TD61-7386

ApresiaLightGM152GT

Ver. 1.03

CLI マニュアル

APRESIA Systems 株式会社

制 定 ・ 改 訂 来 歴 表

No.	年　　月　　日	内　　容
-	2021 年 1 月 20 日	Ver.1.02 CLI マニュアル(TD61-6745)から新規作成 ＜内容変更＞ ・ 3.3.6 show switch の表示結果を変更 ・ 3.37.2 config authentication server failover でオプション追加 ・ 3.37.3 show authentication で表示結果を変更 ・ 3.39.1 enable ssl でオプション追加 ・ 3.39.2 disable ssl でオプション追加 ・ 3.39.5 show ssl で表示結果を変更

はじめに

本書には、スイッチングハブのコマンド説明および操作方法を記述しています。それ以外のハードウェアに関する説明および操作方法については、各適用機種のハードウェアマニュアルを参照ください。

本書適用の機種一覧表

シリーズ名	品名	型式
ApresiaLightGM152GT	ApresiaLightGM152GT	APLGM152GT

この注意シンボルは、そこに記述されている事項が人身の安全と直接関係しない注意書きに関するものであることを示し、注目させる為に用います。

注意事項

本ファームウェアは、ApresiaLightGM152GT 専用に作成されたものです。それ以外の機器(ApresiaLightGM シリーズおよび ApresiaLightFM シリーズ製品全般など)にインストールすることはできません。
また、ApresiaLightGM152GT には、本ファームウェアと旧バージョンを除くソフトウェア (例えば ApresiaLightGM シリーズ用、もしくは ApresiaLightFM シリーズ用のファームウェアなど)をインストールすることはできません。

使用条件と免責事項

ユーザーは、本製品を使用することにより、本ハードウェア内部で動作する全てのソフトウェア(以下、本ソフトウェアといいます)に関して、以下の諸条件に同意したものといたします。

本ソフトウェアの使用に起因する、または本ソフトウェアの使用不能によって生じたいかなる直接的または間接的な損失・損害等(人の生命・身体に対する被害、事業の中断、事業情報の損失またはその他の金銭的損害を含み、これに限定されない)については、その責を負わないものとします。

(1) 本ソフトウェアを逆コンパイル、リバースエンジニアリング、逆アセンブルすることはできません。

(2) 本ソフトウェアを本ハードウェアから分離すること、または本ハードウェアに組み込まれた状態以外で本ソフトウェアを使用すること、または本ハードウェアでの使用を目的とせず本ソフトウェアを移動することはできません。

目次

1. パラメーター設定手順

パラメーターの設定は、設定端末の準備、設定端末の接続、パラメーターの設定手順で行います。
コマンドライン方式によるコマンド詳細については 3 章を参照してください。
なお、WEB ベース GUI 方式については別紙(SW マニュアル)を参照してください。

1.1 出荷時の設定値一覧

全般的な機能に関する出荷時のデフォルト設定値を表 1-1に示します。
設定変更した場合には、「save」コマンドの実行により設定が保存されます。
出荷時の設定に戻す場合には、「reset system」コマンドの実行により設定が初期化されます。

表 1-1 デフォルト設定一覧

設定項目	内　容	出荷時の設定値
Account Admin	管理者アカウント(パスワード)	“adpro”（なし）
Account User	ユーザーアカウント(パスワード)	なし(なし)
Command Prompt	コマンドプロンプト	管理者アカウント“#” 一般アカウント　“>”
Auto Logout	自動ログアウトの時間	10(分)
CLI Paging	画面スクロールの一時停止	Enabled(動作)
Terminal Line	画面表示の行数	24(行)
TELNET	TELNET による装置接続	Enabled(TCP 23)
WEB	WEB ベース GUI による装置接続	Enabled(TCP 80)
IPif DHCP Mode	DHCP による管理 IP アドレス割り当て	Disabled(非動作)
IPif IPaddress※1	管理 IPv4 アドレス	0.0.0.0/0※1
IProute Default	IPv4 デフォルトゲートウェイ	設定なし
IPv6 Address	管理 IPv6 アドレス	設定なし
IPv6 Neighbor	IPv6 スタティックネイバー	設定なし
ARP Aging Time	ARP テーブル学習機能によるエージング時間	20(分)
FDB Aging Time	MAC テーブル学習機能によるエージング時間	300(秒)
VLAN State	VLAN の動作状態	Enabled(動作)
VLAN Name	VLAN 名	default(vid=1)
Port State	ポートの状態(活性/非活性)	活性(Enabled)
Port Speed Duplex	通信速度/通信方式の自動認識	Auto-Nego(自動認識)
Port MDIX	MDI/MDI-X の自動認識	Auto-MDIX(自動認識)
Port Flow Control	フロー制御の動作状態	Disabled(非動作)
Jumbo Frame	Jumbo Frame 機能	Enabled(動作)
Link Aggregation Status	リンクアグリゲーション機能の動作状態	Disabled(非動作)
Link Aggregation Type	リンクアグリゲーションのタイプ(Static/Lacp)	Static
Link Aggregation Algorithm	リンクアグリゲーションのアルゴリズム	MAC source

設定項目	内　容	出荷時の設定値
Mirror	ポートミラーリング機能の動作状態	Disabled(非動作)
Syslog	ログ転送機能の動作状態	Disabled(非動作)
Syslog Host	ログ転送先 IP アドレス	設定なし
SNMP Status※2	SNMP の動作状態	Enabled(動作)
SNMP Community	コミュニティー名	public(Read_Only) private(Read_Write)
SNMP Traps	トラップ送信機能の動作状態	Enabled(動作)
SNMP Host	トラップ送信先 IP アドレス	設定なし
SNMP System Contact	システムコンタクト	設定なし
SNMP System Location	システムロケーション	設定なし
SNMP System Name	システムネーム	設定なし
RMON	リモートモニタリング機能の動作状態	Disabled(非動作)
SSH	SSH 機能	Disabled(非動作)
SSL	SSL 機能の動作状態	Disabled(非動作)
LLDP	LLDP 機能の動作状態	Disabled(非動作)
GVRP	GVRP 機能の動作状態	Disabled(非動作)
IGMP Snooping	IGMP Snooping 機能	Disabled(非動作)
MLD Snooping	MLD Snooping 機能	Disabled(非動作)
Traffic Control Status	パケットストーム制御機能の動作状態	Disabled(非動作)
Traffic Control Action	ストーム検知の動作モード(Drop/Shutdown)	Drop(パケット破棄)
Traffic Control Threshold	ストーム制御の閾値	64 Drop モード(kbps) Shutdown モード(pps)
Traffic Control Interval	ストーム監視の間隔時間	5(秒)
Traffic Control Countdown	ストーム制御時のポート閉塞までの時間	0(秒)閉塞なし
Traffic Control Recover	ストーム制御時のポート開放までの時間	300(秒)
LoopDetect Status	ループ防止機能の動作状態	Disabled(非動作)
LoopDetect Method	ループ検知時の動作モード(Drop/Shutdown)	Shutdown(ポート閉塞)
LoopDetect Interval	ループ監視の間隔時間	10(秒)
LoopDetect Recover Timer	ループ制御時にポート開放するまでの時間	60(秒)
BPDU Guard Status	BPDU ガード機能の動作状態	Disabled(非動作)
BPDU Guard Recovery Time	BPDU ガード制御時にポート開放までの時間	60(秒)
STP Status	スパニングツリープロトコル機能の動作状態	Disabled(非動作)
STP Version	動作バージョン(MSTP/RSTP/STP)	RSTP
STP Max Age	BPDU の最大経過時間	20(秒)
STP Hello Time	ハロー間隔時間	2(秒)
STP Forward Delay	フォワードディレイ時間	15(秒)

設定項目	内　容	出荷時の設定値
STP Max Hop	最大ホップカウント	20
SMTP Status	SMTP クライアント機能の動作状態	Disabled(非動作)
SMTP Server	SMTP サーバーIP アドレス	設定なし(0.0.0.0)
SNTP Status	SNTP クライアント機能の動作状態	Disabled
SNTP Server	SNTP サーバーIP アドレス	設定なし(0.0.0.0)
SNTP Poll Interval	SNTP サーバーへの問い合わせ間隔時間	720(秒)
MAC Auth State	MAC 認証機能	Disabled(非動作)
MAC Auth Method	MAC 認証方法(Local/Radius)	Local
MAC Auth Failover	RADIUS 未応答時の Local/強制認証切り替え	Disabled(非動作)
MAC Auth Format	MAC 認証時のアドレスフォーマット	Case:uppercase Delimiter:none
MAC Auth Password Type	MAC 認証時のパスワードタイプ	Manual_string
WEB Auth State	WEB 認証機能	Disabled(非動作)
WEB Auth Method	WEB 認証方法(Local/Radius)	Local
WEB Auth Virtual IP	WEB 認証用の仮想 IP アドレス	設定なし(0.0.0.0)
WEB Auth Redirect	WEB 認証リダイレクト機能	Enabled(動作)
WEB Auth Session Timeout	WEB 認証のセッションタイムアウト時間	120(秒)
WEB Auth Failover	RADIUS 未応答時の Local 認証/強制認証切り替え	Disabled(非動作)
802.1X Auth State	802.1X 認証機能	Disabled(非動作)
802.1X Auth Protocol	802.1X 認証方法(Local/Radius_EAP)	Radius_EAP
802.1X Auth Failover	RADIUS 未応答時の Local 認証/強制認証切り替え	Disabled(非動作)
RADIUS Server	RADIUS サーバーIP アドレス	設定なし
RADIUS Timeout	RADIUS サーバー応答のタイムアウト時間	5(秒)
RADIUS Retransmit	RADIUS サーバー未応答の再送回数	2(回)
QinQ Status	拡張タグ VLAN 機能の動作状態	Disabled(非動作)
QinQ Role	ポートタイプの分類(NNI/UNI)	NNI
QinQ VLAN Translation	VLAN 変換機能の動作状態	Disabled(非動作)
Bandwidth Control	帯域幅制御	制御なし(no_limit)
COS Mapping	COS マッピング(Eth_Priority/IP_Priority)	Eth_Priority(802.1p)
802.1p User Priority	Tag User Priority 値のハードウェアキュー	802.1p 0 (Class 2) 802.1p 1 (Class 0) 802.1p 2 (Class 1) 802.1p 3 (Class 3) 802.1p 4 (Class 4) 802.1p 5 (Class 5) 802.1p 6 (Class 6) 802.1p 7 (Class 7)
802.1p Default Priority	Tag なし 802.1p 優先値	802.1p 0 Priority
IP Priority TOS Value	TOS 値に関連付けのハードウェアキュー	TOS 0-7 (Class 0)

