製スイッチングハブのサポートツール「ZEQUOASSIST」やパナソニック製ネットワークカメラに搭載された IP アドレス簡単設定プロトコルに対応しており、コンソールケーブルを利用しなくともネットワーク経由で簡単に本装置へ IP アドレスの設定を行うことができます。セキュリティ対策のため、本装置に IP アドレスが既に設定されている場合は、起動後 20 分を経過すると本機能による設定変更は受け付けません。

---

config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} bootp | dhcp | ipv6 [ipv6address <ipv6networkaddr> | state [enable | disable]] | ipv4 state [enable | disable] | ip_directed_broadcast [enable | disable] | dhcpv6_client [enable | disable]]
delete ipif <ipif_name 12> ipv6address <ipv6networkaddr>
enable ipif <ipif_name 12>
disable ipif <ipif_name 12>
show ipif {<ipif_name 12>}
enable ipif_ipv6_link_local_auto <ipif_name 12>
disable ipif_ipv6_link_local_auto <ipif_name 12>
show ipif_ipv6_link_local_auto {<ipif_name 12>}
enable ip_setup_interface
disable ip_setup_interface
show ip_setup_interface

12.1. config ipif

● 概要

IP インターフェースのパラメータを設定します。IPv4 については、IP アドレスの取得方法として唯一指定できるのはシステムインターフェースです。モードが BOOTP または DHCP に設定されている場合、IPv4 アドレスはプロトコル動作を介して取得されます。IP アドレスを手動で設定することはできません。最初にモードが BOOTP または DHCP に設定されており、後でユーザが IP アドレスを設定した場合、モードは手動設定モードに変更されます。IPv6 では、同一 IP インターフェースに対して複数のアドレスを定義できます。

● 構文

config ipif <ipif_name 12> {ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} bootp | dhcp | ipv6 [ipv6address <ipv6networkaddr> | state [enable | disable]] | ipv4 state [enable | disable] | ip_directed_broadcast [enable | disable] | dhcpv6_client [enable | disable]]

● パラメータ

ipif	設定した IP インターフェースを指定します。 <ipif_name 12> 使用する IP インターフェース名を入力します。名前は 12 文字以内で設定できます。デフォルトのインターフェースは System です。
ipaddress	（オプション）作成する IP インターフェースの IP アドレスおよびネットマスクです。 <network_address> 従来のフォーマットでアドレスおよびマスク情報を指定します（例えば、10.1.2.3/255.0.0.0 または CIDR フォーマットにて 10.1.2.3/8）。
vlan	（オプション）IP インターフェースに対応する VLAN 名です。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
state	IP インターフェースを有効または無効にします。 enable IP インターフェースを有効にします。 disable IP インターフェースを無効にします。
bootp	BOOTP による IP アドレスの自動割り当てを指定します。
dhcp	DHCP による IP アドレスの自動割り当てを指定します。
ipv6	IPv6 関連のパラメータです。 ipv6address 作成する IPv6 アドレスおよび IPv6 アドレスのサブネットプレフィックスです。 <ipv6networkaddr> 作成する IPv6 アドレスおよび IPv6 アドレスのサブネットプレフィックスです。 state IP インターフェースの IPv6 状態を有効または無効にします。 enable IP インターフェースの IPv6 状態を有効にします。 disable IP インターフェースの IPv6 状態を無効にします。

ipv4 state	IPv4 インターフェースの状態を指定します。 **enable** IP インターフェースの IPv4 状態を有効にします。 **disable** IP インターフェースの IPv4 状態を無効にします。
dhcpv6_client	DHCPv6 クライアントの状態を指定します。 **enable** DHCPv6 クライアントを有効にします。 **disable** DHCPv6 クライアントを無効にします。
ip_directed_broadcast	インターフェースの IP ディレクティッドブロードキャスト状態を指定します。 **enable** インターフェースの IP ディレクティッドブロードキャスト状態を有効にします。 **disable** インターフェースの IP ディレクティッドブロードキャスト状態を無効にします。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP インターフェース System を設定するには：

```
Zxxx0:admin#config ipif System vlan v1
Command: config ipif System vlan v1

Success.

Zxxx0:admin#
```

12.2. delete ipif

● 概要

このコマンドを用いて、インターフェースまたは IPv6 アドレスを削除します。

● 構文

delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]

● パラメータ

<ipif_name 12>	
	インターフェース名です。
	ipv6address
	（オプション）削除する IPv6 ネットワークアドレスです。
	<ipv6networkaddr>
	削除する IPv6 ネットワークアドレスです。
all	IP インターフェース System を除くすべての IP インターフェースが削除されます。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

インターフェース petrovic1 を削除するには：

```
Zxxx0:admin#delete ipif petrovic1
Command: delete ipif petrovic1

Success.

Zxxx0:admin#
```

12.3. enable ipif

● 概要

このコマンドを用いて、IP インターフェースの状態を有効にします。状態を有効にすると、IP インターフェース上に IPv4 アドレスを設定したときに IPv4 処理が開始します。IPv6 処理は、IP インターフェース上で IPv6 アドレスを明示的に設定したときに開始します。

● 構文

enable ipif [<ipif_name 12> | all]

● パラメータ

<ipif_name 12>	インターフェース名です。
all	すべての IP インターフェースです。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

インターフェース petrovic1 の状態を有効にするには：

```
Zxxx0:admin#enable ipif petrovic1
Command: enable ipif petrovic1

Success.

Zxxx0:admin#
```

12.4. disable ipif

● 概要

このコマンドを用いて、インターフェースの状態を無効にします。

● 構文

disable ipif [<ipif_name 12> | all]

● パラメータ

<ipif_name 12>	インターフェース名です。
all	すべての IP インターフェースです。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

インターフェースの状態を無効にするには：

```
Zxxx0:admin#disable ipif petrovic1
Command: disable ipif petrovic1

Success.

Zxxx0:admin#
```

12.5. show ipif

● 概要

このコマンドを用いて、IP インターフェース設定を表示します。

● 構文

show ipif {<ipif_name 12>}

● パラメータ

<ipif_name 12> （オプション）インターフェース名です。

● 制限

なし

● 実行例

IP インターフェース設定を表示するには：

```
Zxxx0:admin#show ipif
Command: show ipif

IP Interface                : System
VLAN Name                   : default
Interface Admin State       : Enabled
DHCPv6 Client State         : Disabled
Link Status                 : LinkUp
IPv4 Address                : 0.0.0.0/0 (Manual)  Primary
IPv4 State                  : Enabled
IPv6 State                  : Enabled


Total Entries: 1

Zxxx0:admin#
```

12.6. enable ipif_ipv6_link_local_auto

● 概要

このコマンドを用いて、明示的に設定された IPv6 アドレスがない場合に、リンクローカルアドレスの自動設定を有効にします。IPv6 アドレスが明示的に設定されている場合、リンクローカルアドレスは自動的に設定され、IPv6 処理が開始します。IPv6 アドレスが明示的に設定されていない場合、デフォルトではリンクローカルアドレスは設定されず、IPv6 処理は無効です。この自動設定を有効にすることで、リンクローカルアドレスは自動的に設定され、IPv6 処理が開始します。

● 構文

enable ipif_ipv6_link_local_auto <ipif_name 12>

● パラメータ

<ipif_name 12> インターフェース名です。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

インターフェースでリンクローカルアドレスの自動設定を有効にするには：

```
Zxxx0:admin#enable ipif_ipv6_link_local_auto System
Command: enable ipif_ipv6_link_local_auto System

Success.

Zxxx0:admin#
```

12.7. disable ipif_ipv6_link_local_auto

● 概要

このコマンドを用いて、明示的に設定された IPv6 アドレスがない場合に、リンクローカルアドレスの自動設定を無効にします。

● 構文

disable ipif_ipv6_link_local_auto <ipif_name 12>

● パラメータ

<ipif_name 12> インターフェース名です。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

インターフェースでリンクローカルアドレスの自動設定を無効にするには：

```
Zxxx0:admin#disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System

Success.

Zxxx0:admin#
```

12.8. show ipif_ipv6_link_local_auto

● 概要

このコマンドを用いて、リンクローカルアドレスの自動設定状態を表示します。

● 構文

show ipif_ipv6_link_local_auto {<ipif_name 12>}

● パラメータ

<ipif_name 12> （オプション）インターフェース名です。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

リンクローカルアドレスの自動設定状態を表示するには：

```
Zxxx0:admin#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System          Automatic Link Local Address: Disabled

Zxxx0:admin#
```

12.9. enable ip_setup_interface

● 概要

このコマンドを用いて、IP アドレス簡単設定機能を有効にします。工場出荷時設定は有効です。
本機能が有効の場合、「ZEQUOASSIST」をはじめとする IP アドレス簡単設定対応アプリケーションからの機器探索や設定を受け付けます。セキュリティ対策のため、IP アドレスが既に設定されている場合は、起動後 20 分を経過すると機器探索のみ受付け、設定は無視されます。

● 構文

enable ip_setup_interface

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP アドレス簡単設定を有効にするには：

```
Zxxx0:admin#enable ip_setup_interface
Command: enable ip_setup_interface

Success.

Zxxx0:admin#
```

12.10. disable ip_setup_interface

● 概要

このコマンドを用いて、IP アドレス簡単設定機能を無効にします。

● 構文

disable ip_setup_interface

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP アドレス簡単設定を無効にするには：

```
Zxxx0:admin#disable ip_setup_interface
Command: disable ip_setup_interface

Success.

Zxxx0:admin#
```

12.11. show ip_setup_interface

● 概要

このコマンドを用いて、IP アドレス簡単設定の状態を表示します。

● 構文

show ip_setup_interface

● パラメータ

なし

● 制限

なし

● 実行例

IP アドレス簡単設定の状態を表示するには：

```
Zxxx0:admin#show ip_setup_interface
Command: show ip_setup_interface

IP Setup Interface: Enabled

Zxxx0:admin#
```

13.起動コマンド

ここでは、この装置の起動に用いる設定ファイルおよびファームウェアの指定を行います。
最優先で読み込まれる 1st Bootup ファイルは、SD カード上の固定ファイル名である ”sd_config.cfg” および ”sd_runtime.rom” に指定されており、変更はできません。SD カードブートを行う際はこれらのファイル名に変更後 SD カードへ保存し、SD カードスロットへ挿入後に電源を投入してください。
SD カード上に該当ファイルがない、または SD カードが挿入されていない場合は、2nd Bootup ファイルが起動ファイルとして読み込まれます。

show boot_file
config firmware image {unit <unit_id>} <pathname> boot_up
config configuration {unit <unit_id>} <pathname> [boot_up | active]

13.1. show boot_file

● 概要

このコマンドを用いて、起動に用いる設定ファイルおよびファームウェアを表示します。

● 構文

show boot_file

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

起動ファイルを表示するには：

```
Zxxx0:admin#show boot_file
Command: show boot_file

  *1st Bootup Firmware         : /d:/sd_runtime.rom
  *1st Bootup Configuration    : /d:/sd_config.cfg
      *Can not change 1st Bootup File

  2nd Bootup Firmware          : /c:/runtime.had
  2nd Bootup Configuration     : /c:/config.cfg

  Actual Bootup Firmware       : /c:/runtime.had
  Actual Bootup Configuration  : /c:/config.cfg

  SD card: d drive, FLASH: c drive
Zxxx0:admin#
```

13.2. config firmware image

● 概要

このコマンドを用いて、起動用ファームウェアの指定をします。

● 構文

config firmware image {unit <unit_id>} <pathname> boot_up

● パラメータ

unit	（オプション）スタック構成時のユニット ID を指定します。指定がない場合はマスターユニットが対象になります。 <unit_id 1-4> 設定対象とするユニット ID を 1 ～ 4 の間で指定します。
<pathname> 対象とするファイルのパスを指定します。	

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

スタックユニット ID:2 の起動用ファームウェアを指定するには：

```
Zxxx0:admin#config firmware image unit 2 c:/updated_firmware.rom boot_up
Command: config firmware image unit 2 c:/updated_firmware.rom boot_up

Success.

Zxxx0:admin#
```

13.3. config configuration

● 概要

このコマンドを用いて、起動用設定ファイルの指定をします。

● 構文

config configuration {unit <unit_id>} <pathname> [boot_up | active]

● パラメータ

unit	（オプション）スタック構成時のユニット ID を指定します。指定がない場合は Master Box が対象になります。 <unit_id 1-4> 設定対象とするユニット ID を 1 ～ 4 の間で指定します。
<pathname>	対象とするファイルのパスを指定します。
boot_up	（オプション）起動用設定ファイルに指定します。
active	（オプション）設定ファイルの内容を直ちに適用します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

起動用設定ファイルを指定するには：

```
Zxxx0:admin#config configuration c:/new_config.cfg boot_up
Command: config configuration c:/new_config.cfg boot_up

Success.

Zxxx0:admin#
```

14. BPDU Attack Protection コマンド

BPDU（Bridge Protocol Data Unit）とは、スパニングツリープロトコルで、ループの検出を行うためのパケットです。通常は、特定のポート以外から受信されることはありませんが、想定外のポートで BPDU パケットが受信された場合、ループ障害の発生や不正なスイッチの追加による経路変更の可能性があります。
BPDU Attack Protection は、想定外の BPDU パケットを受信した場合に、パケットを破棄したり、ポートをシャットダウンするなどの処置を設定し、ネットワークを保護する機能です。

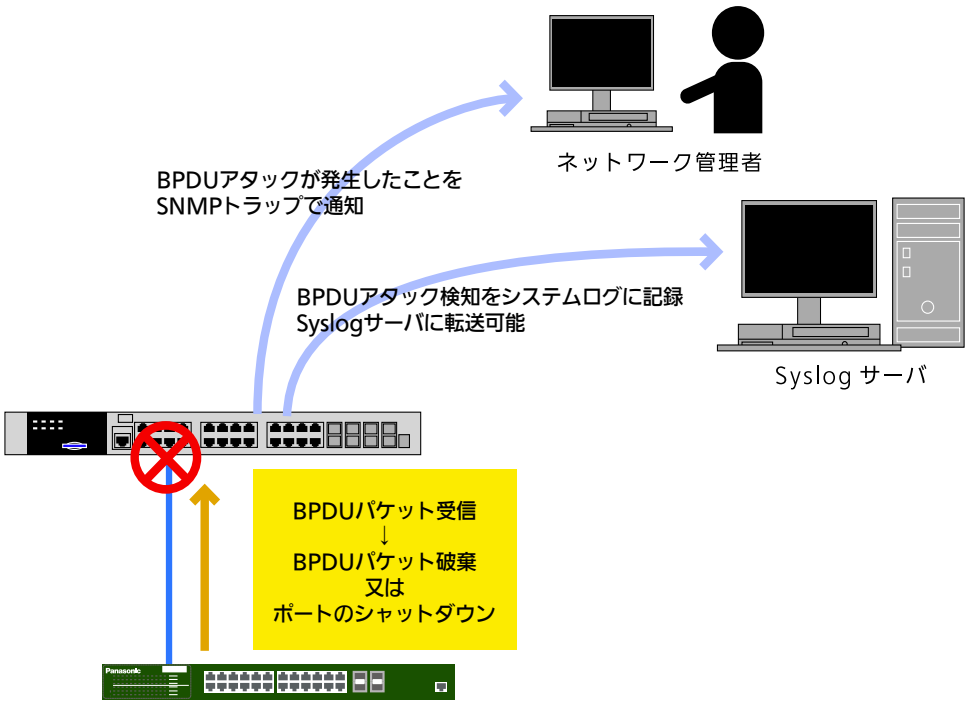


図 14-1　BPDU Attack Protection の概略

保護機能が働きパケットの破棄やポートのシャットダウンが起きた場合、SNMP トラップでの通知やログへの記録を行うよう設定することができます。また、指定した時間経過後に自動復旧するように設定したり、ネットワーク管理者による復旧に任せることもできます。

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}(1)
config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]
config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]
enable bpdu_protection
disable bpdu_protection
show bpdu_protection {ports {<portlist>}}

14.1. config bpdu_protection ports

● 概要

このコマンドを用いて、BPDU Protection のポート状態およびモードを設定します。

● 構文

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]} (1)

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	システムのすべてのポートを設定します。
state	BPDU Protection 状態を指定します。デフォルトの状態では無効です。 enable BPDU Protection 状態を有効にします。 disable BPDU Protection 状態を無効にします。
mode	BPDU Protection モードを指定します。デフォルトのモードは shutdown です。 drop 想定外のポートで BPDU パケットを検出した場合に、受信したすべての BPDU パケットを破棄します。 block 想定外のポートで BPDU パケットを検出した場合に、（BPDU および正常なパケットを含む）すべてのパケットを破棄します。 shutdown 想定外のポートで BPDU パケットを検出した場合に、ポートをシャットダウンします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート状態を enable にし、drop モードを設定するには：

```
Zxxx0:admin#config bpdu_protection ports 1 state enable mode drop
Command: config bpdu_protection ports 1 state enable mode drop

Success.
Zxxx0:admin#
```

14.2. config bpdu_protection recovery_timer

● 概要

想定外のポートで BPDU パケットを検出した場合に、設定に基づいて無効にするかブロックすることができます。アタックが検出された状態は、手動で修復するか、自動修復することができます。このコマンドを用いて、自動修復タイマーを設定します。ポートを手動で修復するには、ユーザがポートを無効にして、再度有効にする必要があります。

● 構文

config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]

● パラメータ

<sec 60-1000000>	ポートを修復する自動修復機能で使用するタイマーを秒で指定します。有効な範囲は60～1000000秒です。自動修復時間は、デフォルトで 60 秒に設定されています。
infinite	ポートが自動修復されないことを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチ全体の BPDU Protection 修復タイマーを 120 秒に設定するには：

```
Zxxx0:admin#config bpdu_protection recovery_timer 120
Command: config bpdu_protection recovery_timer 120

Success.

Zxxx0:admin#
```

14.3. config bpdu_protection

● 概要

このコマンドを用いて、BPDU Protection のトラップ状態またはログ状態を設定します。

● 構文

config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]

● パラメータ

trap	トラップ状態を指定します。
log	ログ状態を指定します。
none	attack_detected および attack_cleared のどちらであっても、トラップ通知およびログへの記録を行わないことを指定します。
attack_detected	BPDU アタックを検出したときに、イベントのログへの記録やトラップ通知を行うことを指定します。
attack_cleared	BPDU アタックをクリアしたときに、イベントのログへの記録やトラップ通知を行うことを指定します。
both	attack_detected および attack_cleared のどちらのイベントでも、トラップ通知またはログへの記録を行うことを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチ全体の BPDU Protection トラップ状態として both を設定するには：

```
Zxxx0:admin#config bpdu_protection trap both
Command: config bpdu_protection trap both

Success.

Zxxx0:admin#
```

14.4. enable bpdu_protection

● 概要

このコマンドを用いて、スイッチ全体で BPDU Protection をグローバルに有効にします。

● 構文

enable bpdu_protection

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチ全体で BPDU Protection を有効にするには：

```
Zxxx0:admin#enable bpdu_protection
Command: enable bpdu_protection

Success.

Zxxx0:admin#
```

14.5. disable bpdu_protection

● 概要

このコマンドを用いて、スイッチ全体で BPDU Protection をグローバルに無効にします。

● 構文

disable bpdu_protection

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

BPDU Protection を無効にするには：

```
Zxxx0:admin#disable bpdu_protection
Command: disable bpdu_protection

Success.

Zxxx0:admin#
```

14.6. show bpdu_protection

● 概要

このコマンドを用いて、BPDU Protection のグローバル設定またはポート毎の設定、さらには現在のステータスを表示します。

● 構文

show bpdu_protection {ports {<portlist>}}

● パラメータ

ports	（オプション）表示するすべてのポートを指定します。
<portlist>	（オプション）表示するポートの範囲を指定します。

● 制限

なし

● 実行例

スイッチ全体の BPDU Protection 情報を表示するには：

```
Zxxx0:admin#show bpdu_protection
Command: show bpdu_protection

BPDU Protection Global Settings
---------------------------------------
BPDU Protection Status        : Disabled
BPDU Protection Recover Time  : 60 seconds
BPDU Protection Trap State    : None
BPDU Protection Log State     : Both

Zxxx0:admin#
```

ポート 1 ～ 3 の BPDU Protection ステータスを表示するには：

```
Zxxx0:admin#show bpdu_protection ports 1-3
Command: show bpdu_protection ports 1-3

Port  State         Mode       Status
----- -----------  ---------- -----------
1     Disabled     Shutdown   Normal
2     Disabled     Shutdown   Normal
3     Disabled     Shutdown   Normal

Zxxx0:admin#
```

15. ケーブル診断コマンド

本装置のポートに接続されたツイストペアケーブルのリンク状態、障害の状態やおおよその障害位置の診断を行います。ケーブルの断線、ショート、クロストークを診断し、断線やショートがない場合にはケーブル長を計測できます。

NOTE 光ファイバケーブルの診断には対応していません。

cable_diag ports [<portlist> | all]

15.1. cable_diag ports

● 概要

このコマンドを用いて、ツイストペアケーブルをテストします。
1000Base-T リンクスピードの場合、ツイストペアケーブルの 4 ペアを診断します。

ケーブルの障害としては、断線、ショート、クロストークがあります。
- **断線**は、ケーブルの特定の位置で、接続がないこと（断線）を意味します。
- **ショート**は、ケーブルの特定の位置で、ショート問題が発生していることを意味します。
- **クロストーク**は、ケーブルの特定の位置で、クロストーク問題が発生していることを意味します。

ギガビットイーサネットポートの場合：
- **リンクパートナの電源オンで障害が発生せず**、Link Up 状態である場合、このコマンドを実行してもケーブル長を計測できません。
- **リンクパートナの電源オンで障害が発生した**場合、このコマンドを実行することで障害が Open、Short、Crosstalk のいずれであるかを診断できます。この場合、このコマンドを実行することで障害位置も診断できます。
- **リンクパートナの電源オフで障害が発生せず**、Link Down 状態である場合、このコマンドを実行してもケーブル長を計測できません。
- **リンクパートナの電源オフで障害が発生した**場合、このコマンドを実行することで障害が Open、Short、Crosstalk のいずれであるかを診断できます。この場合、このコマンドを実行することで障害位置も診断できます。
- **リンクパートナが検出できず、障害が発生せず**、Link Up 状態である場合、このコマンドを実行することでケーブル長を計測できます。
- **リンクパートナが検出できず、障害が発生した**場合、このコマンドを実行することで障害が Open、Short、Crosstalk のいずれであるかを診断できます。この場合、このコマンドを実行することで障害位置も診断できます。

計測可能なケーブル長範囲は、以下のとおりです。
- 50m 未満（<50m）
- 50m 以上 80m 以下（50 ～ 80m）
- 80m 以上 100m 以下（80 ～ 100m）
- 100m 以上（>100m）

ケーブル長の偏差は 5m です。従って、ケーブル長が 5m 未満の場合、「Test Result」カラムの下に「No Cable」と表示されることがあります。

NOTE このテストでは、少量のパケットを使用します。このテストはツイストペアケーブルを対象としているため、ファイバケーブルを使用するポートの診断は行われません。

● 構文

cable_diag ports [<portlist> | all]

● パラメータ

<portlist>テストするポートの範囲を指定します。
<portlist>すべてのポートをテストします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 4 および 8 のケーブルをテストするには：

```
Zxxx0:admin# cable_diag ports 1:1-1:10,1:21
Command: cable_diag ports 1:1-1:10,1:21
Perform Cable Diagnostics ...

Port      Type       Link Status    Test Result                  Cable Length (M)
------  ----------  -------------  ----------------------------  ------------
1:1     1000BASE-T  Link Up        OK                            65
1:2     1000BASE-T  Link Up        OK                             -
1:3     1000BASE-T  Link Down      Shutdown                      25
1:4     1000BASE-T  Link Down      Shutdown                       -
1:5     1000BASE-T  Link Down      Unknown                        -
1:6     1000BASE-T  Link Down      Pair 1 Crosstalk at  30M       -
                                   Pair 2 Crosstalk at  30M
                                   Pair 3 OK        at 110M
                                   Pair 4 OK        at 110M
1:7     1000BASE-T  Link Down      NO Cable                       -
1:8     1000BASE-T  Link Down      Pair 1 Open      at  16M       -
                                   Pair 2 Open      at  16M
                                   Pair 3 OK        at  50M
                                   Pair 4 OK        at  50M
1:9     1000BASE-T  Link Down      Pair 1 Short     at   5M       -
                                   Pair 2 Short     at   5M
                                   Pair 3 OK        at 110M
                                   Pair 4 OK        at 110M
1:10    1000BASE-T  Link Down      Pair 1 Unknown                 -
                                   Pair 2 Short     at   5M
                                   Pair 3 OK        at 110M
                                   Pair 4 OK        at 110M
1:21    1000BASE-X  Link Up        Unknown                        -

Zxxx0:admin#
```

16. コマンドリスト履歴コマンド

“?” コマンドは、本製品で利用可能なコマンド、オプションを表示します。
一度入力したコマンドはコマンド履歴に保存され、入力時に上矢印キーで呼び出すことができます。履歴に保存される数は初期値では 25 で、1 ～ 40 までの数に設定できます。

?{<Command>}
show command_history
config command_history <value 1-40>

16.1. ?

● 概要

このコマンドを用いて、CLI（Command Line Interface）を介して現在のログインアカウントレベルで利用可能なすべてのコマンドを表示します。

● 構文

? {<Command>}

● パラメータ

<Command>
（オプション）コマンドを指定します。

NOTE コマンドを指定しない場合、対応するユーザレベルのすべてのコマンドを表示します。

● 制限

なし

● 実行例

すべてのコマンドを表示するには：

```
Zxxx0:admin#?
Command: ?

..
?
cable_diag ports
cd
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear fdb
clear historical_counters ports
clear igmp_snooping data_driven_group
clear igmp_snooping statistic counter
clear log
clear mac_based_access_control auth_state
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

config account の構文を表示するには：

```
Zxxx0:admin#? config account
Command: ? config account

Command: config account
Usage:  <username> {encrypt [plain_text| sha_1] <password>}
Description: Used to configure user accounts.

Zxxx0:admin#
```

16.2. show command_history

● 概要

このコマンドを用いて、コマンド履歴を表示します。

● 構文

show command_history

● パラメータ

なし

● 制限

なし

● 実行例

コマンド履歴を表示するには：

```
Zxxx0:admin# show command_history
Command: show command_history

?
?
show traffic_segmentation 1-6
config traffic_segmentation 1-6 forward_list 7-8
config radius delete 1
config radius add 1 10.48.74.121 key manager default
config 802.1x reauth port_based ports all
config 802.1x init port_based ports all
config 802.1x auth_mode port_based
config 802.1x auth_parameter ports 1-50 direction both
config 802.1x capability ports 1-5 authenticator
show 802.1x auth_configuration ports 1
show 802.1x auth_state ports 1-5
enable 802.1x
show 802.1x auth_state ports 1-5
show igmp_snooping
enable igmp_snooping

Zxxx0:admin#
```

16.3. config command_history

● 概要

このコマンドを用いて、スイッチで記録可能なコマンド数を設定します。スイッチでは、入力した最新の 40 個（最大数）のコマンドを記録できます。

● 構文

config command_history <value 1-40>

● パラメータ

<value 1-40> スイッチで記録可能なコマンド数（1 ～ 40）を指定します。初期値は 25 です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチで記録可能な最新コマンド数として 20 を設定するには：

```
Zxxx0:admin#config command_history 20
Command: config command_history 20

Success.

Zxxx0:admin#
```

17. コマンドログ記録コマンドリスト

本装置の設定を変更するコマンドについて、その実行履歴をログに記録することができます。

NOTE 設定の変更に影響しないコマンド（例えば show）の履歴は保存されません。

17.1. enable command logging

● 概要

enable command logging コマンドを用いて、コマンドのログ記録機能を有効にします。

NOTE 本装置の起動時と設定のダウンロード中は、設定コマンドのログは記録されません。

● 構文

enable command logging

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

コマンドのログ記録機能を有効にするには：

```
Zxxx0:admin# enable command logging
Command: enable command logging

Success.

Zxxx0:admin#
```

17.2. disable command logging

● 概要

disable command logging コマンドを用いて、コマンドのログ記録機能を無効にします。

● 構文

disable command logging

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

コマンドのログ記録を無効にするには：

```
Zxxx0:admin# disable command logging
Command: disable command logging

Success.

Zxxx0:admin#
```

17.3. show command logging

● 概要

このコマンドを用いて、本装置の基本的なコマンドログ記録設定ステータスを表示します。

● 構文

show command logging

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

コマンドログ記録設定ステータスを表示するには：

```
Zxxx0:admin# show command logging
Command: show command logging

Command Logging State : Disabled

Zxxx0:admin#
```

18.ネットワークアクセス認証コマンド

ここではアクセス認証時のサーバ問い合わせ動作の設定を行います。

config authentication ports [<portlist> | all] {auth_mode [port_based | host_based {vlanid <vidlist> state [enable | disable}(1)
config authentication mac_format {case [lowercase | uppercase] | delimiter {[hyphen | colon | dot | none] | number [1 | 2 | 5]}(1)}(1)
show authentication ports {<portlist>}
enable authorization attributes
disable authorization attributes
show authorization
config authentication server failover [local | permit | block]
show authentication
show authentication mac_format

18.1. config authentication ports

● 概要

このコマンドを用いて、スイッチの認証動作を設定します。

● 構文

config authentication ports [<portlist> | all] {auth_mode [port_based | host_based {vlanid <vid_list> state [enable | disable]}]}(1)

● パラメータ

<portlist>設定するポートの範囲を指定します。	
all	すべてのポートが設定されます。
auth_mode	
	ポートの認証モードを指定します。
	port_based
	ポートベース認証を行います。ポートに接続された任意のホストが認証に成功した場合、同じポート配下のほかのホストについても通信が許可されます。
	host_based
	ホストベース認証を行います。ポート配下に複数のホストが接続されている場合であってもホストごとに認証を行います。（工場出荷時設定）
	vlanid
	（オプション）認証対象とする VLAN を指定します。
	<vidlist>
	VLAN ID のリストを指定します。
	state
	（オプション）VLAN ID ごとの認証状態を指定します。
	enable
	指定された VLAN ID を認証 VLAN に指定します。
	disable
	指定された VLAN ID を認証 VLAN から除外します。VLAN ID が入力されない場合はすべての VLAN を除外します。この状態では、VLAN は考慮されず、MAC アドレスのみを用いて認証が行われます。（工場出荷時設定）

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

すべてのポートで VLAN 1 のホスト認証を有効にするには：

```
Zxxx0:admin# config authentication ports all auth_mode host_based vlanid 1 state
enable
Command: config authentication ports all auth_mode host_based vlanid 1 state enable

Success.

Zxxx0:admin#
```

18.2. config authentication mac_format

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールにて RADIUS 認証を行う際に、ユーザ名として送信される MAC アドレスのフォーマットの設定を行います。

● 構文

config authentication mac_format {case [lowercase | uppercase] | delimiter {[hyphen | colon | dot | none] | number [1 | 2 | 5]}(1)}(1)

● パラメータ

case	（オプション）英字の大文字・小文字の指定を行います。
	lowercase
	（オプション）MAC アドレスを小文字に指定します。（例：aabbccddeeff）
	uppercase
	（オプション）MAC アドレスを大文字に指定します。（例：AABBCCDDEEFF）
delimiter	（オプション）MAC アドレスの区切り文字の種類を指定します。
	hyphen
	（オプション）ハイフン (-) を用いて MAC アドレスを区切ります。（例：aa-bb-cc-dd-ee-ff）
	colon
	（オプション）コロン (:) を用いて MAC アドレスを区切ります。（例：aa:bb:cc:dd:ee:ff）
	dot
	（オプション）ドット (.) を用いて MAC アドレスを区切ります。（例：aa.bb.cc.dd.ee.ff）
	none
	（オプション）MAC アドレスの区切り文字を無しに指定します。（例：aabbccddeeff）
	number
	（オプション）区切り文字の個数を指定します。
	1　区切り文字を 1 個に指定します。（例：aabbcc-ddeeff）
	2　区切り文字を 2 個に指定します。（例：aabb-ccdd-eeff）
	5　区切り文字を 5 個に指定します。（例：aa-bb-cc-dd-ee-ff）

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC アドレスのフォーマットを IEFT 形式に設定するには：

```
Zxxx0:admin# config authentication mac_format case uppercase delimiter hyphen
number 5
Command: config authentication mac_format case uppercase delimiter hyphen number 5


Success.


Zxxx0:admin#
```

18.3. show authentication ports

● 概要

このコマンドを用いて、ポートごとの認証設定を表示します。

● 構文

show authentication ports {<portlist>}

● パラメータ

<portlist>表示するポートの範囲を指定します。

● 制限

なし

● 実行例

全ポートの認証設定を表示するには：

```
Zxxx0:admin# show authentication ports
Command: show authentication ports

 Port  Auth Mode  Authentication VLAN(s)
 ---- ----------- ----------------------
 1    Host-based
 2    Host-based
 3    Host-based
 4    Host-based
 5    Host-based
 6    Host-based
 7    Host-based
 8    Host-based
 9    Host-based
 10   Host-based
 11   Host-based
 12   Host-based
 13   Host-based
 14   Host-based
 15   Host-based
 16   Host-based
 17   Host-based
 18   Host-based
 19   Host-based
 20   Host-based
 21   Host-based
 22   Host-based
 23   Host-based
 24   Host-based
 25   Host-based
 26   Host-based
 27   Host-based
 28   Host-based

Zxxx0:admin#
```

18.4. enable authorization attributes

● 概要

このコマンドを用いて、認証属性の利用を有効にします。デフォルトでは、本機能は有効です。

● 構文

enable authorization attributes

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

認証属性の利用を有効にするには：

```
Zxxx0:admin# enable authorization attributes
Command: enable authorization attributes

Success.

Zxxx0:admin#
```

18.5. disable authorization attributes

● 概要

このコマンドを用いて、認証属性の利用を無効にします。

● 構文

disable authorization attributes

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

機能をに有効にするには：

```
Zxxx0:admin# disable authorization attributes
Command: disable authorization attributes

Success.

Zxxx0:admin#
```

18.6. show authorization

● 概要

このコマンドを用いて、認証属性の利用状態を表示します。

● 構文

show authorization

● パラメータ

なし

● 制限

なし

● 実行例

認証属性の利用状態を表示するには：

```
Zxxx0:admin# show authorization
Command: show authorization

Authorization for Attributes: Disabled

Zxxx0:admin#
```

18.7. config authentication server failover

● 概要

このコマンドを用いて、RADIUS サーバ障害時のフェイルオーバー動作を設定します。デフォルトは block です。

● 構文

config authentication server failover [local | permit | block]

● パラメータ

local	ローカルデータベースを用いて認証を行います。
permit	常に認証を許可します。
block	常に認証を拒否します。（工場出荷時設定）

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

フェイルオーバー設定を local に有効にするには：

```
Zxxx0:admin# config authentication server failover local
Command: config authentication server failover local

Success.

Zxxx0:admin#
```

18.8. show authentication

● 概要

このコマンドを用いて、RADIUS サーバ障害時のフェイルオーバー動作設定を表示します。

● 構文

show authentication

● パラメータ

なし

● 制限

なし

● 実行例

フェイルオーバー動作設定を表示するには：

```
Zxxx0:admin# show authentication
Command: show authentication

Authentication Server Failover: Block.

Zxxx0:admin#
```

18.9. show authentication mac_format

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールにて RADIUS 認証を行う際に、ユーザ名として送信される MAC アドレスのフォーマット設定を表示します。

● 構文

show authentication mac_format

● パラメータ

なし

● 制限

なし

● 実行例

MAC アドレスのフォーマット設定を表示するには：

```
Zxxx0:admin# show authentication mac_format
Command: show authentication mac_format

 Case               : Uppercase
 Delimiter          : None
 Delimiter Number   : 5

Zxxx0:admin#
```

19. DDM(Digital Diagnostic Monitoring) コマンド

config ddm ports [<portlist> | all] [[temperature_threshold{ high_alarm <degrees> | low_alarm <degrees> | high_warning <degrees> | low_warning <degrees>}|voltage_threshold{ high_alarm <voltage> | low_alarm <voltage> | high_warning <voltage> | low_warning<voltage>} | bias_current_threshold { high_alarm <milliampere> | low_alarm <milliampere> | high_warning <milliampere> | low_warning<milliampere>} | tx_power_threshold{ high_alarm <mw_or_dbm> | low_alarm <mw_or_dbm> | high_warning <mw_or_dbm> | low_warning<mw_or_dbm>} | rx_power_threshold{ high_alarm <mw_or_dbm> | low_alarm <mw_or_dbm> | high_warning <mw_or_dbm> | low_warning <mw_or_dbm>}] | {state [enable|disable] | shutdown [alarm | warning | none]}]
config ddm [trap | log] [enable|disable]
config ddm power_unit [mw|dbm]
show ddm
show ddm ports {<portlist>} [status|configuration]

19.1. config ddm ports temperature_threshold

● 概要

このコマンドを用いて、指定したポートの温度のしきい値を設定します。このコマンドは、指定したポートの温度のしきい値を設定します。

● 構文

config ddm ports [<portlist> | all] temperature_threshold { high_alarm <degrees> | low_alarm < degrees > | high_warning < degrees > | low_warning < degrees > } (1)

● パラメータ

ports	
	<portlist>
	設定するポートの範囲を指定します。(<portlist> 形式：UnitID：Port number)
	all　all パラメータを選択した場合、すべての光ポートの動作パラメータが設定されます。
temperature_threshold	
	光モジュールの温度（摂氏）のしきい値を指定します。このしきい値に対して、少なくとも 1 つのパラメータを指定してください。
high_alarm	
	<degrees>
	温度アラームの上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、アラームと関連付けられている動作が実行されます。このパラメータの範囲は、-128 ～ 127.996 度（摂氏）です。

low_alarm	
<degrees>	温度アラームの下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、アラームと関連付けられている動作が実行されます。このパラメータの範囲は、-128 ～ 127.996 度（摂氏）です。
high_warning	
<degrees>	温度警告の上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、警告と関連付けられている動作が実行されます。このパラメータの範囲は、-128 ～ 127.996 度（摂氏）です。
low_warning	
<degrees>	温度警告の下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、警告と関連付けられている動作が実行されます。このパラメータの範囲は、-128 ～ 127.996 度（摂氏）です。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 21 の温度のしきい値を設定するには：

```
Zxxx0:admin#  config ddm ports 21 temperature_threshold high_alarm 84.9555
low_alarm -10 high_warning 70 low_warning 2.2525
Command: config ddm ports 21 temperature_threshold high_alarm 84.9555 low_alarm -10
high_warning 70 low_warning 2.2525


According to the DDM precision definition, closest value 84.9531 and 2.25 are
chosen.


Success.


Zxxx0:admin#
```

19.2. config ddm ports voltage_threshold

● 概要

このコマンドは、指定したポートの電圧のしきい値を設定します。

● 構文

config ddm ports [<portlist> | all] voltage_threshold { high_alarm < voltage > |
low_alarm < voltage > igh_warning < voltage >
| low_warning < voltage > } (1)

● パラメータ

ports	
<portlist>	設定するポートの範囲を指定します。(<portlist> 形式：UnitID：Port number)
all	all パラメータを選択した場合、すべての光ポートの動作パラメータが設定されます。
voltage_threshold	光モジュールの電圧のしきい値を指定します。
high_alarm	
<voltage>	電圧アラームの上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、アラームと関連付けられている動作が実行されます。このパラメータの範囲は、0 ～ 6.5535V です。
low_alarm	
<voltage>	電圧アラームの下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、アラームと関連付けられている動作が実行されます。このパラメータの範囲は、0 ～ 6.5535V です。
high_warning	
<voltage>	電圧警告の上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、警告と関連付けられている動作が実行されます。このパラメータの範囲は、0 ～ 6.5535V です。
low_warning	
<voltage>	電圧警告の下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、警告と関連付けられている動作が実行されます。このパラメータの範囲は、0 ～ 6.5535V です。

NOTE voltage パラメータタイプで、ユーザが CLI コマンドに入力できるのは 10 進数値です。CLI では、任意の桁数の値を入力できます。ただし、コマンドバッファのサイズと浮動小数点精度による桁数の制約があります。ユーザが入力した値は浮動小数点数に変換されてから、設定データベースに適用されます。
浮動小数点数のデフォルトの精度は 6 桁です。
例えば、12.3456 と入力すると浮動小数点値 12.3456、12.3456789 と入力すると浮動小数点値 12.3457 にそれぞれ変換されます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 21 のバイアス電流のしきい値を設定するには：

```
Zxxx0:admin#  config ddm ports 21 voltage_threshold high_alarm 4.25 low_alarm 2.5
high_warning 3.5 low_warning 3
Command: config ddm ports 21 voltage_threshold high_alarm 4.25 low_alarm 2.5 high_w
arning 3.5 low_warning 3

Success.

Zxxx0:admin#
```

19.3. config ddm ports bias_current_threshold

● 概要

このコマンドを用いて、指定したポートのバイアス電流のしきい値を設定します。

● 構文

config ddm ports [<portlist> | all] bias_current_threshold { high_alarm < milliampere >|
low_alarm < milliampere > | high_warning < milliampere > |
low_warning < milliampere > } (1)

● パラメータ

ports	
<portlist>	設定するポートの範囲を指定します。(<portlist> 形式：UnitID：Port number)
all	all パラメータを選択した場合、すべての光ポートの動作パラメータが設定されます。
bias_current_threshold	光モジュールのバイアス電流のしきい値を指定します。
high_alarm	
<milliampere>	バイアス電流アラームの上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、アラームと関連付けられている動作が実行されます。このパラメータの範囲は、0 ～ 131mA です。
low_alarm	
<milliampere>	バイアス電流アラームの下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、アラームと関連付けられている動作が実行されます。このパラメータの範囲は、0 ～ 131mA です。
high_warning	
<milliampere>	バイアス電流警告の上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、警告と関連付けられている動作が実行されます。このパラメータの範囲は、0 ～ 131mA です。
low_warning	
<milliampere>	バイアス電流警告の下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、警告と関連付けられている動作が実行されます。このパラメータの範囲は、0 ～ 131mA です。

NOTE milliampere パラメータタイプで、ユーザが CLI コマンドに入力できるのは 10 進数値です。CLI では、任意の桁数の値を入力できます。
浮動小数点数のデフォルトの精度は 6 桁です。
例えば、12.3456 と入力すると浮動小数点値 12.3456、12.3456789 と入力すると浮動小数点値 12.3457 にそれぞれ変換されます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 21 のバイアス電流のしきい値を設定するには：

```
Zxxx0:admin#  config ddm ports 21 bias_current_threshold high_alarm 7.25 low_alarm
0.004 high_warning 0.5 low_warning 0.008
Command: config ddm ports 21 bias_current_threshold high_alarm 7.25 low_alarm 0.004
high_warning 0.5 low_warning 0.008

Success

Zxxx0:admin#
```

19.4. config ddm ports tx_power_threshold

● 概要

このコマンドを用いて、指定したポートの送信光パワーのしきい値を設定します。

● 構文

config ddm ports [<portlist> | all] tx_power_threshold { high_alarm < milliwatts > | low_alarm < milliwatts > | high_warning < milliwatts > | low_warning < milliwatts > } (1))

● パラメータ

ports	
	<portlist>
	設定するポートの範囲を指定します。(<portlist> 形式：UnitID：Port number)
	all　all パラメータを選択した場合、すべての光ポートの動作パラメータが設定されます。
tx_power_threshold	
	光モジュールの送信光パワーのしきい値を指定します。
high_alarm	
	<mw_or_dbm>
	送信光パワーアラームの上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、アラームと関連付けられている動作が実行されます。 単位が mW である場合は、このパラメータの範囲は 0 ～ 6.5535mW です。単位が dBm である場合は、このパラメータの範囲は -40 ～ 8.1647dBm です。
low_alarm	
	<mw_or_dbm>
	送信光パワーアラームの下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、アラームと関連付けられている動作が実行されます。 単位が mW である場合は、このパラメータの範囲は 0 ～ 6.5535mW です。単位が dBm である場合は、このパラメータの範囲は -40 ～ 8.1647dBm です。

high_warning	
<mw_or_dbm>	送信光パワー警告の上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、警告と関連付けられている動作が実行されます。 単位が mW である場合は、このパラメータの範囲は 0 ～ 6.5535mW です。単位が dBm である場合は、このパラメータの範囲は -40 ～ 8.1647dBm です。
low_warning	
<mw_or_dbm>	送信光パワー警告の下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、警告と関連付けられている動作が実行されます。 単位が mW である場合は、このパラメータの範囲は 0 ～ 6.5535mW です。単位が dBm である場合は、このパラメータの範囲は -40 ～ 8.1647dBm です。

NOTE mW または dBm パラメータタイプで、ユーザが CLI コマンドに入力できるのは 10 進数値です。CLI では、任意の桁数の値を入力できます。
浮動小数点数のデフォルトの精度は 6 桁です。
例えば、12.3456 と入力すると浮動小数点値 12.3456、12.3456789 と入力すると浮動小数点値 12.3457 にそれぞれ変換されます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 21 の送信光パワーのしきい値を設定するには：

```
Zxxx0:admin#  config ddm ports 21 tx_power_threshold high_alarm 0.625 low_alarm
0.006 high_warning 0.55 low_warning 0.008
Command: config ddm ports 21 tx_power_threshold high_alarm 0.625 low_alarm 0.006
high_warning 0.55 low_warning 0.008

Success.

Zxxx0:admin#
```

19.5. config ddm ports rx_power_threshold

● 概要

このコマンドを用いて、指定したポートの受信光パワーのしきい値を設定します。

● 構文

config ddm ports [<portlist> | all] tx_power_threshold { high_alarm < mw_or_dbm > | low_alarm < mw_or_dbm > | high_warning < mw_or_dbm > | low_warning < mw_or_dbm > } (1))

● パラメータ

ports	
	<portlist>
	設定するポートの範囲を指定します。(<portlist> 形式：UnitID：Port number)
	all　all パラメータを選択した場合、すべての光ポートの動作パラメータが設定されます。
tx_power_threshold	
	光モジュールの受信光パワーのしきい値を指定します。
high_alarm	
	<mw_or_dbm>
	受信光パワーアラームの上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、アラームと関連付けられている動作が実行されます。 単位が mW である場合は、このパラメータの範囲は 0 ～ 6.5535mW です。単位が dBm である場合は、このパラメータの範囲は -40 ～ 8.1647dBm です。
low_alarm	
	<mw_or_dbm>
	受信光パワーアラームの下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、アラームと関連付けられている動作が実行されます。 単位が mW である場合は、このパラメータの範囲は 0 ～ 6.5535mW です。単位が dBm である場合は、このパラメータの範囲は -40 ～ 8.1647dBm です。
high_warning	
	<mw_or_dbm>
	受信光パワー警告の上限しきい値を指定します。 動作パラメータがこの値を上回ったときに、警告と関連付けられている動作が実行されます。 単位が mW である場合は、このパラメータの範囲は 0 ～ 6.5535mW です。単位が dBm である場合は、このパラメータの範囲は -40 ～ 8.1647dBm です。
low_warning	
	<mw_or_dbm>
	受信光パワー警告の下限しきい値を指定します。 動作パラメータがこの値を下回ったときに、警告と関連付けられている動作が実行されます。 単位が mW である場合は、このパラメータの範囲は 0 ～ 6.5535mW です。単位が dBm である場合は、このパラメータの範囲は -40 ～ 8.1647dBm です。

NOTE mW または dBm パラメータタイプで、ユーザが CLI コマンドに入力できるのは 10 進数値です。CLI では、任意の桁数の値を入力できます。
浮動小数点数のデフォルトの精度は 6 桁です。
例えば、12.3456 と入力すると浮動小数点値 12.3456、12.3456789 と入力すると浮動小数点値 12.3457 にそれぞれ変換されます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 21 の受信光パワーのしきい値を設定するには：

```
Zxxx0:admin#  config ddm ports 21 rx_power_threshold high_alarm 4.55 low_alarm 0.01
high_warning 3.5 low_warning 0.03
Command: config ddm ports 21 rx_power_threshold high_alarm 4.55 low_alarm 0.01
high_warning 3.5 low_warning 0.03

Success.

Zxxx0:admin#
```

19.6. config ddm ports reload threshold

● 概要

このコマンドを用いて、DDM のしきい値設定を再読み込みします。このコマンドは、特定ポートのデフォルトのしきい値設定を再読み込みします。ポートが光モジュールとリンクアップしている場合は、そのポートのしきい値がすべてハードウェアのデフォルト値に設定されます。ポートが光ポートでない場合や、ポートがリンクダウンしている場合は、すべてのしきい値設定が消去されます。

● 構文

config ddm ports [<portlist> | all] reload_threshold

● パラメータ

ports		
	<portlist>	
		設定するポートの範囲を指定します。(<portlist> 形式：UnitID：Port number)
	all	all パラメータを選択した場合、すべての光ポートの動作パラメータが設定されます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 21 のしきい値設定を再読み込みするには：

```
Zxxx0:admin#  config ddm ports 21 reload_threshold
Command: config ddm ports 21 reload_threshold

Success.

Zxxx0:admin#
```

19.7. config ddm ports state

● 概要

このコマンドを用いて、しきい値超過のアラームまたは警告イベントが発生したときの DDM の状態および / または DDM のシャットダウン動作を設定します。このコマンドは、しきい値超過のアラームまたは警告イベントが発生したときの DDM の状態および / または DDM のシャットダウン動作を設定します。

● 構文

config ddm ports [<portlist> | all] { state [enable | disable] | shutdown [alarm | warning | none] } (1)

● パラメータ

ports	
	<portlist> 設定するポートの範囲を指定します。(ポート：UnitID：Port number)
	all　all パラメータを選択した場合、すべての光ポートの動作パラメータが設定されます。
state	DDM の状態を有効または無効に指定します。state が無効である場合、DDM の動作は有効になりません。
shutdown	
	対応するアラームしきい値または警告しきい値の範囲を動作パラメータが超えたときに、ポートをシャットダウンするかどうかを指定します。
	alarm 設定済みのアラームしきい値の範囲を超えたときに、ポートをシャットダウンします。
	warning 設定済みの警告しきい値の範囲を超えたときに、ポートをシャットダウンします。
	none しきい値の範囲を超えたかどうかに関係なく、ポートはシャットダウンしません。

NOTE シャットダウンしたポートは通常動作に自動復帰できないため、config ports <portlist> state enable コマンドを使用してポートを手動で復帰させる必要があります。
シャットダウン動作は、デフォルトでは none に設定されています。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 21 の動作をアラームと関連付けるよう設定するには：

```
Zxxx0:admin# config ddm ports 11 state enable shutdown alarm
Command: config ddm ports 11 state enable shutdown alarm

Success.

Zxxx0:admin#
```

19.8. config ddm log

● 概要

光モジュールのパラメータが DDM のしきい値を超えたときに、ログを有効または無効にします。このコマンドは、しきい値超過のアラームまたは警告イベントが発生したときの DDM ログの動作を設定します。

● 構文

config ddm log [enable | disable]

● パラメータ

log	対応するしきい値を動作パラメータが超えたときに、ログを送信するかどうかを指定します。 DDM ログは、デフォルトでは有効に設定されています。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

DDM ログの状態を有効に設定するには：

```
Zxxx0:admin#  config ddm log enable
Command: config ddm log enable

Success.

Zxxx0:admin#
```

19.9. config ddm trap

● 概要

このコマンドを用いて、光モジュールのパラメータが DDM のしきい値を超えたときに、トラップを有効または無効にします。このコマンドは、しきい値超過のアラームまたは警告イベントが発生したときの DDM トラップの動作を設定します。

● 構文

config ddm trap [enable | disable]

● パラメータ

trap	対応するしきい値を動作パラメータが超えたときに、トラップを送信するかどうかを指定します。DDM トラップは、デフォルトでは無効に設定されています。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

DDM トラップの状態を有効に設定するには：

```
Zxxx0:admin#  config ddm trap enable
Command: config ddm trap enable

Success.

Zxxx0:admin#
```

19.10. config ddm power_unit

● 概要

このコマンドを用いて、DDM TX/RX 出力の単位を設定します。このコマンドは、DDM TX/RX 出力のグローバル単位を設定します。

● 構文

config ddm power_unit [mw | dbm]

● パラメータ

power_unit	DDM TX/RX 出力の単位を指定します。単位を設定した場合、TX/RX 出力の表示メッセージと設定値には、同じ単位が使用されます。 デフォルトの単位は mW です。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

DDM TX/RX 出力の単位を設定するには：

```
Zxxx0:admin#  config ddm power_unit dbm
Command: config ddm power_unit dbm

Success.

Zxxx0:admin#
```

19.11. show ddm ports status

● 概要

このコマンドを用いて、指定したポートの光モジュールに現在設定されている DDM の動作パラメータ値を表示します。このコマンドは、光モジュールに現在設定されている動作パラメータを表示します。

● 構文

show ddm ports {<portlist> } status

● パラメータ

ports	
	<portlist>
	表示するポートの範囲を指定します。 ports パラメータが指定されていない場合、すべての光ポートの動作パラメータが表示されます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 21 ～ 23 の動作パラメータを表示するには：

```
Zxxx0:admin#  show ddm ports 21-23 status
Command: show ddm ports 21-23 status

Port   Temperature    Voltage    Bias-Current   TX-Power    RX-Power
       (in Celsius)   (V)          (mA)          (dBm)         (dBm)
------ -------------- --------- -------------- ----------- -----------
21      -             -            -            -             -
22     25.0625        3.5036      12.6473       -9.9097       -5.4166
23      -             -            -            -             -









CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

19.12. show ddm ports configuration

● 概要

このコマンドを用いて、光モジュールの現在の設定を表示します。しきい値には、管理設定しきい値と動作設定しきい値という 2 つのタイプがあります。
光ポートの場合、ユーザが特定のしきい値を設定していると、このコマンドでは、そのしきい値はユーザ設定のしきい値であることを示すタグとともに表示されます。タグの表示がなければ、接続した光モジュールから読み込まれたしきい値に該当します。

● 構文

show ddm ports {<portlist>} configuration

● パラメータ

ports	
	<portlist>
	表示するポートの範囲を指定します。 ports パラメータが指定されていない場合、すべての光ポートの動作パラメータが表示されます。

● 制限

なし

● 実行例

ポート 21 の設定を表示するには：

```
Zxxx0:admin#  show ddm ports 21 configuration
Command: show ddm ports 21 configuration

Port 21
------------------------------------
DDM State : Enabled
Shutdown  : Alarm

Threshold     Temperature    Voltage    Bias-Current    TX-Power    RX-Power
              (in Celsius)      (V)          (mA)          (dBm)       (dBm)
------------- ------------ ------------ ------------ ------------ ------------
High Alarm    85.0000(A)   3.5000       100.0540      -8.9997     -2.9904
Low Alarm     -5.0000      3.1000       6.0040        -11.8977    -23.9794
High Warning  80.0000(A)   3.4500       90.0480       -9.5001     -3.4901
Low Warning    0.0000      3.1500       7.0040        -11.4026    -23.0103

A means that the threshold is administratively configured.

Zxxx0:admin#
```

19.13. show ddm

● 概要

このコマンドを用いて、DDM のグローバル設定を表示します。

● 構文

show ddm

● パラメータ

なし

● 制限

なし

● 実行例

DDM のグローバル設定を表示するには：

```
Zxxx0:admin#  show ddm

Command: show ddm

DDM Log                : Enabled
DDM Trap               : Enabled
DDM TX/RX Power Unit   : dBm

Zxxx0:admin#
```

20. ソフトウェアデバッグコマンドリスト

各種プロトコルの通信状態のモニターやログ、エラー発生時の対応等を設定できます。

debug error_log [dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]
debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]
debug output [module <module_list> | all] [buffer | console]
debug config error_reboot [enable | disable]
debug config state [enable | disable]
debug show error_reboot state
debug stp clear counter {ports [<portlist> | all]}
debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief | detail]
debug stp show counter {ports [<portlist> | all]}
debug stp show flag {ports <portlist>}
debug stp show information
debug stp state [disable | enable]
debug show status {module <module_list>}

20.1. debug error_log

● 概要

このコマンドを用いて、ソフトウェアエラーログのダンプ、クリア、または TFTP サーバへのアップロードを行います。

● 構文

debug error_log [dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]

● パラメータ

dump	デバッグログのデバッグメッセージを表示します。
clear	デバッグログをクリアします。
upload_toTFTP	IP アドレスで指定した TFTP サーバに、デバッグログをアップロードします。 <ipaddr> TFTP サーバの IPv4 アドレスを指定します。 <path_filename 64> このパス名は、TFTP サーバの DOS パス名を指定します。相対パス名または絶対パス名のどちらでも指定可能です。値は 64 文字までです。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

エラーログをダンプするには：

```
Zxxx0:admin# debug error_log dump
Command: debug error_log dump

*************************************************************************
# debug log: 1
# firmware version: 1.0.0.xx
# level: CPU exception
# clock: 437453880 ms
# time : 2000-01-08 05:55:40

======================== CPU EXCEPTION ========================
Current Task = IP-Tic Stack Pointer = 4CFEA7A0
---------------------------CP0 Registers-----------------------
Status : 1000FC01  Interrupt enable  Normal level
Cause  : 00000008  TLB exception (load or instruction fetch)
EPC    : 80A0297C        Addr   : 00000008
Stack  : 4CFEA7A0        Return : 80A02938
-------------------------normal registers-----------------------
$0( $0) : 00000000  at( $1) : FFFFFFFE  v0( $2) : 00000000  v1( $3) : 00000001
a0( $4) : 00000000  a1( $5) : 4825B4A8  a2( $6) : 00000001  a3( $7) : 00000001
t0( $8) : 814D7FCC  t1( $9) : 0000FC00  t2($10) : 828100C4  t3($11) : 00000017
t4($12) : 828100BC  t5($13) : 4CFEA430  t6($14) : 82810048  t7($15) : 00000000
s0($16) : 4825D94A  s1($17) : 4825D890  s2($18) : 4825D949  s3($19) : 4825D946
s4($20) : 00000000  s5($21) : 00000008  s6($22) : 81800000  s7($23) : 00090000
t8($24) : 00000000  t9($25) : FFFFFFC0  k0($26) : 00000000  k1($27) : 00000000
gp($28) : 8180ADA0  sp($29) : 4CFEA7A0  fp($30) : 00000001  ra($31) : 80A02938


------------------------- TASK STACKTRACE ------------------------
->81150A58
->809B346C
->809E1DEC
->809D7E6C
->80A038CC
->80A033B0
->80A0297C
```

エラーログを削除するには：

```
Zxxx0:admin# debug error_log clear
Command: debug error_log clear

Success.

Zxxx0:admin#
```

エラーログを TFTP サーバにアップロードするには：

```
Zxxx0:admin# debug error_log upload_toTFTP 10.0.0.90 debug-log.txt
Command: debug error_log upload_toTFTP 10.0.0.90 debug-log.txt

Connecting to server.................. Done.
Upload configuration.................. Done.

Zxxx0:admin#
```

20.2. debug buffer

● 概要

このコマンドを用いて、デバッグバッファの表示か、デバッグバッファのダンプ、クリア、または TFTP サーバへのアップロードを行います。

NOTE デバッグバッファへの出力を選択し、デバッグメッセージが出力されるときには、システムメモリプールがデバッグバッファとして使用されます。システムメモリプールリソースを使用する機能では、ファームウェアのダウンロードやアップロード、あるいは設定の保存などのコマンドの実行に失敗することがあります。これらのコマンドを正しく実行するには、先に debug buffer clear コマンドを実行して、システムのメモリプールリソースを手動で解放しておいてください。

● 構文

debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]

● パラメータ

utilization	デバッグバッファの状態を表示します。
dump	デバッグバッファのデバッグメッセージを表示します。
clear	デバッグバッファをクリアします。
upload_toTFTP	IP アドレスで指定した TFTP サーバに、デバッグバッファをアップロードします。 <ipaddr> TFTP サーバの IPv4 アドレスを指定します。 <path_filename 64> このパス名は、TFTP サーバの DOS パス名を指定します。相対パス名または絶対パス名のどちらでも指定可能です。値は 64 文字までです。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

デバッグバッファの状態を表示するには：

```
Zxxx0:admin# debug buffer utilization
Command: debug buffer utilization

Allocate from          :    System memory
Total size             :    2 MB
Utilization rate       :    30%

Zxxx0:admin#
```

デバッグバッファを削除するには：

```
Zxxx0:admin# debug buffer clear
Command: debug buffer clear

Success.

Zxxx0:admin#
```

デバッグバッファに保存されたメッセージを TFTP サーバにアップロードするには：

```
Zxxx0:admin# debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt
Command: debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt

Connecting to server.................. Done.
Upload configuration.................. Done.

Zxxx0:admin#
```

20.3. debug output

● 概要

このコマンドを用いて、指定したモジュールのデバッグメッセージをデバッグバッファまたはローカルコンソールに出力します。ユーザが Telnet セッションでコマンドを実行した場合、エラーメッセージもローカルコンソールに出力されます。

NOTE デバッグバッファへの出力を選択し、デバッグメッセージが出力されるときには、システムメモリプールがデバッグバッファとして使用されます。システムメモリプールリソースを使用する機能では、ファームウェアのダウンロードやアップロード、あるいは設定の保存などのコマンドの実行に失敗することがあります。これらのコマンドを正しく実行するには、先に debug buffer clear コマンドを実行して、システムのメモリプールリソースを手動で解放しておいてください。

● 構文

debug output [module <module_list> | all] [buffer | console]

● パラメータ

module	モジュールリストを指定します。 <module_list> モジュールリストを入力します。 all すべてのモジュールに対して出力方法を制御します。
buffer	モジュールのデバッグメッセージをデバッグバッファに出力します（デフォルト）。
console	モジュールのデバッグメッセージをローカルコンソールに出力します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

すべてのモジュールのデバッグメッセージをローカルコンソールに出力するには：

```
Zxxx0:admin# debug output all console
Command: debug output all console

Success.

Zxxx0:admin#
```

20.4. debug config error_reboot

● 概要

このコマンドを用いて、致命的なエラーが発生したときにスイッチを再起動させる設定をします。エラーが発生した場合、まずウォッチドッグタイマーが無効になり、すべてのデバッグ情報が NVRAM に保存されます。error_reboot を有効にした場合、すべての情報が NVRAM に保存された後に、ウォッチドッグタイマーが有効になります。

● 構文

debug config error_reboot [enable | disable]

● パラメータ

enable	致命的なエラーが発生した場合に再起動を行います。（デフォルト設定が定義されていない場合は enable がデフォルトとなります）
disable	致命的なエラーが発生しても再起動を行いません。システムはハングアップし、デバッグシェルモードへ移行します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

致命的なエラーが発生した場合に再起動を行わない設定をするには：

```
Zxxx0:admin# debug config error_reboot disable
Command: debug config error_reboot disable

Success.

Zxxx0:admin#
```

20.5. debug config state

● 概要

このコマンドを用いて、デバッグステータスを設定します。

● 構文

debug config state [enable | disable]

● パラメータ

enable	デバッグ状態を有効にします。
disable	デバッグ状態を無効にします。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

デバッグステータスを無効にするには：

```
Zxxx0:admin# debug config state disable
Command: debug config state disable

Success.

Zxxx0:admin#
```

20.6. debug show error_reboot state

● 概要

このコマンドを用いて、エラー再起動ステータスを表示します。

● 構文

debug show error_reboot state

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

エラー再起動ステータスを表示するには：

```
Zxxx0:admin#debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

Zxxx0:admin#
```

20.7. debug stp clear counter

● 概要

このコマンドを用いて、STP カウンタを削除します。

● 構文

debug stp clear counter {ports [<portlist> | all]}

● パラメータ

ports	ポートの範囲を指定します。	
	<portlist>	
		この設定に使用するポートのリストを入力します。
	all	すべてのポートカウンタをクリアします。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

スイッチのすべての STP カウンタを削除するには：

```
Zxxx0:admin# debug stp clear counter ports all
Command : debug stp clear counter ports all

Success.

Zxxx0:admin#
```

20.8. debug stp config ports

● 概要

このコマンドを用いて、指定したポートにポート毎の STP デバッグレベルを設定します。

● 構文

debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief | detail]

● パラメータ

ports	デバッグ対象の STP ポートの範囲を指定します。 <portlist> この設定に使用するポートのリストを入力します。 all スイッチのすべてのポートをデバッグします。
event	外部動作およびイベント処理をデバッグします。
bpdu	送受信した BPDU をデバッグします。
state_machine	STP ステートマシンの状態変化をデバッグします。
all	上記のすべてをデバッグします。
state	デバッグ動作の状態を指定します。 disable デバッグ動作を無効にします。 brief デバッグレベルを brief（簡易）に設定します。 detail デバッグレベルを detail（詳細）に設定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

すべてのポートですべての STP デバッグフラグを brief レベルに設定するには：

```
Zxxx0:admin# debug stp config ports all all state brief
Command: debug stp config ports all all state brief

Success.

Zxxx0:admin#
```

20.9. debug stp show counter

● 概要

このコマンドを用いて、STP カウンタを表示します。

● 構文

debug stp show counter {ports [<portlist> | all]}

● パラメータ

ports	（オプション）表示する STP ポートを指定します。
	<portlist>
	この設定に使用するポートのリストを入力します。
	all　すべてのポートのカウンタを表示します。

パラメータを指定しない場合、グローバルカウンタを表示します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

ポート 9 の STP カウンタを表示するには：

```
Zxxx0:admin# debug stp show counter ports 9
Command: debug stp show counter ports 9

STP Counters
--------------------------------------
 Port 9 :
  Receive:                                  Transmit:
  Total STP Packets             :32         Total STP Packets  :32
  Configuration BPDU            :0          Configuration BPDU :0
  TCN BPDU                      :0          TCN BPDU           :0
  RSTP TC-Flag                  :15         RSTP TC-Flag       :7
  RST BPDU                      :32         RST BPDU           :32

  Discard:
  Total Discarded BPDU          :0
  Global STP Disabled           :0
  Port STP Disabled             :0
  Invalid Packet Format         :0
  Invalid Protocol              :0
  Configuration BPDU Length     :0
  TCN BPDU Length               :0
  RST BPDU Length               :0
  Invalid Type                  :0
  Invalid Timers                :0

Zxxx0:admin#
```

20.10. debug stp show flag

● 概要

このコマンドを用いて、指定したポートの STP デバッグレベルを表示します。

● 構文

debug stp show flag {ports <portlist>}

● パラメータ

ports	（オプション）表示する STP ポートを指定します。
<portlist>	（オプション）この設定に使用するポートのリストを入力します。

パラメータを指定しない場合、スイッチのすべてのポートを表示します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

すべてのポートの STP デバッグレベルを表示するには：

```
Zxxx0:admin# debug stp show flag
Command: debug stp show flag

Global State: Enabled

Port Index           Event flag    BPDU Flag     State Machine Flag
----------           ----------    ---------     ------------------
  1                  Detail         Brief         Disable
  2                  Detail         Brief         Disable
  3                  Detail         Brief         Disable
  4                  Detail         Brief         Disable
  5                  Detail         Brief         Disable
  6                  Detail         Brief         Disable
  7                  Detail         Brief         Disable
  8                  Detail         Brief         Disable
  9                  Detail         Brief         Disable
  10                 Detail         Brief         Disable
  11                 Detail         Brief         Disable
  12                 Detail         Brief         Disable

Zxxx0:admin#
```

20.11. debug stp show information

● 概要

このコマンドを用いて、ハードウェアテーブルや STP ステートマシンなど、STP の詳細情報を表示します。

● 構文

debug stp show information

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

STP デバッグ情報を表示するには：

```
Zxxx0:admin# debug stp show information
Command: debug stp show information

Spanning Tree Debug Information:
---------------------------------------
Port Status In Hardware Table:
Instance 0:
Port 1 :BLK  Port 2 :BLK  Port 3 :BLK  Port 4 :BLK  Port 5 :BLK  Port 6 :BLK
Port 7 :FOR  Port 8 :BLK  Port 9 :BLK  Port 10:BLK  Port 11:BLK  Port 12:BLK
Instance 1:
Port 1 :BLK  Port 2 :BLK  Port 3 :BLK  Port 4 :BLK  Port 5 :BLK  Port 6 :BLK
Port 7 :FOR  Port 8 :BLK  Port 9 :BLK  Port 10:BLK  Port 11:BLK  Port 12:BLK
-------------------------------------
Root Priority And Times :
Instance 0:
 Designated Root Bridge    : 32768/00-01-02-03-04-00
 External Root Cost            : 0
 Regional Root Bridge      : 32768/00-01-02-03-04-00
 Internal Root Cost        : 0
 Designated Bridge             : 32768/00-01-02-03-04-00
 Designated Port           : 0
 Message Age               : 0
 Max Age                       : 20
 Forward Delay             : 15
 Hello Time                : 2
Instance 1:
 Regional Root Bridge      : 32769/00-01-02-03-04-00
 Internal Root Cost        : 0
 Designated Bridge         : 32769/00-01-02-03-04-00
 Designated Port           : 0
 Remaining Hops            : 20
-------------------------------------
Designated  Priority And Times:
 Instance 0:
 Port 1 :
 Designated Root Bridge    : 0    /00-00-00-00-00-00
 External Root Cost        : 0
 Regional Root Bridge      : 0    /00-00-00-00-00-00
 Internal Root Cost        : 0
 Designated Bridge         : 0    /00-00-00-00-00-00
 Designated Port           : 0
 Message Age               : 0
 Max Age                   : 20
 Forward Delay             : 15
 Hello Time                : 2

 Instance 1:
 Port 1 :
 Regional Root Bridge      : 0    /00-00-00-00-00-00
 Internal Root Cost        : 0
 Designated Bridge         : 0    /00-00-00-00-00-00
 Designated Port           : 0
 Remaining Hops            : 20


Zxxx0:admin#
```

20.12. debug stp state

● 概要

このコマンドを用いて、STP デバッグ状態を有効または無効にします。

● 構文

debug stp state [enable | disable]

● パラメータ

state	STP デバッグ状態を指定します。 enable STP デバッグ状態を有効にします。 disable STP デバッグ状態を無効にします。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

STP デバッグ状態を有効にし、その後で無効にするには：

```
Zxxx0:admin# debug stp state enable
Command: debug stp state enable

Success.

Zxxx0:admin# debug stp state disable
Command: debug stp state disable

Success.

Zxxx0:admin#
```

20.13. debug show status

● 概要

デバッグハンドラ状態および指定したモジュールのデバッグステータスを表示します。
入力モジュールリストが空の場合は、モジュールのデバッグをサポートするすべての登録モジュールの状態を表示します。

● 構文

debug show status {module <module_list>}

● パラメータ

module	（オプション）モジュールリストを指定します。
<module_list>	モジュールリストを入力します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

指定したモジュールのデバッグ状態を表示するには：

```
Prompt# debug show status module MSTP
Command: debug show status module MSTP

Debug Global State: Enable

MSTP                : Enable

Prompt#
```

デバッグ状態を表示するには：

```
Prompt# debug show status
Command: debug show status

Debug Global State: Enable

SYS    : Enable
OS     : Enable
MSTP   : Enable
ACL    : Disable
CLI    : Enable
SNMP   : Disable
IGMP   : Enable

Prompt#
```

21. DHCP Snooping コマンド

DHCP サーバから割り当てられた正規の IP アドレスを持つクライアントのみが通信できるようにします。
本機能を有効にすると、すべてのポートは "untrusted" に設定されます。DHCP サーバや DHCP リレーのポートは "trusted" に変更しておきます。"untrusted" ポートに接続されたクライアントからの通信は、最初 DHCP パケットのみが認証され、その他のパケットは破棄されます。スイッチは、"trusted" ポートの DHCP サーバとの通信内容を監視し、割り当てられた IP アドレスと MAC アドレスの対応を本体内の Binding Table に記録します。
Binding Table に記録された IP アドレス、MAC アドレスを持つクライアントのみが通常の通信を認証されます。

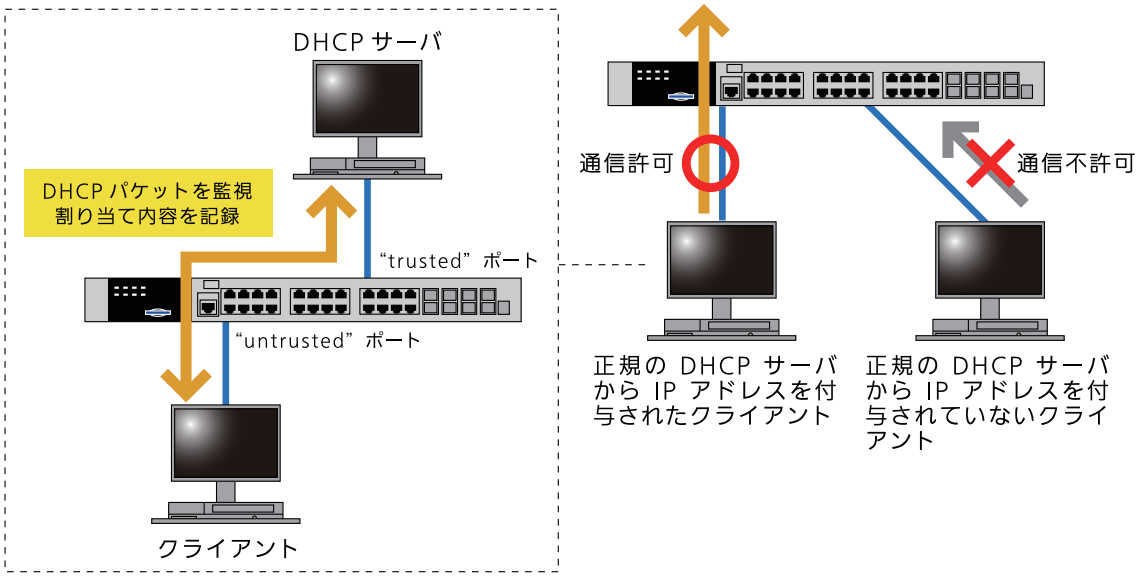


図 21-1

enable dhcp_snoop
disable dhcp_snoop
config dhcp_snoop max_entry ports [all | <portlist>] limit <value 1-50>
show dhcp_snoop
show dhcp_snoop binding_entry { [port <port> | vlan <vlan_name 32> | vlanid <vidlist> | ipaddress <ipaddr> | mac_address <macaddr>] }
show dhcp snoop max_entry [ports <portlist>]

21.1. enable dhcp_snoop

● 概要

このコマンドを用いて、スイッチの DHCP Snooping 動作を有効にします。DHCP Snooping 機能をグローバルに制御します。デフォルトでは、DHCP Snooping 機能は無効です。

● 構文

enable dhcp_snoop

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DHCP Snooping 機能をグローバルに有効にするには：

```
Zxxx0:admin#  enable dhcp_snoop
Command: enable dhcp_snoop

Success.

Zxxx0:admin#
```

21.2. disable dhcp_snoop

● 概要

このコマンドを用いて、スイッチの DHCP Snooping 動作を無効にします。このコマンドは、DHCP Snooping 機能を無効にします。デフォルトでは、DHCP Snooping 機能は無効です。

● 構文

disable dhcp_snoop

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DHCP Snooping 機能をグローバルに無効にするには：

```
Zxxx0:admin#  disable dhcp_snoop
Command: disable dhcp_snoop

Success.

Zxxx0:admin#
```

21.3. config dhcp_snoop max_entry ports

● 概要

このコマンドで、ポートごとの DHCP Snooping 対象とする端末の上限数を設定します。

● 構文

config dhcp_snoop max_entry ports [all | <portlist>] limit [no_limit | <value 1-50>]

● パラメータ

all	すべてのポートを指定します。
<portlist>	特定のポートを指定します。
limit	1 ポートあたりの DHCP Snooping の上限数を指定します。 no_limit 1 ポートあたりの DHCP Snooping の上限数を無制限に指定します。 <value 1-50> 1 ポートあたりの DHCP Snooping の上限数を 1 ～ 50 の間で指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

すべてのポートの DHCP Snooping の上限数を 10 に設定するには：

```
Zxxx0:admin#config dhcp_snoop max_entry ports all limit 10
Command: config dhcp_snoop max_entry ports all limit 10

Success.

Zxxx0:admin#
```

21.4. show dhcp_snoop

● 概要

このコマンドを用いて、DHCP Snooping 設定ステータスを表示します。

● 構文

show dhcp_snoop

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DHCP Snooping 設定ステータスを表示するには：

```
Zxxx0:admin#  show dhcp_snoop
Command: show dhcp_snoop

DHCP Snooping Status : Enabled

Zxxx0:admin#
```

21.5. show dhcp_snoop binding_entry

● 概要

このコマンドを用いて、DHCP Snooping のバインディングテーブル情報を表示します。

● 構文

show dhcp_snoop binding_entry { [port <port> | vlan <vlan_name 32> | vlanid <vidlist> | ipaddress <ipaddr> | mac_address <macaddr>] }

● パラメータ

<port>	特定のポートに対するエントリを表示します。
<vlan_name 32>	特定の VLAN 名に対するエントリを表示します。
<vidlist>	VID リストに示されている VLAN ID に対するエントリを表示します。
<ipaddr>	特定の IP アドレスに対するエントリを表示します。
<macaddr>	特定の MAC アドレスに対するエントリを表示します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザ、およびユーザのみ実行できます。

● 実行例

DHCP Snooping のバインディングテーブルを表示するには：

```
Zxxx0:admin#  admin# show dhcp_snoop binding_entry
Command: show dhcp_snoop binding_entry

Port  VID   IP  Address        MAC Address        Lease Time
----  ----  ----------------  -----------------  -----------
 1     2     10.0.0.1           00-00-00-00-00-01  00:23:59
 1     2     10.0.0.4           00-00-00-00-00-02  00:23:59
 1     2     10.0.0.5           00-00-00-00-00-03  00:23:59
 1     2     10.0.0.6           00-00-00-00-00-04  00:23:59
 1     2     10.0.0.7           00-00-00-00-00-05  00:23:59
 1     2     10.0.0.8           00-00-00-00-00-06  00:23:59
 1     2     10.0.0.9           00-00-00-00-00-07  00:23:59

 Total Entries : 7

Zxxx0:admin#
```

21.6. show dhcp_snoop max_entry

● 概要

このコマンドを用いて、ポートごとの DHCP Snooping 対象とする端末の上限数を表示します。

● 構文

show dhcp_snoop max_entry [ports <portlist>]

● パラメータ

<portlist> 特定ポートの上限数を指定します。
パラメータを指定しない場合、すべてのポートの上限数を表示します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザ、およびユーザのみ実行できます。

● 実行例

ポート 1:1 の端末上限数を表示するには：

```
Zxxx0:admin# show dhcp_snoop max_entry ports 1:1
Command: show dhcp_snoop max_entry ports 1:1

Port  Max Entry
----  ---------
1:1   No Limit

Zxxx0:admin#
```

22. DNS(Domain Name System) リレーコマンド

DNS（Domain Name System）とは、サーバ等のドメイン名を管理するしくみです。ドメイン名は階層構造に基づくルールにより命名され、ドメイン名の各階層に対応した DNS サーバにより、ドメイン名と IP アドレスの対応が管理されています。Web サーバ等へアクセスは、まず DNS サーバに問い合わせを行い、ドメイン名から IP アドレスを取得（名前解決）することにより可能となります。
DNS リレー機能とは、クライアントからの名前解決の要求を本装置で受け取り、本来の DNS サーバに転送する機能です。
TCP/IP ネットワークでは、各クライアント毎に DNS サーバの指定が必要となりますが、DNS リレー機能を利用すれば、本装置を DNS サーバとして設定できます。

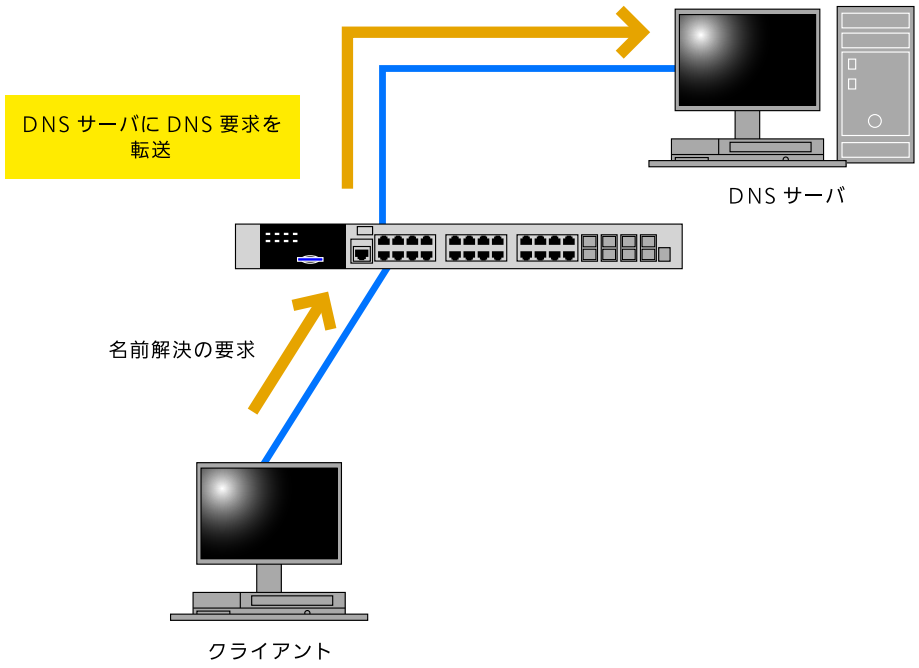


図 22-1　DNS リレー機能の概略

また、単なるリレー機能だけではなく、DNS キャッシュによる名前解決の効率化、スタティック DNS テーブルの設定も行えます。

config dnsr [[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>]
enable dnsr {[cache | static]}
disable dnsr {[cache | static]}
show dnsr {static}

22.1. config dnsr

● 概要

このコマンドを用いて、本装置の DNS 名前解決テーブルへのスタティックエントリの追加または削除を行うか、リレーサーバを設定します。

● 構文

config dnsr [[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>]

● パラメータ

primary	以下の IP アドレスがプライマリ DNS サーバのアドレスであることを指定します。
secondary	以下の IP アドレスがセカンダリ DNS サーバのアドレスであることを指定します。
nameserver	DNS ネームサーバの IP アドレスを指定します。 <ipaddr> DNS ネームサーバの IP アドレスを指定します。
add	DNS リレー機能を追加します。
delete	DNS リレー機能を削除します。
static	エントリのドメイン名を指定します。 <domain_name32> ドメイン名を指定します。 <ipaddr> エントリの IP アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP アドレス 10.24.22.5 をプライマリ DNS サーバとして設定するには：

```
Zxxx0:admin# config dnsr primary nameserver 10.24.22.5
Command: config dnsr primary nameserver 10.24.22.5

Success.

Zxxx0:admin#
```

IP アドレス 10.24.22.5 のエントリ dns1 を DNS スタティックテーブルに追加するには：

```
Zxxx0:admin#config dnsr add static dns1 10.24.22.5
Command: config dnsr add static dns1 10.24.22.5

Success.

Zxxx0:admin#
```