設定項目	内　容	出荷時の設定値
IP Priority DSCP Value	DSCP 値に関連付けのハードウェアキュー	DSCP 0-63 (Class 0)
ACL	アクセス制御リストの設定	設定なし
Command Logging State	コマンドログ機能の動作状態	Enabled(動作)
Green Mode State	省電力機能の動作状態	Disabled(非動作)
Temperature notify	装置内部温度通知機能	高温側：55℃ 低温側：-5℃
EEE state	Energy Efficient Ethernet 機能の動作状態	Disabled(非動作)

※1 IPアドレスのデフォルト設定は0.0.0.0/0ですが、Ver.1.02から実装するIPアドレス自動設定機能によって、装置起動時にMACアドレスに応じたIPアドレスが割り振られます。割り当てられるIPアドレスは、1.3「初期IPアドレス設定」をご確認ください。

※2 SNMP機能はデフォルト設定状態において、SNMPコミュニティー名が一致する全てのSNMPマネージャーからのアクセスが許可されます。SNMP機能を使用しない場合、delete snmp community、delete snmp user 設定でコミュニティー名、ユーザー名を削除する必要があります。

1.2 システム最大値一覧

全般的な機能に関するシステム最大値を表 1-2に示します。

表 1-2 システム最大値一覧

項　目	内　容	最大値
IPif IPaddress	IP アドレス数	1（装置）
IProute	IP ルートテーブル数	16（Default ルート含む）
FDB(MAC Address Table)	MAC アドレステーブル登録数	16383（スタティック含む）
	unicast スタティックエントリー数	256
	multicast スタティックエントリー数	128
ARP	ARP テーブル登録数	508（スタティック含む）
	スタティックエントリー数	255
VLAN	VLAN 数	4094
Q-in-Q	VLAN トランスレーションルール数	1024（Replace）
802.1v	プロトコル VLAN グループ数	16
802.3ad Link Aggregation	リンクアグリゲーショングループ数	26 グループ
	1 グループに対するメンバーポート数	8
QOS	ハードウェアキュー数	8（Class 0-7）
ACL※1	アクセスリストのプロファイル数	4
	全てのプロファイルに対するアクセスルール数	900（装置全体）
Port security	ポートで制限する MAC アドレス学習数	64
Telnet Session	Telnet の同時セッション数	8
User Account	装置ログインのアカウント数	8
Trusted Host	Trusted ホストの IP エントリー数	10
Syslog Host	Syslog 送信先の IP エントリー数	4
IGMP Snooping	IGMP マルチキャストグループ数	1024 グループ
	IP ホスト数	1024
MLD Snooping	MLD マルチキャストグループ数	1024 グループ
MAC Based Access Control	MAC 認証で RADIUS 認証による収容端末数	1000（装置全体） 128（ポート単位の初期値）
	MAC 認証で Local 認証によるエントリー数	128
Web Authentication	WEB 認証で RADIUS 認証による収容端末数	1000（装置全体）
	WEB 認証で Local 認証によるエントリー数	16
	WEB 認証ポートの同時セッション数	128
802.1X Authentication	802.1X 認証で RADIUS 認証による収容端末数	1000（装置全体） 16（ポート単位の初期値）
	802.1X 認証で Local 認証によるエントリー数	128
Radius Server	RADIUS サーバーの IP エントリー数	3

項　目	内　容	最大値
MSTP	MSTP インスタンス数	4
LLDP	LLDP 通知 VLAN 数	32
Bandwidth	トラフィック制限値	1024000(Kbps) (64 単位)
Jumbo	ジャンボフレームサイズ (Un-Tag)	12284(Byte)
	ジャンボフレームサイズ (Tag)	12288(Byte)
SMTP	SMTP サーバーの IP エントリー数	1
SNTP	SNTP サーバーの IP エントリー数	2
SSH	SSH の同時セッション数	8
SNMP	SNMP MIB ビューのエントリー数	30
	SNMP MIB グループのエントリー数	30
	SNMP Community 名のエントリー数	10
	SNMP v3 ユーザー名のエントリー数	10
	SNMP トラップ送信先の IP エントリー数	10
LOG	ログの表示件数	10000(Line)
Mirror	ミラーリングの転送先ポート数	1
SSL Certificate	証明書のインポート数	1

※1 装置に設定可能なアクセスリストの最大ルール数は 900 です。1 つのプロファイルに設定可能な最大ルール数は 256 です。

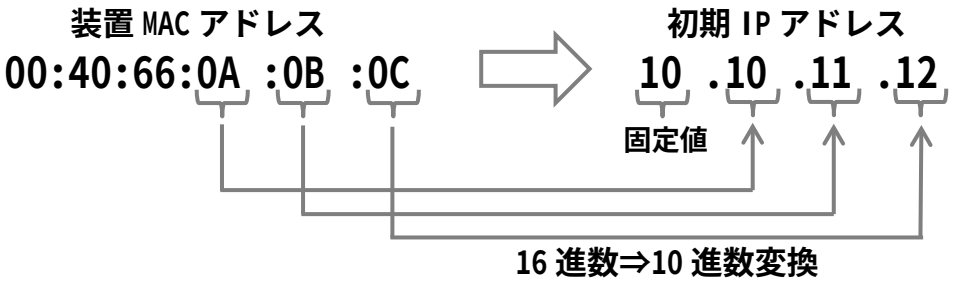
1.3 初期 IP アドレス設定

Ver.1.02 以降のファームウェアでは、初回起動時に初期 IP アドレスが以下の設定ルールに従って自動設定されます。ご使用の環境に合わせて IP アドレスを変更してください(3.2.1「config ipif」参照)。

(1) 初期 IP アドレスの設定ルール

初期 IP アドレスの先頭 1 バイトは 10 の固定とし、2 バイトから 4 バイトまでは装置 MAC アドレスの下位 3 バイトを 16 進数から 10 進数に変換した値で自動的に設定されます。

装置 MAC アドレスが 00:40:66:0A:0B:0C の場合、初期 IP アドレスは 10.10.11.12 となります。

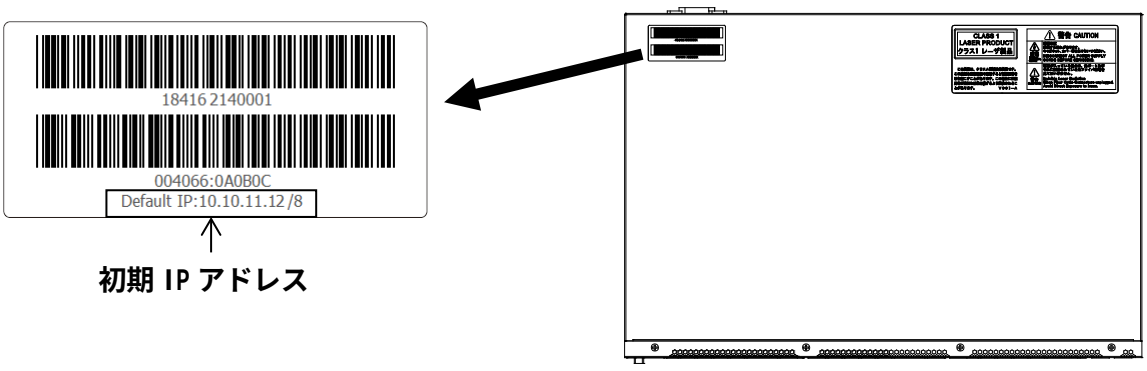


(2) サブネットマスク

サブネットマスクは、固定長 8 ビット（255.0.0.0）に設定されます。

(3) 初期 IP アドレスの確認方法

Ver.1.02 以降のバージョンで出荷された製品では、初期 IP アドレスが装置トップパネルのバーコードラベル上に表記されます。それ以前のバージョンで出荷された製品では初期 IP アドレスの記載がありませんが、バーコードラベル上の MAC アドレス表示あるいは UI 上の MAC アドレス表示を元に、(1)の初期 IP アドレスの設定ルールに従って算出することができます。

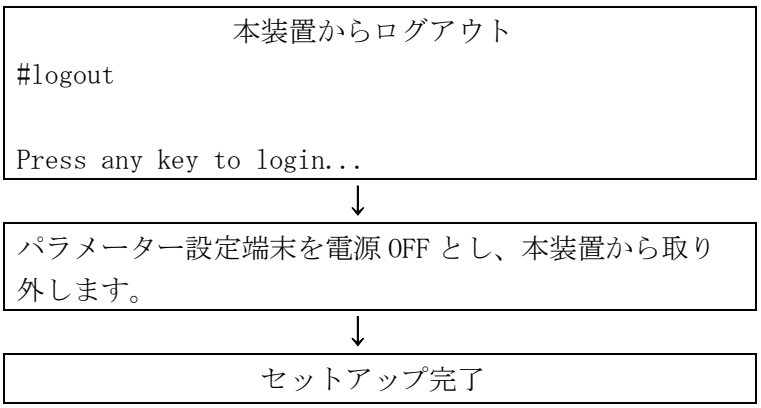


注意事項

デフォルト設定では、初期 IP アドレスは VLAN default（vid=1）に所属します。

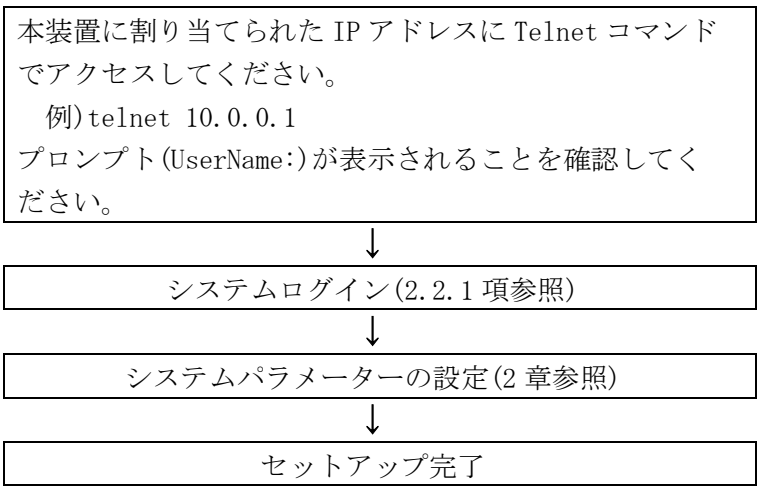
1.4 パラメーター設定手順

(1) パラメーター設定端末を用いたパラメーター設定の手順



(2) Telnet を用いたパラメーター設定の手順

Telnet を用いたパラメーターの設定は、本装置が LAN に接続され IP アドレスが設定されている場合のみ可能です。



1.5 パラメーター設定端末の準備

本装置のパラメーター設定に必要な端末の条件及び通信条件を表 1-3、表 1-4 に示します。

表 1-3 パラメーター設定端末の条件

項番	項　目	仕　様
1	端末の設定	ANSI(VT100 互換)

表 1-4 通信条件

項番	項　目	仕　様
1	キャラクタ	8bit/キャラクタ
2	ストップビット	1bit
3	パリティ	なし
4	フロー制御	なし
5	ボー・レート	9600bps
6	端末接続ケーブル	RS-232C ケーブル(ストレート)、 ただし、本装置側は DB-9 オス型コネクタを使用のこと