IP アドレス 10.24.22.5 のエントリ dns1 を DNS スタティックテーブルから削除するには：

```
Zxxx0:admin#config dnsr delete static dns1 10.24.22.5
Command: config dnsr delete static dns1 10.24.22.5

Success.

Zxxx0:admin#
```

22.2. enable dnsr

● 概要

このコマンドを用いて、DNS リレーを有効にします。

● 構文

enable dnsr {[cache | static]}

● パラメータ

cache	スイッチの DNS リレーのキャッシュルックアップを有効にします。
static	スイッチの DNS リレーのスタティックテーブルルックアップを有効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DNS リレーを有効にするには：

```
Zxxx0:admin#enable dnsr
Command: enable dnsr

Success.

Zxxx0:admin#
```

DNS リレーのキャッシュルックアップを有効にするには：

```
Zxxx0:admin#enable dnsr cache
Command: enable dnsr cache

Success.

Zxxx0:admin#
```

DNS リレーのスタティックテーブルルックアップを有効にするには：

```
Zxxx0:admin#enable dnsr static
Command: enable dnsr static

Success.

Zxxx0:admin#
```

22.3. disable dnsr

● 概要

このコマンドを用いて、スイッチの DNS リレーを無効にします。

● 構文

disable dnsr {[cache | static]}

● パラメータ

cache	（オプション）スイッチの DNS リレーのキャッシュルックアップを無効にします。
static	（オプション）スイッチの DNS リレーのスタティックテーブルルックアップを無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DNS リレーのステータスを無効にするには：

```
Zxxx0:admin#disable dnsr
Command: disable dnsr

Success.

Zxxx0:admin#
```

DNS リレーのキャッシュルックアップを無効にするには：

```
Zxxx0:admin#disable dnsr cache
Command: disable dnsr cache

Success.

Zxxx0:admin#
```

DNS リレーのスタティックテーブルルックアップを無効にするには：

```
Zxxx0:admin#disable dnsr static
Command: disable dnsr static

Success.

Zxxx0:admin#
```

22.4. show dnsr

● 概要

このコマンドを用いて、現在の DNS リレー設定およびスタティックエントリを表示します。

● 構文

show dnsr {static}

● パラメータ

static	（オプション）DNS リレーテーブルのスタティックエントリを表示します。このパラメータを指定しない場合、DNS リレーテーブル全体を表示します。

● 制限

なし

● 実行例

DNS リレーステータスを表示するには：

```
Zxxx0:admin#show dnsr
Command: show dnsr

DNSR Status              : Disabled
Primary Name Server      : 0.0.0.0
Secondary Name Server    : 0.0.0.0
DNSR Cache Status        : Disabled
DNSR Static Table Status : Disabled

DNS Relay Static Table

Domain Name                                IP Address
------------------------------------------ ---------------
www.123.com                                10.12.12.123

Total Entries: 1

Zxxx0:admin#
```

23. DNS リゾルバコマンド

DNS（Domain Name System）とは、サーバ等のドメイン名を管理するしくみです。ドメイン名は階層構造に基づくルールにより命名され、ドメイン名の各階層に対応した DNS サーバにより、ドメイン名と IP アドレスの対応が管理されています。Web サーバ等へアクセスは、まず DNS サーバに問い合わせを行い、ドメイン名から IP アドレスを取得（名前解決）することにより可能となります。
リゾルバ（Resolver）とは、名前解決を DNS サーバへ要求するクライアントのことです。
ここでは、本装置が名前解決を必要とする場合に利用する DNS サーバを設定します。

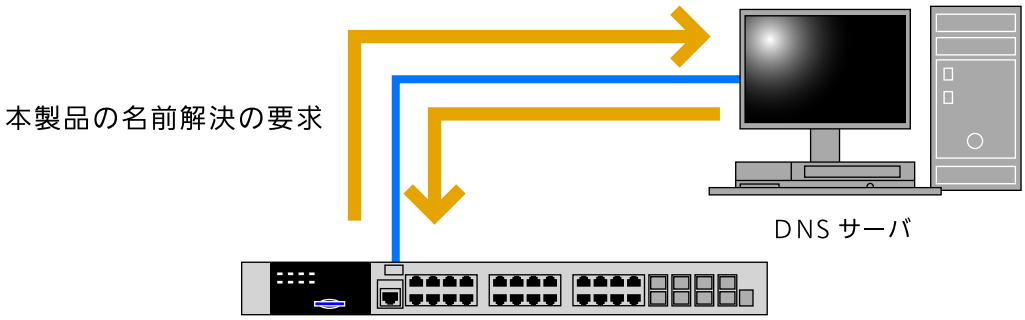


図 23-1　本製品の名前解決

DNS サーバからの応答の待ち時間（1-60 秒）の設定、スタティック DNS テーブルの登録、DNS キャッシュの確認・削除等も行えます。

config name_server add <ipaddr> {primary}
config name_server delete <ipaddr> {primary}
config name_server timeout <second 1-60>
show name_server
create host_name <name 255> <ipaddr>
delete host_name [<name 255> | all]
show host_name {static | dynamic}
enable dns_resolver
disable dns_resolver

23.1. config name_server add

● 概要

このコマンドを用いて、本装置に DNS リゾルバネームサーバを追加します。

● 構文

config name_server add <ipaddr> {primary}

● パラメータ

<ipaddr> 使用する DNS リゾルバネームサーバの IP アドレスを入力します。
primary （オプション）ネームサーバがプライマリネームサーバであることを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DNS リゾルバプライマリネームサーバ 10.10.10.10 を追加するには：

```
Zxxx0:admin# config name_server add 10.10.10.10 primary
Command: config name_server add 10.10.10.10 primary

Success.

Zxxx0:admin#
```

23.2. config name_server delete

● 概要

このコマンドを用いて、本装置から DNS リゾルバネームサーバを削除します。

● 構文

config name_server delete <ipaddr> {primary}

● パラメータ

<ipaddr> 使用する DNS リゾルバネームサーバの IP アドレスを入力します。
primary （オプション）ネームサーバがプライマリネームサーバであることを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DNS リゾルバネームサーバ 10.10.10.1 を削除するには：

```
Zxxx0:admin# config name_server delete 10.10.10.10
Command: config name_server delete 10.10.10.10

Success.

Zxxx0:admin#
```

23.3. config name_server timeout

● 概要

このコマンドを用いて、DNS リゾルバネームサーバのタイムアウト値を設定します。

● 構文

config name_server timeout <second 1-60>

● パラメータ

timeout	指定したネームサーバからの応答を待つ最大時間を指定します。
	<second 1-60>
	使用するタイムアウト値を入力します。この値は、1 ～ 60 秒で指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DNS リゾルバネームサーバのタイムアウトを 10 秒に設定するには：

```
Zxxx0:admin# config name_server timeout 10
Command: config name_server timeout 10

Success.

Zxxx0:admin#
```

23.4. show name_server

● 概要

このコマンドを用いて、本装置の現在の DNS リゾルバネームサーバおよびネームサーバのタイムアウトを表示します。

● 構文

show name_server

● パラメータ

なし

● 制限

なし

● 実行例

現在の DNS リゾルバネームサーバおよびネームサーバのタイムアウトを表示するには：

```
Zxxx0:admin# show name_server
Command: show name_server

Name Server Time Out: 3 seconds

Static Name Server Table:
Server IP Address     Priority
--------------------- --------------
20.20.20.20           Secondary
10.1.1.1              Primary

Dynamic Name Server Table:
Server IP Address     Priority
--------------------- --------------
10.48.74.122          Primary

Zxxx0:admin#
```

23.5. create host_name

● 概要

このコマンドを用いて、本装置のスタティックホスト名エントリを作成します。

● 構文

create host_name <name 255> <ipaddr>

● パラメータ

<name 255>	使用するホスト名を入力します。 最大文字数は、「.」区切りで各パート 63 文字、最大 255 文字です。
<ipaddr>	使用するホストの IP アドレスを入力します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スタティックホスト名 www.example.com を作成するには：

```
Zxxx0:admin# create host_name www.example.com 10.10.10.10
Command: create host_name www.example.com 10.10.10.10

Success.

Zxxx0:admin#
```

23.6. delete host_name

● 概要

このコマンドを用いて、本装置のスタティックまたはダイナミックホスト名エントリを削除します。

● 構文

delete host_name [<name 255> | all]

● パラメータ

<name 255>	使用するホスト名を入力します。 最大文字数は、「.」区切りで各パート 63 文字、最大 255 文字です。
all	すべてのホスト名を削除します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スタティックホスト名エントリ www.example.com を削除するには：

```
Zxxx0:admin# delete host_name www.example.com
Command: delete host_name www.example.com

Success.

Zxxx0:admin#
```

23.7. show host_name

● 概要

このコマンドを用いて、現在のホスト名を表示します。

● 構文

show host_name {static | dynamic}

● パラメータ

static	（オプション）スタティックホスト名エントリを表示します。
dynamic	（オプション）ダイナミックホスト名エントリを表示します。

● 制限

なし

● 実行例

スタティックおよびダイナミックホスト名エントリを表示するには：

```
Zxxx0:admin# show host_name
Command: show host_name

Static Host Name Table
Host Name                          IP Address
-----------------------------   ---------------
www.example.com                   10.10.10.10
www.exampla.com                   20.20.20.20

Total Static Entries: 2

Dynamic Host Name Table
Host Name                          IP Address       TTL
-----------------------------   --------------- --------
www.examplc.com                   30.30.30.30      60 minutes
www.exampld.com                   40.40.40.40      10 minutes

Total Dynamic Entries: 2

Zxxx0:admin#
```

23.8. enable dns_resolver

● 概要

このコマンドを用いて、本装置の DNS リゾルバ状態を有効にします。

● 構文

enable dns_resolver

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DNS リゾルバ状態を有効にするには：

```
Zxxx0:admin# enable dns_resolver
Command: enable dns_resolver

Success.

Zxxx0:admin#
```

23.9. disable dns_resolver

● 概要

このコマンドを用いて、本装置の DNS リゾルバ状態を無効にします。

● 構文

disable dns_resolver

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DNS リゾルバ状態を無効にするには：

```
Zxxx0:admin# disable dns_resolver
Command: disable dns_resolver

Success.

Zxxx0:admin#
```

24. 省電力型イーサネット（EEE）コマンド

IEEE802.3az の省電力型イーサネット (Energy Efficient Ethernet：以下、EEE) 機能により、本機能の対応機器同士でリンクアップしている場合の消費電力の削減を図ることができます。

config eee ports [<portlist> | all] state [enable | disable]
show eee ports {<portlist>}

24.1. config eee ports

● 概要

このコマンドを用いて、ポートの設定を変更します。

● 構文

config eee ports [<portlist> | all] state [enable | disable]

● パラメータ

portlist	設定するポートの範囲を指定します。
all	システムのすべてのポートを設定します。
state	指定したポートの EEE 動作状態を有効または無効にします。初期値は enable です。 enable 指定したポートの EEE を有効にします。 disable 指定したポートの EEE を無効にします。

NOTE ポートスピードを auto 以外に変更する場合は、対象ポートの EEE 動作を無効にする必要があります。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 3 の EEE 動作を無効に指定するには：

```
Zxxx0:admin#config eee ports 1-3 state disable
Command: config eee ports 1-3 state disable

Success.

Zxxx0:admin#
```

24.2. show eee ports

● 概要

このコマンドを用いて、指定した範囲のポートの現在の設定を表示します。

● 構文

show eee ports {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

NOTE このパラメータを指定しない場合、すべてのポートが表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 4 の EEE 設定を表示するには：

```
Zxxx0:admin#show eee ports 1-4
Command: show eee ports 1-4

Port             State
---------     -----------
1             Enabled
2             Enabled
3             Enabled
4             Enabled



Zxxx0:admin#
```

25. FDB コマンド

フォワーディングデータベース（FDB）とは、ネットワーク機器の MAC アドレスと接続先の VLAN やポートの対応テーブルのことです。スイッチは、受信したパケットの MAC アドレス情報から FDB を参照し、転送先の VLAN やポートを決定します。

```
VID  VLAN Name                        MAC Address       Port   Type
---- -------------------------------- ----------------- ------ -------
1    default                          00-00-00-00-00-01 1:25   Dynamic
1    default                          00-00-00-00-00-02 1:25   Dynamic
1    default                          00-00-00-00-00-03 T1     Static
1    default                          00-00-00-00-00-04 T1     Static
1    default                          00-00-00-00-00-0A CPU    Self
1    default                          00-00-00-00-00-06 -      Static
```

通常 FDB は、受信パケットの情報から自動的に作成されます。ただし、管理者が手動で登録することもできます。また、 1 つの宛先に送信するユニキャストのみではなく、複数の宛先に送信するマルチキャストの FDB も作成され、マルチキャストのグループに参加させるポート、参加させないポートの設定なども行えます。

● マルチキャストフィルタリング機能

複数の宛先にデータを同時に送信するマルチキャストでは、マルチキャストグループが存在しない場合に不要なポートへもマルチキャストデータが転送されることがあります。マルチキャストフィルタリング機能を有効にすると、マルチキャストグループが形成されていない場合でも、マルチキャストデータをルータポート以外に転送を行わないようにできます。

create fdb <vlan_name 32> <macaddr> [port <port> | drop]
create fdb vlanid <vidlist> <macaddr> [port <port> | drop]
create multicast_fdb <vlan_name 32> <macaddr>
config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time <sec 10-1000000>
config multicast vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]
delete fdb <vlan_name 32> <macaddr>
clear fdb [vlan <vlan_name 32> | port <port> | all]
show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}
show fdb {[port <port> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static | aging_time | security]}
show multicast vlan_filtering_mode {[vlanid <vidlist> | vlan <vlan_name 32>]}

25.1. create fdb

● 概要

このコマンドを用いて、スイッチのユニキャスト MAC アドレスフォワーディングデータベースにエントリを追加します。

● 構文

create fdb <vlan_name 32> <macaddr> [port <port> | drop]

● パラメータ

<vlan_name 32>	MAC アドレスに関連付けられた VLAN 名を指定します。32 文字以内で設定します。
<macaddr>	スタティックフォワーディングテーブルに追加する MAC アドレスを指定します。
port	スイッチでは、常にこのポートを介して指定装置にトラフィックを転送します。 <port>MAC 宛先アドレスに対応するポート番号を指定します。 drop スイッチでトラフィックを破棄するよう指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ユニキャスト MAC フォワーディングを作成するには：

```
Zxxx0:admin#create fdb default 00-00-00-00-01-02 port 1:5
Command: create fdb default 00-00-00-00-01-02 port 1:5

Success.
Zxxx0:admin#
```

25.2. create fdb vlanid

● 概要

このコマンドを用いて、VLAN ID を指定し、スイッチのユニキャスト MAC アドレスフォワーディングデータベースにエントリを作成します。

● 構文

create fdb vlanid <vidlist> <macaddr> [port <port> | drop]

● パラメータ

<vidlist>	使用する VLAN ID を入力します。
<macaddr>	スタティックフォワーディングテーブルに追加する MAC アドレスを指定します。
port	スイッチでは、常にこのポートを介して指定装置にトラフィックを転送します。 <port>MAC 宛先アドレスに対応するポート番号を指定します。 drop スイッチでトラフィックを破棄するよう指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ユニキャスト MAC フォワーディングを作成するには：

```
Zxxx0:admin#create fdb vlanid 1 00-11-22-33-44-55 port 1:5
Command: create fdb vlanid 1 00-11-22-33-44-55 port 1:5

Success.

Zxxx0:admin#
```

25.3. create multicast_fdb

● 概要

このコマンドを用いて、スイッチのマルチキャスト MAC アドレスフォワーディングデータベースにエントリを追加します。

● 構文

create multicast_fdb <vlan_name 32> <macaddr>

● パラメータ

<vlan_name 32>	その MAC アドレスが存在する VLAN 名を指定します。32 文字以内で設定します。
<macaddr>	スタティックフォワーディングテーブルに追加するマルチキャスト MAC アドレスを指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

マルチキャスト MAC フォワーディングを作成するには：

```
Zxxx0:admin# create multicast_fdb default 01-00-00-00-01-01
Command: create multicast_fdb default 01-00-00-00-01-01

Success.

Zxxx0:admin#
```

25.4. config multicast_fdb

● 概要

このコマンドを用いて、マルチキャスト MAC アドレスフォワーディングテーブルを設定使用します。

● 構文

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

● パラメータ

<vlan_name 32>	その MAC アドレスが存在する VLAN 名を指定します。名前は 32 文字以内で設定します。
<macaddr>	フォワーディングテーブルに追加またはフォワーディングテーブルから削除するMACアドレスを指定します。
add	ポートの追加を指定します。
add	ポートの削除を指定します。
<portlist>	設定するポート範囲を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

マルチキャスト MAC フォワーディングを追加するには：

```
Zxxx0:admin# config multicast_fdb default 01-00-00-00-01-01 add 1-5
Command: config multicast_fdb default 01-00-00-00-01-01 add 1-5

Success.

Zxxx0:admin#
```

25.5. config fdb aging_time

● 概要

このコマンドを用いて、スイッチのダイナミックユニキャスト MAC アドレスフォワーディングテーブルのエージアウトタイマーを設定します。

● 構文

config fdb aging_time <sec 10-1000000>

● パラメータ

<sec 10-1000000>	- ダイナミックに認識された MAC アドレスがデータベースから破棄されるまでに、アクセスされることなくスイッチの MAC アドレスフォワーディングテーブル内に保持される時間を秒で指定します。値の範囲は 10 ～ 1000000 です。初期値は 300 です。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC アドレスエージングタイムを設定するには：

```
Zxxx0:admin#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

Zxxx0:admin#
```

25.6. config multicast vlan_filtering_mode

● 概要

このコマンドを用いて、VLAN にマルチキャストパケットフィルタリングモードを設定します。

● 構文

config multicast vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]

● パラメータ

vlanid	設定する VLAN ID リストを指定します。 <vidlist> 設定する VLAN ID リストを指定します。
vlan	設定する VLAN 名を指定します。 <vlan_name 32> 32 文字以内で設定します。
all	すべての VLAN ID を指定します。
forward_all_groups	すべてのマルチキャストグループを VLAN に基づいて転送します。
forward_unregistered_groups	フィルタリングモードとして forward_unregistered_groups を指定します。これはデフォルトの設定です。
filter_unregistered_groups	フィルタリングモードとして filter_unregistered_groups を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

すべての VLAN に対してマルチキャストパケットフィルタリングモードを設定するには：

```
Zxxx0:admin#config multicast vlan_filtering_mode all forward_unregistered_groups
Command: config multicast port filtering_mode all forward_unregistered_groups

Success.

Zxxx0:admin#
```

25.7. delete fdb

● 概要

このコマンドを用いて、作成した FDB エントリを削除します。

● 構文

delete fdb <vlan_name 32> <macaddr>

● パラメータ

<vlan_name 32> その MAC アドレスが存在する VLAN 名を指定します。32 文字以内で設定します。
<macaddr> スタティックフォワーディングテーブルから削除する MAC アドレスを指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

恒久的な FDB エントリを削除するには：

```
Zxxx0:admin#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

Zxxx0:admin#
```

25.8. clear fdb

● 概要

このコマンドを用いて、スイッチのフォワーディングデータベースから、ダイナミックに認識されたすべての MAC アドレスをクリアします。

● 構文

clear fdb [vlan <vlan_name 32> | port <port> | all]

● パラメータ

vlan	その MAC アドレスが存在する VLAN 名を指定します。 <vlan_name 32> 32 文字以内で設定します。
port	ダイナミックに認識された MAC アドレスに対応するポート番号を指定します。 <port>ダイナミックに認識された MAC アドレスに対応するポート番号を指定します。
all	すべての VLAN およびポートをクリアするよう指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

すべての FDB ダイナミックエントリをクリアするには：

```
Zxxx0:admin#clear fdb all
Command: clear fdb all

Success.

Zxxx0:admin#
```

25.9. show multicast_fdb

● 概要

このコマンドを用いて、スイッチのマルチキャストフォワーディングデータベースを表示します。

● 構文

show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}

● パラメータ

vlan	（オプション）その MAC アドレスが存在する VLAN 名を指定します。 <vlan_name 32> 32 文字以内で設定します。
vlanid	（オプション）その MAC アドレスが存在する VLAN ID を指定します。 <vidlist> 使用する VLAN ID を入力します。
mac_address	（オプション）表示する FDB エントリの MAC アドレスを指定します。 <macaddr> 表示する FDB エントリの MAC アドレスを指定します。

NOTE パラメータを指定しなかった場合、すべてのマルチキャスト FDB エントリを表示します。

● 制限

なし

● 実行例

マルチキャスト MAC アドレステーブルを表示するには：

```
Zxxx0:admin#show multicast_fdb
Command: show multicast_fdb

VLAN Name      : default
MAC Address    : 01-00-00-00-01-01
Egress Ports   : 1-5,26
Mode           : Static

Total Entries : 1

Zxxx0:admin#
```

25.10. show fdb

● 概要

このコマンドを用いて、現在のユニキャスト MAC アドレスフォワーディングデータベースを表示します。

● 構文

show fdb {[port <port> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static | aging_time | security]}

● パラメータ

port	（オプション）1 つのポートに対するエントリを指定します。 <port>1 つのポートに対するエントリを指定します。
vlan	（オプション）特定の VLAN に対するエントリを表示します。 <vlan_name 32> 32 文字以内で設定します。
vlanid	（オプション）VLAN ID リストに基づいてエントリを表示します。 <vidlist> VLAN ID リストに基づいてエントリを表示します。
mac_address	（オプション）MAC アドレスを指定します。 <macaddr> MAC アドレスを指定します。
static	（オプション）作成したすべてのエントリを表示します。
aging_time	ユニキャスト MAC アドレスエージングタイムを表示するよう指定します。
security	セキュリティ設定を表示するよう指定します。

NOTE パラメータを指定しなかった場合、すべてのユニキャスト FDB エントリを表示します。

● 制限

なし

● 実行例

ユニキャスト MAC アドレステーブルを表示するには：

```
Zxxx0:admin#show fdb
Command: show fdb

 Unicast MAC Address Aging Time  = 300

 VID  VLAN Name                         MAC Address       Port  Type    Status
 ---- --------------------------------- ----------------- ----- ------- -------
 1    default                           00-01-02-03-04-00 CPU   Self    Forward
 1    default                           00-26-5A-AE-CA-1C 21    Dynamic Forward

Total Entries: 2

Zxxx0:admin#
```

25.11. show multicast vlan_filtering_mode

● 概要

このコマンドを用いて、VLAN に対するマルチキャストパケットフィルタリングモードを表示します。

● 構文

show multicast vlan_filtering_mode {[vlanid <vidlist> | vlan <vlan_name 32>]}

● パラメータ

vlanid	（オプション）VLAN ID リストに基づいてエントリを表示します。 <vidlist> VLAN ID リストに基づいてエントリを表示します。
vlan	（オプション）特定の VLAN に対するエントリを表示します。 <vlan_name 32> 32 文字以内で設定します。

● 制限

なし

● 実行例

ポートに対するマルチキャストフィルタリングモードを表示するには：

```
Zxxx0:admin#show multicast vlan_filtering_mode
Command: show multicast filtering_mode

VLAN ID/VLAN Name                 Multicast Filter Mode
--------------------------------  ------------------------------
default                           forward_unregistered_groups

Zxxx0:admin#
```

26. ファイルシステム管理コマンド

本装置のストレージメディアのファイル管理を行います。
メディアの情報確認／フォーマット、ドライブの変更、ディレクトリの作成／変更／削除、ファイルの表示／名前変更／削除／コピー／移動を行えます。

show storage_media_info {[unit <unit_id> | all]}
md {{unit <unit_id>} <drive_id>} <pathname>
rd {{unit <unit_id>} <drive_id>} <pathname>
cd {<pathname>}
dir {{unit <unit_id>} <drive_id>} {<pathname>}
rename {{unit <unit_id>} <drive_id>} <pathname> <filename>
erase {{unit <unit_id>} <drive_id>} <pathname>
format {unit <unit_id>} <drive_id> {[fat16 | fat32]} {<label_name>}
del {{unit <unit_id>} <drive_id>} <pathname> {recursive}
move {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>
copy {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>
change drive {unit <unit_id>} <drive_id>

26.1. show storage_media_info

● 概要

このコマンドを用いて、ストレージメディア情報を表示します。

● 構文

show storage_media_info {[unit <unit_id> | all]}

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。
all	スタッキングシステムのストレージメディア情報内のすべてのユニットを表示するよう指定します。

● 制限

なし

● 実行例

ストレージメディア情報を表示するには：

```
Zxxx0:admin#show storage_media_info
Command: show storage_media_info

Unit  Drive  Media Type      Size  Label        FS Type
----  -----  ----------  --------  -----------  -------
   1  c:     Flash         123 MB               FFS

Zxxx0:admin#
```

26.2. md

● 概要

このコマンドを用いて、ディレクトリを作成します。

● 構文

md {{unit <unit_id>} <drive_id>} <pathname>

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。
<pathname>	作成するディレクトリを指定します。パス名は、フルパス名または部分名のどちらかで指定できます。部分パス名の場合、ディレクトリが現在のディレクトリ内にあることを示します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

ディレクトリを作成するには：

```
Zxxx0:admin#md c:/abc
Command: md c:/abc

Success.

Zxxx0:admin#
```

26.3. rd

● 概要

このコマンドを用いて、ディレクトリを削除します。ディレクトリ内にまだファイルおよびディレクトリが存在する場合、このコマンドを実行すると失敗し、エラーメッセージを返します。

● 構文

rd {{unit <unit_id>} <drive_id>} <pathname>

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。
<pathname>	削除するディレクトリを指定します。パス名は、フルパス名または部分名のどちらかで指定できます。部分パス名の場合、ファイルが現在のディレクトリ内にあることを示します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

空のディレクトリを削除するには：

```
Zxxx0:admin#rd c:/abc
Command: rd c:/abc

Success.

Zxxx0:admin#
```

26.4. cd

● 概要

このコマンドを用いて、現在のディレクトリを変更します。ユーザは、このコマンドを使用して、現在のディレクトリを別のドライブに変更できます。<pathname> を指定しなかった場合、現在のドライブおよび現在のディレクトリが表示されます。

● 構文

cd {<pathname>}

● パラメータ

<pathname> （オプション）変更するディレクトリを指定します。パス名は、フルパス名または部分名のどちらかで指定できます。部分パス名の場合、ファイルが現在のディレクトリ内にあることを示します。

● 制限

なし

● 実行例

作業ディレクトリを変更するには：

```
Zxxx0:admin#cd d1
Command: cd d1

Current work directory: "c:/d1"

Zxxx0:admin#
```

26.5. dir

● 概要

このコマンドを用いて、あるドライブのディレクトリ内にあるすべてのファイルをリスト表示します。パス名を指定しなかった場合、指定ドライブ内にあるすべてのファイルが表示されます。パラメータを 1 つも指定しなかった場合、現在のディレクトリ内にあるファイルが表示されます。ユーザがシステムディレクトリをリスト表示した場合、使用中の容量が表示されます。

● 構文

dir {{unit <unit_id>} <drive_id>} {<pathname>}

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。
<pathname> （オプション）リスト表示するディレクトリを指定します。パス名は、フルパス名または部分名のどちらかで指定できます。部分パス名の場合、ファイルが現在のディレクトリ内にあることを示します。このパラメータに含まれるドライブ ID は、d:/config/bootup.cfg などのように指定します。	

● 制限

なし

● 実行例

ディレクトリをリスト表示するには：

```
Zxxx0:admin#dir
Command: dir

Directory of c:/
Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----
  1 RUN(*)  -rw- 4796564  2000/01/22 03:52:03  runtime.rom
  2 CFG(*)  -rw- 24120    2000/01/22 23:22:58  config.cfg
  3 CFG(b)  -rw- 24120    2000/01/23 06:59:39  1
  4         d---          2000/01/23 22:52:50  system
30608 KB total (25700 KB free)

 (*) -with boot up info         (b) -with backup info

Zxxx0:admin#
```

システムディレクトリをリスト表示するには：

```
Zxxx0:admin#dir c:/system
Command: dir c:/system

System reserved directory. Used space 89KB.

Zxxx0:admin#
```

26.6. rename

● 概要

このコマンドを用いて、ファイルシステム内のファイルの名前を変更します。pathname は、名前を変更するファイルを（パス形式で）指定します。filename は、新しいファイル名を指定します。パス名をフルパスで指定しなかった場合、ドライブの現在のディレクトリ下のパスを参照します。名前を変更したファイルは、同じディレクトリ内に残ります。

● 構文

rename {{unit <unit_id>} <drive_id>} <pathname> <filename>

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。
<pathname>	名前を変更するファイルを（パス形式で）指定します。
<filename>	ファイルの新しい名前を指定します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

ファイルまたはディレクトリの名前を変更するには：

```
Zxxx0:admin#rename run.rom run1.rom
Command: rename run.rom run1.rom

Success.

Zxxx0:admin#
```

26.7. erase

● 概要

このコマンドを用いて、ファイルシステムに保存されているファイルを削除します。指定したファイルが起動用イメージファイル、設定ファイルまたは保存されている最後のイメージファイルの場合には、システムでその旨プロンプト表示します。

● 構文

erase {{unit <unit_id>} <drive_id>} <pathname>

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。
<pathname> 削除するファイルを指定します。対応形式で指定された場合、現在のディレクトリに関連しています。	

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

ファイルを削除するには：

```
Zxxx0:admin#erase cfg
Command: erase cfg

Are you sure to remove the boot up Configuration from this device? (y/n)y

Success.

Zxxx0:admin#
```

26.8. format

● 概要

このコマンドを用いて、特定のドライブをフォーマットします。

● 構文

format {unit <unit_id>} <drive_id> {[fat16 | fat32]} {<label_name>}

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。
fat16	（オプション）FAT16 ファイルシステムをサポートするようドライブがフォーマットされます。
fat32	（オプション）FAT32 ファイルシステムをサポートするようドライブがフォーマットされます。
<label_name> （オプション）このドライブで使用するラベル名を入力します。	

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

メディアをフォーマットするには：

```
Zxxx0:admin#format d: fat32
Command: format d: fat32

 Formatting.......................... Done!

Zxxx0:admin#
```

26.9. del

● 概要

このコマンドを用いて、ファイルを削除します。また、ディレクトリとそのコンテンツを削除するためにも使用します。指定したファイルが起動イメージファイル、設定ファイルまたは保存されている最後のイメージファイルの場合には、システムでその旨プロンプト表示します。

● 構文

del {{unit <unit_id>} <drive_id>} <pathname> {recursive}

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。
<pathname>	削除するファイルまたはディレクトリを指定します。対応形式で指定された場合、現在のディレクトリに関連しています。
recursive	（オプション）ディレクトリが空でない場合でもディレクトリとそのコンテンツを削除するために、ディレクトリに対して使用します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

ファイルを削除するには：

```
Zxxx0:admin#del cfg
Command: del cfg

Are you sure to remove the boot up Configuration from this device? (y/n)y

Success.

Zxxx0:admin#
```

パラメータ recursive を指定してディレクトリを削除するには：

```
Zxxx0:admin# del d1 recursive
Command: del d1 recursive

Success.

Zxxx0:admin#
```

26.10. move

● 概要

このコマンドを用いて、ファイルシステム内でファイルを移動します。ファイルを移動するときに、同時に名前も変更するかを指定できます。

● 構文

move {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。
<pathname>	移動するファイルを指定します。パス名は、フルパス名または部分名のどちらかで指定できます。部分パス名の場合、ファイルが現在のディレクトリ内にあることを示します。
unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。
<pathname>	ファイルの移動先となる新しいパスを指定します。パス名は、フルパス名または部分名のどちらかで指定できます。部分パス名の場合、ファイルが現在のディレクトリ内にあることを示します。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

ファイルまたはディレクトリを移動するには：

```
Zxxx0:admin#move c:/log.txt c:/abc/log1.txt
Command: move c:/log.txt c:/abc/log1.txt

Success.

Zxxx0:admin#
```

26.11. copy

● 概要

このコマンドを用いて、あるファイルをファイルシステム内の別のファイルにコピーします。

● 構文

copy {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>

● パラメータ

unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。 <pathname> コピーするファイルを指定します。対応形式で指定された場合、現在のディレクトリに関連しています。
unit	スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。 <drive_id> ドライブ ID を指定します。指定しなかった場合、現在のドライブを参照します。 <pathname> コピー先のファイルを指定します。対応形式で指定された場合、現在のディレクトリに関連しています。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルのユーザのみ実行できます。

● 実行例

ファイルをコピーするには：

```
Zxxx0:admin#copy c:/log.txt c:/log1.txt
Command: copy c:/log.txt c:/log1.txt

Copying.......................... Done!

Zxxx0:admin#
```

26.12. change drive

● 概要

このコマンドを用いて、現在のドライブを変更します。

● 構文

change drive {unit <unit_id>} <drive_id>

● パラメータ

unit	（オプション）スタッキングシステム内のユニット ID を指定します。指定しなかった場合、マスターユニットを参照します。 <unit_id> ユニット ID 値を入力します。
<drive_id>	ドライブ ID を指定します。drive_id は、「c:」または「d:」という形式で指定します。

● 制限

なし

● 実行例

記憶装置の情報を表示するには：

```
Zxxx0:admin# change drive unit 3 c:
Command: change drive unit 3 c:

Current work directory: "/unit3:/c:".

Zxxx0:admin#
```

27.フィルタコマンド

DHCP サーバからのパケット、および NetBIOS over TCP/IP、NetBIOS のパケットをフィルタします。
DHCP サーバからのパケットのフィルタを利用すれば、ネットワーク上に複数の DHCP サーバがある場合に、利用する DHCP サーバを限定することができます。また、不正な DHCP サーバを検出し、ログへの記録や SNMP トラップとして管理サーバに報告することができます。

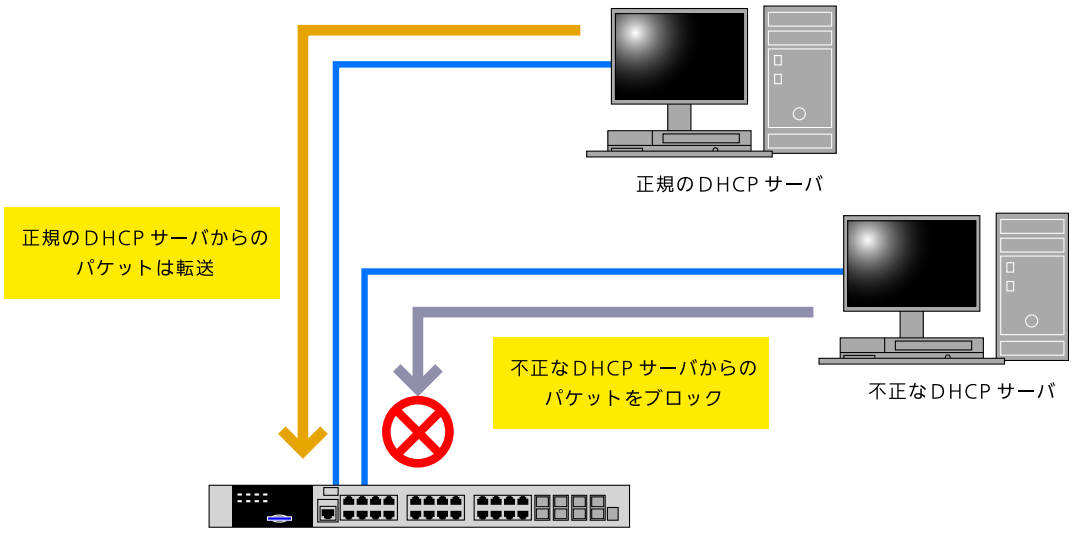


図 27-1　DHCP サーバパケットのフィルタリング

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]
show filter dhcp_server
config filter extensive_netbios [<portlist> | all] state [enable | disable]
show filter extensive_netbios
config filter netbios [<portlist> | all] state [enable | disable]
show filter netbios

27.1. config filter dhcp_server

● 概要

このコマンドには、2 つの用途があります。特定ポートですべての DHCP サーバパケットをフィルタリングすること、および事前定義されたサーバ IP アドレスおよびクライアント MAC アドレスを持つ一部の DHCP サーバパケットを認証することです。この機能を用いて、特定の DHCP クライアントに対してサービスを実行するよう DHCP サーバを制限できます。これは、ネットワーク上に 2 つの DHCP サーバがあるときに役立ちます。一方でプライベート IP アドレスを提供し、もう一方でパブリック IP アドレスを提供できます。
DHCP サーバポートフィルタ状態を有効にすることで、1 つのアクセスプロファイルと、ポート毎に（UDP ポートは 67）1 つのアクセスルールが作成されます。このファイルのフィルタコマンドは、同一アクセスプロファイルを共有します。DHCP 認証エントリを追加することで、1 つのアクセスプロファイルと 1 つのアクセスルールが作成されます。このファイルのフィルタコマンドは、同一アクセスプロファイルを共有します。

● 構文

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]

● パラメータ

add permit server_ip
　認証する DHCP サーバの IP アドレスを指定します。
　<ipaddr>
　　IP アドレスを指定します。
　client_mac
　　（オプション）DHCP クライアントの MAC アドレスを指定します。
　　<macaddr>
　　　MAC アドレスを指定します。
　ports ポートを指定します。
　　<portlist>
　　　設定するポートの範囲を指定します。
　　all　すべてのポートを設定します。

delete permit server_ip
　認証するサーバの IP アドレスの削除を指定します。
　<ipaddr>
　　IP アドレスを指定します。
　client_mac
　　（オプション）DHCP クライアントの MAC アドレスを指定します。
　　<macaddr>
　　　MAC アドレスを指定します。
　ports ポートを指定します。
　　<portlist>
　　　設定するポートの範囲を指定します。
　　all　すべてのポートを設定します。

ports	ポートを指定します。 <portlist> 設定するポートの範囲を指定します。 all すべてのポートを設定します。 state ポートのステータスを指定します。 enable 状態を有効にします。 disable 状態を無効にします。
illegal_server_log_suppress_duration	不正サーバログの抑制時間を指定します。 1min 不正サーバログの抑制時間として 1 分を指定します。 5min 不正サーバログの抑制時間として 5 分を指定します。 30min 不正サーバログの抑制時間として 30 分を指定します。
trap_log	トラップログのステータスを指定します。 enable トラップログ機能を有効にします。 disable トラップログ機能を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DHCP サーバ / クライアントフィルタリストのエントリを本装置のデータベースに追加するには：

```
Zxxx0:admin#config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-00-00-01 port 1-26
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-00-00-01 port 1-26

Success.

Zxxx0:admin#
```

DHCP サーバフィルタ状態を設定するには：

```
Zxxx0:admin#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success.

Zxxx0:admin#
```

27.2. show filter dhcp_server

● 概要

このコマンドを用いて、本装置で作成した DHCP サーバ / クライアントフィルタリストを表示します。

● 構文

show filter dhcp_server

● パラメータ

なし

● 制限

なし

● 実行例

本装置で作成した DHCP サーバ / クライアントフィルタリストを表示するには：

```
Zxxx0:admin#show filter dhcp_server
Command: show filter dhcp_server

Enabled Ports: 1,28
Trap & Log State: Enabled
Illegal Server Log Suppress Duration: 1 minutes
Permit DHCP Server/Client Table
Server IP Address Client MAC Address  Port
----------------- ------------------- ---------------
 Total Entries: 0

Zxxx0:admin#
```

27.3. config filter extensive_netbios

● 概要

このコマンドを用いて、ネットワーク上でやりとりする 802.3 フレームを介した NetBIOS パケットを本装置で拒否します。802.3 フレームを介した NetBIOS パケットのフィルタを有効にすることで、1 つのアクセスプロファイルと、ポート毎に 1 つのアクセスルールが自動的に作成されます。このファイルのフィルタコマンドは、同一アクセスプロファイルを共有します。

● 構文

config filter extensive_netbios [<portlist> | all] state [enable | disable]

● パラメータ

<portlist>設定するポートの範囲を指定します。	
all	すべてのポートを設定します。
state	802.3フレームを介したNetBIOSパケットをブロックするためのフィルタのステータスを指定します。 enable 802.3 フレームを介した NetBIOS パケットをブロックするフィルタを有効にします。 disable 802.3 フレームを介した NetBIOS パケットをブロックするフィルタを無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 10 で NetBIOS 広域フィルタ状態を設定するには：

```
Zxxx0:admin#config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

Success.

Zxxx0:admin#
```

27.4. show filter extensive_netbios

● 概要

このコマンドを用いて、本装置の NetBIOS 広域フィルタ状態を表示します。

● 構文

show filter extensive_netbios

● パラメータ

なし

● 制限

なし

● 実行例

スイッチの NetBIOS 広域フィルタ状態を表示するには：

```
Zxxx0:admin#show filter extensive_netbios
Command: show filter extensive_netbios

Enabled Ports: 1-3

Zxxx0:admin#
```

27.5. config filter netbios

● 概要

このコマンドを用いて、ネットワーク上でやりとりする NetBIOS パケットを本装置で拒否します。NetBIOS フィルタ状態を有効にすることで、1 つのアクセスプロファイルと、ポート毎に（UDP ポート 137 および 138、TCP ポート 139）3 つのアクセスルールが自動的に作成されます。このファイルのフィルタコマンドは、同一アクセスプロファイルを共有します。

● 構文

config filter netbios [<portlist> | all] state [enable | disable]

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを設定します。
state	NetBIOS パケットをブロックするためのフィルタのステータスを指定します。 enable NetBIOS パケットをブロックするフィルタを有効にします。 disable NetBIOS パケットをブロックするフィルタを無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

NetBIOS フィルタ状態を設定するには：

```
Zxxx0:admin#config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

Zxxx0:admin#
```

27.6. show filter netbios

● 概要

このコマンドを用いて、本装置の NetBIOS フィルタ状態を表示します。

● 構文

show filter netbios

● パラメータ

なし

● 制限

なし

● 実行例

NetBIOS フィルタ状態を表示するには：

```
Zxxx0:admin#show filter netbios
Command: show filter netbios

Enabled Ports: 1-3

Zxxx0:admin#
```

28. Gratuitous ARP コマンド

ARP（Address Resolution Protocol）とは、宛先の MAC アドレスが不明な場合に、IP アドレスから MAC アドレスを求めるために利用されます。Gratuitous ARP とは、IP インターフェースの起動時に送信される特別な ARP パケットで、相手の IP アドレスではなく自身の IP アドレスをセットして問い合わせを行います。もし Gratuitous ARP に対して他の機器から応答があれば、その IP アドレスが重複していることがわかります。

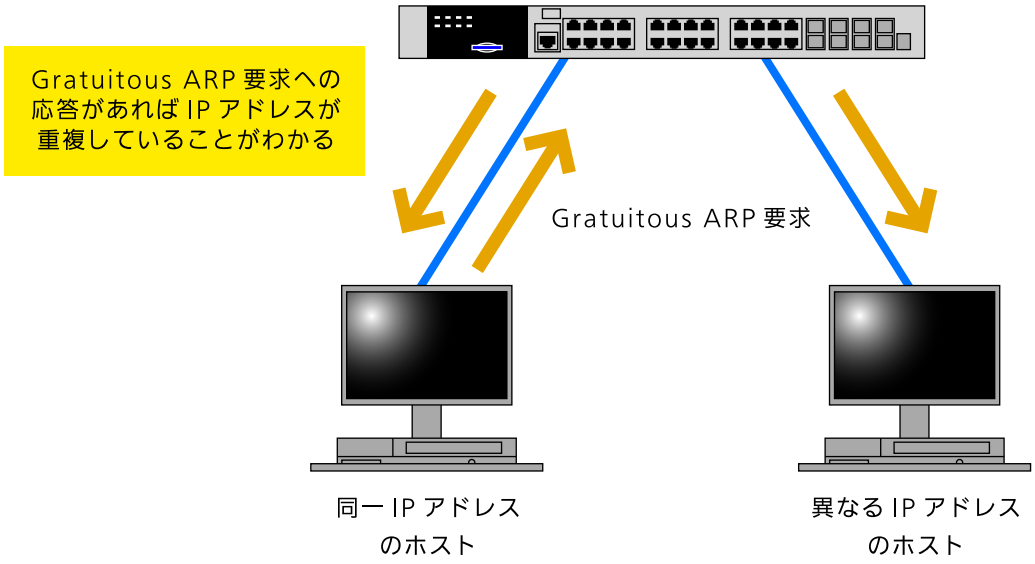


図 28-1　Gratuitous ARP の概略

enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)
disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)
config gratuitous_arp learning [enable | disable]
config gratuitous_arp send dup_ip_detected [enable | disable]
config gratuitous_arp send ipif_status_up [enable | disable]
config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>
show gratuitous_arp {ipif <ipif_name 12>}

28.1. enable gratuitous_arp

● 概要

このコマンドを用いて、Gratuitous ARP のトラップ状態およびログ状態を有効にします。スイッチでは IP 競合イベントのトラップ通知およびログ記録を介して、それらを管理者に通知できます。

● 構文

enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)

● パラメータ

ipif	（オプション）L3 インターフェースの名前を指定します。 <ipif_name 12> インターフェース名を指定します。最大文字数は 12 文字です。
trap	トラップを指定します。トラップは、デフォルトでは無効です。
log	ログを指定します。イベントログは、デフォルトでは有効です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

Gratuitous ARP を有効にするには：

```
Zxxx0:admin#enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

Zxxx0:admin#
```

28.2. disable gratuitous_arp

● 概要

このコマンドを用いて、Gratuitous ARP のトラップ状態およびログ状態を無効にします。

● 構文

disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)

● パラメータ

ipif	（オプション）L3 インターフェースの名前を指定します。 <ipif_name 12> インターフェース名を指定します。最大文字数は 12 文字です。
trap	トラップを指定します。トラップは、デフォルトでは無効です。
log	ログを指定します。イベントログは、デフォルトでは有効です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

Gratuitous ARP、トラップ、およびログ状態を無効にするには：

```
Zxxx0:admin#disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.

Zxxx0:admin#
```

28.3. config gratuitous_arp learning

● 概要

このコマンドを用いて、受信した Gratuitous ARP パケットに基づく ARP キャッシュの ARP エントリの学習を有効または無効にします。

● 構文

config gratuitous_arp learning [enable | disable]

● パラメータ

enable	受信した Gratuitous ARP パケットに基づく ARP エントリの学習を有効にします。
disable	受信した Gratuitous ARP パケットに基づく ARP エントリの学習を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

受信した Gratuitous ARP パケットに基づく ARP キャッシュの ARP エントリの認識を有効にするには：

```
Zxxx0:admin# config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

Zxxx0:admin#
```

28.4. config gratuitous_arp send dup_ip_detected

● 概要

このコマンドを用いて、重複する IP アドレスの検出時の Gratuitous ARP 要求の送信を有効または無効にします。デフォルトではこの状態は無効です。このコマンドにおいて、重複する IP の検出とは、システム自体の IP アドレスに一致する IP アドレスから送信された ARP 要求パケットをシステムで受信したことを意味します。この場合、システムでは、自身の IP アドレスと競合するアドレスが他の端末や装置で使用されていることを把握します。この IP アドレスの正しいホストを認識させる（返還要求する）ために、システムではこの重複 IP アドレスに対して Gratuitous ARP 要求パケットを送信することができます。

● 構文

config gratuitous_arp send dup_ip_detected [enable | disable]

● パラメータ

enable	重複 IP の検出時の Gratuitous ARP 要求パケットの送信を有効にします。
disable	重複 IP の検出時の Gratuitous ARP 要求パケットの送信を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

重複 IP アドレスの検出時の Gratuitous ARP 要求の送信を有効にするには：

```
Zxxx0:admin#config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.

Zxxx0:admin#
```

28.5. config gratuitous_arp send ipif_status_up

● 概要

このコマンドを用いて、IP インターフェースのステータス（リンク）アップ時の Gratuitous ARP 要求の送信を有効または無効にします。インターフェースの IP アドレスを他のノードに自動的に通知する場合に使用します。デフォルトではこの状態は無効です。状態が有効かつ、IP インターフェースがリンクアップしている場合、1 つの Gratuitous ARP パケットがブロードキャストされます。

● 構文

config gratuitous_arp send ipif_status_up [enable | disable]

● パラメータ

enable	IP インターフェースのステータスアップ時の Gratuitous ARP 要求パケットの送信を有効にします。
disable	IP インターフェースのステータスアップ時の Gratuitous ARP 要求パケットの送信を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP インターフェースのステータスアップ時の Gratuitous ARP 要求の送信を有効にするには：

```
Zxxx0:admin#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

Zxxx0:admin#
```

28.6. config gratuitous_arp send periodically ipif

● 概要

このコマンドを用いて、Gratuitous ARP 要求パケットの定期送信の間隔を設定します。

● 構文

config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>

● パラメータ

<ipif_name 12>	L3 インターフェースの名前を指定します。最大文字数は 12 文字です。
interval	Gratuitous ARP 定期送信の間隔を秒で指定します。 <value 0-65535> 値として 0 ～ 65535 を指定します。0（ゼロ）を指定すると、Gratuitous ARP 要求パケットは定期的に送信されません。デフォルトでは間隔は 0（ゼロ）です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP インターフェースの Gratuitous ARP 送信間隔を 5 に設定するには：

```
Zxxx0:admin#config gratuitous_arp send periodically ipif System interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

Zxxx0:admin#
```

28.7. show gratuitous_arp

● 概要

このコマンドを用いて、Gratuitous ARP 設定を表示します。

● 構文

show gratuitous_arp {ipif <ipif_name 12>}

● パラメータ

ipif	（オプション）L3 インターフェースの名前を指定します。 <ipif_name 12> インターフェース名を指定します。最大文字数は 12 文字です。

● 制限

なし

● 実行例

Gratuitous ARP のトラップ状態およびログ状態を表示するには：

```
Zxxx0:admin#show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF Status Up        : Disabled
Send on Duplicate IP Detected : Disabled
Gratuitous ARP Learning       : Disabled

IP Interface Name : System
        Gratuitous ARP Trap                     : Disabled
        Gratuitous ARP Log                      : Enabled
        Gratuitous ARP Periodical Send Interval : 0

Total Entries: 1

Zxxx0:admin#
```

29. IGMP Snooping コマンド

IGMP（Internet Group Management Protocol）は、マルチキャストグループを管理するプロトコルです。
IGMP snooping とは、スイッチの各ポートを流れる IGMP パケットを監視し、不要なポートにデータが流れないようにフィルタリングする機能です。このフィルタリング機能により、動画配信などの大容量データを効率良く処理できます。

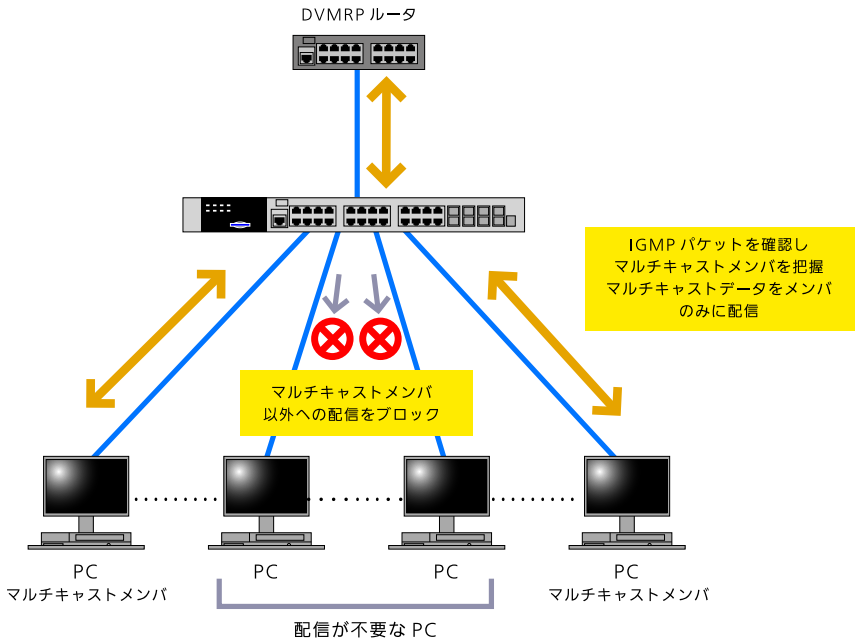


図 29-1　IGMP Snooping の概略

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | proxy_reporting {state [enable | disable] | source_ip <ipaddr>}(1)}
config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)
config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add |delete] <portlist>
config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
enable igmp_snooping
disable igmp_snooping
show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}}
config igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]
create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>
delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}
show igmp_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]
clear igmp_snooping statistics counter
show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
config igmp_snooping unknow_data_learning [all | vlan_name <vlan_name 32> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}
config igmp_snooping unknow_data_learning max_learned_entry <value 1-1024>
clear igmp_snooping data_learning_group [all | [vlan_name <vlan_name 32> | vlanid <vlanid_list>] [<ipaddr> | all]]

29.1. config igmp_snooping

● 概要

このコマンドを用いて、スイッチで IGMP snooping を設定します。

● 構文

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | proxy_reporting {state [enable | disable] | source_ip <ipaddr>}(1)}

● パラメータ

vlan_name	IGMP snooping を設定する VLAN の名前を指定します。 **<vlan_name 32>** VLAN 名を指定します。32 文字以内で設定します。
vlanid	VLAN ID リストを指定します。 **<vlanid_list>** VLAN ID リストを指定します。
all	すべての VLAN を設定するよう指定します。
state	選択した VLAN で IGMP snooping を有効または無効にします。 **enable** 選択した VLAN で IGMP snooping を有効にします。 **disable** 選択した VLAN で IGMP snooping を無効にします。
fast_leave	IGMP snooping 高速脱退機能を有効または無効にします。有効にした場合、システムで IGMP 脱退メッセージを受信すると、ただちにメンバを脱退させます。 **enable** IGMP snooping 高速脱退機能を有効にします。 **disable** IGMP snooping 高速脱退機能を無効にします。

proxy_reporting	プロキシレポートオプションを指定します。 state プロキシレポート状態を指定します。 enable プロキシレポートオプションを有効にします。 disable プロキシレポートオプションを無効にします。
source_ip	使用する送信元 IP アドレスを指定します。 <ipaddr> 使用する送信元 IP アドレスを入力します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IGMP snooping を設定するには：

```
Zxxx0:admin#config igmp_snooping vlan_name default state enable fast_leave enable
Command: config igmp_snooping vlan_name default state enable fast_leave enable

Success.

Zxxx0:admin#
```

29.2. config igmp_snooping querier

● 概要

このコマンドを用いて、IGMP snooping クエリアを設定します。

● 構文

config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>} (1)

● パラメータ

vlan_name	IGMP snooping クエリアを設定する VLAN の名前を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	VLAN ID リストを指定します。 <vlanid_list> VLAN ID リストを指定します。
all	すべての VLAN および VLAN ID を設定するよう指定します。

query_interval
通常のクエリの送信間隔を秒で指定します。
<sec 1-65535>
通常のクエリの送信間隔を秒で指定します。デフォルト設定は 125 秒です。

max_response_time
メンバからのレポートを待つ最大時間を秒で指定します。
<sec 1-25>
メンバからのレポートを待つ最大時間を秒で指定します。デフォルト設定は 10 秒です。

robustness_variable
サブネット上で予想されるパケットロスに対応するための微調整を行えるようになります。robustness_variable の値は、以下の IGMP メッセージ間隔を計算するために使用します。
・ グループメンバ間隔：マルチキャストルータが、ネットワークのグループにメンバがいないと判断するまでの時間です。この間隔は、次の式で計算します。

（robustness_variable× クエリ間隔）+（1× クエリ応答間隔）

・ 他のクエリア存在間隔：マルチキャストルータが、クエリアである他のマルチキャストルータが存在しないと判断するまでの時間です。この間隔は、次の式で計算します。

（robustness_variable× クエリ間隔）+（0.5× クエリ応答間隔）

・ 最終メンバクエリカウント：ルータが、グループにローカルメンバが存在しないとみなすまでに送信する Group-Specific Query 数です。初期値は、robustness_variable の値です。
<value 1-7>
値として 1 ～ 7 を指定します。サブネットでロスが多くなると予想される場合は、値を高くします。robustness_variable は、デフォルトで 2 に設定されています。

last_member_query_interval
Leave Group メッセージの応答として送信したものを含め、Group-Specific Query メッセージ送信の最大間隔を指定します。ルータで、グループの最終メンバのロスを検出するのに要する時間を短縮するには、この間隔を小さくします。
<sec 1-25>
時間として 1 ～ 25 秒を指定します。

state
有効にすると、スイッチを IGMP クエリア（IGMP クエリパケットを送信する）として選択できます。無効にすると、スイッチはクエリアの役割を担うことができません。スイッチに接続されたレイヤ 3 ルータで、IGMP プロキシ機能のみを提供し、マルチキャストルーティング機能を提供しない場合、この state を無効に設定する必要があります。レイヤ 3 ルータをクエリアとして選択しなかった場合、IGMP クエリパケットは送信されません。また、マルチキャストルーティングプロトコルパケットも送信しないため、ポートはルータポートとしてタイムアウトします。
enable
スイッチを IGMP クエリアとして選択できます（IGMP クエリパケットを送信する）。
disable
スイッチはクエリアとして動作しません。

version
このポートから送信される IGMP パケットのバージョンを指定します。インターフェースで受信する IGMP パケットのバージョンが、指定バージョンよりも高い場合、このパケットはルータのポートから転送されるか VLAN フラッディングが発生します。
<value 1-3>
値として 1 ～ 3 を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IGMP snooping クエリアを設定するには：

```
Zxxx0:admin#config igmp_snooping querier vlan_name default query_interval 125
state enable
Command: config igmp_snooping querier vlan_name default query_interval 125 state
enable

Success.

Zxxx0:admin#
```

29.3. config router_ports

● 概要

このコマンドを用いて、マルチキャスト対応ルータに接続されるポートの範囲を指定します。これにより、そうしたルータを宛先とするすべてのパケットは、プロトコルにかかわらず、マルチキャスト対応ルータに到達するようになります。

● 構文

config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

● パラメータ

<vlan_name 32>	ルータポートが存在する VLAN の名前を指定します。
vlanid	VLAN ID リストを指定します。 <vlanid_list> VLAN ID リストを指定します。
add	ルータポートを追加します。
delete	ルータポートを削除します。
<portlist>	設定するポート範囲を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スタティックルータポートを設定するには：

```
Zxxx0:admin#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

Zxxx0:admin#
```

29.4. config router_ports_forbidden

● 概要

このコマンドを用いて、マルチキャスト対応ルータに接続されないポートの範囲を指定します。これにより、禁止ルータポートからルーティングパケットを出力することはありません。

● 構文

config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

● パラメータ

<vlan_name 32>	ルータポートが存在する VLAN の名前を指定します。
vlanid	VLAN ID リストを指定します。 <vlanid_list> VLAN ID リストを指定します。
add	ルータポートを追加します。
delete	ルータポートを削除します。
<portlist>	設定するポート範囲を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート範囲 1 ～ 7 をデフォルト VLAN の禁止ルータポートとして設定するには :

```
Zxxx0:admin#config router_ports_forbidden default add 1-7
Command: config router_ports_forbidden default add 1-7

Success.

Zxxx0:admin#
```

29.5. enable igmp_snooping

● 概要

このコマンドは、本装置の IGMP snooping を有効にするために使用します。

● 構文

enable igmp_snooping

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

本装置の IGMP snooping を有効にするには：

```
Zxxx0:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

Zxxx0:admin#
```

29.6. disable igmp_snooping

● 概要

このコマンドを用いて、本装置の IGMP snooping を無効にします。IP マルチキャストルーティングを使用していない場合のみ、IGMP snooping を無効にできます。IGMP snooping を無効にすることで、任意の IP インターフェース内で、すべての IGMP および IP マルチキャストトラフィックのフラッディングを認証できます。

● 構文

disable igmp_snooping

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IGMP snooping を無効にするには：

```
Zxxx0:admin#disable igmp_snooping
Command: disable igmp_snooping

Success.

Zxxx0:admin#
```

29.7. show igmp_snooping

● 概要

このコマンドを用いて、スイッチでの現在の IGMP snooping 設定を表示します。

● 構文

show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

● パラメータ

vlan	（オプション）IGMP snooping 設定を表示する VLAN 名を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	（オプション）IGMP snooping 設定を表示する VLAN ID を指定します。 <vlanid_list> VLAN ID 範囲を指定します。

NOTE パラメータを指定しない場合、現在のすべての IGMP snooping 設定を表示します。

● 制限

なし

● 実行例

IGMP snooping を表示するには：

```
Zxxx0:admin#show igmp_snooping
Command: show igmp_snooping

 IGMP Snooping Global State              : Disabled
 Unknown Data Learning Max Entries       : 50

 VLAN Name                           : default
 Query Interval                      : 125
 Max Response Time                   : 10
 Robustness Value                    : 2
 Last Member Query Interval          : 1
 Querier State                       : Disabled
 Querier Role                        : Non-Querier
 Querier IP                          : 0.0.0.0
 Querier Expiry Time                 : 0 secs
 State                               : Enabled
 Fast Leave                          : Disabled
 Rate Limit                          : No Limitation
 Proxy Reporting                     : Disabled
 Proxy Reporting Source IP           : 0.0.0.0
 Version                             : 3
 Unknown Data Learning State         : Enabled
 Unknown Data Learning Aged Out      : Enabled
 Data Learning Group Expiry Time     : 260

Total Entries: 1

Zxxx0:admin#
```

29.8. show igmp_snooping group

● 概要

このコマンドを用いて、スイッチでの現在の IGMP snooping グループ設定を表示します。

● 構文

show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}}

● パラメータ

vlan	（オプション）IGMP snooping グループ設定情報を表示する VLAN 名を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	（オプション）IGMP snooping グループ設定情報を表示する VLAN ID を指定します。 <vlanid_list> VLAN ID リストを指定します。
ports	（オプション）IGMP snooping グループ情報を表示するポートのリストを指定します。 <portlist> 設定するポート範囲を指定します。

<ipaddr>（オプション）IGMP snooping グループ情報を表示するグループ IP アドレスを指定します。

NOTE パラメータを指定しない場合、スイッチの現在のすべての IGMP snooping グループ設定を表示します。

● 制限

なし

● 実行例

IGMP snooping グループを表示するには：

```
Zxxx0:admin#show igmp_snooping group
Command: show igmp_snooping group

 Source/Group    : NULL  / 224.106.0.211
 VLAN Name/VID   : default/1
 Member Ports    : 1
 UP Time         : 223
 Expiry Time     : 37
 Filter Mode     : EXCLUDE


 Source/Group    : NULL  / 234.54.163.75
 VLAN Name/VID   : default/1
 Member Ports    : 1
 UP Time         : 223
 Expiry Time     : 37
 Filter Mode     : EXCLUDE


 Source/Group    : 110.56.32.100 / 235.10.160.5
 VLAN Name/VID   : default/1
 Member Ports    : 2
 UP Time         : 221
 Expiry Time     : 0
 Filter Mode     : EXCLUDE


  Total Entries : 3

Zxxx0:admin#
```

29.9. config igmp_snooping rate_limit

● 概要

このコマンドを用いて、受信 IGMP 制御パケットの 1 秒あたりの上限値を設定します。

● 構文

config igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

● パラメータ

ports	設定するポート範囲を指定します。 <portlist> 設定するポート範囲を指定します。
vlanid	設定する VLAN 範囲を指定します。 <vlanid_list> VLAN ID リストを指定します。
<value 1-1000>	特定のポート /VLAN 上でスイッチが処理できる IGMP 制御パケットレートを指定します。レートは、1 秒あたりのパケット数で指定します。この制限レートを超過したパケットは破棄されます。
no_limit	デフォルト設定は制限なしです。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 2 に IGMP snooping レート制限なしを設定するには：

```
Zxxx0:admin#config igmp_snooping rate_limit ports 1-2 no_limit
Command: config igmp_snooping rate_limit ports 1-2 no_limit

Success.

Zxxx0:admin#
```

29.10. show igmp_snooping rate_limit

● 概要

このコマンドを用いて、IGMP snooping のレート制限の設定を表示します。

● 構文

show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

● パラメータ

ports	表示するポート範囲を指定します。 <portlist> 表示するポート範囲を指定します。
vlanid	表示する VLAN 範囲を指定します。 <vlanid_list> VLAN ID リストを指定します。

● 制限

なし

● 実行例

ポート 1 ～ 2 の IGMP snooping レート制限を表示するには：

```
Zxxx0:admin#show igmp_snooping rate_limit ports 1-2
Command: show igmp_snooping rate_limit ports 1-2

Port      Rate Limit
--------  ------------
1              No Limit
2              No Limit

Total Entries: 2
Zxxx0:admin#
```

29.11. create igmp_snooping static_group

● 概要

このコマンドを使用して、IGMP snooping スタティックグループを作成できます。スタティックグループには、メンバポートを追加できます。グループのメンバポートは、スタティックメンバポートおよびダイナミックメンバポートで構成されます。VLAN で IGMP snooping を有効にしたときのみ、スタティックグループが有効になります。それらのスタティックメンバポートについては、装置でクエリアに対して IGMP プロトコル動作をエミュレートし、マルチキャストグループを接続先とするトラフィックをメンバポートに転送する必要があります。
また、レイヤ 3 装置については、この特定グループを接続先とするパケットをスタティックメンバポートに送信することも必要です。スタティックメンバポートは、IGMP V2 動作にのみ影響します。予約済みの IP マルチキャストアドレス 224.0.0.X は、設定されたグループから除外する必要があります。先に VLAN を作成してから、スタティックグループを作成しなければなりません。

● 構文

create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

● パラメータ

vlan	ルータポートが存在する VLAN の名前を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	VLAN ID リストを指定します。 <vlanid_list> VLAN ID リストを指定します。
<ipaddr>	（レイヤ 3 スイッチ用の）マルチキャストグループ IP アドレスを指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

デフォルト VLAN のグループ 239.1.1.1 に IGMP snooping スタティックグループを作成するには:

```
Zxxx0:admin#create igmp_snooping static_group vlan default 239.1.1.1
Command: create igmp_snooping static_group vlan default 239.1.1.1

Success.

Zxxx0:admin#
```

29.12. config igmp_snooping static_group

● 概要

このコマンドを用いて、本装置で IGMP snooping スタティックグループを設定します。ポートがスタティックメンバポートとして設定されている場合、そのポートで IGMP プロトコルは動作しません。例えば、あるポートが IGMP から認識されたダイナミックメンバポートであると想定します。このポートを後でスタティックメンバポートとして設定すると、このポートで IGMP プロトコルは動作しなくなります。このポートをスタティックメンバポートから除外すると、IGMP プロトコル動作は再開します。スタティックメンバポートは、IGMP V2 動作にのみ影響します。

● 構文

config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>

● パラメータ

vlan	スタティックグループが存在する VLAN の名前を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	スタティックグループが存在する VLAN の ID を指定します。 <vlanid_list> VLAN ID リストを指定します。
<ipaddr>	（レイヤ 3 スイッチ用の）マルチキャストグループ IP アドレスを指定します。
add	メンバポートを追加します。
delete	メンバポートを削除します。
<portlist>	設定するポート範囲を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 9 ～ 10 を、デフォルト VLAN のグループ 239.1.1.1 の IGMP snooping スタティックメンバポートとして追加するには：

```
Zxxx0:admin#config igmp_snooping static_group vlan default 239.1.1.1 add 9-10
Command: config igmp_snooping static_group vlan default 239.1.1.1 add 9-10

Success.

Zxxx0:admin#
```

29.13. delete igmp_snooping static_group

● 概要

このコマンドを用いて、本装置の IGMP snooping スタティックグループを削除します。IGMP snooping スタティックグループを削除しても、グループの IGMP snooping ダイナミックメンバポートには影響しません。

● 構文

delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

● パラメータ

vlan	ルータポートが存在する VLAN の名前を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	ルータポートが存在する VLAN ID リストを指定します。 <vlanid_list> VLAN ID リストを指定します。
<ipaddr>	（レイヤ 3 スイッチ用の）マルチキャストグループ IP アドレスを指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

デフォルト VLAN のグループ 239.1.1.1 から IGMP snooping スタティックグループを削除するには:

```
Zxxx0:admin#delete igmp_snooping static_group vlan default 239.1.1.1
Command: delete igmp_snooping static_group vlan default 239.1.1.1

Success.

Zxxx0:admin#
```

29.14. show igmp_snooping static_group

● 概要

このコマンドを用いて、IGMP snooping スタティックマルチキャストグループを表示します。

● 構文

show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}

● パラメータ

vlan	ルータポートが存在する VLAN の名前を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	ルータポートが存在する VLAN ID リストを指定します。 <vlanid_list> VLAN ID リストを指定します。
<ipaddr>	（レイヤ 3 スイッチ用の）マルチキャストグループ IP アドレスを指定します。

● 制限

なし

● 実行例

すべての IGMP snooping スタティックグループを表示するには：

```
Zxxx0:admin#show igmp_snooping static_group
Command: show igmp_snooping static_group

VLAN ID/Name                              IP Address      Static Member Ports
----------------------------------------  --------------  --------------------
1/Default                                 239.1.1.1       9-10

Total Entries : 1

Zxxx0:admin#
```

29.15. show igmp_snooping statistic counter

● 概要

このコマンドを用いて、IGMP snooping を有効にした後に、本装置から送信または受信した IGMP プロトコルパケットの IGMP snooping 統計カウンタを表示します。

● 構文

show igmp_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]

● パラメータ

vlan	表示する VLAN を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	表示する VLAN のリストを指定します。 <vlanid_list> VLAN ID リストを指定します。
ports	表示するポートのリストを指定します。 <portlist> ポートのリストを指定します。

● 制限

なし

● 実行例

ポート 1 の IGMP snooping 統計カウンタを表示するには：

```
Zxxx0:admin#show igmp_snooping statistic counter ports 1
Command: show igmp_snooping statistic counter ports 1

Port #           : 1
-------------------------------------------------
Group Number     : 0

Receive Statistics
    Query
      IGMP v1 Query                  : 0
      IGMP v2 Query                  : 0
      IGMP v3 Query                  : 0
      Total                          : 0
      Dropped By Rate Limitation     : 0
     Dropped By Multicast VLAN       : 0

     Report & Leave
      IGMP v1 Report                  : 0
      IGMP v2 Report                  : 0
      IGMP v3 Report                  : 0
      IGMP v2 Leave                   : 0
      Total                           : 0
      Dropped By Rate Limitation       : 0
      Dropped By Max Group Limitation  : 0
      Dropped By Group Filter          : 0
      Dropped By Multicast VLAN        : 0

Transmit Statistics
    Query
      IGMP v1 Query                  : 0
      IGMP v2 Query                  : 0
      IGMP v3 Query                  : 8
      Total                          : 8

    Report & Leave
      IGMP v1 Report                 : 0
      IGMP v2 Report                 : 0
      IGMP v3 Report                 : 0
      IGMP v2 Leave                  : 0
      Total                          : 0

 Total Entries : 1
Zxxx0:admin#
```

29.16. clear igmp_snooping statistics counter

● 概要

このコマンドを用いて、本装置の IGMP snooping 統計カウンタをクリアします。

● 構文

clear igmp_snooping statistics counter

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IGMP snooping 統計カウンタをクリアするには：

```
Zxxx0:admin#clear igmp_snooping statistics counter
Command: clear igmp_snooping statistics counter

Success.

Zxxx0:admin#
```

29.17. show igmp_snooping forwarding

● 概要

このコマンドを用いて、本装置の現在の IGMP snooping フォワーディングテーブルを表示します。マルチキャストグループの具体的な送信元となるポートリストを簡単に確認できる方法が提供されます。パケットは、送信元 VLAN から送信され、フォワーディングポートに転送されます。

● 構文

show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

● パラメータ

vlan	（オプション）表示する VLAN を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。

vlanid	（オプション）表示する VLAN のリストを指定します。 <vlanid_list> VLAN ID リストを指定します。

NOTE パラメータを指定しない場合、本装置の現在のすべての IGMP snooping フォワーディングテーブルエントリを表示します。

● 制限

なし

● 実行例

本装置上に存在するすべての IGMP snooping フォワーディングエントリを表示するには：

```
Zxxx0:admin#show igmp_snooping forwarding
Command: show igmp_snooping forwarding

VLAN Name      : default
Source IP      : 10.90.90.114
Multicast Group: 225.0.0.0
Port Member    : 2,7

VLAN Name      : default
Source IP      : 10.90.90.10
Multicast Group: 225.0.0.1
Port Member    : 2,5

Total Entries : 2

Zxxx0:admin#
```

29.18. show router_ports

● 概要

このコマンドを用いて、本装置上の現在のルータポートを表示します。

● 構文

show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

● パラメータ

vlan	ルータポートが存在する VLAN の名前を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。

vlanid	ルータポートが存在する VLAN ID を指定します。 <vlanid_list> VLAN ID リストを指定します。 all すべての VLAN を表示します。
static	（オプション）スタティックに設定されたルータポートを表示します。
dynamic	（オプション）ダイナミックに登録されたルータポートを表示します。
forbidden	（オプション）スタティックに設定された禁止ルータポートを表示します。

NOTE パラメータを指定しない場合、本装置上の現在のすべてのルータポートを表示します。

● 制限

なし

● 実行例

デフォルト VLAN 上のルータポートを表示するには：

```
Zxxx0:admin#show router_ports vlan default
Command: show router_ports vlan default

VLAN Name                 : default
Static Router Port        :
Dynamic Router Port       :
Router IP                 :
Forbidden Router Port     :

Total Entries: 1

Zxxx0:admin#
```

29.19. config igmp_snooping unknow_data_learning

● 概要

このコマンドを用いて、unknow data learning の状態を指定します。
unknow data learning が対象の VLAN にて有効の場合は、IP マルチキャストパケットの受信により IGMP snooping グループが学習されます。無効の場合は IGMP メンバーシップレポートが受信された場合のみ IGMP snooping グループが学習されます。本機能で学習されたグループについては、エージアウトの有無を設定することができます。
unknow data learning が有効かつグループテーブルのエントリが上限に達していない場合は、マルチキャストフィルタリング設定に基づきマルチキャストパケットがルータポートへ転送されます。

NOTE unknow data learning グループ作成後に対象ポートが IGMP メンバーとなった場合は通常の IGMP グループのメンバーとして登録されます。

● 構文

config igmp_snooping unknow_data_learning [all | vlan_name <vlan_name 32> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}

● パラメータ

all	すべての VLAN を指定します。
vlan_name	VLAN 名を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	VLAN ID を指定します。 <vlanid_list> VLAN ID リストを指定します。
state	（オプション）unknow data learning の状態を指定します。 enable unknow data learning を有効にします。 disable unknow data learning を無効にします。
aged_out	（オプション）エントリのエージアウト処理の有無を指定します。 enable エントリのエージアウトを有効にします。 disable エントリのエージアウトを無効にします。

expiry_time
（オプション）unknow data learning グループの生存時間指定します。エージアウトが有効な場合のみ有効です。
<sec 1-65535>
1 ～ 65535 の値を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

default VLAN 上の IGMP snooping グループの unknow data learning を有効にするには：

```
Zxxx0:admin#config igmp_snooping unknow_data_learning vlan_name default state
enable aged_out enable expiry_time 260
Command: config igmp_snooping unknow_data_learning vlan_name default state enable
aged_out enable expiry_time 260

Success.

Zxxx0:admin#
```

29.20. config igmp_snooping unknow_data_learning max_learned_entry

● 概要

このコマンドを用いて、unknow data learning により学習可能なグループ数を指定します。
テーブルが上限に達した場合は、新規の unknow data learning グループ学習を停止します。本グループのトラフィックは、マルチキャストフィルタリング設定に基づき転送されます。

● 構文

config igmp_snooping unknow_data_learning max_learned_entry <value 1-512>

● パラメータ

<value 1-512>
unknown data learning による学習可能なグループの最大値。1 ～ 512 の値を指定します。工場出荷時は 64 です。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

unknow data learning による学習可能なグループの最大数を設定するには：

```
Zxxx0:admin#config igmp_snooping unknow_data_learning max_learned_entry 50
Command: config igmp_snooping unknow_data_learning max_learned_entry 50

Success.

Zxxx0:admin#
```

29.21. clear igmp_snooping data_learning_group

● 概要

このコマンドを用いて、unknow data learning で学習された IGMP snooping グループの削除を行います。

● 構文

clear igmp_snooping data_learning_group [all | [vlan_name <vlan_name 32> | vlanid <vlanid_list>] [<ipaddr> | all]]

● パラメータ

all	すべての unknow data learning グループを指定します。
vlan_name	VLAN 名を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	VLAN ID を指定します。 <vlanid_list> VLAN ID リストを指定します。
<ipaddr>	IGMP snooping グループの IP アドレスを指定します。
all	すべての IGMP snooping グループを指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

unknow data learning で学習されたグループを削除するには：

```
Zxxx0:admin#clear igmp_snooping data_learning_group all
Command: clear igmp_snooping data_learning_group all


Success.

Zxxx0:admin#
```

30. IP ルーティングコマンド

ここでは、本装置のデフォルトゲートウェイの登録を行います。IPv4、IPv6 それぞれの IP アドレスを対象にできます。

create iproute [default] <ipaddr>
delete iproute [default]
show iproute
create ipv6route [default] [<ipif_name 12> <ipv6addr>]
delete ipv6route [default] [<ipif_name 12> <ipv6addr>]
show ipv6route

30.1. create iproute

● 概要

このコマンドを用いて、本装置のデフォルトゲートウェイを指定します。

● 構文

create iproute [default] <ipaddr>

● パラメータ

default デフォルトゲートウェイを作成します。
<ipaddr> デフォルトゲートウェイの IP アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

デフォルトゲートウェイ 10.48.74.21 を追加するには：

```
Zxxx0:admin#create iproute default 10.48.74.121
Command: create iproute default 10.48.74.121

Success.

Zxxx0:admin#
```

30.2. delete iproute

● 概要

このコマンドを用いて、本装置のデフォルトゲートウェイを削除します。

● 構文

delete iproute [default]

● パラメータ

default	デフォルトの IP 経路エントリを削除します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

デフォルトゲートウェイを削除するには：

```
Zxxx0:admin#delete iproute default
Command: delete iproute default

Success.

Zxxx0:admin#
```

30.3. show iproute

● 概要

このコマンドを用いて、本装置のデフォルトゲートウェイの設定を表示します。

● 構文

show iproute

● パラメータ

なし

● 制限

なし

● 実行例

デフォルトゲートウェイの内容を表示するには：

```
Zxxx0:admin#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway          Interface     Protocol
------------------  ---------------  ------------  --------
10.0.0.0/8          0.0.0.0          System        Local


Total Entries : 1

Zxxx0:admin#
```

30.4. create ipv6route

● 概要

このコマンドを用いて、本装置に IPv6 デフォルトゲートウェイを設定します。ネクストホップがグローバルアドレスの場合は、インターフェース名を指定する必要はありません。ネクストホップがリンクローカルアドレスの場合は、インターフェース名を指定する必要があります。

● 構文

create ipv6route [default] [<ipif_name 12> <ipv6addr> |<ipv6addr>]

● パラメータ

default	デフォルトゲートウェイを指定します。
<ipif_name 12>	対象のインターフェースを指定します。
<ipv6addr>	デフォルトゲートウェイの IPv6 アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IPv6 デフォルトゲートウェイを作成するには：

```
Zxxx0:admin#create ipv6route default System FEC0::5
Command: create ipv6route default System FEC0::5

Success.

Zxxx0:admin#
```

30.5. delete ipv6route

● 概要

このコマンドを用いて、本装置の IPv6 デフォルトゲートウェイを削除します。ネクストホップがグローバルアドレスの場合は、インターフェース名を指定する必要はありません。ネクストホップがリンクローカルアドレスの場合は、インターフェース名を指定する必要があります。

● 構文

delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr>]

● パラメータ

default	デフォルトゲートウェイを指定します。
<ipif_name 12>	対象のインターフェースを指定します。
<ipv6addr>	デフォルトゲートウェイの IPv6 アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IPv6 デフォルトゲートウェイを削除するには：

```
Zxxx0:admin#delete ipv6route default System FEC0::5
Command: delete ipv6route default System FEC0::5

Success.

Zxxx0:admin#
```

30.6. show ipv6route

● 概要

このコマンドを用いて、本装置の IPv6 デフォルトゲートウェイを表示します。

● 構文

show ipv6route

● パラメータ

なし

● 制限

なし

● 実行例

IPv6 デフォルトゲートウェイを表示するには：

```
Zxxx0:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                              Protocol: Static  Metric: 1
Next Hop   : FEC0::5                           IPIF    : System


Total Entries: 1

Zxxx0:admin#
```

31.IP Source Address Verify コマンド

config ip_verify_source ports [<portlist>	all] state [enable	disable]
config arp_inspection ports [<portlist>	all] state [enable	disable]
create ip_source_binding ipaddress [<ipaddr> mac_address <macaddr> port <port>]
delete ip_source_binding [ipaddress <ipaddr> mac_address<macaddr>| all]
config ip_source_binding ipaddress [<ipaddr> mac_address <macaddr> port <port>]
show ip_source_binding [all	ipaddress <ipaddr> mac_address <macaddr>]
show ip_verify_source { ports {<portlist>} }
enable dhcp_snoop
disable dhcp_snoop
clear dhcp_snoop binding_entry ports [<portlist>|all]
show dhcp_snoop {[max_entry {ports <portlist>}	binding_entry {port <port>}]}
config dhcp_snoopmax_entry ports [<portlist>	all] limit [<value 1-n>	no_limit]
enable ip_verify_source log
disable ip_verify_source log

31.1. config ip_verify_source ports

● 概要

このコマンドを用いて、スイッチの IPSG のポート毎の状態を設定します。ポートがリンクアグリゲーションのグループメンバとして設定されている場合、IPSG 機能は有効にできません。ポートで IPSG が有効である場合、すべての IP パケットがチェックされます。正規の IP パケットは転送されるのに対して、不正な IP パケットは破棄されます。デフォルトでは、非 IP パケット（L2 パケットや ARP など）はすべて転送されます。

● 構文

config ip_verify_source ports [<portlist>| all] state [enable | disable]

● パラメータ

state	
	enable
	IPSG 機能を有効にします。正規の IP パケットは転送されるのに対して、不正な IP パケットは破棄されます。
	disable
	IPSG 機能を無効にします。デフォルト値は disable です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 で IPSG を有効にするには：

```
Zxxx0:admin#  config ip_verify_source ports 1 state enable
Command: config ip_verify_source ports 1 state enable

Success.

Zxxx0:admin#
```

31.2. config arp_inspection ports

● 概要

このコマンドを用いて、スイッチのダイナミック ARP 検査のポート毎の状態を設定します。ポートがリンクアグリゲーションのグループメンバとして設定されている場合、ダイナミック ARP 検査機能は有効にできません。ポートでダイナミック ARP 検査が有効である場合、このモードでは、すべての ARP パケットがチェックされます。このモードでは、正規の ARP パケットは転送されるのに対して、不正なパケットは破棄されます。