1.6 パラメーター設定端末の接続

パラメーター設定端末と本装置のコンソールポートを標準添付されている専用コンソールケーブル(ストレート)を用いて接続します。

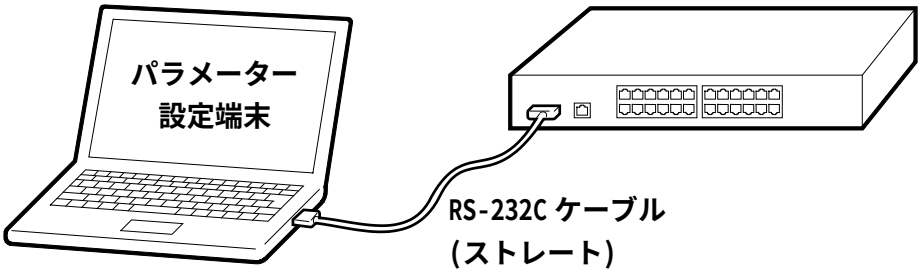


図 1-1 RS-232C ケーブルの接続

下記に本装置のコンソールポートのピン仕様を記載します。コンソールポートは、RS-232C(DTE 仕様，メス)になっています。

表 1-5 コンソールポートのピン仕様

ピン No.	信号名	信号の内容	備考
1	-	-	-
2	SD	送信データ	出力
3	RD	受信データ	入力
4	-	-	-
5	SG	回路アース	-
6	-	-	-
7	-	-	-
8	-	-	-
9	-	-	-

注意事項

コンソールポートには、パラメーター設定時のみに RS-232C ケーブルを接続し、誤入力防止のため通常の運用時には接続しないでください。

RS-232C ケーブルのピン配置を下記に記載します。

表 1-6 RS-232C ケーブル接続結線例 (D-SUB9 ピン-9 ピンの場合)

本装置側コネクタ 9 ピン D-SUB(オス)	接続	パラメーター設定用端末 コネクタ 9 ピン D-SUB
ピン番号		ピン番号
1	———	1
2	———	2
3	———	3
4	———	4
5	———	5
6	———	6
7	———	7
8	———	8
9	———	9

2. コマンドラインインターフェースの基本操作

コマンドライン方式によるパラメーターの表示/設定方法を説明します。

2.1 コマンドの表記規則

2 章および 3 章のコマンドの詳細にて記述される、各コマンドの引数の表記規則を表 2-1 に示します。

表 2-1 コマンド引数の表記規則

シンボル	説明
< >	文字列、または値の指定が必要
A | B	A または B のどちらかを選択
[ ]	省略可能
( )	複数のパラメーターを 1 つの集合として扱う
ITALIC 体	複数のパラメーターに分割

2.2 概要

コマンドライン方式の概要を説明します。

2.2.1 ログイン

login 名：adpro によりシステムにログインします。初回立ち上げ時にはパスワードは設定されていませんので、そのままリターンを押してログインしてください。

```
                ApresiaLightGM152GT Gigabit Ethernet Switch
                        Command Line Interface

                             Firmware: 1.03.00
          Copyright(C) 2020 APRESIA Systems, Ltd. All rights reserved.
UserName:adpro
PassWord:

#
```

2.2.2 初期化アカウント ap_recovery

「ap_recovery」は装置のパスワード、設定を全て初期化することができる特別なアカウントです。

ログインと同時に、ユーザーが設定したアカウント、パスワード、フラッシュメモリーに保存されたコンフィグ設定（ID1/ID2）、ログの全てを消去して再起動が行われます。アカウント「ap_recovery」のパスワードはありません。このアカウントはコンソールポートのみで有効です。

```
                ApresiaLightGM152GT Gigabit Ethernet Switch
                        Command Line Interface

                             Firmware: 1.03.00
          Copyright(C) 2020 APRESIA Systems, Ltd. All rights reserved.
UserName:ap_recovery
System will be reset, save and reboot!
Load Factory Default Configuration...  Done.
Saving all configurations to NV-RAM... Done.
Please wait, the switch is rebooting...
```

2.2.3 コマンド入力

2.2.3.1 コマンド入力文字

本コマンドライン方式は大文字/小文字を区別します。

2.2.3.2 入力補完機能

(1) コマンドの入力の際は、そのコマンドを認識可能な文字列のみ入力すればよく、全ての文字列の入力は必要ありません。

(例) “save config”コマンドを省略して入力

```
# save config
```

↓

```
# sa c
```

(2) 使用可能なコマンドを知りたい場合には、[?]キーを押してください。入力文字列から選択可能なコマンドを表示します。複数のコマンドが選択できる場合には、選択可能な全てのコマンドが表示されます。また、パラメーターを設定するコマンドの場合に、[?]キーを入力すると、パラメーターの設定範囲を表示することができます。[TAB]キーを押すと、入力可能なコマンドがあればその文字列をコマンドラインに自動的に表示しますので、全ての文字列を入力する必要がありません。例えば “sa”という文字列から選択可能なコマンドは “save”であることを知ることができます。

(例)

```
# sa[TAB]キー
```

↓

```
# save
```

2.2.3.3 設定の保存

変更内容をフラッシュメモリーに書き込むには、“save config”コマンドを使ってください。

(例)

```
#save config
Command: save config

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

#
```

2.2.3.4 画面のスクロール

コマンド実行時に表示できる内容が 1 画面に収まらない場合は、画面下に表示制御キーが表示されます。この状態で、必要に応じた表示制御キーを入力して下さい。

注意事項

コマンドの文字列が長い場合、行のズレが起きます。その場合はお使いのターミナルソフトの 1 行辺りの文字列数を 80 文字に設定ください。

2.2.3.5 キーの使い方

コマンド編集キーと表示制御キーの使い方を以下に記載します。

表 2-2 コマンド編集キーの使い方

Delete キー	カーソルを当てた文字を削除して、次に、その行に残った文字を左にシフトします。
Backspace キー	文字をカーソルの左方向に削除して、次に、その行に残っている文字を左にシフトします。
Insert キーまたは Ctrl+R	オンとオフを切り替えます。 オンの場合、文字を挿入し、前の文字を右にシフトします。
左向き矢印キー	左にカーソルを移動します。
右向き矢印キー	右にカーソルを移動します。
上向き矢印キー	前に入力したコマンドを繰り返します。 上向き矢印キーを押すたびに表示されているものよりも前のコマンドが表示されます。このように、現在のセッションのコマンド履歴を見直すことができます。コマンド履歴を順番に沿って前に進めるためには、下向き矢印キーを使用します。
下向き矢印キー	下向き矢印キーは現在のセッションに入力されたコマンド履歴において次のコマンドを表示します。各コマンドは、入力した順番に表示されます。上向き矢印キーを使用して、前のコマンドを見直します。
Tab キー	左にある次のフィールドにカーソルをシフトします。

表 2-3 表示制御キーの使い方

スペースバー	次のページを表示します。
CTRL+C	複数のページが表示される場合、残りのページの表示を止めます。
ESC キー	複数のページが表示される場合、残りのページの表示を止めます。
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	複数のページが表示される場合、残りのページの表示を止めます。
r	現在表示されているページを更新します。
a	ページ表示を中断せずに、残りのページを表示します。
Enter キー	次の行またはテーブルエントリーを表示します。

3. コマンドの詳細

注意事項

本ファームウェア(Ver. 1.03)では、本章に記載しているコマンドのみサポートしております。未記載のコマンドを入力した場合の動作は保証されません。

3.1 ツイストケーブル診断コマンド

3.1.1 cable_diag ports

目的	ツイストケーブルの接続をテストします。 ツイストケーブルにエラーが発生した場合、エラーのタイプと発生箇所を診断します。
構文	cable_diag ports < <portlist> | all >
説明	ツイストケーブルを診断します。ツイストケーブルのエラータイプは、「open」または「short」です。「open」とは、エラーになっている対のツイストケーブルが特定された箇所で接続していないことを示します。「short」とは、エラーになっている対のツイストケーブルが特定された箇所でショートしていることを示します。ステータスがリンクアップの場合、「short」や「open」エラーの問題はありませんが、リンクダウンでは調査の必要があります。テストで正常なツイストケーブルが接続されておりリモートパートナーの電源が落ちている場合には、リモートパートナーの電源が入っているとしてツイストケーブルの健全性を診断することができます。ツイストケーブル接続されていない場合には、No Cable と表示されます。テストでは、ツイストケーブルの長さも検出しますが参考値としてください。ケーブル種類やインターフェースの状態により実際の長さと異なる場合があります。本テストの実行時に診断パケットを送出します。また、ポートのリンクアップおよびリンクダウンが発生しますのでご注意ください。 なお、光ファイバーケーブルを接続しているポートでは、本テストの対象にはなりません。
パラメーター	<portlist> - テストするポート範囲を指定します。 all - すべてのポートを指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 21～24 のツイストケーブル診断を行うには

```
#cable_diag ports 21-24
Command: cable_diag ports 21-24

Perform Cable Diagnostics ...

 Port   Type      Link Status          Test Result            Cable Length (M)
 ----  -------  --------------  -------------------------  -----------------
  21    GE         Link Up       OK                                3
  22    GE         Link Down     No Cable                          -
  23    GE         Link Down     No Cable                          -
  24    GE         Link Down     No Cable                          -

#
```

3.2 基本的な IP コマンド

3.2.1 config ipif

目的	スイッチに IP インターフェースを設定します。
構文	config ipif System 〈 *ipaddress* | bootp | dhcp | ipv6 ipv6address 〈ipv6networkaddr〉 | dhcpv6_client 〈 enable | disable 〉〉 *Ipaddress* =ipaddress 〈network_address〉〈 vlan 〈vlan_name 32〉 | state 〈 enable | disable 〉〉
説明	本コマンドは、スイッチに IP インターフェースを設定します。
パラメーター	ipaddress 〈network_address〉- 作成する IP インターフェースの IP アドレスとネットマスクを入力します。 従来の形式でアドレスとマスクの情報を指定できます（例：10.1.2.3/255.0.0.0 または 10.1.2.3/8 の CIDR 形式など)。本コマンドで 0.0.0.0/0 を指定した場合、IP アドレスが未割当の状態になります。Ver.1.02 以降では、装置起動時に IP インターフェースが有効で、かつ IP アドレスが 0.0.0.0/0 に設定されていると、自動的にが 0.0.0.0/0 から初期 IP アドレスに置き換えられます(current_config の書き換え)。 〈vlan_name 32〉- IP インターフェースに対応する VLAN 名を指定します。 state 〈enable | disable〉- IP インターフェースを「enable」(有効)または「disable」(無効)にします。 bootp - スイッチの IP インターフェースに IP アドレスを割り当てるために、BOOTP プロトコルを選択します。 dhcp -スイッチの IP インターフェースに IP アドレスを割り当てるために、DHCP プロトコルを選択します。 ipv6 ipv6address 〈ipv6networkaddr〉- IPV6 ネットワークアドレスを指定します。このアドレスはホストアドレスとネットワークプレフィックスの長さを定義します。 一つのインターフェースに複数の IPv6 アドレスを設定することができます。 新しいアドレスが定義されると、この ipif に追加されます。 dhcpv6_client 〈 enable | disable 〉- DHCPv6 プロトコルで IP アドレスを取得することを「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチに IP インターフェースを設定するには

```
#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

#
```