● 構文

config arp_inspection ports [<portlist>| all] state [enable | disable]

● パラメータ

state	
	enable
	ダイナミック ARP 検査機能を有効にします。正規の ARP パケットは転送されるのに対して、不正な ARP パケットは破棄されます。
	disable
	ダイナミック ARP 検査機能を無効にします。デフォルト値は disable です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 でダイナミック ARP 検査を有効にするには：

```
Zxxx0:admin#  config arp_inspection ports 1 state enable
Command: config arp_inspection ports 1 state enable

Success.

Zxxx0:admin#
```

31.3. create ip_source_binding

● 概要

このコマンドを用いて、IPSG エントリを作成します。1 つの MAC アドレスを複数の IP アドレスにマッピングできます。

● 構文

create ip_source_binding ipaddress <ipaddr> mac_address <macaddr> port <port>

● パラメータ

ipaddr	IPSG エントリに使用する IP アドレスを指定します。
macaddr	IPSG エントリに使用する MAC アドレスを指定します。
port	エントリを適用するポートを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 3 で IP アドレス 10.1.1.1 を MAC アドレス 00-00-00-00-00-11 にバインドする IPSG エントリを作成するには：

```
Zxxx0:admin#  create ip_source_binding ipaddress 10.1.1.1 mac_address 00-00-00-00-
00-11 port 3
Command: create ip_source_binding ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
port 3

Success

Zxxx0:admin#
```

31.4. delete ip_source_binding

● 概要

このコマンドを用いて、IPSG エントリを削除します。

● 構文

delete ip_source_binding [ipaddress <ipaddr> mac_address <macaddr>| all]

● パラメータ

ipaddr	エントリの IP アドレスを指定します。
macaddr	エントリの MAC アドレスを指定します。
all	IPSG のマニュアルバインディングエントリをすべて削除します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP アドレス 10.1.1.1.1 を MAC アドレス 00-00-00-00-00-11 にバインドする IPSG エントリを削除するには：

```
Zxxx0:admin#  delete ip_source_binding ipaddress 10.1.1.1 mac_address 00-00-00-00-
00-11
Command: delete ip_source_binding ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

Zxxx0:admin#
```

31.5. config ip_source_binding

● 概要

このコマンドを用いて、IPSG エントリを更新します。

● 構文

config ip_source_binding ipaddress <ipaddr> mac_address <macaddr> port <port>]

● パラメータ

ipaddr	更新するエントリの IP アドレスを指定します。
macaddr	更新するエントリの MAC アドレスを指定します。
ports	更新された IPSG エントリを使用するポートを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 10 で IP アドレス 10.1.1.1 を MAC アドレス 00-00-00-00-00-11 にバインドするよう IPSG エントリを設定するには：

```
Zxxx0:admin#  config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-
00-00-00-11 port 10
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-
00-11 port 10


Success.


Zxxx0:admin#
```

31.6. show ip_source_binding

● 概要

このコマンドを用いて、バインディングエントリを表示します。

● 構文

show ip_source_binding [all | ipaddress <ipaddr> mac_address <macaddr>]

● パラメータ

ipaddr	データベースのエントリの学習済み IP アドレスを指定します。
macaddr	エントリの MAC アドレスまたはブロックされている MAC アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

バインディングエントリを表示するには：
ハードウェア ACL がアクティブであるかどうかにかかわらず、ACL ステータスが表示されます。

```
Zxxx0:admin#  show ip_source_binding all
Command: show ip_source_binding all

M(Mode) - D:DHCP,S:Static    ACL - A:Active I:Inactive

IP Address                              MAC Address       M  ACL Port
--------------------------------------- ----------------- -- --  -----
10.1.1.1                                00-00-00-00-00-11 S  I   3
10.1.1.2                                00-00-00-00-00-12 S  A   1
10.1.1.10                               00-00-00-00-00-aa D  A   1

Total Entries : 3

Zxxx0:admin#
```

IP アドレスおよび MAC アドレスを指定してバインディングエントリを表示するには：

```
Zxxx0:admin#  show ip_source_binding ipaddress10.1.1.1 mac_address 00-00-00-00-00-
11
Command: show ip_source_binding ipaddress10.1.1.1 mac_address 00-00-00-00-00-11

M(Mode) - D:DHCP,S:Static   ACL - A:Active I:Inactive

IP Address                              MAC Address       M  ACL Port
--------------------------------------- ----------------- -- --  -----
10.1.1.1                                00-00-00-00-00-11 S  I   3

Total Entries : 1

Zxxx0:admin#
```

31.7. show ip_verify_source

● 概要

このコマンドを用いて、IP 送信元アドレス検証情報を表示します。

● 構文

show ip_verify_source { ports {<portlist>} }

● パラメータ

ports	情報を表示するポートを指定します。指定しない場合、すべてのポートが表示されます。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP 送信元アドレス検証のグローバル設定を表示するには：

```
Zxxx0:admin# show ip_verify_source
Command: show ip_verify_source

Log        : Enabled
DHCP Snoop : Disabled

Zxxx0:admin#
```

ポート毎の IP 送信元アドレス検証情報を表示するには：

```
Zxxx0:admin# show ip_verify_source ports
Command: show ip_verify_source ports

Port  ARP Inspection  IP Verify Source
----- --------------  ----------------
1     Disabled        Disabled
2     Enabled         Disabled
3     Enabled         Enabled
4     Disabled        Disabled
5     Disabled        Enabled
6     Disabled        Enabled
7     Disabled        Enabled
8     Disabled        Disabled
9     Disabled        Disabled
10    Disabled        Disabled
11    Disabled        Enabled
12    Disabled        Enabled

Zxxx0:admin#
```

31.8. enable dhcp_snoop

● 概要

このコマンドを用いて、DHCP Snooping を有効にします。デフォルトでは、DHCP Snooping は無効です。ユーザが DHCP Snooping を有効にした場合、スイッチは DHCP パケットから IP アドレスを学習して、IP ソースガードまたはダイナミック ARP 検査が有効になっているポートに対する DHCP バインディングエントリを作成します。

● 構文

enable dhcp_snoop

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DHCP Snooping モードを有効にするには：

```
Zxxx0:admin#  admin# enable dhcp_snoop
Command: enable dhcp_snoop

Success.

Zxxx0:admin#
```

31.9. disable dhcp_snoop

● 概要

このコマンドを用いて、DHCP Snooping を無効にします。
DHCP Snooping 機能が無効になると、DHCP Snooping のバインディングエントリはすべて削除されます。

● 構文

disable dhcp_snoop

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

DHCP Snooping モードを無効にするには：

```
Zxxx0:admin#  disable dhcp_snoop
Command: disable dhcp_snoop

Success.

Zxxx0:admin#
```

31.10. clear dhcp_snoop binding_entry

● 概要

このコマンドを用いて、指定したポートの学習済み DHCP Snooping エントリを消去します。

● 構文

clear dhcp_snoop binding_entry ports [<portlist>|all]

● パラメータ

ports	学習済み DHCP Snooping エントリの消去に使用するポートのリストを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 3 で DHCP Snooping エントリを消去するには：

```
Zxxx0:admin#  clear dhcp_snoop binding_entry ports 1-3
Command: clear dhcp_snoop binding_entry ports 1-3

Success.

Zxxx0:admin#
```

31.11. show dhcp_snoop

● 概要

このコマンドを用いて、DHCP Snooping 設定と学習データベースをすべて表示します。

● 構文

show dhcp_snoop {[max_entry {ports <portlist>} | binding_entry {port <port>}]}

● パラメータ

max_entry	ポートあたりの最大エントリ数を表示します。
binding_entry	ポートの DHCP Snooping のバインディングエントリを表示します。ポートを指定しなかった場合、すべてのバインディングエントリが表示されます。

パラメータを指定しない場合、すべての DHCP Snooping 設定が表示されます。

● 制限

このコマンドは、管理者、オペレータ、ユーザ、およびパワーユーザレベルのユーザのみ実行できます。

● 実行例

DHCP Snooping の状態を表示するには：

```
Zxxx0:admin#  show dhcp_snoop
Command: show dhcp_snoop

DHCP_Snoop : Enabled

Zxxx0:admin#
```

DHCP Snooping の最大エントリ設定を表示するには：

```
Zxxx0:admin#  show dhcp_snoop max_entry
Command: show dhcp_snoop max_entry

Port        Max Entry
--------------
1           10
2           10
3           10
4          No Limit
5          No Limit
6          No Limit
7          No Limit
8          No Limit
9          No Limit
10         No Limit
11         No Limit
12         No Limit

Zxxx0:admin#
```

DHCP Snooping のバインディングエントリを表示するには：

NOTE Inactive は、ポートのリンクダウンにより、エントリが現在、非アクティブであることを示します。

31.12. config dhcp_snoop max_entry

● 概要

このコマンドを用いて、特定のポートで学習できる最大エントリ数を指定します。デフォルトでは、ポートエントリの最大数は無制限です。このコマンドは、特定のポートで学習できる最大エントリ数を指定します。

● 構文

config dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-n> | no_limit]

● パラメータ

portlist	学習できる DHCP Snooping アドレスのバインディングエントリの最大数を制限する必要があるポートのリストを指定します。 all　スイッチのすべてのポートが使用されることを示します。
limit	 <value 1-n> 最大数を指定します。 no_limit 学習されるエントリの最大数が無制限であることを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 3 で学習できる DHCP Snooping エントリの最大数を 10 に設定するには：

```
Zxxx0:admin#  config dhcp_snoop max_entry ports 1-3 limit 10.
Command: config dhcp_snoop max_entry ports 1-3 limit 10.

Success.

Zxxx0:admin#
```

31.13. enable ip_verify_source log

● 概要

このコマンドを用いて、IP 送信元アドレス検証のログを有効にします。
このコマンドを用いて、IP 送信元アドレス検証モジュールが不正な IP アドレスおよび MAC アドレスを検出したときに、ログを生成します。

● 構文

enable ip_verify_source log

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP 送信元アドレス検証のログ機能を有効にするには：

```
Zxxx0:admin#  enable ip_verify_source log
Command: enable ip_verify_source log

Success.

Zxxx0:admin#
```

31.14. disable ip_verify_source log

● 概要

このコマンドを用いて、IP 送信元アドレス検証のログを無効にします。

● 構文

disable ip_verify_source log

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP 送信元アドレス検証のログを無効にするには：

```
Zxxx0:admin#  disable ip_verify_source log
Command: disable ip_verify_source log

Success.

Zxxx0:admin#
```

32. IPv6 NDP コマンド

IPv6 では、ルータに接続された機器のグローバル IP アドレスの設定に NDP（Neighbor Discovery Protocol）というプロトコルを利用します。ルータは、指定したインターフェースに RA（Router Advertisement）というパケットを定期的に送信します。RA パケットには、ネットワークプレフィックスや寿命などのパラメータが含まれており、RA パケットを受信した機器はネットワークプレフィックスと自身のリンクローカルアドレスとを組み合わせて、IPv6 アドレスを生成します。また、RA パケットの送信元をデフォルトルータとして扱います。アドレスが付与された機器の情報はルータの NDP テーブルに登録されます。

ここでは、NDP テーブルの表示／削除、項目の手動での登録を行います。また、RA の動作に関わるパラメータの設定を行います。

```
create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]
show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic |
    all] {hardware}
config ipv6 nd ns ipif <ipif_name 12> retrans_time <millisecond 0-4294967295>
config ipv6 nd ra ipif <ipif_name 12> {state [enable | disable] | life_time <sec 0-9000> |
    reachable_time <millisecond 0-3600000> | retrans_time <millisecond 0-4294967295> |
    hop_limit <value 0-255> | managed_flag [enable | disable] | other_config_flag [enable |
    disable] | min_rtr_adv_interval <sec 3-1350> | max_rtr_adv_interval <sec 4-1800>}(1)
config ipv6 nd ra prefix_option ipif <ipif_name 12> <ipv6networkaddr> {preferred_life_time <sec 0-
    4294967295> | valid_life_time <sec 0-4294967295> | on_link_flag [enable | disable] |
    autonomous_flag [enable | disable]}(1)
show ipv6 nd {ipif <ipif_name 12>}
```

32.1. create ipv6 neighbor_cache ipif

● 概要

このコマンドを用いて、IPv6 インターフェースにスタティックネイバー機器を追加します。

● 構文

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>

● パラメータ

<ipif_name 12>	インターフェース名を指定します。

<ipv6addr>	近傍の IP アドレスを指定します。
<macaddr>	近傍の MAC アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

NDP テーブルにスタティックエントリを追加するには：

```
Zxxx0:admin#create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05
Command: create ipv6 neighbor_cache ipif System 3FFC::1 00-01-02-03-04-05

Success.

Zxxx0:admin#
```

32.2. delete ipv6 neighbor_cache ipif

● 概要

このコマンドを用いて、アドレスキャッシュから近傍キャッシュエントリまたはスタティックネイバー機器キャッシュエントリを削除するか、この IP インターフェースのすべてのアドレスキャッシュエントリを削除します。スタティックおよびダイナミックのどちらのエントリも削除できます。

● 構文

delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]

● パラメータ

<ipif_name 12>	IPv6 インターフェース名を指定します。
all	すべての IPv6 インターフェースを指定します。
<ipv6addr>	近傍の IP アドレスを指定します。
static	IPv6 スタティックエントリを削除します。
dynamic	IPv6 ダイナミックエントリを削除します。
all	スタティックおよびダイナミックを含む、削除するすべての IPv6 エントリを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP インターフェース System 上の IPv6 アドレス 3ffc::1 に対する近傍キャッシュエントリを削除するには：

```
Zxxx0:admin#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

Zxxx0:admin#
```

32.3. show ipv6 neighbor_cache ipif

● 概要

このコマンドを用いて、指定したインターフェースの近傍キャッシュエントリを表示します。特定のエントリ、すべてのスタティックエントリ、すべてのダイナミックエントリ、またはすべてのエントリを表示できます。

● 構文

show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all] {hardware}

● パラメータ

<ipif_name 12>	IPv6 インターフェース名を指定します。
all	すべての IPv6 インターフェース名を指定します。
ipv6address	近傍の IPv6 アドレスを指定します。 <ipv6addr> IPv6 アドレスを指定します。
static	IPv6 スタティックネイバー機器キャッシュエントリを表示します。
dynamic	IPv6 ダイナミックエントリを表示します。
all	スタティックおよびダイナミックを含む、すべての IPv6 アドレスを表示します。
hardware	(オプション) ハードウェアテーブルに書き込まれたすべての近傍キャッシュエントリを表示します。

● 制限

なし

● 実行例

IP インターフェース System に対するすべての近傍キャッシュエントリを表示するには：

```
Zxxx0:admin#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

FE80::215:72FF:FE36:104                 State: Reachable
MAC Address : 00-15-72-36-01-04         Port : 1:21
Interface   : System                    VID  : 1

Total Entries: 1

Zxxx0:admin#
```

32.4. config ipv6 nd ns ipif

● 概要

このコマンドを用いて、指定したインターフェースの NS 再送時間を設定します。

● 構文

config ipv6 nd ns ipif <ipif_name 12> retrans_time <millisecond 0-4294967295>

● パラメータ

<ipif_name 12>	インターフェース名を指定します。最大文字数は 12 文字です。
retrans_time	ネイバー要請の再送タイマーをミリ秒で指定します。config ipv6 nd raコマンドのra retrans_time と同じ値を持ちます。一方を設定すると、もう一方も変更されます。
<millisecond 0-4294967295>	ネイバー要請の再送タイマーをミリ秒で指定します。config ipv6 nd ra コマンドの ra retrans_time と同じ値を持ちます。一方を設定すると、もう一方も変更されます。時間として 0 ～ 4294967295 ミリ秒を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

指定したインターフェースの NS 再送時間を設定するには：

```
Zxxx0:admin#config ipv6 nd ns ipif System retrans_time 400
Command: config ipv6 nd ns ipif System retrans_time 400

Success.

Zxxx0:admin#
```

32.5. config ipv6 nd ra ipif

● 概要

このコマンドを用いて、指定したインターフェースの RA パラメータを設定します。

● 構文

config ipv6 nd ra ipif <ipif_name 12> {state [enable | disable] | life_time <sec 0-9000> | reachable_time <millisecond 0-3600000> | retrans_time <millisecond 0-4294967295> | hop_limit <value 0-255> | managed_flag [enable | disable] | other_config_flag [enable | disable] | min_rtr_adv_interval <sec 3-1350> | max_rtr_adv_interval <sec 4-1800>}(1)

● パラメータ

<ipif_name 12>	インターフェース名を指定します。
state	ルータアドバタイズステータスを指定します。 enable ルータアドバタイズステータスを有効にします。 disable ルータアドバタイズステータスを無効にします。
life_time	デフォルトルータとしてのルータの有効期間を秒で指定します。 <sec 0-9000> 時間として 0 ～ 9000 秒を指定します。
reachable_time	到達可能性確認を受け取り後に、ノードで近傍ノードが到達可能であるとみなすことができる時間をミリ秒で指定します。 <millisecond 0-3600000> 時間として 0 ～ 3600000 ミリ秒を指定します。
retrans_time	ルータアドバタイズメッセージの再送およびルータアドバタイズパケットによってホストに到達する時間間隔をミリ秒で指定します。 <millisecond 0-4294967295> 時間として 0 ～ 4294967295 ミリ秒を指定します。
hop_limit	この RA メッセージを受け取るホストから送信されるパケットの IPv6 ヘッダのホップ制限フィールドの初期値を指定します。 <value 0-255> 値として 0 ～ 255 を指定します。
managed_flag	機能を有効または無効にします。 enable enable に設定した場合、この RA を受け取るホストでは、ステートレスアドレス設定から導き出したアドレスの他に、ステートフルアドレス設定プロトコルを使用してアドレスを取得しなければならないことを示します。 disable disable に設定した場合、RA を受け取るホストでは、ステートフルアドレス設定プロトコルを使用したアドレスの取得を停止します。

other_config_flag	機能を有効または無効にします。 enable enable に設定した場合、この RA を受け取るホストでは、ステートフルアドレス設定プロトコルを使用して on-address 設定情報を取得しなければならないことを示します。 disable disable に設定した場合、この RA を受け取るホストでは、ステートフルアドレス設定プロトコルを使用した on-address 設定情報の取得を停止します。
min_rtr_adv_interval	インターフェースからの非要請マルチキャストルータアドバタイズの最小送信間隔を秒で指定します。3 秒以上かつ .75 * MaxRtrAdvInterval 以内に設定する必要があります。デフォルトは 0.33 * MaxRtrAdvInterval です。 <sec 3-1350> 時間として 3 ～ 1350 秒を指定します。
max_rtr_adv_interval	インターフェースからの非要請マルチキャストルータアドバタイズの最大送信間隔を秒で指定します。4 秒以上かつ 1800 秒以内に設定する必要があります。デフォルトは 600 秒です。 <sec 4-1800> 時間として 4 ～ 1800 秒を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

RA 状態を有効にし、インターフェース tiberius の life_time を 1000 秒に設定するには：

```
Zxxx0:admin#config ipv6 nd ra ipif tiberius state enable life_time 1000
Command: config ipv6 nd ra ipif tiberius state enable life_time 1000

Success.

Zxxx0:admin#
```

32.6. config ipv6 nd ra prefix_option ipif

● 概要

このコマンドを用いて、ルータアドバタイズ機能のプレフィックスオプションを設定します。

● 構文

config ipv6 nd ra prefix_option ipif <ipif_name 12> <ipv6networkaddr> {preferred_life_time <sec 0-4294967295> | valid_life_time <sec 0-4294967295> | on_link_flag [enable | disable] | autonomous_flag [enable | disable]}(1)

● パラメータ

<ipif_name 12>
インターフェース名を指定します。最大文字数は 12 文字です。

<ipv6networkaddr>
IPv6 ネットワークアドレスを指定します。

preferred_life_time
ステートレスアドレス設定を用いた指定プレフィックスに基づくアドレスが推奨状態に維持される秒数を指定します。
<sec 0-4294967295>
時間として 0 ～ 4294967295 秒を指定します。値を 4294967295 に設定すると、有効期間は無制限になります。

valid_life_time
ステートレスアドレス設定を用いた指定プレフィックスに基づくアドレスが有効に維持される秒数を指定します。
<sec 0-4294967295>
時間として 0 ～ 4294967295 秒を指定します。値を 4294967295 に設定すると、有効期間は無制限になります。

on_link_flag
機能を有効または無効にします。
enable
このフィールドを enable に設定した場合、IPv6 パケット内において、ここで設定した IPv6 プレフィックスがこのリンクローカルネットワークに割り当てられることを示します。トラフィックがこの特定の IPv6 プレフィックスを持つノードに正しく送信されると、これらのノードはリンクローカルネットワーク上で到達可能であるとみなされます。
disable
disable に設定した場合、指定したプレフィックスで暗黙的に設定されるアドレスは、RA メッセージを受け取るリンクでは利用できません。

autonomous_flag
機能を有効または無効にします。
enable
このフィールドを enable に設定した場合、このプレフィックスを使用してリンクローカルネットワーク上の IPv6 アドレスを自動設定できることを示します。
disable
disable に設定した場合、指定したプレフィックスを使用して自律アドレス設定を作成できません。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

インターフェース ip1 のプレフィックスである 3ffe:501:ffff:100::/64 に対して、プレフィックスオプションの preferred_life_time 値として 1000 秒を設定するには：

```
Zxxx0:admin#config ipv6 nd ra prefix_option ipif ip1 3ffe:501:ffff:100::/64
preferred_life_time 1000
Command: config ipv6 nd ra prefix_option ipif ip1 3ffe:501:ffff:100::/64
preferred_life_time 1000

Success.

Zxxx0:admin#
```

32.7. show ipv6 nd

● 概要

このコマンドを用いて、IPv6 ND（Neighbor Discover）関連設定を表示します。

● 構文

show ipv6 nd {ipif <ipif_name 12>}

● パラメータ

ipif	（オプション）インターフェース名を指定します。
<ipif_name 12>	インターフェース名を指定します。最大文字数は 12 文字です。

NOTE IP インターフェースを指定しない場合、すべてのインターフェースの IPv6 ND 関連設定を表示します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IPv6 ND 関連設定を表示するには：

```
Zxxx0:admin#show ipv6 nd ipif System
Command: show ipv6 nd ipif System


Interface Name            : System
Hop Limit                 : 64
NS Retransmit Time        : 400 (ms)
Router Advertisement      : Disabled
RA Max Router AdvInterval : 600 (sec)
RA Min Router AdvInterval : 198 (sec)
RA Router Life Time       : 1800 (sec)
RA Reachable Time         : 1200000 (ms)
RA Retransmit Time        : 400 (ms)
RA Managed Flag           : Disabled
RA Other Configure Flag   : Disabled
Prefix                              Preferred  Valid      OnLink   Autonomous
1000:A111:B111:C111::/64            604800     2592000    Enabled  Enabled

Zxxx0:admin#
```

33.ジャンボフレームコマンド

Ethernet では、通信データを「フレーム」と呼ぶ一定サイズの単位に分割して送受信します。標準では、フレームサイズを 1518byte に固定していますが、このフレームサイズを大きくして、効率的にデータを送受信できるようにしたものが、ジャンボフレーム（Jumbo Frame）です。
本製品では、13000byte までのジャンボフレームに対応し、全ポート一括または各ポート個別に対応を設定できます。
ジャンボフレームで送受信を行うには、本製品を含め経路上のすべての機器がジャンボフレームに対応している必要があります。対応しない機器がある場合、標準のフレームサイズでの送受信となります。

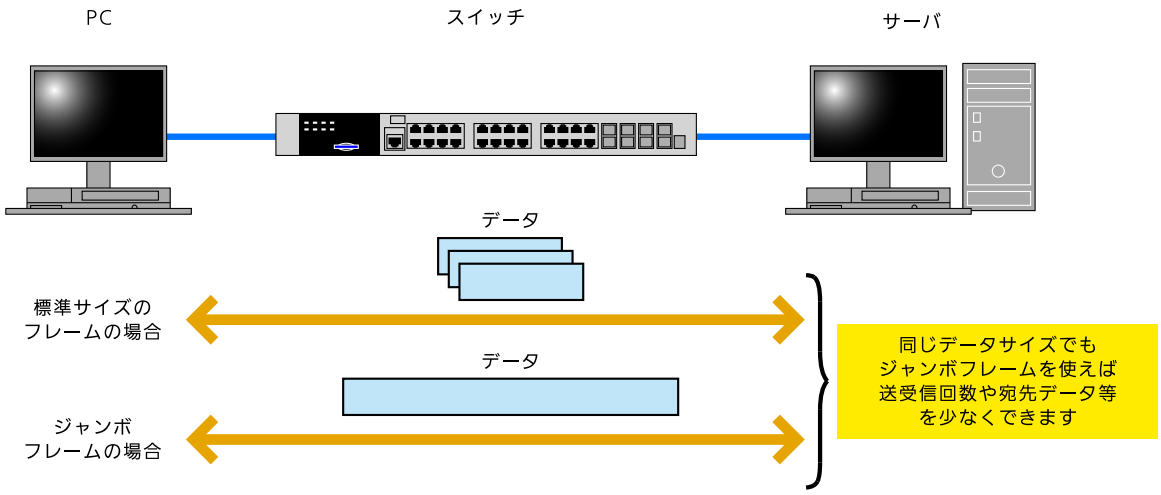


図 33-1　ジャンボフレーム概略

enable jumbo_frame
disable jumbo_frame
config jumbo_frame ports [<portlist> | all] state [enable | disable]
show jumbo_frame {<portlist>}

33.1. enable jumbo_frame

● 概要

このコマンドを用いて、ジャンボフレームのサポートを有効にします。

● 構文

enable jumbo_frame

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ジャンボフレームを有効にするには：

```
Zxxx0:admin#enable jumbo_frame
Command: enable jumbo_frame

Zxxx0:admin#
```

33.2. disable jumbo_frame

● 概要

このコマンドを用いて、ジャンボフレームのサポートを無効にします。

● 構文

disable jumbo_frame

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ジャンボフレームを無効にするには：

```
Zxxx0:admin#disable jumbo_frame
Command: disable jumbo_frame

Success.

Zxxx0:admin#
```

33.3. config jumbo_frame ports

● 概要

このコマンドを用いて、指定したポートでのジャンボフレームの状態を設定します。

● 構文

config jumbo_frame ports [<portlist> | all] state [enable | disable]

● パラメータ

<portlist>	この設定に使用するポートのリストを入力します。
all	この設定に、すべてのポートを使用します。
state	指定した範囲のポートに適用するジャンボフレームの状態を指定します。 enable　ジャンボフレームの状態を有効にします。 disable　ジャンボフレームの状態を無効にします。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1:1 ～ 1:5 でジャンボフレームを有効にするには：

```
Zxxx0:admin# config jumbo_frame ports 1:1-1:5 state enable
Command: config jumbo_frame ports 1:1-1:5 state enable

Success.

Zxxx0:admin#
```

33.4. show jumbo_frame

● 概要

このコマンドを用いて、ジャンボフレームの設定状態を表示します。

● 構文

show jumbo_frame {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートのリストを入力します。

● 制限

なし

● 実行例

ポート 1 ～ 5 のジャンボフレームの設定状態を表示するには：

```
Zxxx0:admin#show jumbo_frame 1-5
Command: show jumbo_frame 1-5

 Jumbo Frame Global State : Disabled

 Maximum Jumbo Frame Size : 1536 Bytes

 Port       Jumbo Frame State
 -------    --------------------
 1          Enabled
 2          Enabled
 3          Enabled
 4          Enabled
 5          Enabled

Zxxx0:admin#
```

34. LACP 設定コマンド

リンクアグリゲーションとは、2 つスイッチ間を複数のポートで接続し、それらを束ねて 1 つのポートとして扱う技術です。経路の冗長化、帯域幅の増強を行えます。

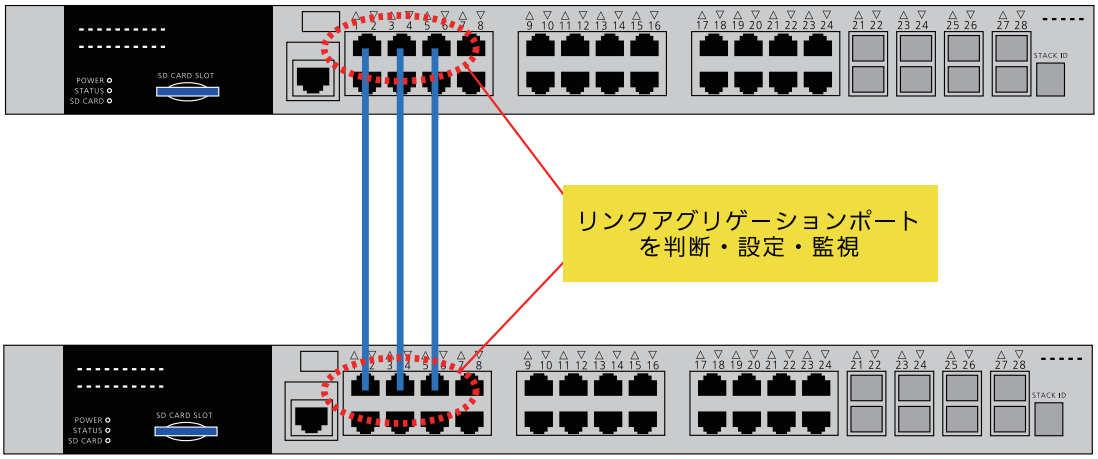


図 34-1　LACP の概略

LACP（Link Aggregate Control Protocol）は、リンクアグリゲーションおいて、ポートの接続状況の判断、設定、監視等を自動的に行うプロトコルです。
ポート毎に LACP 動作モードの設定を行う必要があります。

- Active：LACP フレームを送信するポート
- Passive：LACP フレームを受信するポート

> **NOTE**　リンクアグリゲーションの有効化等については、「Link Aggregation Commands」を参照してください。

config lacp_port <portlist> mode [active | passive]
show lacp_port {<portlist>}

34.1.　config lacp_port

● 概要

このコマンドを用いて、ポート毎に LACP モードを設定します。

● 構文

config lacp_port <portlist> mode [active | passive]

● パラメータ

<portlist>設定するポートの範囲を指定します。	
mode	ポートモードを指定します。
	active　モードを Active に指定します。
	passive　モードを Passive に指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 3 の LACP モードを設定するには：

```
Zxxx0:admin#config lacp_port 1-3 mode active
Command: config lacp_port 1-3 mode active

Success.

Zxxx0:admin#
```

34.2. show lacp_port

● 概要

このコマンドを用いて、ポート毎に LACP モードを表示します。

● 構文

show lacp_port {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

NOTE　パラメータを指定しない場合、すべてのポートの現在の LACP モードが表示されます。

● 制限

なし

● 実行例

スイッチのポート 1 ～ 3 の現在の LACP モードを表示するには：

```
Zxxx0:admin#show lacp_port 1-3
Command: show lacp_port 1-3

Port    Activity
------  --------
1       Active
2       Active
3       Active

Zxxx0:admin#
```

35. L2PT(Layer 2 Protocol Tunneling) コマンドリスト

L2PT とは、異なるネットワークへ STP や GVRP などの L2 プロトコルのフレーム転送を実現するための機能です。
ここでは、L2PT の設定を行います。

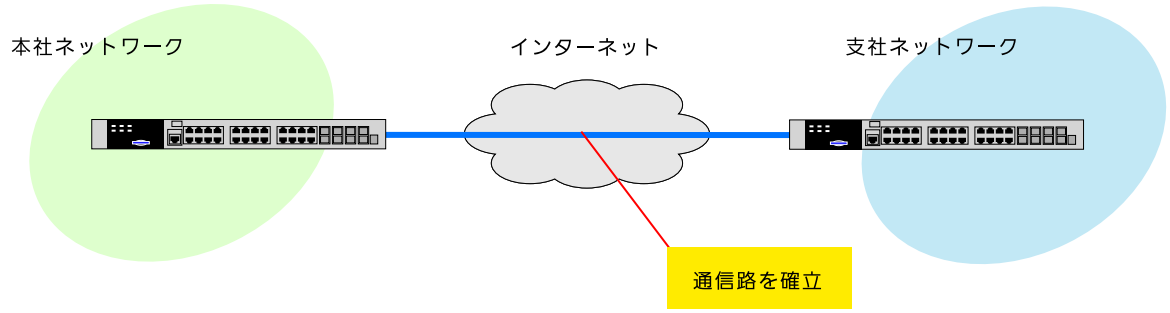


図 35-1　L2PT の概略

config l2protocol_tunnel ports [<portlist> | all] type [uni tunneled_protocol [{stp | gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]}(1) | all] {threshold <value 0-65535>} | nni | none]
show l2protocol_tunnel {[uni | nni]}
enable l2protocol_tunnel
disable l2protocol_tunnel

35.1. config l2protocol_tunnel ports

● 概要

このコマンドを用いて、ポートで L2PT を設定します。
L2PT を使用して、レイヤ 2 プロトコルパケットをトンネリングします。
UNI でレイヤ 2 プロトコルのトンネリングを有効にした場合、このポートで PDU を受け取ると、PDU のマルチキャスト宛先アドレスが L2PT マルチキャストアドレスで置き換えられます。L2PT マルチキャストアドレスは、STP の場合は 01-05-5D-00-00-00、GVRP の場合は 01-05-5D-00-00-21、レイヤ 2 プロトコル MAC 01-00-0C-CC-CC-CC の場合は 01-05-5D-00-00-10、プロトコル MAC 01-00-0C-CC-CC-CD の場合は 01-05-5D-00-00-11 となります。

● 構文

config l2protocol_tunnel ports [<portlist> | all] type [uni tunneled_protocol [{stp | gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]}(1) | all] {threshold <value 0-65535>} | nni | none]

● パラメータ

ports	L2PT を設定するポートを指定します。 <portlist> 設定するポートのリストを入力します。 all この設定をすべてのポートで使用します。
type	ポートのタイプを指定します。
uni	ポートが UNI ポートであることを指定します。
tunneled_protocol	この UNI ポートでトンネリングを有効にするプロトコルを指定します。all を指定した場合、このポートでは、トンネリングに対応するすべてのレイヤ 2 プロトコルがトンネリングされます。 stp （オプション）STP プロトコルの使用を指定します。 gvrp （オプション）GVRP プロトコルの使用を指定します。 protocol_mac （オプション）使用するプロトコル MAC アドレスを指定します。 01-00-0C-CC-CC-CCこのプロトコル MAC アドレスの使用を指定します。 01-00-0C-CC-CC-CDこのプロトコル MAC アドレスの使用を指定します。
all	すべての MAC アドレスを使用します。
threshold	（オプション）この UNI ポートで受け入れる 1 秒あたりのパケット数の破棄しきい値を指定します。プロトコルのしきい値を超過した場合、ポートでは PDU を破棄します。しきい値の範囲は 0 ～ 65535（パケット / 秒）です。値 0 を指定した場合、すべて認証されます。デフォルトでは、値は 0 に設定されます。 <value 0-65535> 1 秒あたりのパケット数のしきい値を入力します。この値は、0 ～ 65535 の範囲で指定します。
nni	ポートが NNI ポートであることを指定します。
none	そのポートでのトンネルを無効にします。デフォルトでは、ポートは none に設定されます。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 4 で STP トンネリングを設定するには：

```
Zxxx0:admin# config l2protocol_tunnel ports 1-4 type uni tunneled_protocol stp
Command: config l2protocol_tunnel ports 1-4 type uni tunneled_protocol stp

Success.

Zxxx0:admin#
```

35.2. show l2protocol_tunnel

● 概要

このコマンドを用いて、L2PT 情報を表示します。

● 構文

show l2protocol_tunnel {[uni | nni]}

● パラメータ

uni	（オプション）トンネリングおよび破棄された PDU 統計を含む、UNI 詳細情報を表示します。
nni	（オプション）カプセル化解除されたレイヤ 2 PDU 統計を含む、NNI 詳細情報を表示します。

● 制限

なし

● 実行例

L2PT の要約情報を表示するには：

```
Zxxx0:admin# show l2protocol_tunnel
Command: show l2protocol_tunnel

Global State: Enabled
UNI Ports: 1-2
NNI Ports: 3-4

Zxxx0:admin#
```

UNI ポートの L2PT 詳細情報を表示するには：

```
Zxxx0:admin# show l2protocol_tunnel uni
Command: show l2protocol_tunnel uni

 UNI   Tunneled           Threshold
 Port  Protocol           (packet/sec)
 ----  -----------------  ------------
 1:1   STP                10
       GVRP               10
       01-00-0C-CC-CC-CC  10
 1:2   STP                20
       GVRP               20
       01-00-0C-CC-CC-CC  20
 1:3   STP                0
 1:4   STP                0

Zxxx0:admin#
```

NNI ポートの L2PT 詳細情報を表示するには：

```
Zxxx0:admin# show l2protocol_tunnel nni
Command: show l2protocol_tunnel nni

NNI     Protocol
Port
----   --------------------
1       STP
        GVRP
        01-00-0C-CC-CC-CC
        01-00-0C-CC-CC-CD
2       STP
        GVRP
        01-00-0C-CC-CC-CC
        01-00-0C-CC-CC-CD

Zxxx0:admin#
```

35.3. enable l2protocol_tunnel

● 概要

このコマンドを用いて、L2PT 機能を有効にします。

● 構文

enable l2protocol_tunnel

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

L2PT 機能を有効にするには：

```
Zxxx0:admin# enable l2protocol_tunnel
Command: enable l2protocol_tunnel

Success.

Zxxx0:admin#
```

35.4. disable l2protocol_tunnel

● 概要

このコマンドを用いて、L2PT 機能を無効にします。

● 構文

disable l2protocol_tunnel

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

L2PT 機能を無効にするには：

```
Zxxx0:admin# disable l2protocol_tunnel
Command: disable l2protocol_tunnel

Success.

Zxxx0:admin#
```

36. マルチキャスト IP アドレス制限コマンド

IGMP/MLD snooping やレイヤ 3 機能の対象外とするマルチキャストパケットのフィルタリングを設定します。

create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-60> profile_name <name 32>
config mcast_filter_profile [profile_id <value 1-60> | profile_name <name 32>] {profile_name <name 32> | [add | delete] <mcast_address_list>}(1)
config mcast_filter_profile ipv6 [profile_id <value 1-60> | profile_name <name 32>] {profile_name <name 32> | [add | delete] <mcastv6_address_list>}(1)
delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-60> | all] | profile_name <name 32>]
show mcast_filter_profile {[ipv4 | ipv6]} {[profile_id <value 1-60> | profile_name <name 32>]}
config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {[add | delete] [profile_id <value 1-60> | profile_name <name 32>] | access [permit | deny]}(1)
show limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
config max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {max_group [<value 1-1024> | infinite] | action [drop | replace]} (1)
show max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}

36.1. create mcast_filter_profile

● 概要

このコマンドを用いて、マルチキャストアドレスプロファイルを作成します。IPv4 または IPv6 オプションを指定しない場合、暗黙的に IPv4 が選択されます。

● 構文

create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-60> profile_name <name 32>

● パラメータ

ipv4	（オプション）IPv4 マルチキャストプロファイルを追加します。
ipv6	（オプション）IPv6 マルチキャストプロファイルを追加します。
profile_id	プロファイルの ID を指定します。 **<value 1-60>** プロファイル ID は 1 ～ 60 の範囲で指定する必要があります。
profile_name	プロファイルの内容がわかりやすい名前を指定します。 **<name 32>** プロファイル名は 32 文字までです。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MOD という名前のマルチキャストアドレスプロファイルを作成するには：

```
Zxxx0:admin#create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

Zxxx0:admin#
```

36.2. config mcast_filter_profile

● 概要

このコマンドを用いて、プロファイル名の変更、以前に定義したマルチキャスト IP アドレスのプロファイルへの追加またはプロファイルからの削除を行います。

● 構文

config mcast_filter_profile [profile_id <value 1-60> | profile_name <name 32>]
{profile_name <name 32> | [add | delete] <mcast_address_list>}(1)

● パラメータ

profile_id	プロファイルの ID を指定します。 <value 1-60> プロファイル ID が 1 ～ 60 の必要があります。
profile_name	プロファイルの名前を指定します。 <name 32> プロファイル名は 32 文字までです。
profile_name	プロファイルの新しい名前を指定します。 <name 32> プロファイル名は 32 文字までです。 add マルチキャスト IP アドレスの範囲を追加します。 delete マルチキャスト IP アドレスの範囲を削除します。 <mcast_address_list> プロファイルに追加または削除するマルチキャストアドレスのリストです。1 つのマルチキャスト IP アドレスを指定するか、ハイフンを用いてマルチキャストアドレスの範囲を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

プロファイルにマルチキャストアドレスの範囲を追加するには：

```
Zxxx0:admin#config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.100
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.100

Success.

Zxxx0:admin#
```

36.3. config mcast_filter_profile ipv6

● 概要

このコマンドを用いて、以前に定義した IPv6 マルチキャスト IP アドレスの範囲をプロファイルに追加するか、プロファイルから削除します。

● 構文

config mcast_filter_profile ipv6 [profile_id <value 1-60> | profile_name <name 32>] {profile_name <name 32> | [add | delete] <mcastv6_address_list>}(1)

● パラメータ

profile_id	プロファイルの ID を指定します。 <value 1-60> プロファイル ID が 1 ～ 60 の必要があります。
profile_name	プロファイルの名前を指定します。 <name 32> プロファイル名は 32 文字までです。
profile_name	プロファイルの新しい名前を指定します。 <name 32> プロファイル名は 32 文字までです。 add マルチキャスト IP アドレスの範囲を追加します。 delete マルチキャスト IP アドレスの範囲を削除します。 <mcastv6_address_list> プロファイルに追加または削除する IPv6 マルチキャストアドレスのリストです。1 つの IPv6 マルチキャスト IP アドレスを指定するか、ハイフンを用いて IPv6 マルチキャストアドレスの範囲を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

プロファイル ID 3 に、IPv6 マルチキャストアドレスの範囲 FF0E::100:0:0:20 - FF0E::100:0:0:22 を追加するには：

```
Zxxx0:admin#config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20 -
FF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20 -
FF0E::100:0:0:22


Success.


Zxxx0:admin#
```

36.4. delete mcast_filter_profile

● 概要

このコマンドを用いて、マルチキャストアドレスプロファイルを削除します。IPv4 または IPv6 オプションを指定しない場合、暗黙的に IPv4 が選択されます。

● 構文

delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-60> | all] | profile_name <name 32>]

● パラメータ

ipv4	（オプション）IPv4 マルチキャストプロファイルを削除します。
ipv6	（オプション）IPv6 マルチキャストプロファイルを削除します。
profile_id	プロファイルの ID を指定します。範囲は 1 ～ 60 です。 <value 1-60> プロファイル ID が 1 ～ 60 の必要があります。
all	すべてのマルチキャストアドレスプロファイルが削除されます。
profile_name	プロファイル名に基づいてプロファイルを指定します。 <name 32> プロファイル名は 32 文字までです。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

プロファイル ID が 3 のマルチキャストプロファイルを削除するには：

```
Zxxx0:admin#delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id 3

Success.

Zxxx0:admin#
```

プロファイル名が MOD のマルチキャストプロファイルを削除するには：

```
Zxxx0:admin#delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Success.

Zxxx0:admin#
```

36.5. show mcast_filter_profile

● 概要

このコマンドを用いて、定義されたマルチキャストアドレスプロファイルを表示します。IPv4 または IPv6 オプションを指定しない場合、暗黙的に IPv4 が選択されます。

● 構文

show mcast_filter_profile {[ipv4 | ipv6]} {[profile_id <value 1-60> | profile_name <name 32>]}

● パラメータ

ipv4	（オプション）IPv4 マルチキャストプロファイルを表示します。
ipv6	（オプション）IPv6 マルチキャストプロファイルを表示します。
profile_id	（オプション）プロファイルの ID を指定します。profile_id と profile_name の両方を指定しない場合、すべてのプロファイルが表示されます。 <value 1-60> プロファイル ID が 1 ～ 60 の必要があります。
profile_name	（オプション）プロファイル名に基づいてプロファイルを表示します。profile_id と profile_name の両方を指定しない場合、すべてのプロファイルが表示されます。 <name 32> プロファイル名は 32 文字までです。

● 制限

なし

● 実行例

定義されているすべてのマルチキャストアドレスプロファイルを表示するには：

```
Zxxx0:admin#show mcast_filter_profile
Command: show mcast_filter_profile

Profile ID Name                        Multicast Addresses
---------- --------------------------- ------------------------------
1          MOD                         234.1.1.1 - 238.244.244.244
                                       234.1.1.1 - 238.244.244.244
2          customer                    224.19.62.34 - 224.19.162.200

Total Entries: 2

Zxxx0:admin#
```

36.6. config limited_multicast_addr

● 概要

このコマンドを用いて、ポートまたは VLAN のマルチキャストアドレスのフィルタリング機能を設定します。ポートまたは VLAN に対してプロファイルを指定していない場合、この限定機能は有効になりません。ポートまたは VLAN にこの機能が設定されている場合、IGMP/MLD snooping 機能およびレイヤ 3 機能により動作するマルチキャストグループが限定されます。IPv4 または IPv6 オプションを指定しない場合、暗黙的に IPv4 が選択されます。

● 構文

config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {[add | delete] [profile_id <value 1-60> | profile_name <name 32>] | access [permit | deny]}(1)

● パラメータ

ports	マルチキャストアドレスのフィルタリング機能を設定するポートの範囲を指定します。 <portlist> 設定するポートの範囲を指定します。
vlanid	マルチキャストアドレスのフィルタリング機能を設定する VLAN の VLAN ID を指定します。 <vlanid_list> マルチキャストアドレスのフィルタリング機能を設定する VLAN の VLAN ID を入力します。
ipv4	（オプション）IPv4 マルチキャストプロファイルを指定します。
ipv6	（オプション）IPv6 マルチキャストプロファイルを指定します。
add	（オプション）ポートまたは VLAN にマルチキャストアドレスプロファイルを追加します。
delete	（オプション）ポートまたは VLAN からマルチキャストアドレスプロファイルを削除します。
profile_id	（オプション）ポートまたは VLAN に対して追加または削除するプロファイル ID を指定します。 <value 1-60> プロファイル ID が 1 ～ 60 の必要があります。
profile_name	（オプション）ポートまたは VLAN に対して追加または削除するプロファイル名を指定します。 <name 32> プロファイル名は 32 文字までです。

access	（オプション）アクセスを認証するか拒否するかを指定します。 permit プロファイルで定義されたアドレスに一致するパケットが認証されます。 deny プロファイルで定義されたアドレスに一致するパケットが拒否されます。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 と 3 にマルチキャストアドレスプロファイル 2 を追加するには：

```
Zxxx0:admin#config limited_multicast_addr ports 1,3 add profile_id 2
Command: config limited_multicast_addr ports 1,3 add profile_id 2

Success.

Zxxx0:admin#
```

36.7. show limited_multicast_addr

● 概要

このコマンドを用いて、ポート別または VLAN 別にマルチキャストアドレスの範囲を表示します。ポートまたは VLAN にこの機能が設定されている場合、IGMP/MLD snooping 機能およびレイヤ 3 機能により動作するマルチキャストグループが限定されます。IPv4 または IPv6 オプションを指定しない場合、暗黙的に IPv4 が選択されます。

● 構文

show limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}

● パラメータ

ports	マルチキャストアドレス制限設定を表示するポートの範囲を指定します。 <portlist> 表示するポートの範囲を指定します。
vlanid	マルチキャストアドレスのフィルタリング機能に関する情報を表示する必要がある VLAN の VLAN ID を指定します。 <vlanid_list> VLAN の VLAN ID を入力します。
ipv4	（オプション）ポートまたはVLANに関連付けられたIPv4マルチキャストプロファイルを表示します。
ipv6	（オプション）ポートまたはVLANに関連付けられたIPv6マルチキャストプロファイルを表示します。

● 制限

なし

● 実行例

VLAN 1 のマルチキャストアドレス制限範囲を表示するには：

```
Zxxx0:admin#show limited_multicast_addr vlanid 1
Command: show limited_multicast_addr vlanid 1

VLAN    : 1
Access  : Deny

Profile ID      Name                Multicast Addresses
-----------    -----------          ----------------------------
1              customer             224.19.62.34 - 224.19.162.200

Zxxx0:admin#
```

ポート 1 と 3 のマルチキャストアドレス制限範囲を表示するには：

```
Zxxx0:admin#show limited_multicast_addr ports 1,3
Command: show limited_multicast_addr ports 1,3

Port    : 1
Access  : Deny

Profile ID      Name                Multicast Addresses
-----------    -----------          ----------------------------
1              customer             224.19.62.34 - 224.19.162.200


Port    : 3
Access  : Deny

Profile ID      Name                Multicast Addresses
-----------    ----------------     ----------------------------
1              customer             224.19.62.34 - 224.19.162.200


Zxxx0:admin#
```

36.8. config max_mcast_group

● 概要

このコマンドを用いて、ポートまたは VLAN が参加できるマルチキャストグループの最大数を設定します。IPv4 または IPv6 オプションを指定しない場合、暗黙的に IPv4 が選択されます。ポートまたは VLAN が参加するグループが最大数に達した場合、動作が drop に指定されているときは新しく学習されたグループが破棄されます。動作が replace に指定されているときは、新しく学習されたグループが最も古いグループと置き換えられます。

● 構文

config max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {max_group [<value 1-1024> | infinite] | action [drop | replace]} (1)

● パラメータ

ports	最大マルチキャストグループを設定するポートの範囲を指定します。 <portlist> 設定するポートの範囲を指定します。
vlanid	最大マルチキャストグループを設定する VLAN ID を指定します。 <vlanid_list> VLAN の VLAN ID を入力します。
ipv4	（オプション）学習された IPv4 アドレスの最大数を限定します。
ipv6	（オプション）学習された IPv6 アドレスの最大数を限定します。
max_group	（オプション）マルチキャストグループの最大数を指定します。 <value 1-1024> 範囲は 1 ～ 1024 または無限です。 infinite infinite がデフォルト設定です。
action	（オプション）レジスタが一杯になったときに、新しく学習されたグループを処理する動作を指定します。 drop 新しいグループが破棄されます。 replace 新しいグループがレジスタテーブルの最も古いグループと置き換わります。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 と 3 が参加できるマルチキャストグループの最大数を 100 に設定するには：

```
Zxxx0:admin# config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

Zxxx0:admin#
```

36.9. show max_mcast_group

● 概要

このコマンドを用いて、ポートまたは VLAN が参加できるマルチキャストグループの最大数を表示します。IPv4 または IPv6 オプションを指定しない場合、暗黙的に IPv4 が選択されます。

● 構文

show max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}

● パラメータ

ports	マルチキャストグループの最大数を表示するポートの範囲を指定します。 <portlist> 表示するポートの範囲を指定します。
vlanid	マルチキャストグループの最大数を表示する VLAN ID を指定します。 <vlanid_list> VLAN の VLAN ID を入力します。
ipv4	（オプション）認識された IPv4 アドレスの最大数を表示します。
ipv6	（オプション）認識された IPv6 アドレスの最大数を表示します。

● 制限

なし

● 実行例

ポート 1 ～ 2 のマルチキャストグループの最大数を表示するには：

```
Zxxx0:admin# show max_mcast_group ports 1-2
Command: show max_mcast_group ports 1-2

Port     Max Multicast Group Number  Action
-----    --------------------------- ---------
1        Infinite                     Drop
2        Infinite                     Drop

Total Entries : 2
Zxxx0:admin#
```

37. リンクアグリゲーションコマンド

リンクアグリゲーションとは、2 つスイッチ間を複数のポートで接続し、それらを束ねて 1 つのポートとして扱う技術です。経路の冗長化、帯域幅の増強を行えます。束ねたポートに対する通信の振り分けは、複数の方式から選択することができます。

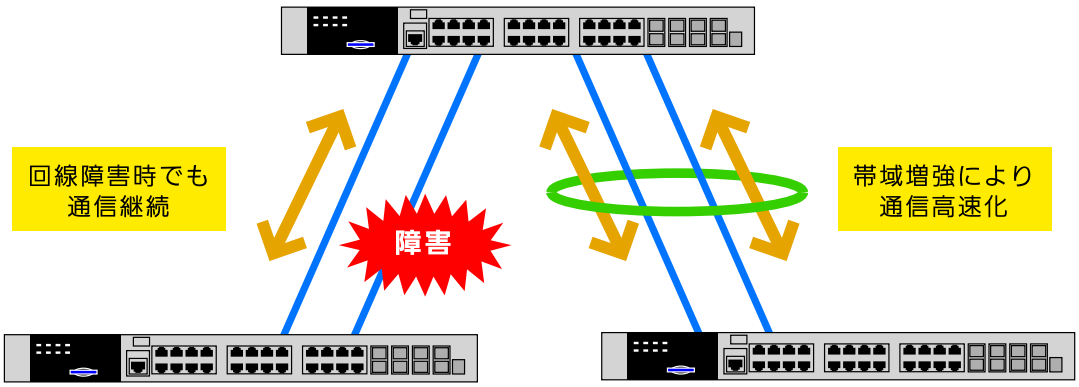


図 37-1　リンクアグリゲーションの概略

NOTE　リンクアグリゲーションの設定／監視等を自動で行う LACP プロトコルを利用する場合は、ここで LACP の使用を有効にするとともに、「LACP Configuration Commands」を参照してプロトコルの設定を行います。

```
create link_aggregation group_id <value 1-32> {type [lacp | static]}
delete link_aggregation group_id <value 1-32>
config link_aggregation group_id <value 1-32> {master_port <port> | ports <portlist> | state
    [enable | disable]} (1)
config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source
    | ip_destination | ip_source_dest]
show link_aggregation {group_id <value 1-32> | algorithm}
```

37.1.　create link_aggregation group_id

● 概要

このコマンドを用いて、リンクアグリゲーショングループを作成します。

● 構文

create link_aggregation group_id <value 1-32> {type [lacp | static]}

● パラメータ

<value 1-32>	グループ ID を指定します。グループ番号により各グループを識別します。スイッチに対して最大 32 のリンクアグリゲーショングループを設定できます。
type	（オプション）スタティックまたは LACP のグループタイプを指定します。タイプを指定しない場合、デフォルトのスタティックタイプになります。 lacp　グループタイプを LACP として指定します。 static グループタイプをスタティックとして指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

リンクアグリゲーショングループを作成するには：

```
Zxxx0:admin#create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp

Success

Zxxx0:admin#
```

37.2. delete link_aggregation group_id

● 概要

このコマンドを用いて、以前に設定されたリンクアグリゲーショングループを削除します。

● 構文

delete link_aggregation group_id <value 1-32>

● パラメータ

<value 1-32>	グループ ID を指定します。グループ番号により各グループを識別します。スイッチに対して最大 32 のリンクアグリゲーショングループを設定できます。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

リンクアグリゲーショングループを削除するには：

```
Zxxx0:admin#delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

Zxxx0:admin#
```

37.3. config link_aggregation group_id

● 概要

このコマンドを用いて、上記の create link_aggregation コマンドで作成したリンクアグリゲーショングループを設定できます。

● 構文

config link_aggregation group_id <value 1-32> {master_port <port> | ports <portlist> | state [enable | disable]} (1)

● パラメータ

<value 1-32>	グループ ID を指定します。グループ番号により各グループを識別します。スイッチに対して最大 32 のリンクアグリゲーショングループを設定できます。
master_port	リンクアグリゲーショングループ内のマスターポートを（番号で）指定します。リンクアグリゲーショングループのすべてのポートがマスターポートとポート設定を共有します。 <port> マスターポート ID を指定します。
ports	リンクアグリゲーショングループに属するポートの範囲を指定します。ポートリストにマスターポートが含まれる必要があります。 <portlist> 設定するポートの範囲を指定します。
state	指定したリンクアグリゲーショングループを有効または無効にします。 enable 指定したリンクアグリゲーショングループを有効にします。 disable 指定したリンクアグリゲーショングループを無効にします。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

リンクアグリゲーショングループ、グループ ID 1、マスターポート 7、メンバポート 5 ～ 7 を設定するには：

```
Zxxx0:admin#config link_aggregation group_id 1 master_port 7 ports 5-7
Command: config link_aggregation group_id 1 master_port 7 ports 5-7

Success.

Zxxx0:admin#
```

37.4. config link_aggregation algorithm

● 概要

このコマンドを用いて、負荷分散データを転送するための出力ポートを選択したときに、スイッチが調べるパケットの部分を設定します。
負荷分散アルゴリズムが IP 情報に基づくときに、パケットが非 IP パケットの場合は、送信元 MAC に基づきます。
負荷分散アルゴリズムがレイヤ 4 情報に基づくときに、パケットが TCP/UDP パケットでない場合は、以下のように処理されます。

1)パケットが非 IP パケットの場合は、送信元 MAC に基づきます。
2)パケットが IP パケットの場合、TCP/UDP ポートについて初期値の「0」が用いられます。つまり、TCP/UDP IP パケットでない場合は、TCP/UDP パケットと同様に扱われますが、TCP/UDP 値が 0 になります。

● 構文

config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest]

● パラメータ

mac_source	スイッチが MAC 送信元アドレスを調べるように指定します。
mac_destination	スイッチが MAC 宛先アドレスを調べるように指定します。
mac_source_dest	スイッチが MAC 送信元アドレスと MAC 宛先アドレスを調べるように指定します。
ip_source	スイッチが IP 送信元アドレスを調べるように指定します。
ip_destination	スイッチが IP 宛先アドレスを調べるように指定します。
ip_source_dest	スイッチが IP 送信元アドレスと IP 宛先アドレスを調べるように指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

リンクアグリゲーションアルゴリズムを mac-source-dest に設定するには：

```
Zxxx0:admin#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

Zxxx0:admin#
```

37.5. show link_aggregation

● 概要

このコマンドを用いて、スイッチの現在のリンクアグリゲーション設定を表示します。

● 構文

show link_aggregation {group_id <value 1-32> | algorithm}

● パラメータ

group_id	（オプション）グループ ID を指定します。グループ番号により各グループを識別します。 <value 1-32> スイッチに対して最大 32 のリンクアグリゲーショングループを設定できます。
algorithm	（オプション）特定のグループにより使用されているアルゴリズムによりリンクアグリゲーションの表示を指定します。

NOTE パラメータを指定しない場合、システムによりすべてのリンクアグリゲーション情報が表示されます。

● 制限

なし

● 実行例

リンクアグリゲーションが有効なときに、現在のリンクアグリゲーション設定を表示するには：

```
Zxxx0:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC_Source_Dest

Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   : 7
Status        : Enabled
Flooding Port : 7

Total Entries: 1

Zxxx0:admin#
```

リンクアグリゲーションが無効なときに、現在のリンクアグリゲーション設定を表示するには：

```
Zxxx0:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest
Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   :
Status        : Disabled
Flooding Port :

Total Entries: 1

Zxxx0:admin#
```

38. LLDP コマンド

LLDP（Link Layer Discovery Protocol）は、接続された機器の情報を定期的に収集するしくみです。IP 電話機、プリンタ、ネットワークカメラ等、機器が LLDP に対応していれば、どのような機器がどこに接続されているかを知ることができます。また、収集された情報から設定ミス等を識別したり、各種プロトコルの設定やスイッチの動作等を情報にあわせて変更することも可能になります。

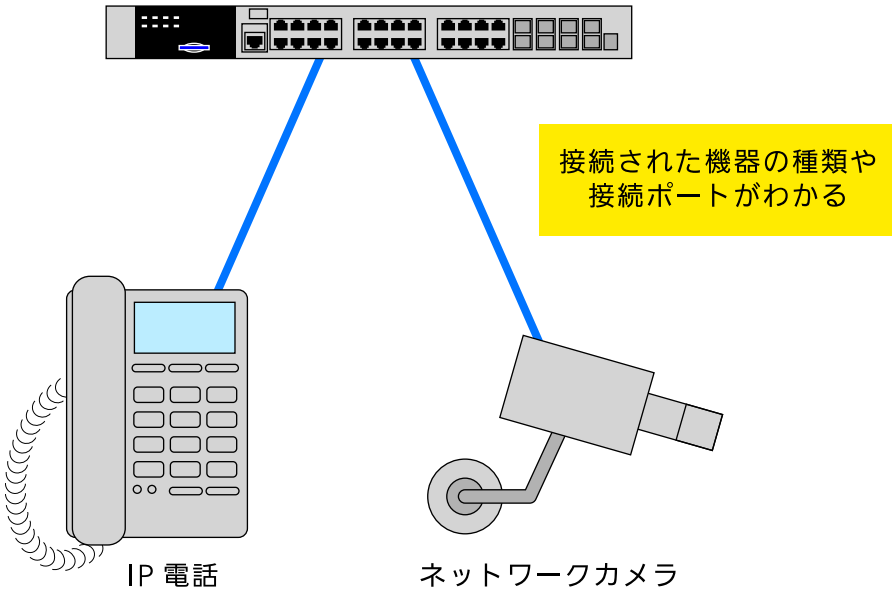


図 38-1　LLDP の概略

```
enable lldp
disable lldp
config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> |
    tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]
show lldp
config lldp forward_message [enable | disable]
config lldp notification_interval <sec 5-3600>
config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only |
    tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] |
    basic_tlvs [{all} | {port_description | system_name | system_description |
    system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] |
    dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] |
    dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] |
    dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs
    [{all} | {mac_phy_configuration_status | link_aggregation | maximum_frame_size}] [enable
    | disable]]
show lldp ports {<portlist>}
config lldp_med fast_start repeat_count <value 1-10>
config lldp_med log state [enable | disable]
config lldp_med notification topo_change ports [<portlist> | all] state [enable | disable]
```

config lldp_med ports [<portlist> | all] med_transmit_capabilities [all | {capabilities | network_policy | inventory}(1)] state [enable | disable]
show lldp_med ports {<portlist>}
show lldp_med
show lldp_med local_ports {<portlist>}
show lldp_med remote_ports {<portlist>}
show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}
show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp statistics
show lldp statistics ports {<portlist>}

38.1. enable lldp

● 概要

このコマンドを用いて、LLDP を有効にします。この機能を有効にすると、スイッチで LLDP パケットの送信、受信、および処理を開始できるようになります。各ポートの具体的な機能は、ポート毎の LLDP 設定に基づきます。LLDP パケットのアドバタイズメントについては、スイッチはポートを介して近傍に情報を通知します。LLDP パケットの受信については、スイッチはネイバーテーブル内からアドバタイズされる LLDP パケットから情報を受け取って認識します。LLDP の状態は、デフォルトでは無効に設定されています。

● 構文

enable lldp

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

LLDP を有効にするには：

```
Zxxx0:admin#enable lldp
Command: enable lldp

Success.

Zxxx0:admin#
```

38.2. disable lldp

● 概要

このコマンドを用いて、LLDP を無効にします。スイッチでは、LLDP アドバタイズメントパケットの送受信を停止します。

● 構文

disable lldp

● パラメータ

なし

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

LLDP を無効するには：

```
Zxxx0:admin#disable lldp
Command: disable lldp

Success.

Zxxx0:admin#
```

38.3. config lldp

● 概要

このコマンドを用いて、LLDP タイマー値を設定します。メッセージ TX 間隔は、アクティブなポートから近傍へのアドバタイズメント再送頻度を制御します。メッセージ TX 保持乗数は、LLDPDU における txTTL の TTL 値を計算するために使用する msgTxInterval の乗数です。TTL は、LLDPDU パケットによって送信されます。その保持期間は、65535 と message_tx_interval * message_tx_hold_multiplier の小さい方の値になります。パートナスイッチでは、指定されたアドバタイズメント TTL の期限が切れると、近傍スイッチの MIB からアドバタイズされたデータが削除されます。TX 遅延は、LLDP MIB コンテンツの変化によって、任意の LLDP ポートにて連続する LLDP アドバタイズメントを遅延する最小時間（遅延間隔）を変更するための値です。TX 遅延は、常に変化する MIB コンテンツに伴う LLDP メッセージの最小送信間隔を定義します。再度有効にした LLDP ポートでは、最後の無効コマンド実行後、再初期化遅延時間が経過してから再初期化を行います。

● 構文

config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> | tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]

● パラメータ

message_tx_interval	任意ポートで連続する LLDP アドバタイズメント送信のメッセージ TX 間隔を指定します。 <sec 5-32768> 5 ～ 32768 秒の範囲で指定します。デフォルト設定は 30 秒です。
message_tx_hold_multiplier	メッセージ TX 保持乗数を指定します。 <int 2-10> 2 ～ 10 の範囲で指定します。デフォルト設定は 4 です。
tx_delay	TX 遅延時間を指定します。 <sec 1-8192> 1 ～ 8192 秒の範囲で指定します。デフォルト設定は 2 秒です。txDelay は、0.25 * msgTxInterval 以下に設定しなければなりません。
reinit_delay	再初期化遅延時間を指定します。 <sec 1-10> 1 ～ 10 秒の範囲で指定します。デフォルト設定は 2 秒です。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

パケット送信間隔を変更するには：

```
Zxxx0:admin#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

Zxxx0:admin#
```

乗数の値を変更するには：

```
Zxxx0:admin#config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

Zxxx0:admin#
```

遅延間隔を設定するには：

```
Zxxx0:admin#config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

Zxxx0:admin#
```

再初期化遅延間隔を 5 秒に変更するには：

```
Zxxx0:admin#config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

Zxxx0:admin#
```

38.4. show lldp

● 概要

このコマンドを用いて、LLDP を表示します。

● 構文

show lldp

● パラメータ

なし

● 制限

なし

● 実行例

LLDP を表示するには：

```
Zxxx0:admin#show lldp
Command: show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 00-11-22-33-44-55
    System Name               :
    System Description        : Gigabit Ethernet Switch
    System Capabilities       : Repeater, Bridge

LLDP Configurations
    LLDP Status               : Disabled
    LLDP Forward Status       : Disabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2
    TX Delay                  : 2
    Notification Interval     : 5

Zxxx0:admin#
```

38.5. config lldp forward_message

● 概要

このコマンドを用いて、LLDP フォワーディングメッセージを設定します。LLDP を無効にし、LLDP フォワーディングメッセージを有効にした場合、受信した LLDPDU パケットを転送します。デフォルトの状態では無効です。

● 構文

config lldp forward_message [enable | disable]

● パラメータ

enable	LLDP フォワーディングメッセージを有効にします。
disable	LLDP フォワーディングメッセージを無効にします。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

LLDP フォワーディングメッセージを有効にするには：

```
Zxxx0:admin#config lldp forward_message enable
Command: config lldp forward_message enable

Success.

Zxxx0:admin#
```

38.6. config lldp notification_interval

● 概要

このコマンドを用いて、LLDP タイマー値を設定します。これにより、スイッチで生成される LLDP 変更通知の連続送信間隔が変更されます。

● 構文

config lldp notification_interval <sec 5-3600>

● パラメータ

<sec 5-3600> 通知間隔を 5 ～ 3600 秒の範囲で指定します。デフォルト設定は 5 秒です。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

通知間隔を 10 秒に変更するには：

```
Zxxx0:admin#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

Zxxx0:admin#
```

38.7. config lldp ports

● 概要

このコマンドを用いて、各ポートの LLDP オプションを設定します。LLDP 近傍からポートで受信したアドバタイズメント内で LLDP データ変更が検出された場合に、設定された SNMP トラップ受信装置への変更通知の送信を各ポートにて有効または無効にします。変更の定義には、新しい情報、情報タイムアウト、情報更新が含まれます。変更のタイプとしては、データの更新、挿入、削除が含まれます。管理者ステータスオプションでは、LLDP トラフィックにどのポートを参加させるか、さらに参加ポートで LLDP トラフィックを一方向のみまたは双方向でサポートするかどうかを制御します。
管理アドレス設定コマンドは、システムの IP アドレスを指定ポートからアドバタイズする必要があるかどうかを指定します。レイヤ 3 装置の場合、各管理アドレスを個別に指定できます。リストに追加した管理アドレスは、各管理アドレスに対応付けられた指定インターフェースからの LLDP 内でアドバタイズされます。その管理アドレスに対応するインターフェースも、if-index 形式でアドバタイズされます。
スイッチのアクティブな LLDP ポートでは、必ずアウトバウンドアドバタイズメントに必須データを含みます。また、4 つのオプションデータがあり、ポート毎またはポートグループに対して、アウトバウンド LLDP アドバタイズメントからこれらのオプションデータのうち 1 つまたは複数のデータタイプを除外するよう設定できます。必須データタイプには、4 つの基本的な情報タイプが含まれます（End of LLDPDU TLV、Chassis ID TLV、Port ID TLV、Time to Live TLV）。必須タイプは、無効にすることができません。さらにオプションで選択できるデータタイプが 4 つあり、それらは port_description、system_name、system_description、system_capability です。
アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有ポート VLAN ID TLV データタイプを除外するよう、個別ポートまたはポートグループを設定します。
アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有ポートおよびプロトコル VLAN ID TLV データタイプを除外するよう、個別ポートまたはポートグループを設定します。
アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有 VLAN 名 TLV データタイプを除外するよう、個別ポートまたはポートグループを設定します。
アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有プロトコル ID TLV データタイプを除外するよう、個別ポートまたはポートグループを設定します。この TLV オプションデータタイプは、対応するローカルシステムのプロトコル ID インスタンスがポートで送信されるかどうかを示します。プロトコル ID TLV は、ネットワーク運用で重要となるプロトコルをステーションでアドバタイズできるようにする 1 つの方法です。STP（Spanning Tree Protocol）、LACP（Link Aggregation Control Protocol）、さらにベンダ独自の各種類似プロトコルによって、ネットワークのトポロジと接続性が維持されます。このポートで EAPOL、GVRP、STP（MSTP を含む）、および LACP プロトコル ID を有効にし、それらのアドバタイズメントも有効にした場合、このプロトコル ID はアドバタイズされます。

● 構文

config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation |maximum_frame_size}] [enable | disable]]

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	システムのすべてのポートを設定します。
notification	近傍装置から受け取るアドバタイズメントで検出される LLDP データ変更の SNMP トラップ通知を有効または無効にします。デフォルトの通知状態では無効です。 enable 近傍装置から受け取るアドバタイズメントで検出されるLLDPデータ変更のSNMPトラップ通知を有効にします。 disable 近傍装置から受け取るアドバタイズメントで検出されるLLDPデータ変更のSNMPトラップ通知を無効にします。
admin_status	目的のポート毎の管理状態を選択します。デフォルトのポート毎の状態は tx_and_rx です。 tx_only LLDP パケットは送信するが、近傍装置からのインバウンド LLDP パケットをブロックするよう、指定したポートを設定します。 rx_only 近傍からの LLDP パケットは受信するが、近傍へのアウトバウンド LLDP パケットをブロックするよう、指定したポートを設定します。 tx_and_rx LLDP パケットを送受信するよう、指定したポートを設定します。 disable 指定したポートで LLDP パケットの送受信を無効にします。
mgt_address	指定の管理アドレスインスタンスをアドバタイズするよう指定したポートタイプです。 ipv4 IPv4 の IP アドレスを指定します。 <ipaddr> IPv4 の IP アドレスを指定します。 ipv6 IPv6 の IP アドレスを指定します。 <ipv6addr> IPv6 の IP アドレスを指定します。 enable 指定の管理アドレスインスタンスをアドバタイズするよう指定したポートを有効にします。 disable 指定の管理アドレスインスタンスをアドバタイズするよう指定したポートを無効にします。

basic_tlvs
アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の TLV オプションデータタイプを除外するよう、個別ポートまたはポートグループを設定します。
all （オプション）以下に示す 4 つの TLV データタイプをすべて設定します。
port_description
（オプション）この TLV オプションデータタイプは、LLDP エージェントがポートで Port Description TLV を送信することを示します。デフォルトの状態では無効です。
system_name
（オプション）この TLV オプションデータタイプは、LLDP エージェントが System Name TLV を送信することを示します。デフォルトの状態では無効です。
system_description
（オプション）この TLV オプションデータタイプは、LLDP エージェントが System Description TLV を送信することを示します。デフォルトの状態では無効です。
system_capabilities
（オプション）この TLV オプションデータタイプは、LLDP エージェントが System Capabilities TLV を送信することを示します。system_capabilities は、装置がリピータ、ブリッジ、またはルータ機能を提供するかどうか、および提供された機能が現在有効であるかどうかを示します。デフォルトの状態では無効です。
enable アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の TLV オプションデータタイプを除外するよう、個別ポートまたはポートグループの設定を有効にします。
disable アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の TLV オプションデータタイプを除外するための、個別ポートまたはポートグループの設定を無効にします。

dot1_tlv_pvid
この TLV オプションデータタイプは、任意の LLDP 送信対応ポートで、IEEE 802.1 組織固有に定義されたポート VLAN ID TLV 送信を認証するかどうかを決定します。デフォルトの状態では無効です。
enable 任意の LLDP 送信対応ポートでのポート VLAN ID TLV 送信を有効にします。
disable 任意の LLDP 送信対応ポートでのポート VLAN ID TLV 送信を無効にします。

dot1_tlv_protocol_vid
この TLV オプションデータタイプは、任意の LLDP 送信対応ポートで、IEEE 802.1 組織固有に定義されたポートおよびプロトコル VLAN ID TLV 送信を認証するかどうかを決定します。デフォルトの状態では無効です。
vlan （オプション）送信する VLAN を指定します。
all （オプション）すべての VLAN 名を送信します。
<vlan_name 32>
（オプション）送信する VLAN 名を指定します。
vlanid （オプション）送信する VLAN ID リストを指定します。
<vidlist> 送信する VLAN ID リストを指定します。
enable アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有ポートおよびプロトコル VLAN ID TLV データタイプを除外するよう、個別ポートまたはポートグループの設定を有効にします。
disable アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有ポートおよびプロトコル VLAN ID TLV データタイプを除外するための、個別ポートまたはポートグループの設定を無効にします。

dot1_tlv_vlan_name

この TLV オプションデータタイプは、対応するローカルシステムの VLAN 名インスタンスがポートで送信されるかどうかを示します。1 つのポートが複数の VLAN と対応付けられている場合、有効になっている VLAN ID がアドバタイズされます。デフォルトの状態では無効です。

vlan （オプション）送信する VLAN を指定します。

all （オプション）すべての VLAN 名を送信します。

<vlan_name 32>

（オプション）送信する VLAN 名を指定します。

vlanid （オプション）送信する VLAN ID リストを指定します。

<vidlist>

送信する VLAN ID リストを指定します。

enable アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有 VLAN 名 TLV データタイプを除外するよう、個別ポートまたはポートグループの設定を有効にします。

disable アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有 VLAN 名 TLV データタイプを除外するための、個別ポートまたはポートグループの設定を無効にします。

dot1_tlv_protocol_identity

この TLV オプションデータタイプは、対応するローカルシステムのプロトコル ID インスタンスがポートで送信されるかどうかを示します。プロトコル ID TLV は、ネットワークのトポロジと接続性を維持する役割を果たす STP（Spanning Tree Protocol）、LACP（Link Aggregation Control Protocol）、さらにベンダ独自の各種類似プロトコルなど、ネットワーク運用で重要となるプロトコルをステーションでアドバタイズできるようにする 1 つの方法です。このポートで EAPOL、GVRP、STP（MSTP を含む）、および LACP プロトコル ID を有効にし、それらのアドバタイズメントも有効にした場合、プロトコル ID はアドバタイズされます。デフォルトの状態では無効です。

all 以下に示すすべてのプロトコルをアドバタイズします。

eapol （オプション）EAPOL をアドバタイズします。

lacp （オプション）LACP をアドバタイズします。

gvrp （オプション）GVRP をアドバタイズします。

stp （オプション）STP をアドバタイズします。

enable アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有プロトコル ID TLV データタイプを除外するよう、個別ポートまたはポートグループの設定を有効にします。

disable アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.1 組織固有プロトコル ID TLV データタイプを除外するための、個別ポートまたはポートグループの設定を無効にします。

dot3_tlvs	アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.3 組織固有 TLV データタイプを除外する個別ポートまたはポートグループです。
	all　（オプション）以下に示すすべての TLV オプションデータタイプを設定します。
	mac_phy_configuration_status （オプション）この TLV オプションデータタイプは、LLDP エージェントが MAC/PHY configuration/status TLV を送信することを示します。このタイプは、IEEE 802.3 リンクの両端にて、それぞれ異なる全 / 半二重設定および / または通信速度を設定しても、ある程度制限されたネットワーク接続性を確立できることを示します。より正確にいえば、この情報にはポートでオートネゴシエーション機能をサポートするか、その機能が有効であるか、オートネゴシエーションによるアドバタイズ機能、および動作可能な MAU タイプが含まれています。デフォルトの状態では無効です。
	link_aggregation （オプション）この TLV オプションデータタイプは、LLDP エージェントが Link Aggregation TLV を送信することを示します。このタイプは、IEEE 802.3 MAC の現在のリンクアグリゲーションステータスを示します。より正確にいえば、この情報にはポートでリンクアグリゲーションをサポートするか、ポートがリンクアグリゲーションでアグリゲートされているか、およびアグリゲートされたポート ID が含まれています。デフォルトの状態では無効です。
	maximum_frame_size （オプション）この TLV オプションデータタイプは、LLDP エージェントが Maximum-frame-size TLV を送信することを示します。デフォルトの状態では無効です。
	enable　アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.3 組織固有 TLV データタイプを除外するよう、個別ポートまたはポートグループの設定を有効にします。
	disable　アウトバウンド LLDP アドバタイズメントから 1 つまたは複数の IEEE 802.3 組織固有 TLV データタイプを除外するための、個別ポートまたはポートグループの設定を無効にします。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 5 の SNMP 通知状態を有効に変更するには：

```
Zxxx0:admin#config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

Zxxx0:admin#
```

ポート 1 ～ 5 の送信および受信モードを設定するには：

```
Zxxx0:admin#config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

Zxxx0:admin#
```

ポート 1 ～ 5 でのアドレスエントリ管理を有効にするには：

```
Zxxx0:admin#config lldp ports 1-5 mgt_addr ipv4 192.168.254.10 enable
Command: config lldp ports 1-5 mgt_addr ipv4 192.168.254.10 enable

Success.

Zxxx0:admin#
```

すべてのポートで、アウトバウンド LLDP アドバタイズメントからシステム名 TLV を除外するには：

```
Zxxx0:admin#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

Zxxx0:admin#
```

すべてのポートで、アウトバウンド LLDP アドバタイズメントから VLAN 名 TLV を除外するには：

```
Zxxx0:admin#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

Zxxx0:admin#
```

すべてのポートで、アウトバウンド LLDP アドバタイズメントからポートおよびプロトコル VLAN ID TLV を除外するには：

```
Zxxx0:admin#config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable

Success.

Zxxx0:admin#
```

すべてのポートで、アウトバウンド LLDP アドバタイズメントから VLAN 名 TLV を除外するには：

```
Zxxx0:admin#config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable

Success.

Zxxx0:admin#
```

すべてのポートで、アウトバウンド LLDP アドバタイズメントからプロトコル ID TLV を除外するには：

```
Zxxx0:admin#config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

Zxxx0:admin#
```

すべてのポートで、アウトバウンド LLDP アドバタイズメントから MAC/PHY 設定 / ステータス TLV を除外するには：

```
Zxxx0:admin#config lldp ports all dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

Zxxx0:admin#
```

38.8. show lldp ports

● 概要

このコマンドを用いて、アドバタイズメントオプションのポート毎の LLDP 設定を表示します。

● 構文

show lldp ports {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートを指定します。

NOTE ポートリストを指定しない場合、すべてのポートの情報を表示します。

● 制限

なし

● 実行例

ポート 1 の LLDP TLV オプションを表示するには：

```
Zxxx0:admin#show lldp ports 1
Command: show lldp ports 1

Port ID                 : 1
------------------------------------------------------------
Admin Status            : TX_and_RX
Notification Status     : Disabled
Advertised TLVs Option  :
    Port Description                                Disabled
    System Name                                     Disabled
    System Description                              Disabled
    System Capabilities                             Disabled
    Enabled Management Address
        (None)
    Port VLAN ID                                    Disabled
Enabled Port_and_Protocol_VLAN_ID
    (None)
Enabled VLAN Name
    (None)
Enabled Protocol Identity
        (None)
    MAC/PHY Configuration/Status                     Disabled
    Link Aggregation                                 Disabled
    Maximum Frame Size                               Disabled

Zxxx0:admin#
```

38.9. config lldp_med fast_start repeat_count

● 概要

このコマンドを用いて、ファストスタート実行回数（fast start repeat count）を設定します。既存の LLDP リモートシステム MIB に関連付けられていない MSAP 識別子に対して LLDP-MED Capabilities TLV が検出されると、アプリケーションレイヤはファストスタートメカニズムを起動し、medFastStart タイマーの medFastStartRepeatCount 回数を 1 に設定します。初期値は 4 です。

● 構文

config lldp_med fast_start repeat_count <value 1-10>

● パラメータ

<value 1-10> ファストスタート実行回数の値を 1 ～ 10 の範囲で指定します。初期値は 4 です。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルユーザのみ実行できます。

● 実行例

LLDP-MED ファストスタート実行回数を 5 に設定するには：

```
Zxxx0:admin#config lldp_med fast_start repeat_count 5
Command: config lldp_med fast_start repeat_count 5

Success.

Zxxx0:admin#
```

38.10. config lldp_med log state

● 概要

このコマンドを用いて、LLDP-MED イベントのログ状態を設定します。

● 構文

config lldp_med log state [enable | disable]

● パラメータ

enable	LLDP-MED イベントのログ状態を有効にします。
disable	LLDP-MED イベントのログ状態を無効にします。デフォルトでは無効です。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルユーザのみ実行できます。

● 実行例

LLDP-MED イベントのログ状態を有効にするには：

```
Zxxx0:admin#config lldp_med log state enable
Command: config lldp_med log state enable

Success.

Zxxx0:admin#
```

38.11. config lldp_med notification topo_change ports

● 概要

このコマンドを用いて、エンドポイント装置が削除された場合または別のポートに移動した場合に、設定されたSNMPトラップ受信装置へのトポロジ変更通知の送信を各ポートにて有効または無効にします。デフォルトの状態では無効です。

● 構文

config lldp_med notification topo_change ports [<portlist> | all] state [enable | disable]

● パラメータ

<portlist>設定するポート範囲を指定します。	
all	システム内のすべてのポートを設定します。
state	トポロジ変更検出状態の SNMP トラップ通知を有効または無効にします。 enable トポロジ変更検出時の SNMP トラップ通知を有効にします。 disable トポロジ変更検出時の SNMP トラップ通知を無効にします。デフォルトの通知状態では無効です。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルユーザのみ実行できます。

● 実行例

ポート 1 ～ 2 のトポロジ変更通知を有効にするには：

```
Zxxx0:admin#config lldp_med notification topo_change ports 1-2 state enable
Command: config lldp_med notification topo_change ports 1-2 state enable

Success.

Zxxx0:admin#
```

38.12. config lldp_med ports

● 概要

このコマンドを用いて、LLDP-MED TLV の送信を有効または無効にします。このコマンドは、TLV 送信機能を無効にすることで、ポート単位で LLDP-MED を無効にすることができます。この場合、該当ポートに対応する LLDP-MED MIB 内のリモートテーブルオブジェクトは格納されません。

● 構文

config lldp_med ports [<portlist> | all] med_transmit_capabilities [all | {capabilities | network_policy | inventory}(1)] state [enable | disable]

● パラメータ

<portlist>	設定するポート範囲を指定します。
all	システム内のすべてのポートを設定します。
med_transit_capabilities	指定した LLDP-MED TLV 機能を送信します。
all	機能、ネットワークポリシー、およびインベントリを送信することを選択します。
capabilities	（オプション）LLDP エージェントが LLDP-MED Capabilities TLV を送信します。LLDP-MED PDU を送信するには、この TLV タイプを有効にしてください。有効でない場合、このポートで LLDP-MED PDU を送信できません。
network_policy	（オプション）LLDP エージェントが LLDP-MED network policy TLV を送信します。
inventory	（オプション）LLDP エージェントが LLDP-MED inventory TLV を送信します。
state	LLDP-MED TLV の送信を有効または無効にします。 enable　LLDP-MED TLV の送信を有効にします。 disable　LLDP-MED TLV の送信を無効にします。

● 制限

このコマンドは、管理者レベルおよびオペレータレベルユーザのみ実行できます。

● 実行例

ポート 1 ～ 2 ですべての機能の送信を有効にするには：

```
Zxxx0:admin#config lldp_med ports 1-2 med_transmit_capabilities all state enable
Command: config lldp_med ports 1-2 med_transmit_capabilities all state enable

Success.

Zxxx0:admin#
```

38.13. show lldp_med ports

● 概要

このコマンドを用いて、アドバタイズメントオプションのポート毎の LLDP-MED 設定を表示します。

● 構文

show lldp_med ports {<portlist>}

● パラメータ

<portlist>表示するポート範囲を指定します。

NOTE ポートリストを指定しない場合、すべてのポートの情報を表示します。

● 制限

なし

● 実行例

ポート 1 の LLDP-MED 設定を表示するには：

```
Zxxx0:admin#show lldp_med ports 1
Command: show lldp_med ports 1

Port ID : 1
------------------------------------------------------------
Topology Change Notification Status         : Enabled
LLDP-MED Capabilities TLV                   : Enabled
LLDP-MED Network Policy TLV                 : Enabled
LLDP-MED Inventory TLV                      : Enabled

Zxxx0:admin#
```

38.14. show lldp_med

● 概要

このコマンドを用いて、スイッチの基本的な LLDP-MED 設定ステータスを表示します。

● 構文

show lldp_med

● パラメータ

なし

● 制限

なし

● 実行例

スイッチの基本的な LLDP-MED 設定ステータスを表示するには：

```
Zxxx0:admin#show lldp_med
Command: show lldp_med

LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : A1
    Firmware Revision         : 1.0.0.xx
    Software Revision         : 1.0.0.xx
    Serial Number             :
    Manufacturer Name         : MANAGER
    Model Name                : Zxxx0 Gigabit Ethernet S
    Asset ID                  :

LLDP-MED Configuration:
    Fast Start Repeat Count   : 4

LLDP-MED Log State:Disabled

Zxxx0:admin#
```

38.15. show lldp_med local_ports

● 概要

このコマンドを用いて、アウトバウンド LLDP-MED アドバタイズメントを格納するために現在利用できるポート毎の LLDP-MED 情報を表示します。

● 構文

show lldp_med local_ports {<portlist>}

● パラメータ

<portlist>表示するポート範囲を指定します。

NOTE ポートリストを指定しない場合、すべてのポートの情報を表示します。

● 制限

なし

● 実行例

アウトバウンド LLDP-MED アドバタイズメントを格納するためにポート 1 で現在利用できる LLDP-MED 情報を表示するには：

```
Zxxx0:admin#show lldp_med local_ports  1
Command: show lldp_med local_ports 1

Port ID                 : 1
----------------------------------------------------------------
LLDP-MED Capabilities Support:
    Capabilities               :Support
    Network Policy             :Support
    Location Identification    :Not Support
    Extended Power Via MDI PSE :Not Support
    Extended Power Via MDI PD  :Not Support
    Inventory                  :Support

Network Policy:
  None

Extended Power Via MDI:
  None

Zxxx0:admin#
```

38.16. show lldp_med remote_ports

● 概要

このコマンドを用いて、近傍から認識した LLDP-MED 情報を表示します。

● 構文

show lldp_med remote_ ports {<portlist>}

● パラメータ

<portlist>（オプション）表示するポート範囲を指定します。

NOTE ポートリストを指定しない場合、すべてのポートの情報を表示します。

● 制限

なし

● 実行例

リモートエントリ情報を表示するには：

```
Zxxx0:admin#show lldp_med remote_ports 1
Command: show lldp_med remote_ports 1

Port ID : 1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
   Chassis ID Subtype                          : MAC Address
   Chassis ID                                  : 00-01-02-03-04-00
   Port ID Subtype                             : Net Address
   Port ID                                     : 172.18.10.11

   LLDP-MED capabilities:
       LLDP-MED Device Class: Endpoint Device Class III
       LLDP-MED Capabilities Support:
           Capabilities                        : Support
           Network Policy                      : Support
           Location Identification             : Support
           Extended Power Via MDI              : Support
           Inventory                           : Support
       LLDP-MED Capabilities Enabled:
          Capabilities                         : Enabled
          Network Policy                       : Enabled
          Location Identification              : Enabled
          Extended Power Via MDI               : Enabled
          Inventory                            : Enabled

   Network Policy:
      Application Type : Voice
         VLAN ID                               :
         Priority                              :
         DSCP                                  :
         Unknown                               : True
         Tagged                                :
    Application Type : Softphone Voice
         VLAN ID                               : 200
         Priority                              : 7
         DSCP                                  : 5
         Unknown                               : False
         Tagged                                : True

      Location Identification:
         Location Subtype: CoordinateBased
            Location Information               :
         Location Subtype: CivicAddress
            Location Information               :

Extended Power Via MDI
     Power Device Type: PD Device
           Power Priority                      : High
           Power Source                        : From PSE
           Power Request                       : 8 Watts
```

```
  Inventory Management:
     Hardware Revision                    :
     Firmware Revision                    :
     Software Revision                    :
     Serial Number                        :
     Manufacturer Name                    :
     Model Name                           :
     Asset ID                             :

Zxxx0:admin#
```

38.17. show lldp local_ports

● 概要

このコマンドを用いて、アウトバウンド LLDP アドバタイズメントを格納するために現在利用できるポート毎の情報を表示します。

● 構文

show lldp local ports {<portlist>} {mode [brief | normal | detailed]}

● パラメータ

<portlist>	（オプション）表示するポートを指定します。ポートリストを指定しない場合、すべてのポートの情報を表示します。
mode	（オプション）モードとして brief、normal、または detailed を選択します。 brief　情報を brief（簡易）モードで表示します。 normal　情報を normal（通常）モードで表示します。デフォルトは表示モードです。 detailed　情報を detailed（詳細）モードで表示します。

● 制限

なし

● 実行例

ポート 1 の LLDP ローカルポート情報を表示するには：

```
Zxxx0:admin#show lldp local_ports  1
Command: show lldp local_ports 1

Port ID : 1
------------------------------------------------------------------------------
Port ID Subtype                          : MAC Address
Port ID                                  : 00-01-02-03-05-00
Port Description                         : Zxxx0 R1.0.0.xx
                                           Port 1 on Unit 1
Port PVID                                : 1
Management Address Count                 : 1
PPVID Entries Count                      : 0
VLAN Name Entries Count                  : 1
Protocol Identity Entries Count          : 0
MAC/PHY Configuration/Status             : (See Detail)
Link Aggregation                         : (See Detail)
Maximum Frame Size                       : 1536

Zxxx0:admin#
```

38.18. show lldp mgt_addr

● 概要

このコマンドを用いて、LLDP 管理アドレスを表示します。

● 構文

show lldp mgmt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}

● パラメータ

ipv4	（オプション）LLDP 管理アドレスエントリの IPv4 アドレスを指定します。 <ipaddr> LLDP 管理アドレスエントリの IPv4 アドレスを指定します。
ipv6	（オプション）LLDP 管理アドレスエントリの IPv6 アドレスを指定します。 <ipv6addr> LLDP 管理アドレスエントリの IPv6 アドレスを指定します。

● 制限

なし

● 実行例

LLDP 管理アドレスを表示するには：

```
Zxxx0:admin#show lldp mgt_addr
Command: show lldp mgt_addr

Address 1 :
-----------------------------------------------------
    Subtype                                 : IPv4
    Address                                 : 10.19.72.38
    IF Type                                 : Unknown
    OID                                     : 1.3.6.1.4.1.396.5.4.1.xx
    Advertising Ports                       :
Total Entries : 1

Zxxx0:admin#
```

38.19. show lldp remote_ ports

● 概要

このコマンドを用いて、近傍パラメータから認識した情報を表示します。

● 構文

show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}

● パラメータ

<portlist>	（オプション）表示するポートを指定します。ポートリストを指定しない場合、すべてのポートの情報を表示します。
mode	（オプション）モードとして brief、normal、または detailed を選択します。 brief 情報を brief（簡易）モードで表示します。 normal 情報を normal（通常）モードで表示します。デフォルトは表示モードです。 detailed 情報を detailed（詳細）モードで表示します。

● 制限

なし

● 実行例

リモートポート 1 および 2 の LLDP 情報を表示するには：

```
Zxxx0:admin#show lldp remote_ports 1-2
Command: show lldp remote_ports 1-2

Remote Entities Count : 0


Zxxx0:admin#
```

38.20. show lldp statistics

● 概要

このコマンドを用いて、スイッチでの近傍検出動作の概要を表示します。

● 構文

show lldp statistics

● パラメータ

なし

● 制限

なし

● 実行例

LLDP 統計を表示するには：

```
Zxxx0:admin#show lldp statistics
Command: show lldp statistics

Last Change Time       : 3648
Number of Table Insert : 0
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0

Zxxx0:admin#
```

38.21. show lldp statistics ports

● 概要

このコマンドを用いて、個別ポートの LLDP 統計情報を表示します。

● 構文

show lldp statistics ports {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートを指定します。

NOTE ポートリストを指定しない場合、すべてのポートの情報を表示します。

● 制限

なし

● 実行例

ポート 1 の LLDP 統計情報を表示するには：

```
Zxxx0:admin#show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID : 1
----------------------------------------------
    LLDPStatsTXPortFramesTotal           : 0
    LLDPStatsRXPortFramesDiscardTotal    : 0
    LLDPStatsRXPortFramesErrors          : 0
    LLDPStatsRXPortFramesTotal           : 0
    LLDPStatsRXPortTLVsDiscardedTotal    : 0
    LLDPStatsRXPortTLVsUnrecognizedTotal : 0
    LLDPStatsRXPortAgeoutsTotal          : 0

Zxxx0:admin#
```

39.ループバックインターフェースコマンド

ループバックインターフェースとは、本装置自身を出力先とする仮想のインターフェースです。
ループバックインターフェースにネットワークアドレスを割り当てることにより、仮想のネットワークを設定できます。
ここでは、ループバックインターフェースの作成や削除を行います。

create loopback ipif <ipif_name 12> {<network_address>} {state [enable | disable]}
config loopback ipif <ipif_name 12> [{ipaddress <network_address> | state [enable | disable]}(1)]
show loopback ipif {<ipif_name 12>}
delete loopback ipif [<ipif_name 12> | all]

39.1. create loopback ipif

● 概要

このコマンドを用いて、本装置にループバックインターフェースを作成します。

● 構文

create loopback ipif <ipif_name 12> {<network_address>} {state [enable | disable]}

● パラメータ

<ipif_name 12>	この設定に使用する IP インターフェース名を入力します。名前は 12 文字以内で設定できます。
<network_address>	（オプション）ループバックインターフェースの IPv4 ネットワークアドレスを入力します。ホストアドレスおよびネットワークマスクの長さを指定します。
state	（オプション）ループバックインターフェースの状態を指定します。 enable　ループバックインターフェースの状態を有効にします。 disable　ループバックインターフェースの状態を無効にします。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

サブネットアドレス 20.1.1.1/8 を持つ loopback1 という名前のループバックインターフェースを 1 つ作成して、管理状態を有効にするには：

```
Zxxx0:admin# create loopback ipif loopback1 20.1.1.1/8 state enable
Command: create loopback ipif loopback1 20.1.1.1/8 state enable

Success.

Zxxx0:admin#
```

39.2. config loopback ipif

● 概要

このコマンドを用いて、ループバックインターフェースパラメータを設定します。

● 構文

config loopback ipif <ipif_name 12> [{ipaddress <network_address> | state [enable | disable]}(1)]

● パラメータ

<ipif_name 12>	この設定に使用する IP インターフェース名を入力します。名前は 12 文字以内で設定できます。
ipaddress	（オプション）ループバックインターフェースの IPv4 ネットワークアドレスを指定します。
<network_address>	ループバックインターフェースの IPv4 ネットワークアドレスを入力します。ホストアドレスおよびネットワークマスクの長さを指定します。
state	（オプション）ループバックインターフェースの状態を指定します。 enable　ループバックインターフェースの状態を有効にします。 disable　ループバックインターフェースの状態を無効にします。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

サブネットアドレス 10.0.0.1/8 を持つ loopback1 という名前のループバックインターフェースを設定するには：

```
Zxxx0:admin# config loopback ipif loopback1 ipaddress 10.0.0.1/8
Command: config loopback ipif loopback1 ipaddress 10.0.0.1/8

Success.

Zxxx0:admin#
```

39.3. show loopback ipif

● 概要

このコマンドを用いて、ループバックインターフェースの情報を表示します。

● 構文

show loopback ipif {<ipif_name 12>}

● パラメータ

<ipif_name 12>	（オプション）この設定に使用する IP インターフェース名を入力します。名前は 12 文字以内で設定できます。

● 制限

なし

● 実行例

loopback1 という名前のループバックインターフェースの情報を表示するには：

```
Zxxx0:admin# show loopback ipif loopback1
Command: show loopback ipif loopback1

Loopback Interface          : loopback1
Interface Admin State       : Enabled
IPv4 Address                : 10.0.0.1/8 (MANUAL)

Total Entries:1

Zxxx0:admin#
```

39.4. delete loopback ipif

● 概要

このコマンドを用いて、ループバックインターフェースを削除します。

● 構文

delete loopback ipif [<ipif_name 12> | all]

● パラメータ

<ipif_name 12>	この設定に使用する IP インターフェース名を入力します。名前は 12 文字以内で設定できます。
all	すべての IP ループバックインターフェースを削除します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

loopback1 という名前のループバックインターフェースを削除するには：

```
Zxxx0:admin# delete loopback ipif loopback1
Command: delete loopback ipif loopback1

Success.

Zxxx0:admin#
```

40. MAC 通知コマンド

本製品の MAC アドレステーブルに新しいエントリが登録された際に、SNMP トラップを利用して管理サーバに通知を行います。不正な機器のネットワークへの接続等を検出できます。

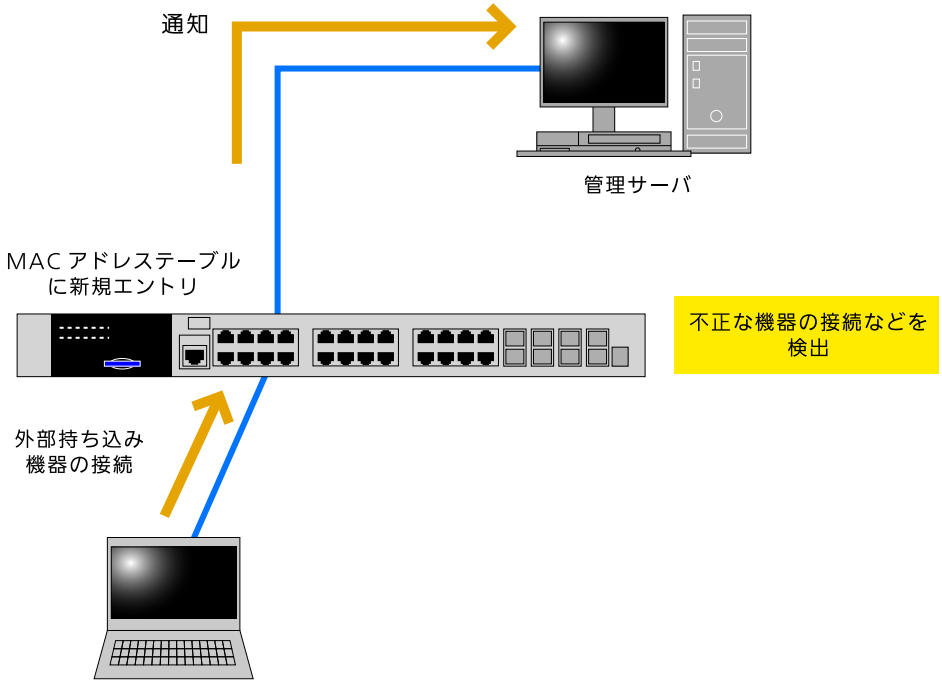


図 40-1　MAC Notification の概略

enable mac_notification
disable mac_notification
config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>}(1)
config mac_notification ports [<portlist> | all] [enable | disable]
show mac_notification
show mac_notification ports {<portlist>}

40.1.　enable mac_notification

● 概要

このコマンドを用いて、本装置の新しく学習された MAC アドレスのトラップ通知を有効にします。

● 構文

enable mac_notification

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

MAC 通知機能を有効にするには：

```
Zxxx0:admin#enable mac_notification
Command: enable mac_notification

Success.

Zxxx0:admin#
```

40.2. disable mac_notification

● 概要

このコマンドを用いて、本装置の新しく学習された MAC アドレスのトラップ通知を無効にします。

● 構文

disable mac_notification

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

MAC 通知機能を無効にするには：

```
Zxxx0:admin#disable mac_notification
Command: disable mac_notification

Success.

Zxxx0:admin#
```

40.3. config mac_notification

● 概要

このコマンドを用いて、スイッチの MAC アドレステーブルの通知に関するグローバル設定を行います。

● 構文

config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>}(1)

● パラメータ

interval	通知を起動する時間間隔を秒単位で指定します。 <int 1-2147483647> 1 ～ 2147483647 秒の範囲で指定します。
historysize	通知を起動するための、新しく学習された MAC のエントリを指定します。 <int 1-500> 500 までのエントリを指定できます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

スイッチの MAC アドレステーブルの通知に関するグローバル設定を指定するには：

```
Zxxx0:admin#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

Zxxx0:admin#
```

40.4. config mac_notification ports

● 概要

このコマンドを用いて、ポートの MAC アドレステーブルの通知のステータス設定を行います。

● 構文

config mac_notification ports [<portlist> | all] [enable | disable]

● パラメータ

<portlist>設定するポートの範囲を指定します。	
all	システムのすべてのポートを設定します。
enable	ポートの MAC アドレステーブルの通知を有効にします。
disable	ポートの MAC アドレステーブルの通知を無効にします。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 7 の MAC アドレステーブルの通知を有効にするには：

```
Zxxx0:admin#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

Zxxx0:admin#
```

40.5. show mac_notification

● 概要

このコマンドを用いて、スイッチの MAC アドレステーブルの通知に関するグローバル設定を表示します。

● 構文

show mac_notification

● パラメータ

なし

● 制限

なし

● 実行例

スイッチの MAC アドレステーブルの通知に関するグローバル設定を表示するには：

```
Zxxx0:admin#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State        : Enabled
Interval     : 1
History Size : 500

Zxxx0:admin#
```

40.6. show mac_notification ports

● 概要

このコマンドを用いて、ポートの MAC アドレステーブルの通知のステータス設定を表示します。

● 構文

show mac_notification ports {<portlist>}

● パラメータ

<portlist>（オプション）設定するポートの範囲を指定します。

● 制限

なし

● 実行例

すべてのポートの MAC アドレステーブルの通知のステータス設定を表示するには：

```
Zxxx0:admin#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
------  ------------------------------------
1                  Disabled
2                  Disabled
3                  Disabled
4                  Disabled
5                  Disabled
6                  Disabled
7                  Disabled
8                  Disabled
9                  Disabled
10                 Disabled

Zxxx0:admin#
```

41.MAC ベースアクセスコントロールコマンド

MAC ベースアクセスコントロール（MAC-based Access Control）とは、スイッチに接続された機器をその MAC アドレスに基づき認証し、ネットワークへの接続を制御するしくみです。
認証サーバとして、RADIUS サーバまたは本製品内のローカルデータベースを選択できます。認証されなかった場合に、接続を遮断する以外にゲスト VLAN への接続を認証し、インターネットの利用のみを認証するなどのアクセス制御を設定できます。

enable mac_based_access_control
disable mac_based_access_control
config mac_based_access_control password <passwd 16>
config mac_based_access_control method [local | radius]
config mac_based_access_control guest_vlan ports <portlist>
config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-4000> | no_limit]}(1)
create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid < vlanid 1-4094>]
clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]
create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
config mac_based_access_control max_users [<value 1-4000> | no_limit]
config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)
delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
show mac_based_access_control auth_state ports {<portlist>}
show mac_based_access_control {ports {<portlist>}}
show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
config mac_based_access_control log state [enable | disable]
config mac_based_access_control trap state [enable | disable]
config mac_based_access_control password_type [manual_string | client_mac_address]

41.1. enable mac_based_access_control

● 概要

このコマンドを用いて、MAC ベースアクセスコントロール機能を有効にします。

● 構文

enable mac_based_access_control

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC ベースアクセスコントロールを有効にするには：

```
Zxxx0:admin#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

Zxxx0:admin#
```

41.2. disable mac_based_access_control

● 概要

このコマンドを用いて、MAC ベースアクセスコントロール機能を無効にします。

● 構文

disable mac_based_access_control

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC ベースアクセスコントロールを無効にするには：

```
Zxxx0:admin#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

Zxxx0:admin#
```

41.3. config mac_based_access_control password

● 概要

このコマンドを用いて、RADIUS サーバを介した認証に使用するパスワードを設定します。

● 構文

config mac_based_access_control password <passwd 16>

● パラメータ

<passwd 16>	RADIUS モードでは、このパスワードを使用して、スイッチが RADIUS サーバと通信します。キーの最大文字数は 16 文字です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

RADIUS サーバを介した認証に「rosebud」というパスワードを使用するよう設定するには：

```
Zxxx0:admin#config mac_based_access_control password rosebud
Command: config mac_based_access_control password rosebud

Success.

Zxxx0:admin#
```

41.4. config mac_based_access_control method

● 概要

このコマンドを用いて、ローカルデータベースまたは RADIUS サーバを介した認証を行います。

● 構文

config mac_based_access_control method [local | radius]

● パラメータ

local	ローカルデータベースを介して認証を行います。
radius	RADIUS サーバを介して認証を行います。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC ベースアクセスコントロール方法を local に設定するには：

```
Zxxx0:admin#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

Zxxx0:admin#
```

41.5. config mac_based_access_control guest_vlan ports

● 概要

このコマンドを用いて、指定したポートをゲスト VLAN モードにします。ポートリストに含まれないポートは、非ゲスト VLAN モードです。ゲスト VLAN モードの動作の詳細については、MAC ベースアクセスコントロールポートを設定するコマンドの説明を参照してください。

● 構文

config mac_based_access_control guest_vlan ports <portlist>

● パラメータ

<portlist>ポートをゲスト VLAN のメンバポートとして設定すると、そのポートの MAC ベースアクセスコントロール状態が有効な場合は、ポートがゲスト VLAN になります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 8 を MAC ベースアクセスコントロールのゲスト VLAN メンバとして設定するには：

```
Zxxx0:admin# config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

Zxxx0:admin#
```

41.6. config mac_based_access_control ports

● 概要

このコマンドを用いて、MAC ベースアクセスコントロール設定を指定します。ポートの MAC ベースアクセスコントロール機能が有効で、ポートが MAC ベースアクセスコントロールのゲスト VLAN メンバでない場合は、このポートに関連付けられたユーザは、認証されない限りトラフィックを転送できません。ユーザが認証されると、割り当てられた VLAN でトラフィックを転送できます。
ポートの MAC ベースアクセスコントロール機能が有効で、ポートが MAC ベースアクセスコントロールのゲスト VLAN メンバの場合は、ポートが元の VLAN メンバポートから削除され、MAC ベースアクセスコントロールのゲスト VLAN メンバポートに追加されます。認証プロセスが開始する前に、ユーザがゲスト VLAN でトラフィックを転送できます。認証プロセス後に、ユーザが割り当てられた VLAN にアクセスできます。
ポートの承認モードがポートベースモードの場合、ポートがいったん VLAN に承認されると、後続のユーザは再認証されません。後続のユーザは、現在承認されている VLAN で動作します。ポートの承認モードがホストベースモードの場合は、各ユーザが個々に承認され、それぞれに VLAN が割り当てられます。

● 構文

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-4000> | no_limit]}(1)

● パラメータ

<portlist>MAC ベースアクセスコントロール設定を指定するポートの範囲を指定します。	
all	すべてのポートを選択します。
state	MAC ベースアクセスコントロール機能を有効または無効に指定します。 enable MAC ベースアクセスコントロール機能を有効にします。 disable MAC ベースアクセスコントロール機能を無効にします。
aging_time	認証されたホストが認証を維持する期間を指定します。この期間がタイムアウトすると、ホストが認証されていない状態に戻ります。 infinite エージングタイムの期間を無制限に指定します。 <min 1-1440> エージアウトタイムを 1 ～ 1440 分に指定します。
block_time	ブロッキングタイムを 0 ～ 300 秒に指定します。 <second 0-300> ブロッキングタイムを指定します。ブロッキングタイムの値は 0 ～ 300 秒の必要があります。
max_users	最大ユーザ数を指定します。初期値は 1024 ユーザです。 <value 1-4000> 最大ユーザ数を 1 ～ 4000 の範囲で指定します。 no_limit 最大ユーザ数の 4000 まで制限なしに指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 8 のポート状態を設定するには：

```
Zxxx0:admin# config mac_based_access_control ports 1-8 state enable
Command: config mac_based_access_control ports 1-8 state enable

Success.

Zxxx0:admin#
```

41.7. create mac_based_access_control

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールのゲスト VLAN を作成します。

● 構文

create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]

● パラメータ

guest_vlan	ゲスト VLAN の名前を指定します。
<vlan_name 32>	ゲスト VLAN の名前を指定します。ゲスト VLAN の名前は 32 文字までです。
guest_vlanid	ゲスト VLAN の VLAN ID を指定します。
<vlanid 1-4094>	ゲスト VLAN の VLAN ID を指定します。ゲスト VLAN ID は 1 ～ 4094 の必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC ベースアクセスコントロールのゲスト VLAN を作成するには：

```
Zxxx0:admin#create mac_based_access_control guest_vlan default
Command: create mac_based_access_control guest_vlan default

Success.

Zxxx0:admin#
```

41.8. delete mac_based_access_control

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールのゲスト VLAN を削除します。

● 構文

delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid < vlanid 1-4094>]

● パラメータ

guest_vlan	ゲスト VLAN の名前を指定します。
<vlan_name 32>	ゲスト VLAN の名前を指定します。ゲスト VLAN の名前は 32 文字までです。
guest_vlanid	ゲスト VLAN の VLAN ID を指定します。
<vlanid 1-4094>	ゲスト VLAN の VLAN ID を指定します。ゲスト VLAN ID は 1 ～ 4094 の必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC ベースアクセスコントロールのゲスト VLAN を削除するには：

```
Zxxx0:admin#delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

Zxxx0:admin#
```

41.9. clear mac_based_access_control auth_state

● 概要

このコマンドを用いて、ユーザ（またはポート）の認証をクリアします。ポート（またはユーザ）が認証されていない状態に戻ります。ポート（またはユーザ）と関連付けられたすべてのタイマーがリセットされます。

● 構文

clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]

● パラメータ

ports	認証をクリアするポートの範囲を指定します。 all　すべてのポートを指定します。 <portlist> ポートの範囲を指定します。
mac_addr	指定したホストの認証をクリアします。 <macaddr> MAC アドレスを入力します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

すべてのポートの認証をクリアするには：

```
Zxxx0:admin#clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

Zxxx0:admin#
```

41.10. create mac_based_access_control_local mac

● 概要

このコマンドを用いて、データベースエントリを作成します。

● 構文

create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

● パラメータ

<macaddr>	ローカルモードでアクセスが認証される MAC アドレスを指定します。
vlan	（オプション）MAC アドレスが承認されると、ポートがこの VLAN に割り当てられます。 <vlan_name 32> VLAN の名前を 32 文字以内で指定します。
vlanid	（オプション）MAC アドレスが承認されると、ポートがこの VLAN ID に割り当てられます。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ローカルデータベースエントリを作成するには：

```
Zxxx0:admin#create mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

Zxxx0:admin#
```

41.11. config mac_based_access_control_local mac

● 概要

このコマンドを用いて、データベースエントリを変更します。

● 構文

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

● パラメータ

<macaddr>	ローカルモードでアクセスが認証される MAC アドレスを指定します。
vlan	MAC アドレスが承認されると、ポートが指定した VLAN に割り当てられます。 <vlan_name 32> VLAN の名前を 32 文字以内で指定します。
vlanid	MAC アドレスが承認されると、ポートが指定した VLAN ID に割り当てられます。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。
clear_vlan	指定した VLAN をクリアします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ローカルデータベースエントリを設定するには：

```
Zxxx0:admin#config mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

Zxxx0:admin#
```

41.12. config mac_based_access_control max_users

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールの認証ユーザの最大数を設定します。

● 構文

config mac_based_access_control max_users [<value 1-4000> | no_limit]

● パラメータ

<value 1-4000>	認証ユーザの最大数を指定します。
no_limit	最大ユーザ数の 4000 まで制限なしに指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC ベースアクセスコントロールの認証ユーザの最大数を設定するには：

```
Zxxx0:admin#config mac_based_access_control max_users 2
Command: config mac_based_access_control max_users 2

Success.

Zxxx0:admin#
```

41.13. config mac_based_access_control authorization attributes

● 概要

このコマンドを用いて、承認された設定の受け入れを有効または無効にします。RADIUS 認証による MAC ベースアクセスコントロールの認証が有効な場合、グローバル認証ステータスが有効なときは、RADUIS サーバにより認証された属性（VLAN、802.1p デフォルトプライオリティ、ACL など）を受け入れます。ローカル認証による MAC ベースアクセスコントロールの承認が有効な場合は、ローカルデータベースにより認証された属性を受け入れます。

● 構文

config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

● パラメータ

radius	RADIUS サーバにより認証された属性の受け入れの有効または無効を指定します。 enable 有効に指定すると、グローバル認証ステータスが有効なときは、RADUIS サーバにより認証された属性（VLAN、802.1p デフォルトプライオリティ、ACL など）を受け入れます。デフォルトの状態は有効です。 disable 無効に指定すると、グローバル認証ステータスが有効な場合でも、RADUIS サーバにより認証された属性（VLAN、802.1p デフォルトプライオリティ、ACL など）を受け入れません。
local	ローカルデータベースにより認証された属性を有効または無効に指定します。 enable 有効に指定すると、グローバル認証ステータスが有効なときは、ローカルデータベースにより認証された属性を受け入れます。デフォルトの状態は有効です。 disable 無効に指定すると、グローバル認証ステータスが有効な場合でも、ローカルデータベースにより認証された属性を受け入れません。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ローカルデータベースから承認された設定を無効にするには：

```
Zxxx0:admin#config mac_based_access_control authorization attributes local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

Zxxx0:admin#
```

41.14. delete mac_based_access_control_local

● 概要

このコマンドを用いて、データベースエントリを削除します。

● 構文

delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

● パラメータ

mac	MAC アドレスに基づいてデータベースを削除します。 <macaddr> MAC アドレスを入力します。
vlan	この VLAN 名に基づいてデータベースを削除します。 <vlan_name 32> VLAN の名前を 32 文字以内で指定します。
vlanid	この VLAN ID に基づいてデータベースを削除します。 <vlanid 1-4094> 指定する VLAN ID の値は 1 ～ 4094 の必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC アドレスに基づいて、ローカルの MAC ベースアクセスコントロールを削除するには：

```
Zxxx0:admin#delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

Zxxx0:admin#
```

VLAN 名に基づいて、ローカルの MAC ベースアクセスコントロールを削除するには：

```
Zxxx0:admin#delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

Zxxx0:admin#
```

41.15. show mac_based_access_control auth_state ports

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールの MAC 認証情報を表示します。

● 構文

show mac_based_access_control auth_state ports {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートを指定します。

● 制限

なし

● 実行例

MAC ベースアクセスコントロールの MAC 認証情報を表示するには：

```
Zxxx0:admin# show mac_based_access_control auth_state ports
Command: show mac_based_access_control auth_state ports

(P): Port-based    Prio: Priority

Port    MAC Address       Original  State       VID  Prio Aging Time/
                           RX VID                       Block Time
------ ------------------- ---- -------------- ---- ---- -----------
1      00-00-00-00-00-01    1    Authenticated  -    6    1439
1      00-00-12-00-03-00    1    Blocked        -    -    286
3      00-00-00-00-00-02(P) 1    Authenticated  -    6    1440

Total Authenticating Hosts  : 0
Total Authenticated Hosts   : 2
Total Blocked Hosts         : 1

Zxxx0:admin#
```

41.16. show mac_based_access_control

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールの情報を表示します。

● 構文

show mac_based_access_control {ports {<portlist>}}

● パラメータ

ports	（オプション）MAC ベースアクセスコントロールのポートの状態を表示します。 <portlist> 表示するポートの範囲を指定します。

● 制限

なし

● 実行例

MAC ベースアクセスコントロールの情報を表示するには：

```
Zxxx0:admin#show mac_based_access_control
Command: show mac_based_access_control

MAC-based Access Control
-----------------------------------
State                   : Disabled
Method                  : Local
Password Type           : Manual String
Password                : default
Max User                : No Limit
Guest VLAN              :
Guest VLAN Member Ports:
RADIUS Authorization    : Enabled
Local Authorization     : Enabled
Trap State              : Enabled
Log State               : Enabled

Zxxx0:admin#
```

ポート 1 ～ 4 の MAC ベースアクセスコントロールの情報を表示するには：

```
Zxxx0:admin#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4


Port    State     Aging Time   Block Time  Max User
                    (min)        (sec)
-----  --------   ----------   ---------   --------
1      Disabled   1440         300         1024
2      Disabled   1440         300         1024
3      Disabled   1440         300         1024
4      Disabled   1440         300         1024

Zxxx0:admin#
```

41.17. show mac_based_access_control_local

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールのローカルデータを表示します。

● 構文

show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

● パラメータ

mac	（オプション）この MAC アドレスに基づいて、MAC ベースアクセスコントロールのローカルデータベースを表示します。 <macaddr> MAC アドレスを入力します。
vlan	（オプション）VLAN を指定します。 <vlan_name 32> VLAN の名前を 32 文字以内で指定します。
vlanid	（オプション）VLAN ID を指定します。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID 値を指定します。

● 制限

なし

● 実行例

MAC ベースアクセスコントロールのローカルデータを表示するには：

```
Zxxx0:admin#show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address             VID
-----------------       ------
00-00-00-00-00-01       1

Total Entries:1

Zxxx0:admin#
```

MAC アドレスに基づいて、MAC ベースアクセスコントロールのローカルデータを表示するには：

```
Zxxx0:admin#show mac_based_access_control_local mac 00-00-00-00-00-01
Command: show mac_based_access_control_local mac 00-00-00-00-00-01

MAC Address         VID
-----------------   ------
00-00-00-00-00-01   1

Total Entries:1

Zxxx0:admin#
```

VLAN に基づいて、MAC ベースアクセスコントロールのローカルデータを表示するには：

```
Zxxx0:admin#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address          VID
-----------------    ------
00-00-00-00-00-01    1

Total Entries: 1

Zxxx0:admin#
```

41.18. config mac_based_access_control log state

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールのログの生成を有効または無効にします。

● 構文

config mac_based_access_control log state [enable | disable]

● パラメータ

state	MAC ベースアクセスコントロールのログの状態を指定します。 enable MAC ベースアクセスコントロールのログを有効にします。 disable MAC ベースアクセスコントロールのログを無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC ベースアクセスコントロールのログの状態を無効にするには：

```
Zxxx0:admin# config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable

Success.

Zxxx0:admin#
```

41.19. config mac_based_access_control trap state

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールのトラップ送信を有効または無効にします。

● 構文

config mac_based_access_control trap state [enable | disable]

● パラメータ

state	MAC ベースアクセスコントロールのトラップの状態を指定します。 enable MAC ベースアクセスコントロールのトラップの状態を有効にします。 disable MAC ベースアクセスコントロールのトラップの状態を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MAC ベースアクセスコントロールのトラップの状態を有効にするには：

```
Zxxx0:admin# config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

Zxxx0:admin#
```

41.20. config mac_based_access_control password_type

● 概要

このコマンドを用いて、MAC ベースアクセスコントロールの RADIUS 認証のパスワードのタイプを設定します。

● 構文

config mac_based_access_control password_type [manual_string | client_mac_address]

● パラメータ

manual_string	すべてのクライアントの RADIUS 認証に、同じ文字列をパスワードとして使用します。この文字列は config mac_based_access_control password コマンドを用いて設定できます。
client_mac_address	RADIUS 認証に、クライアントの MAC アドレスをパスワードとして使用します。MAC アドレスの形式は config authentication mac_format コマンドを用いて設定できます。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

クライアントの MAC アドレスを認証パスワードとして用いる MAC ベースアクセスコントロールを設定するには：

```
Zxxx0:admin# config mac_based_access_control password_type client_mac_address
Command: config mac_based_access_control password_type client_mac_address

Success.

Zxxx0:admin#
```

manual_string を認証パスワードとして用いる MAC ベースアクセスコントロールを設定するには：

```
Zxxx0:admin# config mac_based_access_control password_type manual_string
Command: config mac_based_access_control password_type manual_string

Success.

Zxxx0:admin#
```

42. ミラーコマンド

指定したポートの送受信パケットを別のポートにミラーリング（コピー）し、パケットの内容をモニターすることができます。複数のポートをミラーグループに設定し送受信パケットを一括してのミラーリング、送信パケットのみまたは受信パケットのみをミラーリングする設定を行えます。

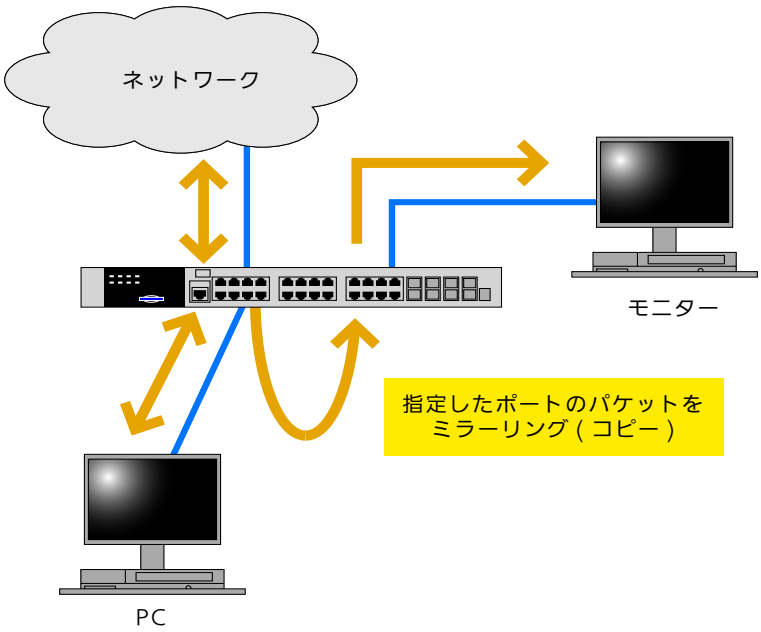


図 42-1　ミラーリングの概要

create mirror group_id <value 1-4>
config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}
config mirror group_id <value 1-4> {target_port <port> | [add | delete] source ports <portlist> [rx | tx | both] | state [enable | disable]}(1)
delete mirror group_id <value 1-4>
enable mirror
disable mirror
show mirror {group_id <value 1-4>}

42.1.　create mirror group_id

● 概要

このコマンドを用いて、ミラーグループを作成します。

● 構文

create mirror group_id <value 1-4>

● パラメータ

<value 1-4> 使用するミラーグループ ID を入力します。この値は 1 ～ 4 の必要があります。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ミラーグループ 3 を作成するには：

```
Zxxx0:admin# create mirror group_id 3
Command: create mirror group_id 3

Success.

Zxxx0:admin#
```

42.2. config mirror port

● 概要

このコマンドを用いて、任意の範囲のポートのすべてのトラフィックを、指定したポートに送信することを認証します。このポートでは、ネットワークスニファまたは他の装置がネットワークトラフィックを監視できます。さらに、受信のみ、送信のみ、または送受信両方のトラフィックをミラーリング先ポートにミラーリングするように指定できます。

NOTE Tx 方向のミラーリングパケットには受信した VLAN ID の VLAN タグが付加されます。

● 構文

config mirror port <port> {[add |delete] source ports <portlist> [rx | tx | both]}

● パラメータ

<port>	ミラーポートにコピーされるパケットを受信するポートを指定します。
add	（オプション）追加するミラーエントリを指定します。
delete	（オプション）削除するミラーエントリを指定します。
source ports	（オプション）ミラーリングされるポートを指定します。このポートに出入りするすべてのパケットをミラーポートにコピーできます。 <portlist> 設定するポートの範囲を指定します。
rx	（オプション）ポートリストのポートで受信するパケットのみのミラーリングを認証します。
tx	（オプション）ポートリストのポートで送信するパケットのみのミラーリングを認証します。
both	（オプション）ポートリストのポートで受信または送信するすべてのパケットをミラーリングします。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ミラーリング先ポート 6、ミラーリング元ポート 1 ～ 5、および送受信両方のパケットのミラーリングを追加するには：

```
Zxxx0:admin#config mirror port 6 add source ports 1-5 both
Command: config mirror port 6 add source ports 1-5 both

Success.

Zxxx0:admin#
```

42.3. config mirror group_id

● 概要

このコマンドを用いて、ミラーグループのパラメータを設定します。ミラーグループのミラーリング先ポート、状態、ミラーリング元ポートを設定できます。ミラーリング先ポートを、すべてのミラーグループのミラーリング元ポートのメンバにすることはできません。各ミラーグループのミラーリング先ポートを同じポートにすることができます。しかし、各ミラーグループのミラーリング元ポートを重複させることはできません。

● 構文

config mirror group_id <value 1-4> {target_port <port> | [add | delete] source ports <portlist> [rx | tx | both] | state [enable | disable]}

● パラメータ

<value 1-4>	使用するミラーグループ ID を入力します。この値は 1 ～ 4 の必要があります。
target_port	（オプション）ミラーポートにコピーされるパケットを受信するポートを指定します。 <port> 使用するミラーリング先ポート番号を入力します。
add	（オプション）追加するミラーリング元ポートを指定します。
delete	（オプション）削除するミラーリング元ポートを指定します。
source	（オプション）使用するミラーリング元ポートを指定します。
ports	（オプション）ミラーリング元ポートとして使用するポートのリストを指定します。 <portlist> ミラーリング元ポートとして使用するポートのリストを入力します。
rx	（オプション）ミラーグループのミラーリング元ポートで受信したパケットのみが、ミラーグループのミラーリング先ポートにミラーリングされます。
tx	（オプション）ミラーグループのミラーリング元ポートから送信したパケットのみが、ミラーグループのミラーリング先ポートにミラーリングされます。

both	（オプション）ミラーグループのミラーリング元ポートで受信および送信した両方のパケットが、ミラーグループのミラーリング先ポートにミラーリングされます。
state	（オプション）ミラーグループの状態を指定して、ミラーグループ機能を有効または無効にします。 enable ミラーグループの状態が有効になります。 disable ミラーグループの状態が無効になります。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ミラーグループ 2 の状態を有効に設定し、ミラーリング元ポート 4 ～ 9 を追加するには：

```
Zxxx0:admin# config mirror group_id 2 state enable add source ports 4-9 both
Command: config mirror group_id 2 state enable add source ports 4-9 both

Success.

Zxxx0:admin#
```

42.4. delete mirror group_id

● 概要

このコマンドを用いて、本装置のミラーグループを削除します。

● 構文

delete mirror group_id <value 1-4>

● パラメータ

<value 1-4>	使用するミラーグループ ID を入力します。この値は 1 ～ 4 の必要があります。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ミラーグループ 3 を削除するには：

```
Zxxx0:admin# delete mirror group_id 3
Command: delete mirror group_id 3

Success.

Zxxx0:admin#
```

42.5. enable mirror

● 概要

このコマンドを以下の disable mirror コマンドと組み合わせて、ミラーセッションの設定を変更せずに、ミラー機能を有効または無効にすることができます。

NOTE ミラーリング先ポートが設定されていない場合は、enable mirror は適用されません。

● 構文

enable mirrorg

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ミラーリング設定を有効にするには：

```
Zxxx0:admin#enable mirror
Command: enable mirror

Success.

Zxxx0:admin#
```

42.6. disable mirror

● 概要

このコマンドを上記の enable mirror コマンドと組み合わせて、ミラーセッションの設定を変更せずに、ミラー機能を有効または無効にすることができます。

● 構文

disable mirror

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ミラーリング設定を無効にするには：

```
Zxxx0:admin#disable mirror
Command: disable mirror

Success.

Zxxx0:admin#
```

42.7. show mirror

● 概要

このコマンドを用いて、スイッチの現在のポートのミラーリング設定を表示します。

● 構文

show mirror {group_id <value 1-4>}

● パラメータ

group_id（オプション）表示に用いるグループ ID を指定します。	
<value 1-4>	表示に用いるグループ ID を入力します。この値は 1 ～ 4 の必要があります。

● 制限

なし

● 実行例

ミラーリング設定を表示するには：

```
Zxxx0:admin#show mirror
Command: show mirror

 Mirror Global State:   Disabled

 Group   State      Target Port   Source Ports
 ------- ---------- ------------- ------------------------------------------------
 1       Enabled    1             RX: 2-3
                                  TX: 2-3

Zxxx0:admin#
```

43. MLD snooping コマンド

MLD（Multicast Listener Discovery）は、IPv6 環境でマルチキャストグループを管理するプロトコルです。IPv4 における IGMP と同等のプロトコルになります。
MLD snoopingとは、スイッチの各ポートを流れるMLDパケットを監視し、不要なポートにデータが流れないようにフィルタリングする機能です。この防止機能により、動画配信などの大容量データを効率良く処理できます。

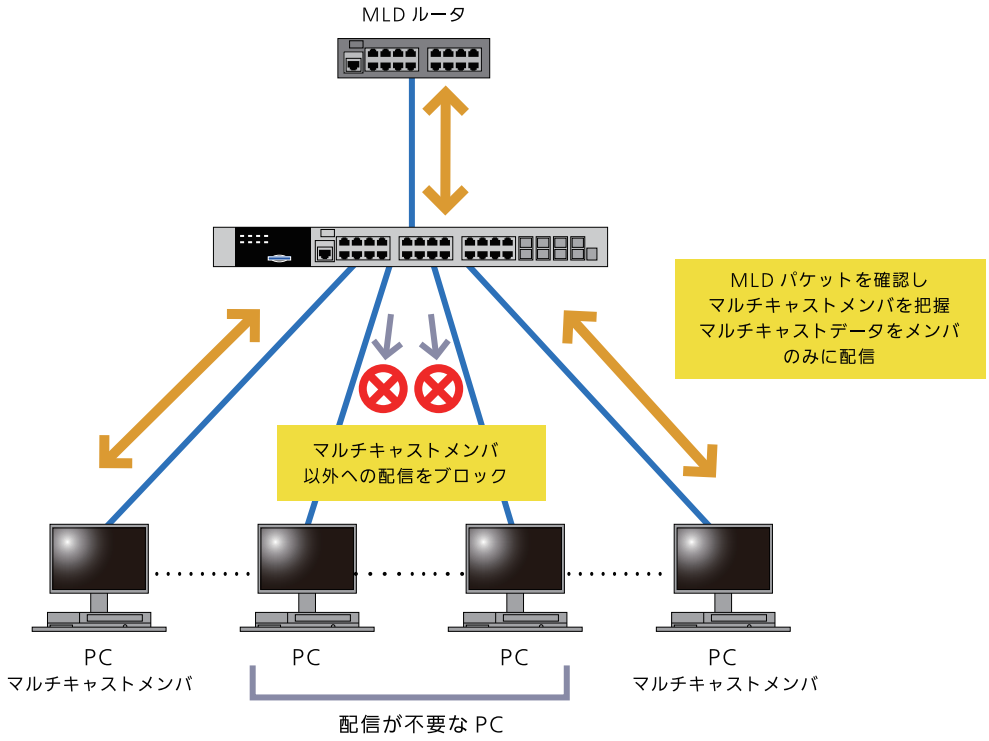


図 43-1　MLD Snooping の概略

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | proxy_reporting {state [enable | disable]| source_ip <ipv6addr>}(1)}
config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]
create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>
delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}
show mld_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]
clear mld_snooping statistics counter
config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)
config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
enable mld_snooping
disable mld_snooping
show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list >]}
show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}}
show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
config mld_snooping unknow_data_learning [all | vlan_name <vlan_name 32> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}
config mld_snooping unknow_data_learning max_learned_entry <value 1-1024>
clear mld_snooping data_learning_group [all | [vlan_name <vlan_name 32> | vlanid <vlanid_list>] [<ipv6addr> | all]]

43.1. config mld_snooping

● 概要

このコマンドを用いて、本装置の MLD snooping を設定します。

● 構文

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | proxy_reporting {state [enable | disable] | source_ip <ipv6addr>}(1)}

● パラメータ

vlan_name	MLD snooping を設定する VLAN の名前を指定します。 **<vlan_name 32>** VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	VLAN ID のリストを指定します。 **<vlanid_list>** VLAN ID のリストを指定します。
all	すべての VLAN を設定します。
state	選択した VLAN の MLD snooping を有効または無効にします。 **enable** 選択した VLAN の MLD snooping を有効にします。 **disable** 選択した VLAN の MLD snooping を無効にします。

fast_done	MLD snooping の高速脱退機能を有効または無効にします。有効にすると、システムが MLD Leave メッセージを受信すると即座にメンバシップが削除されます。 enable MLD snooping の高速脱退機能を有効にします。 disable MLD snooping の高速脱退機能を無効にします。
proxy_reporting	プロキシレポート機能を設定します。 state プロキシレポート機能の状態を指定します。 enableプロキシレポート機能を有効にします。 disableプロキシレポート機能を無効にします。
source_ip	使用する送信元 IPv6 アドレスを指定します。 <ipv6addr> 使用する送信元 IPv6 アドレスを入力します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MLD snooping を設定するには：

```
Zxxx0:admin#config mld_snooping vlan_name default state enable
Command: config mld_snooping vlan_name default state enable

Success.

Zxxx0:admin#
```

43.2. config mld_snooping rate_limit

● 概要

このコマンドを用いて、入力 MLD 制御パケットの 1 秒当たりの上限を設定します。

● 構文

config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

● パラメータ

ports	設定するポートの範囲を指定します。 <portlist> 設定するポートの範囲を指定します。

vlanid	設定する VLAN の範囲を指定します。 <vlanid_list> VLAN ID のリストを指定します。
<value 1-1000>	特定のポート /VLAN について、本装置が処理できる MLD 制御パケットのレートの制限を指定します。レートはパケット / 秒で指定します。レートの制限を超えたパケットは破棄されます。
no_limit	デフォルト設定は制限なしです。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 の MLD snooping パケットのレート制限を 100pps に設定するには：

```
Zxxx0:admin#config mld_snooping rate_limit ports 1 100
Command: config mld_snooping rate_limit ports 1 100

Success.

Zxxx0:admin#
```

43.3. show mld_snooping rate_limit

● 概要

このコマンドを用いて、MLD snooping のレート制限の設定を表示します。

● 構文

show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

● パラメータ

ports	表示するポートの範囲を指定します。 <portlist> 表示するポートの範囲を指定します。
vlanid	表示する VLAN の範囲を指定します。 <vlanid_list> VLAN ID のリストを指定します。

● 制限

なし

● 実行例

ポート 1 ～ 2 の MLD snooping パケットのレート制限を表示するには：

```
Zxxx0:admin#show mld_snooping rate_limit ports 1-2
Command: show mld_snooping rate_limit ports 1-2

 Port      Rate Limit
--------  ------------
1              No Limit
2              No Limit

Total Entries: 2
Zxxx0:admin#
```

43.4. create mld_snooping static_group

● 概要

このコマンドを用いて、MLD snooping のマルチキャストスタティックグループを作成します。スタティックグループにメンバポートを追加できます。グループのメンバポートは、スタティックメンバポートとダイナミックメンバポートにより構成されます。
スタティックグループは、VLAN の MLD snooping が有効な場合のみ有効になります。このようなスタティックメンバポートの場合、装置がクエリアに対する MLD プロトコルの動作をエミュレートして、マルチキャストグループ宛てのトラフィックをメンバポートに転送します。レイヤ 3 装置の場合、この特定のグループ宛てのパケットをスタティックメンバポートにルーティングする役目も持ちます。スタティックメンバポートは MLD v2 の動作のみに影響します。予約された IP マルチキャストアドレス FF0x::/16 は、設定されたグループから除外する必要があります。スタティックグループを作成する前に、まず、VLAN を作成する必要があります。

● 構文

create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

● パラメータ

vlan	スタティックグループを配置する VLAN の名前を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	VLAN ID のリストを指定します。 <vlanid_list> VLAN ID のリストを指定します。
<ipv6addr> マルチキャストグループの IPv6 アドレスを指定します。	

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

vlan1、グループ FF1E::1 に、MLD snooping のスタティックグループを作成するには：

```
Zxxx0:admin#create mld_snooping static_group vlan vlan1 FF1E::1
Command: create mld_snooping static_group vlan vlan1 FF1E::1

Success.

Zxxx0:admin#
```

43.5. config mld_snooping static_group

● 概要

このコマンドを用いて、本装置の MLD snooping のスタティックグループを設定します。ポートをスタティックメンバポートとして設定すると、そのポートでは MLD プロトコルが動作しません。従って、ポートを MLD によって学習されるダイナミックメンバポートとみなします。後でこのポートをスタティックメンバとして設定すると、このポートでは MLD プロトコルの動作が停止します。このポートをスタティックメンバポートから削除すると、MLD プロトコルの動作が再開します。スタティックメンバポートは MLD v1 の動作のみに影響します。

● 構文

config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>

● パラメータ

vlan	スタティックグループを配置する VLAN の名前を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	スタティックグループを配置する VLAN の ID を指定します。 <vlanid_list> VLAN ID のリストを指定します。
<ipv6addr>	マルチキャストグループの IPv6 アドレスを指定します（レイヤ 3 スイッチの場合）。
add	メンバポートを追加します。
delete	メンバポートを削除します。
<portlist>	設定するポートの範囲を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

デフォルト VLAN のグループ FF1E::1 について、ポート 9 ～ 10 を MLD snooping のスタティックメンバポートから削除するには：

```
Zxxx0:admin#config mld_snooping static_group vlan default FF1E::1 delete 9-10
Command: config mld_snooping static_group vlan default FF1E::1 delete 9-10

Success.

Zxxx0:admin#
```

43.6. delete mld_snooping static_group

● 概要

このコマンドを用いて、本装置の MLD snooping のスタティックグループを削除します。MLD snooping のスタティックグループを削除しても、グループの MLD snooping のダイナミックメンバポートには影響しません。

● 構文

delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

● パラメータ

vlan	スタティックグループを配置する VLAN の名前を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	スタティックグループを配置する VLAN の ID を指定します。 <vlanid_list> VLAN ID のリストを指定します。
<ipv6addr> マルチキャストグループの IPv6 アドレスを指定します（レイヤ 3 スイッチの場合）。	

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

デフォルト VLAN のグループ FF1E::1 から、MLD snooping のスタティックグループを削除するには:

```
Zxxx0:admin#delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

Zxxx0:admin#
```

43.7. show mld_snooping static_group

● 概要

このコマンドを用いて、MLD snooping のスタティックグループを表示します。

● 構文

show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}

● パラメータ

vlan	（オプション）スタティックグループを配置する VLAN の名前を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）スタティックグループを配置する VLAN の ID を指定します。 <vlanid_list> VLAN ID のリストを指定します。
<ipv6addr>	（オプション）マルチキャストグループの IPv6 アドレスを指定します（レイヤ 3 スイッチの場合）。

● 制限

なし

● 実行例

すべての MLD snooping のスタティックグループを表示するには：

```
Zxxx0:admin#show mld_snooping static_group
Command: show mld_snooping static_group

VLAN ID/Name       IP Address       Static Member Ports
-------------    ---------------  ----------------------
1/Default          FF1E::1          9-10

Total Entries : 1

Zxxx0:admin#
```

43.8. show mld_snooping statistic counter

● 概要

このコマンドを用いて、MLD snooping の統計カウンタを表示します。これは、MLD snooping が有効になって以降、本装置が送信または受信した MLD プロトコルパケットについてのカウンタです。

● 構文

show mld_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]

● パラメータ

vlan	表示する VLAN を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	表示する VLAN のリストを指定します。 <vlanid_list> VLAN ID のリストを指定します。
ports	表示するポートのリストを指定します。 <portlist> ポートのリストを指定します。

● 制限

なし

● 実行例

ポート 1 について、MLD snooping の統計カウンタを表示するには：

```
Zxxx0:admin#show mld_snooping statistic counter ports 1
Command: show mld_snooping statistic counter ports 1

Port #           : 1
--------------------------------------------------
Group Number     : 0

Receive Statistics
    Query
      MLD v1 Query                    : 0
      MLD v2 Query                    : 0
      Total                           : 0
      Dropped By Rate Limitation       : 0
     Dropped By Multicast VLAN        : 0

     Report & Done
      MLD v1 Report                    : 0
      MLD v2 Report                    : 0
      MLD v1 Done                      : 0
      Total                            : 0
      Dropped By Rate Limitation        : 0
      Dropped By Max Group Limitation   : 0
      Dropped By Group Filter           : 0
      Dropped By Multicast VLAN         : 0

Transmit Statistics
    Query
      MLD v1 Query                    : 0
      MLD v2 Query                    : 0
      Total                           : 0

     Report & Done
      MLD v1 Report                    : 0
      MLD v2 Report                    : 0
      MLD v1 Done                      : 0
      Total                            : 0

 Total Entries : 1

Zxxx0:admin#
```

43.9. clear mld_snooping statistics counter

● 概要

このコマンドを用いて、MLD snooping の統計カウンタをクリアします。

● 構文

clear mld_snooping statistics counter

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MLD snooping の統計カウンタをクリアするには：

```
Zxxx0:admin#clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter

Success.

Zxxx0:admin#
```

43.10. config mld_snooping querier

● 概要

このコマンドを用いて、一般的なクエリの転送間隔、リスナからのレポートを待つ最大時間、および MLD snooping を保証する許容パケット損失を秒単位の時間で設定します。

● 構文

config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>} (1)

● パラメータ

vlan_name
MLD snooping クエリアを設定する VLAN の名前を指定します。
<vlan_name 32>
VLAN の名前を指定します。最大文字数は 32 文字です。

vlanid MLD snooping クエリアを設定する VLAN の ID を指定します。
<vlanid_list>
VLAN ID のリストを指定します。

all MLD snooping クエリアを設定する VLAN として、すべての VLAN を指定します。

query_interval
一般的なクエリ転送間隔を秒単位で指定します。
<sec 1-65535>
一般的なクエリ転送間隔を秒単位で指定します。デフォルト設定は 125 秒です。

max_response_time
メンバからのレポートを待つ最大時間を秒単位で指定します。
<sec 1-25>
メンバからのレポートを待つ最大時間を秒単位で指定します。デフォルト設定は 10 秒です。

robustness_variable
サブネットの予期されるパケット損失に対して微調整します。この robustness_variable の値を用いて、以下の MLD メッセージの間隔を計算します。
- グループメンバの間隔－この時間が過ぎると、マルチキャストルータが、ネットワークにグループのメンバがないと判断します。この間隔は次のように計算します。（robustness_variable×query_interval）+（1×query_response_interval)。
- 他のクエリアの存在間隔－この時間が過ぎると、マルチキャストルータが、クエリアである別のマルチキャストルータが存在しないと判断します。この間隔は次のように計算します。（robustness_variable×query_interval）+（0.5×query_response_interval)。
- 最後のメンバのクエリ数－グループ固有の送信クエリ数で、これを超えるとルータがグループのローカルメンバがないと判断します。デフォルトの数は、robustness_variable の値です。

<value 1-7>
1 ～ 7 の値を指定します。サブネットの損失が大きいと考えられる場合は、値を大きくします。デフォルトの robustness_variable の値は 2 です。

last_member_query_interval
グループ固有のクエリメッセージ間隔の最大時間を指定します。グループ脱退メッセージの応答として送信されたメッセージも含まれます。ルータがグループの最後のメンバの脱退を検出するために必要な時間を短縮したい場合は、この間隔を短くしてみてください。
<sec 1-25>
1 ～ 25 秒の時間を指定します。

state スイッチを MLD クエリア（MLD クエリパケットを送信する）または非クエリア（MLD クエリパケットを送信しない）と指定します。有効または無効に設定します。
enable
スイッチを MLD クエリア（MLD クエリパケットを送信する）として選択できます。
disable
無効にすると、スイッチがクエリアとしての役割を実行できません。

version ポートから送信する MLD パケットのバージョンを指定します。インターフェースが受信する MLD パケットのバージョンが、指定したバージョンよりも高い場合は、このパケットがルータポートから転送されるか、フラッディングされます。
<value 1-2>
1 ～ 2 の値を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MLD snooping クエリアを設定するには：

```
Zxxx0:admin#config mld_snooping querier vlan_name default query_interval 125 state
enable
Command: config mld_snooping querier vlan_name default query_interval 125 state
enable

Success.

Zxxx0:admin#
```

43.11. config mld_snooping mrouter_ports

● 概要

このコマンドを用いて、マルチキャストが有効なルータに接続するポートの範囲をユーザが指定できます。これにより、プロトコルに関係なく、このようなルータを宛先とするすべてのパケットが、マルチキャストが有効なルータに確実に到達します。

● 構文

config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

● パラメータ

vlan	ルータポートが配置される VLAN の名前を指定します。 <vlan_name 32> ルータポートが配置される VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	ルータポートが配置される VLAN の ID を指定します。 <vlanid_list> VLAN ID のリストを指定します。
add	ルータポートを追加します。
delete	ルータポートを削除します。
<portlist>	設定するポートの範囲を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スタティックルータポートを設定するには：

```
Zxxx0:admin#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

Zxxx0:admin#
```

43.12. config mld_snooping mrouter_ports_forbidden

● 概要

このコマンドを用いて、マルチキャストが有効なルータに接続されないポートの範囲を指定できます。これにより、禁止されたルータポートはルーティングパケットを伝搬しません。

● 構文

config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

● パラメータ

vlan	ルータポートが配置される VLAN の名前を指定します。 <vlan_name 32> ルータポートが配置される VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	ルータポートが配置される VLAN の ID を指定します。 <vlanid_list> VLAN ID のリストを指定します。
add	ルータポートを追加します。
delete	ルータポートを削除します。
<portlist>	設定するポートの範囲を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポートを禁止されたルータポートとして設定するには：

```
Zxxx0:admin#config mld_snooping mrouter_ports_forbidden vlan default add 1-10
Command: config mld_snooping mrouter_ports_forbidden vlan default add 1-10

Success.

Zxxx0:admin#
```

43.13. enable mld_snooping

● 概要

このコマンドを用いて、スイッチの MLD snooping を有効にします。

● 構文

enable mld_snooping

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチの MLD snooping を有効にするには：

```
Zxxx0:admin#enable mld_snooping
Command: enable mld_snooping

Success.

Zxxx0:admin#
```

43.14. disable mld_snooping

● 概要

このコマンドを用いて、スイッチの MLD snooping を無効にします。MLD snooping を無効にできるのは、IPv6 マルチキャストルーティングを使用していない場合のみです。MLD snooping を無効にすると、すべての MLD および IPv6 マルチキャストトラフィックが所定の IPv6 インターフェース内にフラッディングされます。

● 構文

disable mld_snooping

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチの MLD snooping を無効にするには：

```
Zxxx0:admin#disable mld_snooping
Command: disable mld_snooping

Success.

Zxxx0:admin#
```

43.15. show mld_snooping

● 概要

このコマンドを用いて、スイッチの現在の MLD snooping 設定を表示します。

● 構文

show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

● パラメータ

vlan	（オプション）MLD snooping 設定を表示する VLAN の名前を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。

vlanid	（オプション）MLD snooping 設定を表示する VLAN の ID を指定します。 <vlanid_list> VLAN ID のリストを指定します。

NOTE パラメータを指定しない場合、システムにより現在のすべての MLD snooping 設定が表示されます。

● 制限

なし

● 実行例

MLD snooping を表示するには：

```
Zxxx0:admin#show mld_snooping
Command: show mld_snooping

 MLD Snooping Global State               : Disabled
 Unknown Data Learning Max Entries       : 50

 VLAN Name                           : default
 Query Interval                      : 125
 Max Response Time                   : 10
 Robustness Value                    : 2
 Last Listener Query Interval        : 1
 Querier State                       : Disabled
 Querier Role                        : Non-Querier
 Querier IP                          : ::
 Querier Expiry Time                 : 0 secs
 State                               : Disabled
 Fast Done                           : Disabled
 Rate Limit                          : No Limitation
 Proxy Reporting                     : Disabled
 Proxy Reporting Source IP           : ::
 Version                             : 2
 Unknown Data Learning State         : Enabled
 Unknown Data Learning Aged Out      : Disabled
 Data Learning Group Expiry Time     : 260

Total Entries: 1

Zxxx0:admin#
```

43.16. show mld_snooping group

● 概要

このコマンドを用いて、スイッチの現在の MLD snooping のグループ情報を表示します。

● 構文

show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}}

● パラメータ

vlan	（オプション）MLD snooping のグループ情報を表示する VLAN の名前を指定します。VLAN、ポートおよび IP アドレスを指定しない場合、現在のすべての MLD snooping のグループ情報が表示されます。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）MLD snooping のグループ情報を表示する VLAN の ID を指定します。 <vlanid_list> VLAN ID のリストを指定します。
ports	（オプション）MLD snooping のグループ情報を表示するポートのリストを指定します。 <portlist> 表示するポートの範囲を指定します。
<ipv6addr>	（オプション）MLD snooping のグループ情報を表示するグループの IPv6 アドレスを指定します。

● 制限

なし

● 実行例

MLD snooping のグループを表示するには：

```
Zxxx0:admin#show mld_snooping group
Command: show mld_snooping group
Source/Group         : 2001::1/FE1E::1
VLAN Name/VID        :default/1
Member Ports         : 1-2
UP Time              : 26
Expiry Time         : 258
Filter Mode          : INCLUDE

Source/Group         : 2002::2/FE1E::1
VLAN Name/VID:       : default/1
Member Ports         : 3
UP Time              : 29
Expiry Time         : 247
Filter Mode          : EXCLUDE

Source/Group         : NULL/FE1E::2
VLAN Name/VID        : default/1
Member Ports         : 4-5
UP Time              : 40
Expiry Time         : 205
Filter Mode          : EXCLUDE

Total Entries : 3

Zxxx0:admin#
```

43.17. show mld_snooping mrouter_ports

● 概要

このコマンドを用いて、スイッチのルータポートを表示します。

● 構文

show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

● パラメータ

vlan	ルータポートが配置される VLAN の名前を指定します。 <vlan_name 32> ルータポートが配置される VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	ルータポートが配置される VLAN の ID を指定します。 <vlanid_list> VLAN ID のリストを指定します。
all	ルータポートが配置されているすべての VLAN を指定します。
static	（オプション）スタティックに設定されているルータポートを表示します。
dynamic	（オプション）ダイナミックに学習されたルータポートを表示します。
forbidden	（オプション）スタティックに設定されている禁止されたルータポートを表示します。

NOTE パラメータを指定しない場合、本装置のすべてのルータポートが表示されます。

● 制限

なし

● 実行例

ルータポートを表示するには：

```
Zxxx0:admin#show mld_snooping mrouter_ports all
Command: show mld_snooping mrouter_ports all

VLAN Name               : default
Static Router Port      :
Dynamic Router Port     :
Router IP               :
Forbidden Router Port   :

Total Entries: 1

Zxxx0:admin#
```

43.18. show mld_snooping forwarding

● 概要

このコマンドを用いて、スイッチの現在の MLD snooping フォワーディングテーブルを表示します。これにより、特定の送信元から送信されたマルチキャストグループが転送されるポートのリストを確認できます。

● 構文

show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

● パラメータ

vlan	（オプション）MLD snooping フォワーディングテーブルの情報を表示する VLAN の名前を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）MLD snooping フォワーディングテーブルの情報を表示する VLAN の ID を指定します。 <vlanid_list> VLAN ID のリストを指定します。

NOTE パラメータを指定しない場合、現在設定されているすべての MLD snooping フォワーディングエントリが表示されます。

● 制限

なし

● 実行例

スイッチにあるすべての MLD snooping フォワーディングエントリを表示するには：

```
Zxxx0:admin#show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name     : default
Source IP     : 2001::1
Multicast Group: FE1E::1
Port Member   : 2,7

VLAN Name     : default
Source IP     : 2001::1
Multicast Group: FE1E::2
Port Member   : 5

Total Entries: 2

Zxxx0:admin#
```

43.19. config mld_snooping unknow_data_learning

● 概要

このコマンドを用いて、unknow data learning の状態を指定します。
unknow data learning が対象の VLAN にて有効の場合は、IP マルチキャストパケットの受信により MLD snooping グループが学習されます。無効の場合は MLD メンバーシップレポートが受信された場合のみ MLD snooping グループが学習されます。本機能で学習されたグループについては、エージアウトの有無を設定することができます。
unknow data learning が有効かつグループテーブルのエントリが上限に達していない場合は、マルチキャストフィルタリング設定に基づきマルチキャストパケットがルータポートへ転送されます。

NOTE unknow data learning グループ作成後に対象ポートが MDL メンバーとなった場合は通常の MLD グループのメンバーとして登録されます。

● 構文

config mld_snooping unknow_data_learning [all | vlan_name <vlan_name 32> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}

● パラメータ

all	すべての VLAN を指定します。
vlan_name	VLAN 名を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	VLAN ID を指定します。 <vlanid_list> VLAN ID リストを指定します。
state	（オプション）unknow data learning の状態を指定します。 enable unknow data learning を有効にします。 disable unknow data learning を無効にします。
aged_out	（オプション）エントリのエージアウト処理の有無を指定します。 enable エントリのエージアウトを有効にします。 disable エントリのエージアウトを無効にします。

expiry_time
（オプション）unknow data learning グループの生存時間指定します。エージアウトが有効な場合のみ有効です。
<sec 1-65535>
1 ～ 65535 の値を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

default VLAN 上の MLD snooping グループの unknow data learning を有効にするには：

```
Zxxx0:admin#config mld_snooping unknow_data_learning vlan_name default state
enable aged_out enable expiry_time 260
Command: config mld_snooping unknow_data_learning vlan_name default state enable
aged_out enable expiry_time 260

Success.

Zxxx0:admin#
```

43.20. config mld_snooping unknow_data_learning max_learned_entry

● 概要

このコマンドを用いて、unknow data learning により学習可能なグループ数を指定します。
テーブルが上限に達した場合は、新規の unknow data learning グループ学習を停止します。本グループのトラフィックは、マルチキャストフィルタリング設定に基づき転送されます。

● 構文

config mld_snooping unknow_data_learning max_learned_entry <value 1-1024>

● パラメータ

<value 1-1024>
unknown data learning による学習可能なグループの最大値。1 ～ 1024 の値を指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

unknow data learning による学習可能なグループの最大数を設定するには：

```
Zxxx0:admin#config mld_snooping unknow_data_learning max_learned_entry 50
Command: config mld_snooping unknow_data_learning max_learned_entry 50

Success.

Zxxx0:admin#
```

43.21. clear mld_snooping data_learning_group

● 概要

このコマンドを用いて、unknow data learning で学習された MLD snooping グループの削除を行います。

● 構文

clear mld_snooping data_learning_group [all | [vlan_name <vlan_name 32> | vlanid <vlanid_list>] [<ipv6addr> | all]]

● パラメータ

all	すべての unknow data learning グループを指定します。
vlan_name	VLAN 名を指定します。 <vlan_name 32> VLAN 名を指定します。32 文字以内で設定します。
vlanid	VLAN ID を指定します。 <vlanid_list> VLAN ID リストを指定します。
<ipv6addr>	IGMP snooping グループの IPv6 アドレスを指定します。
all	すべての IGMP snooping グループを指定します。

● 制限

このコマンドは、管理者レベル、オペレータレベル、パワーユーザレベルのユーザのみ実行できます。

● 実行例

unknow data learning で学習されたグループを削除するには：

```
Zxxx0:admin#clear mld_snooping data_learning_group all
Command: clear mld_snooping data_learning_group all


Success.

Zxxx0:admin#
```

44. コマンドプロンプト変更コマンド

コマンドラインインターフェース（CLI）のコマンドプロンプトを変更します。

config command_prompt [<string 16> | username | default]

44.1. config command_prompt

● 概要

このコマンドを用いて、コマンドプロンプトを変更します。現在のコマンドプロンプトは、“製品名”＋“:”＋”ユーザレベル”＋”#”（“**Zxxx0:admin#**”など）の 4 つの部分から成り立っています。このコマンドを用いて、最初の部分（1.“製品名”）を 16 文字以内の文字列またはユーザのログインユーザ名と置き換えることができます。

● 構文

config command_prompt [<string 16> | username | default]

● パラメータ

<string 16>	16 文字以内でコマンドプロンプトの新しい文字列を指定します。
username	コマンドプロンプトとしてログインユーザ名を指定します。
default	コマンドプロンプトを工場出荷時の値に戻します。

● 制限

ユーザが reset コマンドを実行しても、現在のコマンドプロンプトは変化しません。reset system を実行すると、コマンドプロンプトが工場出荷時の値に戻ります。
このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

コマンドプロンプトを編集するには：

```
Zxxx0:admin#config command_prompt HQ0001
Command: config command_prompt HQ0001

Success.

HQ0001:admin#
```

45. NLB(Network Load Balancing) コマンド

NLB とは、Windows サーバにおける負荷分散のしくみです。同一のサービスを提供する複数のサーバに共通の仮想 IP アドレスを割り当て、クライアントからのアクセスを均等に割り振ります。
NLB には、ユニキャストモードとマルチキャストモードがあり、マルチキャストモードの場合、クライアントからの宛先 MAC アドレスがマルチキャスト MAC アドレスであると転送されないことがあります。
この場合には、NLB サーバの実際の MAC アドレスをフォワーディングテーブルに登録します。

create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
config nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>
show nlb fdb

45.1. create nlb multicast_fdb

● 概要

このコマンドを用いて、NLB マルチキャストの FDB エントリを作成します。NLB コマンドセットを用いて、Microsoft サーバの負荷分散アプリケーションをサポートします。この場合、複数のサーバが同じ IP アドレスと MAC アドレスを共有できます。クライアントからの要求がすべてのサーバに転送されますが、処理はその中の 1 つによって行われます。マルチキャストモードでは、クライアントがマルチキャスト MAC アドレスを宛先 MAC として使用してサーバに到達します。モードに関しては、この宛先 MAC が名前付きの共有 MAC です。サーバは応答パケットの送信元 MAC アドレスとして、（共有 MAC ではなく）独自の MAC アドレスを使用します。

● 構文

create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>

● パラメータ

<vlan_name 32>	NLB マルチキャストの FDB エントリの VLAN 名を入力します。名前は 32 文字までです。
vlanid	VLAN ID を指定します。 **<vlanid>** VLAN ID を入力します。
<macaddr>	作成する NLB マルチキャストの MAC アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

NLB マルチキャストの FDB エントリを作成するには：

```
Zxxx0:admin# create nlb multicast_fdb default 03-bf-01-01-01-01
Command: create nlb multicast_fdb default 03-bf-01-01-01-01

Success.

Zxxx0:admin#
```

45.2. delete nlb multicast_fdb

● 概要

このコマンドを用いて、NLB マルチキャストの FDB エントリを削除します。

● 構文

delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>

● パラメータ

<vlan_name 32>	NLB マルチキャストの FDB エントリの VLAN 名を入力します。名前は 32 文字までです。
vlanid	VLAN ID を指定します。 <vlanid> VLAN ID を入力します。
<macaddr>	削除する NLB マルチキャストの MAC アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

NLB マルチキャストの FDB エントリを削除するには：

```
Zxxx0:admin# delete nlb multicast_fdb default 03-bf-01-01-01-01
Command: delete nlb multicast_fdb default 03-bf-01-01-01-01

Success.

Zxxx0:admin#
```

45.3. config nlb multicast_fdb

● 概要

このコマンドを用いて、NLB マルチキャストの FDB エントリを設定します。

● 構文

config nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>

● パラメータ

<vlan_name 32>	NLB マルチキャストの FDB エントリの VLAN 名を入力します。名前は 32 文字までです。
vlanid	VLAN ID を指定します。 <vlanid> VLAN ID を入力します。
<macaddr>	設定する NLB マルチキャストの MAC アドレスを指定します。
add	追加するフォワーディングポートのリストを指定します。
delete	削除するフォワーディングポートのリストを指定します。
<portlist>	追加または削除するフォワーディングポートのリストを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

NLB マルチキャストをフォワーディングデータベースに追加するには：

```
Zxxx0:admin# config nlb multicast_fdb default 03-bf-01-01-01-01 add 1:1-1:5
Command: config nlb multicast_fdb default 03-bf-01-01-01-01 add 1:1-1:5

Success.

Zxxx0:admin#
```

45.4. show nlb fdb

● 概要

このコマンドを用いて、NLB の設定エントリを表示します。

● 構文

show nlb fdb

● パラメータ

なし

● 制限

なし

● 実行例

NLB フォワーディングテーブルを表示するには：

```
Zxxx0:admin# show nlb fdb
Command: show nlb fdb

MAC Address          VLAN ID        Egress Ports
-----------------  ----------  ---------------------------------
02-bf-01-01-01-01    -           1:1-1:5,1:26,2:26
02-bf-01-01-01-02    -           1:1-1:5,1:26,2:26
03-bf-01-01-01-01   100          1:1-1:5,1:26,2:26
03-bf-01-01-01-01    1           1:1-1:5,1:26,2:26

Total Entries : 4

Zxxx0:admin#
```

46.ネットワーク管理コマンド

SNMP（Simple Network Management Protocol）とは、ネットワークに接続された機器をネットワーク経由で監視・制御するためのプロトコルです。対象機器は MIB（Management Information Base）と呼ばれる管理情報データベースを持ち、外部の管理マネージャで機器の MIB にアクセスして監視・制御を行います。

enable snmp
disable snmp
create trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}
config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}
delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address>| ipv6_prefix <ipv6networkaddr> | all]
show trusted_host
config snmp system_name <sw_name>
config snmp system_location <sw_location>
config snmp system_contact <sw_contact>
enable snmp traps
disable snmp traps
enable snmp authenticate_traps
disable snmp authenticate_traps
enable snmp linkchange_traps
disable snmp linkchange_traps
show snmp traps {linkchange_traps {ports <portlist>}}
config snmp linkchange_traps ports [all | <portlist>] [enable | disable]
config snmp coldstart_traps [enable | disable]
config snmp warmstart_traps [enable | disable]
config trap source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]
show trap source_ipif
config rmon trap {rising_alarm [enable | disable] | falling_alarm [enable | disable]}
show rmon

46.1. enable snmp

● 概要

このコマンドを用いて、SNMP 機能を有効にします。SNMP 機能を有効にすると、ネットワークマネージャが SNMP MIB オブジェクトにアクセス可能となります。
またネットワークマネージャにトラップ通知が可能となります。

● 構文

enable snmp

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

SNMP を有効にするには：

```
Zxxx0:admin#enable snmp
Command: enable snmp

Success.

Zxxx0:admin#
```

46.2. disable snmp

● 概要

このコマンドを用いて、SNMP 機能を無効にします。SNMP 機能を無効にすると、ネットワークマネージャが SNMP MIB オブジェクトにアクセス不可となります。
またネットワークマネージャにトラップ通知を送信しません。

● 構文

disable snmp

● パラメータ

なし。デフォルトでは SNMP は無効です。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

SNMP を無効にするには：

```
Zxxx0:admin#disable snmp
Command: disable snmp

Success.

Zxxx0:admin#
```

46.3. create trusted_host

● 概要

このコマンドを用いて、信頼されたホストを作成します。本装置では、SNMP または Telnet ベースの管理ソフトウェアによりスイッチを管理できる IP アドレス（または IP 範囲）を最大 20 まで指定できます。これらの IP アドレスは、管理 VLAN のメンバである必要があります。IP アドレスを指定しない場合は、ユーザ名とパスワードを用いて、任意の IP アドレスでスイッチにアクセスできます。

● 構文

create trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}

● パラメータ

<ipaddr>	信頼されたホストの IP アドレスを指定します。
<ipv6addr>	信頼されたホストの IPv6 アドレスを指定します。
network	信頼されたネットワークのネットワークアドレスを指定します。ネットワークアドレスの形式は、xxx.xxx.xxx.xxx/y です。 <network_address> 信頼されたネットワークのネットワークアドレスを指定します。ネットワークアドレスの形式は、xxx.xxx.xxx.xxx/y です。
ipv6_prefix	信頼されたネットワークの IPv6 ネットワークアドレスを指定します。 <ipv6networkaddr> 信頼されたネットワークの IPv6 ネットワークアドレスを指定します。
snmp	（オプション）SNMP の信頼されたホストを指定します。
telnet	（オプション）Telnet の信頼されたホストを指定します。
ssh	（オプション）SSH の信頼されたホストを指定します。
http	（オプション）HTTP の信頼されたホストを指定します。
https	（オプション）HTTPs の信頼されたホストを指定します。
ping	（オプション）Ping の信頼されたホストを指定します。

NOTE 管理方法を指定しない場合、いずれの方法でも IP（範囲）が本装置にアクセスできます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

信頼されたホストを作成するには：

```
Zxxx0:admin#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

Zxxx0:admin#
```

46.4. config trusted_host

● 概要

このコマンドを用いて、信頼されたホストのアクセスインターフェースを設定します。

● 構文

config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}

● パラメータ

<ipaddr>	信頼されたホストの IP アドレスを指定します。
<ipv6addr>	信頼されたホストの IPv6 アドレスを指定します。
network	信頼されたネットワークのネットワークアドレスを指定します。ネットワークアドレスの形式は、xxx.xxx.xxx.xxx/y です。 <network_address> 信頼されたネットワークのネットワークアドレスを指定します。ネットワークアドレスの形式は、xxx.xxx.xxx.xxx/y です。
ipv6_prefix	信頼されたネットワークの IPv6 ネットワークアドレスを指定します。 <ipv6networkaddr> 信頼されたネットワークの IPv6 ネットワークアドレスを指定します。
add	信頼されたホストのアプリケーション管理を認証します。
delete	信頼されたホストのアプリケーション管理を実行できないようにします。
snmp	（オプション）SNMP の信頼されたホストを指定します。
telnet	（オプション）Telnet の信頼されたホストを指定します。
ssh	（オプション）SSH の信頼されたホストを指定します。
http	（オプション）HTTP の信頼されたホストを指定します。
https	（オプション）HTTPs の信頼されたホストを指定します。
ping	（オプション）Ping の信頼されたホストを指定します。
all	すべてのアプリケーションの信頼されたホストを指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

信頼されたホストを設定するには：

```
Zxxx0:admin#config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

Zxxx0:admin#
```

46.5. delete trusted_host

● 概要

このコマンドを用いて、信頼されたホストエントリを削除します。

● 構文

delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr> | all]

● パラメータ

ipaddr	信頼されたホストの IP アドレスを指定します。 <ipaddr> 信頼されたホストの IP アドレスを指定します。
ipv6address	信頼されたホストの IPv6 アドレスを指定します。 <ipv6addr> 信頼されたホストの IPv6 アドレスを指定します。
network	信頼されたネットワークのネットワークアドレスを指定します。ネットワークアドレスの形式は、xxx.xxx.xxx.xxx/y です。 <network_address> 信頼されたネットワークのネットワークアドレスを指定します。ネットワークアドレスの形式は、xxx.xxx.xxx.xxx/y です。
ipv6_prefix	信頼されたネットワークの IPv6 ネットワークアドレスを指定します。 <ipv6networkaddr> 信頼されたネットワークの IPv6 ネットワークアドレスを指定します。
all	すべての信頼されたホストを削除します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

信頼されたホストを削除するには：

```
Zxxx0:admin#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

Zxxx0:admin#
```

46.6. show trusted_host

● 概要

このコマンドを用いて、信頼されたホストを表示します。

● 構文

show trusted_host

● パラメータ

なし

● 制限

なし

● 実行例

信頼されたホストを表示するには：

```
Zxxx0:admin#show trusted_host
Command: show trusted_host

Management Stations

IP Address                                              Access Interface
------------------------------------------------------------------------------
10.48.93.100
10.51.17.1
10.50.95.90

Total Entries : 3

Zxxx0:admin#
```

46.7. config snmp system_name

● 概要

このコマンドを用いて、本装置の SNMP システム名を設定します。

● 構文

config snmp system_name <sw_name>

● パラメータ

<sw_name> 本装置の SNMP システム名を指定します。255 文字まで使用できます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

「Zxxx0 Gigabit Ethernet Switch」という本装置の SNMP システム名を設定するには：

```
Zxxx0:admin# config snmp system_name Zxxx0 Gigabit Ethernet Switch
Command: config snmp system_name Zxxx0 Gigabit Ethernet Switch

Success.

Zxxx0:admin#
```

46.8. config snmp system_location

● 概要

このコマンドを用いて、本装置の SNMP システムの場所を入力します。255 文字まで使用できます。

● 構文

config snmp system_location <sw_location>

● パラメータ

<sw_location> 本装置の SNMP システムの場所を指定します。255 文字まで使用できます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

本装置の場所を「7F Server Room」に設定するには：

```
Zxxx0:admin#config snmp system_location 7F Server Room
Command: config snmp system_location 7F Server Room

Success.

Zxxx0:admin#
```

46.9. config snmp system_contact

● 概要

このコマンドを用いて、本装置のSNMPシステムの窓口を識別する名前やその他の情報を入力します。255 文字まで使用できます。

● 構文

config snmp system_contact <sw_contact>

● パラメータ

<sw_contact> SNMP システムの連絡窓口を入力します。255 文字まで使用できます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

本装置の窓口を「Network Manager」に設定するには：

```
Zxxx0:admin#config snmp system_contact "Network Manager"
Command: config snmp system_contact "Network Manager"

Success.

Zxxx0:admin#
```

46.10. enable snmp traps

● 概要

このコマンドを用いて、本装置の SNMP トラップのサポートを有効にします。

● 構文

enable snmp traps

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

SNMP トラップのサポートを有効にするには：

```
Zxxx0:admin#enable snmp traps
Command: enable snmp traps

Success.

Zxxx0:admin#
```

46.11. disable snmp traps

● 概要

このコマンドを用いて、本装置の SNMP トラップのサポートを無効にします。

● 構文

disable snmp traps

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

本装置から SNMP トラップを送信しないようにするには：

```
Zxxx0:admin#disable snmp traps
Command: disable snmp traps

Success.

Zxxx0:admin#
```

46.12. enable snmp authenticate_traps

● 概要

このコマンドを用いて、SNMP 認証失敗トラップのサポートを有効にします。

● 構文

enable snmp authenticate_traps

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

SNMP 認証トラップのサポートを有効にするには：

```
Zxxx0:admin#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

Zxxx0:admin#
```

46.13. disable snmp authenticate_traps

● 概要

このコマンドを用いて、SNMP 認証失敗トラップのサポートを無効にします。

● 構文

disable snmp authenticate_traps

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

SNMP 認証トラップのサポートを無効にするには：

```
Zxxx0:admin#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

Zxxx0:admin#
```

46.14. enable snmp linkchange_traps

● 概要

このコマンドを用いて、SNMP リンクチェンジトラップのサポートを有効にします。

● 構文

enable snmp linkchange_traps

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

SNMP リンクチェンジトラップのサポートを有効にするには：

```
Zxxx0:admin#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

Zxxx0:admin#
```

46.15. disable snmp linkchange_traps

● 概要

このコマンドを用いて、SNMP リンクチェンジトラップのサポートを無効にします。

● 構文

disable snmp linkchange_traps

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

SNMP リンクチェンジトラップのサポートを無効にするには：

```
Zxxx0:admin#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

Zxxx0:admin#
```

46.16. config snmp linkchange_traps ports

● 概要

このコマンドを用いて、リンクチェンジトラップの送信、およびチェンジトラップ送信のポート毎の制御を設定します。

● 構文

config snmp linkchange_traps ports [all | <portlist>] [enable | disable]

● パラメータ

all	すべてのポートを指定します。
<portlist>	1 つのポートまたはポートの範囲を指定します。
enable	このポートのリンクチェンジトラップの送信を有効にします。
disable	このポートのリンクチェンジトラップの送信を無効にします。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 4 の SNMP リンクチェンジトラップを有効にするには：

```
Zxxx0:admin#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

Zxxx0:admin#
```

46.17. show snmp traps

● 概要

このコマンドを用いて、SNMP トラップの状態を表示します。

● 構文

show snmp traps {linkchange_traps {ports <portlist>}}

● パラメータ

linkchange_traps （オプション）リンクチェンジトラップのステータスを表示します。

ports	（オプション）1 つのポートまたはポート範囲を設定します。 <portlist> 1 つのポートまたはポート範囲を指定します。

● 制限

なし

● 実行例

SNMP トラップを表示するには：

```
Zxxx0:admin#show snmp traps
Command: show snmp traps

SNMP Traps          : Enabled
Authenticate Trap   : Enabled
Linkchange Traps    : Enabled
Coldstart Traps     : Enabled
Warmstart Traps     : Enabled

Zxxx0:admin#
```

SNMP リンクチェンジトラップを表示するには：

```
Zxxx0:admin#show snmp traps linkchange_traps
Command: show snmp traps linkchange_traps

Linkchange Traps    : Enabled
  Port 1 : Enabled
  Port 2 : Enabled
  Port 3 : Enabled
  Port 4 : Enabled
  Port 5 : Enabled
  Port 6 : Enabled
  Port 7 : Enabled
  Port 8 : Enabled
  Port 9 : Enabled
  Port 10: Enabled
  Port 11: Enabled
  Port 12: Enabled
  Port 13: Enabled
  Port 14: Enabled
  Port 15: Enabled
  Port 16: Enabled
  Port 17: Enabled
  Port 18: Enabled
  Port 19: Enabled
  Port 20: Enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

46.18. config snmp coldstart_traps

● 概要

このコマンドを用いて、コールドスタートイベントのトラップ状態を設定します。

● 構文

config snmp coldstart_traps [enable | disable]

● パラメータ

enable	コールドスタートイベントのトラップを有効にします。デフォルトの状態は有効です。
disable	コールドスタートイベントのトラップを無効にします。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

コールドスタートイベントのトラップを有効にするには：

```
Zxxx0:admin#config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

Success.