使用例:スイッチの IP インターフェースを初期化するには

```
#config ipif System ipaddress 0.0.0.0/0
Command: config ipif System ipaddress 0.0.0.0/0

Success.

#
```

注意事項

(Ver.1.02 以降)
コマンドで IP インターフェースを 0.0.0.0/0 に設定すると、IP アドレスが未割当の状態になります。IP アドレス自動設定機能で初期 IP アドレスの値に置き換える場合、設定を保存して再起動する必要があります。

IP インターフェースを 0.0.0.0/0 に設定する場合はコンソールポートを使用してください。telnet などのリモート接続を用いた場合、コマンド入力後直ちに IP アドレスが未割当の状態になり、リモートからアクセスできなくなります。

使用例:スイッチの IP インターフェースを無効化するには

```
# config ipif System ipaddress 0.0.0.0/0 state disable
Command: config ipif System ipaddress 0.0.0.0/0 state disable

Success.

#
```

注意事項

(Ver.1.02 以降)
IP インターフェースを完全に無効化する場合、state disable オプションを使用してください。state enable の状態で IP アドレスを 0.0.0.0/0 に設定すると、入力時点では IP アドレスが未割当となり IP インターフェースが使用できなくなりますが、再起動すると Ver.1.02 で実装された IP アドレス自動設定機能により、初期 IP アドレスが自動的に割り当てられます。

3.2.2 show ipif

目的	スイッチの IP インターフェース設定を表示します。
構文	show ipif
説明	本コマンドは、スイッチの IP インターフェース設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチの IP インターフェース設定を表示するには

```
#show ipif
Command: show ipif

IP Interface Settings

Interface Name              : System
IP Address                  : 10.10.11.12 (MANUAL)
Subnet Mask                 : 255.0.0.0
VLAN Name                   : default
Admin. State                : Enabled
DHCPv6 Client State         : Disabled
Link Status                 : Link Down
Member Ports                : 1-52

Total Entries: 1

#
```

3.3 基本的なスイッチコマンド

3.3.1 create account

目的	アカウントを作成します。
構文	create account 〈 admin ｜ user 〉〈username 15〉
説明	本コマンドは、1～15 文字までのユーザー名と 0～15 文字までのパスワードでユーザーアカウントを作成します。 アカウントは 8 個まで作成することができます。
パラメーター	admin〈username〉- 管理者アカウントの名前を設定します。 user〈username〉- ユーザーアカウントの名前を設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。 ユーザー名は 1～15 文字以内で入力します。 パスワードは 0～15 文字以内で入力します。
対応バージョン	1.00.00 以降

使用例:「APS」というユーザー名を使用して管理者アカウントを作成するには

```
#create account admin APS
Command: create account admin APS

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

#
```

3.3.2 config account

目的	アカウントにパスワードを設定します。
構文	config account〈username〉
説明	本コマンドは、「create account」 コマンドで作成したアカウントにパスワードを設定します。コマンド入力後に、古いパスワード、新しいパスワード、新しいパスワードの再入力を促す表示がされます。
パラメーター	〈username〉- アカウント名を指定します。アカウントは「create account」コマンドによって既に定義されている必要があります。
制限事項	管理者アカウントのみ本コマンドを実行できます。 ユーザー名は 1～15 文字以内で入力します。 パスワードは 0～15 文字以内で入力します。
対応バージョン	1.00.00 以降

使用例:「APS」というアカウントのパスワードを設定するには

```
#config account APS
Command: config account APS

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

#
```

3.3.3 show account

目的	作成したアカウント情報を表示します。
構文	show account
説明	本コマンドは、作成したアカウント情報を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 作成したアカウント情報を表示するには

```
#show account
Command: show account

Current Accounts:
Username          Access Level
----------        ------------
APS               Admin

Total Entries: 1

#
```

3.3.4 delete account

目的	既存のアカウントを削除します。
構文	delete account <username>
説明	本コマンドは、「create account」コマンドで作成したアカウントを削除します。
パラメーター	<username> - 削除するアカウント名を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:「APS」という既存のアカウントを削除するには

```
#delete account APS
Command: delete account APS

Success.

#
```

3.3.5 show session

目的	現在ログイン中のユーザーのリストを表示します。
構文	show session
説明	本コマンドは、ログイン中の全ユーザーのリストを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ログイン中の全ユーザーのリストを表示するには

```
#show session
Command: show session

ID  Live Time                   From                                Level      Name
-- ------------ ------------------------------------ ----- ---------------
8  0:0:53.410   Serial Port                          4     adpro
Total Entries: 1

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

3.3.6 show switch

目的	スイッチに関する一般的な情報を表示します。
構文	show switch
説明	本コマンドは、スイッチに関する情報を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに関する情報を表示するには

```
#show switch
Command: show switch

Device Type         : APLGM152GT Gigabit Ethernet Switch
MAC Address         : 00-40-66-0A-0B-0C
IP Address          : 10.10.11.12 (Manual)
VLAN Name           : default
Subnet Mask         : 255.0.0.0
Default Gateway     : 0.0.0.0
Boot PROM Version   : 1.00.00
Firmware Version    : 1.03.00
System Name         :
System Location     :
System Contact      :
Serial Number       : 184162130020
Spanning Tree       : Disabled
GVRP                : Disabled
IGMP Snooping       : Disabled
802.1X              : Disabled
Telnet              : Enabled (TCP 23)
Web                 : Enabled (TCP 80)
RMON                : Disabled
SSH                 : Disabled
SSL                 : Disabled
CLI Paging          : Enabled
Syslog Global State: Disabled
Dual Image          : Supported

#
```

3.3.7 show serial_port

目的	シリアルポート設定を表示します。
構文	show serial_port
説明	本コマンドは、シリアルポート設定を表示します。
パラメーター	なし。
制限事項	なし
対応バージョン	1.00.00 以降

使用例:シリアルポート設定を表示するには

```
#show serial_port
Command: show serial_port

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

#
```

3.3.8 config serial_port

目的	シリアルポートの設定をします。
構文	config serial_port 〈 *baud_rate* | *auto_logout* 〉 *baud_rate* =baud_rate 〈 9600 | 19200 | 38400 | 115200 〉 *auto_logout* =auto_logout 〈 never | 2_minutes | 5_minutes | 10_minutes | 15_minutes 〉
説明	本コマンドは、シリアルポートのボーレートと自動ログアウト時間を設定します。
パラメーター	baud_rate〈9600 | 19200 | 38400 | 115200〉- 管理ホストとの通信に使用されるシリアルボーレートを指定します。 9600/19200/38400/115200 bps のいずれかを設定します。 never - ユーザーからの入力がなくなってもコンソールはログアウトせずに開いた状態を維持します。 2_minutes - ユーザーからの入力がなくなってから 2 分経過後に、コンソールは自動的にログアウトします。 5_minutes- ユーザーからの入力がなくなってから 5 分経過後に、コンソールは自動的にログアウトします。 10_minutes - ユーザーからの入力がなくなってから 10 分経過後に、コンソールは自動的にログアウトします。 15_minutes - ユーザーからの入力がなくなってから 15 分経過後に、コンソールは自動的にログアウトします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:シリアルポートのボーレートを設定するには

```
#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Please change your baud rate to 115200 for new baud rate !!
```

3.3.9 enable clipaging

目的	コマンド表示情報が 1 画面以上となる場合、次画面へのスクローリングを一時停止する機能を有効にします。
構文	enable clipaging
説明	コマンド表示情報が 1 画面以上となる場合、次画面へのスクローリングを一時停止する機能を有効にします。デフォルト設定は「enable」(有効)です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:「show」コマンドの出力がページの最後に達したとき、画面の表示を一時停止させるには

```
#enable clipaging
Command: enable clipaging

Success.

#
```

3.3.10 disable clipaging

目的	コマンド表示情報が 1 画面以上となる場合、次画面へのスクローリングを一時停止する機能を無効にします。
構文	enable clipaging
説明	コマンド表示情報が 1 画面以上となる場合、次画面へのスクローリングを一時停止する機能を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:「show」コマンドの出力がページの最後に達したとき、画面表示の一時停止を無効にするには

```
#disable clipaging
Command: disable clipaging

Success.

#
```

3.3.11 enable telnet

目的	Telnet プロトコルを使用したスイッチとの通信を有効にします。
構文	enable telnet [<tcp_port_number 1-65535>]
説明	本コマンドは、スイッチの Telnet プロトコルを有効にします。スイッチの Telnet リクエストポート番号を指定できます。
パラメーター	<tcp_port_number 1-65535> - TCP ポート番号を入力します。TCP ポート番号は、1～65535 の範囲で設定してください。デフォルト値は、23 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Telnet を有効にし、ポート番号「23」を設定するには

```
#enable telnet 23
Command: enable telnet 23

Success.

#
```

3.3.12 disable telnet

目的	スイッチの Telnet プロトコルを無効にします。
構文	disable telnet
説明	本コマンドは、スイッチの Telnet プロトコルを無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの Telnet プロトコルを無効にするには

```
#disable telnet
Command: disable telnet

Success.

#
```

3.3.13 telnet

目的	telnet プロトコルを介して他の機器に接続します。
構文	telnet <ipaddr> [tcp_port <value 0-65535>]
説明	本コマンドは、Telnet プロトコルを介して他の機器に接続します。
パラメーター	<ipaddr> - Telnet を使用して接続する機器の IP アドレスを入力します。 tcp_port <value 0-65535> - 接続に使用する TCP ポート番号を入力します。 デフォルト値は、23 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。 本装置からの IPv6 Telnet クライアント機能には対応しておりません。 本装置への IPv6 Telnet アクセスは可能です。
対応バージョン	1.00.00 以降

使用例:TCP ポート番号「23」の Telnet プロトコルを介して IP アドレス（10.53.13.99）の機器に接続するには

```
#telnet 10.53.13.99 tcp_port 23
Command: telnet 10.53.13.99 tcp_port 23
```

3.3.14 enable web

目的	スイッチの web ベース GUI を有効にします。
構文	enable web [<tcp_port_number 1-65535>]
説明	本コマンドは、スイッチの web ベース GUI を有効にします。スイッチの HTTP ポート番号を指定できます。
パラメーター	<tcp_port_number 1-65535>- TCP ポート番号を入力します。 TCP ポート番号は、1～65535 の範囲で設定してください。デフォルト値は、80 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:HTTP を有効にし、ポート番号「80」を設定するには

```
#enable web 80
Command: enable web 80

Note: SSL will be disabled if web is enabled.
Success.