Zxxx0:admin#
```

46.19. config snmp warmstart_traps

● 概要

このコマンドを用いて、ウォームスタートイベントのトラップ状態を設定します。

● 構文

config snmp warmstart_traps [enable | disable]

● パラメータ

enable	ウォームスタートイベントのトラップを有効にします。デフォルトの状態は有効です。
disable	ウォームスタートイベントのトラップを無効にします。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ウォームスタートイベントのトラップを有効にするには：

```
Zxxx0:admin#config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

Zxxx0:admin#
```

46.20. config trap source_ipif

● 概要

このコマンドを用いて、トラップメッセージの ipif 情報を強制的に変更します。デフォルトでは、トラップメッセージが属する ipif の情報が、トラップメッセージに含まれます。

● 構文

config trap source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

● パラメータ

<ipif_name 12>	IP インターフェースの名前を指定します。このパラメータのみを指定する場合、IPv4 アドレスおよび ipif_name の最も小さい IPv6 アドレスが送信元 IP アドレスとして使用されます。
<ipaddr>	（オプション）IPv4 アドレスを指定します。
<ipv6addr>	（オプション）IPv6 アドレスを指定します。
none	設定された送信元 IP インターフェースをクリアします。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

トラップの送信元 IP インターフェースを設定するには：

```
Zxxx0:admin#config trap source_ipif inter4
Command: config trap source_ipif inter4

Success.

Zxxx0:admin#
```

設定されたトラップの送信元 IP インターフェースをクリアするには：

```
Zxxx0:admin#config trap source_ipif none
Command: config trap source_ipif none

Success.

Zxxx0:admin#
```

46.21. show trap source_ipif

● 概要

このコマンドを用いて、トラップの送信元 IP インターフェースを表示します。

● 構文

show trap source_ipif

● パラメータ

なし

● 制限

なし

● 実行例

トラップの送信元 IP インターフェースを表示するには：

```
Zxxx0:admin#show trap source_ipif
Command: show trap source_ipif

Trap Source IP Interface Configuration:

IP Interface        : ipif4
IPv4 Address        : None
IPv6 Address        : 3000::52

Zxxx0:admin#
```

46.22. config rmon trap

● 概要

このコマンドを用いて、RMON イベントのトラップ状態を設定します。

● 構文

config rmon trap {rising_alarm [enable | disable] | falling_alarm [enable | disable]}

● パラメータ

rising_alarm	（オプション）上昇アラームのトラップ状態を設定します。デフォルトの状態は有効です。
enable	上昇アラームのトラップ状態を有効にします。
disable	上昇アラームのトラップ状態を無効にします。
falling_alarm	（オプション）下降アラームのトラップ状態を設定します。デフォルトの状態は有効です。
enable	下降アラームのトラップ状態を有効にします。
disable	下降アラームのトラップ状態を無効にします。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

RMON のトラップ状態を無効にするには：

```
Zxxx0:admin#config rmon trap rising_alarm disable
Command: config rmon trap rising_alarm disable

Success.

Zxxx0:admin#
```

46.23. show rmon

● 概要

このコマンドを用いて、RMON 関連の設定を表示します。

● 構文

show rmon

● パラメータ

なし

● 制限

なし

● 実行例

現在の RMON 設定を表示するには：

```
Zxxx0:admin#show rmon
Command: show rmon

RMON Rising Alarm Trap   : Enabled
RMON Falling Alarm Trap  : Enabled

Zxxx0:admin#
```

47.ネットワーク監視コマンド

本製品の稼動状況について、以下のようなデータを表示します。

- ポート毎の転送パケット量、エラー情報の集計
- 現在のポート使用率、CPU 使用率、DRAM 使用率、フラッシュ使用率の表示

また、以下の機能を実行します。

- ポート毎の集計カウンタのクリア
- ヒストリログ、システムログ、エラーログの表示や設定

show packet ports <portlist>
show error ports <portlist>
show utilization [ports | cpu]
show utilization dram {unit <unit_id>}
show utilization flash {unit <unit_id>}
clear counters {ports <portlist>}
clear log
show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>} | module <module_list>]}
show log_save_timing
show log_software_module
config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]
enable syslog
disable syslog
show syslog
config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress [<ipaddr> | <ipv6addr>] | state [enable | disable]}(1)
create syslog host <index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}
delete syslog host [<index 1-4> | all]
show syslog host {<index 1-4>}
config syslog source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]
show syslog source_ipif
show attack_log {index <value_list>}
clear attack_log

47.1. show packet ports

● 概要

このコマンドを用いて、本装置が送受信したパケットについての統計を表示します。

● 構文

show packet ports <portlist>

● パラメータ

<portlist>表示する 1 つのポートまたはポートの範囲を指定します。

● 制限

なし

● 実行例

ポート 7 のパケット解析を表示するには：

```
Zxxx0:admin#show packet ports 7
Command: show packet ports 7

 Port number : 7
 Frame Size/Type       Frame Counts                  Frames/sec
 ---------------       ----------------------        -----------
 64                    0                             0
 65-127                0                             0
 128-255               0                             0
 256-511               0                             0
 512-1023              0                             0
 1024-1518             0                             0
 1519-1522             0                             0
 1519-2047             0                             0
 2048-4095             0                             0
 4096-9216             0                             0
 Unicast RX            0                             0
 Multicast RX          0                             0
 Broadcast RX          0                             0

             Quit         Next Page   Previous Page   Refresh

Port number : 7
 Frame Type            Total                         Total/sec
 ---------------       ----------------------        -----------
 RX Bytes              0                             0
 RX Frames             0                             0
 TX Bytes              0                             0
 TX Frames             0                             0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

47.2. show error ports

● 概要

このコマンドを用いて、指定した範囲のポートのエラー統計を表示します。

● 構文

show errors ports <portlist>

● パラメータ

<portlist>表示する 1 つのポートまたはポートの範囲を指定します。

● 制限

なし

● 実行例

ポート 3 のエラーを表示するには：

```
Zxxx0:admin#show error ports 3
Command: show error ports 3

 Port Number : 3
                 RX Frames                                  TX Frames
                 ---------                                  ---------
 CRC Error       0                     Excessive Deferral   0
 Undersize       0                     CRC Error            0
 Oversize        0                     Late Collision       0
 Fragment        0                     Excessive Collision  0
 Jabber          0                     Single Collision     0
 Drop Pkts       0                     Collision            0
 Symbol Error    0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

47.3. show utilization

● 概要

このコマンドを用いて、リアルタイムのポート使用率または CPU 統計を表示します。
ポート使用率で表示される "TX/sec" は 1 秒毎の送信パケット数 (pps)、"RX/sec" は 1 秒毎の受信パケット数 (pps)、"Util" は送信・受信を合計した帯域の使用率 (%) を表します。

● 構文

show utilization [ports | cpu]

● パラメータ

ports	リアルタイムのポート使用率を表示します。
cpu	リアルタイムの CPU 統計を表示します。

● 制限

なし

● 実行例

ポート使用率を表示するには：

```
Zxxx0:admin#show utilization ports
Command: show utilization ports

Port     TX/sec     RX/sec     Util    Port    TX/sec      RX/sec    Util
------ ----------  ----------  ----    ------ ----------  ----------  ----
1      0           0           0       21    0           0           0
2      0           0           0       22    0           0           0
3      0           0           0       23    0           0           0
4      0           0           0       24    0           0           0
5      0           0           0       25    0           0           0
6      0           0           0       26    0           0           0
7      0           0           0       27    0           0           0
8      0           0           0       28    0           0           0
9      0           0           0
10     0           0           0
11     0           0           0
12     0           0           0
13     0           0           0
14     0           0           0
15     0           0           0
16     0           0           0
17     0           0           0
18     0           0           0
19     0           0           0
20     0           0           0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

CPU 使用率を表示するには：

```
Zxxx0:admin# show utilization cpu
Command: show utilization cpu

CPU utilization :
-------------------------------------------------------------------------------
Five seconds - 20%        One minute - 10%         Five minutes - 70%


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

47.4. show utilization dram

● 概要

このコマンドを用いて、リアルタイムの DRAM 使用率の統計を表示します。

● 構文

show utilization dram {unit <unit_id>}

● パラメータ

unit	スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 <unit_id> 使用するユニット ID を入力します。

● 制限

なし

● 実行例

DRAM 使用率を表示するには：

```
Zxxx0:admin# show utilization dram
Command: show utilization dram

DRAM utilization :
           Total DRAM     : 262144   KB
           Used DRAM      :  119586   KB
           Utilization    :  45%


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

47.5. show utilization flash

● 概要

このコマンドを用いて、リアルタイムのフラッシュ使用率の統計を表示します。

● 構文

show utilization flash {unit <unit_id>}

● パラメータ

unit	スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 <unit_id> 使用するユニット ID を入力します。

● 制限

なし

● 実行例

フラッシュ使用率を表示するには：

```
Zxxx0:admin# show utilization flash
Command: show utilization flash

FLASH Memory Utilization :
           Total FLASH     : 30608   KB
           Used FLASH      :  4786    KB
           Utilization     :  15%


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

47.6. clear counters

● 概要

このコマンドを用いて、スイッチの集計カウンタを消去します。

● 構文

clear counters {ports <portlist>}

● パラメータ

ports	ポートの範囲を指定します。ポートリストの範囲の最初と最後をダッシュで区切ります。 <portlist> ポートの範囲を指定します。

NOTE パラメータを指定しない場合、すべてのポートがカウンタの対象になります。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 7 ～ 9 について、本装置の集計カウンタを消去するには：

```
Zxxx0:admin#clear counters ports 7-9
Command: clear counters ports 7-9

Success.

Zxxx0:admin#
```

47.7. clear log

● 概要

このコマンドを用いて、本装置の履歴ログを消去します。

● 構文

clear log

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

本装置の履歴ログを消去するには：

```
Zxxx0:admin#clear log
Command: clear log

Success

Zxxx0:admin#
```

47.8. show log

● 概要

このコマンドを用いて、本装置の履歴ログを表示します。

● 構文

show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>} | module <module_list>]}

● パラメータ

index	（オプション）2 つの値の間の履歴ログを表示します。 <value_list> 2 つの値の間の履歴ログを表示します。例えば、show log index 1-5 の場合は、1 ～ 5 の履歴ログが表示されます。

severity	（オプション）重大性のレベル（emergency、alert、critical、error、warning、notice、informational または debug）を指定します。 module （オプション）表示するモジュールを指定します。モジュールは show log_software_module コマンドで取得できます。複数のモジュールを区切る場合はカンマを用います。 <module_list> 表示するモジュールを指定します。
emergency	（オプション）重大性のレベル 0 を指定します。
alert	（オプション）重大性のレベル 1 を指定します。
critical	（オプション）重大性のレベル 2 を指定します。
error	（オプション）重大性のレベル 3 を指定します。
warning	（オプション）重大性のレベル 4 を指定します。
notice	（オプション）重大性のレベル 5 を指定します。
informational	（オプション）重大性のレベル 6 を指定します。
debug	（オプション）重大性のレベル 7 を指定します。
<level_list 0-7>	(オプション）表示する重大性のレベルのリストを指定します。複数の重大性のレベルを指定する場合は、カンマで区切ります。重大性のレベルを示す数字は 0 ～ 7 です。
module	表示するモジュールを指定します。モジュールは show log_software_module コマンドで取得できます。複数のモジュールを区切る場合はカンマを用います。 <module_list> 表示するモジュールを指定します。

NOTE パラメータを指定しない場合、すべての履歴ログエントリが表示されます。

● 制限

なし

● 実行例

本装置の履歴ログを表示するには：

```
Zxxx0:admin#show log index 1-5
Command: show log index 1-5

Index Date       Time     Level   Log Text
----- ---------- -------- ------- --------------------------------------------

3     2000-03-01 00:26:51 INFO(6) Successful login through Console (Username:
Anonymous)
2     2000-03-01 00:26:49 CRIT(2) System started up
1     2000-03-01 00:26:49 CRIT(2) System warm start

Zxxx0:admin#
```

47.9. show log_save_timing

● 概要

このコマンドを用いて、ログを保存する方法を表示します。

● 構文

show log_save_log_timing

● パラメータ

なし

● 制限

なし

● 実行例

ログを保存する方法を表示するには：

```
Zxxx0:admin#show log_save_timing
Command: show log_save_timing

Saving Log Method:  On_demand

Zxxx0:admin#
```

47.10. show log_software_module

● 概要

このコマンドを用いて、拡張ログをサポートするプロトコルまたはアプリケーションを表示します。

● 構文

show log_software_module

● パラメータ

なし

● 制限

なし

● 実行例

拡張ログをサポートするプロトコルまたはアプリケーションを表示するには：

```
Zxxx0:admin#show log_software_module
Command: show log_software_module

DHCPv6_CLIENT       ERROR_LOG           MSTP

Zxxx0:admin#
```

47.11. config log_save_timing

● 概要

このコマンドを用いて、ログを保存する方法を設定します。

● 構文

config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]

● パラメータ

time_interval	xxx 分毎にログをフラッシュに保存するよう指定します。この期間にログが発生しない場合は、何も保存されません。 <min 1-65535> 1 ～ 65535 分の時間を指定します。初期値は 60 分です。
on_demand	ユーザが save log または save all と入力したときに、フラッシュにログを保存します。
log_trigger	ログが発生したときに、ログをフラッシュに保存します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ログを保存する方法を on_demand に設定するには：

```
Zxxx0:admin# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

Zxxx0:admin#
```

47.12. enable syslog

● 概要

このコマンドを用いて、syslog のグローバル設定を有効にして、ログメッセージをリモートサーバに送信します。

● 構文

enable syslog

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

syslog を有効にしてメッセージを送信するには：

```
Zxxx0:admin#enable syslog
Command: enable syslog

Success

Zxxx0:admin#
```

47.13. disable syslog

● 概要

このコマンドを用いて、syslog を無効にしてメッセージを送信しないようにします。

● 構文

disable syslog

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

syslog を無効にしてメッセージを送信しないようにするには：

```
Zxxx0:admin#disable syslog
Command: disable syslog

Success

Zxxx0:admin#
```

47.14. show syslog

● 概要

このコマンドを用いて、syslog プロトコルのグローバル設定状態を表示します。

● 構文

show syslog

● パラメータ

なし

● 制限

なし

● 実行例

syslog プロトコルのグローバル設定状態を表示するには：

```
Zxxx0:admin#show syslog
Command: show syslog

Syslog Global State: Enabled

Zxxx0:admin#
```

47.15. config syslog host

● 概要

このコマンドを用いて、syslog ホストの設定をします。

● 構文

config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress[<ipaddr> | <ipv6addr>] | state [enable | disable]} (1)

● パラメータ

<index>	ホストのインデックスを指定します。
all	すべてのホストを指定します。
severity	（オプション）サポートされる重大性のレベル（emergency、alert、critical、error、warning、notice、informational または debug）を指定します。 emergency emergency メッセージを指定します。 alert alert メッセージを指定します。 critical critical メッセージを指定します。 error error メッセージを指定します。 warning warning メッセージを指定します。 noticenotice メッセージを指定します。 informational informational メッセージを指定します。 debugdebug メッセージを指定します。 <level 0-7> 0 ～ 7 のレベルを指定します。
facility	一部のオペレーティングシステムデーモンとプロセスには、facility 値が割り当てられています。facility が明示的に割り当てられていないプロセスとデーモンは、任意の "local use" facility を使用するか、"user-level" facility を使用することができます。指定済みの facility を以下に示します。 local0 ユーザ定義 facility local1 ユーザ定義 facility local2 ユーザ定義 facility local3 ユーザ定義 facility local4 ユーザ定義 facility local5 ユーザ定義 facility local6 ユーザ定義 facility local7 ユーザ定義 facility
udp_port UDP ポート番号を指定します。 <udp_port_number> UDP ポート番号を指定します。	

ipaddress	ホストの IPv4 または IPv6 アドレスを指定します。 **<ipaddr>** ホストの IPv4 アドレスを指定します。 **<ipv6addr>** ホストの IPv6 アドレスを指定します。
state	ネットワークのイベント通知メッセージをホストへ送信するのに、syslog プロトコルが使用されています。このオプションで、ホストがこのようなメッセージを受信するかどうかを設定します。 **enable** ホストがメッセージを受信します。 **disable** ホストがメッセージを受信しません。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

syslog ホストの設定を行うには：

```
Zxxx0:admin# config syslog host all severity informational facility local0
Command: config syslog host all severity informational facility local0

Success.

Zxxx0:admin#
```

47.16. create syslog host

● 概要

このコマンドを用いて、新しい syslog ホストを作成します。

● 構文

create syslog host <index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}

● パラメータ

<index 1-4>	ホストのインデックスを指定します。

ipaddress	ホストの IPv4 または IPv6 アドレスを指定します。 **<ipaddr>** ホストの IPv4 アドレスを指定します。 **<ipv6addr>** ホストの IPv6 アドレスを指定します。
severity	（オプション）サポートされる重大性のレベル（emergency、alert、critical、error、warning、notice、informational または debug）を指定します。 **emergency** emergency メッセージを指定します。 **alert** alert メッセージを指定します。 **critical** critical メッセージを指定します。 **error** error メッセージを指定します。 **warning** warning メッセージを指定します。 **notice**notice メッセージを指定します。 **informational** informational メッセージを指定します。 **debug**debug メッセージを指定します。 **<level 0-7>** 0 ～ 7 のレベルを指定します。
facility	一部のオペレーティングシステムデーモンとプロセスには、facility 値が割り当てられています。facility が明示的に割り当てられていないプロセスとデーモンは、任意の "local use" facility を使用するか、"user-level" facility を使用することができます。指定済みの facility を以下に示します。 **local0** ユーザ定義 facility **local1** ユーザ定義 facility **local2** ユーザ定義 facility **local3** ユーザ定義 facility **local4** ユーザ定義 facility **local5** ユーザ定義 facility **local6** ユーザ定義 facility **local7** ユーザ定義 facility
udp_port	UDP ポート番号を指定します。 **<udp_port_number>** UDP ポート番号を指定します。
state	ネットワークのイベント通知メッセージをホストへ送信するのに、syslog プロトコルが使用されています。このオプションで、ホストがこのようなメッセージを受信するかどうかを指定します。 **enable** ホストがメッセージを受信します。 **disable** ホストがメッセージを受信しません。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

新しい syslog ホストを作成するには：

```
Zxxx0:admin# create syslog host 1 ipaddress 10.1.1.1
Command: create syslog host 1 ipaddress 10.1.1.1

Success.

Zxxx0:admin#
```

47.17. delete syslog host

● 概要

このコマンドを用いて、syslog ホストを削除します。

● 構文

delete syslog host [<index 1-4> | all]

● パラメータ

<inex 1-4>	ホストのインデックスを指定します。
all	すべてのホストを指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

syslog ホストを削除するには：

```
Zxxx0:admin#delete syslog host 4
Command: delete syslog host 4

Success

Zxxx0:admin#
```

47.18. show syslog host

● 概要

このコマンドを用いて、syslog ホスト設定を表示します。

● 構文

show syslog host {<index 1-4>}

● パラメータ

<index 1-4> （オプション）ホストのインデックスを指定します。

NOTE パラメータを指定しない場合、すべてのホストが表示されます。

● 制限

なし

● 実行例

syslog ホスト設定を表示するには：

```
Zxxx0:admin#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host 1
  IP Address      : 10.1.1.2
  Severity        : Warning
  Facility        : Local10
  UDP port        : 514
  Status          : Disabled

Host 2
  IP Address      : 3000:501:100:ffff:101:202:303:1
  Severity        : Emergency
  Facility        : Local10
  UDP port        : 514
  Status          : Disabled

Total Entries : 2

Zxxx0:admin#
```

47.19. config syslog source_ipif

● 概要

このコマンドを用いて、syslog の ipif 情報を強制的に変更します。デフォルトでは、syslog が属する ipif の情報が、syslog に含まれます。

● 構文

config syslog source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

● パラメータ

<ipif_name 12>	IP インターフェースの名前を指定します。このパラメータのみを指定する場合、IPv4 アドレスおよび ipif_name の最も小さい IPv6 アドレスが送信元 IP アドレスとして使用されます。
<ipaddr>	（オプション）IPv4 アドレスを指定します。
<ipv6addr>	（オプション）IPv6 グローバルアドレスを指定します。
none	設定された送信元 IP インターフェースをクリアします。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

syslog の送信元 IP インターフェースを設定するには：

```
Zxxx0:admin#config syslog source_ipif Sysetm
Command: config syslog source_ipif System

Success.

Zxxx0:admin#
```

設定された syslog の送信元 IP インターフェースをクリアするには：

```
Zxxx0:admin#config syslog source_ipif none
Command: config syslog source_ipif none

Success.

Zxxx0:admin#
```

47.20. show syslog source_ipif

● 概要

このコマンドを用いて、syslog の送信元 IP インターフェースを表示します。

● 構文

show syslog source_ipif

● パラメータ

なし

● 制限

なし

● 実行例

syslog の送信元インターフェースを表示するには：

```
Zxxx0:admin#show syslog source_ipif
Command: show syslog source_ipif

Syslog Source IP Interface Configuration:

IP Interface        : System
IPv4 Address        : None
IPv6 Address        : None

Zxxx0:admin#
```

47.21. show attack_log

● 概要

このコマンドを用いて、本装置の攻撃ログを表示します。

● 構文

show attack_log {index <value_list>}

● パラメータ

index	（オプション）表示する必要があるエントリのインデックスのリストを指定します。 <value_list> 表示する必要があるエントリのインデックスのリストを指定します。例えば、show attack_log index 1-5 の場合は、1 ～ 5 の攻撃ログメッセージが表示されます。

NOTE パラメータを指定しない場合、攻撃ログのすべてのエントリが表示されます。

● 制限

なし

● 実行例

本装置の攻撃ログを表示するには：

```
Zxxx0:admin#show attack_log index 1-3
Command: show attack_log index 1-3

Index Date       Time      Level     Log Text
----- ---------- -------- -------- ------------------------------------------------
3     2009-12-26 14:15:45  WARN(4) Port security violation mac addrss 00-18-F3-10-
94-89 on locking address full port 28
2     2009-12-26 14:15:45  WARN(4)  Port security violation mac addrss 00-18-F3-10-
94-89 on locking address full port 28
1     2009-12-26 14:15:45  WARN(4)  Port security violation mac addrss 00-18-F3-10-
94-89 on locking address full port 28

Zxxx0:admin#
```

47.22. clear attack_log

● 概要

このコマンドを用いて、本装置の攻撃ログをクリアします。

● 構文

clear attack_log

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

本装置の攻撃ログをクリアするには：

```
Zxxx0:admin#clear attack_log
Command: clear attack_log

Success.

Zxxx0:admin#
```

48. パケットストームコマンド

パケットストーム（Packet Storm）とは、パケットがネットワーク上にあふれる現象です。ブロードキャストやマルチキャストが同時に大量に送信された場合や、ネットワーク機器の障害等により発生します。パケットストームの発生により、ネットワークの効率が低下し、正常の通信が阻害されます。

本製品では、以下の方法で、指定したポートのパケットストームを監視し、制御することができます。

- 破棄（drop）：パケットが設定したしきい値を超えた場合、超過分のパケットを破棄します。
- シャットダウン（shutdown）：パケットが設定したしきい値を超えた場合、パケットの転送を停止します。指定した時間内にパケットストームが治まらない場合は、手動で解除するまでポートを遮断し続けます。

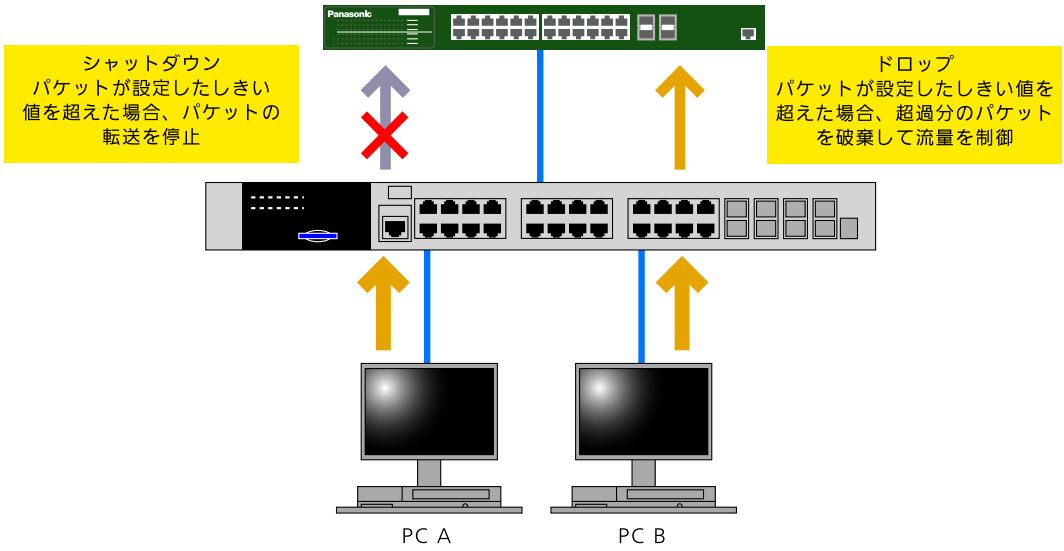


図 48-1　パケットストームの制御

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}(1)
config traffic control auto_recover_time [<min 0> | <min 1-65535>]
config traffic control log state [enable | disable]
config traffic trap [none | storm_occurred | storm_cleared | both]
show traffic control {<portlist>}

48.1. config traffic control

● 概要

このコマンドを用いて、ブロードキャスト / マルチキャスト / ユニキャストのストーム制御を設定します。ブロードキャストストーム制御コマンドは、ハードウェアストーム制御メカニズムのみを提供します。これらのパケットストーム制御コマンドには、シャットダウン、回復およびトラップ通知機能を提供するためのハードウェアメカニズムおよびソフトウェアメカニズムが含まれます。

● 構文

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}(1)

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートが設定されます。
broadcast	ブロードキャストストームステータスを指定します。 enable ブロードキャストストーム制御を有効にします。 disable ブロードキャストストーム制御を無効にします。
multicast	マルチキャストストームステータスを指定します。 enable マルチキャストストーム制御を有効にします。 disable マルチキャストストーム制御を無効にします。
unicast	不明なユニキャストパケットストームのステータスを指定します。 enable 不明なユニキャストパケットストーム制御を有効にします（破棄動作のみをサポート）。 disable 不明なユニキャストパケットストーム制御を無効にします。
action	どちらで動作するかを指定します。 drop パケットが設定したしきい値を超えた場合、超過分のパケットを破棄する制御をハードウェア上で実装されます。 shutdown パケットが設定したしきい値を超えた場合、パケットの転送を停止し、指定した時間外内にパケットストームが治まらない場合、手動で解除するまでポート遮断する制御をソフトウェア上で実装されます。これを選択した場合は、threshold、countdown、time_interval も設定する必要があります。
threshold	指定したストーム制御がオンになる上限しきい値。 これは、ストームトラフィック制御を起動するスイッチが受信する 1 秒当たりのブロードキャスト / マルチキャスト / 不明なユニキャストのパケット数です。符号なし整数で指定する必要があります。 <value 0-255000> 0 ～ 255000 の値を指定します。

countdown	シャットダウンモードのタイマーです。ポートが受信シャットダウン状態になり、この時間が過ぎると、ポートが永久にシャットダウンされます。デフォルトは 0 分です。 <min 0> ゼロの場合は永久に無効になります。 <min 3-30> 3 ～ 30 分の値を入力します。 disable 動作が shutdown で countdown が無効な場合、本装置がストームを検出すると、本装置が直接ポートをシャットダウンします。
time_interval	受信したパケット数のサンプリング間隔。動作としてパケットの破棄を選択した場合は、このパラメータは意味がありません。 <value 5-600> 5 ～ 600 の値を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

トラフィック制御と状態を設定するには：

```
Zxxx0:admin#config traffic control 1-10 broadcast enable action shutdown threshold
640 time_interval 10
Command: config traffic control 1-10 broadcast enable action shutdown threshold 640
time_interval 10


Success.


Zxxx0:admin#
```

48.2. config traffic control auto_recover_time

● 概要

このコマンドを用いて、ポートが永久シャットダウンステータスから回復するためのトラフィック自動回復時間を設定します。これは、ポートがシャットダウンから自動回復する時間です。初期値は 0 で、自動回復はできません。ポートは永久シャットダウンモードのままになります。ポートをフォワーディング状態に戻すには、手動で CLI コマンド config ports [<portlist> | all] state enable を入力する必要があります。初期値は0であるため自動回復モードは無効で、永久シャットダウンになります。

● 構文

config traffic control auto_recover_time [<min 0> | <min 1-65535>]

● パラメータ

<min 0> 自動回復モードを無効にします。
<min 1-65535> 自動回復時間を入力します。この値は 1 ～ 65535 分の必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

自動回復時間を 5 分に設定するには：

```
Zxxx0:admin# config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

Zxxx0:admin#
```

48.3. config traffic control log state

● 概要

このコマンドを用いて、トラフィック制御ログの状態を設定します。ログの状態が有効な場合は、ストームが発生したとき、およびストームがクリアされたときに、トラフィック制御状態がログに記録されます。ログの状態が無効な場合は、トラフィック制御イベントがログに記録されません。
ログの状態はシャットダウンモードのみに適用されます。シャットダウンモードはブロードキャストおよびマルチキャストストーム制御のみをサポートし、ユニキャストストーム制御はサポートしません。このため、ブロードキャストおよびマルチキャストストーム制御のログのみが生成されます。

● 構文

config traffic control log state [enable | disable]

● パラメータ

state	トラフィック制御ログの状態を指定します。 enable ストームが発生すると、トラフィック制御状態がログに記録されます。 disable トラフィック制御状態が無効になります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

本装置のトラフィックログの状態を設定するには：

```
Zxxx0:admin# config traffic control log state enable
Command: config traffic control log state enable

Success.

Zxxx0:admin#
```

48.4. config traffic trap

● 概要

このコマンドを用いて、ソフトウェアトラフィックストーム制御メカニズムによりトラフィックストームイベントが検出された場合に、ストーム制御通知を行うかどうかを設定します。

> **NOTE** トラフィック制御トラップは、制御動作がシャットダウンに設定されている場合のみ有効です。制御動作が破棄の場合は、ストームイベントが検出されてもトラップは発行されません。

● 構文

config traffic trap [none | storm_occurred | storm_cleared | both]

● パラメータ

none	ストームイベントが検出またはクリアされても通知は行われません。
storm_occurred	ストームイベントが検出されると、通知が行われます。
storm_cleared	ストームイベントがクリアされると、通知が行われます。
both	ストームイベントが検出されたときとクリアされたときの両方に、通知が行われます。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

トラフィック制御トラップを設定するには：

```
Zxxx0:admin#config traffic trap both
Command: config traffic trap both

Success.

Zxxx0:admin#
```

48.5. show traffic control

● 概要

このコマンドを用いて、現在のトラフィック制御設定を表示します。

● 構文

show traffic control {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

NOTE パラメータを指定しない場合、すべてのポートのパケットストーム制御設定が表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 3 のパケットストーム制御設定を表示するには：

```
Zxxx0:admin#show traffic control 1-3
Command: show traffic control 1-3

Traffic Control Trap              : [None]
Traffic Control Log               : Enabled
Traffic Control Auto Recover Time: 0 Minutes

Port Thres  Broadcast Multicast Unicast  Action   Count    Time     Shutdown
     hold   Storm     Storm     Storm              down     Interval Forever
---- ------ --------- --------- -------- -------- -------- -------- --------
1    640    Enabled   Disabled  Disabled shutdown 0        10
2    640    Enabled   Disabled  Disabled shutdown 0        10
3    640    Enabled   Disabled  Disabled shutdown 0        10

Zxxx0:admin#
```

49.ポートセキュリティコマンド

ポートセキュリティでは、本製品で学習される MAC アドレスの数を制限することでアクセスする端末数を制限します。指定した端末数を超えるアクセスがあった場合、超過したアクセスは破棄されます。
以下の 4 つのレベルで端末数を設定できます。

- システム全体
- ポート毎
- VLAN 毎
- VLAN 内のポート毎

config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-3328> | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1) | {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]}]
config port_security system max_learning_addr [<max_lock_no 1-3328> | no_limit]
config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]
delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>
clear port_security_entry {ports [<portlist> | all] | {[vlan <vlan_name 32> | vlanid <vidlist>]}}
show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}
show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}
enable port_security trap_log
disable port_security trap_log

49.1. config port_security ports

● 概要

このコマンドを用いて、ポートの状態、サポートされる MAC アドレスエントリの最大数、デフォルトのエントリタイプを設定します。さらに、特定のポートの特定の VLAN で学習されるポートセキュリティエントリの最大数を設定します。学習されるエントリ数の制限には、システム全体、ポート毎、VLAN 毎、特定の VLAN 内のポート毎の 4 つのレベルがあります。いずれかの制限を超えると、新しいエントリが破棄されます。

● 構文

config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-3328> | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1) | {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]}]

● パラメータ

<portlist>設定するポートの範囲を指定します。

all　すべてのポートが設定されます。

admin_state
ポートリストで指定されたポートについて、ポートセキュリティを有効または無効にできます。デフォルト設定は無効です。
enable
ポートリストで指定したポートに対してポートセキュリティを有効にします。
disable
ポートリストで指定したポートに対してポートセキュリティを無効にします。

max_learning_addr
このポートで学習できる MAC アドレスエントリの最大数を指定します。この値を 0 に設定すると、このポートのポートセキュリティ機能では、どのユーザも認証されないことになります。このポートで学習された現在のエントリ数よりも小さい数を設定すると、コマンドが拒否されます。初期値は 32 です。
<max_lock_no 0-3328>
0 ～ 3328 の値を指定します。

lock_address_mode
アドレスロックモードを示します。デフォルトモードは deleteonreset です。
permanent
ユーザが手動でアドレスを削除するか、エントリの VLAN が削除されるか、ポートが VLAN から削除されるか、アドレスが配置されたポートのポートセキュリティが無効にされた場合以外、アドレスは削除されません。
deleteontimeout
エージングタイマーが期限切れになった後で、ロックされたアドレスをエージアウトできます。
deleteonreset
スイッチがリセットまたは再起動されると、このアドレスが削除されます。永久的なエントリが削除されるケースでも、deleteonreset エントリに適用されます。

vlan　（オプション）アドレス学習を制限する VLAN を指定します。
<vlan_name 32>
VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid アドレス学習を制限する VLAN のリストを、VLAN ID で指定します。
<vidlist>
VLAN ID のリストを指定します。

max_learning_addr
（オプション）このポートで学習できる MAC アドレスエントリの最大数を指定します。この値を 0 に設定すると、このポートのポートセキュリティ機能では、どのユーザも認証されないことになります。このポートで学習された現在のエントリ数よりも小さい数を設定すると、コマンドが拒否されます。初期値は 32 です。
<max_lock_no 0-3328>
0 ～ 3328 の値を指定します。
no_limit
エントリ数に制限がないことを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポートセキュリティを設定するには：

```
Zxxx0:admin#config port_security ports 6 admin_state enable max_learning_addr 10
lock_address_mode permanent
Command: config port_security ports 6 admin_state enable max_learning_addr 10
lock_address_mode permanent

Success.

Zxxx0:admin#
```

ポートセキュリティ設定を指定するには：

```
Zxxx0:admin#config port_security ports 1 vlan vlanid 1 max_learning_addr 16
Command: config port_security ports 1 vlan vlanid 1 max_learning_addr 16

Success.

Zxxx0:admin#
```

49.2. config port_security system max_learning_addr

● 概要

このコマンドを用いて、システム全体で認証される MAC アドレスエントリの最大数を設定します。学習されるエントリ数の制限には、システム全体、ポート毎、VLAN 毎、特定の VLAN 内のポート毎の 4 つのレベルがあります。いずれかの制限を超えると、新しいエントリが破棄されます。システムレベルでの学習される最大ユーザ数の設定は、すべてのポートで学習されるユーザの最大数の合計よりも大きくする必要があります。

● 構文

config port_security system max_learning_addr [<max_lock_no 1-3328> | no_limit]

● パラメータ

<max_lock_no 1-3328>	システムで学習できる MAC アドレスエントリの最大数を指定します。有効なすべてのポートで学習された現在のエントリ数よりも小さい数を設定すると、コマンドが拒否されます。
no_limit	上記の数が制限なしに設定されます。（デフォルト）

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポートセキュリティエントリの最大数を 256 に設定するには：

```
Zxxx0:admin# config port_security system max_learning_addr 256
Command: config port_security system max_learning_addr 256

Success.

Zxxx0:admin#
```

49.3. config port_security vlan

● 概要

このコマンドを用いて、特定の VLAN で学習できる MAC アドレスエントリの最大数を指定します。学習されるエントリ数の制限には、システム全体、ポート毎、VLAN 毎、特定の VLAN 内のポート毎の 4 つのレベルがあります。いずれかの制限を超えると、新しいエントリが破棄されます。

● 構文

config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]

● パラメータ

<vlan_name 32>	VLAN を名前で指定します。最大文字数は 32 文字です。
vlanid	VLAN のリストを VLAN ID で指定します。 <vidlist> VLAN ID を指定します。
max_learning_addr	この VLAN で学習できる MAC アドレスエントリの最大数を指定します。このパラメータを 0 に設定すると、この VLAN ではどのユーザも認証されないことになります。この VLAN で学習された現在のエントリ数よりも小さい数を設定すると、コマンドが拒否されます。 <max_lock_no 0-3328> 0 ～ 3328 の値を指定します。 no_limit デフォルト設定は制限なしです。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

学習可能なエントリの最大数を 64 に設定するには：

```
Zxxx0:admin#config port_security vlan vlanid 1 max_learning_addr 64
Command: config port_security vlan vlanid 1 max_learning_addr 64

Success.

Zxxx0:admin#
```

49.4. delete port_security_entry

● 概要

このコマンドを用いて、VLAN、VLAN ID および MAC アドレスに基づいてポートセキュリティエントリを削除します。

● 構文

delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>

● パラメータ

vlan	VLAN を名前で指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	VLAN のリストを VLAN ID で指定します。 <vlanid 1-4094> VLAN ID を指定します。この値は 1 ～ 4094 の必要があります。
mac_address	エントリの MAC アドレスを指定します。 <macaddr> エントリの MAC アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

デフォルト VLAN の MAC アドレスが 00-01-30-10-2c-c7 のポートセキュリティエントリを削除するには：

```
Zxxx0:admin#delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7
Command: delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7

Success.

Zxxx0:admin#
```

49.5. clear port_security_entry

● 概要

このコマンドを用いて、ポートセキュリティ機能のために、指定したポートまたは VLAN で学習された MAC エントリをクリアします。

● 構文

clear port_security_entry {ports [<portlist> | all] | {[vlan <vlan_name 32> | vlanid <vidlist>]}}

● パラメータ

ports	（オプション）指定したポートで学習されたポートセキュリティエントリがクリアされます。 <portlist> 設定するポートの範囲を指定します。 all システムで学習されたすべてのポートセキュリティエントリがクリアされます。
vlan	（オプション）指定した VLAN で学習されたポートセキュリティエントリがクリアされます。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）VLAN のリストを VLAN ID で指定します。 <vidlist> VLAN ID のリストを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 6 のポートセキュリティエントリをクリアするには：

```
Zxxx0:admin#clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

Zxxx0:admin#
```

49.6. show port_security_entry

● 概要

このコマンドを用いて、ポートセキュリティエントリを表示します。

● 構文

show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

● パラメータ

ports	（オプション）表示するポートの範囲を指定します。 <portlist> 表示するポートの範囲を指定します。
vlan	（オプション）エントリを表示する VLAN を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）エントリを表示する VLAN のリストを指定します。 <vidlist> VLAN ID のリストを指定します。

● 制限

なし

● 実行例

ポートセキュリティエントリを表示するには：

```
Zxxx0:admin#show port_security_entry
Command: show port_security_entry


MAC Address         VID   Port    Lock Mode
------------------  ---   ----    ----------
00-00-00-00-00-01   1     25      DeleteOnTimeout

Total Entry Number: 1

Zxxx0:admin#
```

49.7. show port_security

● 概要

このコマンドを用いて、ポートセキュリティの管理状態、学習されるアドレスの最大数、ロックモードなど、本装置のポートのポートセキュリティ関連の情報を表示します。

● 構文

show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

● パラメータ

ports	（オプション）表示するポートの範囲を指定します。 <portlist> 表示するポートの範囲を指定します。
vlan	（オプション）設定を表示する VLAN を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）設定を表示する VLAN のリストを指定します。 <vidlist> VLAN ID のリストを指定します。

● 制限

なし

● 実行例

ポートセキュリティのグローバル設定を表示するには：

```
Zxxx0:admin# show port_security
Command: show port_security

Port Security Trap/Log          : Disabled
System Maximum Address          : 512

 VLAN Configuration (Only VLANs with limitation are displayed)
 VID   VLAN Name                         Max. Learning Addr.
 ----  --------------------------------  -------------------
 1     default                           64
 2     TstVLAN                           8

Zxxx0:admin#
```

本装置のポート 1 ～ 6 のポートセキュリティ情報を表示するには：

```
Zxxx0:admin#show port_security ports 1-6
Command: show port_security ports 1-6

Port   State    Lock Address Mode   Max. Learning Addr.
-----  -------  ------------------  -----------------
1      Disabled DeleteOnReset       32
2      Disabled DeleteOnReset       32
3      Disabled DeleteOnReset       32
4      Disabled DeleteOnReset       32
5      Disabled DeleteOnReset       32
6      Disabled DeleteOnReset       32

Zxxx0:admin#
```

49.8. enable port_security trap_log

● 概要

このコマンドを用いて、ポートセキュリティトラップ / ログを有効にします。このコマンドが有効な場合、事前に定義されたポートセキュリティ設定に違反する新しい MAC が検出されると、MAC とポート情報とともにトラップが送信され、関連情報がログに記録されます。

● 構文

enable port_security trap_log

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポートセキュリティトラップを有効にするには：

```
Zxxx0:admin#enable port_security trap_log
Command: enable port_security trap_log

Success.

Zxxx0:admin#
```

49.9. disable port_security trap_log

● 概要

このコマンドを用いて、ポートセキュリティトラップ / ログを無効にします。ポートセキュリティトラップが無効な場合、MAC 違反があってもトラップは送信されず、ログも記録されません。

● 構文

disable port_security trap_log

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

本装置からポートセキュリティトラップが送信されないようにするには：

```
Zxxx0:admin#disable port_security trap_log
Command: disable port_security trap_log

Success.

Zxxx0:admin#
```

50.省電力コマンド

省電力モードを設定します。
ポートがリンク状態でない場合に、ポートへの電力提供の ON/OFF を周期的に繰り返し、常時 ON にした場合に比べて消費電力を抑えます。

config power_saving state [enable | disable]
show power_saving

50.1. config power_saving

● 概要

このコマンドを用いて、システムの省電力モードを設定します。デフォルトでは省電力モードは無効です。以下のメカニズムで省電力を行います。
ポートにリンクパートナがない場合はポートが自動的に OFF になり、1 秒に 1 回 ON になって単一のリンクパルスが送信されます。ポートが OFF の場合、簡単なエネルギー検出回路により継続してケーブルのエネルギーを監視します。エネルギーが検出された瞬間に、IEEE 仕様の要件に従って、ポートが完全に ON になります。リンクが検出されないときは省電力機能が実行されます。これは、リンクアップ時のポートの機能には影響しません。

● 構文

config power_saving state [enable | disable]

● パラメータ

state	（オプション）省電力状態を有効または無効に設定します。初期値は Desable です。 enable 省電力機能を有効にします。 disable 省電力機能を無効にします。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

省電力モードを設定するには：

```
Zxxx0:admin# config power_saving state enable
Command: config power_saving state enable

Success

Zxxx0:admin#
```

50.2. show power_saving

● 概要

このコマンドを用いて、省電力情報を表示します。

● 構文

show power_saving

● パラメータ

なし

● 制限

なし

● 実行例

省電力情報を表示するには：

```
Zxxx0:admin#show power_saving
Command: show power_saving

Power Saving State: Enabled

Zxxx0:admin#
```

51.PPS コマンド

PPS（Power to Progress SDN）は、ネットワークを構成する複数の装置を一つのソフトウェアで管理し、運用や設定を容易にするための機能です。この機能を用いることで、PPS アプリケーション（別売）から本装置を制御することが可能となります。PPS アプリケーション（別売）から管理できる内容については、PPS アプリケーションの取扱説明書をご参照ください。

---

enable PPS
disable PPS
config pps start_status {standalone | cpnl}
config pps controller-id {<string 6> {<macaddr>} | none}
show pps
clear pps neighbor {<macaddr> | all}
config pps neighbor aging_time <sec 60-86400>
show pps neighbor [<macaddr>]
show pps notification
config pps notification syslog enable
config pps notification syslog disable
config pps notification counter interval <value 1-120>
config pps notification counter add <port-list>
config pps notification counter delete <port-list>
show pps connection
config pps ports <portlist> **priority** <value 0-255>
show pps ports
restart pps [connection]
config pps connection add <macaddr> <macaddr> <vlanid 1-4094> <port> {send [tagged | untagged]}
config pps connection delete <macaddr> <macaddr>
config pps retry count <value 1-5>
config pps timeout <sec 1-10>

NOTE 起動後、Standalone の状態で 1 時間経過すると自動的に PPSP 機能を停止します。
1 時間経過後、PPS コントローラを認識させるには機器の PPSP 機能を再起動、または機器の再起動を行ってください。

NOTE 本機能を無効にした場合、PPS コントローラから管理できる内容が制限されます。

NOTE 多拠点の機器（IP セグメントを超えた機器）への設定変更等をする場合は PPSP に対応した当社製レイヤ 3 スイッチングハブにて仮想リンク転送先 IP アドレスの設定が必要です。

51.1. enable pps

● 概要

このコマンドは、PPS グローバルステータスを有効にするために使用され、スイッチはコントローラを自動的に検出します。

● 構文

enable pps

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS グローバルステータスを有効にするには：

```
Zxxx0:admin#enable pps
Command: enable pps
Success.

Zxxx0:admin#
```

51.2. disable pps

● 概要

このコマンドは、PPS グローバルステータスを無効にするために使用します。

● 構文

disable pps

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS グローバルステータスを無効にするには：

```
Zxxx0:admin#disable pps
Command: disable pps
Success.

Zxxx0:admin#
```

51.3. config pps start_status

● 概要

このコマンドは、PPS 開始ステータスを設定するために使用します。
ユーザーがデバイスの電源を入れるか、デバイスを再起動すると、デバイスはこのモードから起動します。
「start-status」が「standalone」の場合、「standalone」から開始されます。
「start-status」が「CPNL」の場合、「コントローラ ID」がチェックされます。
コンフィグレーションファイルに「コントローラ ID」が存在する場合、または PPS 情報が存在する場合は、直ちに「CPNL」になります。
「コントローラ ID」が存在しない場合は、「standalone」から開始します。

● 構文

config pps start_status [standalone | cpnl]

● パラメータ

standalone	PPS コントローラに管理されていない状態を指定します。
cpnl	Controller Port Neighbor Lost の略でスイッチングハブがコントローラを認識しているが、コントローラと通信不可能な状態を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS 設定の初期動作状態ををを設定するには：

```
Zxxx0:admin#config pps start_status standalone
Command: config pps start_status standalone

Success.

Zxxx0:admin#
```

51.4. config pps controller-id

● 概要

このコマンドは、PPS コントローラ ID と MAC アドレスを手動で設定するために使用します。コントローラ ID は、コントローラを識別するために使用されます。Controller ID が一致しない場合、スイッチは PPS メッセージを無視します。

● 構文

config pps controller-id [<string 6> {<macaddr>} | none]

● パラメータ

<string 6>	PPS コントロー ラの ID を指定します。PPS コントロー ラの ID に指定できる文字数は 6 文字です。
<macaddr>	PPS コントローラの MAC アドレスを指定します。
none	PPS コントロー ラの ID を指定しません。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS コントロー ラの ID を設定するには：

```
Zxxx0:admin#config pps controller_id 123456
Command: config pps controller_id 123456

Success.

Zxxx0:admin#
```

51.5. show pps

● 概要

このコマンドを用いて、PPS 設定情報を表示します。

● 構文

show pps

● パラメータ

なし

● 制限

なし

● 実行例

PPS 設定情報を表示するには：

```
Zxxx0:admin#show pps
Command: show pps

PPS Global Status      : Enabled
 PPS Status             : Controlled
 PPS Start Status       : CPNL
 Retry Count            : 3
 Timeout                : 3
 Controller ID          : PPS-ID
 Controller Uptime      : 000 day(s) 00 hour(s) 00 min(s) 24 sec(s)
 Controller MAC Address : 12-34-56-78-9A-BC
 PPS Gateway            : 12-34-56-78-9A-BC
 Controller Port        : 24
 Expired                : 112

Zxxx0:admin#
```

51.6. clear pps neighbor

● 概要

このコマンドを用いて、登録されている PPS Neighbor のエントリを削除します。

● 構文

clear pps neighbor [<macaddr> | all]

● パラメータ

<macaddr>	削除する PPS Neighbor のエントリの MAC アドレスを指定します。
all	登録されている全ての PPS Neighbor のエントリを削除します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

登録されている PPS Neighbor のエントリを削除するには：

```
Zxxx0:admin# clear pps neighbor 00-00-00-00-00-01
Command: clear pps neighbor 00-00-00-00-00-01

Success.

Zxxx0:admin#
```

51.7. config pps neighbor aging_time

● 概要

このコマンドを用いて、PPS Neighbor のエントリ保有時間を秒単位で指定します。

● 構文

config pps neighbor aging_time <sec 60-86400>

● パラメータ

<sec 60-86400>
PPS Neighbor エントリを保有する秒数を 指定します。PPS Neighbor のエントリ保有時間の値は 60 ～ 86400 秒です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS Neighbor のエントリ保有時間を設定するには：

```
Zxxx0:admin#config pps neighbor aging_time 1240
Command: config pps neighbor aging_time 1240

Success.

Zxxx0:admin#
```

51.8. show pps neighbor

● 概要

このコマンドを用いて、PPS Neighbor テーブルを表示します。

● 構文

show pps neighbor {<macaddr>}

● パラメータ

<macaddr> 表示する PPS Neighbor のエントリの MAC アドレスを指定します。パラメータが指定されていない場合、すべてのネイバーの情報を表示します。

● 制限

なし

● 実行例

PPS Neighbor テーブルを表示するには：

```
Zxxx0:admin# show pps neighbor
Command: show pps neighbor

 Neighbor Aging Time = 60

 MAC Address       Port  Expired
 ----------------- ----- -------
 00-C0-8F-00-77-02 21    51
 12-34-56-78-9A-BC 23    60

Total Entries : 2

Zxxx0:admin#
```

51.9. show pps notification

● 概要

このコマンドを用いて、PPS システムログと PPS パケット統計情報の通知設定状態を表示します。

● 構文

show pps notification

● パラメータ

なし

● 制限

なし

● 実行例

PPS 通知設定情報を表示するには：

```
Zxxx0:admin# show pps notification
Command: show pps notification

 System Log :
   Status   : Enabled
 Counter    :
   Ports    : 1-28
   Interval : 5 sec(s)

Zxxx0:admin#
```

51.10. config pps notification syslog enable

● 概要

このコマンドは、PPS システムログ通知ステータスを設定するために使用します。PPS システムログ通知を有効にすると、スイッチ上のすべての システムログが PPS コントローラに送信されます。

● 構文

config pps notification syslog enable

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS システムログ通知を有効にするには：

```
Zxxx0:admin# config pps notification syslog enable
Command: config pps notification syslog enable

Success.

Zxxx0:admin#
```

51.11. config pps notification syslog disable

● 概要

このコマンドを用いて、PPS システムログ通知を無効にします。

● 構文

config pps notification syslog disable

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS システムログ通知を無効にするには：

```
Zxxx0:admin# config pps notification syslog disable
Command: config pps notification syslog disable

Success.

Zxxx0:admin#
```

51.12. config pps notification counter interval

● 概要

このコマンドを用いて、PPS パケット統計情報通知間隔を設定します。

● 構文

config pps notification counter interval <value 1-120>

● パラメータ

<value 1-120>	パケットの統計情報を通知する間隔が秒単位で指定します。工場出荷時は 5 秒に設定されています。 PPS パケット統計情報通知間隔の値は 1 ～ 120 秒です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS パケット統計情報通知間隔を設定するには：

```
Zxxx0:admin# config pps notification counter interval 50
Command: config pps notification counter interval 50

Success.

Zxxx0:admin#
```

51.13. config pps notification counter add

● 概要

このコマンドを用いて、PPS パケット統計情報通知を有効にします。

● 構文

config pps notification counter add <portlist>

● パラメータ

<portlist>	パケットの統計情報を取得する対象ポートを指定します。工場出荷時は全てのポートが指定されています。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS パケット統計情報通知を有効にするには：

```
Zxxx0:admin# config pps notification counter add 1-4
Command: config pps notification counter add 1-4

Success.

Zxxx0:admin#
```

51.14. config pps notification delete add

● 概要

このコマンドを用いて、PPS パケット統計情報通知を無効にします。

● 構文

config pps notification counter delete <portlist>

● パラメータ

<portlist> パケットの統計情報取得を無効にする対象ポートを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS パケット統計情報通知を無効にするには：

```
Zxxx0:admin# config pps notification counter delete 1-4
Command: config pps notification counter delete 1-4

Success.

Zxxx0:admin#
```

51.15. show pps connection

● 概要

このコマンドを用いて、PPS コネクションテーブルを表示します。

● 構文

show pps connection

● パラメータ

なし

● 制限

なし

● 実行例

PPS コネクションテーブルを表示するには：

```
Zxxx0:admin# show pps connection
Command: show pps connection

 PPS Destination   PPS Gateway       Port  VID  Tag
 ----------------- ----------------- ----- ---- ---
 00-06-A5-5C-25-7A 00-06-A5-5C-25-7A 23    1    No

 Total Entries : 1

Zxxx0:admin#
```

51.16. config pps ports

● 概要

このコマンドは、PPS ポートプライオリティを設定するために使用します。PPS ポートプライオリティは、PPS コントローラポートを選択するために使用されます。
* 注意：優先度 0 のポートは PPS パケットを送信しません。

● 構文

config pps ports <portlist> priority <value 0-255>

● パラメータ

<portlist> 設定する PPS ポートを指定します。。
<value 0-255> PPS ポートの優先度を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS ポートプライオリティを設定するには：

```
Zxxx0:admin# config pps ports 10 priority 255
Command: config pps ports 10 priority 255

Success.


Zxxx0:admin#
```

51.17. show pps ports

● 概要

このコマンドは、PPS ポートの状態を表示するために使用します。

● 構文

show pps ports

● パラメータ

なし

● 制限

なし

● 実行例

PPS ポートの状態を表示するには：

```
Zxxx0:admin#show pps ports
Command: show pps ports

 Port  State      AdminPri. OperPri.
 ----- ---------- --------- --------
 1     Forwarding 128       128
 2     Forwarding 128       128
 3     Forwarding 128       128
 4     Forwarding 128       128
 5     Forwarding 128       128
 6     Forwarding 128       128
 7     Forwarding 128       128
 8     Forwarding 128       128
 9     Forwarding 128       128
 10    Forwarding 128       128
 11    Forwarding 128       128
 12    Forwarding 128       128
 13    Forwarding 128       128
 14    Forwarding 128       128
 15    Forwarding 128       128
 16    Forwarding 255       255
 17    Forwarding 128       128
 18    Forwarding 128       128
 19    Forwarding 128       128
 20    Forwarding 128       128
 21    Forwarding 128       128
 22    Forwarding 128       128
 23    Forwarding 128       0
 24    Forwarding 128       128
 25    Forwarding 128       128
 26    Forwarding 128       128
 27    Forwarding 128       128
 28    Forwarding 128       128

Zxxx0:admin#
```

51.18. restart pps

● 概要

restart pps コマンドは、機器のステータスを standalonen にし、PPSP 機能を再始動するために使用されます。
restart pps connection コマンドは、PPS コントローラの接続ポートを再認識するために使用されます。このコマンドを実行すると、Connection && Retry パケットが送信されます。

● 構文

restart pps [connection]

● パラメータ

[connection] Connection && Retry パケットを送信するために使用されます。
オプションは指定しない場合は PPSP 機能を再起動するために使用されます。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPSP 機能を再始動するには：

```
Zxxx0:admin# restart pps
Command: restart pps
Success.

Zxxx0:admin#
```

51.19. config pps connection add

● 概要

このコマンドを用いて、PPS コネクションを作成します。

● 構文

config pps connection add <macaddr> <macaddr> <vlanid 1-4094> <port> {send [tagged | untagged]}

● パラメータ

<macaddr> 1 番目の <macaddr> は PPS コネクションに追加する MAC アドレスを指定します。
<macaddr> 2 番目の <macaddr> は PPS コネクションに追加するゲートウェイ MAC アドレスを指定します。
<vlanid 1-4094> PPS コネクションに追加する VLAN ID を指定します。
<port> PPS コネクションに追加するポート番号を指定します。
[tagged | untagged] PPS コネクションに追加するタグを指定します。このタグフィールドは、ゲートウェイへの PPS パケットの送信に使用されます。このフィールドが指定されていない場合、デフォルトではタグなしが使用されます。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS コネクションを作成するには：

```
Zxxx0:admin#config pps connection add 00-00-00-00-00-02 00-00-00-00-00-01 1 23
Command: config pps connection add 00-00-00-00-00-02 00-00-00-00-00-01 1 23

Success.

Zxxx0:admin#
```

51.20. config pps connection delete

● 概要

このコマンドを用いて、PPS コネクションを削除します。

● 構文

config pps connection delete <macaddr> <macaddr>

● パラメータ

<macaddr> 1 番目の <macaddr> は削除する PPS コネクションの MAC アドレスを指定します。
<macaddr> 2番目の<macaddr>は削除するPPSコネクションのゲートウェイMACアドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS コネクションを削除するには：

```
Zxxx0:admin#config pps connection delete 00-00-00-00-00-02 00-00-00-00-00-01
Command: config pps connection delete 00-00-00-00-00-02 00-00-00-00-00-01

Success.

Zxxx0:admin#
```

51.21. config pps retry count

● 概要

このコマンドは、PPS 再試行回数を設定するために使用します。ターゲットデバイスからの応答がなければ、パケットの送信を再試行します。

● 構文

config pps retry count <value 1-5>

● パラメータ

<value 1-5> PPS の再試行回数を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS 再試行回数を設定するには：

```
Zxxx0:admin#config pps retry count 1
Command: config pps retry count 1

Success.

Zxxx0:admin#
```

51.22. config pps timeout

● 概要

このコマンドは、PPS タイムアウトを設定するために使用されます。PPS コントローラ応答を待つために使用されます。

● 構文

config pps timeout <sec 1-10>

● パラメータ

<sec 1-10> PPS のタイムアウト時間を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

PPS タイムアウトを設定するには：

```
Zxxx0:admin#config pps timeout 5
Command: config pps timeout 5

Success.


Zxxx0:admin#
```

52. プロトコル VLAN コマンド

プロトコル VLAN とは、受信パケットのヘッダに記載されたプロトコル情報に基づいて、所属する VLAN を決定するしくみです。
Ethernet ver2、Sub Network Access Protocol（SNAP）または Link Logical Control（LLC）のフレームタイプを指定し、VLAN に対応づけることができます。

create dot1v_protocol_group group_id <id> group_name <name 32>
config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]
delete dot1v_protocol_group [group_id <id> | group_name <name 32>| all]
show dot1v_protocol_group {group_id <id> | group_name <name 32>}
config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id> | group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]
show port dot1v {ports <portlist>}

52.1. create dot1v_protocol_group

● 概要

このコマンドを用いて、プロトコル VLAN 機能のプロトコルグループを作成します。

● 構文

create dot1v_protocol_group group_id <id> group_name <name 32>

● パラメータ

group_id **プロトコルのセットを識別するために用いるプロトコルグループの ID を指定します。** **<id>** ID の範囲は 1 ～ 16 です。
group_name プロトコルグループの名前を指定します。 **<name 32>** プロトコルグループの名前を指定します。最大文字数は 32 文字です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

プロトコルグループを作成するには：

```
Zxxx0:admin#create dot1v_protocol_group group_id 4 group_name General_Group
Command: create dot1v_protocol_group group_id 4 group_name General_Group

Success.
Zxxx0:admin#
```

52.2. config dot1v_protocol_group

● 概要

このコマンドを用いて、プロトコルグループにプロトコルを追加します。事前に定義されたフレームタイプのプロトコル値を指定できます。

● 構文

config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]

● パラメータ

group_id プロトコルのセットを識別するために用いるプロトコルグループの ID を指定します。
<id> ID の範囲は 1 ～ 16 です。

group_name
プロトコルグループの名前を指定します。
<name 32>
プロトコルグループの名前を指定します。最大文字数は 32 文字です。

add protocol
追加するプロトコルを指定します。フレームタイプに応じて、オクテット文字列が以下のいずれかの値を持ちます。入力形式は 0x0 ～ 0xffff です。
ethernet_2
16 ビット（2 オクテット）の 16 進数値です。例：IPv4 は 800、IPv6 は 86dd、ARP は 806 など。
ieee802.3_snap
16 ビット（2 オクテット）の 16 進数値です。例：IPv4 は 800、IPv6 は 86dd、ARP は 806 など。
ieee802.3_llc
2 オクテットの IEEE 802.2 LSAP（Link Service Access Point）ペアです。最初のオクテットは DSAP（Destination Service Access Point）、2 番目のオクテットは SSAP（Source Service Access Port）を示します。

<protocol_value>
フレームタイプのプロトコルを識別するためのプロトコル値を指定します。入力形式は 0x0 ～ 0xffff です。フレームタイプに応じて、オクテット文字列が以下のいずれかの値を持ちます。Ethernet II の場合、16 ビット（2 オクテット）の 16 進数値です。例えば、IPv4 は 800、IPv6 は 86dd、ARP は 806 などです。IEEE802.3 SNAP の場合、これは 16 ビット（2 オクテット）の 16 進数値です。IEEE802.3 LLC の場合、これは 2 オクテットの IEEE 802.2 LSAP（Link Service Access Point）ペアです。最初のオクテットは DSAP（Destination Service Access Point）、2 番目のオクテットは SSAP（Source Service Access Port）です。

delete protocol

削除するプロトコルを指定します。フレームタイプに応じて、オクテット文字列が以下のいずれかの値を持ちます。入力形式は 0x0 ～ 0xffff です。

ethernet_2

16 ビット（2 オクテット）の 16 進数値です。例：IPv4 は 800、IPv6 は 86dd、ARP は 806 など。

ieee802.3_snap

16 ビット（2 オクテット）の 16 進数値です。例：IPv4 は 800、IPv6 は 86dd、ARP は 806 など。

ieee802.3_llc

2 オクテットの IEEE 802.2 LSAP（Link Service Access Point）ペアです。最初のオクテットは DSAP（Destination Service Access Point）、2 番目のオクテットは SSAP（Source Service Access Port）を示します。

<protocol_value>

フレームタイプのプロトコルを識別するためのプロトコル値を指定します。入力形式は 0x0 ～ 0xffff です。フレームタイプに応じて、オクテット文字列が以下のいずれかの値を持ちます。Ethernet II の場合、16 ビット（2 オクテット）の 16 進数値です。例えば、IPv4 は 800、IPv6 は 86dd、ARP は 806 などです。IEEE802.3 SNAP の場合、これは 16 ビット（2 オクテット）の 16 進数値です。IEEE802.3 LLC の場合、これは 2 オクテットの IEEE 802.2 LSAP（Link Service Access Point）ペアです。最初のオクテットは DSAP（Destination Service Access Point）、2 番目のオクテットは SSAP（Source Service Access Port）です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

プロトコルグループ ID4 にプロトコル IPv6 を追加するには：

```
Zxxx0:admin# config dot1v_protocol_group group_id 4 add protocol ethernet_2 86dd
Command: config dot1v_protocol_group group_id 4 add protocol ethernet_2 86dd

Success.
Zxxx0:admin#
```

プロトコルグループ ID4 からプロトコル IPv6 を削除するには：

```
Zxxx0:admin# config dot1v_protocol_group_group_id 4 delete protocol ethernet_2
86dd
Command: config dot1v_protocol_group group_id 4 delete protocol ethernet_2 86dd

Success.
Zxxx0:admin#
```

52.3. delete dot1v_protocol_group

● 概要

このコマンドを用いて、プロトコルグループを削除します。

● 構文

delete dot1v_protocol_group [group_id <id> | group_name <name 32> | all]

● パラメータ

group_id	削除するグループ ID を指定します。 <id> 削除するグループ ID を指定します。
group_name	削除するプロトコルグループの名前を指定します。 <name 32> 削除するプロトコルグループの名前を指定します。最大文字数は 32 文字です。
all	すべてのプロトコルグループを削除します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

プロトコルグループ ID4 を削除するには：

```
Zxxx0:admin# delete dot1v_protocol_group group_id 4
Command: delete dot1v_protocol_group group_id 4

Success.
Zxxx0:admin#
```

52.4. show dot1v_protocol_group

● 概要

このコマンドを用いて、プロトコルグループに定義されているプロトコルを表示します。

● 構文

show dot1v_protocol_group {group_id <id> | group_name <name 32>}

● パラメータ

group_id	（オプション）表示するグループ ID を指定します。 <id> 表示するグループ ID を指定します。

group_name （オプション）表示するプロトコルグループの名前を指定します。 <name 32> 表示するプロトコルグループの名前を指定します。最大文字数は 32 文字です。

NOTE パラメータを指定しない場合、設定されたすべてのプロトコルグループが表示されます。

● 制限

なし

● 実行例

プロトコルグループ ID4 を表示するには：

```
Zxxx0:admin# show dot1v_protocol_group group_id 4
Command: show dot1v_protocol_group group_id 4

Protocol         Protocol              Frame Type             Protocol
Group ID        Group Name                                     Value
---------     ---------------      ------------        ------------
4             General Group         EthernetII              86dd

Total Entries: 1

Zxxx0:admin#
```

52.5. config port dot1v ports

● 概要

このコマンドを用いて、設定されたプロトコルグループに基づいて、入ってくるタグなしパケットにポートリストから VLAN を割り当てます。この割り当ては、delete protocol_group オプションを用いて削除できます。
コマンドでプライオリティを指定しない場合、ポートのデフォルトプライオリティが、プロトコル VLAN で分類されたタグなしパケットのプライオリティになります。

● 構文

config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id>| group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]

● パラメータ

<portlist>	このコマンドを適用するポートの範囲を指定します。
all	すべてのポートを指定します。

add protocol_group	プロトコルグループを追加します。 group_id プロトコルグループのグループ ID を指定します。 <id> プロトコルグループのグループ ID を指定します。 group_name プロトコルグループの名前を指定します。 <name 32> プロトコルグループの名前を指定します。最大文字数は 32 文字です。
vlan	このポートのプロトコルグループに関連付ける VLAN の名前を指定します。 <vlan_name 32> このポートのプロトコルグループに関連付ける VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	このポートのプロトコルグループに関連付ける VLAN ID を指定します。 <id> このポートのプロトコルグループに関連付ける VLAN ID を指定します。
priority	プロトコルにより指定の VLAN に分類されているパケットに関連付けるプライオリティを指定します。 <value 0-7> 0 ～ 7 の値を指定します。
delete protocol_group	プロトコルグループを削除します。 group_id 削除するグループ ID を指定します。 <id> グループ ID を指定します。 all すべてのグループを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 3 のグループ ID 4 を VLAN 2 に関連付けるように設定するには：

```
Zxxx0:admin# config port dot1v ports 3 add protocol_group group_id 4 vlan VLAN2
Command: config port dot1v ports 3 add protocol_group group_id 4 vlan VLAN2

Success.
Zxxx0:admin#
```

52.6. show port dot1v

● 概要

このコマンドを用いて、プロトコルグループに基づいて、ポートで受信されたタグなしパケットに関連付けられる VLAN を表示します。

● 構文

show port dot1v {ports <portlist>}

● パラメータ

ports	（オプション）表示するポートの範囲を指定します。 <portlist> 表示するポートの範囲を指定します。

NOTE パラメータを指定しない場合、すべてのポートの情報が表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 2 のプロトコル VLAN の情報を表示するには：

```
Zxxx0:admin# show port dot1v ports 1-2
Command: show port dot1v ports 1-2

Port: 1
 Protocol Group ID     VLAN Name                          Protocol Priority
 -------------------   --------------------------------   -----------------
 1                     default                            -

 Port: 2
 Protocol Group ID     VLAN Name                          Protocol Priority
 -------------------   --------------------------------   -----------------
 1                     default                            1

Total Entries  :  2

Zxxx0:admin#
```

53. QoS コマンド

QoS（Quality of Service）とは、通信の目的に応じて最適な帯域割り当てを行うことで、それぞれの通信に求められるレスポンスタイムやスループットを確保するしくみです。
受信パケットのヘッダに付加されたプライオリティタグ（優先順位情報）に基づいて、通信の優先制御を行います。
また、ポート毎の送受信やプライオリティタグに応じた帯域制限を行うことができます。

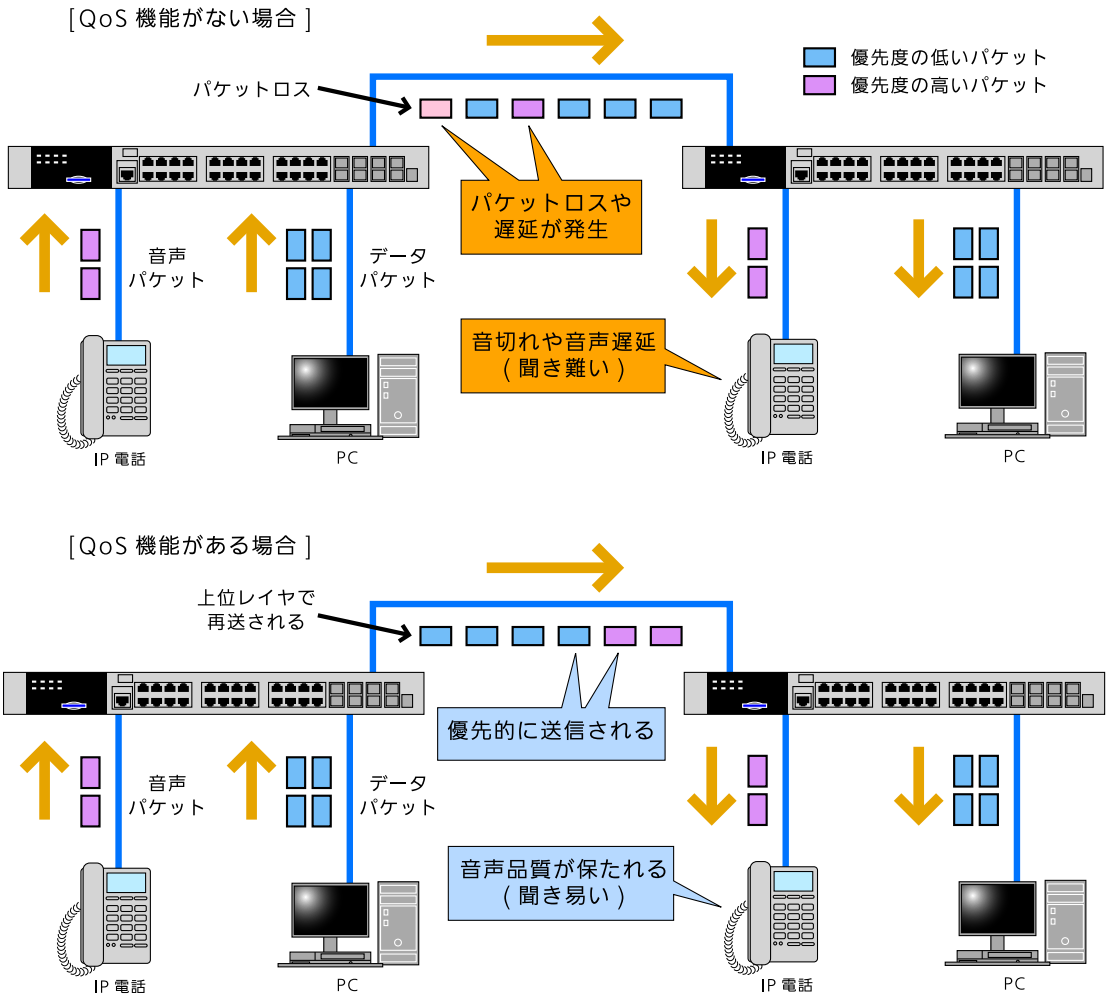


図 53-1　QoS の概略

config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-10240000>] | tx_rate [no_limit | <value 64-10240000>]}(1)
show bandwidth_control {<portlist>}
config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate [no_limit | <value 64-10240000>]} max_rate [no_limit | <value 64-10240000>]}(1)
show per_queue bandwidth_control {<portlist>}
config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]
config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr]
show scheduling {<portlist>}
show scheduling_mechanism {<portlist>}
config 802.1p user_priority <priority 0-7> <class_id 0-7>
show 802.1p user_priority
config 802.1p default_priority [<portlist> | all] <priority 0-7>
show 802.1p default_priority {<portlist>}
enable hol_prevention
disable hol_prevention
show hol_prevention
config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63>]
config dscp trust [<portlist> | all] state [enable | disable]
show dscp map {<portlist>} [dscp_priority | dscp_dscp] {dscp <dscp_list>}
show dscp trust {<portlist>}

53.1. config bandwidth_control

● 概要

このコマンドを用いて、ポートの帯域の最大制限値を設定します。

● 構文

config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-10240000>] | tx_rate [no_limit | <value 64-10240000>]}(1)

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを指定します。
rx_rate	（オプション）受信データレートの制限を指定します。 no_limit 受信ポートの帯域に制限を設けないことを指定します。 <value 64-10240000> 64 ～ 10240000 の整数値を指定して、Kbit/ 秒単位で最大制限値を設定します。指定した帯域制限と等しくなる場合はありますが、超えることはありません。正確な論理制限またはトークン値は、ハードウェアによって決定されます。注：1Kbit = 1000bit、1Gigabit = 1000*1000 Kbit。 実際に表示される値は次の計算式によって算出されます。小数点以下は切り捨てられますので、設定される値は 64 の倍数です。実際のレート = （入力レート /64) * 64。

tx_rate	（オプション）送信データレートの制限を指定します。 no_limit 送信ポートの帯域に制限を設けないことを指定します。 <value 64-10240000> 64 ～ 10240000 の整数値を指定して、Kbit/ 秒単位で最大制限値を設定します。指定した帯域制限と等しくなる場合はありますが、超えることはありません。正確な論理制限またはトークン値は、ハードウェアによって決定されます。注：1Kbit = 1000bit、1Gigabit = 1000*1000 Kbit。 実際に表示される値は次の計算式によって算出されます。小数点以下は切り捨てられますので、設定される値は 64 の倍数です。実際のレート = （入力レート /64) * 64。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポートの帯域を設定するには：

```
Zxxx0:admin#config bandwidth_control 1-10 tx_rate 1024
Command: config bandwidth_control 1-10 tx_rate 1024

Success.

Zxxx0:admin#
```

53.2. show bandwidth_control

● 概要

このコマンドを用いて、ポートの帯域設定を表示します。RADIUS サーバにより、認証プロセス中に帯域を割り当てることもできます。RADIUS サーバにより帯域を割り当てた場合は、RADIUS により割り当てられた帯域が有効になります。

● 構文

show bandwidth_control {<portlist>}

● パラメータ

<portlist>	（オプション）表示するポートの範囲を指定します。

NOTE パラメータを指定しない場合、すべてのポートの帯域設定が表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 2 のポート帯域制御テーブルを表示するには：

```
Zxxx0:admin#show bandwidth_control 1-2
Command: show bandwidth_control 1-2

Bandwidth Control Table

Port   RX Rate       TX Rate       Effective RX        Effective TX
      (Kbit/sec)    (Kbit/sec)    (Kbit/sec)          (Kbit/sec)
----  ----------    ----------    ----------------    ----------------
 1    No Limit      No Limit      No Limit            No Limit
 2    No Limit      No Limit      No Limit            No Limit

Zxxx0:admin#
```

53.3. config per_queue bandwidth_control

● 概要

このコマンドを用いて、指定したポートの特定の出力キューそれぞれの帯域制御を設定します。最大レートにより帯域を制限します。これを指定すると、追加の帯域を利用できる場合でも、キューから転送されるパケットが指定された制限を超えることはありません。キューが strict モードまたは SDWRR（Shaped Deficit Weighted Round Robin）モードのいずれで動作しているかに関係なく、最大レートの指定が有効になります。

● 構文

config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate [no_limit | <value 64-10240000>]} max_rate [no_limit | <value 64-10240000>]}(1)

● パラメータ

ports	（オプション）設定するポートの範囲を指定します。 <portlist> 設定するポートの範囲を指定します。 all　システムのすべてのポートを設定します。パラメータを指定しない場合、すべてのポートが設定されます。
<cos_id_list 0-7>	プライオリティキューのリストを指定します。プライオリティキューの番号は 0 ～ 7 です。
min_rate	以下のパラメータの 1 つが、最小レートに適用されます。上記で指定したクラスがこのレートでパケットを転送できます。 no_limit 指定したポート帯域の出力キューに制限はありません。 <value 64-10240000> 64 ～ 10240000 の整数値を指定して、Kbit/ 秒単位で最小制限値を設定します。指定した帯域制限と等しくなる場合はありますが、超えることはありません。正確な論理制限またはトークン値は、ハードウェアによって決定されます。注：1Kbit = 1000bit、1Gigabit = 1000*1000 Kbit。実際のレート = （入力レート /64) * 64。

max_rate以下のパラメータの 1 つが、最大レートに適用されます。上記で指定したクラスがこのレートでパケットを転送できます。 no_limit 指定したポート帯域の出力キューに制限はありません。 <value 64-10240000> 64 ～ 10240000 の整数値を指定して、Kbit/ 秒単位で最大制限値を設定します。指定した帯域制限と等しくなる場合はありますが、超えることはありません。正確な論理制限またはトークン値は、ハードウェアによって決定されます。注：1Kbit = 1000bit、1Gigabit = 1000*1000 Kbit。実際のレート = （入力レート /64) * 64。	

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 10 のキュー 1 の最大レートを 100 に設定するには：

```
Zxxx0:admin#config per_queue bandwidth_control ports 1-10 1 max_rate 100
Command: config per_queue bandwidth_control ports 1-10 1 max_rate 100

 Granularity: TX: 64. Actual Rate: MAX: 64.

Success.

Zxxx0:admin#
```

53.4. show per_queue bandwidth_control

● 概要

このコマンドを用いて、各ポートの出力キューそれぞれの帯域制御設定を表示します。

● 構文

show per_queue bandwidth_control {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。	

● 制限

なし

● 実行例

ポート 1 のポート帯域制御テーブルを表示するには：

```
Zxxx0:admin#show per_queue bandwidth_control 1
Command: show per_queue bandwidth_control 1

Queue Bandwidth Control Table On Port: 1

Queue     Min Rate(Kbit/sec)     Max Rate(Kbit/sec)
0         No Limit               No Limit
1         No Limit               No Limit
2         64                     1024
3         64                     No Limit
4         No Limit               No Limit
5         No Limit               No Limit
6         No Limit               No Limit
7         No Limit               No Limit

Zxxx0:admin#
```

53.5. config scheduling

● 概要

このコマンドを用いて、各 CoS キューのトラフィックのスケジューリングメカニズムを設定します。

● 構文

config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]

● パラメータ

ports	（オプション）設定するポートの範囲を指定します。 <portlist> ポートのリストを入力します。 all すべてのポートを使用します。
<class_id 0-7>	config scheduling コマンドを適用する 8 つのハードウェアプライオリティキューを指定します。8 つのハードウェアプライオリティキューは 0 ～ 7 の番号で識別します。一番優先順位が低いのが 0 のキューです。
strict	キューが strict モードで動作します。
weight	重み付きラウンドロビンの重み付け値を指定します。ポートモードが WRR の場合は、キューが WRR モードで動作します。ポートモードが strict の場合は、strict モードで動作します。 <value 1-127> 重み付け値を入力します。この値は 1 ～ 127 の必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

最大パケット値を 10 にして、CoS キュー 0 のトラフィックのスケジューリングを設定するには：

```
Zxxx0:admin#config scheduling 0 weight 10
Command: config scheduling 0 weight 10

Success.

Zxxx0:admin#
```

ポート 1:10 で、重み付け値を 25 にして、CoS キュー 1 のトラフィックのスケジューリングを設定するには：

```
Zxxx0:admin# config scheduling ports 1:10 1 weight 25
Command: config scheduling ports 1:10 1 weight 25

Success.

Zxxx0:admin#
```

53.6. config scheduling_mechanism

● 概要

このコマンドを用いて、各 CoS キューのトラフィックのスケジューリングメカニズムを設定します。

● 構文

config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr]

● パラメータ

ports	（オプション）設定するポートの範囲を指定します。 <portlist> ポートのリストを入力します。 all すべてのポートを使用します。
strict	すべてのキューが strict モードで動作します。
wrr	各キューが重み付け設定に基づいて動作します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

各 CoS キューのトラフィックのスケジューリングメカニズムを設定するには：

```
Zxxx0:admin# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

Zxxx0:admin#
```

ポート 1:1 の CoS キューのトラフィックのスケジューリングメカニズムを設定するには：

```
Zxxx0:admin# config scheduling_mechanism ports 1:1 strict
Command: config scheduling_mechanism ports 1:1 strict

Success.

Zxxx0:admin#
```

53.7. show scheduling

● 概要

このコマンドを用いて、現在のトラフィックのスケジューリングパラメータを表示します。

● 構文

show scheduling {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

● 制限

なし

● 実行例

各 CoS キューのトラフィックのスケジューリングパラメータを表示するには：

```
Zxxx0:admin#show scheduling
Command: show scheduling

QOS Output Scheduling On Port: 1
Class ID  Weight
--------  ------
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8

QOS Output Scheduling On Port: 2
Class ID  Weight
--------  ------
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

ポート 1:1 の各 CoS キューのトラフィックのスケジューリングパラメータを表示するには：

```
Zxxx0:admin#show scheduling 1
Command: show scheduling 1

QOS Output Scheduling On Port: 1
Class ID  Weight
--------  ------
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8

Zxxx0:admin#
```

53.8. show scheduling_mechanism

● 概要

このコマンドを用いて、トラフィックのスケジューリングメカニズムを表示します。

● 構文

show scheduling_mechanism {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

● 制限

なし

● 実行例

すべてのポートのスケジューリングメカニズムを表示するには：

```
Zxxx0:admin#show scheduling_mechanism
Command: show scheduling_mechanism

Port    Mode
-----   ------
1       Strict
2       Strict
3       Strict
4       Strict
5       Strict
6       Strict
7       Strict
8       Strict
9       Strict
10      Strict
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

ポート 1 ～ 10 のスケジューリングメカニズムを表示するには：

```
Zxxx0:admin#show scheduling_mechanism 1-10
Command: show scheduling_mechanism 1-10

Port    Mode
-----   ------
1       Strict
2       Strict
3       Strict
4       Strict
5       Strict
6       Strict
7       Strict
8       Strict
9       Strict
10      Strict

Zxxx0:admin#
```

53.9. config 802.1p user_priority

● 概要

このコマンドを用いて、802.1p ユーザプライオリティに基づいて、スイッチが受信パケットをマッピングする方法を、スイッチの利用可能な 8 つのハードウェアプライオリティキューの 1 つに設定します。スイッチのデフォルトでは、以下の 802.1p ユーザプライオリティ値が 8 つのハードウェアプライオリティキューにマッピングされます。以下の表に推奨マッピングを示します。802.1p ユーザプライオリティを指定して<class_id>に割り当てることにより、ユーザがこのマッピングを変更できます。

フレームの プライオリティ	ASIC のプライオリティキュー	注釈
0	2	中の下
1	0	最低
2	1	最低
3	3	中の下
4	4	中の上
5	5	中の上
6	6	最高
7	7	最高

● 構文

config 802.1p user_priority <priority 0-7> <class_id 0-7>

● パラメータ

<priority 0-7>
<class_id>(ハードウェアキューの番号)に関連付ける 802.1p ユーザプライオリティを指定します。

<class_id 0-7>	スイッチのハードウェアプライオリティキューの番号を指定します。スイッチには 8 つのハードウェアプライオリティキューがあります。キューには、0（最低の優先順位）から 7（最高の優先順位）の番号が付いています。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

802.1p ユーザプライオリティの 1 を、3 のクラス ID に割り当てるには：

```
Zxxx0:admin#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

Zxxx0:admin#
```

53.10. show 802.1p user_priority

● 概要

このコマンドを用いて、802.1p ユーザプライオリティを表示します。

● 構文

show 802.1p user_priority

● パラメータ

● 制限

なし

● 実行例

802.1p ユーザプライオリティを表示するには：

```
Zxxx0:admin#show 802.1p user_priority
Command: show 802.1p user_priority

 QoS Class of Traffic

 Port 1
     Priority-0  ->  <Class-2>
     Priority-1  ->  <Class-0>
     Priority-2  ->  <Class-1>
     Priority-3  ->  <Class-3>
     Priority-4  ->  <Class-4>
     Priority-5  ->  <Class-5>
     Priority-6  ->  <Class-6>
     Priority-7  ->  <Class-7>

 Port 2
     Priority-0  ->  <Class-2>
     Priority-1  ->  <Class-0>
     Priority-2  ->  <Class-1>
     Priority-3  ->  <Class-3>
     Priority-4  ->  <Class-4>
     Priority-5  ->  <Class-5>
     Priority-6  ->  <Class-6>
     Priority-7  ->  <Class-7>

Zxxx0:admin#
```

53.11. config 802.1p default_priority

● 概要

このコマンドを用いて、スイッチのポートで受信したタグのないパケットのデフォルトプライオリティを指定します。

● 構文

config 802.1p default_priority [<portlist> | all] <priority 0-7>

● パラメータ

<portlist>	デフォルトプライオリティを設定するポートの範囲を指定します。つまり、指定した範囲のポートでは、受信したすべてのタグのないパケットに、以下で指定するプライオリティが割り当てられます。ポートリストの範囲の最初と最後をダッシュで区切ります。
all	スイッチのすべてのポートにコマンドが適用されます。
<priority 0-7>	スイッチまたは指定した範囲のポートが受信したタグのないパケットに割り当てるプライオリティ値（0 ～ 7）を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

本装置のすべてのポートについて、802.1p デフォルトプライオリティ設定を 5 に指定するには：

```
Zxxx0:admin#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

Zxxx0:admin#
```

53.12. show 802.1p default_priority

● 概要

このコマンドを用いて、スイッチの現在のデフォルトプライオリティ設定を表示します。デフォルトプライオリティは、RADIUS サーバにより認証プロセス中に割り当てることもできます。RADIUS サーバによる認証はポート毎またはユーザ毎に実行できます。ポート毎の認証の場合、RADIUS サーバにより割り当てられるプライオリティが、有効なポートのデフォルトプライオリティになります。ユーザ毎の認証の場合、RADIUS が割り当てるプライオリティは、MAC アドレスに関連付けられたプライオリティが割り当てられるため有効なポートのデフォルトプライオリティにはなりません。ユーザ毎の認証を行うことができるのは、MAC ベースの VLAN をサポートする装置のみであることにご注意ください。

● 構文

show 802.1p default_priority {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

NOTE パラメータを指定しない場合、802.1p デフォルトプライオリティを持つすべてのポートが表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 4 の 802.1p デフォルトプライオリティを表示するには：

```
Zxxx0:admin#show 802.1p default_priority 1-4
Command: show 802.1p default_priority 1-4

Port       Priority      Effective Priority
----       -----------   ------------------
1          0             0
2          0             0
3          0             0
4          0             0

Zxxx0:admin#
```

53.13. enable hol_prevention

● 概要

このコマンドを用いて、スイッチの HOL ブロッキングを有効にします。

● 構文

enable hol_prevention

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチの HOL ブロッキングを有効にするには：

```
Zxxx0:admin#enable hol_prevention
Command: enable hol_prevention

Success.

Zxxx0:admin#
```

53.14. disable hol_prevention

● 概要

このコマンドを用いて、スイッチの HOL ブロッキングを無効にします。

● 構文

disable hol_prevention

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチの HOL ブロッキングを無効にするには：

```
Zxxx0:admin#disable hol_prevention
Command: disable hol_prevention

Success.

Zxxx0:admin#
```

53.15. show hol_prevention

● 概要

このコマンドを用いて、スイッチの HOL ブロッキングの状態を表示します。

● 構文

show hol_prevention

● パラメータ

なし

● 制限

なし

● 実行例

スイッチの HOL ブロッキングの状態を表示するには：

```
Zxxx0:admin#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled

Zxxx0:admin#
```

53.16. config dscp map

● 概要

このコマンドを用いて、DSCP からプライオリティへのマッピングを指定します。

● 構文

config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63>]

● パラメータ

<portlist>	(オプション) 設定対象ポートを指定します。指定がない場合はすべてのポートが対象になります。
all	(オプション) スイッチのすべてのポートにコマンドが適用されます。
dscp_priority	DSCP から特定のプライオリティへのマッピングを指定します。 <dscp_list> DSCP 値のリストを指定します。 <priority 0-7> マッピング先のプライオリティを指定します。
dscp_dscp	DSCP から特定の DSCP へのマッピングを指定します。 <dscp_list> DSCP 値のリストを指定します。 <dscp 0-63> マッピング先の DSCP を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 8 に対して DSCP 1 をプライオリティ 1 にマッピングするには：

```
Zxxx0:admin#config dscp map 1-8 dscp_priority 1 to 1
Command: config dscp map 1-8 dscp_priority 1 to 1

Success.

Zxxx0:admin#
```

53.17. config dscp trust

● 概要

このコマンドを用いて、DSCP トラスト状態を指定します。本状態を有効にすることで、プライオリティではなく DSCP の値が利用されます。

● 構文

config dscp trust [<portlist> | all] state [enable | disable]

● パラメータ

<portlist>	設定対象ポートを指定します。
all	スイッチのすべてのポートにコマンドが適用されます。
state	DSCP トラストの状態を指定します。 enable DSCP トラストを有効にします。 disable DSCP トラストを無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 8 の DSCP トラストを有効にするには：

```
Zxxx0:admin#config dscp trust 1-8 state enable
Command: config dscp trust 1-8 state enable

Success.

Zxxx0:admin#
```

53.18. show dscp map

● 概要

このコマンドを用いて、DSCP マップの設定を表示します。

● 構文

show dscp map {<portlist>} [dscp_priority | dscp_dscp] {dscp <dscp_list>}

● パラメータ

<portlist>	(オプション) を指定します。
dscp_priority	プライオリティとマッピングしている DSCP のリストを指定します。
dscp_dscp	DSCP とマッピングしている DSCP のリストを指定します。
dscp	(オプション)DSCP を指定します。 <dscp_list> DSCP リストを指定します。

● 制限

なし

● 実行例

ポート 1 の DSCP- プライオリティマッピングを表示するには :

```
Zxxx0:admin# show dscp map 1 dscp_priority
Command: show dscp map 1 dscp_priority

DSCP to 802.1p Priority Mapping:

Port 1
DSCP 0,2-7 is mapped to 0
DSCP 1,8-15 is mapped to 1
DSCP 16-23 is mapped to 2
DSCP 24-31 is mapped to 3
DSCP 32-39 is mapped to 4
DSCP 40-47 is mapped to 5
DSCP 48-55 is mapped to 6
DSCP 56-63 is mapped to 7

Zxxx0:admin#
```

ポート 1 の DSCP-DSCP マッピングを表示するには：

```
Zxxx0:admin# show dscp map 1 dscp_dscp
Command: show dscp map 1 dscp_dscp

DSCP to DSCP Mapping:
-------------------------------------------------------------
Port 1      |   0    1    2    3    4    5    6    7    8    9
------------+------------------------------------------------
          0 |   0    1    2    3    4    5    6    7    8    9
          1 |  10   11   12   13   14   15   16   17   18   19
          2 |  20   21   22   23   24   25   26   27   28   29
          3 |  30   31   32   33   34   35   36   37   38   39
          4 |  40   41   42   43   44   45   46   47   48   49
          5 |  50   51   52   53   54   55   56   57   58   59
          6 |  60   61   62   63
-------------------------------------------------------------

Zxxx0:admin#
```

53.19. show dscp trust

● 概要

このコマンドを用いて、DSCP トラストの設定を表示します。

● 構文

show dscp trust {<portlist>}

● パラメータ

<portlist> (オプション)ポートリストを指定します。指定がない場合は、すべてのポートの設定が表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 8 の DSCP トラスト設定を表示するには :

```
Zxxx0:admin# show dscp trust 1-8
Command: show dscp trust 1-8

Port DSCP-Trust
---- ----------
1    Enabled
2    Enabled
3    Enabled
4    Enabled
5    Enabled
6    Enabled
7    Enabled
8    Enabled

Zxxx0:admin#
```

54. リングプロトコルコマンド

リングプロトコルを用いることで、リング状の冗長ネットワークが構築でき、機器や通信経路上で異常が発生した場合は直ちに経路の切り替えを行うことで、障害発生時の高速復旧を実現することができます。
1 つのリングの単位を「ドメイン」、リングの監視・制御を行うスイッチを「Master ノード」、他のリング構成スイッチを「Transit ノード」と呼びます。Master ノードとするスイッチは 1 つのドメインに必ず 1 つのみ設定してください。
ドメインの作成には、リングの制御を行うための「Control VLAN」、および実際のネットワークデータが流れる「Data VLAN」の指定が必要です。

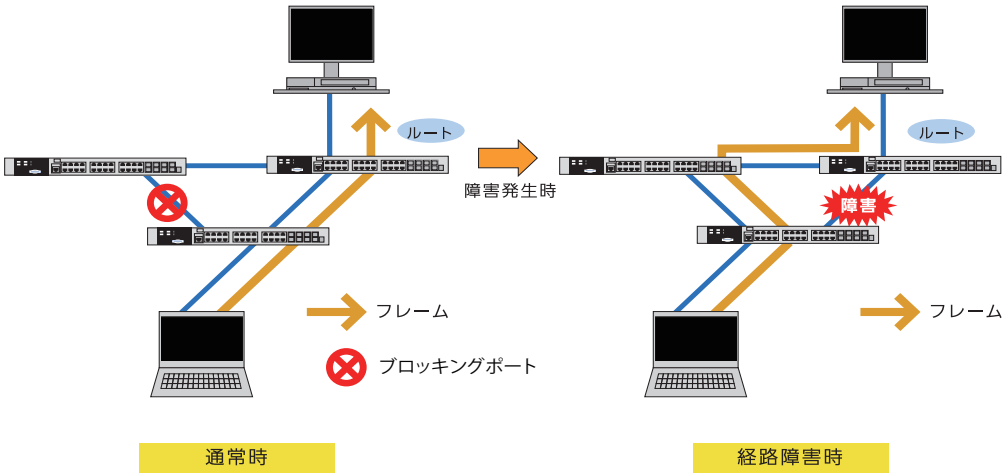


図 54-1　リングプロトコルの概要

config rrp domain <domain name> [type {master|transit}] [control_vlan_id <vid>] [data_vlan_id <vid list>] [primary_port <port num>] [secondary_port <port num>] [polling_interval <1-2sec>] [fail_period <2-5sec>] [ring_guard_port {primary|secondary|both|disable}]
create rrp domain <domain name> type {master|transit} control_vlan_id <vid> data_vlan_id <vid list> primary_port <port num> secondary_port <port num> [polling_interval <1-2sec>] [fail_period <2-5sec>] [ring_guard_port {primary|secondary|both|disable}]
delete rrp domain <domain name>
disable rrp
disable rrp domain <domain name>
enable rrp
enable rrp domain <domain name>
show rrp
show rrp status

54.1. config rrp domain

● 概要

このコマンドを用いて、リングプロトコルのドメインを編集します。

● 構文

config rrp domain <domain name> [type {master|transit}] [control_vlan_id <vid>] [data_vlan_id <vid list>] [primary_port <port num>] [secondary_port <port num>] [polling_interval <1-2sec>] [fail_period <2-5sec>] [ring_guard_port {primary|secondary|both|disable}]

● パラメータ

<domain name>
リングプロトコルで使用するドメインの名前を半角英数 1 ～ 25 文字で指定します。

type
リング構成時の役割を指定します。
master
リング構成を監視する Master ノードに指定します。Master ノードは 1 つのドメイン内に必ず 1 台のみ設定してください。
transit
リングを構成する Transit ノードに指定します。

control_vlan_id
リングの制御に必要な制御 VLAN ID を指定します。
<vid>
制御 VLAN ID を 2 ～ 4094 の間で指定します。すでに作成されている VLAN ID は指定できません。

data_vlan_id
ドメインでのデータ通信に利用するデータ VLAN ID を指定します。
<vid list>
データ VLAN ID を 1 ～ 4094 の間で指定します。複数指定する場合は、-（ハイフン）または ,（カンマ）で指定します。存在しない VLAN ID は指定できません。

primary_port
ノード間接続のためのプライマリポートを指定します。
<port num>
対象のポート番号を指定します。

secondary_port
ノード間接続のためのセカンダリポートを指定します。
<port num>
対象のポート番号を指定します。

polling_interval
リングプロトコルの制御フレームの送信間隔 (秒) を指定します。工場出荷時は 1 秒です。
<1-2 sec>
送信間隔を 1 ～ 2 秒の間で指定します。polling_interval と fail_period は同値には指定できません。

fail_period	リングプロトコルの制御フレームが受信できなくなった場合に、異常と判断するまでのタイムアウト時間を指定します。 **<2-5 sec>** タイムアウト時間を 2～5 秒の間で指定します。polling_interval と fail_period は同値には指定できません。
ring_guard_port	（オプション）リングガード機能を指定します。工場出荷時は disable に設定されています。 **primary** プライマリポートをリングガード対象ポートに指定します。 **secondary** セカンダリポートをリングガード対象ポートに指定します。 **both** プライマリポート、セカンダリポート双方をリングガード対象ポートに指定します。 **disable** リングガード機能を無効に指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

リングドメイン「pc-ring」のノードタイプを「Transit」、制御用 VLAN を 30、プライマリポートをポート 9、セカンダリポートをポート 10、データ VLAN を 1、Polling Interval を 1 秒、Fail Period を 2 秒に変更するには：

```
Zxxx0:admin# config rrp domain pc-ring type transit control_vlan_id 30 primary_port
9 secondary_port 10 data_vlan_id 1 polling_interval 1 fail_period 2
Command: config rrp domain pc-ring type transit control_vlan_id 30 primary_port 9
secondary_port 10 data_vlan_id 1 polling_interval 1 fail_period 2

Success.

Zxxx0:admin#
```

54.2. create rrp domain

● 概要

このコマンドを用いて、リングプロトコルのドメインを作成します。

● 構文

create rrp domain <domain name> type {master|transit} control_vlan_id <vlanid> data_vlan_id <vid list> primary_port <port> secondary_port <port num> [polling_interval <1-2sec>] [fail_period <2-5sec>] [ring_guard_port {primary|secondary|both|disable}]

● パラメータ

<domain name>
リングプロトコルで使用するドメインの名前を半角英数 1 ～ 25 文字で指定します。

type
リング構成時の役割を指定します。
master
リング構成を監視する Master ノードに指定します。Master ノードは 1 つのドメイン内に必ず 1 台のみ設定してください。
transit
リングを構成する Transit ノードに指定します。

control_vlan_id
リングの制御に必要な制御 VLAN ID を指定します。
<vid>
制御 VLAN ID を 2 ～ 4094 の間で指定します。すでに作成されている VLAN ID は指定できません。

data_vlan_id
ドメインでのデータ通信に利用するデータ VLAN ID を指定します。
<vid list>
データ VLAN ID を 1 ～ 4094 の間で指定します。複数指定する場合は、-（ハイフン）または ,（カンマ）で指定します。存在しない VLAN ID は指定できません。

primary_port
ノード間接続のためのプライマリポートを指定します。
<port num>
対象のポート番号を指定します。

secondary_port
ノード間接続のためのセカンダリポートを指定します。
<port num>
対象のポート番号を指定します。

polling_interval
リングプロトコルの制御フレームの送信間隔 (秒) を指定します。工場出荷時は 1 秒です。
<1-2 sec>
送信間隔を 1 ～ 2 秒の間で指定します。polling_interval と fail_period は同値には指定できません。

fail_period
リングプロトコルの制御フレームが受信できなくなった場合に、異常と判断するまでのタイムアウト時間を指定します。
<2-5 sec>
タイムアウト時間を 2 ～ 5 秒の間で指定します。polling_interval と fail_period は同値には指定できません。

ring_guard_port
（オプション）リングガード機能を指定します。工場出荷時は disable に設定されています。
primary
プライマリポートをリングガード対象ポートに指定します。
secondary
セカンダリポートをリングガード対象ポートに指定します。
both
プライマリポート、セカンダリポート双方をリングガード対象ポートに指定します。
disable
リングガード機能を無効に指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ノードタイプが「Transit」、制御用 VLAN が 30、プライマリポートがポート 9、セカンダリポートがポート 10、データ VLAN が 1、Polling Interval が 1 秒、Fail Period が 2 秒のリングドメイン「pc-ring」を作成するには：

```
Zxxx0:admin# create rrp domain pc-ring type transit control_vlan_id 30 primary_port
9 secondary_port 10 data_vlan_id 1 polling_interval 1 fail_period 2
Command: create rrp domain pc-ring type transit control_vlan_id 30 primary_port 9
secondary_port 10 data_vlan_id 1 polling_interval 1 fail_period 2

Success.

Zxxx0:admin#
```

54.3. delete rrp domain

● 概要

このコマンドを用いて、対象のリングドメインを削除します。

● 構文

delete rrp domain <domain name>

● パラメータ

<domain name> 削除対象とするリングドメイン名を指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

・リングドメイン「pc-ring」を削除するには：

```
Zxxx0:admin# delete rrp domain pc-ring
Command: delete rrp domain pc-ring

Success.

Zxxx0:admin#
```

54.4. disable rrp

● 概要

このコマンドを用いて、スイッチ全体のリングプロトコル機能を無効にします。工場出荷時は、リングプロトコルの動作は無効に設定されています。

● 構文

disable rrp

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

スイッチのリングプロトコル機能を無効にするには：

```
Zxxx0:admin# disable rrp
Command: disable rrp

Success.

Zxxx0:admin#
```

54.5. disable rrp domain

● 概要

このコマンドを用いて、特定のリングドメインの動作を無効にします。

● 構文

disable rrp domain <domain name>

● パラメータ

<domain name> 動作を無効にするリングドメイン名を指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

リングドメイン「pc-ring」の動作を無効にするには：

```
Zxxx0:admin# disable rrp domain pc-ring
Command: disable rrp domain pc-ring

Success.

Zxxx0:admin#
```

54.6. enable rrp

● 概要

このコマンドを用いて、スイッチ全体のリングプロトコル機能を有効にします。工場出荷時は、リングプロトコルの動作は無効に設定されています。

● 構文

enable rrp

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

スイッチ全体のリングプロトコル機能を有効にするには：

```
Zxxx0:admin# enable rrp
Command: enable rrp

Success.

Zxxx0:admin#
```

54.7. enable rrp domain

● 概要

このコマンドを用いて、特定のリングドメインの動作を有効にします。

● 構文

enable rrp domain <domain name>

● パラメータ

<domain name> 動作を有効にするリングドメイン名を指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

リングドメイン「pc-ring」の動作を有効にするには：

```
Zxxx0:admin# enable rrp domain pc-ring
Command: enable rrp domain pc-ring

Success.

Zxxx0:admin#
```

54.8. show rrp

● 概要

このコマンドを用いて、リングプロトコルの設定を表示します。

● 構文

show rrp

● パラメータ

なし

● 制限

なし

● 実行例

リングプロトコルの設定を表示するには：

```
Zxxx0:admin# show rrp
Command: show rrp

RRP Status : Enabled
Total Domain Number(s) : 1

Domain Name  Ctrl VLAN  Data VLAN(s)                                Ring Status
------------ ---------- ------------------------------------------- -----------
pc-ring      30         1                                           Link-Up

Zxxx0:admin#
```

54.9. show rrp status

● 概要

このコマンドを用いて、リングドメインの設定を表示します。

● 構文

show rrp status <domain name>

● パラメータ

<domain name> 設定の表示対象のリングドメイン名を指定します。

● 制限

なし

● 実行例

リングドメイン「pc-ring」の設定を表示するには：

```
Zxxx0:admin# show rrp status pc-ring
Command: show rrp status pc-ring

RRP Domain Name         : pc-ring
RRP Domain Status       : Enabled
RRP Node Type           : Transit
RRP Ring Status         : Link-Up

Primary Port            : 10
Primary Port Status     : Forwarding
Primary Port Role       : Upstream

Secondary Port          : 11
Secondary Port Status   : Forwarding
Secondary Port Role     : Downstream

Polling Interval        : 1
Fail Period             : 2

Ring Guard Port         : Disable

Control VLAN            : 30
Data VLAN(s)            : 1

Zxxx0:admin#
```

55. RSPAN コマンド

RSPAN（Remote Switched Port ANalyzer）とは、他のスイッチ宛てに受信パケットをミラーリングする機能です。
パケットの送信元（ソーススイッチ）では、RSPAN VLAN ソース設定を行い、ミラーパケットを中継するスイッチでは、RSPAN VLAN リダイレクト設定を行う必要があります。

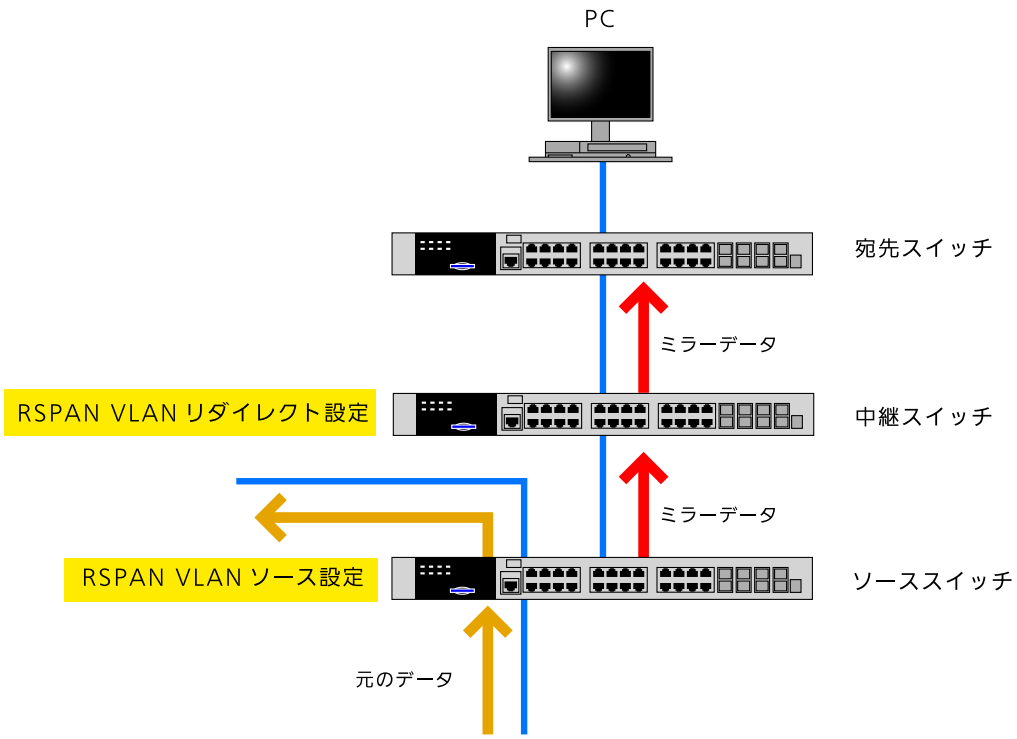


図 55-1　RSPAN の概略

enable rspan
disable rspan
create rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]
delete rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]
config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[mirror_group_id <value 1-4> | [add | delete] ports <portlist> [rx | tx | both]]}]
show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

55.1. enable rspan

● 概要

このコマンドを用いて、RSPAN をグローバルに有効にします。

● 構文

enable rspan

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

RSPAN をグローバルに有効にするには：

```
Zxxx0:admin#enable rspan
Command: enable rspan

Success.

Zxxx0:admin#
```

55.2. disable rspan

● 概要

このコマンドを用いて、RSPAN をグローバルに無効にします。

● 構文

disable rspan

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

RSPAN をグローバルに無効にするには：

```
Zxxx0:admin#disable rspan
Command: disable rspan

Success.

Zxxx0:admin#
```

55.3. create rspan vlan

● 概要

このコマンドを用いて、RSPAN VLAN を作成します。最大 16 の RSPAN VLAN を作成できます。

● 構文

create rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]

● パラメータ

vlan_name	VLAN 名に基づいて RSPAN VLAN を作成します。 <vlan_name> VLAN の名前を指定します。
vlan_id	VLAN ID に基づいて RSPAN VLAN を作成します。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

VLAN 名「v2」により、RSPAN VLAN エントリを作成するには：

```
Zxxx0:admin#create rspan vlan vlan_name v2
Command: create rspan vlan vlan_name v2

Success.

Zxxx0:admin#
```

VLAN ID「3」により、RSPAN VLAN エントリを作成するには：

```
Zxxx0:admin#create rspan vlan vlan_id 3
Command: create rspan vlan vlan_id 3

Success.

Zxxx0:admin#
```

55.4. delete rspan vlan

● 概要

このコマンドを用いて、RSPAN VLAN を削除します。

● 構文

delete rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]

● パラメータ

vlan_name	VLAN 名により RSPAN VLAN を指定します。 <vlan_name> VLAN の名前を指定します。
vlan_id	VLAN ID により RSPAN VLAN を指定します。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

VLAN 名「v2」により、RSPAN VLAN エントリを削除するには：

```
Zxxx0:admin#delete rspan vlan vlan_name v2
Command: delete rspan vlan vlan_name v2

Success.

Zxxx0:admin#
```

VLAN ID「3」により、RSPAN VLAN エントリを削除するには：

```
Zxxx0:admin#delete rspan vlan vlan_id 3
Command: delete rspan vlan vlan_id 3

Success.

Zxxx0:admin#
```

55.5. config rspan vlan

● 概要

ソーススイッチでこのコマンドを用いて、RSPAN VLAN の送信元の設定を指定します。中継スイッチまたは宛先スイッチでリダイレクトコマンドを用いて、RSPAN VLAN パケットの出力ポートを設定し、RSPAN VLAN パケットがリダイレクトポートに出て行くようにします。また、RSPAN VLAN が正しく機能するように、VLAN 設定を正しく指定する必要があります。具体的には、中継スイッチの場合、リダイレクトポートが RSPAN VLAN のタグ付きメンバポートである必要があります。宛先スイッチの場合、リダイレクトポートが RSPAN VLAN のタグ付きメンバポートまたはタグなしメンバポートのいずれかである必要があります。これはユーザの要件によって異なります。タグなしメンバシップを指定した場合、RSPAN VLAN タグが削除されます。リダイレクト機能は、RSPAN が有効な場合のみ機能します。複数の RSPAN VLAN に、同時にリダイレクト設定を指定できます。
1 つの RSPAN VLAN に、同時に送信元設定とリダイレクト設定を指定できます。

● 構文

config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[mirror_group_id <value 1-4> | [add | delete] ports <portlist> [rx | tx | both]]}]

● パラメータ

vlan_name	VLAN 名により RSPAN VLAN を指定します。 <vlan_name> VLAN の名前を指定します。
vlan_id	VLAN ID により RSPAN VLAN を指定します。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。
redirect	RSPAN VLAN パケットの出力ポートリストを指定します。リダイレクトポートがリンクアグリゲーションポートの場合、RSPAN パケットにリンクアグリゲーション動作が適用されます。 add リダイレクトポートを追加します。 deleteリダイレクトポートを削除します。
ports	RSPAN パケットを追加または削除する出力ポートリストを指定します。 <portlist> 設定するポートの範囲を指定します。

source	このコマンドでポートを指定しない場合、ミラーコマンドにより指定された送信元、または ACL により指定されたフローベースの送信元が、RSPAN の送信元になります。送信元のパラメータを指定しない場合、設定済みの送信元のパラメータが削除されます。 mirror_group_id ミラーグループ ID により、RSPAN 送信元機能に用いるミラーセッションを指定します。ミラーポートを設定するときにミラーグループを指定しない場合、ミラーグループ 1 がデフォルトグループになります。 <value 1-4> ミラーグループ ID 値を入力します。この値は 1 ～ 4 の必要があります。 add （オプション）送信元ポートを追加します。 delete（オプション）送信元ポートを削除します。
ports	（オプション）RSPAN 送信元に追加または削除する送信元ポートリストを指定します。 <portlist> 設定するポートの範囲を指定します。 rx （オプション）受信パケットのみを監視します。 tx （オプション）着信パケットのみを監視します。 both （オプション）受信パケットと着信パケットの両方を監視します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

RSPAN 送信元エントリを設定するには：

```
Zxxx0:admin#config rspan vlan vlan_name vlan2 source add ports 2-5 rx
Command: config rspan vlan vlan_name vlan2 source add ports 2-5 rx

Success.

Zxxx0:admin#
```

フロー毎の RSPAN の RSPAN 送信元エントリを設定するには：

```
Zxxx0:admin#config rspan vlan vlan_id 2 source
Command: config rspan vlan vlan_id 2 source

Success.

Zxxx0:admin#
```

VLAN 2 の RSPAN リダイレクトをポート 18 および 19 に設定するには：

```
Zxxx0:admin#config rspan vlan vlan_name vlan2 redirect add ports 18-19
Command: config rspan vlan vlan_name vlan2 redirect add ports 18-19

Success.

Zxxx0:admin#
```

55.6. show rspan

● 概要

このコマンドを用いて、RSPAN 設定を表示します。

● 構文

show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

● パラメータ

vlan_name	VLAN 名により RSPAN VLAN を指定します。 <vlan_name> VLAN の名前を指定します。
vlan_id	VLAN ID により RSPAN VLAN を指定します。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。

● 制限

なし

● 実行例

特定の RSPAN 設定を表示するには：

```
Zxxx0:admin# show rspan vlan_id 63
Command: show rspan vlan_id 63
RSPAN  : Enabled

RSPAN VLAN ID : 63
-------------------
Mirror Group ID  : 1
Target Port       : 1:1
Source Ports
RX          : 1:2-1:5
TX          : 1:2-1:5
Redirect Ports   : 1:9-1:12

Total RSPAN VLAN : 1
Zxxx0:admin#
```

すべての RSPAN 設定を表示するには：

```
Zxxx0:admin# show rspan
Command: show rspan

RSPAN: Enabled

RSPAN VLAN ID: 1
--------------------
Mirror Group ID  : 1
Target Port       : 1:1
Source Ports
                    RX:
                    TX:

RSPAN VLAN ID: 2
--------------------
Redirect Ports        : 1:6-1:10

RSPAN VLAN ID: 3
----------------------
Redirect Ports        : 1:6-1:10

Total RSPAN VLAN :3
Zxxx0:admin#
```

56. SNMPv1/v2c/v3 コマンド

SNMP（Simple Network Management Protocol）とは、ネットワークに接続された機器をネットワーク経由で監視・制御するためのプロトコルです。対象機器は MIB（Management information base）と呼ばれる管理情報データベースを持ち、外部の管理マネージャで機器の MIB にアクセスして監視・制御を行います。
ここでは、管理マネージャと管理対象（エージェント）からなる SNMP グループ（SNMP コミュニティ）の管理に関わる設定を行います。
なお、SNMP には v1/v2c/v3 という異なるバージョンがあり、本製品ではすべてのバージョンに対応しています。

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> |[sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user <user_name 32>
show snmp user
show snmp groups
create snmp view <view_name 32> <oid> view_type [included | excluded]
delete snmp view <view_name 32> [all | <oid>]
show snmp view {<view_name 32>}
create snmp community <community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community <community_string 32>
show snmp community {<community_string 32>}
create snmp community_masking view <view_name 32> [read_only | read_write]
config snmp engineID <snmp_engineID 10-64>
show snmp engineID
create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}(1)
delete snmp group <groupname 32>
create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>
delete snmp [host <ipaddr> | v6host <ipv6addr>]
show snmp v6host {<ipv6addr>}
show snmp host {<ipaddr>}
enable community_encryption
disable community_encryption
show community_encryption

56.1. create snmp user

● 概要

このコマンドを用いて、このコマンドの対象となる SNMP グループに新規ユーザを作成します。認証とプライバシについては、ユーザがパスワードかキーのいずれを使用するかを選択できます。

● 構文

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> |[sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

● パラメータ

<user_name 32>	エージェントに接続するホストのユーザ名を指定します。1 ～ 32 文字の範囲で指定します。
<groupname 32>	ユーザを関連付けるグループ名を指定します。1 ～ 32 文字の範囲で指定します。
encrypted	（オプション）パスワードを暗号化された形式で表示するかどうか指定します。
by_password auth	認証のための入力パスワードを指定します。
MD5	HMAC-MD5-96 の認証レベルを指定します。8 ～ 16 文字の範囲で指定します。 <auth_password 8-16> HMAC-MAC-96 の認証レベルを 8 ～ 16 文字の範囲で指定します。
sha	HMAC-SHA-96 の認証レベルを指定します。8 ～ 20 文字の範囲で指定します。 <auth_password 8-20> HMAC-SHA-96 の認証レベルを 8 ～ 20 文字の範囲で指定します。
priv	プライバシのための入力パスワードを指定します。オプションは none と DES です。 none プライバシ文字列はありません。 des DES で使用するプライバシ文字列を 8 ～ 16 文字で指定します。 <priv_password 8-16> DES で使用するプライバシ文字列を 8 ～ 16 文字で指定します。
by_key auth	認証のための入力キーを指定します。
sha	SHA1 で使用する認証キーを指定します。これは 40 文字の 16 進数文字列タイプです。 <auth_key 40-40> SHA1 で使用する認証キーを指定します。これは 40 文字の 16 進数文字列タイプです。
priv	プライバシのための入力キーを指定します。オプションは none と DES です。 none プライバシキーはありません。 des DES で使用するプライバシキーを指定します。これは 32 文字の 16 進数文字列タイプです。 <priv_key 32-32> DES で使用するプライバシキーを指定します。これは 32 文字の 16 進数文字列タイプです。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

このコマンドの対象となる SNMP グループに新規ユーザを作成するには：

```
Zxxx0:admin#create snmp user manager MANAGER_group encrypted by_password auth sha
12345678 priv des 12345678
Command: create snmp user manager MANAGER_group encrypted by_password auth sha
12345678 priv des 12345678


Success.


Zxxx0:admin#
```

56.2. delete snmp user

● 概要

このコマンドを用いて、SNMP グループからユーザを削除し、SNMP グループ内の関連付けられたグループを削除します。

● 構文

delete snmp user <user_name 32>

● パラメータ

<user_name 32>
削除するホストのユーザ名を指定します。1 ～ 32 文字の範囲で指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

SNMP ユーザを削除するには：

```
Zxxx0:admin#delete snmp user manager
Command: delete snmp user manager


Success.


Zxxx0:admin#
```

56.3. show snmp user

● 概要

このコマンドを用いて、グループユーザ名テーブルの各 SNMP ユーザ名の情報を表示します。

● 構文

show snmp user

● パラメータ

なし

● 制限

なし

● 実行例

SNMP ユーザ情報を表示するには：

```
Zxxx0:admin#show snmp user
Command: show snmp user

Username                        Group Name                      VerAuthPriv
------------------------------  ------------------------------  ------------
initial                         initial                         V3 NoneNone

Total Entries : 1

Zxxx0:admin#
```

56.4. show snmp groups

● 概要

このコマンドを用いて、スイッチの SNMP グループの名前を表示し、さらにセキュリティモデル、レベル、さまざまなビューのステータスを表示します。

● 構文

show snmp groups

● パラメータ

なし

● 制限

なし

● 実行例

スイッチの SNMP グループの名前を表示するには：

```
Zxxx0:admin#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group    Name     : public
ReadView Name     : CommunityView
WriteView Name    :
Notify View Name  : CommunityView
Security Model    : SNMPv1
Security Level    : NoAuthNoPriv

Group    Name     : public
ReadView Name     : CommunityView
WriteView Name    :
Notify View Name  : CommunityView
Security Model    : SNMPv2
Security Level    : NoAuthNoPriv

Group    Name     : private
ReadView Name     : CommunityView
WriteView Name    : CommunityView
Notify View Name  : CommunityView
Security Model    : SNMPv2
Security Level    : NoAuthNoPriv

Total Entries: 3

Zxxx0:admin#
```

56.5. create snmp view

● 概要

このコマンドを用いて、コミュニティ名にビューを割り当て、SNMP マネージャがアクセスできる MIB オブジェクトを制限します。

● 構文

create snmp view <view_name 32> <oid> view_type [included | excluded]

● パラメータ

<view_name 32>	作成するビューの名前を指定します。
<oid>	オブジェクト識別ツリー（MIB ツリー）を指定します。
view_type	このビューの MIB ツリーのアクセスタイプを指定します。
included	このビューを含めます。
excluded	このビューを除外します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

コミュニティ名にビューを割り当て、SNMP マネージャがアクセスできる MIB オブジェクトを制限するには：

```
Zxxx0:admin#create snmp view managerview 1.3.6 view_type included
Command: create snmp view managerview 1.3.6 view_type included

Success.

Zxxx0:admin#
```

56.6. delete snmp view

● 概要

このコマンドを用いて、ビューレコードを削除します。

● 構文

delete snmp view <view_name 32> [all | <oid>]

● パラメータ

<view_name 32>	削除するユーザのビュー名を指定します。
all	すべてのレコードを表示します。
<oid>	オブジェクト識別ツリー（MIB ツリー）を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

ビューレコードを削除するには：

```
Zxxx0:admin#delete snmp view managerview all
Command: delete snmp view managerview all

Success.

Zxxx0:admin#
```

56.7. show snmp view

● 概要

このコマンドを用いて、SNMP ビューレコードを表示します。

● 構文

show snmp view {<view_name 32>}

● パラメータ

<view_name 32> （オプション）表示するユーザのビュー名を指定します。

● 制限

なし

● 実行例

SNMP ビューレコードを表示するには：

```
Zxxx0:admin#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name              Subtree                    View Type
---------------------  -------------------------  ----------
restricted             1.3.6.1.2.1.1              Included
restricted             1.3.6.1.2.1.11             Included
restricted             1.3.6.1.6.3.10.2.1         Included
restricted             1.3.6.1.6.3.11.2.1         Included
restricted             1.3.6.1.6.3.15.1.1         Included
CommunityView          1                          Included
CommunityView          1.3.6.1.6.3                Excluded
CommunityView          1.3.6.1.6.3.1              Included

Total Entries: 8

Zxxx0:admin#
```

56.8. create snmp community

● 概要

このコマンドを用いて、SNMP コミュニティ名を作成します。SNMP コミュニティ名を用いて、SNMP マネージャとエージェントの関係を定義します。コミュニティ名はパスワードのように機能して、スイッチのエージェントへのアクセスを認証します。名には、1 つまたは複数の機能を関連付けることができ、MIB ビューを指定すると、所定のコミュニティにアクセス可能なすべての MIB オブジェクトのサブセットを定義できます。また、コミュニティにアクセス可能な MIB オブジェクトの読み書き権限や読み取り専用権限を指定できます。

● 構文

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

● パラメータ

<community_string 32>	コミュニティ名を指定します。最大文字数は 32 文字です。
view	MIB のビュー名を指定します。最大文字数は 32 文字です。 <view_name 32> MIB のビュー名を指定します。最大文字数は 32 文字です。
read_only	読み取り専用権限を指定します。
read_write	読み書き権限を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

SNMP コミュニティ名を作成するには：

```
Zxxx0:admin#create snmp community manager view CommunityView read_write
Command: create snmp community manager view CommunityView read_write

Success.

Zxxx0:admin#
```

56.9. delete snmp community

● 概要

このコマンドを用いて、特定のコミュニティ名を削除します。

● 構文

delete snmp community <community_string 32>

● パラメータ

<community_string 32>
削除するコミュニティ名を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

SNMP コミュニティを削除するには：

```
Zxxx0:admin#delete snmp community manager
Command: delete snmp community manager

Success.

Zxxx0:admin#
```

56.10. show snmp community

● 概要

このコマンドを用いて、コミュニティ名の設定を表示します。

● 構文

show snmp community {<community_string 32>}

● パラメータ

<community_string 32>
（オプション）表示するコミュニティ名を指定します。

NOTE コミュニティ名を指定しない場合、すべてのコミュニティ名の情報が表示されます。

● 制限

なし

● 実行例

現在のコミュニティ名の設定を表示するには：

```
Zxxx0:admin#show snmp community
Command: show snmp community

SNMP Community Table
Community Name                 View Name                 Access Right
-----------------------------  ------------------------  ------------
private                        CommunityView             read_write
public                         CommunityView             read_only

Total Entries : 2

Zxxx0:admin#
```

56.11. create snmp community_masking view

● 概要

このコマンドを用いて、SNMP コミュニティ名を作成する際のセキュリティ手段を選択します。ただし、コミュニティ名が暗号化されるかどうかは、SNMP コミュニティの暗号化の状態に依存します。ユーザがこのコマンドを用いて SNMP コミュニティ名を作成すると、ユーザが入力するコミュニティ名が「*」で表示されます。また、SNMP コミュニティを作成するときに、SNMP コミュニティ名を（確認のために）2 回入力する必要があります。

● 構文

create snmp community_masking view <view_name 32> [read_only | read_write]

● パラメータ

<view_name 32>	使用する MIB ビューの名前を入力します。名前は 32 文字までです。
read_only	コミュニティ名を用いるユーザが、スイッチの SNMP エージェントに対する読み取り専用のアクセス権を持ちます。
read_write	コミュニティ名を用いるユーザが、スイッチの SNMP エージェントに対する読み書きのアクセス権を持ちます。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

セキュリティ手段が「read_only」の「community123」というSNMPコミュニティ名を作成するには:

```
Zxxx0:admin# create snmp community_masking view CommunityView read_only
Command: create snmp community_masking view CommunityView read_only

Enter a case-sensitive community:************
Enter the community again for confirmation:************

Success.

Zxxx0:admin#
```

56.12. config snmp engineID

● 概要

このコマンドを用いて、スイッチの SNMP エンジンの ID を設定します。各 SNMP エンティティに一意のエンジン ID が関連付けられます。

● 構文

config snmp engineID <snmp_engineID 10-64>

● パラメータ

<snmp_engineID 10-64> スイッチの SNMP エンジンの ID を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

スイッチの SNMP エンジンの ID を設定するには：

```
Zxxx0:admin#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

Zxxx0:admin#
```

56.13. show snmp engineID

● 概要

このコマンドを用いて、スイッチの SNMP エンジンの ID を表示します。

● 構文

show snmp engineID

● パラメータ

なし

● 制限

なし

● 実行例

SNMP エンジンの ID を表示するには：

```
Zxxx0:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

Zxxx0:admin#
```

56.14. create snmp group

● 概要

このコマンドを用いて、新しい SNMP グループを作成します。

● 構文

create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}(1)

● パラメータ

<groupname 32>	グループの名前を指定します。
v1	利用可能なセキュリティモデルの中で最も安全性が低いものを指定します。
v2c	利用可能なセキュリティモデルの中で 2 番目に安全性が低いものを指定します。

v3	利用可能なセキュリティモデルの中で最も安全性が高いものを指定します。パケットの認証を指定します。
noauth_nopriv パケット認証も暗号化もサポートしません。	
auth_nopriv パケット認証をサポートします。	
auth_priv パケット認証と暗号化をサポートします。	
read_view ビューの名前を 1 ～ 32 文字で指定します。 <view_name 32> ビューの名前を 1 ～ 32 文字で指定します。	
write_view ビューの名前を 1 ～ 32 文字で指定します。 <view_name 32> ビューの名前を 1 ～ 32 文字で指定します。	
notify_view ビューの名前を 1 ～ 32 文字で指定します。 <view_name 32> ビューの名前を 1 ～ 32 文字で指定します。	

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

新しい SNMP グループを作成するには：

```
Zxxx0:admin#create snmp group MANAGER_group v3 auth_priv read_view
CommunityViewwrite_view CommunityView notify_view CommunityView
Command: create snmp group MANAGER_group v3 auth_priv read_view CommunityView
write_view CommunityView notify_view CommunityView

Success.

Zxxx0:admin#
```

56.15. delete snmp group

● 概要

このコマンドを用いて、SNMP グループを削除します。

● 構文

delete snmp group <groupname 32>

● パラメータ

<groupname 32> 削除するグループの名前を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

SNMP グループを削除するには：

```
Zxxx0:admin#delete snmp group MANAGER_group
Command: delete snmp group MANAGER_group

Success.

Zxxx0:admin#
```

56.16. create snmp

● 概要

このコマンドを用いて、SNMP 動作の受信側を作成します。

● 構文

create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>

● パラメータ

host	トラップの宛先である受信側の IP アドレスを指定します。 <ipaddr> トラップの宛先である受信側の IP アドレスを指定します。
v6host	トラップパケットの宛先の v6host の IP アドレスを指定します。 <ipv6addr> トラップパケットの宛先の v6host の IP アドレスを指定します。
v1	利用可能なセキュリティモデルの中で最も安全性が低いものを指定します。
v2c	利用可能なセキュリティモデルの中で 2 番目に安全性が低いものを指定します。
v3	利用可能なセキュリティモデルの中で最も安全性が高いものを指定します。
noauth_nopriv パケット認証も暗号化もサポートしません。	
auth_nopriv パケット認証をサポートします。	
auth_priv パケット認証と暗号化をサポートします。	

<auth_string 32>	認証文字列を指定します。v1 または v2 を指定した場合、auth_string はコミュニティ名を表します。これは、コミュニティテーブルのエントリの中のいずれかである必要があります。v3 を指定した場合、auth_string はユーザ名を表します。これは、ユーザテーブルのエントリの中のいずれかである必要があります。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

SNMP 動作の受信側を作成するには：

```
Zxxx0:admin#create snmp host 10.48.74.100 v3 noauth_nopriv initial
Command: create snmp host 10.48.74.100 v3 noauth_nopriv initial

Success.

Zxxx0:admin#
```

56.17. delete snmp

● 概要

このコマンドを用いて、SNMP トラップ動作の受信側を削除します。

● 構文

delete snmp [host <ipaddr> | v6host <ipv6addr>]

● パラメータ

host	削除する受信側 SNMP ホストの IP アドレスを指定します。 <ipaddr> 削除する受信側 SNMP ホストの IP アドレスを指定します。
v6host	削除する受信側 SNMP ホストの IPv6 アドレスを指定します。 <ipv6addr> 削除する受信側 SNMP ホストの IPv6 アドレスを指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

SNMP トラップ動作の受信側を削除するには：

```
Zxxx0:admin#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

Zxxx0:admin#
```

56.18. show snmp host

● 概要

このコマンドを用いて、トラップの宛先である受信側を表示します。

● 構文

show snmp host {<ipaddr>}

● パラメータ

<ipaddr>（オプション）トラップの宛先である受信側の IP アドレスを指定します。

NOTE パラメータを指定しない場合、すべての SNMP ホストが表示されます。

● 制限

なし

● 実行例

トラップの宛先である受信側を表示するには：

```
Zxxx0:admin# show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3 User Name
---------------  ---------------  ---------------------------------
10.48.76.100     V3 noauthnopriv  initial
10.51.17.1       V2c              public

Total Entries : 2

Zxxx0:admin#
```

56.19. show snmp v6host

● 概要

このコマンドを用いて、トラップの宛先である受信側を表示します。

● 構文

show snmp v6host {<ipv6addr>}

● パラメータ

<ipv6addr>
（オプション）v6host の IP アドレスを指定します。

NOTE パラメータを指定しない場合、すべての SNMP IPv6 ホストが表示されます。

● 制限

なし

● 実行例

トラップの宛先である受信側を表示するには：

```
Zxxx0:admin# show snmp v6host
Command: show snmp v6host

SNMP Host Table
-------------------------------------------------------------------
Host IPv6 Address: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
SNMP Version     : V3 na/np
Community Name/SNMPv3 User Name: 12345678910234567890

Host IPv6 Address: FECO:1A49:2AA:FF:FE34:CA8F
SNMP Version     : V3 a/np
Community Name/SNMPv3 User Name: abcdefghijk

Total Entries : 2

Zxxx0:admin#
```

56.20. enable community_encryption

● 概要

このコマンドを用いて、SNMP コミュニティ名の暗号化を有効にします。

● 構文

enable community_encryption

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

SNMP コミュニティ名の暗号化を有効にするには：

```
Zxxx0:admin# enable community_encryption
Command: enable community_encryption

Success.

Zxxx0:admin#
```

暗号化の状態を有効にした後で、SNMP コミュニティ名を作成すると、以下のように、コミュニティ名が暗号化された文字列（6つの「*」）で表示され、それ以外の場合はプレーンテキストで表示されます。

```
Zxxx0:admin# show snmp community
Command: show snmp community

SNMP Community Table
Community Name          View Name               Access Right
----------------------  ----------------------  ------------
******                  CommunityView           read_write
******                  CommunityView           read_only
private                 CommunityView           read_write
public                  CommunityView           read_only

Total Entries : 4

Zxxx0:admin#
```

56.21. disable community_encryption

● 概要

このコマンドを用いて、SNMP コミュニティ名の暗号化を無効にします。

● 構文

disable community_encryption

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

SNMP コミュニティ名の暗号化を無効にするには：

```
Zxxx0:admin# disable community_encryption
Command: disable community_encryption

Success.

Zxxx0:admin#
```

56.22. show community_encryption

● 概要

このコマンドを用いて、SNMP コミュニティ名の暗号化を表示します。

● 構文

show community_encryption

● パラメータ

なし

● 制限

なし

● 実行例

SNMP コミュニティ名の暗号化を表示するには：

```
Zxxx0:admin# show community_encryption
Command: show community_encryption

SNMP Community Encryption State : Enabled

Zxxx0:admin#
```

57.STP(Spanning Tree Protocol) コマンド

● STP

STP（Spanning Tree Protocol）とは、複数のブリッジを接続して構築されたネットワークにおいて、ループを防止しながら経路の冗長化を持たせるしくみです。通信経路の片方がダウンしても、経路を迂回することで、通信を継続させることができます。
通常、ケーブルをループ状に接続すると、フレームが永遠に回り続けてしまうブロードキャストストームと呼ばれる現象が発生し、ネットワークがダウンしてしまいます。
STP 機能は、各スイッチ間で BPDU フレームと呼ばれる制御フレームを相互交換し、最短経路の計算を行います。そしてフレームがループしないネットワークとなるようにポートを自動的にブロックすることで、論理的にループしないネットワークを構築することができます。
経路に障害が発生した場合は、最大 50 秒以内に通信経路の復旧が可能となります。

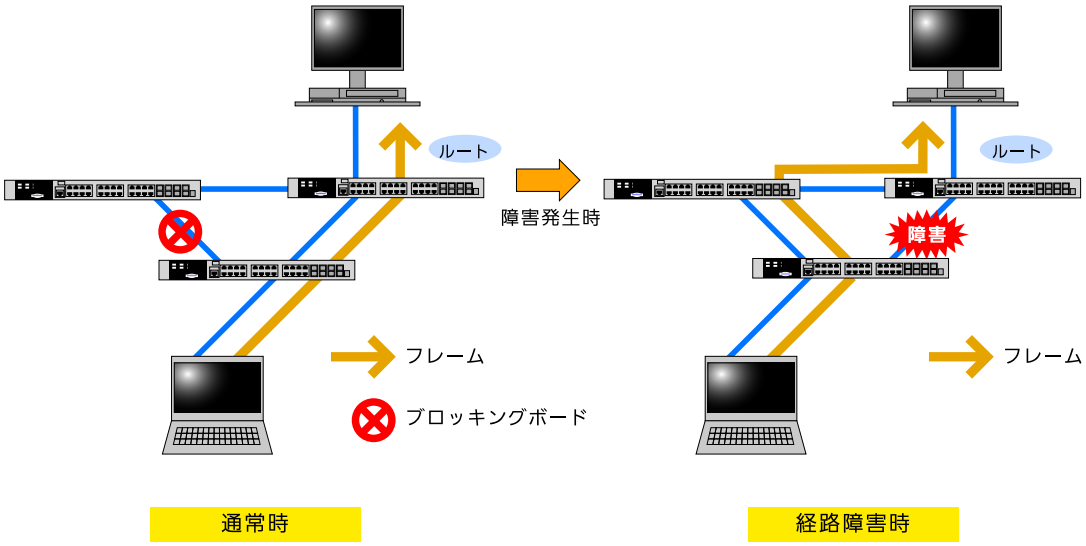


図 57-1　STP の概略

● RSTP

RSTP（Rapid Spanning Tree Protocol）とは STP を改良したプロトコルで、経路障害時の復旧時間を数秒に短縮することができます。
RSTP 機能では、経路変更時に、STP で使われる各種タイマーは使わず、スイッチ同士の情報交換（プロポーザル／アグリーメント）によって、ポートの役割を決め、経路をすぐに変更することができます。

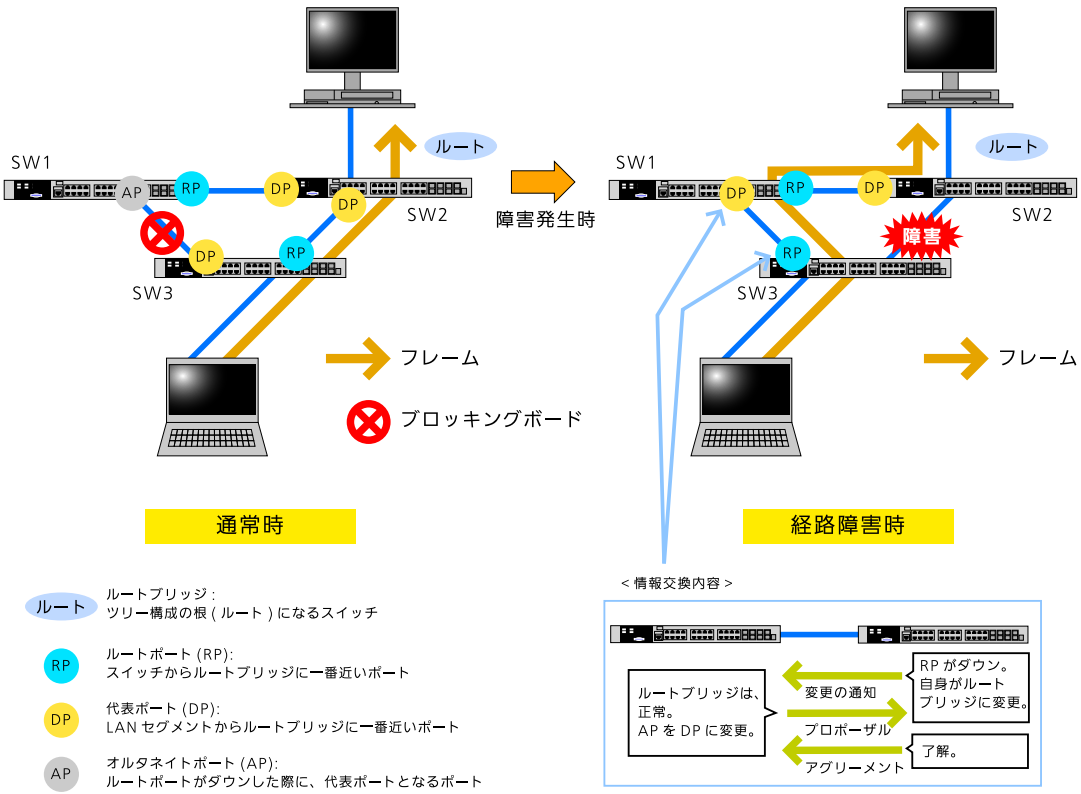


図 57-2　RSTP の概略

● MSTP

MSTP（Multiple Spanning Tree Protocol）も STP を改良したプロトコルで、VLAN 毎のデータを異なる経路で通信させることができます。これにより、帯域の有効活用が可能となります。
複数の VLAN をインスタンスと呼ばれるグループに集約することで、VLAN 毎にスパニングツリーインスタンスを設計する場合と比較し、CPU 負荷が軽減できます。
MSTP 機能を使用することで、大規模なネットワークにおいてもサポートすることが可能となります。

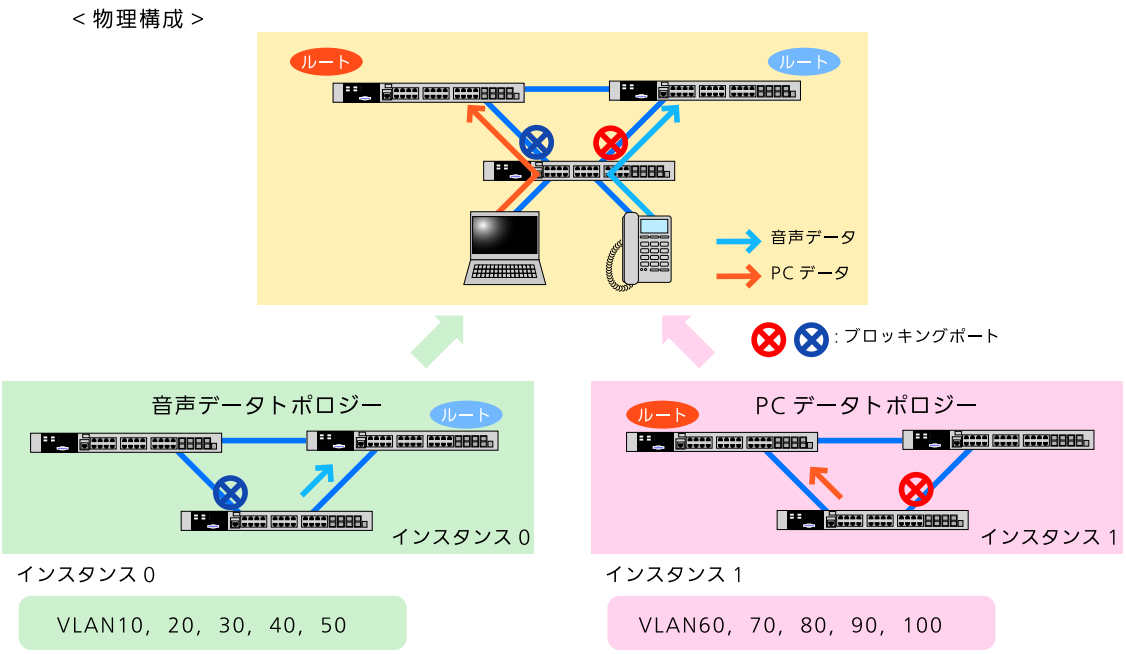


図 57-3　MSTP の概略

show stp **show stp instance** {<value 0-64>} **show stp ports** {<portlist>} show stp mst_config_id **create stp instance_id** <value 1-64> **delete stp instance_id** <value 1-64> **config stp instance_id** <value 1-64> [add_vlan | remove_vlan] <vidlist> **config stp mst_config_id** {revision_level <int 0-65535> | name <string>} (1) **enable stp** **disable stp** **config stp version** [mstp | rstp | stp] **config stp priority** <value 0-61440> instance_id <value 0-64> **config stp** {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] }(1) **config stp ports** <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable] | restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]} (1) **config stp mst_ports** <portlist> instance_id <value 0-64> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}(1)

57.1. show stp

● 概要

このコマンドを用いて、ブリッジパラメータのグローバル設定を表示します。

● 構文

show stp

● パラメータ

なし

● 制限

なし

● 実行例

STP を表示するには：

```
Zxxx0:admin#show stp
Command: show stp

STP Bridge Global Settings
------------------------------
STP Status          : Enabled
STP Version         : MSTP
Max Age             : 20
Forward Delay       : 15
Max Hops            : 20
TX Hold Count       : 6
Forwarding BPDU     : Enabled
NNI BPDU Address    : dot1d

Zxxx0:admin#
```

57.2. show stp instance

● 概要

このコマンドを用いて、各インスタンスのパラメータ設定を表示します。値はインスタンス ID です。この値を入力しない場合、すべてのインスタンスが表示されます。

● 構文

show stp instance {<value 0-64>}

● パラメータ

<value 0-64>	（オプション）MSTP インスタンス ID を指定します。インスタンス 0 はデフォルトインスタンス CIST を表します。この値は 0 ～ 64 の必要があります。

● 制限

なし

● 実行例

STP インスタンスを表示するには：

```
Zxxx0:admin#show stp instance
Command: show stp instance

STP Instance Settings
--------------------------
Instance Type           : CIST
Instance Status         : Enabled
Instance Priority       : 32768(Bridge Priority : 32768, SYS ID Ext : 0 )

STP Instance Operational Status
--------------------------------
Designated Root Bridge : 32768/00-22-22-22-22-00
External Root Cost     : 0
Regional Root Bridge   : 32768/00-22-22-22-22-00
Internal Root Cost     : 0
Designated Bridge      : 32768/00-22-22-22-22-00
Root Port              : None
Max Age                : 20
Forward Delay          : 15
Last Topology Change   : 2430
Topology Changes Count : 0

Zxxx0:admin#
```

57.3. show stp ports

● 概要

このコマンドを用いて、スイッチの現在のポート毎の STP 設定を表示します。
STP ポートの設定、STP ポートの役割（Disabled、Alternate、Backup、Root、Designated、NonStp）、および STP ポートのステータス（Disabled、Discarding、Learning、Forwarding）を表示できます。

● 構文

show stp ports {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

● 制限

なし

● 実行例

STP ポートを表示するには：

```
Zxxx0:admin#show stp ports
Command: show stp ports

MSTP Port Information
Port Index        : 1     ,  Hello Time       : 2 /2 ,  Port STP : enabled
External PathCost : Auto/200000   ,  Edge Port : No /No ,  P2P    : False/No
Port RestrictedRole : False,  Port RestrictedTCN : False
Port Forward BPDU : Enabled

MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
-----  ------------------  -----------------  ----  ----------  ----------
0      N/A                 200000             128   Disabled    Disabled
2      N/A                 200000             128   Disabled    Disabled

Zxxx0:admin#
```

57.4. show stp mst_config_id

● 概要

このコマンドを用いて、MST 設定 ID の 3 つの要素（設定名、リビジョンレベル、MST 設定テーブル）を表示します。デフォルトの設定名はブリッジの MAC アドレスです。mst_config_id の 3 つの要素が、2 つのブリッジで同一の場合は、この 2 つが同じ MST リージョンにあることを意味します。

● 構文

show stp mst_config_id

● パラメータ

なし

● 制限

なし

● 実行例

STP MST 設定 ID を表示するには：

```
Zxxx0:admin#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
---------------------------------------

Configuration Name : 00-22-22-22-22-00                        Revision Level :0
MSTI ID     Vid list
-------     -----------
   CIST     1-4094

Zxxx0:admin#
```

57.5. create stp instance_id

● 概要

このコマンドを用いて、デフォルトインスタンスの CIST（インスタンス 0）から独立した新しい MST インスタンスを作成します。MST インスタンスを作成した後で、（67.7 のコマンドを使用して）ユーザが VLAN を設定する必要があります。設定しない場合、新しく作成した MST インスタンスは無効なままです。

● 構文

create stp instance_id <value 1-64>

● パラメータ

<value 1-64>
MSTP インスタンス ID を指定します。インスタンス 0 はデフォルトインスタンス CIST を表します。この値は 1 ～ 64 の必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MSTP インスタンスを作成するには：

```
Zxxx0:admin#create stp instance_id 2
Command: create stp instance_id 2

Warning:There is no VLAN mapping to this instance_id!
Success.

Zxxx0:admin#
```

57.6. delete stp instance_id

● 概要

このコマンドを用いて、指定した MST インスタンスを削除します。CIST（インスタンス 0）は削除できません。また、一度に 1 つのインスタンスのみを削除できます。

● 構文

delete stp instance_id <value 1-64>

● パラメータ

<value 1-64> MSTP インスタンス ID を指定します。インスタンス 0 はデフォルトインスタンス CIST を表します。この値は 1 ～ 64 の必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MSTP インスタンスを削除するには：

```
Zxxx0:admin#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

Zxxx0:admin#
```

57.7. config stp instance_id

● 概要

MST インスタンスの処理には以下 2 つのタイプがあります。

1）add_vlan：指定した VLAN リストを既存の MST インスタンスにマッピングします。

2）remove_vlan：指定した VLAN リストを既存の MST インスタンスから削除します。

● 構文

config stp instance_id <value 1-64> [add_vlan | remove_vlan] <vidlist>

● パラメータ

<value 1-64>	MSTP インスタンス ID を指定します。インスタンス 0 はデフォルトインスタンス CIST を表します。スイッチは最大 65 のインスタンス（0 ～ 64）をサポートします。
add_vlan	MST インスタンスに VLAN を追加する場合に指定します。
remove_vlan	MST インスタンスから VLAN を削除する場合に指定します。
<vidlist>	VLAN ID を指定します。値の範囲は 1 ～ 4094 です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

VLAN ID を MSTP インスタンスにマッピングするには：

```
Zxxx0:admin#config stp instance_id 2 add_vlan 1
Command: config stp instance_id 2 add_vlan 1

Success.

Zxxx0:admin#
```

VLAN ID を MSTP インスタンスから削除するには：

```
Zxxx0:admin#config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

Zxxx0:admin#
```

57.8. config stp mst_config_id

● 概要

このコマンドを用いて、MST 設定 ID の設定名またはリビジョンレベルを設定します。デフォルトの設定名はスイッチの MAC アドレスです。

● 構文

config stp mst_config_id {revision_level <int 0-65535> | name <string>} (1)

● パラメータ

revision_level	リビジョンレベルを指定します。 <int 0-65535> リビジョンレベルを指定します。
name	MST リージョンの名前を指定します。 <string> MST リージョンの名前を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

MST 設定 ID の名前とリビジョンレベルを変更するには：

```
Zxxx0:admin#config stp mst_config_id revision_level 1 name R&D_BlockG
Commands: config stp mst_config_id revision_level 1 name R&D_BlockG

Success.

Zxxx0:admin#
```

57.9. enable stp

● 概要

ユーザがインスタンス毎に STP を有効にできるように変更することができますが、他のインスタンスを有効にする前に、まず CIST を有効にする必要があります。VERSION が MSTP に設定され、このインスタンスに少なくとも 1 つの VLAN がマッピングされている場合、ユーザが CIST を有効にすると、すべての MSTI が自動的に有効になります。

● 構文

enable stp

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

STP を有効にするには：

```
Zxxx0:admin#enable stp
Command: enable stp

Success.

Zxxx0:admin#
```

57.10. disable stp

● 概要

このコマンドを用いて、既存のすべてのインスタンスの STP 機能を無効にします。

● 構文

disable stp

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

STP を無効にするには：

```
Zxxx0:admin#disable stp
Command: disable stp

Success.

Zxxx0:admin#
```

57.11. config stp version

● 概要

このコマンドを用いて、STP をグローバルに有効にします。バージョンが STP または RSTP に設定されている場合は、現在実行中のすべての MSTI を無効にする必要があります。バージョンが MSTP として設定されている場合は、利用可能なすべての MSTI に対して有効になります（CIST が有効な場合）。

● 構文

config stp version [mstp | rstp | stp]

● パラメータ

mstp	MSTP（Multiple Spanning Tree Protocol）を使用します。
rstp	RSTP（Rapid Spanning Tree Protocol）を使用します。これがデフォルトです。
stp	STP（Spanning Tree Protocol）を使用します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

STP バージョンを設定するには：

```
Zxxx0:admin#config stp version mstp
Command: config stp version mstp

Success.

Zxxx0:admin#
```

57.12. config stp priority

● 概要

ルートブリッジを選択するために用いるパラメータの 1 つです。

● 構文

config stp priority <value 0-61440> instance_id <value 0-64>

● パラメータ

<value 0-61440>	ブリッジのプライオリティ値を指定します。値は　4096　の倍数である必要があります。初期値は 32768 です。
instance_id	STP インスタンスを区別するために、ID 値を指定します。 <value 0-64> STP インスタンスを区別するために、ID 値を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

STP インスタンス ID を設定するには：

```
Zxxx0:admin#config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

Zxxx0:admin#
```

57.13. config stp

● 概要

このコマンドを用いて、ブリッジパラメータのグローバル設定を指定します。

● 構文

config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] } (1)

● パラメータ

maxage	BPDU の最大エイジ時間を設定します。 <value 6-40> BPDU の最大エイジ時間を設定します。初期値は 20 です。
maxhops	BPDU の最大ホップ数を設定します。 <value 6-40> BPDU の最大ホップ数を設定します。初期値は 20 です。
hellotime	ルートブリッジが設定 BPDU を送信する時間間隔を指定します。このパラメータは STP および RSTP バージョンに使用します。MSTP バージョンではポート毎の hellotime パラメータを使用します。 <value 1-2> ルートブリッジが BPDU を送信する時間間隔を指定します。このパラメータは STP および RSTP バージョンに使用します。MSTP バージョンではポート毎の hellotime パラメータを使用します。初期値は 2 秒です。
forwarddelay	ブリッジの転送遅延時間を設定します。 <value 4-30> ブリッジの転送遅延時間を設定します。初期値は 15 です。
txholdcount	特定の時間間隔（Hello 時間毎）に送信される BPDU の数を制限します。 <value 1-10> 特定の時間間隔（Hello 時間毎）に送信される BPDU の数を制限します。
fbpdu	STP 機能が無効なときに、ブリッジが STP BPDU をフラッディングするかどうかを決定します。 enable FBPDU を有効にします。 disable FBPDU を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

STP を設定するには：

```
Zxxx0:admin# config stp maxage 25
Command: config stp maxage 25

Success.

Zxxx0:admin#
```

57.14. config stp ports

● 概要

このコマンドを用いて、内部パスコストとポートプライオリティを除くポートのすべてのパラメータを設定します。

● 構文

config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable] | restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]} (1)

● パラメータ

<portlist>	ポートの範囲を指定します。
externalCost	送信ブリッジから CIST ルートブリッジまでの MST リージョン間のパスコストを指定します。これは CIST レベルでのみ使用されます。 auto　パスコストを自動的に選択します。 <value 1-200000000> 1 ～ 200000000 の値を指定します。
hellotime	RSTP ではブリッジ毎のパラメータですが、MSTP ではポート毎のパラメータになります。 <value 1-2> RSTP ではブリッジ毎のパラメータですが、MSTP ではポート毎のパラメータになります。初期値は 2 です。
migrate	一定の遅延時間後にポートが MSTP BPDU を送信するように指定する管理動作です。 yes　一定の遅延時間後にポートが MSTP BPDU を送信します。 no　一定の遅延時間後にポートが MSTP BPDU を送信しません。
edge	ポートが LAN に接続されるか、Bridged LAN に接続されるかを決定します。auto モードの場合、BPDU を受信しないときは、ブリッジがエッジポートになるまでに遅延があります。 true　エッジ接続の場合に指定します。 false　エッジ接続でない場合に指定します。 auto　スイッチが自動的ポートモードを設定します。BPDU を受信しないときは、ブリッジがエッジポートになるまでに遅延があります。
p2p	ポートが全二重または半二重モードかを決定します。 true　全二重モードを指定します。 false　半二重モードを指定します。 auto　スイッチが自動的に P2P モードを決定します。
state	ポートが STP 機能をサポートするかを決定します。 enable STP 機能のサポートを有効にします。 disable STP 機能のサポートを無効にします。
restricted_role	ポートをルートポートとして選択するかどうかを決定します。初期値は false です。 true　ポートがルートポートとして選択されません。 false　ポートがルートポートとして選択されます。
restricted_tcn	ポートがトポロジ変更を伝搬するかどうかを決定します。初期値は false です。 true　トポロジ変更を伝搬しません。 false　トポロジ変更を伝搬します。
fbpdu	STP 機能が無効なときに、ポートが STP BPDU をフラッディングするかどうかを決定します。 enable STP 機能が無効なときに、ポートが STP BPDU をフラッディングします。 disable STP 機能が無効なときに、ポートが STP BPDU をフラッディングしません。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

STP ポートを設定するには：

```
Zxxx0:admin# config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

Zxxx0:admin#
```

57.15. config stp mst_ports

● 概要

MSTI のポートの内部パスコストとポートプライオリティについては、CIST（インスタンス ID = 0）の設定とは異なる値を個別に設定できます。

● 構文

config stp mst_ports <portlist> instance_id <value 0-64> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}(1)

● パラメータ

<portlist>ポートの範囲を指定します。	
instance_id	インスタンス ID を指定します。 <value 0-64> インスタンス = 0 は CIST を、インスタンス 1 ～ 64 は MSTI1 ～ MSTI 64 を表します。
internalCost	MSTP で用いられるポートのパスコストです。 auto 内部コストを自動的に決定します。 <value 1-200000000> 1 ～ 200000000 の値を指定します。
priority	ポートプライオリティを指定します。 <value 0-240> 0 ～ 240 の値を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

STP MST ポートを設定するには：

```
Zxxx0:admin# config stp mst_ports 1 instance_id 0 internalCost auto
Command: config stp mst_ports 1 instance_id 0 internalCost auto

Success.