#
```

3.3.15 disable web

目的	スイッチの web ベース GUI を無効にします。
構文	disable web
説明	スイッチの web ベース GUI を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:web ベース GUI を無効にするには

```
#disable web
Command: disable web

Success.

#
```

3.3.16 save

目的	NV-RAM にスイッチのコンフィグレーションを保存します。
構文	save [< config_id < value 1-2 > | log | all >]
説明	本コマンドは、NV-RAM に現在のコンフィグレーションを保存します。保存されたコンフィグレーションは、スイッチを再起動するたびに現在のスイッチのコンフィグレーションに展開されます。
パラメーター	config_id < value 1-2 > - コンフィグレーションを保存するセクション ID 番号を入力します。セクション ID 番号を指定することによって、2 種類のコンフィグレーションをスイッチ内に格納できます。 log - 現在のログを NV-RAM に保存します。保存されたログは削除できません。 all - 現在アクチベートされたコンフィグレーションの変更とログを保存します。現在のコンフィグレーションとログの両方を NV-RAM に保存します。 パラメーターを指定しない場合、コンフィグレーションのみ保存されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:NV-RAM にスイッチの現在のコンフィグレーションを保存するには

```
#save config_id 1
Command: save config_id 1

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

#
```

使用例:NV-RAM にスイッチの現在のログを保存するには

```
#save log
Command: save log

Saving all log information to NV-RAM..... Done.
Success.

#
```

使用例:NV-RAM にスイッチの現在のコンフィグレーションとログを保存するには

```
#save all
Command: save all

Saving all configurations and log information to NV-RAM..... Done.
Success.

#
```

注意事項

save コマンドの実行時、CPU 高負荷状態を示す CPU utilization (OVERLOADING)ログが出力される場合があります。

3.3.17 reboot

目的	スイッチを再起動します。
構文	reboot [force_agree]
説明	本コマンドは、スイッチを再起動します。
パラメーター	force_agree - force_agree を指定すると、再起動の確認を行わずに、すぐに再起動が始まります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチを再起動するには

```
#reboot
Command: reboot

If you do not save the settings, all changes made in this session will be lost.
Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

注意事項

電源を再投入する場合、電源切断後 5 秒以上間隔をあけて電源を入れてください。

3.3.18 reset

目的	スイッチをデフォルト設定に戻します。
構文	reset [config | system] [force_agree]
説明	本コマンドは、スイッチのコンフィグレーションをデフォルト設定に戻します。
パラメーター	config - config のキーワードを指定すると、IP アドレス、アカウント、スイッチ履歴ログなどを含むすべての設定がデフォルト設定に戻ります。スイッチは再起動せずに、即時設定が反映されます。IP アドレスは(初期 IP アドレスではなく)0.0.0.0/0 に変更され、IP アドレスが未割当の状態になりますのでご注意ください。 system - system のキーワードを指定すると、スイッチの設定がデフォルト値に変更された後、保存および再起動が行われます。再起動するとフォワーディングデータベース内のすべてのエントリーがクリアされます。 force_agree - force_agree を指定すると、確認を行わずに、Reset コマンドがすぐに実行されます。 パラメーターを指定しない場合、スイッチの現在の IP アドレス、アカウント、スイッチ履歴ログは変更されません。他のすべてのパラメーターはデフォルト設定にリストアされます。スイッチのコンフィグレーション保存および再起動は行われません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:IP アドレス、ユーザーアカウント、およびスイッチログ履歴以外のデフォルト値にスイッチパラメーターをリストアするには

```
#reset
Command: reset

Are you sure you want to proceed with system reset
except IP address, log and user account?(y/n) y
Success.

#
```

使用例:スイッチパラメーターをデフォルト値にリストアするには

```
#reset config
Command: reset config

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

Success.

#
```

使用例:すべてのスイッチパラメーターをデフォルト値にリストアし、スイッチを再起動するには

```
#reset system
Command: reset system

Are you sure you want to proceed with system reset, save and reboot?(y/n)
Load Factory Default Configuration... Done.
Saving all configurations to NV-RAM.. Done.
Please wait, the switch is rebooting...
```

注意事項

reset system コマンドを実行した場合、コンフィグ設定ファイル（ID1/ID2 ともに）の初期化と再起動が行われます。

3.3.19 login

目的	スイッチに再ログインします。
構文	login
説明	本コマンドは、スイッチに再ログインします。 ユーザー名とパスワードプロンプトが表示されます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに再ログインするには

```
#login
Command: login

UserName:
```

3.3.20 logout

目的	スイッチからログアウトします。
構文	logout
説明	本コマンドは、スイッチからログアウトします。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチからログアウトするには

```
#logout
```

3.3.21 enable jumbo_frame

目的	ジャンボフレーム機能を有効にします。
構文	enable jumbo_frame
説明	本コマンドは、ジャンボフレームを有効に設定します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.01 以降

使用例:ジャンボフレーム機能を有効にするには

```
#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of jumbo frame is 12288 bytes.
Success.

#
```

3.3.22 disable jumbo_frame

目的	ジャンボフレーム機能を無効にします。
構文	disable jumbo_frame
説明	本コマンドは、ジャンボフレームを無効に設定します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ジャンボフレーム機能を無効にするには

```
#disable jumbo_frame
Command: disable jumbo_frame

Success.

#
```

3.3.23 show jumbo_frame

目的	ジャンボフレーム機能の設定を表示します。
構文	show jumbo_frame
説明	本コマンドは、ジャンボフレーム機能の設定を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ジャンボフレームの設定を表示するには

```
#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State   : Enabled
Maximum Jumbo Frame Size : 12288 Bytes

#
```

3.3.24 config default_language

目的	Web ユーザーインターフェースの表示言語を設定します。
構文	config default_language < japanese | English >
説明	本コマンドは、Web ユーザーインターフェース使用時の表示言語を設定します。 デフォルト設定は、「japanese」です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Web ユーザーインターフェースの表示言語を日本語にするには

```
#config default_language japanese
Command: config default_language japanese


Success.


#
```

3.3.25 show default_language

目的	Web ユーザーインターフェースの使用言語を表示します。
構文	show default_laguage
説明	本コマンドは、Web ユーザーインターフェースの使用言語を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Web ユーザーインターフェースの使用言語を表示するには

```
#show default_language
Command: show default_language


Default language : Japanese


#
```

3.3.26 show tech_support

目的	テクニカルサポート情報を表示します。
構文	show tech_support
説明	本コマンドは、テクニカルサポートに必要となるスイッチの動作情報を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: テクニカルサポート情報を表示するには

```
# show tech_support
Command: show tech_support

================================================================================
                      APLGM152GT Gigabit Ethernet Switch
                      Technical Information Report
================================================================================



[CPU Utilization 2014-3-10 20:53:37]

CPU Utilization
-------------------------------------------------------------------------------
Five seconds -  25 %         One minute -  24 %         Five minutes -  13 %
Maximum      -  85 %         Minimum    -  13 %

[Device Information 2014-3-10 20:53:37]

Device Type         : APLGM152GT Gigabit Ethernet Switch
MAC Address         : 00-40-66-0A-0B-0C
IP Address          : 10.10.11.12 (Manual)
VLAN Name           : default
Subnet Mask         : 255.0.0.0
Default Gateway     : 0.0.0.0
Boot PROM Version   : Build 1.00.00
Firmware Version    : Build 1.03.00
Hardware Version    : A1
Serial Number       : 184162130020
Spanning Tree       : Disabled
GVRP                : Disabled
IGMP Snooping       : Disabled
802.1X              : Disabled
Telnet              : Enabled (TCP 23)
Web                 : Enabled (TCP 80)
RMON                : Disabled
```

```
SSH                : Disabled
SSL                : Disabled
CLI Paging         : Enabled
Syslog Global State: Disabled
Dual Image         : Supported

[Connection Session Status 2014-3-10 20:53:37]

 ID   Live Time       From           Level   Name
 ---  ------------    ------------   -----   ---------------
 8    0:0:16.430      Serial Port    4       adpro

 (続く)
```

3.3.27 upload tech_support_toTFTP

目的	テクニカルサポート情報を TFTP サーバーにアップロードします。
構文	upload tech_support_toTFTP <ipaddr> <path_filename 64>
説明	本コマンドは、テクニカルサポートに必要となるスイッチの動作情報を TFTP サーバーにアップロードします。
パラメーター	<ipaddr> - TFTP サーバーの IP アドレスを入力します。 <path_filename 64> - TFTP サーバーに保存するファイル名を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:テクニカルサポート情報を TFTP サーバーにアップロードするには

```
#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.

#
```

注意事項

upload コマンドの実行中、CPU 高負荷状態を示す CPU utilization (OVERLOADING) ログが出力される場合があります。

3.4 スイッチユーティリティコマンド

3.4.1 download firmware_fromTFTP

目的	TFTP サーバー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_fromTFTP < <ipaddr> | <ipv6addr> > <path_filename 64> image_id <value 1-2>
説明	本コマンドは、TFTP サーバーからファームウェアをダウンロードして、装置 NV-RAM に保存します。ダウンロードしたファームウェアを反映するには、装置再起動が必要です。
パラメーター	<ipaddr> - TFTP サーバーの IP アドレスを入力します。 <ipv6addr> - TFTP サーバーの IPv6 アドレスを入力します。 <path_filename 64> - TFTP サーバーにあるファームウェアのファイル名を入力します。例：tmp¥aplgm152R10300.img image_id <value 1-2> - ファームウェアを保存するセクション ID を入力します。セクション ID 指定により、2 種類のファームウェアを格納できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

注意事項

ファームウェアのダウンロード時、CPU 高負荷状態を示す CPU utilization (OVERLOADING)ログが出力される場合があります。

ファームウェアのダウンロード状況を示す数値が 100%になっても内部処理が継続して行われます。Success が表示されるまでお待ちください。

3.4.2 download cfg_fromTFTP

目的	TFTP サーバーからコンフィグレーションファイルをダウンロードします。
構文	download cfg_fromTFTP < <ipaddr> | <ipv6addr> > <path_filename 64> [< increment | config_id<value 1-2> >]
説明	本コマンドは、TFTP サーバーからコンフィグレーションファイルをダウンロードして、現在のコンフィグレーションを変更するか、または装置 NV-RAM へ保存のみ行うかを選択することができます。
パラメーター	<ipaddr> - TFTP サーバーの IP アドレスを入力します。 <ipv6addr> - TFTP サーバーの IPv6 アドレスを入力します。 <path_filename 64> - TFTP サーバーにあるコンフィグレーションファイルのファイル名を入力します。例：tmp¥setting.txt increment - ダウンロードしたコンフィグレーションファイルで明示のコマンドは、現在のコンフィグレーションに変更コマンドとして実行します。 config_id <value 1-2> - コンフィグレーションファイルを保存するセクション ID を入力します。セクション ID 指定により、2 種類のコンフィグレーションを格納できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ダウンロードしたコンフィグレーションファイルをセクション ID1 へ保存するには

```
#download cfg_fromTFTP 10.48.74.121 tmp¥setting.txt config_id 1
Command: download cfg_fromTFTP 10.48.74.121 tmp¥setting.txt config_id 1

 Connecting to server................... Done.
 Download configuration.................. Done.
 Please wait, programming flash......... Done.

Success.

#
```

注意事項

ダウンロードしたコンフィグレーションファイルを現在の設定に置き換えるため、リンクアップしているポートは一時リンクダウンが発生します。

3.4.3 config firmware image_id

目的	次回起動させるファームウェアのセクション ID 指定、またはファームウェアの削除を行います。
構文	config firmware image_id <value 1-2> < delete | boot_up >
説明	本コマンドは、2 つの保存されたファームウェアで次回起動のセクション ID の指定、またはファームウェアの削除を行います。
パラメーター	<value 1-2> - 保存されているファームウェアのセクション ID を指定します。 delete - 指定したセクション ID のファームウェアを削除します。 boot_up - 指定したセクション ID のファームウェアで次回起動します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:セクション ID 1 のファームウェアで次回起動するには

```
#config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

#
```

注意事項

指定したセクション ID 番号のファームウェア異常により起動できない場合、自動的に別 ID 番号のファームウェアで起動します。

3.4.4 show firmware information

目的	スイッチに保存されているファームウェアのセクション情報を表示します。
構文	show firmware information
説明	本コマンドは、スイッチに保存されているファームウェアのセクション情報を表示します。
パラメーター	なし。
制限事項	なし
対応バージョン	1.00.00 以降

使用例:スイッチに保存されているファームウェアのセクション情報を表示するには

```
#show firmware information
Command: show firmware information

Image ID   : 1(Boot up firmware)
Version    : 1.03.00
Size       : 4750040 Bytes
Update Time: 2021/01/12 10:46:03
User       : adpro(CONSOLE)

Image ID   : 2
Version    : 1.03.00
Size       : 4750040 Bytes
Update Time: 2021/01/12 10:55:23
User       : adpro(CONSOLE)

#
```

3.4.5 show config

<table>
<tr><td>目的</td><td colspan="2">スイッチが現在動作している、または保存されているコンフィグレーションを表示します。</td></tr>
<tr><td>構文</td><td colspan="2">show config < current_config | config_in_nvram config_id < value 1-2 > [modified | information >]</td></tr>
<tr><td>説明</td><td colspan="2">本コマンドは、スイッチが現在動作しているコンフィグレーション、または NV-RAM に保存されているコンフィグレーションを表示します。
表示端末のキーボード入力で、「Enter」で 1 行ずつ、「Space」で 1 ページずつ、「a」ですべての設定を表示します。
コンフィグレーションは、以下の順でカテゴリ別にリストされます。</td></tr>
<tr><td></td><td># DEVICE
BASIC
UTILIZATION_NOTIFY
STORM
MIRROR
QOS
SYSLOG
TRAF-SEGMENTATION
SSL
EEE
DDM
MANAGEMENT
VLAN
PORT_SECURITY
ACL
PROTOCOL_VLAN
QINQ
8021X
FDB
RADIUS
sRED
STP
LOOP_DETECT
BPDU_GUARD
BANNER_PROMP</td><td># SSH
TELNETS
SMTP
SNTP
LACP
IP
DHCPv6_SERVER
SNMPv3
WAC
LLDP
MBA
AUTHENTICATION_SETTINGS
IGMP_SNOOPING
PORTMCFILTER
MLDSNP
ACCESS_AUTHENTICATION_CONTROL
AAA_LOCAL_ENABLE_PASSWORD
DHCP_RELAY
NDP
ARP
ROUTE
PORT
DHCP_SERVER
RELAY6</td></tr>
<tr><td>パラメーター</td><td colspan="2">current_config - 現在動作している設定を表示します。
config_in_nvram - NV-RAM に保存されている設定を表示します。
config_id < value 1-2 > - 表示するセクション ID 番号を選択します。
modified - デフォルト状態から変更された設定のみを表示します。
information - コンフィグレーションのセクション ID 情報を表示します。</td></tr>
<tr><td>制限事項</td><td colspan="2">管理者アカウントのみ本コマンドを実行できます。</td></tr>
<tr><td>対応バージョン</td><td colspan="2">1.00.00 以降</td></tr>
</table>

注意事項

パラメーター current_config により表示される設定情報には、account 情報は含まれません。

802.1X 認証でローカルユーザーにより登録したパスワード情報は、暗号化されずに表示されます。

使用例:現在のコンフィグレーション情報をすべて表示するには

```
#show config current_config
Command: show config current_config

#-------------------------------------------------------------------------------
#                  ApresiaLightGM152GT Gigabit Ethernet Switch
#                                  Configuration
#
#                                 Firmware: 1.03.00
#          Copyright(C) 2020 APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------



# DEVICE

config temperature polling_interval 60
config temperature notify high state enable threshold 55 trap_state enable log_state enable
config temperature notify low state enable threshold -5 trap_state enable log_state enable
fan_led error enable

# BASIC

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

使用例:現在のコンフィグレーションでデフォルト状態から変更された情報のみ表示するには

```
#show config current_config modified
Command:show current_config modified

enable loopdetect
enable ssl
config ipif System vlan default ipaddress 192.168.3.4/8 state enable

#
```

使用例:スイッチに保存されているコンフィグレーションのセクション ID 情報を表示するには

```
#show config information
Command: show config information

Configuration ID: 1(Boot up Configuration)
Version         : 1.03.00
Size            : 32391 Bytes
Update Time     : 2021/01/13 12:03:14
User            : adpro(CONSOLE)(Local)

Configuration ID: 2
Version         : 1.03.00
Size            : 32391 Bytes
Update Time     : 2021/01/13 12:03:20
User            : adpro(CONSOLE)(Local)

#
```

3.4.6 upload

目的	コンフィグレーション情報またはログ情報を TFTP にアップロードします。
構文	upload < cfg_toTFTP <ipaddr> | <ipv6addr> > <path_filename 64> [config_id <value 1-2>] | log_toTFTP <ipaddr> | <ipv6addr> > <path_filename 64>
説明	本コマンドは、スイッチのコンフィグレーション情報またはログ情報のどちらかを指定して TFTP サーバーにアップロードします。
パラメーター	cfg_toTFTP - スイッチのコンフィグレーション情報を TFTP サーバーにアップロードする場合に指定します。 log_toTFTP - スイッチのログ情報を TFTP サーバーにアップロードする場合に指定します。 <ipaddr> - TFTP サーバーの IP アドレスを入力します。 <ipv6addr> - TFTP サーバーの IPv6 アドレスを入力します。 <path_filename 64> - TFTP サーバーにアップロードするファイル名を入力します。 config_id < value 1-2> - スイッチに保存されたコンフィグレーションのセクション ID を入力します。パラメーター指定がない場合、現在のコンフィグレーションを TFTP サーバーにアップロードします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

注意事項

パラメーター cfg_toTFTP によりアップロードした設定情報には、account 情報は含まれません。

使用例:現在のコンフィグレーションをアップロードするには

```
#upload cfg_toTFTP 10.48.74.121 coufig_up.txt
Command: upload cfg_toTFTP 10.48.74.121 coufig_up.txt

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

#
```

3.4.7 ping

目的	ネットワーク機器間の接続性をテストします。
構文	ping <ipaddr> [times <value 0-255>] [size <value 1-60000>] [timeout <sec 1-99>]
説明	本コマンドは、リモート IP アドレスに Internet Control Message Protocol(ICMP)エコーメッセージを送信します。 その後、リモート IP アドレスは、メッセージを返します。これは、スイッチとリモートデバイス間の接続性を確認するために使用されます。
パラメーター	<ipaddr> - リモートホストの IP アドレスを入力します。 times <value 0-255> - 送信する ICMP エコーメッセージ数を入力します。指定しない場合または 0 に設定した場合、ICMP エコーメッセージを送信し続けます。デフォルト値は 0 です。 size <value 1-60000> - テスト用パケットサイズを入力します。値の範囲は、1～60000 byte です。 timeout <sec 1-99> - リモートデバイスからの応答を待つタイムアウト時間を定義します。1～99 秒の範囲で指定できます。デフォルト値は 1 秒です。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:IP アドレス「10.48.74.121」に 4 回 ping するには

```
#ping 10.48.74.121 times 4
Command: ping 10.48.74.121

Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms

Ping statistics for 10.48.74.121
Packets: Sent =4, Received =4, Lost =0

#
```

3.4.8 ping6

目的	IPv6 ネットワークの診断を行います。
構文	ping6 〈ipv6addr〉[times 〈value 1-255〉 | size 〈value 1-6000〉 | timeout 〈 sec 1-99〉]
説明	本コマンドは、IPv6 ネットワークの診断に使用します。
パラメーター	〈ipv6addr〉- リモートホストの IPv6 アドレスを指定します。 times 〈value 1-255〉- 送信する ICMP エコーメッセージ数を入力します。指定しない場合は、ICMP エコーメッセージを送信し続けます。 size 〈value 1-6000〉- テスト用パケットのサイズを入力します。値の範囲は、1～6000 byte です。 timeout 〈sec 1-99〉- リモートデバイスからの応答を待つタイムアウト時間を定義します。1～99 秒の範囲で指定できます。デフォルト値は 1 秒です。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:IPv6 アドレス「FE80::254:85FF:FE32:1804」に 6 回 ping を行うには

```
#ping6 FE80::254:85FF:FE32:1804%System times 6
Command: ping6 FE80::254:85FF:FE32:1804%System times 6

Reply from FE80::254:85FF:FE32:1804, bytes=100 time=10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
 Ping Statistics for FE80::254:85FF:FE32:1804
 Packets: Sent =6, Received =6, Lost =0
Success.

#
```

3.4.9 traceroute

目的	スイッチと送信先間の経路を追跡します。
構文	traceroute <ipaddr> [ttl <value 1-60>] [port <value 30000-64900>] [timeout <sec 1-65535>] [probe <value 1-9>]
説明	本コマンドは、スイッチと送信先間の経路を追跡します。
パラメーター	<ipaddr> - 送信先の IP アドレスを入力します。 ttl <value 1-60> -経由するルーターの最大数を入力します。デフォルト値は 30 です。 port <value 30000-64900> - 使用する UDP ポート番号を入力します。デフォルト値は 33435 です。 timeout <sec 1-65535> - リモートデバイスからの応答を待つタイムアウト時間を入力します。デフォルト値は 5 秒です。 probe <value 1-9> - プローブの回数です。デフォルト値は 1 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチと 10.48.74.121 間の経路を追跡するには

```
#traceroute 10.48.74.121 probe 2
Command: traceroute 10.48.74.121 probe 2

 <10 ms.     10.48.74.121
 <10 ms.     10.48.74.121

Trace complete.