Zxxx0:admin#
```

58. SSH コマンド

SSH（Secure Shell）とは、認証機能と通信の暗号化により、なりすましや盗聴を防止します。通常の Telnet 接続に比べてより安全に本製品に遠隔からログインできます。
本製品を SSH サーバとして機能させ、SSH クライアントから接続できるようにします。
ユーザ認証として、以下の方式に対応します。

- パスワード認証（password）
- 公開鍵認証（publickey）
- ホストベース認証（hostbased）

クライアントとサーバ間で送受信されるメッセージの暗号化アルゴリズムとして以下を設定できます。

- 3DES
- blowfish
- AES（128、192、256）
- arcfour
- cast128
- twofish（128、192、256）

---

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 |MD5 | SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm
config ssh authmode [password | publickey | hostbased] [enable | disable]
show ssh authmode
config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]
show ssh user authmode
config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}(1)
enable ssh
disable ssh
show ssh server

58.1. config ssh algorithm

● 概要

このコマンドを用いて、SSH サービスアルゴリズムを設定します。

● 構文

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 |MD5 | SHA1 | RSA | DSA] [enable | disable]

● パラメータ

3DES	3DES 暗号化アルゴリズムを指定します。
blowfish	Blowfish 暗号化アルゴリズムを指定します。
AES(128,192,256)	AES 暗号化アルゴリズムを指定します。
arcfour	Actfour 暗号化アルゴリズムを指定します。
cast128	Cast128 暗号化アルゴリズムを指定します。
twofish (128,192,256)	Twofish 暗号化アルゴリズムを指定します。
MD5	MD5 暗号化アルゴリズムを指定します。
SHA1	SHA1 暗号化アルゴリズムを指定します。
DSA	DSA 暗号化アルゴリズムを指定します。
RSA	RSA 暗号化アルゴリズムを指定します。
enable	アルゴリズムを有効にします。
disable	アルゴリズムを無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

SSH サーバの公開鍵アルゴリズムを有効にするには：

```
Zxxx0:admin#config ssh algorithm DSA enable
Command: config ssh algorithm DSA enable

Success.

Zxxx0:admin#
```

58.2. show ssh algorithm

● 概要

このコマンドを用いて、SSH 認証アルゴリズムを表示します。

● 構文

show ssh algorithm

● パラメータ

なし

● 制限

なし

● 実行例

SSH サーバアルゴリズムを表示するには：

```
Zxxx0:admin#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
--------------------------
3DES        : Enabled
AES128      : Enabled
AES192      : Enabled
AES256      : Enabled
arcfour     : Enabled
blowfish    : Enabled
cast128     : Enabled
twofish128  : Enabled
twofish192  : Enabled
twofish256  : Enabled

Data Integrity Algorithm
--------------------------
SHA1        : Enabled

Public Key Algorithm
--------------------------
RSA         : Enabled
DSA         : Enabled

Zxxx0:admin#
```

58.3. config ssh authmode

● 概要

このコマンドを用いて、SSH 設定のユーザ認証を更新します。

● 構文

config ssh authmode [password | publickey | hostbased] [enable | disable]

● パラメータ

password	ユーザ認証方法を指定します。
publickey	ユーザ認証方法を指定します。
hostbased	ユーザ認証方法を指定します。
enable	ユーザ認証方法を有効にします。
disable	ユーザ認証方法を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

SSH ユーザ認証方法を設定するには：

```
Zxxx0:admin#config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

Zxxx0:admin#
```

58.4. show ssh authmode

● 概要

このコマンドを用いて、ユーザ認証方法を表示します。

● 構文

show ssh authmode

● パラメータ

なし

● 制限

なし

● 実行例

SSH ユーザ認証方法を表示するには：

```
Zxxx0:admin#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password    : Enabled
Public Key  : Enabled
Host-based  : Enabled

Zxxx0:admin#
```

58.5. config ssh user

● 概要

このコマンドを用いて、SSH ユーザ情報を更新します。

● 構文

config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]

● パラメータ

<username 15>	ユーザ名を指定します。
authmode	認証モードを指定します。

hostbased	ユーザ認証方法を指定します。 hostname ホストのドメイン名を指定します。 <domain_name 32> ホストのドメイン名を指定します。ホスト名の値は 32 文字までです。 hostname_IP ホストのドメイン名と IP アドレスを指定します。 <domain_name 32> ホストのドメイン名を指定します。ホスト名の値は 32 文字までです。 <ipaddr> ホストの IPv4 アドレスを指定します。 <ipv6addr> ホストの IPv6 アドレスを指定します。
password	ユーザ認証方法を指定します。
publickey	ユーザ認証方法を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

NOTE まず、ユーザアカウントを作成する必要があります。

● 実行例

認証モードで admin というユーザを更新するには：

```
Zxxx0:admin#config ssh user admin authmode publickey
Command: config ssh user admin authmode publickey

Success.

Zxxx0:admin#
```

58.6. show ssh user authmode

● 概要

このコマンドを用いて、SSH ユーザ情報を表示します。

● 構文

show ssh user authmode

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

SSH 設定に関するユーザ情報を表示するには：

```
Zxxx0:admin# show ssh user authmode
Command: show ssh user authmode

Current Accounts
User Name       Authentication         Host Name            Host IP
--------------  ---------------        ---------------      -------------
test              Public Key
manager           Host-based           manager-local        172.18.61.180
beta              Host-based           beta-local           3000::105

Total Entries : 3

Zxxx0:admin#
```

58.7. config ssh server

● 概要

このコマンドを用いて、SSH サーバの一般情報を設定します。

● 構文

config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}(1)

● パラメータ

maxsession	SSH サーバの同時最大セッション数を指定します。 <int 1-8> SSH サーバの同時最大セッション数を指定します。最大セッション数の値は 1 ～ 8 です。初期値は 8 です。
contimeout	SSH サーバの接続タイムアウトを指定します。 <sec 120-600> SSH サーバの接続タイムアウトを指定します。接続タイムアウトの値は 120 ～ 600 秒です。初期値は 120 秒です。
authfail	ユーザの試行失敗の最大回数を指定します。 <int 2-20> ユーザの試行失敗の最大回数を指定します。認証試行の最大失敗回数の値は 2 ～ 20 です。初期値は 2 です。
rekey	（オプション）セッションキーを再生成する時間を指定します。 10min セッションキーの再生成に 10 分を指定します。 30min セッションキーの再生成に 30 分を指定します。 60min セッションキーの再生成に 60 分を指定します。 never セッションキーを再生成しません。
port	TCP ポート番号を 1 ～ 65535 の範囲で指定します。 <tcp_port_number 1-65535> TCP ポート番号を 1 ～ 65535 の範囲で指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

SSH サーバの最大セッション数を 3 に設定するには：

```
Zxxx0:admin#config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

Zxxx0:admin#
```

58.8. enable ssh

● 概要

このコマンドを用いて、SSH サーバサービスを有効にします。

● 構文

enable ssh

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

SSH を有効にするには：

```
Zxxx0:admin#enable ssh
Command: enable ssh

Success.

Zxxx0:admin#
```

58.9. disable ssh

● 概要

このコマンドを用いて、SSH サーバサービスを無効にします。

● 構文

disable ssh

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

SSH を無効にするには：

```
Zxxx0:admin#disable ssh
Command: disable ssh

Success.

Zxxx0:admin#
```

58.10. show ssh server

● 概要

このコマンドを用いて、SSH サーバの一般情報を表示します。

● 構文

show ssh server

● パラメータ

なし

● 制限

なし

● 実行例

SSH サーバを表示するには：

```
Zxxx0:admin# show ssh server
Command: show ssh server

The SSH Server Configuration
Maximum Session                  : 3
Connection Timeout               : 300
Authentication Fail Attempts     : 2
Rekey Timeout                    : 60min
TCP Port Number                  : 22

Zxxx0:admin#
```

59. スタティック MAC ベース VLAN コマンド

MAC ベース VLAN では、送信元の MAC アドレスに基づき、所属する VLAN を決定します。

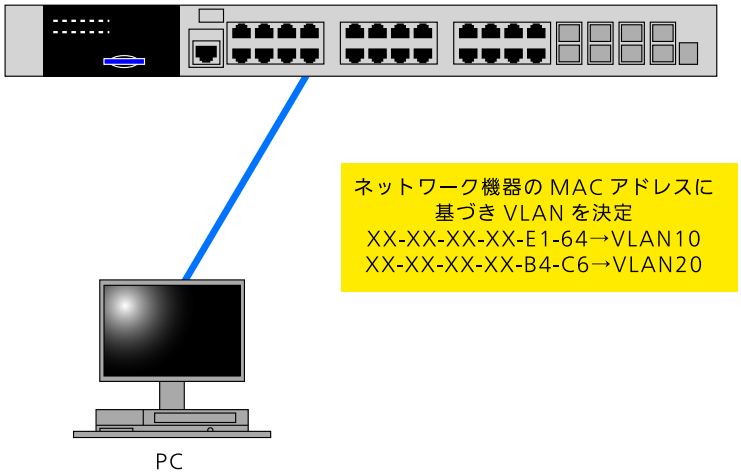


図 59-1　Static MAC-based Subnet VLAN の概略

NOTE　MAC ベース VLAN とサブネット VLAN を併用することができます。併用する場合、MAC ベース VLAN とサブネット VLAN のどちらの機能を優先するかを設定できます。

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}
delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>]}
show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

59.1.　create mac_based_vlan mac_address

● 概要

このコマンドを用いて、スタティック MAC ベース VLAN エントリを作成します。

● 構文

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}

● パラメータ

<macaddr>
MAC アドレスを指定します。

vlan	MAC アドレスと関連付ける VLAN を指定します。名前は既存のスタティック VLAN 名の必要があります。 **<vlan_name 32>** VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	MAC アドレスと関連付ける VLAN ID を指定します。ID は既存のスタティック VLAN ID の必要があります。 **<vlanid 1-4094>** 1 ～ 4094 の VLAN ID を指定します。
priority	（オプション）タグなしパケットに割り当てるプライオリティを指定します。指定しない場合、プライオリティが初期値の 0 になります。 **<value 0-7>** 使用するプライオリティの値を入力します。この値は 0 ～ 7 の必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スタティック MAC ベース VLAN エントリを作成するには：

```
Zxxx0:admin#create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Success.

Zxxx0:admin#
```

59.2. delete mac_based_vlan

● 概要

このコマンドを用いて、スタティック MAC ベース VLAN エントリを削除します。

● 構文

delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>]}

● パラメータ

mac_address	（オプション）削除する MAC アドレスを指定します。 **<macaddr>** 削除する MAC アドレスを指定します。
vlan	（オプション）MAC アドレスと関連付けられた VLAN を指定します。 **<vlan_name 32>** VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）MAC アドレスと関連付けられた VLAN ID を指定します。 **<vlanid 1-4094>** 1 ～ 4094 の VLAN ID を指定します。

NOTE MACアドレスとVLANを指定しない場合、ポートと関連付けられたすべてのスタティックエントリが削除されます。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スタティック MAC ベース VLAN エントリを削除するには：

```
Zxxx0:admin#delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: delete mac_based_vlan mac mac_address 00-00-00-00-00-01 vlan default
Success.

Zxxx0:admin#
```

59.3. show mac_based_vlan

● 概要

このコマンドを用いて、MAC ベース VLAN エントリを表示します。

● 構文

show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

● パラメータ

mac_address	（オプション）表示する MAC アドレスを指定します。 <macaddr> 表示する MAC アドレスを指定します。
vlan	（オプション）MAC アドレスと関連付けられた VLAN を指定します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）MAC アドレスと関連付けられた VLAN ID を指定します。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。

● 制限

なし

● 実行例

以下の例では、手動設定により MAC アドレス「00-80-c2-33-c3-45」が VLAN 300 に割り当てられています。MAC-AC によりこれが VLAN 400 に割り当てられます。MAC AC は手動設定よりプライオリティが高いため、手動で設定されたエントリが無効になります。MAC ベース VLAN エントリを表示するには：

```
Zxxx0:admin#show mac_based_vlan

MAC Address          VLAN ID      Status       Type
-------------------  ------------  ----------- --------
00-80-e0-14-a7-57    200           Active      Static
00-80-c2-33-c3-45    300           Inactive    Static
00-80-c2-33-c3-45    400           Active      MAC_based Access Control
00-a2-44-17-32-98    400           Active      WAC

Total Entries : 4

Zxxx0:admin#
```

60. サブネット VLAN コマンド

サブネット（Subnet）VLAN では、送信元 IP アドレスに基づき、所属する VLAN を決定します。IP アドレスの範囲をサブネットで指定し、VLAN と対応づけます。IPv4 および IPv6 のいずれでも利用できます。

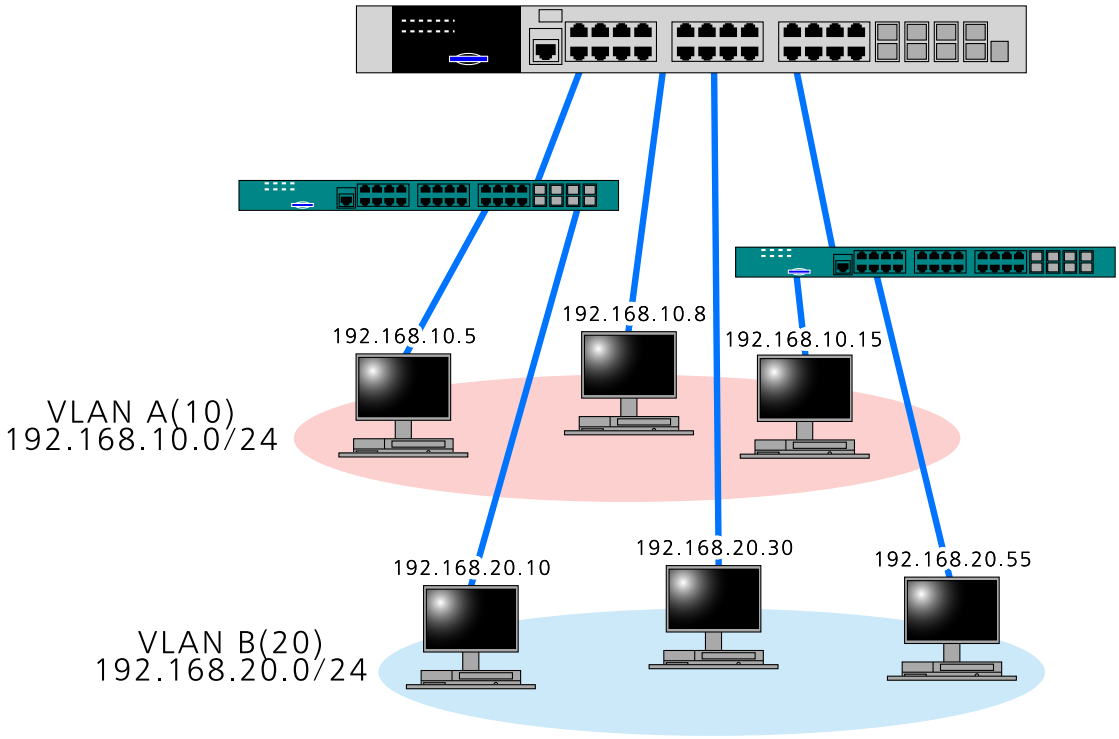


図 60-1　Subnet VLAN の概略

NOTE　MAC ベース VLAN とサブネット VLAN を併用することができます。併用する場合、MAC ベース VLAN とサブネット VLAN のどちらの機能を優先するかを設定できます。

create subnet_vlan [network <network_address> | ipv6network <ipv6networkaddr>] [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}
delete subnet_vlan [network <network_address> | ipv6network <ipv6networkaddr> | vlan <vlan_name 32> | vlanid <vidlist> | all]
show subnet_vlan {[network <network_address> | ipv6network <ipv6networkaddr> | vlan <vlan_name 32> | vlanid <vidlist>]}
config vlan_precedence ports <portlist> [mac_based_vlan | subnet_vlan]
show vlan_precedence ports {<portlist>}

60.1. create subnet_vlan

● 概要

このコマンドを用いて、サブネット VLAN エントリを作成します。サブネット VLAN エントリは IP サブネットベースの VLAN 分類ルールです。タグなしまたはプライオリティタグ付きの IP パケットをポートで受信すると、その送信元 IP アドレスを用いて、サブネット VLAN エントリと照合します。送信元 IP がエントリのサブネットに含まれる場合は、パケットが、このサブネットに定義された VLAN に分類されます。

● 構文

create subnet_vlan [network <network_address> | ipv6network <ipv6networkaddr>] [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}

● パラメータ

network	IPv4 ネットワークアドレスを指定します。 <network_address> IPv4 ネットワークアドレスを指定します。形式は ipaddress/prefix length です。
ipv6network	IPv6 ネットワークアドレスを指定します。 <ipv6networkaddr> IPv6 ネットワークアドレスを指定します。形式は ipaddress/prefix length です。IPv6 ネットワークアドレスのプレフィックス長は 64 以下です。
vlan	サブネットと関連付ける VLAN の名前を指定します。VLAN は既存のスタティック VLAN の必要があります。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	サブネットと関連付ける VLAN ID を指定します。VLAN は既存のスタティック VLAN の必要があります。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。
priority	（オプション）サブネットと関連付けるプライオリティを指定します。 <value 0-7> （オプション）サブネットと関連付けるプライオリティを指定します。範囲は 0 ～ 7 です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

サブネット VLAN エントリを作成するには：

```
Zxxx0:admin#create subnet_vlan network 172.168.1.1/24 vlan v2 priority 2
Command: create subnet_vlan network 172.168.1.1/24 vlan v2 priority 2

Success.

Zxxx0:admin#
```

IPv6 サブネット VLAN エントリを作成するには：

```
Zxxx0:admin# create subnet_vlan ipv6network fe80:250:baff::0/64 vlan v2 priority 2
Command: create subnet_vlan ipv6network fe80:250:baff::0/64 vlan v2 priority 2

Success.

Zxxx0:admin#
```

60.2. delete subnet_vlan

● 概要

このコマンドを用いて、スイッチからサブネット VLAN を削除します。ユーザが IP サブネットまたは VLAN に基づいてサブネット VLAN エントリを削除したり、すべてのサブネット VLAN エントリを削除することができます。

● 構文

delete subnet_vlan [network <network_address> | ipv6network <ipv6networkaddr> | vlan <vlan_name 32> | vlanid <vidlist> | all]

● パラメータ

network	IPv4 ネットワークアドレスを指定します。 <network_address> IPv4 ネットワークアドレスを指定します。形式は ipaddress/prefix length です。
ipv6network	IPv6 ネットワークアドレスを指定します。 <ipv6networkaddr> IPv6 ネットワークアドレスを指定します。形式は ipaddress/prefix length です。
vlan	この VLAN に関連付けられたすべてのサブネット VLAN エントリを削除します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	VLAN のリストを VLAN ID で指定します。 <vidlist> VLAN ID を指定します。
all	すべてのサブネット VLAN エントリを削除します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

サブネット VLAN エントリを削除するには：

```
Zxxx0:admin#delete subnet_vlan network 172.168.1.1/24
Command: delete subnet_vlan network 172.168.1.1/24

Success.

Zxxx0:admin#
```

すべてのサブネット VLAN エントリを削除するには：

```
Zxxx0:admin#delete subnet_vlan all
Command: delete subnet_vlan all

Success.

Zxxx0:admin#
```

60.3. show subnet_vlan

● 概要

このコマンドを用いて、サブネット VLAN を表示します。

● 構文

show subnet_vlan {[network <network_address> | ipv6network <ipv6networkaddr> | vlan <vlan_name 32> | vlanid <vidlist>]}

● パラメータ

network	（オプション）IPv4 ネットワークアドレスを指定します。 <network_address> IPv4 ネットワークアドレスを指定します。形式は ipaddress/prefix length です。
ipv6network	（オプション）IPv6 ネットワークアドレスを指定します。 <ipv6networkaddr> IPv6 ネットワークアドレスを指定します。形式は ipaddress/prefix length です。
vlan	（オプション）この VLAN に関連付けられたすべてのサブネット VLAN エントリを表示します。 <vlan_name 32> VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）VLAN のリストを VLAN ID で指定します。 <vidlist> VLAN ID を指定します。

NOTE パラメータを指定しない場合、すべてのサブネット VLAN 情報が表示されます。

● 制限

なし

● 実行例

指定したサブネット VLAN エントリを表示するには：

```
Zxxx0:admin#show subnet_vlan network 172.168.1.1/24
Command: show subnet_vlan network 172.168.1.1/24

IP Address/Subnet Mask          VLAN      Priority
------------------------        -----    ----------
172.168.1.0/255.255.255.0       10          2

Zxxx0:admin#
```

指定した IPv6 サブネット VLAN エントリを表示するには：

```
Zxxx0:admin# show subnet_vlan ipv6network fe80:250:baff::0/64
Command: show subnet_vlan ipv6network FE80:250:BAFF::/64

IP Address/Subnet Mask          VLAN      Priority
------------------------        -----    ----------
FE80:250:BAFF::/64              10          2

Zxxx0:admin#
```

すべてのサブネット VLAN エントリを表示するには：

```
Zxxx0:admin#show subnet_vlan
Command: show subnet_vlan

IP Address/Subnet Mask          VLAN      Priority
------------------------        -----    ----------
172.18.211.0/255.255.255.0       20          3
172.168.1.0/255.255.255.0        10          2
FE80:250:BAFF::/64               10          2

Total Entries: 3

Zxxx0:admin#
```

60.4. config vlan_precedence ports

● 概要

このコマンドを用いて、各ポートの VLAN の優先度を設定します。
MAC ベース VLAN およびサブネット VLAN の順序を指定できます。
ポートの VLAN が MAC ベース優先の場合は、MAC ベース VLAN が最初に処理されます。MAC ベース VLAN が失敗した場合は、サブネット VLAN が実行されます。
ポートの VLAN がサブネット VLAN 優先の場合は、サブネット VLAN が最初に処理されます。サブネット VLAN が失敗した場合は、MAC ベース VLAN が実行されます。

● 構文

config vlan_precedence ports <portlist> [mac_based_vlan | subnet_vlan]

● パラメータ

<portlist>この設定に使用するポートのリストを入力します。
mac_based_vlan MAC ベース VLAN がサブネット VLAN より優先されます。
subnet_vlan サブネット VLAN が MAC ベース VLAN より優先されます。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 に対してサブネット VLAN 優先するには：

```
Zxxx0:admin# config vlan_precedence ports 1 subnet_vlan
Command: config vlan_precedence ports 1 subnet_vlan

Success.

Zxxx0:admin#
```

60.5. show vlan_precedence ports

● 概要

このコマンドを用いて、VLAN の優先度を表示します。

● 構文

show vlan_precedence ports {<portlist>}

● パラメータ

<portlist>（オプション）表示に使用するポートのリストを指定します。

● 制限

なし

● 実行例

ポート 1 ～ 5 の VLAN の優先度を表示するには：

```
Zxxx0:admin#show vlan_precedence ports 1:1-1:5
Command: show vlan_precedence ports 1:1-1:5

Port      VLAN Precedence
----      -----------------
1         MAC-Based VLAN
2         Subnet VLAN
3         MAC-Based VLAN
4         MAC-Based VLAN
5         Subnet VLAN

Zxxx0:admin#
```

61.スイッチポートコマンド

本製品の各ポートについて、以下の内容を設定します。

- ポートスピード、フロー制御
- オートネゴシエーションオプション
- MAC アドレス学習の有無
- MDI/MDIX の設定
- コンボポートのメディア設定

config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto {capability_advertised {10_half | 10_full | 100_half | 100_full | 1000_full}} | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | auto_negotiation [restart_an | remote_fault_advertised [disable | offline | link_fault | auto_negotiation_error]] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description]}(1)
show ports {<portlist>} {[description | err_disabled | auto_negotiation | details | media_type]}

61.1. config ports

● 概要

このコマンドを用いて、スイッチのポート設定を変更します。

● 構文

config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto {capability_advertised {10_half | 10_full | 100_half | 100_full | 1000_full}} | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | auto_negotiation [restart_an | remote_fault_advertised [disable | offline | link_fault | auto_negotiation_error]] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description]}(1)

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	システムのすべてのポートを設定します。
medium_type	（オプション）コンボポートであるポートを設定するときに、メディアタイプを指定します。 fiber　ファイバ (SFP) ポートを指定します。 copper　銅 (UTP) ポートを指定します。

speed 指定したポートのポートスピードを設定します。
auto 以外に設定する場合は、はじめに EEE 機能を無効にしてください。
auto ポートスピードをオートネゴシエーションに設定します。
capability_advertised
オートネゴシエーションでアドバタイズするポートスピードを設定します。
10_half
ポートスピードを 10_half に設定します。**コンボポートでは設定できません。**
10_full
ポートスピードを 10_full に設定します。
100_half
ポートスピードを 100_half に設定します。**コンボポートでは設定できません。**
100_full
ポートスピードを 100_full に設定します。
1000_full
ポートスピードを 1000_full に設定します。ファイバーポートのスピードを 1000_full に設定する場合、ユーザが 1000-BASE T のペアのマスター / スレーブモードを設定する必要があります。ファイバの場合は、マスター / スレーブ設定なしのままにします。
master （オプション）マスターに設定します。
slave （オプション）スレーブに設定します。

auto_negotiation
オートネゴシエーションを設定します。
restart_an
オートネゴシエーションプロセスを再起動します。
remote_fault_advertised
リモート障害アドバタイズを設定します。
disable
リモート障害アドバタイズを無効にします。
offline
電源オフ、トランスミッタテストの実行、または有効な構成からローカルデバイスを削除する前に、ローカルデバイスがオフラインであることを示します。これを設定した場合にオフラインが検出されると、次回のオートネゴシエーション時にアドバタイズされます。
link_fault
これを設定した場合、ローカルデバイスが検出され、同期喪失によって Link_Failure 状態が示されると、次回のオートネゴシエーション時にアドバタイズされます。
auto_negotiation_error
次回のオートネゴシエーション時にアドバタイズされるローカルデバイスとリンクパートナ間の動作を除外する解決を指定します。

flow_control
flow_control を有効または無効に設定して、いくつかのポートのフロー制御をオンまたはオフにします。初期値は無効です。
enable
フロー制御を有効にします。
disable
フロー制御を無効にします。

learning いくつかのポートの MAC アドレス学習をオンまたはオフにします。初期値は enable です。
enable
MAC アドレス学習を有効にします。
disable
MAC アドレス学習を無効にします。

state	指定したポートの状態を有効または無効にします。ポートが error-disabled ステータスの場合、状態を enable に設定すると、これらのポートを無効状態から有効状態に回復できます。初期値は enable です。 **enable** 指定したポートを有効にします。 **disable** 指定したポートを無効にします。
mdix	ケーブルのタイプを指定します。初期値は auto です。 **auto** ケーブルの最適なタイプを自動的に感知します。 **normal** MDI-X モードとして動作します。 ストレートケーブルを使用して、端末を接続する場合に使用します。 **cross** MDI モードとして動作します。 ストレートケーブルを使用して、別のスイッチのポート（MDI-X モード）に接続する場合に使用します。
description	（オプション）ポートインターフェースの説明を表示します。 **<desc 1-32>** ポートインターフェースの説明を表示します。 **clear_description** （オプション）ポートインターフェースの現在の説明を削除します。

NOTE ポートスピードを auto 以外に設定する場合は、EEE 動作設定を無効にする必要があります。

NOTE コンボポートは半二重モード（10_half/100_half）に設定できません。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 3 のスピードを 10Mbps に設定し、全二重、learning 有効、state 有効、フロー制御有効に指定するには：

```
Zxxx0:admin#config ports 1-3 speed 10_full state enable learning enable
flow_control enable
Command: config ports 1-3 speed 10_full state enable learning enable flow_control
enable

Success.

Zxxx0:admin#
```

61.2. show ports

● 概要

このコマンドを用いて、指定した範囲のポートの現在の設定を表示します。

● 構文

show ports {<portlist>} {[description | err_disabled | auto_negotiation | details | media_type]}

● パラメータ

<portlist>	（オプション）表示するポートの範囲を指定します。
description	（オプション）ポートの説明を表示します。
err_disabled	（オプション）無効に関する情報を表示します。
auto_negotiation	（オプション）オートネゴシエーションに関する詳細情報を表示します。
details	（オプション）ポートの詳細情報を表示に含めるかどうかを指定します。
media_type	（オプション）現在のポートのメディアタイプを表示します。FE　ポートの場合、メディアタイプは 100BASE-T の必要があります。コンボポートの場合、現在有効なポートがファイバポートのときは、メディアタイプは 1000BASE-X です。現在有効なポートが銅ポートのときは、メディアタイプは 1000BASE-T です。

NOTE　このパラメータを指定しない場合、すべてのポートが表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 4 の設定を表示するには：

```
Zxxx0:admin#show ports 1:1-1:4
Command: show ports 1:1-1:4

 Port      State/          Settings             Connection          Address
           MDIX      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
 -------  --------  ---------------------  ----------------------  ---------
 1:1       Enabled   Auto/Disabled          Link Down               Enabled
           Auto
 1:2       Enabled   Auto/Disabled          Link Down               Enabled
           Auto
 1:3       Enabled   Auto/Disabled          Link Down               Enabled
           Auto
 1:4       Enabled   Auto/Disabled          Link Down               Enabled
           Auto
              Quit         Next Page    Previous Page    Refresh
```

ポート 1 ～ 4 の説明情報を表示するには：

```
Zxxx0:admin# show ports 1-4 description
Command: show ports 1:1-1:4 description

 Port      State/          Settings             Connection          Address
           MDIX      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
 -------  --------  ---------------------  ----------------------  ---------
 1:1       Enabled   Auto/Disabled          Link Down               Enabled
           Auto
           Description:
 1:2       Enabled   Auto/Disabled          Link Down               Enabled
           Auto
           Description:
 1:3       Enabled   Auto/Disabled          Link Down               Enabled
           Auto
           Description:
           Enabled   Auto/Disabled          Link Down               Enabled
           Auto
           Description:
              Quit         Next Page    Previous Page    Refresh
```

NOTE 接続ステータスには、Link Down、Speed/Duplex/FlowCtrl（リンクアップ）、および Err-Disabled があります。

error-disabled 情報を表示するには：

```
Zxxx0:admin# show ports err_disabled
Command: show ports err_disabled

Port    Port      Connection Status      Reason
        State
------  --------  ---------------------  ----------------
1       Enabled   Err-Disabled           Storm control
        Description: port1.
8       Enabled   Err-Disabled           Storm control
        Description: port8.

Zxxx0:admin#
```

62.システム重大性コマンド

SNMP（Simple Network Management Protocol）を利用したトラップやログの管理において、トラップの実施やログの記録を行うイベントの重大性のレベルを設定します。

config system_severity [trap | log | all] [emergency | alert | critical | error | warning | notice | information | debug | <level 0-7>]
show system_severity

62.1. config system_severity

● 概要

このコマンドを用いて、システムの重大性レベルの制御を設定します。

● 構文

config system_severity [trap | log | all] [emergency | alert | critical | error | warning | notice | information | debug | <level 0-7>]

● パラメータ

trap	トラップの重大性レベルの制御を設定します。
log	ログの重大性レベルの制御を設定します。
all	トラップとログの重大性レベルの制御を設定します。
emergency	emergency メッセージの重大性レベルを設定します。
alert	alert メッセージの重大性レベルを設定します。
critical	critical メッセージの重大性レベルを設定します。
error	error メッセージの重大性レベルを設定します。
warning	warning メッセージの重大性レベルを設定します。
notice	notice メッセージの重大性レベルを設定します。
informational	informational メッセージの重大性レベルを設定します。
debug	debug メッセージの重大性レベルを設定します。
<level 0-7>	0 ～ 7 の重大性レベルを指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

トラップの重大性レベルの制御を information レベルに設定するには：

```
Zxxx0:admin#config system_severity trap information
Command: config system_severity trap information

Success.

Zxxx0:admin#
```

62.2. show system_severity

● 概要

このコマンドを用いて、システムの重大性レベルの制御を表示します。

● 構文

show system_severity

● パラメータ

なし

● 制限

なし

● 実行例

システムの重大性レベルの制御を表示するには：

```
Zxxx0:admin#show system_severity
Command: show system_severity

System Severity Trap : warning
System Severity Log  : information

Zxxx0:admin#
```

63.技術サポートコマンド

本製品の稼動状況等の情報を出力します。技術サポートの参考データとして利用します。
出力結果を指定した TFTP サーバに送信することもできます。

show tech_support upload tech_support_toTFTP <ipaddr> <path_filename 64>

63.1. show tech_support

● 概要

このコマンドを用いて、技術サポート情報を表示します。特に本装置の全体的な稼動状況に関する情報を必要とする技術サポート担当者に有益なコマンドです。

● 構文

show tech_support

● パラメータ

なし

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

NOTE このコマンドを実行する時に、本装置にアクセスできなくなる場合があります。

NOTE このコマンドを実行中に設定されたセッションタイムアウト時間を超過すると、管理セッションがタイムアウトすることがあります。コンソールセッションの自動切断を無効にしないように、コンソールポートのタイムアウトを設定することを推奨します。

● 実行例

技術サポート情報を表示するには：

```
Zxxx0:admin#show tech_support
Command: show tech_support

#------------------------------------------------------------------------------
#                      Zxxx0 Gigabit Ethernet Switch
#                          Technical Support Information
#
#                            Firmware: Build 1.0.0.xx
#------------------------------------------------------------------------------


********************   Basic System Information   ********************

[SYS 2000-2-29 22:41:48]

Boot Time           : 29 Feb 2000  17:54:29
RTC Time            : 2000/02/29 22:41:48
Boot PROM Version   : Build 1.0.0.xx
Firmware Version    : Build 1.0.0.xx
Hardware Version    : A1
Serial number       :
MAC Address         : 00-01-02-03-04-00
[STACKING 2000-2-29 22:41:48]

 #Topology Information

 Stable Topology:
 My Box ID : 1              Role          : Master
 Box Cnt   : 1              Topology Type : Duplex Chain
 Unit  Prio-                                        Device Runtime   Stacking
 ID    rity  Role           MAC        Type        option version   version
 ----- ----  ------- ----------------- ---------- ------ --------- -------
 1     32 32 Master  00-01-02-03-04-00 Zxxx0 0x0002 1.0.0.xx  2.0.1
```

63.2. upload tech_support_toTFTP

● 概要

このコマンドを用いて、技術サポート情報を TFTP サーバにアップロードします。このコマンドを停止するには、実行中に Ctrl+C または ESC を押します。

● 構文

upload tech_support_toTFTP <ipaddr> <path_filename 64>

● パラメータ

<ipaddr> TFTP サーバの IPv4 アドレスを指定します。
<path_filename 64> TFTP サーバに送信する技術サポート情報ファイルのファイル名を指定します。ファイル名の最大文字数は 64 文字です。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

技術サポート情報をアップロードするには：

```
Zxxx0:admin#upload tech_support_toTFTP 10.0.0.66 tech_suppport.txt
Command: upload tech_support_toTFTP 10.0.0.66 tech_suppport.txt

Connecting to server.................. Done.
Upload techsupport file.............. Done.

Success.

Zxxx0:admin#
```

64. 時刻および SNTP コマンド

本製品の内蔵時計の時刻合わせを行います。
手動または SNTP（Simple Network Time Protocol）を利用した自動での時刻合わせを行えます。
また、タイムゾーンの設定、サマータイムの設定も行えます。

```
config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>} (1)
show sntp
enable sntp
disable sntp
config time <date ddmthyyyy> <time hh:mm:ss>
config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>} (3)
config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth
    <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4, last> | e_day
    <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 |
    90 | 120]} (9) | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time
    <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time
    hh:mm> | offset [30 | 60 | 90 | 120]}(7)]
show time
```

64.1. config sntp

● 概要

このコマンドを用いて、SNTP 設定を変更します。

● 構文

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>} (1)

● パラメータ

primary	（オプション）SNTP プライマリサーバの IP アドレスを指定します。
	<ipaddr> SNTP プライマリサーバの IP アドレスを指定します。
secondary	
	（オプション）SNTP セカンダリサーバの IP アドレスを指定します。
	<ipaddr> SNTP セカンダリサーバの IP アドレスを指定します。
poll-interval	
	（オプション）ポーリング間隔を指定します。
	<int 30-99999> 30 ～ 99999 秒のポーリング間隔を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

SNTP を設定するには：

```
Zxxx0:admin#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

Zxxx0:admin#
```

64.2. show sntp

● 概要

このコマンドを用いて、現在の SNTP の時刻配信元および設定を表示します。

● 構文

show sntp

● パラメータ

なし

● 制限

なし

● 実行例

SNTP を表示するには：

```
Zxxx0:admin#show sntp
Command: show sntp

Current Time Scource  : System Clock
SNTP                  : Disabled
SNTP Primary Server   : 10.1.1.1
SNTP Secondary Server : 10.1.1.2
SNTP Poll Interval    : 720 sec

Zxxx0:admin#
```

64.3. enable sntp

● 概要

このコマンドを用いて、SNTP のサポートを有効にします。

● 構文

enable sntp

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

SNTP を有効にするには：

```
Zxxx0:admin#enable sntp
Command: enable sntp

Success.

Zxxx0:admin#
```

64.4. disable sntp

● 概要

このコマンドを用いて、SNTP のサポートを無効にします。

● 構文

disable sntp

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

SNTP を無効にするには：

```
Zxxx0:admin#disable sntp
Command: disable sntp

Success.

Zxxx0:admin#
```

64.5. config time

● 概要

このコマンドを用いて、時間設定を変更します。

● 構文

config time <date ddmthyyyy> <time hh:mm:ss>

● パラメータ

<date ddmthyyyy>	システムクロックの日付を指定します。(日は 01 ～ 31、月は Jan ～ Dec、年は 2000-2100 を入力してください)
<time hh:mm:ss>	システムクロックの時刻を指定します。(時間は 0 ～ 23、分と秒は 0 ～ 59 を入力してください)

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

時間を設定するには：

```
Zxxx0:admin# config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

Zxxx0:admin#
```

64.6. config time_zone

● 概要

このコマンドを用いて、タイムゾーン設定を変更します。

● 構文

config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>} (3)

● パラメータ

operator	タイムゾーンの演算子を指定します。 +　正 -　負
hour	タイムゾーンの時間を指定します。 <gmt_hour 0-13> タイムゾーンの時間を 0 ～ 13 で指定します。
min	タイムゾーンの分を指定します。 <minute 0-59> タイムゾーンの分を 0 ～ 59 で指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

タイムゾーンを設定するには：

```
Zxxx0:admin#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

Zxxx0:admin#
```

64.7. config dst

● 概要

このコマンドを用いて、サマータイム（サマータイム）設定を変更します。

● 構文

config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4, last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} (9) | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} (7)]

● パラメータ

disable	本装置のサマータイム設定を無効にします。
repeating	このモードを指定すると、〇月〇週目〇曜日～〇月〇週目〇曜日の形式でサマータイム設定の期間を指定できます。
annual	このモードを指定すると、〇月〇日～〇月〇日の形式でサマータイム設定の期間を指定できます。
s_week	サマータイムを開始する週を数で設定します。 <start_week 1-4,last> サマータイムを開始する週を数で設定します。値は 1 ～ 4、lost です。
s_day	サマータイムを開始する曜日を設定します。 <start_day sun-sat> サマータイムを開始する曜日を設定します。値は、sun、mon、tue、wed、thu、fri、sat です。
s_mth	サマータイムを開始する月を設定します。 <start_mth 1-12> サマータイムを開始する月を設定します。値は 1 ～ 12 です。
s_time	サマータイムを開始する時刻を設定します。 <start_time hh:mm> サマータイムの開始時刻を hh:mm で設定します。
e_week	サマータイムを終了する週を数で設定します。 <end_week 1-4,last> サマータイムを終了する週を数で設定します。値は 1 ～ 4、lost です。
e_day	サマータイムを終了する曜日を設定します。 <end_day sun-sat> サマータイムを終了する曜日を設定します。値は、sun、mon、tue、wed、thu、fri、sat です。
e_mth	サマータイムを終了する月を設定します。 <end_mth 1-12> サマータイムを終了する月を設定します。値は 1 ～ 12 です。
e_time	サマータイムを終了する時刻を設定します。 <end_time hh:mm> サマータイムの終了時刻を hh:mm で設定します。

offset	サマータイム中に加算または減算する時間を分単位で指定します。オフセットの範囲は 30、60、90、120 です。初期値は 60 です。 30　サマータイム中に加算または減算する時間を 30 分に指定します。 60　サマータイム中に加算または減算する時間を 60 分に指定します。 90　サマータイム中に加算または減算する時間を 90 分に指定します。 120　サマータイム中に加算または減算する時間を 120 分に指定します。
annual	○月○日～○月○日の形式でサマータイム設定の期間を指定できます。
s_date	サマータイムを開始する日を設定します。 <start_date 1-31> サマータイムを開始する日を設定します。値は 1 ～ 31 です。
e_date	サマータイムを終了する日を設定します。 <end_date 1-31> サマータイムを終了する日を設定します。値は 1 ～ 31 です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

時間を設定するには：

```
Zxxx0:admin#config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e_day wed e_mth 10 e_time 15:30 offset 30

Success.

Zxxx0:admin#
```

64.8. show time

● 概要

このコマンドを用いて、現在の時間の状態を表示します。

● 構文

show time

● パラメータ

なし

● 制限

なし

● 実行例

時間を表示するには：

```
Zxxx0:admin#show time
Command: show time

Current Time Source  : System Clock
Boot Time    : 8 Jan 2000  21:44:33
Current Time : 9 Jan 2000  03:25:17
Time Zone    : GMT +00:00
Daylight Saving Time : Disabled
Offset In Minutes: 60
         Repeating From   : Apr 1st  Sun 00:00
                   To     : Oct last Sun 00:00
         Annual    From   : 29 Apr 00:00
                   To     : 12 Oct 00:00
Zxxx0:admin#
```

65.トラフィックセグメンテーションコマンド

トラフィックセグメンテーションでは、ポート毎に受信データを転送可能なポートを設定します。
VLAN 内でさらに詳細にトラフィックを制限したい場合に利用します。

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation {<portlist>}

65.1. config traffic_segmentation

● 概要

このコマンドを用いて、トラフィックセグメンテーションを設定します。

● 構文

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを指定します。
forward_list	ポートのフォワーディングドメインの範囲を指定します。 null　ポートのフォワーディングドメインの範囲をヌルに指定します。 all　すべてのポートを指定します。 <portlist>設定するポートの範囲を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

トラフィックセグメンテーションを設定するには：

```
Zxxx0:admin#config traffic_segmentation 1-6 forward_list 7-8
Command: config traffic_segmentation 1-6 forward_list 7-8

Success.

Zxxx0:admin#
```

65.2. show traffic_segmentation

● 概要

このコマンドを用いて、トラフィックセグメンテーションテーブルを表示します。

● 構文

show traffic_segmentation {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

NOTE パラメータを指定しない場合、現在のすべてのトラフィックセグメンテーションテーブルが表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 3 のトラフィックセグメンテーションテーブルを表示するには：

```
Zxxx0:admin#show traffic_segmentation 1-3
Command: show traffic_segmentation 1-3

Traffic Segmentation Table

Port    Forward Portlist
------  ------------------------------------------------
1       1-28
2       1-28
3       1-28

Zxxx0:admin#
```

66.ユーティリティコマンド

ここでは、以下のようなユーティリティコマンドについて説明しています。

- TFTP サーバまたは RCP サーバを利用したファームウェアやコンフィグレーションファイル、ログファイルのダウンロードおよびアップロード
- 起動時に使用するファームウェアやコンフィグレーションファイルの選択
- RCP サーバの設定
- IPv4 または IPv6 用の ping、traceroute
- Telnet サーバへのログイン
- ブロードキャストアドレス宛ての ping 応答の設定

---

download [firmware_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {[unit <unit_id 1-4> | all]} {dest_file <pathname>} {boot_up} | cfg_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {[unit <unit_id 1-4> | all]} {[increment | dest_file <pathname>]}]

download cfg_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> | rcp:<string 128>] {[unit <unit_id 1-4> | all]} {dest_file <pathname>}

download firmware_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> | rcp:<string 128>] {[unit <unit_id 1-4> | all]} {dest_file <pathname>} {boot_up}

upload [cfg_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-4>} {src_file <pathname>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> | attack_log_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-4>} | firmware_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-4>} {src_file <pathname>}]

upload attack_log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp:<string 128>] {unit <unit_id 1-4>}

upload cfg_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp:<string 128>] {unit <unit_id 1-4>} {src_file <pathname>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}

upload firmware_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp:<string 128>] {unit <unit_id 1-4>} {src_file <pathname>}

upload log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp:<string 128>]

show config [effective | modified | current_config | boot_up | file <pathname>] {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}

config rcp server {ipaddress <ipaddr> | username <username>}

config rcp server clear [ipaddr | username | both]

show rcp server

ping [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99> | source_ip <ipaddr>}

---

ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99> | source_ip <ipv6addr>}
traceroute [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}
traceroute6 <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}
telnet [<ipaddr> | <domain_name 255> | <ipv6addr>] {tcp_port <value 1-65535>}
enable broadcast_ping_reply
disable broadcast_ping_reply
show broadcast_ping_reply

66.1. download

● 概要

このコマンドを用いて、新しいファームウェアまたはスイッチ設定ファイルをダウンロードします。

● 構文

download [firmware_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {[unit <unit_id 1-4> | all]} {dest_file <pathname>} {boot_up} | cfg_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {[unit <unit_id 1-4> | all]} {[increment | dest_file <pathname>]}]

● パラメータ

firmware_fromTFTP	TFTP サーバからスイッチの新しいファームウェアをダウンロードしてインストールします。 **<ipaddr>** TFTP サーバの IP アドレスを指定します。 **<ipv6addr>** TFTP サーバの IPv6 アドレスを指定します。 **<domain_name 255>** TFTP サーバのドメイン名を指定します。最大文字数は、「.」区切りで各パート 63 文字、最大 255 文字です。
src_file	TFTP サーバのパス名とファイル名を指定します。相対パス名または絶対パス名を指定できます。パス名を指定しない場合、TFTP サーバパスが参照されます。最大文字数は 64 文字です。 **<path_filename 64>** TFTP サーバのパス名とファイル名を指定します。相対パス名または絶対パス名を指定できます。パス名を指定しない場合、TFTP サーバパスが参照されます。最大文字数は 64 文字です。
unit	スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 **<unit_id 1-4>**使用するユニット ID を入力します。 **all** スタッキングシステムのすべてのユニットを使用します。
dest_file	（オプション）装置ファイルシステムの絶対パス名を指定します。パス名を指定しない場合、本装置の起動イメージが上書きされます。 **<pathname>** 装置ファイルシステムの絶対パス名を指定します。
boot_up	（オプション）起動ファイルとして指定します。

cfg_fromTFTP	TFTP サーバからスイッチの新しい設定ファイルをダウンロードしてインストールします。 <ipaddr> TFTP サーバの IP アドレスを指定します。 <ipv6addr> TFTP サーバの IPv6 アドレスを指定します。 <domain_name 255> TFTP サーバのドメイン名を指定します。最大文字数は、「.」区切りで各パート 63 文字、最大 255 文字です。
src_file	FTP サーバのパス名とファイル名を指定します。相対パス名または絶対パス名を指定できます。パス名を指定しない場合、TFTP サーバパスが参照されます。最大文字数は 64 文字です。 <path_filename 64> FTP サーバのパス名とファイル名を指定します。相対パス名または絶対パス名を指定できます。パス名を指定しない場合、TFTP サーバパスが参照されます。最大文字数は 64 文字です。
unit	スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 <unit_id 1-4>使用するユニット ID を入力します。 all スタッキングシステムのすべてのユニットを使用します。
increment	increment を指定すると、新しい設定を適用する前に、既存の設定が消去されません。指定しない場合は、新しい設定を適用する前に、既存の設定が消去されます。
dest_file	（オプション）装置の絶対パス名を指定します。パス名を指定しない場合、起動設定ファイルが参照されます。 <pathname> 装置の絶対パス名を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

TFTP サーバからランタイムファームウェアをダウンロードするには：

```
Zxxx0:admin#download firmware_fromTFTP 10.0.0.66 src_file runtime.rom dest_file
runtime.rom
Command: download firmware_fromTFTP 10.0.0.66 src_file runtime.rom dest_file
runtime.rom

 Connecting to server................... Done.
 Download firmware...................... Done.  Do not power off!
 Please wait, programming flash......... Done.


Zxxx0:admin#
```

66.2. download cfg_fromRCP

● 概要

このコマンドを用いて、RCP（Remote Copy Protocol）サーバから設定ファイルをダウンロードします。

● 構文

download cfg_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> | rcp: <string 128>] {[unit <unit_id 1-4> | all]} {dest_file <pathname>}

● パラメータ

username	（オプション）RCP サーバのリモートユーザ名を指定します。 <username> RCP サーバのリモートユーザ名を指定します。
<ipaddr>	（オプション）RCP サーバの IP アドレスを指定します。
src_file	RCP サーバのスイッチ設定ファイルのパスとファイル名を指定します。最大文字数は 64 文字です。 <path_filename 64> RCP サーバのスイッチ設定ファイルのパスとファイル名を指定します。最大文字数は 64 文字です。
rcp:	構文：rcp: username@ipaddr/directory/filename フルパスの例：user_name@10.1.1.1/home/user_name/desxxxx.rom 相対パスの例：user_name@10.1.1.1./desxxxx.rom。 注：<string> ではスペースは使用しません。 <string 128> 構文：rcp: username@ipaddr/directory/filename フルパスの例：user_name@10.1.1.1/home/user_name/desxxxx.rom 相対パスの例：user_name@10.1.1.1./desxxxx.rom RCP 文字列のユーザ名を省略した例：10.1.1.1./desxxxx.rom 注：<string> ではスペースは使用しません。
unit	スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 <unit_id 1-4> 使用するユニット ID を入力します。この値は 1 ～ 4 の必要があります。 all スタッキングシステムのすべてのユニットを使用します。
dest_file	（オプション）装置の目的のファイルのパスとファイル名を指定します。 <pathname> 目的のファイルのパスとファイル名を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

RCP サーバから設定ファイルをダウンロードするには：

```
Zxxx0:admin#download cfg_fromRCP username rcp_user 172.18.212.106 src_file /home/
runtime.cfg
Command: download cfg_fromRCP username rcp_user 172.18.212.106 src_file /home/
runtime.cfg

Connecting to server................... Done.
Download configuration................. Done.

Zxxx0:admin#
```

66.3. download firmware_fromRCP

● 概要

このコマンドを用いて、RCP（Remote Copy Protocol）サーバからファームウェアファイルをダウンロードします。

● 構文

download firmware_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> | rcp: <string 128>] {[unit <unit_id 1-4> | all]} {dest_file <pathname>} {boot_up}

● パラメータ

username	（オプション）RCP サーバのリモートユーザ名を指定します。 <username> RCP サーバのリモートユーザ名を指定します。
<ipaddr>	（オプション）RCP サーバの IP アドレスを指定します。
src_file	RCP サーバまたはローカルのパス名を指定します。注：ユーザが相対ファイルパスを指定した場合、パス検索方法はサーバシステムに依存します。 <path_filename 64> RCP サーバまたはローカルのパス名を指定します。注：ユーザが相対ファイルパスを指定した場合、パス検索方法はサーバシステムに依存します。

rcp:	構文：rcp: username@ipaddr/directory/filename フルパスの例：user_name@10.1.1.1/home/user_name/desxxxx.rom 相対パスの例：user_name@10.1.1.1./desxxxx.rom RCP 文字列のユーザ名を省略した例：10.1.1.1./desxxxx.rom 注：<string> ではスペースは使用できません。 **<string 128>** 構文：rcp: username@ipaddr/directory/filename フルパスの例：user_name@10.1.1.1/home/user_name/desxxxx.rom 相対パスの例：user_name@10.1.1.1./desxxxx.rom RCP 文字列のユーザ名を省略した例：10.1.1.1./desxxxx.rom。 注：<string> ではスペースは使用できません。
unit	スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 **<unit_id 1-4>** 使用するユニット ID を入力します。この値は 1 ～ 4 の必要があります。 **all** スタッキングシステムのすべてのユニットを使用します。
dest_file	（オプション）装置の目的のファイルのパスとファイル名を指定します。 **<pathname>** 目的のファイルのパスとファイル名を指定します。
boot_up	起動ファイルとして指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

RCP サーバからファームウェアをダウンロードするには：

```
Zxxx0:admin#download firmware_fromRCP username rcp_user 10.90.90.90 src_file /
home/Zxxx0.rom
Command: download firmware_fromRCP username rcp_user 10.90.90.90 src_file /home/
Zxxx0.rom

Connecting to server................... Done.
Download firmware...................... Done.   Do not power off !!
Please wait, programming flash......... Done.
Saving current settings to NV-RAM...... Done.

Zxxx0:admin#
```

66.4. upload

● 概要

このコマンドを用いて、ファームウェアまたは設定ファイルを装置から TFTP サーバにアップロードします。

● 構文

upload [cfg_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-4>} {src_file <pathname>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> | attack_log_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-4>} | firmware_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-4>} {src_file <pathname>}]

● パラメータ

cfg_toTFTP	設定ファイルを装置から TFTP サーバにアップロードします。 <ipaddr> TFTP サーバの IP アドレスを指定します。 <ipv6addr> TFTP サーバの IPv6 アドレスを指定します。 <domain_name 255> TFTP サーバのドメイン名を入力します。最大文字数は、「.」区切りで各パート 63 文字、最大 255 文字です。
dest_file	TFTP サーバのパス名を指定します。相対パス名または絶対パス名を指定できます。 <path_filename 64> TFTP　サーバのスイッチ設定ファイルの場所を指定します。このファイルが、スイッチからアップロードしたファイルと置き換えられます。最大文字数は 64 文字です。
unit	（オプション）スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 <unit_id 1-4> 使用するユニット ID を入力します。
src_file	（オプション）装置ファイルシステムの絶対パス名を指定します。パス名を指定しない場合、起動設定ファイルが参照されます。 <pathname> 装置のスイッチ設定ファイルの場所を指定します。
include	（オプション）指定したフィルタ文字列を含む行を含めます。
exclude	（オプション）指定したフィルタ文字列を含む行を除外します。

begin	（オプション）指定したフィルタ文字列を含む最初の行が、出力の最初の行になります。 <filter_string 80> 引用符で囲んでフィルタ文字列を指定します。フィルタ文字列自体に引用符を含めることはできません。フィルタ文字列は大文字小文字が区別されます。 <filter_string 80> 引用符で囲んでフィルタ文字列を指定します。 <filter_string 80> 引用符で囲んでフィルタ文字列を指定します。
log_toTFTP	ログファイルを装置から TFTP サーバにアップロードします。 <ipaddr> TFTP サーバの IP アドレスを指定します。 <ipv6addr> TFTP サーバの IPv6 アドレスを指定します。 <domain_name 255> TFTP サーバのドメイン名を入力します。最大文字数は、「.」区切りで各パート 63 文字、最大 255 文字です。
dest_file	TFTP サーバの場合にパス名を指定します。 <path_filename 64> TFTP サーバのパス名を指定します。相対パス名または絶対パス名を指定できます。
attack_log_toTFTP	攻撃ログを TFTP サーバにアップロードします。 <ipaddr> TFTP サーバの IP アドレスを指定します。 <ipv6addr> TFTP サーバの IPv6 アドレスを指定します。 <domain_name 255> TFTP サーバのドメイン名を入力します。最大文字数は、「.」区切りで各パート 63 文字、最大 255 文字です。
dest_file	TFTP サーバの場合にパス名を指定します。 <path_filename 64> TFTP サーバのパス名を指定します。相対パス名または絶対パス名を指定できます。
unit	（オプション）スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 <unit_id 1-4> 使用するユニット ID を入力します。
firmware_toTFTP	ファームウェアを装置から TFTP サーバにアップロードします。 <ipaddr> TFTP サーバの IP アドレスを指定します。 <ipv6addr> TFTP サーバの IPv6 アドレスを指定します。 <domain_name 255> TFTP サーバのドメイン名を入力します。最大文字数は、「.」区切りで各パート 63 文字、最大 255 文字です。
dest_file	TFTP サーバの場合にパス名を指定します。 <path_filename 64> TFTP サーバの場合にパス名を指定します。
unit	（オプション）スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 <unit_id 1-4> 使用するユニット ID を入力します。

src_file	（オプション）装置ファイルシステムの絶対パス名を指定します。パス名を指定しない場合、起動イメージが参照されます。 <pathname> 装置ファイルシステムの絶対パス名を指定します。パス名を指定しない場合、起動イメージが参照されます。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ファイルシステム装置から TFTP サーバにファームウェアをアップロードするには：

```
Zxxx0:admin#upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.rom src_file
1.0.0.xx.rom
Command: upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.rom src_file
1.0.0.xx.rom

Connecting to server.................. Done.
Upload firmware....................... Done.

Zxxx0:admin#
```

現在の設定ファイルを TFTP サーバにアップロードするには：

```
Zxxx0:admin#upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\Zxxx0.cfg
Command: upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\Zxxx0.cfg

Connecting to server.................. Done.
Upload configuration.................. Done.

Zxxx0:admin#
```

すべてのログを TFTP サーバにアップロードするには：

```
Zxxx0:admin#upload log_toTFTP 10.48.74.121 dest_file c:\log\Zxxx0.log
Command: upload log_toTFTP 10.48.74.121 dest_file c:\log\Zxxx0.log

Connecting to server.................. Done.
Upload log............................ Done.

Zxxx0:admin#
```

危険ログをアップロードするには：

```
Zxxx0:admin# upload attack_log_toTFTP 10.48.74.121 dest_file c:\alert.txt
Command: upload attack_log_toTFTP 10.48.74.121 dest_file c:\alert.txt

 Connecting to server................... Done.
 Upload attack log...................... Done.

Success.

Zxxx0:admin#
```

66.5. upload attack_log_toRCP

● 概要

このコマンドを用いて、攻撃ログファイルを装置から RCP サーバにアップロードします。

NOTE ユーザが相対ファイルパスを指定した場合、パス検索方法はサーバシステムに依存します。一部のシステムでは、まず、ユーザの現在の作業ディレクトリが検索され、次に環境パスが検索されます。

● 構文

upload attack_log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-4>}

● パラメータ

username	（オプション）RCP サーバのリモートユーザ名をです。 <username> 使用するリモートユーザ名を入力します。
<ipaddr>	（オプション）設定に使用する IP アドレスを入力します。
dest_file	使用する目的ファイルを指定します。 <path_filename 64> RCP サーバまたはローカル装置のパス名を指定します。
rcp:	構文：rcp: username@ipaddr/directory/filename フルパスの例：user_name@10.1.1.1/home/user_name/desxxxx.rom 相対パスの例：user_name@10.1.1.1./desxxxx.rom 注：<string> ではスペースを使用しないでください。 <string 128> RCP 文字列を入力します。
unit	（オプション）スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 <unit_id 1-4> 使用するユニット ID を入力します。この値は 1 ～ 4 の必要があります。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

攻撃ログを装置から RCP サーバにアップロードするには：

```
Zxxx0:admin# upload attack_log_toRCP username rcp_user 172.18.212.104 dest_file /
home/Zxxx0.log unit 2
Command: upload attack_log_toRCP username rcp_user 172.18.212.104 dest_file /home/
Zxxx0.log unit 2

Connecting to server.......... Done.
Upload Attack log.............. Done.
Success.

Zxxx0:admin#
```

66.6. upload cfg_toRCP

● 概要

このコマンドを用いて、装置から RCP（Remote Copy Protocol）サーバに設定ファイルをアップロードします。

● 構文

upload cfg_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-4>} {src_file <pathname>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}

● パラメータ

username	（オプション）RCP サーバのリモートユーザ名を指定します。 <username> RCP サーバのリモートユーザ名を指定します。
<ipaddr>	（オプション）RCP サーバの IP アドレスを指定します。
dest_file	RCP サーバのパス名を指定します。注：ユーザが相対ファイルパスを指定した場合、パス検索方法はサーバシステムに依存します。一部のシステムでは、まず、ユーザの現在の作業ディレクトリが検索され、次に環境パスが検索されます。 <path_filename 64> RCP サーバまたはローカル RCP クライアントのパス名を指定します。
rcp:	RCP サーバまたはローカル RCP クライアントのパスを指定します。注：ユーザが相対ファイルパスを指定した場合、パス検索方法はサーバシステムに依存します。一部のシステムでは、まず、ユーザの現在の作業ディレクトリが検索され、次に環境パスが検索されます。 <string 128> RCP サーバまたはローカル RCP クライアントのパスを指定します。

unit	（オプション）スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 <unit_id 1-4> 使用するユニット ID を入力します。この値は 1 ～ 4 の必要があります。
src_file	（オプション）ソースファイルのパス名を指定します。 <pathname> ソースファイルのパス名を指定します。パス名を指定しない場合、現在の装置設定のみがアップロードされることにご注意ください。
include	（オプション）指定したフィルタ文字列を含む行を含めます。
exclude	（オプション）指定したフィルタ文字列を含む行を除外します。
begin	（オプション）指定したフィルタ文字列を含む最初の行が、出力の最初の行になります。 <filter_string 80> 引用符で囲んでフィルタ文字列を指定します。フィルタ文字列自体に引用符を含めることはできません。フィルタ文字列は大文字小文字が区別されます。 <filter_string 80> 引用符で囲んでフィルタ文字列を指定します。 <filter_string 80> 引用符で囲んでフィルタ文字列を指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

装置から RCP サーバに現在の設定をアップロードするには：

```
Zxxx0:admin#upload cfg_toRCP username rcp_user 10.48.74.121 dest_file /home/
Zxxx0.cfg
Command: upload cfg_toRCP username rcp_user 10.48.74.121 dest_file /home/Zxxx0.cfg

Connecting to server... Done.
Upload configuration... Done.

Zxxx0:admin#
```

66.7. upload firmware_toRCP

● 概要

このコマンドを用いて、装置から RCP（Remote Copy Protocol）サーバにファームウェアをアップロードします。

● 構文

upload firmware_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-4>} {src_file <pathname>}

● パラメータ

username	（オプション）RCP サーバのリモートユーザ名を指定します。 **<username>** RCP サーバのリモートユーザ名を指定します。
<ipaddr>	（オプション）RCP サーバの IP アドレスを指定します。
dest_file	RCP サーバのパス名を指定します。注：ユーザが相対ファイルパスを指定した場合、パス検索方法はサーバシステムに依存します。一部のシステムでは、まず、ユーザの現在の作業ディレクトリが検索され、次に環境パスが検索されます。 **<path_filename 64>** RCP サーバのパス名を指定します。
rcp:	RCP サーバまたはローカル RCP クライアントのパス名を指定します。 構文：rcp: username@ipaddr/directory/filename フルパスの例：user_name@10.1.1.1/home/user_name/desxxxx.rom 相対パスの例：user_name@10.1.1.1./desxxxx.rom 注：<string> ではスペースは使用できません。 **<string 128>** RCP サーバまたはローカル RCP クライアントのパス名を指定します。 構文：rcp: username@ipaddr/directory/filename フルパスの例：user_name@10.1.1.1/home/user_name/desxxxx.rom 相対パスの例：user_name@10.1.1.1./desxxxx.rom 注：<string> ではスペースは使用できません。
unit	（オプション）スタッキングシステムのユニットを指定します。指定しない場合、マスターユニットが参照されます。 **<unit_id 1-4>** 使用するユニット ID を入力します。この値は 1 ～ 4 の必要があります。
src_file	（オプション）ソースファイルのパス名を指定します。指定しない場合、装置の起動イメージがアップロードされます。 **<pathname>** ソースファイルのパス名を指定します。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

RCP サーバにファームウェアイメージをアップロードするには：

```
Zxxx0:admin#upload firmware_toRCP rcp: rcp_user@172.18.212.106/Zxxx0.rom src_file
2.00.009.rom
Command: upload firmware_toRCP rcp: rcp_user@172.18.212.106/Zxxx0.rom src_file
2.00.009.rom

Connecting to server.............. Done.
Upload firmware................... Done.

Zxxx0:admin#
```

66.8. upload log_toRCP

● 概要

このコマンドを用いて、装置から RCP（Remote Copy Protocol）サーバにログファイルをアップロードします。

● 構文

upload log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>]

● パラメータ

username	（オプション）RCP サーバのリモートユーザ名を指定します。 <username> RCP サーバのリモートユーザ名を指定します。
<ipaddr>	（オプション）RCP サーバの IP アドレスを指定します。
dest_file	RCP サーバのパス名を指定します。注：ユーザが相対ファイルパスを指定した場合、パス検索方法はサーバシステムに依存します。一部のシステムでは、まず、ユーザの現在の作業ディレクトリが検索され、次に環境パスが検索されます。 <path_filename 64> RCP サーバのパス名を指定します。
rcp:	RCP サーバのパス名を指定します。 <string 128> RCP サーバのパス名を指定します。 構文：rcp: username@ipaddr/directory/filename フルパスの例：user_name@10.1.1.1/home/user_name/desxxxx.rom 相対パスの例：user_name@10.1.1.1./desxxxx.rom 注：<string> ではスペースは使用できません。

● 制限

このコマンドは、管理者およびオペレータレベルのユーザのみ実行できます。

● 実行例

ログを装置から RCP サーバにアップロードするには：

```
Zxxx0:admin#upload log_toRCP username rcp_user 172.18.212.104 dest_file /home/
Zxxx0.log
Command: upload log_toRCP username rcp_user 172.18.212.104 dest_file /home/
Zxxx0.log

 Connecting to server................... Done.
 Upload log............................. Done.

Success.
```

RCP を使って、ログを装置から RCP サーバにアップロードするには：

```
Zxxx0:admin#upload log_toRCP rcp: tld2@172.18.212.104/home/Zxxx0.log
Command: upload log_toRCP rcp: tld2@172.18.212.104/home/Zxxx0.log

 Connecting to server.................. Done.
 Upload log............................ Done.

Success.

Zxxx0:admin#
```

66.9. show config

● 概要

このコマンドを用いて、設定情報を表示します。コマンドの最後で指定する式により、設定データの出力ストリームをフィルタリングできます。式には最大 3 つのフィルタ評価を含めることができます。フィルタ評価はフィルタタイプ（include、exclude、begin）で始まり、その後に最大 3 つのフィルタ文字列（stp など）が続きます。フィルタ文字列は記号で囲みます。次に各フィルタタイプの意味について説明します。include は、指定したフィルタ文字列を含む行を含みます。exclude は、指定したフィルタ文字列を含む行を除外します。begin は、指定したフィルタ文字列を含む最初の行が、出力の最初の行になります。
同じフィルタタイプに続く複数のフィルタ文字列の関係は OR です。つまり、指定したフィルタ文字列のうち 1 つが一致した場合、1 つの行が一致とみなされます。複数のフィルタ評価を指定した場合、前の評価でフィルタされた出力が、後の評価の入力として用いられます。

● 構文

show config [effective | modified | current_config | boot_up | file <pathname>] {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}

● パラメータ

effective	装置の動作に影響するコマンドのみが表示されます。
modified	デフォルト設定にリセットされたものではないコマンドのみが表示されます。
current_config	現在の設定を指定します。
boot_up	起動設定を指定します。
file	装置ファイルシステムの絶対パス名を指定します。 <pathname> 装置ファイルシステムの絶対パス名を指定します。
include	（オプション）指定したフィルタ文字列を含む行を含めます。
exclude	（オプション）指定したフィルタ文字列を含む行を除外します。

begin	（オプション）指定したフィルタ文字列を含む最初の行が、出力の最初の行になります。 <filter_string 80> 引用符で囲んでフィルタ文字列を指定します。フィルタ文字列自体に引用符を含めることはできません。フィルタ文字列は大文字小文字が区別されます。 <filter_string 80> 引用符で囲んでフィルタ文字列を指定します。 <filter_string 80> 引用符で囲んでフィルタ文字列を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

設定情報を表示するには：

```
Zxxx0:admin#show config current_config
Command: show config current_config

#------------------------------------------------------------------------------
#                   Zxxx0 Gigabit Ethernet Switch
#                              Configuration
#
#                         Firmware: Build 1.0.0.xx
#------------------------------------------------------------------------------


# STACK

config stacking force_master_role state disable

# DEVICE

config temperature threshold high 79
config temperature threshold low 11
config temperature trap state enable
config temperature log state enable

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

66.10. config rcp server

● 概要

このコマンドを用いて、RCP（Remote Copy Protocol）グローバルサーバ情報を設定します。サーバまたはリモートユーザ名が指定されない場合に、このグローバル RCP サーバ設定を使用できます。各システムに 1 つの RCP サーバのみを設定できます。ユーザが CLI コマンドで RCP サーバを指定しておらず、グローバル RCP サーバが設定されていない場合は、スイッチは RCP コマンドの実行中、ユーザにサーバ IP アドレスまたはリモートユーザ名を入力するよう求めます。

● 構文

config rcp server {ipaddress <ipaddr> | username <username>}

● パラメータ

ipaddress	（オプション）グローバル RCP サーバの IP アドレスを指定します。デフォルトではサーバは指定されていません。 <ipaddr> RCP サーバの IP アドレスを指定します。
username	（オプション）RCP サーバのリモートユーザ名を指定します。 <username> RCP サーバのリモートユーザ名を指定します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

ユーザ名 travel の RCP グローバルサーバ情報を設定するには：

```
Zxxx0:admin#config rcp server username travel
Command: config rcp server username travel

Success.

Zxxx0:admin#
```

66.11. config rcp server clear

● 概要

このコマンドを用いて、RCP（Remote Copy Protocol）グローバルサーバ情報を消去します。

● 構文

config rcp server clear [ipaddr | username | both]

● パラメータ

ipaddr	RCP サーバの IP アドレスを消去します。
username	RCP サーバのユーザ名を消去します。
both	RCP サーバの IP アドレスとユーザ名の両方を消去します。

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

RCP グローバルサーバの現在のユーザ名を消去するには：

```
Zxxx0:admin#config rcp server clear username
Command: config rcp server clear username

Success.

Zxxx0:admin#
```

66.12. show rcp server

● 概要

このコマンドを用いて、RCP（Remote Copy Protocol）グローバルサーバ情報を表示します。

● 構文

show rcp server

● パラメータ

なし

● 制限

このコマンドは、管理者レベルのユーザのみ実行できます。

● 実行例

RCP グローバルサーバ情報を表示するには：

```
Zxxx0:admin#show rcp server
Command: show rcp server

RCP Server Address        :
RCP Server Username       : travel

Zxxx0:admin#
```

66.13. ping

● 概要

このコマンドを用いて、リモート IP アドレスに ICMP（Internet Control Message Protocol）エコーメッセージを送信します。次に、リモート IP アドレスがエコーまたはメッセージを返します。これにより、スイッチとリモート装置間の接続を確認します。

● 構文

ping [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99> | source_ip <ipaddr>}

● パラメータ

<ipaddr>	ホストの IP アドレスを指定します。
<domain_name 255>	ホストのドメイン名を指定します。最大文字数は、「.」区切りで各パート 63 文字、最大 255 文字です。
times	（オプション）送信する個々の ICMP エコーメッセージの数を指定します。 <value 1-255> 送信する個々の ICMP エコーメッセージの数を指定します。0 を指定すると、ICMP エコーメッセージが無限に送信されます。最大値は 255 です。デフォルトは 0 です。
timeout	（オプション）リモート装置からの応答を待つ際のタイムアウト期間を指定します。1 ～ 99 秒の値を指定可能です。デフォルトは 1 秒です。 <sec 1-99> リモート装置からの応答を待つ際のタイムアウト期間を指定します。1 ～ 99 秒の値を指定可能です。デフォルトは 1 秒です。
source_ip	ping パケットの送信元 IP アドレスを指定します。指定した場合、その IP アドレスをパケットの送信元 IP アドレスとして、リモートホストに ping が送信されます。 <ipaddr> 使用する送信元 IP アドレスを入力します。

● 制限

なし

● 実行例

ICMP エコーメッセージを「10.51.17.1」に 4 回送信するには：

```
Zxxx0:admin#ping 10.51.17.1 times 4
Command: ping 10.51.17.1 times 4

Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms

Ping Statistics for 10.51.17.1
Packets: Sent =4, Received =4, Lost =0

Zxxx0:admin#
```

66.14. ping6

● 概要

このコマンドを用いて、リモート IPv6 アドレスに ICMP（Internet Control Message Protocol）エコーメッセージを送信します。次に、リモート IPv6 アドレスがエコーまたはメッセージを返します。これにより、スイッチとリモート装置間の接続を確認します。

● 構文

ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99> | source_ip <ipv6addr>}

● パラメータ

<ipv6addr>	ホストの IPv6 アドレスを指定します。
times	（オプション）送信する個々の ICMP エコーメッセージの数を指定します。 <value 1-255> 送信する個々の ICMP エコーメッセージの数を指定します。0 を指定すると、ICMP エコーメッセージが無限に送信されます。最大値は 255 です。デフォルトは 0 です。
size	（オプション）サイズを指定します。 <value 1-6000> サイズを指定します。1 ～ 6000 の値を指定可能です。デフォルトは 100 です。
timeout	（オプション）リモート装置からの応答を待つ際のタイムアウト期間を指定します。 <value 1-99> リモート装置からの応答を待つ際のタイムアウト期間を指定します。1 ～ 99 の値を指定可能です。デフォルトは 1 秒です。
source_ip	ping パケットの送信元 IPv6 アドレスを指定します。指定した場合、その IPv6 アドレスをパケットの送信元 IPv6 アドレスとして、リモートホストに ping が送信されます。 <ipv6addr> 使用する送信元 IPv6 アドレスを入力します。

● 制限

なし

● 実行例

ICMP エコーメッセージを「3FFE:2::D04D:7878:66D:E5BC」に 10 回送信するには：

```
Zxxx0:admin#ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout 10
Command: ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout 10

Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Ping Statistics for 3FFE:2::D04D:7878:66D:E5BC
Packets: Sent =10, Received =10, Lost =0

Zxxx0:admin#
```

66.15. traceroute

● 概要

このコマンドを用いて、スイッチとネットワークの所定のホスト間の経路をトレースします。

● 構文

traceroute [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

● パラメータ

<ipaddr>	宛先エンドステーションの IP アドレスを指定します。
<domain_name 255>	宛先エンドステーションのドメイン名を指定します。
ttl	（オプション）経路トレース要求の有効期間を指定します。 <value 1-60> 経路トレース要求の有効期間を指定します。これは、2 つの装置間のネットワークパスを探索するときに、経路トレースパケットが通過できるルータの最大数です。TTL の範囲は 1 ～ 60 ホップです。初期値は 30 です。
port	（オプション）ポート番号を指定します。 <value 30000-64900> ポート番号を指定します。値の範囲は 30000 ～ 64900 です。デフォルトは 33435 です。

timeout	（オプション）リモート装置からの応答を待つ際のタイムアウト期間を指定します。 <sec 1-65535> リモート装置からの応答を待つ際のタイムアウト期間を指定します。1 ～ 65535 秒の値を指定可能です。デフォルトは 5 秒です。
probe	（オプション）プローブの数を指定します。 <value 1-9> プローブの数を指定します。範囲は 1 ～ 9 です。指定しない場合の初期値は 1 です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチと 10.48.74.121 の間の経路パスをトレースするには：

```
Zxxx0:admin#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

 <10 ms  10.12.73.254
 <10 ms  10.12.73.254
 <10 ms  10.12.73.254
 <10 ms  10.19.68.1
 <10 ms  10.19.68.1
 <10 ms  10.19.68.1
 <10 ms  10.48.74.121
Trace complete.

Zxxx0:admin#
```

66.16. traceroute6

● 概要

このコマンドを用いて、本装置と宛先エンドステーション間の IPv6 経路のパスをトレースします。

● 構文

traceroute6 <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

● パラメータ

<ipv6addr>	宛先エンドステーションの IPv6 アドレスを指定します。
ttl	（オプション）経路トレース要求の有効期間を指定します。 <value 1-60> 経路トレース要求の有効期間を指定します。これは、2 つの装置間のネットワークパスを探索するときに、経路トレースパケットが通過できるルータの最大数です。TTL の範囲は 1 ～ 60 ホップです。初期値は 30 です。

port	（オプション）ポート番号を指定します。 <value 30000-64900> ポート番号を指定します。値の範囲は 30000 ～ 64900 です。デフォルトは 33435 です。
timeout	（オプション）リモート装置からの応答を待つ際のタイムアウト期間を指定します。 <sec 1-65535> リモート装置からの応答を待つ際のタイムアウト期間を指定します。1 ～ 65535 秒の値を指定可能です。デフォルトは 5 秒です。
probe	（オプション）プローブの数を指定します。 <value 1-9> プローブの数を指定します。範囲は 1 ～ 9 です。指定しない場合の初期値は 1 です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

スイッチと 3000::1 の間の IPv6 経路のパスをトレースするには：

```
Zxxx0:admin# traceroute6 3000::1 probe 3
Command: traceroute6 3000::1 probe 3

1   <10 ms.     1345:142::11
2   <10 ms.     2011:14::100
3   <10 ms.     3000::1

Trace complete.
Zxxx0:admin#
```

ポート 40000 を指定して、スイッチと 1210:100::11 の間の IPv6 経路のパスをトレースするには：

```
Zxxx0:admin# traceroute6 1210:100::11 port 40000
Command: traceroute6 1210:100::11 port 40000

1   <10 ms.     3100::25
2   <10 ms.     4130::100
3   <10 ms.     1210:100::11

Trace complete.

Zxxx0:admin#
```

66.17. telnet

● 概要

このコマンドを用いて、Telnet サーバにログインします。

● 構文

telnet [<ipaddr> | <domain_name 255> | <ipv6addr>] {tcp_port <value 1-65535>}

● パラメータ

<ipaddr>（オプション）Telnet サーバの IP アドレスを指定します。
<domain_name 255> Telnet サーバのドメイン名を指定します。
<ipv6addr> Telnet サーバの IPv6 アドレスを指定します。
tcp_port（オプション）Telnet サーバの接続ポート番号を指定します。指定しない場合のデフォルトポートは 23 です。 <value 1-65535> 1 ～ 65535 の値を入力します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

IP アドレスを指定してスイッチに Telnet 接続するには：

```
Zxxx0:admin#telnet 10.1.1.1
Command: telnet 10.1.1.1

Zxxx0 Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 1.0.0.xx

UserName:
```

66.18. enable broadcast_ping_reply

● 概要

enable broadcast_ping_reply コマンドを用いて、ブロードキャスト ping 応答を有効にすると、装置がブロードキャスト ping 要求に応答します。

● 構文

enable broadcast_ping_reply

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ブロードキャスト ping 応答を有効にするには：

```
Zxxx0:admin# enable broadcast_ping_reply
Command: enable broadcast_ping_reply

Success.

Zxxx0:admin#
```

66.19. disable broadcast_ping_reply

● 概要

disable broadcast_ping_reply コマンドを用いて、ブロードキャスト ping 応答を無効にすると、装置がブロードキャスト ping 要求に応答しません。

● 構文

disable broadcast_ping_reply

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ブロードキャスト ping 応答を無効にするには：

```
Zxxx0:admin# disable broadcast_ping_reply
Command: disable broadcast_ping_reply

Success.

Zxxx0:admin#
```

66.20. show broadcast_ping_reply

● 概要

show broadcast_ping_reply コマンドを用いて、ブロードキャスト ping 応答の状態を表示します。

● 構文

show broadcast_ping_reply

● パラメータ

なし

● 制限

なし

● 実行例

ブロードキャスト ping 応答の状態を表示にするには：

```
Zxxx0:admin# show broadcast_ping_reply
Command: show broadcast_ping_reply

Broadcast Ping Reply State:  Enabled

Zxxx0:admin#
```

67. 音声 VLAN コマンド

音声 VLAN（Voice VLAN）とは、ネットワーク上に通常の通信データと IP 電話等の音声データが混在する場合に、音声専用の VLAN を設定し、音声データの帯域を確保するしくみです。ネットワーク上のトラフィックの状態に関わらず、音声データの遅延等を避け、品質を一定に保つことができます。
音声 VLAN を使用するには、接続される IP 電話のベンダコード（OUI）を事前に登録する必要があります。

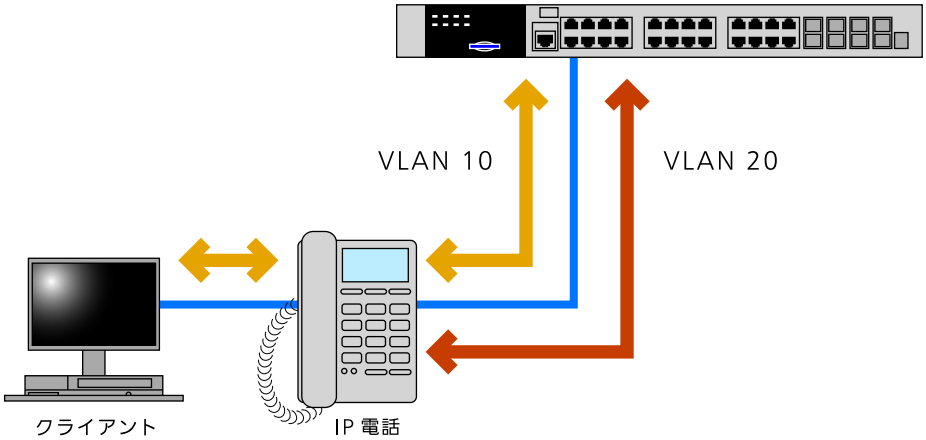


図 67-1　Voice VLAN の概略

enable voice_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]
disable voice_vlan
config voice_vlan priority <int 0-7>
config voice_vlan oui [add | delete] <macaddr> <macmask> {description <desc 32>}
config voice_vlan ports [<portlist> | all] [state [enable | disable] | mode [auto {[tag | untag]} | manual]]
config voice_vlan log state [enable | disable]
config voice_vlan aging_time <min 1-65535>
show voice_vlan
show voice_vlan lldp_med voice_device
show voice_vlan oui
show voice_vlan ports {<portlist>}
show voice_vlan voice_device {ports <portlist>}

67.1. enable voice_vlan

● 概要

このコマンドを用いて、スイッチの音声 VLAN 機能のグローバル設定を有効にします。音声 VLAN のグローバル設定を有効にするには、音声 VLAN が割り当てられている必要があります。また、VLAN が既存のスタティック 802.1Q VLAN の必要があります。音声 VLAN を変更するには、ユーザが音声 VLAN グローバル設定を無効にして、このコマンドを再実行する必要があります。デフォルトでは、音声 VLAN のグローバル設定は無効です。

● 構文

enable voice_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]

● パラメータ

<vlan_name 32>	音声 VLAN の名前を指定します。最大文字数は 32 文字です。名前は既存のスタティック VLAN 名の必要があります。
vlanid	音声 VLAN の VLAN ID を指定します。ID は既存のスタティック VLAN ID の必要があります。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

Voice という名前の音声 VLAN を有効にするには：

```
Zxxx0:admin#enable voice_vlan Voice
Command: enable voice_vlan Voice

Success.

Zxxx0:admin#
```

67.2. disable voice_vlan

● 概要

このコマンドを用いて、スイッチの音声 VLAN のグローバル設定を無効にします。音声 VLAN のグローバル設定を無効にすると、音声 VLAN の割り当てが解除されます。

● 構文

disable voice_vlan

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

音声 VLAN を無効するには：

```
Zxxx0:admin#disable voice_vlan
Command: disable voice_vlan

Success.

Zxxx0:admin#
```