#
```

3.4.10 config terminal_line

目的	1 画面に表示できるコマンド表示情報の行数を設定します。
構文	config terminal_line < default | <value 20-80> >
説明	本コマンドは、1 画面の表示行数を設定します。
パラメーター	default - デフォルト値の 24 に設定します。 <value 20-80> - 表示行数 20～80 の範囲で設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:画面に表示されるコマンドの行数を 30 行に設定するには

```
#config terminal_line 30
Command: config terminal_line 30

Success.

#
```

3.4.11 show terminal_line

目的	1 画面に表示できる行数を表示します。
構文	show terminal_line
説明	本コマンドは、画面に表示できるコマンドの行数を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:表示できる行数を表示するには

```
#show terminal_line
Command: show terminal_line

Terminal Line : 24 (Default)

#
```

3.4.12 show self-test result

目的	スイッチの起動時に実施された self test 結果を表示します。
構文	show self-test result
説明	本コマンドは、スイッチの起動時に実施された DRAM、FLASH メモリ、SW-LSI、PHY の self test 結果を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:self test 結果を表示するには

```
 #show self-test result
 Command: show self-test result


 Self-test Result
 ---------------------
 DRAM  Test : No error
 FLASH Test : No error
 SWLSI Test : No error
 PHY   Test : No error
 POE   Test : N/A


#
```

3.4.13 show sfp diag

目的	SFP の光送受信レベルを表示します。
構文	show sfp diag [<portlist>]
説明	本コマンドは、SFP の光送受信レベルを(dBm)単位で表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	SFF-8472 に準拠した SFP が対象です。型式(H-FX-SFP/R)は表示されません。
対応バージョン	1.00.00 以降

使用例:SFP ポートの光送受信レベルを表示するには

```
#show sfp diag
Command: show sfp diag

  Port         TX Power       RX Power
                 (dBm)          (dBm)
---------    ------------   ------------
   49           -6.41           -5.90
   50           -5.02           -7.20
   51
   52
#
```

3.4.14 show sfp info

目的	SFP のベンダー情報を表示します。
構文	show sfp info [<portlist>]
説明	本コマンドは、SFP のベンダー情報を表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:SFP ポートのベンダー情報を表示するには

```
#show sfp info 49
Command: show sfp info 49

SFP Port              : 49
Vendor Name           : FINISAR CORP.
Vendor Part Number    : FTLF8519P2BCL-EX
Serial Number         : PGK3GAF

#
```

3.4.15 config configuration config_id

目的	装置に設定するコンフィグレーションファイルを指定します。
構文	config configuration config_id < value 1-2 > < delete | boot_up | active >
説明	本コマンドは、2 つの保存されたコンフィグレーションで選択したセクション ID のファイル削除、次回起動で使用するセクション ID の指定、または現在のコンフィグレーションに置き換えを行います。
パラメーター	config_id < value 1-2 > - 対象とするコンフィグレーションのセクション ID を選択します。 delete - 選択したセクション ID のコンフィグレーションを削除します。 boot_up - 選択したセクション ID のコンフィグレーションで次回起動します。 active - 選択したセクション ID のコンフィグレーションを現在のコンフィグレーションに置き換えを行います。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:セクション ID 2 のコンフィグレーションファイルで次回起動するには

```
#config configuration config_id 2 boot_up
Command: config configuration config_id 2 boot_up

Success.

#
```

注意事項

パラメーターで active を選択した場合、選択したセクション ID のコンフィグレーションファイルを現在の設定に置き換えるため、リンクアップしているポートは一時切断されます。

3.5 コマンド履歴コマンド

3.5.1 ?

目的	コマンドラインインターフェース(CLI)におけるすべてのコマンドを表示します。
構文	? [<command>]
説明	本コマンドは、コマンドラインインターフェース(CLI)で利用可能なすべてのコマンドを表示します。
パラメーター	[<command>] - 適切なコマンドと共に「?」を入力すると、指定したコマンドに対するすべてのパラメーターの一覧がコマンド機能の簡単な説明とコマンド内に同じ用語を持つ類似のコマンドを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:CLI に含まれるすべてのコマンドを表示するには

```
#?


..
?
cable_diag ports
clear
clear arptable
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear dhcpv6 binding
clear fdb
clear log
clear mac_based_access_control auth_mac
clear port_security_entry port
clear utilization
clear web_authentication auth_state
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x authorization network radius
config 802.1x capability ports
config 802.1x fwd_pdu ports
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

使用例:特定のコマンドに対するパラメーターを表示するには

```
#? config account
Command:? config account

Command: config account
Usage: <username>
Description: Used to configure user accounts.

#
```

3.5.2 dir

目的	コマンドラインインターフェース(CLI)におけるすべてのコマンドを表示します。
構文	dir
説明	本コマンドは、コマンドラインインターフェース(CLI)で利用可能なすべてのコマンドを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:すべてのコマンドを表示するには

```
 #dir
 ..
 ?
 cable_diag ports
 clear
 clear arptable
 clear counters
 clear dhcp binding
 clear dhcp conflict_ip
 clear dhcpv6 binding
 clear fdb
 clear log
 clear mac_based_access_control auth_mac
 clear port_security_entry port
 clear utilization
 clear web_authentication auth_state
 config 802.1p default_priority
 config 802.1p user_priority
 config 802.1x auth_parameter ports
 config 802.1x auth_protocol
 config 802.1x authorization network radius
 config 802.1x capability ports
 config 802.1x fwd_pdu ports
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.5.3 config command_history

目的	コマンド履歴の表示件数を設定します。
構文	config command_history <value 1-40>
説明	本コマンドは、コマンド履歴の表示件数を設定します。
パラメーター	<value 1-40> - コマンド履歴を最大 40 件まで表示することができます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:コマンド履歴の表示件数を「20」に設定するには

```
#config command_history 20
Command: config command_history 20

Success.

#
```

3.5.4 show command_history

目的	コマンド履歴を表示します。
構文	show command_history
説明	本コマンドは、コマンド履歴を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:コマンド履歴を表示するには

```
#show command_history
Command: show command_history

?
? show
show vlan
show command history

#
```

3.6 LLDP コマンド

3.6.1 enable lldp

目的	スイッチの LLDP 機能を有効にします。
構文	enable lldp
説明	本コマンドは、LLDP 機能を有効にします。 本機能を有効にするとスイッチは、LLDP パケットの送受信を開始し、LLDP パケットの処理を行います。 各ポートの具体的な機能は、ポートごとの LLDP 設定に依存します。スイッチはポートを介して情報をネイバー装置に知らせます。 LLDP パケットを受信するためには、スイッチはネイバーデバイステーブル内のネイバーデバイスから通知された LLDP パケットより情報を学習します。 デフォルト設定は、「disable」(無効)です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:LLDP を有効にするには

```
#enable lldp
Command: enable lldp

Success.

#
```

3.6.2 disable lldp

目的	スイッチの LLDP 機能を無効にします。
構文	disable lldp
説明	本コマンドは、LLDP 通知パケットの送受信を中止します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:LLDP を無効にするには

```
# disable lldp
Command: disable lldp

Success.

#
```

3.6.3 config lldp message_tx_interval

目的	パケット送信間隔を変更します。
構文	config lldp message_tx_interval <sec 5-32768>
説明	本コマンドは、アクティブなポートがネイバーに通知する再送時間を指定します。
パラメーター	message_tx_interval - LLDP 通知の送信間隔を入力します。範囲は、5～32768 秒です。デフォルト値は、30 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:パケット送信間隔を「30」に設定するには

```
#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

#
```

3.6.4 config lldp message_tx_hold_multiplier

目的	本コマンドは、メッセージホールドマルチプライヤを設定します。
構文	config lldp message_tx_hold_multiplier <int 2-10>
説明	本コマンドは、LLDPDU での txTTL における TTL 値を計算するのに使用される 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）の小さい方になります。パートナースイッチでは、指定された通知の保持期間（TTL）の期限が来ると、通知データはネイバースイッチの MIB から削除されます。
パラメーター	message_tx_hold_multiplier - 値の範囲は、2～10 です。デフォルト値は 4 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:マルチプライヤの値を「3」に変更するには

```
#config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

#
```

3.6.5 config lldp tx_delay

目的	LLDP ポートの最短時間（遅延間隔）を変更します。 LLDP MIB コンテンツの変更のために、連続した LLDP 通知を遅延します。 「tx delay」は、MIB コンテンツの頻繁な変更のために LLDP メッセージを送信する最小間隔を定義します。
構文	config lldp tx_delay <sec 1-8192>
説明	LLDP message_tx_interval（送信間隔）は 4 x tx_delay（遅延間隔）以上である必要があります。
パラメーター	tx_delay – 値の範囲は、1 から 8192 秒です。デフォルト値は 2 秒です。 注意： Tx Delay は、0.25 * msgTxInterval 以下となる必要があります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:遅延時間を「8」設定するには

```
#config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

#
```

3.6.6 config lldp reinit_delay

目的	再初期化間隔の最小値を変更します。
構文	config lldp reinit_delay <sec 1-10>
説明	再度有効とされる LLDP ポートは、最後の「disable」(無効)コマンドの後、reinit_delay(再初期化遅延)時間待機します。
パラメーター	reinit_delay – 値の範囲は、1～10 秒です。デフォルト値は 2 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:再初期化遅延間隔を「5」に変更するには

```
#config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

#
```

3.6.7 config lldp notification_interval

目的	SNMP トラップレシーバに送信する LLDP 変更通知の送信タイマーを設定します。
構文	config lldp notification_interval <sec 5 - 3600>
説明	スイッチで生成される LLDP 変更通知の送信間隔を設定します。
パラメーター	notification_interval - 値の範囲は、5 秒～3600 秒です。デフォルト値は 5 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:通知間隔の値を「10」に変更するには

```
#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

#
```

3.6.8 config lldp ports notification

目的	SNMP トラップレシーバに送信する LLDP 変更通知のポートを設定します。
構文	config lldp ports < <portlist> | all > notification < enable | disable >
説明	LLDP のデータ変更が検出された場合、SNMP トラップレシーバへ変更通知の送信を「enable」(有効) または「disable」(無効)にします。変更の検出には、新しい有効な情報、タイムアウト情報、更新情報が含まれます。変更のタイプには、データの更新/挿入/削除が含まれます。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 notification - ネイバーのデバイスから受信した通知で検出された 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。 デフォルト設定は、「disable」(無効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1-5 の変更通知を有効にするには