67.3. config voice_vlan priority

● 概要

このコマンドを用いて、音声 VLAN のプライオリティを設定します。音声 VLAN のプライオリティは、音声 VLAN トラフィックに関連付けられたプライオリティで、音声トラフィックの QoS をデータトラフィックと区別します。

● 構文

config voice_vlan priority <int 0-7>

● パラメータ

<int 0-7>	音声VLANのプライオリティを指定します。範囲は0～7です。デフォルトのプライオリティは5です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

音声 VLAN のプライオリティを 6 に設定するには：

```
Zxxx0:admin#config voice_vlan priority 6
Command: config voice_vlan priority 6

Success.

Zxxx0:admin#
```

67.4. config voice_vlan oui

● 概要

このコマンドを用いて、ユーザ定義の音声トラフィックの OUI を設定します。OUI は、音声トラフィックの識別に使用されます。いくつかの事前定義された OUI があります。必要に応じて、さらにユーザ定義の OUI を定義できます。ユーザ定義の OUI は、事前定義された OUI と同一にすることはできません。事前定義された音声トラフィックの OUI を以下に示します。

OUI	ベンダ	簡略名
00:E0:BB	3COM	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

● 構文

config voice_vlan oui [add | delete] <macaddr> <macmask> {description <desc 32>}

● パラメータ

add	音声装置ベンダのユーザ定義 OUI を追加します。
delete	音声装置ベンダのユーザ定義 OUI を削除します。
<macaddr>	ユーザ定義 OUI の MAC アドレスを指定します。
<macmask>	ユーザ定義 OUI の MAC アドレスマスクを指定します。
description	（オプション）ユーザ定義 OUI の説明を指定します。 <desc 32> ユーザ定義 OUI の説明を指定します。最大文字数は 32 文字です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

音声装置のユーザ定義 OUI を追加するには：

```
Zxxx0:admin#config voice_vlan oui add 00-C0-8F-00-00-00 FF-FF-FF-00-00-00
Command: config voice_vlan oui add 00-C0-8F-00-00-00 FF-FF-FF-00-00-00

Success.

Zxxx0:admin#
```

67.5. config voice_vlan ports

● 概要

このコマンドを用いて、ポートまたはポート毎のモードや音声 VLAN 機能の有効または無効を設定します。

● 構文

config voice_vlan ports [<portlist> | all] [state [enable | disable] | mode [auto {[tag | untag]} | manual]]

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを設定します。
state	ポートの音声 VLAN 機能の状態を指定します。デフォルトの状態は無効です。 enable　ポートの音声 VLAN 機能の状態を有効にします。 disable　ポートの音声 VLAN 機能の状態を無効にします。
mode	音声 VLAN モード。デフォルトモードは auto です。 auto　モードが auto の場合、自動学習によりポートが音声 VLAN メンバポートになることができます。受信パケットの MAC アドレスが設定された OUI に一致すると、ポートがダイナミックメンバポートとして学習されます。ダイナミックメンバシップはエージアウトメカニズムにより削除されます。初期値は untag に設定されます。 tag　（オプション）OUI を基に音声デバイスを学習した場合に、自動的にタグメンバとして音声 VLAN に所属します。音声デバイスがタグ無しでパケットを送信する場合は PVID に従って該当する VLAN へ転送されます。 untag（オプション）OUI を基に音声デバイスを学習した場合に、自動的にタグ無しメンバとして音声 VLAN に所属します。LLDP-MED パケットを受信した場合は、VLAN ID、タグフラグ、優先度フラグを確認します。 manual　モードを manual に設定した場合は、802.1Q VLAN 設定コマンドを用いて、音声 VLAN へのポートの追加と削除を手動で行う必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

音声 VLAN ポート 4 ～ 6 を有効に設定するには：

```
Zxxx0:admin#config voice_vlan ports 4-6 state enable
Command: config voice_vlan ports 4-6 state enable

Success.

Zxxx0:admin#
```

音声 VLAN ポート 4 ～ 6 を auto モードに設定するには：

```
Zxxx0:admin#config voice_vlan ports 4-6 mode auto
Command: config voice_vlan ports 4-6 mode auto

Success.

Zxxx0:admin#
```

67.6. config voice_vlan log state

● 概要

このコマンドを用いて、音声 VLAN のログの状態を設定します。

● 構文

config voice_vlan log state [enable | disable]

● パラメータ

enable	音声 VLAN のログの状態を有効にします。
disable	音声 VLAN のログの状態を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

音声 VLAN のログの状態を有効にするには：

```
Zxxx0:admin#config voice_vlan log state enable
Command: config voice_vlan log state enable

Success.

Zxxx0:admin#
```

67.7. config voice_vlan aging_time

● 概要

このコマンドを用いて、音声 VLAN のエージングタイムを設定します。ポートのモードが auto の場合、エージングタイムを用いて音声 VLAN からポートを削除します。最後の音声装置がトラフィック送信を停止し、この音声装置の MAC アドレスがエージアウトしたときに、音声 VLAN のエージングタイマーが始動します。音声 VLAN のエージングタイマーの期限が切れると、ポートが音声 VLAN から削除されます。エージングタイム中に音声トラフィックが再開すると、エージングタイマーがリセットされて停止します。

● 構文

config voice_vlan aging_time <min 1-65535>

● パラメータ

<min 1-65535> エージングタイムを指定します。範囲は 1 ～ 65535 分です。初期値は 720 分です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

音声 VLAN のエージングタイムを 60 分に設定するには：

```
Zxxx0:admin#config voice_vlan aging_time 60
Command: config voice_vlan aging_time 60

Success.

Zxxx0:admin#
```

67.8. show voice_vlan

● 概要

このコマンドを用いて、音声 VLAN のグローバル情報を表示します。

● 構文

show voice_vlan

● パラメータ

なし

● 制限

なし

● 実行例

音声 VLAN の情報を表示するには：

```
Zxxx0:admin#show voice_vlan
Command: show voice_vlan

Voice VLAN State    : Disabled
Voice VLAN          : Unassigned
Priority            : 5
Aging Time          : 720 minutes
Log State           : Enabled

Zxxx0:admin#
```

67.9. show voice_vlan lldp_med voice_device

● 概要

このコマンドを用いて、LLDP-MED により検出された音声装置を表示します。

● 構文

show voice_vlan lldp_med voice_device

● パラメータ

なし

● 制限

なし

● 実行例

LLDP-MED により検出された音声装置を表示するには：

```
Zxxx0:admin# show voice_vlan lldp_med voice_device
Command: show voice_vlan lldp_med voice_device

Index                : 1
Local Port           : 1:1
Chassis ID Subtype   : MAC Address
Chassis ID           : 00-C0-8F-00-00-11
Port ID Subtype      : Network Address
Port ID              : 00-C0-8F-00-00-00
Create Time          : 9/1/2013 08:30
Remain Time          : 120 Seconds

Index                : 2
Local Port           : 1:3
Chassis ID Subtype   : MAC Address
Chassis ID           : 00-C0-8F-00-00-12
Port ID Subtype      : Network Address
Port ID              : 00-C0-8F-00-00-00
Create Time          : 9/1/2013 08:30
Remain Time          : 120 Seconds

Total Entries: 2

Zxxx0:admin#
```

67.10. show voice_vlan oui

● 概要

このコマンドを用いて、音声 VLAN の OUI 情報を表示します。

● 構文

show voice_vlan oui

● パラメータ

なし

● 制限

なし

● 実行例

音声 VLAN の OUI を表示するには：

```
Zxxx0:admin#show voice_vlan oui
Command: show voice_vlan oui

OUI Address         Mask              Description
------------------  ----------------  ---------------
00-01-E3-00-00-00   FF-FF-FF-00-00-00  Siemens
00-03-6B-00-00-00   FF-FF-FF-00-00-00  Cisco
00-09-6E-00-00-00   FF-FF-FF-00-00-00  Avaya
00-0F-E2-00-00-00   FF-FF-FF-00-00-00  Huawei&3COM
00-60-B9-00-00-00   FF-FF-FF-00-00-00  NEC&Phillips
00-D0-1E-00-00-00   FF-FF-FF-00-00-00  Pingtel
00-E0-75-00-00-00   FF-FF-FF-00-00-00  Veritel
00-E0-BB-00-00-00   FF-FF-FF-00-00-00  3COM

Total Entries: 8

Zxxx0:admin#
```

67.11. show voice_vlan ports

● 概要

このコマンドを用いて、ポートの音声 VLAN 情報を表示します。

● 構文

show voice_vlan ports {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

NOTE パラメータを指定しない場合、すべての音声 VLAN ポートの情報が表示されます。

● 制限

なし

● 実行例

音声 VLAN ポート 1 ～ 3 を表示するには：

```
Zxxx0:admin#show voice_vlan ports 1-3
Command: show voice_vlan ports 1-3

Ports  Status     Mode
-----  ---------  --------
 1      Disabled   Auto
 2      Disabled   Auto
 3      Disabled   Auto

Zxxx0:admin#
```

67.12. show voice_vlan voice_device

● 概要

このコマンドを用いて、ポートに接続された音声装置を表示します。Start Time はこのポートで装置が検出された時間を示し、Last Active Time は装置がトラフィックを送信した最遅時間を示します。

● 構文

show voice_vlan voice_device {ports <portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

NOTE パラメータを指定しない場合、すべてのポートの接続された音声装置が表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 2 に接続された音声 VLAN 装置を表示するには：

```
Zxxx0:admin#show voice_vlan voice_device ports 1-2
Command: show voice_vlan voice_device ports 1-2

Ports  Voice Device       Start Time        Last Active Time
-----  -----------------  ----------------  -----------------

Total Entries : 0

Zxxx0:admin#
```

68. VLAN コマンド

VLAN（Virtual LAN）とは、本装置のポートをグループ化して分割し、仮想的な複数の LAN 環境を作成するものです。1 つの VLAN がブロードキャストドメインに対応しますので、ネットワーク上のトラフィックの軽減を図れるとともに、VLAN 間の通信を抑止することでセキュリティを向上できます。
本装置では、ポートベースの VLAN の他、IEEE 802.1Q 準拠のタグ VLAN、MAC ベース VLAN、サブネット VLAN 等の各種 VLAN に対応しています。

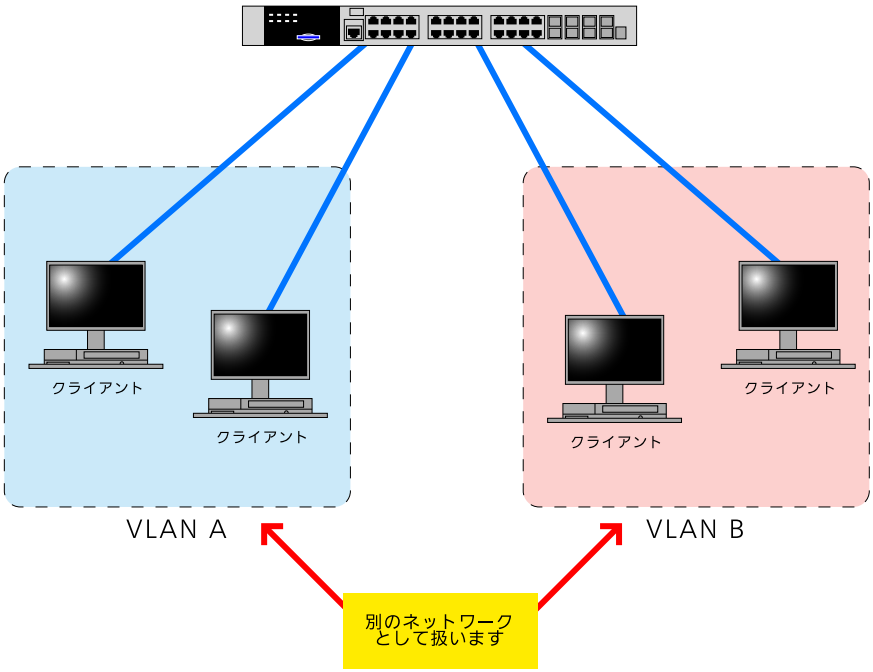


図 68-1　VLAN の概略

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}
create vlan vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}
delete vlan <vlan_name 32>
delete vlan vlanid <vidlist>
config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)
config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] | name <vlan_name 32>}(1)
config port_vlan [<portlist> | all] {gvrp_state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}(1)
show port_vlan {<portlist>}
config gvrp [timer [join | leave | leaveall] <value 100-100000>]
enable gvrp
disable gvrp
show vlan {<vlan_name 32>}
show vlan vlanid <vidlist>
show vlan ports {<portlist>}

show gvrp
config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]
show private_vlan {[<vlan_name 32> | vlanid <vidlist>]}

68.1. create vlan

● 概要

このコマンドを用いて、本装置の VLAN を作成します。VLAN を作成する場合、必ず VLAN ID を指定する必要があります。

● 構文

create vlan <vlan_name 32 > tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}

● パラメータ

<vlan_name 32 >	作成する VLAN の名前を指定します。最大文字数は 32 文字です。
tag	作成する VLAN の VLAN ID を指定します。 <vlanid 2-4094> 範囲は 2 ～ 4094 です。
type	（オプション）作成する VLAN のタイプを指定します。 1q_vlan VLAN を 802.1q VLAN に指定します。 private_vlan VLAN をプライベート VLAN に指定します。
advertisement	（オプション）本装置が GVRP パケットを外部ソースに送信することを認証します。これにより、既存の VLAN に参加することを通知します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

名前「v2」および VLAN ID 2 を指定して、VLAN を作成するには：

```
Zxxx0:admin#create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

Zxxx0:admin#
```

名前「v3」および VLAN ID 3 を指定して、プライベート VLAN を作成するには：

```
Zxxx0:admin#create vlan v3 tag 3 type private_vlan
Command: create vlan v3 tag 3 type private_vlan

Success.

Zxxx0:admin#
```

68.2. create vlan vlanid

● 概要

このコマンドを用いて、本装置の VLAN を作成します。VLAN を作成する場合、必ず VLAN ID を指定する必要があります。

● 構文

create vlan vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}

● パラメータ

<vidlist>	作成する VLAN の VLAN ID を指定します。
type	（オプション）作成する VLAN のタイプを指定します。 1q_vlan VLAN を 802.1q VLAN に指定します。 private_vlan VLAN をプライベート VLAN に指定します。
advertisement	（オプション）本装置が GVRP パケットを外部ソースに送信することを認証します。これにより、既存の VLAN に参加することを通知します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

VLAN ID 2 を指定して、VLAN を作成するには：

```
Zxxx0:admin#create vlan vlanid 2 type 1q_vlan advertisement
Command: create vlan vlanid 2 type 1q_vlan advertisement

Success.

Zxxx0:admin#
```

VLAN ID 3 を指定して、プライベート VLAN を作成するには：

```
Zxxx0:admin#create vlan vlanid 3 type private_vlan
Command: create vlan vlanid 3 type private_vlan

Success.

Zxxx0:admin#
```

68.3. delete vlan

● 概要

このコマンドを用いて、以前に設定された VLAN を削除します。

● 構文

delete vlan <vlan_name 32>

● パラメータ

<vlan_name 32> 削除する VLAN の VLAN 名を指定します。最大文字数は 32 文字です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

VLAN v1 を削除するには：

```
Zxxx0:admin#delete vlan v1
Command: delete vlan v1

Success.

Zxxx0:admin#
```

68.4. delete vlan vlanid

● 概要

このコマンドを用いて、以前に設定された VLAN ID を削除します。

● 構文

delete vlan vlanid <vidlist>

● パラメータ

<vidlist> 削除する VLAN ID の範囲を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

VLAN ID 2 を削除するには：

```
Zxxx0:admin#delete vlan vlanid 2
Command: delete vlan vlanid 2

Success.

Zxxx0:admin#
```

68.5. config vlan

● 概要

このコマンドを用いて、以前に設定された VLAN のポートリストへの、ポートの追加または削除を行います。追加するポートを、タグ付き、タグなし、または禁止として指定できます。

● 構文

config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)

● パラメータ

<vlan_name 32>	ポートを追加または削除する VLAN の名前を指定します。最大文字数は 32 文字です。
add	追加するポートの属性を指定します。 tagged 追加するポートをタグ付きとして指定します。 untagged 追加するポートをタグなしとして指定します。 forbidden ポートが動的に VLAN のメンバとなることを禁止します。また、この VLAN でパケットを転送することはできません。
delete	指定した VLAN を削除します。
<portlist>	VLAN に追加または削除するポートの範囲を指定します。

advertisement
この VLAN の GVRP を送信するかどうかを指定します。送信しない場合、VLAN を動的に結合することはできません。
enable
GVRP を有効にします。
disable
GVRP を無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

VLAN v1 にポート 4 ～ 8 をタグ付きとして追加するには：

```
Zxxx0:admin#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

Zxxx0:admin#
```

VLAN v1 からポート 4 ～ 8 を削除するには：

```
Zxxx0:admin#config vlan v1 delete 4-8
Command: config vlan v1 delete 4-8

Success.

Zxxx0:admin#
```

VLAN のデフォルトアドバタイズを有効にするには：

```
Zxxx0:admin#config vlan default advertisement enable
Command: config vlan default advertisement enable

Success.

Zxxx0:admin#
```

68.6. config vlan vlanid

● 概要

このコマンドを用いて、以前に設定された VLAN のポートリストへの、ポートの追加または削除を行います。追加するポートを、タグ付き、タグなし、または禁止として指定できます。

● 構文

config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] | name <vlan_name 32>}(1)

● パラメータ

<vidlist>	ポートを追加または削除する VLAN の VLAN ID を指定します。
add	追加するポートの属性を指定します。 tagged 追加するポートをタグ付きとして指定します。 untagged 追加するポートをタグなしとして指定します。 forbidden ポートが動的に VLAN のメンバとなることを禁止します。また、この VLAN でパケットを転送することはできません。
delete	指定した VLAN の Vid を削除します。
<portlist>	VLAN に追加または削除するポートの範囲を指定します。
advertisement	この VLAN の GVRP を送信するかどうかを指定します。送信しない場合、VLAN を動的に結合することはできません。 enable GVRP を有効にします。 disable GVRP を無効にします。
name	VLAN の名前を指定します。 <vlan_name 32> 最大文字数は 32 文字です。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

VLAN 1 にポート 4 ～ 8 をタグ付きとして追加するには：

```
Zxxx0:admin#config vlan vlanid 1 add tagged 4-8
Command: config vlan vlanid 1 add tagged 4-8

Success.

Zxxx0:admin#
```

VLAN 1 からポート 4 ～ 8 を削除するには：

```
Zxxx0:admin#config vlan vlanid 1 delete 4-8
Command: config vlan vlanid 1 delete 4-8

Success.

Zxxx0:admin#
```

VLAN のデフォルトアドバタイズを有効にするには：

```
Zxxx0:admin#config vlan vlanid default advertisement enable
Command: config vlan vlanid default advertisement enable

Success.

Zxxx0:admin#
```

68.7. config port_vlan

● 概要

このコマンドを用いて、入口チェックステータスおよび GVRP 情報の送受信を設定します。

● 構文

config port_vlan [<portlist> | all] {gvrp_state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1- 4094>} (1)

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを設定します。
gvrp_state	GVRP を受信したときに、ポートが動的に VLAN のメンバになることを認証するかどうか指定します。 enable：ポートリストで指定したポートに対して GVRP を有効にします。 disable：ポートリストで指定したポートに対して GVRP を無効にします。
ingress_checking	入口チェックを有効にすると、入口ポートが VLAN メンバである場合に、着信パケットが同じ VLAN に割り当てられているかを本装置がチェックします。着信パケットと入口ポートが同じ VLAN にない場合は、パケットが破棄されます。 enable：指定したポートリストの入口チェックを有効にします。 disable：指定したポートリストの入口チェックを無効にします。

acceptable_frame	ポートが受け入れるフレームのタイプを指定します。 tagged_only タグ付きフレームのみを受信します。 admit_all タグ付きとタグなしフレームの両方を受け入れます。
pvid	ポートと関連付けられる PVID（ポート VID）を指定します。 <vlanid 1- 4094> 1 ～ 4094 の VLAN ID を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポートの VLAN を設定するには：

```
Zxxx0:admin#config port_vlan 1-5 gvrp_state enable ingress_checking enable
acceptable_frame tagged_only pvid 2
Command: config port_vlan 1-5 gvrp_state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Success.

Zxxx0:admin#
```

68.8. show port_vlan

● 概要

このコマンドを用いて、本装置のポートリストの GVRP ステータスを表示します。

● 構文

show port_vlan {<portlist>}

● パラメータ

<portlist>（オプション）表示するポートの範囲を指定します。

NOTE このパラメータを指定しない場合、すべてのポートの GVRP 情報が表示されます。

● 制限

なし

● 実行例

ポート 1 ～ 3 の 802.1q ポート設定を表示するには：

```
Zxxx0:admin#show port_vlan 1-3
Command: show port_vlan 1-3

Port     PVID  GVRP      Ingress Checking  Acceptable Frame Type
-------  ----  --------  ----------------  ----------------------------
 1       1     Disabled  Enabled           All Frames
 2       1     Disabled  Enabled           All Frames
 3       1     Disabled  Enabled           All Frames

Total Entries : 3

Zxxx0:admin#
```

68.9. config gvrp

● 概要

このコマンドを用いて、GVRP タイマーの値を設定します。

● 構文

config gvrp [timer [join | leave | leaveall] <value 100-100000>]

● パラメータ

timer	GVRP タイマーを指定します。 join　Join 時間が設定されます。初期値は 200 ミリ秒です。 leave　Leave 時間が設定されます。初期値は 600 ミリ秒です。 leaveall LeaveAll 時間を指定します。初期値は 10000 ミリ秒です。
<value 100-100000>	時間の値を指定します。値の範囲は 100 ～ 100000 ミリ秒です。さらに、Leave 時間には Join 時間の 2 倍よりも大きい値を、LeaveAll 時間には Leave 時間よりも大きい値を設定する必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

Join 時間を 200 ミリ秒に設定するには：

```
Zxxx0:admin#config gvrp timer join 200
Command: config gvrp timer join 200

Success.

Zxxx0:admin#
```

68.10. enable gvrp

● 概要

このコマンドを用いて、GVRP（Generic VLAN Registration Protocol）を有効にします。デフォルトは無効です。

● 構文

enable gvrp

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

GVRP（Generic VLAN Registration Protocol）を有効にするには：

```
Zxxx0:admin#enable gvrp
Command: enable gvrp

Success.

Zxxx0:admin#
```

68.11. disable gvrp

● 概要

このコマンドを用いて、GVRP（Generic VLAN Registration Protocol）を無効にします。

● 構文

disable gvrp

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

GVRP（Generic VLAN Registration Protocol）を無効にするには：

```
Zxxx0:admin#disable gvrp
Command: disable gvrp

Success.

Zxxx0:admin#
```

68.12. show vlan

● 概要

このコマンドを用いて、各 VLAN についてのサマリ情報を表示します。VLAN ID、VLAN 名、各ポートのタグ付き / タグなし / 禁止ステータス、および各ポートのメンバ / 非メンバステータスを表示できます。

● 構文

show vlan {<vlan_name 32>}

● パラメータ

<vlan_name 32>	（オプション）表示する VLAN の名前を指定します。最大文字数は 32 文字です。

● 制限

なし

● 実行例

VLAN 設定を表示するには：

```
Zxxx0:admin#show vlan
Command: show vlan

VLAN Trunk State         : Disabled
VLAN Trunk Member Ports  :

VID              : 1               VLAN Name       : default
VLAN Type        : Static          Advertisement   : Enabled
Member Ports     : 1-28
Static Ports     : 1-28
Current Tagged Ports  :
Current Untagged Ports: 1-28
Static Tagged Ports   :
Static Untagged Ports : 1-28
Forbidden Ports       :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0

Zxxx0:admin#
```

68.13. show vlan vlanid

● 概要

このコマンドを用いて、各 VLAN についてのサマリ情報を表示します。VLAN ID、VLAN 名、各ポートのタグ付き / タグなし / 禁止ステータス、および各ポートのメンバ / 非メンバステータスを表示できます。

● 構文

show vlan vlanid <vidlist>

● パラメータ

<vidlist>	表示する VLAN ID 番号を指定します。

● 制限

なし

● 実行例

VLAN ID 1 の VLAN 設定を表示するには：

```
Zxxx0:admin#show vlan vlanid 1
Command: show vlan vlanid 1

VID              : 1               VLAN Name       : default
VLAN Type        : Static          Advertisement   : Enabled
Member Ports     : 1-28
Static Ports     : 1-28
Current Tagged Ports  :
Current Untagged Ports: 1-28
Static Tagged Ports   :
Static Untagged Ports : 1-28
Forbidden Ports       :

Total Entries : 1

Zxxx0:admin#
```

68.14. show vlan ports

● 概要

このコマンドを用いて、各ポートのタグ付き、タグなし、禁止ステータスについてのサマリ情報を表示します。

● 構文

show vlan ports {<portlist>}

● パラメータ

<portlist>	VLAN を表示するポートの範囲を指定します。ポートリストの範囲の最初と最後をダッシュで区切ります。

● 制限

なし

● 実行例

VLAN のポート設定を表示するには：

```
Zxxx0:admin#show vlan ports 1-2
Command: show vlan ports 1-2

Port      VID    Untagged   Tagged   Dynamic  Forbidden
------     -----  --------   ------   -------  ---------
 1         1       X          -         -       -
 2         1       X          -         -       -

Zxxx0:admin#
```

68.15. show gvrp

● 概要

このコマンドを用いて、本装置の GVRP ステータスを表示します。

● 構文

show gvrp

● パラメータ

なし

● 制限

なし

● 実行例

本装置の GVRP ステータスを表示するには：

```
Zxxx0:admin#show gvrp
Command: show gvrp

Global GVRP   : Disabled
Join Time     : 200 Milliseconds
Leave Time    : 600 Milliseconds
LeaveAll Time : 10000 Milliseconds
NNI BPDU Address: dot1d

Zxxx0:admin#
```

68.16. config private_vlan

● 概要

プライベート VLAN は、プライマリ VLAN、1 つの独立 VLAN、およびいくつかのコミュニティ VLAN から構成されます。プライベート VLAN の ID は、プライマリ VLAN の VLAN ID により表されます。このコマンドを用いて、セカンダリ VLAN をプライマリ VLAN に関連付けるか、関連付けを解除します。プライマリ VLAN は create vlan type private_vlan コマンドを用いて作成します。セカンダリ VLAN は create vlan type 1q_vlan コマンドを用いて作成します。セカンダリ VLAN を複数のプライマリ VLAN に関連付けることはできません。プライマリ VLAN のタグなしメンバポートは、プロミスキャスポートと名付けられます。プライマリ VLAN のタグ付きメンバポートは、トランクポートと名付けられます。プライベート VLAN のプロミスキャスポートが、他のプライベート VLAN のプロミスキャスポートになることはできません。プライマリ VLAN のメンバポートが、同時にセカンダリ VLAN のメンバになることはできません。また、その逆も不可です。セカンダリ VLAN は、タグなしメンバポートのみを持つことができます。セカンダリ VLAN のメンバポートが、同時に他のセカンダリ VLAN のメンバポートになることはできません。VLAN がセカンダリ VLAN としてプライマリ VLAN に関連付けられている場合、プライマリ VLAN のプロミスキャスポートがセカンダリ VLAN のタグなしメンバとして動作し、プライマリ VLAN のトランクポートがセカンダリ VLAN のタグ付きメンバとして動作します。セカンダリ VLAN にアドバタイズを指定することはできません。プライマリ VLAN のみをレイヤ 3 インターフェースとして設定できます。プライベート VLAN のメンバポートに、トラフィックセグメンテーション機能を設定することはできません。

● 構文

config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]

● パラメータ

<vlan_name 32>	プライベート VLAN の名前を指定します。最大文字数は 32 文字です。
vid	プライベート VLAN の VLAN ID を指定します。 <vlanid 1-4094> 1 ～ 4094 の VLAN ID を指定します。
add	独立 VLAN またはコミュニティ VLAN を追加します。 isolated セカンダリ VLAN を独立 VLAN として指定します。 community セカンダリ VLAN をコミュニティ VLAN として指定します。
remove	指定したプライベート VLAN を削除します。
<vlan_name 32>	一定の範囲のセカンダリ VLAN を指定して、プライベート VLAN に追加したり、プライベート VLAN から削除します。最大文字数は 32 文字です。
vlanid	セカンダリ VLAN ID の範囲を指定して、プライベート VLAN に追加したり、プライベート VLAN から削除します。 <vidlist> VLAN ID を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

セカンダリ VLAN をプライベート VLAN p1 に関連付けるには：

```
Zxxx0:admin#config private_vlan p1 add community vlanid 2-5
Command: config private_vlan p1 add community vlanid 2-5

Success.

Zxxx0:admin#
```

68.17. show private_vlan

● 概要

このコマンドを用いて、本装置のプライベート VLAN 情報を表示します。

● 構文

show private_vlan {[<vlan_name 32> | vlanid <vidlist>]}

● パラメータ

<vlan_name 32>	（オプション）プライベート VLAN の名前を指定します。最大文字数は 32 文字です。
vlanid	（オプション）プライベート VLAN の VLAN ID を指定します。 <vidlist> プライベート VLAN の VLAN ID を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

プライベート VLAN 設定を表示するには：

```
Zxxx0:admin#show private_vlan
Command: show private_vlan

Private VLAN 100
------------------
   Promiscuous Ports: 1
   Trunk Ports      : 2
   Isolated Ports   : 3-5           Isolated VLAN : 20
   Community Ports  : 6-8           Community VLAN: 30
   Community Ports  : 9-10          Community VLAN: 40

Private VLAN 200
------------------
   Promiscuous Ports: 11
   Trunk Ports      : 12
   Isolated Ports   : 13-15           Isolated VLAN : 50
   Community Ports  : 16-18           Community VLAN: 60


Zxxx0:admin#
```

69. VLAN Trunking コマンド

複数のスイッチをまたがる VLAN を構築する場合、スイッチ同士を接続するポートでは VLAN Trunking を有効にします。Trunking ポートでは、パケットに VLAN タグが付与されてスイッチからスイッチに転送され、転送先のスイッチでタグの情報に基づく VLAN へと配送されます。

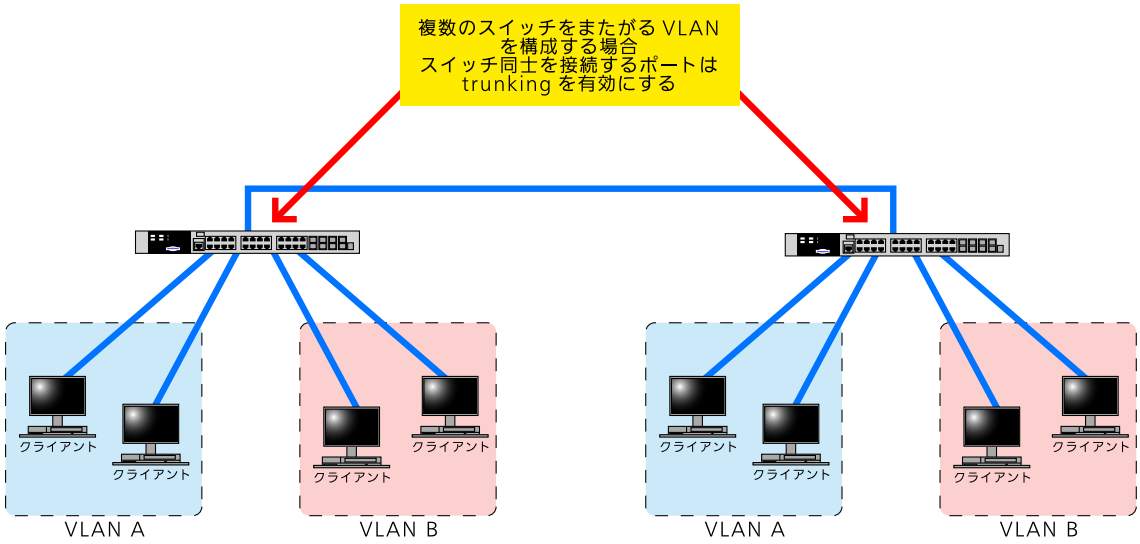


図 69-1　VLAN Trunking の概略

NOTE リンクアグリゲーションを行っているポートで VLAN Trunking の設定を行う場合、リンクアグリゲーションのマスターポートに対して設定を行います。

enable vlan_trunk
disable vlan_trunk
config vlan_trunk ports [<portlist> | all] state [enable | disable]
show vlan_trunk

69.1.　enable vlan_trunk

● 概要

このコマンドを用いて、VLAN Trunking を有効にします。VLAN Trunking 機能を有効にすると、VLAN トランクポートから任意の VID のすべてのタグ付きフレームを送信できるようになります。

● 構文

enable vlan_trunk

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

VLAN Trunking を有効にするには：

```
Zxxx0:admin#enable vlan_trunk
Command: enable vlan_trunk

Success

Zxxx0:admin#
```

69.2. disable vlan_trunk

● 概要

このコマンドを用いて、VLAN Trunking を無効にします。

● 構文

disable vlan_trunk

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

VLAN Trunking を無効にするには：

```
Zxxx0:admin#disable vlan_trunk
Command: disable vlan_trunk

Success.

Zxxx0:admin#
```

69.3. config vlan_trunk ports

● 概要

このコマンドを用いて、ポートを VLAN Trunking ポートとして設定します。デフォルトでは、いずれのポートも VLAN Trunking ポートとして設定されていません。VLAN Trunking ポートと非 VLAN Trunking ポートをリンクアグリゲーションとしてグループ化することはできません。リンクアグリゲーションを行っているポートの VLAN Trunking 設定を変更するには、マスターポートにコマンドを適用する必要があります。マスター以外のリンクアグリゲーションのメンバポートにコマンドを適用すると、コマンドが拒否されます。VLAN 設定が異なるポートを使用して、リンクアグリゲーションを形成することはできません。ただし、VLAN Trunking ポートとして指定されているポートの場合は、リンクアグリゲーションを形成できます。

● 構文

config vlan_trunk ports [<portlist> | all] | state [enable | disable]

● パラメータ

ports	設定するポートを指定します。 <portlist> 設定するポートのリストを指定します。 all すべてのポートが設定されます。
state	ポートを VLAN Trunking ポートまたは非 VLAN Trunking ポートとして指定します。 enable ポートを VLAN Trunking ポートとして指定します。 disable ポートを非 VLAN Trunking ポートとして指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 5 を VLAN Trunking ポートとして設定するには：

```
Zxxx0:admin#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

Zxxx0:admin#
```

69.4. show vlan_trunk

● 概要

このコマンドを用いて、VLAN Trunking 情報を表示します。

● 構文

show vlan_trunk

● パラメータ

なし

● 制限

なし

● 実行例

現在の VLAN Trunking 情報を表示するには：

```
Zxxx0:admin#show vlan_trunk
Command: show vlan_trunk

VLAN Trunk Global Setting
-----------------------------
VLAN Trunk Status  : Disabled
VLAN Trunk Member Ports :

Zxxx0:admin#
```

70. WAC(Web-based Access Control) コマンド

WAC（Web ベースアクセスコントロール、Web ベース認証）とは、PC の Web ブラウザを利用した端末認証方式です。
HTTP または HTTPS プロトコルを使用し、認証サーバとして本製品内のローカルデータベース、または外部の RADIUS サーバを利用し、認証処理を実行します。

enable wac
disable wac
config wac authorization attributes {radius [enable | disable] | local [enable | disable]}(1)
config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}(1)
config wac method [local | radius]
config wac default_redirpath <string 128>
config wac clear_default_redirpath
config wac virtual_ip {<ipaddr>}
config wac switch_http_port <tcp_port_number 1-65535>}
create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
delete wac [user <username 15> | all_users]
config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
show wac
show wac ports {<portlist>}
show wac user
show wac auth_state ports {<portlist>}
clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]
config wac authentication_page element [default | page_title <desc 128> | login_window_title <desc 64> | user_name_title <desc 32> | password_title <desc 32> | logout_window_title <desc 64> | notification_line <value 1-5> <desc 128>]
show wac authenticate_page

70.1. enable wac

● 概要

このコマンドを用いて、WAC 機能を有効にします。

● 構文

enable wac

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

WAC 機能を有効にするには：

```
Zxxx0:admin#enable wac
Command: enable wac

Success.

Zxxx0:admin#
```

70.2. disable wac

● 概要

このコマンドを用いて、WAC 機能を無効にします。

● 構文

disable wac

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

WAC 機能を無効にするには：

```
Zxxx0:admin#disable wac
Command: disable wac

Success.

Zxxx0:admin#
```

70.3. config wac authorization attributes

● 概要

このコマンドを用いて、認証された設定の受け入れについて指定します。WAC の RADIUS の認証が有効な場合、グローバル認証ネットワークが有効なときは、RADIUS サーバにより割り当てられた認証されたデータを受け入れます。WAC のローカルの認証が有効な場合、ローカルデータベースにより割り当てられた認証されたデータを受け入れます。

● 構文

config wac authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

● パラメータ

radius	有効に指定すると、グローバル認証ネットワークが有効なときは、RADIUS サーバにより割り当てられた認証されたデータを受け入れます。デフォルトの状態は有効です。 enable RADIUS サーバにより割り当てられた認証されたデータの受け入れを有効にします。 disable RADIUS サーバにより割り当てられた認証されたデータの受け入れを無効にします。
local	有効に指定すると、グローバル認証ネットワークが有効なときは、ローカルデータベースにより割り当てされた認証されたデータを受け入れます。デフォルトの状態は有効です。 enable ローカルデータベースにより割り当てられた認証されたデータの受け入れを有効にします。 disable ローカルデータベースにより割り当てられた認証されたデータの受け入れを無効にします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

認証された設定の受け入れを指定するには：

```
Zxxx0:admin#config wac authorization attributes local disable
Command: config wac authorization attributes local disable

Success.

Zxxx0:admin#
```

70.4. config wac ports

● 概要

このコマンドを用いて、WAC ポートパラメータを設定します。

● 構文

config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}(1)

● パラメータ

<portlist>	設定するポートの範囲を指定します。
all	すべてのポートを設定します。
state	WAC の状態を有効にするか無効にするか指定します。 enable　WAC の状態を有効にします。 disable　WAC の状態を無効にします。
aging_time	認証されたホストが認証を維持する期間を指定します。初期値は 1440 分です。 infinite　ポートの認証されたホストがエージアウトしません。 <min 1-1440>　1 ～ 1440 分のエージアウト値を指定します。
idle_time	ここで指定した期間にトラフィックがない場合、認証されたホストが非認証に移行します。初期値は infinite です。 infinite　トラフィックがアイドル状態の場合でも、ホストが認証から除外されません。 <min 1-1440>　1 ～ 1440 分のアイドル時間を指定します。
block_time	ホストの認証が失敗したときに、再認証をブロックする期間を指定します。この期間が過ぎると、ホストを再認証できます。初期値は 60 秒です。 <sec 0-300>　0 ～ 300 秒のブロック時間を指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

WAC ポートの状態を設定するには：

```
Zxxx0:admin#config wac ports 1-8 state enable
Command: config wac ports 1-8 state enable

Success.

Zxxx0:admin#
```

WAC ポートのエージングタイムを設定するには：

```
Zxxx0:admin#config wac ports 1-5 aging_time 200
Command: config wac ports 1-5 aging_time 200

Success.

Zxxx0:admin#
```

70.5. config wac method

● 概要

このコマンドを用いて、RADIUS 認証を完了するために WAC で使用する RADIUS プロトコルを指定できます。WAC の他の RADIUS 設定は 802.1X と共通です。このコマンドを用いて RADIUS プロトコルを設定するときは、config radius コマンドにより追加された RADIUS サーバがそのプロトコルをサポートすることを確認する必要があります。

● 構文

config wac method [local | radius]

● パラメータ

local	ローカルデータベースを介して認証を行います。
radius	RADIUS サーバを介して認証を行います。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

WAC の認証方法を設定するには：

```
Zxxx0:admin#config wac method radius
Command: config wac method radius

Success.

Zxxx0:admin#
```

70.6. config wac default_redirpath

● 概要

このコマンドを用いて、WAC のデフォルトリダイレクトパスを設定します。デフォルトリダイレクトパスを設定した場合、認証が成功すると、ユーザがこのパスにリダイレクトされます。この文字列を消去すると、認証が成功したときに、クライアントが別の URL にリダイレクトされません。

● 構文

config wac default_redirpath <string 128>

● パラメータ

<string 128> 認証が成功したときに、クライアントがリダイレクトされる URL を指定します。デフォルトでは、リダイレクトパスが消去されています。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

WAC のデフォルトリダイレクトパスを設定するには：

```
Zxxx0:admin#config wac default_redirpath http://www.manager.com
Command: config wac default_redirpath http://www.manager.com

Success.

Zxxx0:admin#
```

70.7. config wac clear_default_redirpath

● 概要

このコマンドを用いて、WAC のデフォルトリダイレクトパスを消去します。この文字列を消去すると、認証が成功したときに、クライアントが別の URL にリダイレクトされません。

● 構文

config wac clear_default_redirpath

● パラメータ

なし

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

WAC のデフォルトリダイレクトパスを消去するには：

```
Zxxx0:admin#config wac clear_default_redirpath
Success.

Zxxx0:admin#
```

70.8. config wac virtual_ip

● 概要

このコマンドを用いて、WAC の仮想 IP アドレスを設定します。仮想 IP を指定すると、仮想 IP に送信される TCP パケットが応答を受け取ります。仮想 IP が有効な場合、仮想 IP または物理 IPIF の IP アドレスに送信される TCP パケットが応答を受け取ります。仮想 IP を 0.0.0.0 に設定すると、仮想 IP が無効になります。デフォルトでは仮想 IP は 0.0.0.0 です。仮想 IP は ARP 要求または ICMP パケットに応答しません。この機能が正しく動作するように、仮想 IP を既存の IP アドレスに設定しないでください。また、既存のサブネットに配置しないでください。

● 構文

config wac virtual_ip {<ipaddr>}

● パラメータ

<ipaddr>（オプション）仮想 IP の IPv4 アドレスを指定します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

認証されていないホストから認証要求を受け入れるために WAC 仮想 IP アドレスを設定するには：

```
Zxxx0:admin# config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

Zxxx0:admin#
```

70.9. config wac switch_http_port

● 概要

このコマンドを用いて、WAC スイッチの待ち受け先 TCP ポートを設定します。

● 構文

config wac switch_http_port <tcp_port_number 1-65535> }

● パラメータ

<tcp_port_number 1-65535> TCP ポートを指定します。WAC スイッチがこのポートをリッスンし、認証プロセスを完了します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

WAC スイッチの待ち受け先 TCP ポートを設定するには：

```
Zxxx0:admin# config wac switch_http_port 8888
Command: config wac switch_http_port 8888

Success.

Zxxx0:admin#
```

70.10. create wac user

● 概要

このコマンドを用いて、Web ベースアクセスコントロールのアカウントを作成します。このユーザアカウントはログインユーザアカウントとは別個のものです。VLAN が指定されていない場合、認証後にユーザに VLAN は割り当てられません。

● 構文

create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

● パラメータ

<username 15>	Web ベースアクセスコントロールのユーザアカウントを指定します。
vlan	（オプション）認証 VLAN の名前を指定します。 <vlan_name 32> 認証 VLAN の名前を指定します。VLAN 名は 32 文字までです。
vlanid	（オプション）認証 VLAN の ID 番号を指定します。 <vlanid 1-4094> 認証 VLAN の ID 番号を指定します。VLAN ID は 1 ～ 4094 の必要があります。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

WAC アカウントを作成するには：

```
Zxxx0:admin# create wac user abc vlanid 123
Command: create wac user abc vlanid 123
Enter a case-sensitive new password:**
 Enter the new password again for confirmation:**
Success.

Zxxx0:admin#
```

70.11. delete wac

● 概要

このコマンドを用いて、アカウントを削除します。

● 構文

delete wac [user <username 15> | all_users]

● パラメータ

user	Web ベースアクセスコントロールのユーザアカウントを指定します。 <username 15> Web ベースアクセスコントロールのユーザアカウントを指定します。ユーザ名は 15 文字までです。
all_users	現在のすべての WAC ユーザを削除します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

WAC アカウントを削除するには：

```
Zxxx0:admin#delete wac user duhon
Command: delete wac user duhon

Success.

Zxxx0:admin#
```

70.12. config wac user

● 概要

このコマンドを用いて、ユーザと関連付けられた VLAN を変更します。

● 構文

config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

● パラメータ

<username 15>	VID を変更するユーザアカウントの名前を指定します。
vlan	認証 VLAN の名前を指定します。 <vlan_name 32> 認証 VLAN の名前を指定します。VLAN 名は 32 文字までです。
vlanid	認証 VLAN ID を指定します。 <vlanid 1-4094> 認証 VLAN ID を指定します。VLAN ID は 1 ～ 4094 の必要があります。
clear_vlan	指定した VLAN をクリアします。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ユーザの VLAN を設定するには：

```
Zxxx0:admin# config wac user abc vlanid 100
Command: config wac user abc vlanid 100

Enter a old password:**
Enter a case-sensitive new password:**
Enter the new password again for confirmation:**
Success.

Zxxx0:admin#
```

70.13. show wac

● 概要

このコマンドを用いて、WAC のグローバル設定を表示します。

● 構文

show wac

● パラメータ

なし

● 制限

なし

● 実行例

WAC を表示するには：

```
Zxxx0:admin# show wac
Command: show wac

Web-based Access Control
-----------------------------
State                    : Enabled
Method                   : RADIUS
Redirect Path            : http://www.manager.com
Virtual IP               : 0.0.0.0
Switch HTTP Port         : 80 (HTTP)
RADIUS Authorization     : Enabled
Local Authorization      : Enabled

Zxxx0:admin#
```

70.14. show wac ports

● 概要

このコマンドを用いて、WAC ポート情報を表示します。

● 構文

show wac ports {<portlist>}

● パラメータ

<portlist>（オプション）ステータスを表示するメンバポートの範囲を指定します。

● 制限

なし

● 実行例

WAC ポート 1 ～ 3 を表示するには：

```
Zxxx0:admin# show wac ports 1-3
Command: show wac ports 1-3

Port         State          Aging Time      Idle Time      Block Time
                            (min)           (min)          (sec)
-------    --------      ------------     ----------     -----------
1          Disabled      1440             Infinite       60
2          Disabled      1440             Infinite       60
3          Disabled      1440             Infinite       60

Zxxx0:admin#
```

70.15. show wac user

● 概要

このコマンドを用いて、WAC ユーザアカウントを表示します。

● 構文

show wac user

● パラメータ

なし

● 制限

なし

● 実行例

Web 認証ユーザアカウントを表示するには：

```
Zxxx0:admin# show wac user
Command: show wac user

User Name           Password           VID
-----------------  -----------------  ---------
123                ************       1000

Total Entries   : 1

Zxxx0:admin#
```

70.16. show wac auth_state ports

● 概要

このコマンドを用いて、ポートの認証を表示します。

● 構文

show wac auth_state ports {<portlist>}

● パラメータ

<portlist>（オプション）WAC 認証を表示するポートのリストを指定します。

● 制限

なし

● 実行例

ポートの WAC 認証ステータスを表示するには：

```
Zxxx0:admin# show wac auth_state ports
Command: show wac auth_state ports

P:Port-based   Pri:Priority

Port    MAC Address       Original  State       VID Pri Aging Time/ Idle
                           RX VID                    Block Time  Time
------ ------------------- ---- -------------- ---- -- ----------- ----
  31   00-05-5D-F9-16-76    1    Authenticating -    -  27          -

 Total Authenticating Hosts  : 1
 Total Authenticated Hosts   : 0
 Total Blocked Hosts         : 0

Zxxx0:admin#
```

70.17. clear wac auth_state

● 概要

このコマンドを用いて、ポートの認証をクリアします。これにより、ポートが認証されていない状態に戻ります。ポートと関連付けられたすべてのタイマーがリセットされます。

● 構文

clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]

● パラメータ

ports	WAC 状態をクリアするポートのリストを指定します。 <portlist> ポートの範囲を指定します。 all すべてのポートをクリアします。
authenticated	（オプション）ポートのすべての認証されたユーザをクリアします。
authenticating	（オプション）ポートのすべての認証中のユーザをクリアします。
blocked	（オプション）ポートのすべてのブロックされたユーザをクリアします。
macaddr	特定のユーザをクリアします。 <macaddr> MAC アドレスを入力します。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

ポート 1 ～ 5 の WAC 認証をクリアするには：

```
Zxxx0:admin# clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5

Success.

Zxxx0:admin#
```

70.18. config wac authentication_page element

● 概要

このコマンドを用いて、認証ページの要素をカスタマイズします。

● 構文

config wac authentication_page element [default | page_title <desc 128> | login_window_title <desc 64> | user_name_title <desc 32> | password_title <desc 32> | logout_window_title <desc 64> | notification_line <value 1-5> <desc 128>]

● パラメータ

default	ページ要素をデフォルトにリセットします。
page_title	認証ページのタイトルを設定します。 <desc 128> 使用するページタイトルを入力します。この値は 128 文字までです。
login_window_title	認証ページのログインウィンドウのタイトルを設定します。 <desc 64> 使用するログインウィンドウのタイトルを入力します。この値は 64 文字までです。
user_name_title	認証ページのユーザ名のタイトルを設定します。 <desc 32> 使用するユーザ名のタイトルを入力します。この値は 32 文字までです。
password_title	認証ページのパスワードのタイトルを設定します。 <desc 32> 使用するパスワードのタイトルを入力します。この値は 32 文字までです。
logout_window_title	認証ページのログアウトウィンドウのタイトルを設定します。 <desc 64> 使用するログアウトウィンドウのタイトルを入力します。この値は 64 文字までです。
notification_line	認証 Web ページの通知情報を行別に設定します。 <value 1-5> 使用する通知の行番号を入力します。この値は 1 ～ 5 の必要があります。 <desc 128> 使用する通知の行の説明を入力します。この値は 128 文字までです。

● 制限

このコマンドは、管理者、オペレータ、パワーユーザレベルのユーザのみ実行できます。

● 実行例

認証ページの要素をカスタマイズするには：

```
Zxxx0:admin# config wac authentication_page element notification_line 1 Copyright
@ All Rights Reserved
Command: config wac authentication_page element notification_line 1 Copyright @ All
Rights Reserved


Success.


Zxxx0:admin#
```

70.19. show wac authenticate_page

● 概要

このコマンドを用いて、カスタマイズした認証ページの要素を表示します。

● 構文

show wac authenticate_page

● パラメータ

なし

● 制限

なし

● 実行例

認証ページの要素を表示するには：

```
Zxxx0:admin# show wac authenticate_page
Command: show wac authenticate_page

Page Title                              : MANAGER
Login Window Title                      : Authentication Login
User Name Title                         : User Name
Password Title                          : Password
Logout Window Title                     : Logout
Notification                            :
Copyright @ All Rights Reserved
Site: http://support.manager.com

Zxxx0:admin#
```

71.システムログ一覧

システムログへ記録されるログの一覧です。

71.1. MAC ベースアクセスコントロール

番号	Serverity	ログメッセージ／説明
1	Critical	MAC-based Access Control unauthenticated host (MAC: <macaddr>, Port <[unitID:]portNum>, VID: <vid>)
		ホストの認証に失敗したことを表します。
2	Warning	Port < [unitID:]portNum> enters MAC-based Access Control stop learning state.
		ポートの最大認証可能ユーザ数が上限値に達したことを表します。
3	Warning	Port <[unitID:]portNum> recovers from MAC-based Access Control stop learning state.
		ポートの認証可能ユーザ数が上限値を下回ったことを表します。
4	Warning	MAC-based Access Control enters stop learning state.
		装置全体の認証可能ユーザ数が上限値に達したことを表します。
5	Warning	MAC-based Access Control recovers from stop learning state.
		装置全体の認証可能ユーザ数が上限値を下回ったことを表します。
6	Warning	MAC-based Access Control host login successful (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>)
		ホストの認証が成功したことを表します。
7	Informational	MAC-based Access Control host aged out (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>)
		認証済みホストがエージアウトしたことを表します。

71.2. RCP

番号	Serverity	ログメッセージ／説明
1	Informational	[Unit <unitID>,] Firmware upgraded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ファームウェアの更新が成功したことを表します。
2	Warning	[Unit <unitID>,] Firmware upgrade by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ファームウェアの更新が失敗したことを表します。
3	Informational	Firmware uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ファームウェアのアップロードが成功したことを表します。
4	Warning	Firmware upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ファームウェアのアップロードが失敗したことを表します。
5	Informational	Configuration downloaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のダウンロードが成功したことを表します。
6	Warning	Configuration download by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のダウンロードが失敗したことを表します。
7	Informational	Configuration uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のアップロードが成功したことを表します。
8	Warning	Configuration upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のアップロードが失敗したことを表します。
9	Informational	Log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ログのアップロードが成功したことを表します。
10	Warning	Log message upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ログのアップロードが失敗したことを表します。
11	Informational	The downloaded configurations executed by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のダウンロード実行処理が成功したことを表します。

番号	Serverity	ログメッセージ／説明
12	Warning	The downloaded configurations executed by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のダウンロード実行処理が失敗したことを表します。
13	Informational	Attack log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		攻撃ログのアップロードが成功したことを表します。
14	Warning	Attack log message upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		攻撃ログのアップロードが失敗したことを表します。

71.3. TFTP クライアント

番号	Serverity	ログメッセージ／説明
1	Informational	[Unit <unitID>,] Firmware upgraded by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ファームウェアの更新が成功したことを表します。
2	Warning	[Unit <unitID>,] Firmware upgrade by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ファームウェアの更新が失敗したことを表します。
3	Informational	Firmware successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ファームウェアのアップロードが成功したことを表します。
4	Warning	Firmware upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ファームウェアのアップロードが失敗したことを表します。
5	Informational	Configuration successfully downloaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のダウンロードが成功したことを表します。
6	Warning	Configuration download by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のダウンロードが失敗したことを表します。
7	Informational	Configuration successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のアップロードが成功したことを表します。
8	Warning	Configuration upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		設定のアップロードが失敗したことを表します。
9	Informational	Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ログのアップロードが成功したことを表します。
10	Warning	Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		ログのアップロードが失敗したことを表します。
11	Informational	Attack log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		攻撃ログのアップロードが成功したことを表します。

番号	Serverity	ログメッセージ／説明
12	Warning	Attack log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)
		攻撃ログのアップロードが失敗したことを表します。

71.4. DNS リゾルバ

番号	Serverity	ログメッセージ／説明
1	Informational	Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr>
		DNS キャッシュが Static と Dynamic で重複したため、Dynamic キャッシュを削除したことを表します。

71.5. ARP

番号	Serverity	ログメッセージ／説明
1	Warning	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>).
		Gratuitous ARP にて IP アドレスの重複が検出されたことを表します。

71.6. Telnet

番号	Serverity	ログメッセージ／説明
1	Informational	Successful login through Telnet (Username: <username>, IP: <ipaddr>)
		Telnet によるログインが成功したことを表します。
2	Warning	Login failed through Telnet (Username: <username>, IP: <ipaddr>)
		Telnet によるログインが失敗したことを表します。
3	Informational	Logout through Telnet (Username: <username>, IP: <ipaddr>)
		Telnet がログアウトされたことを表します。
4	Informational	Telnet session timed out (Username: <username>, IP: <ipaddr>).
		Telnet セッションがタイムアウトしたことを表します。

71.7. Interface

番号	Serverity	ログメッセージ／説明
1	Informational	Port <[unitID:]portNum> link up, <link state>
		リンクアップが発生したことを表します。
2	Informational	Port <[unitID:]portNum> link down
		リンクダウンが発生したことを表します。

71.8. IEEE802.1X

番号	Serverity	ログメッセージ／説明
1	Warning	802.1X Authentication failure [for <reason>] from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>)
		IEEE802.1X 認証が失敗したことを表します。
2	Informational	802.1X Authentication successful from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>)
		IEEE802.1X 認証が成功したことを表します。

71.9. RADIUS

番号	Serverity	ログメッセージ／説明
1	Informational	RADIUS server <ipaddr> assigned VID :<vlanID> to port <[unitID:]portNum> (account :<username>)
		RADIUS 認証が成功し、RADIUS サーバより対象ポートの VLAN ID（タグなし VLAN ポートメンバー）が割り当てられたことを表します。
2	Informational	RADIUS server <ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <[unitID:]portNum> (account : <username>)
		RADIUS 認証が成功し、RADIUS サーバより対象ポートの入力帯域幅が割り当てられたことを表します。
3	Informational	RADIUS server <ipaddr> assigned egress bandwith :<egressBandwidth> to port <[unitID:]portNum> (account: <username>)
		RADIUS 認証が成功し、RADIUS サーバより対象ポートの出力帯域幅が割り当てられたことを表します。
4	Informational	RADIUS server <ipaddr> assigned 802.1p default priority:<priority> to port <[unitID:]portNum> (account : <username>)
		RADIUS 認証が成功し、RADIUS サーバより対象ポートの IEEE802.1p プライオリティ値が割り当てられたことを表します。
5	Warning	RADIUS server <ipaddr> assigns <username> ACL failure at port <[unitID]portNum> (<string>)
		RADIUS サーバからの ACL 割り当てが失敗したことを表します。

71.10. LLDP-MED

番号	Serverity	ログメッセージ／説明
1	Notice	LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)
		LLDP-MED の構成情報が変更されたことを表します。
2	Notice	Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)
		LLDP-MED のデバイス情報が衝突したことを表します。
3	Notice	Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)
		非対応の LLDP-MED TLV を検出したことを表します。

71.11. Voice VLAN

番号	Serverity	ログメッセージ／説明
1	Informational	New voice device detected (Port <portNum>, MAC <macaddr>)
		対象のポートで新規の端末を検出したことを表します。
2	Informational	Port < portNum > add into Voice VLAN <vid >
		対象のポートが Voice VLAN に追加されたことを表します。
3	Informational	Port < portNum > remove from Voice VLAN <vid >
		対象のポートが Voice VLAN から削除されたことを表します。

71.12. SNMP

番号	Serverity	ログメッセージ／説明
1	Informational	SNMP request received from <ipaddr> with invalid community string.
		不正な Community 名への SNMP リクエストを受信したことを表します。

71.13. ポートセキュリティ

番号	Serverity	ログメッセージ／説明
1	Warning	Port security violation (MAC: < macaddr > on port:: < unitID: portNum >)
		使用可能端末数が最大値に到達したことを表します。

71.14. AAA

番号	Serverity	ログメッセージ／説明
1	Informational	Successful login through <Console | Telnet | Web(SSL) | SSH>(Username: <username>, IP: <ipaddr | ipv6address>).
		ログインに成功したことを表します。
2	Warning	Login failed through <Console | Telnet | Web(SSL)| SSH> (Username: <username>, IP: <ipaddr | ipv6address>).
		ログインに失敗したことを表します。
3	Informational	Logout through <Console | Telnet | Web(SSL)| SSH> (Username: <username>, IP: <ipaddr | ipv6address>).
		ログアウトしたことを表します。
4	Informational	<Console | Telnet | Web(SSL)| SSH> session timed out (Username: <username>, IP: <ipaddr | ipv6address>).
		セッションがタイムアウトしたことを表します。
5	Informational	SSH server is enabled
		SSH が有効になったことを表します。
6	Informational	SSH server is disabled
		SSH が無効になったことを表します。
7	Informational	Authentication Policy is enabled (Module: AAA).
		認証ポリシーが有効になったことを表します。
8	Informational	Authentication Policy is disabled (Module: AAA).
		認証ポリシーが無効になったことを表します。
9	Warning	Login failed through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>).
		認証サーバとの通信タイムアウト、または不適切な設定によりログイン認証に失敗したことを表します。
10	Informational	Successful Enable Admin through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>).
		管理者権限でログイン認証に成功したことを表します。

番号	Serverity	ログメッセージ／説明
11	Warning	Enable Admin failed through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>)
		認証サーバとの通信タイムアウト、または不適切な設定により管理者権限でログイン認証に失敗したことを表します。
12	Warning	Enable Admin failed through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> authenticated by AAA < local | server <ipaddr | ipv6address>> (Username: <username>).
		管理者権限でログイン認証に失敗したことを表します。
13	Informational	Successful login through <Console | Telnet | Web(SSL) | SSH> from < ipaddr | ipv6address > authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>).
		ログイン認証に成功したことを表します。
14	Warning	Login failed through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> authenticated by AAA <local | server <ipaddr | ipv6address>> (Username: <username>).
		ログイン認証に失敗したことを表します。

71.15. WAC

番号	Serverity	ログメッセージ／説明
1	Warning	WAC unauthenticated user (User Name: <string>, IP: <ipaddr >, MAC: <macaddr>, Port: <[unitID:]portNum>)
		認証に失敗したことを表します。
2	Warning	WAC enters stop learning state.
		認証された端末数がポート、または装置に設定された認証可能端末数に到達したことを表します。
3	Warning	WAC recovered from stop learning state.
		認証された端末数がポート、または装置に設定された認証可能端末数より少なくなったことを表します。
4	Informational	WAC authenticated user (Username: <string>, IP: <ipaddr >, MAC: <macaddr>, Port: <[unitID:] portNum>)
		認証に成功したことを表します。

71.16. Traffic Control

番号	Serverity	ログメッセージ／説明
1	Warning	Port <portNum> Broadcast storm is occurring.
		ブロードキャストのストームを検知したことを表します。
2	Informational	Port <portNum> Broadcast storm has cleared.
		ブロードキャストのストームが解消したことを表します。
3	Warning	Port <portNum> Multicast storm is occurring.
		マルチキャストのストームを検知したことを表します。
4	Informational	Port <portNum>Multicast storm has cleared.
		マルチキャストのストームが解消したことを表します。
5	Warning	Port <portNum> is currently shut down due to a packet storm
		ストームによってポートをシャットダウンしたことを表します。

71.17. DHCP Server Screening

番号	Serverity	ログメッセージ／説明
1	Informational	Detected untrusted DHCP server(IP: <ipaddr>, Port <portNum>)
		信頼されていない DHCP サーバを検知したことを表します。

71.18. MSTP Debug Enhancement

番号	Serverity	ログメッセージ／説明
1	Notice	Topology changed [([Instance:<InstanceID>] ,port:<[unitID:] portNum> ,MAC: <macaddr>)]
		トポロジーチェンジが発生したことを表します。
2	Informational	[CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>)
		新しいルートブリッジを検知したことを表します。
3	Informational	Spanning Tree Protocol is enabled
		STP が有効になったことを表します。
4	Informational	Spanning Tree Protocol is disabled
		STP が無効になったことを表します。
5	Notice	New root port selected [([Instance:<InstanceID>], port:<[unitID:] portNum>)]
		新たにルートポートを選定したことを表します。
6	Notice	Spanning Tree port status changed [([Instance:<InstanceID>], port:<[unitID:] portNum>)] <old_status> -> <new_status>
		STP のポート状態が変更になったことを表します。
7	Informational	Spanning Tree port status changed. [([Instance:<InstanceID>], port:<[unitID:] portNum>)] <old_role> -> <new_role>
		STP のポートの役割が変更になったことを表します。
8	Informational	Spanning Tree instance created. Instance:<InstanceID>
		STP のインスタンスが作成されたことを表します。
9	Informational	Spanning Tree instance deleted. Instance:<InstanceID>
		STP のインスタンスが削除されたことを表します。
10	Informational	Spanning Tree version changed. New version:<new_version>
		STP のバージョンが変更されたことを表します。
11	Informational	Spanning Tree MST configuration ID name and revision level changed (name:<name> ,revision level <revision_level>).
		MSTP のリビジョン名、またはリビジョン番号が変更されたことを表します。
12	Informational	Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> delete vlan <startvlanid> [-<endvlanid>]).
		MST インスタンスから VLAN を削除したことを表します。

番号	Serverity	ログメッセージ／説明
13	Informational	Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [-<endvlanid>]).
		MST インスタンスに VLAN を追加したことを表します。

71.19. IP/ パスワード変更

番号	Serverity	ログメッセージ／説明
1	Informational	[Unit <unitID>,] Management IP address was changed by console(Username: <username>,IP:<ipaddr>)
		IP アドレスが変更されたことを表します。
2	Informational	[Unit <unitID>,] Password was changed by console (Username: <username>,IP:<ipaddr>)
		パスワードが変更されたことを表します。

71.20. DDM

番号	Serverity	ログメッセージ／説明
1	Critical	Port <[unitID:]portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] alarm threshold
		DDM のアラームで設定している閾値を上回った、または下回ったことを表します。
2	Warning	Port <[unitID:]portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] warning threshold
		DDM の警告で設定している閾値を上回った、または下回ったことを表します。

71.21. BPDU

番号	Serverity	ログメッセージ／説明
1	Informational	Port<[unitID:]portNum> enter BPDU under attacking state (mode: drop / block / shutdown)
		BPDU アタックが発生したことを表します。
2	Informational	Port <[unitID:]portNum> recover from BPDU under attacking state automatically
		BPDU アタックから自動的に復旧したことを表します。
3	Informational	Port<[unitID:]portNum> recover from BPDU under attacking state manually
		BPDU アタックから手動で復旧させたことを表します。

71.22. ファン

番号	Serverity	ログメッセージ／説明
1	Critical	Unit <unitID>, Right Side Fan <value> failed
		内部ファンが異常または停止状態となったことを表します。
2	Critical	Unit <unitID>, Right Side Fan <value> recovered
		内部ファンが正常状態に復旧したことを表します。

71.23. 温度

番号	Serverity	ログメッセージ／説明
1	Warning	[Uint <unitID>] Temperature sensor: <sensorID> enter alarm state. (current Temperature: <temperature>)
		内部温度が閾値を超えたことを表します。
2	Informational	[Uint <unitID>] Temperature sensor: <sensorID> recovers to normal state. (current Temperature: <temperature>)
		内部温度が閾値未満へ下がったことを表します。
3	Informational	Sensor value <value>
		温度センサーを正しく読み込めたことを表します。
4	Informational	Sensor value fail
		温度センサーが正しく読み込めなかったことを表します。

71.24. IP Source Address

番号	Serverity	ログメッセージ／説明
1	Warning	Dynamic DHCP binding entry conflicts with static ARP (IP:<ipaddr>, MAC:<macaddr>, Port:<[unitID:]portNum>).
		DHCP でバインディングしたアドレスが手動で ARP 登録したアドレスと競合したことを表します。
2	Warning	Dynamic DHCP binding entry conflicts with static IPSG entry (IP:<ipaddr>, MAC:<macaddr>, Port:<[unitID:]portNum>).
		DHCP でバインディングしたアドレスが手動で登録したアドレスと競合したことを表します。
3	Warning	Creating DHCP binding entry failed due to no ACL rule being available (IP:<ipaddr>, MAC:<macaddr>, Port:<[unitID:]portNum>).
		DHCP のバインディングに失敗したことを表します。
4	Warning	Unauthenticated IP-MAC address and discarded by [IPSG | DAI] (IP:< ipaddr >, MAC:< macaddr >, Port:<[unitID:]portNum >).
		認められていない送信元 IP アドレスのパケット、または ARP を破棄したことを表します。

71.25. Spoofing Attack

番号	Serverity	ログメッセージ／説明
1	Critical	Possible spoofing attack from IP: <ipaddr>, MAC:<macaddr>, port:<portNum>
		スイッチと同じ IP アドレスを持った IP パケット、または ARP パケットを受信したことを表します。

71.26. リングプロトコル (RRP)

番号	Serverity	ログメッセージ／説明
1	Notice	Ring topology was recovered to complete.
		リングトポロジが Complete に復帰したことを表します。
2	Warning	Ring topology was failed.
		リングトポロジに異常が発生したことを表します。
3	Informational	FDB was flushed.
		リングトポロジが変化したため FDB を消去したことを表します。
4	Warning	RRP ring status was changed to Link-Up
		リングの状態が Link-Up に変化したことを表します。
5	Notice	RRP ring status was changed to Link-Down
		リングの状態が Link-Down に変化したことを表します。
6	Informational	RRP ring status was changed to Pre-Forwarding
		リングの状態が Pre-Forwarding に変化したことを表します。
7	Informational	Ring Guard was activated on “<domain name>” domain at port < port num>.
		リングガードが作動したことを表します。

71.27. その他

番号	Serverity	ログメッセージ／説明
1	Emergency	[Uint <unitID>] System re-start reason: system fatal error
		CPU の異常により装置が再起動したことを表します。

付録 A. 仕様

○インターフェース

- ツイストペアポート　ポート 1 ～ 20 （RJ45 コネクタ）

伝送方式	IEEE802.3 10BASE-T
	IEEE802.3u 100BASE-TX
	IEEE802.3ab 1000BASE-T

-SFP 拡張ポート　ポート 17 ～ 20(ツイストペアポートと排他利用)

伝送方式	IEEE802.3z 1000BASE-SX/1000BASE-LX
DMI(Diagnostic Monitoring Interface):	
	SFF-8472

- コンソールポート ×1（RJ45 コネクタ）

RS-232C(ITU-TS V.24)

-SD カードスロット ×1

規格	：SD/SDHC
クラス	：2/4/6/10
容量	：128MB ～ 32GB

○システムパフォーマンス

- ストア・アンド・フォワード方式

- スイッチング容量	40Gbps	
- フォワーディング・レート	10BASE-T	14,880pps
	100BASE-TX	148,800pps
	1000BASE-T	1,488,000pps
- バッファメモリ	1.5M バイト	
- フロー制御	バックプレッシャー (半二重時、ポート 17 ～ 20 を除く)	
	IEEE802.3x(全二重時)	
	HOL ブロッキング防止	

○レイヤ 2 機能

- MAC アドレステーブル	16K エントリ / ユニット
- IGMP Snooping	v1/v2/v3、512 グループ、固定 64 グループ （※IGMP Snooping v3 フィルタモード 未サポート）
- MLD Snooping	v1/v2、512 グループ、固定 64 グループ （※MLD Snooping v2 フィルタモード 未サポート）
- スパニングツリー	IEEE802.1D
- ラピッドスパニングツリー	IEEE802.1D
- マルチプルスパニングツリー	IEEE802.1Q(インスタンス：32)
- リンクアグリゲーション	IEEE802.1ad(1 グループ最大 8 ポート /32 グループ)
- ポートモニタリング	1:N(最大 4 グループ、内 送信モニタリング：最大 1 グループ) RSPAN
- リングプロトコル	最大 8 ドメインのリング構成が可能

○他主要搭載機能

- タグ VLAN	IEEE802.1Q、最大 4094 個（デフォルト含む）
- QoS	IEEE802.1p(8 段階)、PQ/WRR
- アクセスコントロール	
- ストームコントロール	
- ポートベース認証	IEEE802.1X、ゲスト VLAN
- MAC ベース認証	ゲスト VLAN
- Web 認証	ゲスト VLAN

○管理方式

- Console、Telnet、SSHv2、SNMP v1/v2c/v3、ZEQUO assist Plus
- PPS(Power to Progress SDN)

○エージェント仕様

- SNMP v1/v2c/v3(RFC1157/1901/2570/2575)
- TELNET(RFC854)
- SSH v2(RFC4250,4251,4252,4253,4254)
- TFTP(RFC783)
- BOOTP(RFC951)
- SNTP(RFC1769)
- PPSP(オリジナルプロトコル)

○サポート MIB

- RFC1213-MIB(MIB II)(RFC1213)
- BRIDGE-MIB(RFC4188)
- SNMPv2-MIB(RFC1907)
- RMON-MIB(RFC1757,2819)[グループ 1,2,3,9]
- RMON2-MIB(RFC2021)
- EtherLike-MIB(RFC1643,2358,2665)
- MAU-MIB(RFC4836)
- P-BRIDGE-MIB(RFC4363)
- IF-MIB(RFC2233,2863)
- RADIUS-AUTH-CLIENT-MIB(RFC2618)
- RADIUS-ACC-CLIENT-MIB(RFC2620)
- DISMAN-PING-MIB(RFC2925)
- DISMAN-TRACEROUTE-MIB(RFC2925)
- IPV6-MIB(RFC2465)

○電源仕様

- 電源	AC100V　50/60Hz　2.0A
- 入力電圧範囲	AC90 ～ 132V
- 消費電力	定常時最大：20.2W、最小：10.4W

○環境仕様

- 動作環境温度	0 ～ 50 ℃
- 動作環境湿度	20 ～ 80%RH（結露なきこと）
- 保管環境温度	-20 ～ 70 ℃
- 保管環境湿度	10 ～ 90%RH（結露なきこと）

○外形仕様

- 寸法	440mm(W)×312mm(D)×44mm(H) （突起部は除く）
- 質量｛重量｝	3,750g

○適合規制

- 電波放射	一般財団法人 VCCI 協会 クラス A 情報技術装置 (VCCI Council Class A)

付録 B.　ZEQUO assist Plus によるコンソール ポート設定手順

付属 CD-ROM に同梱されている弊社スイッチングハブのサポートアプリケーション「ZEQUO assist Plus」に搭載のターミナルエミュレータを利用することにより、コンソールポートや Telnet、SSH 経由での設定画面アクセスが可能です。
本項ではコンソールポートを使用する場合の手順をご紹介します。
（※ZEQUO assist Plus の詳細な説明・操作手順については、ZEQUO assist Plus に付属の取扱説明書を参照してください）

①付属 CD-ROM 内の書庫ファイル「ZEQUOASSISTPLUS_vxxxx.zip」を PC の任意の場所に展開します。

②「ZEQUOASSIST.exe」を起動し、アプリケーションの起動用ユーザ名・パスワードを登録します。（2 回目以降の起動時の認証情報として利用します）

③「 ZEQUO assist ランチャー」ウィンドウが現われますので、ご利用のスイッチに合わせて「 ZEQUO シリーズ」または「MNO/XG シリーズ」をクリックします。

④ZEQUO assist のメインウィンドウが現れますので、画面左の「ターミナルエミュレータ」ボタンをクリックします。

⑤「ターミナルエミュレータ 接続方式」で「コンソール」を選択し、利用する COM ポートの番号を選択します。

⑥画面下部の「ターミナルエミュレータ起動」ボタンをクリックします。

⑦ 設定画面が表示されます。

付録 C.　IP アドレス簡単設定機能について

IP アドレス簡単設定機能を使用する際の注意点について説明します。

【動作確認ソフトウェア】
・パナソニック LS ネットワークス株式会社製『ZEQUO asssit Plus』Ver.1.2.7.1
・パナソニック株式会社製『Panasonic IP 簡単設定ソフトウェア』Ver.4.24
・パナソニックシステムネットワークス株式会社製『かんたん設定』Ver.3.14

【設定可能項目】
・IP アドレス、サブネットマスク、デフォルトゲートウェイ
・ホスト名（※ ソフトウェアによっては ” カメラ名 ” と表示されます）

【制限事項】
・セキュリティ確保のため、電源投入時より 20 分間のみ設定変更が可能です。ただし、IP アドレス、サブネットマスク、デフォルトゲートウェイ、ホスト名が工場出荷時状態の間は、時間の制限に関わらず設定が可能です。
　また、制限時間を過ぎている場合であっても、ソフトウェアの機器探索機能による一覧表示での設定確認は可能です。

・ZEQUO assist Plus 以外のソフトウェアに搭載されている『自動設定』には対応していません。

※ZEQUO assist Plus 以外のソフトウェアに関する詳細は、各メーカ様へご確認ください。

付録 D. Private MIB Trap 一覧

この装置がサポートしている独自の Trap は以下のとおりです。

Trap 名称	OID	説明
swL2macNotification	1.3.6.1.4.1.396.5.5.3.1.1	MAC Notification 機能による新規学習 MAC アドレスの通知
swMacBasedAccess-ControlLoggedSuc-cess	1.3.6.1.4.1.396.5.5.3.2.1	MAC-based Access Control 機能による認証成功
swMacBasedAccess-ControlLoggedFail	1.3.6.1.4.1.396.5.5.3.2.2	MAC-based Access Control 機能による認証失敗
swMacBasedAccess-ControlAgesOut	1.3.6.1.4.1.396.5.5.3.2.3	MAC-based Access Control 機能の認証ホストのエージアウト
agentGratuitou-sARPTrap	1.3.6.1.4.1.396.5.5.3.6.1	Gratuitous ARP にて IP アドレス重複を検出
swL2PortSecurityViola tionTrap	1.3.6.1.4.1.396.5.5.3.3.1	Port Security 機能にて不正な MAC アドレスを検出
swBpduProtectionUn derAttackingTrap	1.3.6.1.4.1.396.5.5.3.4.1	BPDU Attack 機能にてポートの Drop/Block/Shutdown が発生
swBpduProtectionRec overyTrap	1.3.6.1.4.1.396.5.5.3.4.2	BPDU Attack 機能でのポート制御が復帰
swFilterDetectedTrap	1.3.6.1.4.1.396.5.5.3.7.1	DHCP Server Screening 機能にて不正な DHCP サーバを検出
swPktStormOccurred	1.3.6.1.4.1.396.5.5.3.5.1	Traffic Control 機能にてパケットストームを検出、ポートを遮断
swPktStormCleared	1.3.6.1.4.1.396.5.5.3.5.2	パケットストームが解消
swPktStormDisablePo rt	1.3.6.1.4.1.396.5.5.3.5.3	Traffic Control 機能にてポートを無効化
swDdmAlarmTrap	1.3.6.1.4.1.396.5.5.1.4.1	DDM のパラメータが Alarm 値を超過・復帰
swDdmWarningTrap	1.3.6.1.4.1.396.5.5.1.4.2	DDM のパラメータが Warning 値を超過・復帰
mnoFanFailure	1.3.6.1.4.1.396.5.5.1.1	Fan 異常
mnoTemperatureRis-ingAlarm	1.3.6.1.4.1.396.5.5.1.2.1	内部温度が閾値を超過
mnoTemperatureFall-ingAlarm	1.3.6.1.4.1.396.5.5.1.2.2	内部温度が閾値超過から復帰

故障かな？と思ったら

故障かなと思った場合には、まず下記の項目に従って確認してください。

◆ LED

○ POWER(電源)LED が点灯しない場合

●電源プラグが外れていませんか？
確実に接続されているか確認してください。

●動作環境温度を 0 ～ 50 ℃の場所で使用していますか？
動作環境温度の範囲内でお使いください。
※ 動作環境温度の範囲外でご使用の場合、保護装置が働き電源の供給を停止します。
動作環境温度範囲は 0 ～ 50 ℃です。

○ SD CARD(SD カード) LED が点灯しない場合

● SD カードが外れていませんか？
確実に挿入されているか確認してください。

◆通信ができない場合

●ケーブルを該当するポートに正しく接続していますか？

●ケーブル類は適切なものを使用していますか？

●該当するポートに接続している端末は 10BASE-T、100BASE-TX、もしくは 1000BASE-T 対応ですか？

●リンクアップしていますか？
Power Saving Mode（省電力モード）や EEE（IEEE802.3az、省電力型イーサネット）有効な場合、接続機器によってはリンクしない場合があります。以下のとおり設定を変更してください。

1. Power Saving Mode の設定を「disable」に変更
2. EEE（IEEE802.3az）の設定を「disable」に変更

●装置の通信速度、通信モードが正しく設定されていますか？
通信モードを示す適切な信号が得られない場合は、半二重モードで動作します。
オート・ネゴシエーションの設定を再確認してください。

●この装置を接続しているネットワークの使用率が高すぎませんか？
ネットワークからこの装置を分離してみてください。

●通信モードが固定の機器をポート 17 ～ 20 に接続していませんか？
この装置のポート 17 ～ 20 と対向ポートの設定をオートネゴシエーション、もしくは全二重モードの同一通信速度に変更してください。

●通信モードが半二重モードの機器をポート 17 ～ 20 に接続していませんか？
ポート 17 ～ 20 は半二重モードの機器とはリンクアップしません。
ポート 1 ～ 16 に接続を変更してください。

保証とアフターサービスについて

1. 保証書について

保証書は本装置に付属の取扱説明書（紙面）についています。必ず保証書の『お買い上げ日、販売店（会社名）』などの記入をお確かめの上、販売店から受け取っていただき、内容を良くお読みのうえ大切に保管してください。保証期間はお買い上げの日より 1 年間です。

2. 修理を依頼されるとき

『故障かな？と思われたら』に従って確認をしていただき、なお異常がある場合は次ページの『便利メモ』をご活用のうえ、下記の内容とともにお買上げの販売店へご依頼ください。

◆品名　　◆品番

◆製品シリアル番号（製品に貼付されている 11 桁の英数字）

◆ファームウェアバージョン（個装箱に貼付されている "Ver." 以下の番号）

◆異常の状況（できるだけ具体的にお伝えください）

●保証期間中は：

保証書の規定に従い修理をさせていただきます。

お買い上げの販売店まで製品に保証書を添えてご持参ください。

●保証期間が過ぎているときは：

診断して修理できる場合は、ご要望により有料で修理させていただきます。

お買い上げの販売店にご相談ください。

3. アフターサービス・商品に関するお問い合わせ

お買い上げの販売店もしくは下記の連絡先にお問い合わせください。

パナソニックLSネットワークス株式会社

TEL 03-6402-5301 / FAX 03-6402-5304

4. ご購入後の技術的なお問い合わせ

■ご購入後の技術的な問い合わせはフリーダイヤルをご利用ください。
IP 電話 (050 番号) からはご利用いただけません。お近くの弊社営業部にお問い合わせください。

フリーダイヤル 0120-312-712 受付 9:30～12:00／13:00～17:00
(土・日・祝日、および弊社休日を除く)

弊社ホームページによくあるご質問 (FAQ) および設定例を掲載しておりますのでご活用ください。
ご不明点が解決できない場合は、ホームページのサポート内容をご確認の上、お問合せください。
URL:http://panasonic.co.jp/ls/plsnw/support/index.html

なお、ご購入前のお問い合わせは、弊社各営業部にお願いいたします。
URL:http://panasonic.co.jp/ls/plsnw/resume/guideline/index.html

便利メモ（おぼえのため、記入されると便利です）

<table>
<tr><td rowspan="2">お買い上げ日</td><td colspan="6" rowspan="2">年　　月　　日</td><td>品名</td><td colspan="4">ZEQUO 2210</td></tr>
<tr><td>品番</td><td colspan="4">PN26161</td></tr>
<tr><td rowspan="2">バージョン（※）</td><td colspan="3">Boot PROM</td><td colspan="8"></td></tr>
<tr><td colspan="3">Firmware</td><td colspan="8"></td></tr>
<tr><td rowspan="2">シリアル番号</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="11">（製品に貼付されている 11 桁の英数字）</td></tr>
<tr><td>販売店名
または
販売会社名</td><td colspan="11">電話（　　）　　－</td></tr>
<tr><td>お客様
ご相談窓口</td><td colspan="11">電話（　　）　　－</td></tr>
</table>

（※ 確認画面は 5.8 項を参照）

パナソニックLSネットワークス株式会社

〒 105-0021　東京都港区東新橋 2 丁目 12 番 7 号　住友東新橋ビル 2 号館 4 階
TEL 03-6402-5301 / FAX 03-6402-5304
URL: http://panasonic.co.jp/ls/plsnw/

P1014-11049