```
#config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

#
```

3.6.9 config lldp ports admin_status

目的	各ポートの送信モードと受信モードを設定します。
構文	config lldp ports < <portlist> | all > admin_status < tx_only | rx_only | tx_and_rx | disable >
説明	本コマンドは、各ポートの LLDP パケットの送受信モードを設定します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 tx_only - 指定ポートは LLDP パケットを送信しますが、ネイバーデバイスからの入力側パケットはブロックします。 rx_only - 指定ポートはネイバーデバイスからの LLDP パケットを受信しますが、ネイバーデバイスへの出力側パケットはブロックします。 tx_and_rx - 指定ポートは LLDP パケットの送受信両方を行います。 disable - 指定ポートにおける LLDP パケットの送受信を無効にします。 各ポートステータスはデフォルトにより tx_and_rx になっています。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1-5 の送受信モードを設定するには

```
#config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

#
```

3.6.10 config lldp ports mgt_addr

目的	管理アドレスのインスタンスを表す通知用に指定されたポートを「enable」(有効)または「disable」(無効)にします。
構文	config lldp ports < <portlist> | all > mgt_addr ipv4 <ipaddr> < enable | disable >
説明	本コマンドは、システムの IP アドレスが指定ポートから通知される必要があるかどうかを指定します。レイヤ 3 デバイスでは、各管理アドレスを個別に指定できます。リストに追加される管理アドレスは、各管理アドレスに対応付けされた特定のインターフェースからの LLDP に通知されます。さらに、その管理アドレスのインターフェースは ifIndex 形式で通知されます。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 ipv4 - IPv4 の IP アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1-2 に対してアドレスエントリーの管理を有効にするには

```
#config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable
Command: config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable

Success

#
```

3.6.11 config lldp ports basic_tlvs

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上のオプションの TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> | all > basic_tlvs < all | < port_description | system_name | system_description | system_capabilities > > < enable | disable >
説明	スイッチのアクティブな LLDP ポートには、通常、出力側の通知に常に必須データを含んでいます。出力側 LLDP 通知からこれらのデータタイプを 1 個以上除外するために、個別のポートまたはポートグループに設定できる 4 つのオプションデータがあります。必須データタイプには、4 つの基本的な情報タイプ (end f LLDPDU TLV、chassis ID TLV、port ID TLV、Time to Live TLV) があります。必須データタイプを無効にすることはできません。さらに、オプションで選択可能な 4 つのデータタイプがあります。これらは、「port_description」、「system_name」、「system_description」、および「system_capability」です。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 port_description - この TLV のオプションデータタイプは、LLDP エージェントがポートの「Port Description TLV」を送信する必要があることを示します。 デフォルトでは無効になっています。 system_name - この TLV のオプションデータタイプは、LLDP エージェントが「System Name TLV」を送信する必要があることを示します。デフォルトでは無効になっています。 system_description - この TLV のオプションデータタイプは、LLDP エージェントが「System Description TLV」を送信する必要があることを示します。 デフォルトでは無効になっています。 system_capabilities - この TLV のオプションデータタイプは、LLDP エージェントが「System Capabilities TLV」を送信する必要があることを示します。 System capability は、デバイスがリピータ、ブリッジ、またはルーター機能を提供するかどうか、また提供された機能が現在有効であるかどうかを示します。 デフォルトでは無効になっています。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートに対して出力側の LLDP 通知から、システム名 TLV を除外するには

```
#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

#
```

3.6.12 config lldp ports dot1_tlv_pvid

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.1 準拠のポート VLAN ID TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> | all > dot1_tlv_pvid < enable | disable >
説明	この TLV のオプションのデータタイプは、IEEE 802.1 準拠のポート VLAN TLV 送信が指定した LLDP 送信が可能なポートに許可されるかどうかを決定します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 dot1_tlv_pvid - この TLV のオプションのデータタイプは、IEEE 802.1 準拠のポート VLAN ID TLV 送信が指定した LLDP 送信が可能なポートに許可されるかどうかを決定します。デフォルトでは「disable」(無効)になっています。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートに対して出力側の LLDP 通知から VLAN 名 TLV を設定するには

```
#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

#
```

3.6.13 config lldp ports dot1_tlv_protocol_vid

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.1 準拠のプロトコルアイデンティティ TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> | all > dot1_tlv_protocol_vid < vlan < all | < vlan_name 32 > > | vlanid <vlanid_list> > < enable | disable >
説明	この TLV のオプションのデータタイプは、対応するローカルシステムのプロトコルアイデンティティのインスタンスがポートに送信されるかどうかを示します。 プロトコルアイデンティティ TLV は、ステーションにネットワークの操作に重要なプロトコルを通知する方法を提供します。スパニングツリープロトコル、リンクアグリゲーション制御プロトコルおよび多数のベンダが所有するプロトコルのバリエーションは、ネットワークのトポロジーと接続性を保持する責任があります。 指定ポートで EAPOL、GVRP、STP (MSTP を含む)、および LACP プロトコルアイデンティティを有効にすると、通知が有効になり、このプロトコルアイデンティティは通知を送信します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 dot1_tlv_protocol_vid - この TLV のオプションのデータタイプは、IEEE 802.1 準拠のポート VLAN ID TLV 送信が指定した LLDP 送信が可能なポートに許可されるかどうかを決定します。デフォルト設定は「disable」(無効)です。 vlanid_list - このコマンド用に設定される VLAN ID のリストを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートに対して出力側の LLDP 通知から VLAN 名 TLV を設定するには

```
#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

#
```

3.6.14 config lldp ports dot1_tlv_vlan_name

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.1 準拠の VLAN 名 TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> | all > dot1_tlv_vlan_name < vlan < all | <vlan_name 32> > | vlanid <vidlist> > < enable | disable >
説明	この TLV のオプションのデータタイプは、対応するローカルシステムの VLAN 名のインスタンスがポートに送信されるかどうかを示します。 ポートが複数の VLAN に対応付けされた場合、有効な VLAN ID が通知されます。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 dot1_tlv_vlan_name - この TLV のオプションのデータタイプは、対応するローカルシステムの VLAN 名のインスタンスがポートに送信されるかどうかを示します。 ポートが複数の VLAN に対応付けされた場合、有効な VLAN ID が通知されます。 デフォルト設定は、「disable」(無効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートに対して出力側の LLDP 通知から VLAN 名 TLV を設定するには

```
#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.

#
```

3.6.15 config lldp ports dot1_tlv_protocol_identity

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.1 準拠のプロトコルアイデンティティ TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> | all > dot1_tlv_ protocol_identity < all | [eapol | lacp | gvrp | stp] > <enable | disable>
説明	この TLV のオプションのデータタイプは、対応するローカルシステムのプロトコルアイデンティティのインスタンスがポートに送信されるかどうかを示します。 プロトコルアイデンティティ TLV は、ステーションにネットワークの操作に重要なプロトコルを通知する方法を提供します。 スパニングツリープロトコル、リンクアグリゲーション制御プロトコルおよび多数のベンダが所有するプロトコルのバリエーションは、ネットワークのトポロジーと接続性を保持する責任があります。 指定ポートで EAPOL、GVRP、STP (MSTP を含む) 、および LACP プロトコルアイデンティティを有効にすると、通知が有効になり、このプロトコルアイデンティティは通知を送信します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。dot1_tlv_protocol_identity - この TLV のオプションのデータタイプは、対応するローカルシステムのプロトコルアイデンティティのインスタンスがポートに送信されるかどうかを示します。 プロトコルアイデンティティ TLV は、ステーションにネットワークの操作に重要なプロトコルを通知する方法を提供します。 スパニングツリープロトコル、リンクアグリゲーション制御プロトコルおよび多数のベンダが所有するプロトコルのバリエーションは、ネットワークのトポロジーと接続性を保持する責任があります。 指定ポートで EAPOL、GVRP、STP (MSTP を含む) 、および LACP プロトコルアイデンティティを有効にすると、通知が有効になり、このプロトコルアイデンティティは通知を送信します。 デフォルト設定は、「disable」(無効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートに出力側の LLDP 通知からプロトコルアイデンティティ TLV を設定するには

```
#config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success

#
```

3.6.16 config lldp ports dot3_tlvs

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.3 準拠の組織固有の TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> | all > dot3_tlvs < all | [mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size] > < enable | disable >
説明	この TLV のオプションの各 TLV を個別に有効にすることができます。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 mac_phy_configuration_status - この TLV の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'を送信する必要があることを示します。このタイプは、IEEE 802.3 リンクの 2 つの終端が異なるデュプレックスおよび/または速度設定で、何らかの限定的なネットワークの接続性を確立することが可能であることを示しています。詳しく説明すると、情報はポートがオートネゴシエーション機能をサポートしているかどうか、機能が有効であるかどうか、自動通知機能、および操作可能な MAU タイプを含みます。デフォルトでは無効になっています。 link_aggregation - この TLV のオプションデータタイプは、LLDP エージェントが「Link Aggregation TLV」を送信する必要があることを示します。このタイプは IEEE 802.3 MAC におけるリンクアグリゲーションステータスを示します。情報は、ポートがリンクアグリゲーションできるかどうか、ポートが集約した 1 つのリンクにまとめられるかどうか、および束ねられたポートの ID を持っている必要があります。デフォルトでは無効になっています。 power_via_mdi -この TLV のオプションデータタイプは、 LLDP エージェントが「MDI TLV」を送信する必要があることを示します。3 つの IEEE 802.3 PMD（10BASE-T、100BASE-TX および 1000BASE-T）では、接続された未供給のシステムにリンク上で電力を供給することができます。MDI TLV 経由の電力供給により、ネットワーク管理で送信する IEEE 802.3 LAN ステーションの MDI パワーサポート機能をアドバタイズし検出することができます。デフォルトでは無効になっています。 maximum_frame_size - この TLV のオプションデータタイプは、LLDP エージェントが「Maximum-frame-size TLV」を送信する必要があることを示します。 デフォルト設定は、「disable」(無効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートに対して出力側の LLDP 通知から MAC/PHY 設定/ステータスを設定するには

```
#config lldp ports all dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

#
```

3.6.17 config lldp forward_message

目的	LLDP が無効の際の LLDP DU パケットの転送を設定します。
構文	config lldp forward_message < enable | disable >
説明	LLDP を無効にして、LLDP forward message を有効にしたとき、受信された LLDP DU パケットを転送します。デフォルト設定は、「disable」(無効)です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:LLDP forward LLDP DU を設定するには

```
#config lldp forward_ message enable
Command: config lldp forward_ message  enable

Success.

#
```

3.6.18 show lldp

目的	本コマンドは、スイッチの通常の LLDP 設定ステータスを表示します。
構文	show lldp
説明	本コマンドは、スイッチの通常の LLDP 設定ステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:LLDP 設定ステータスを表示するには

```
#show lldp
Command: show lldp

LLDP System Information
    Chassis Id Subtype        : MAC Address
    Chassis Id                : 00-40-66-00-24-00
    System Name               :
    System Description        : Gigabit Ethernet Switch
    System Capabilities       : Repeater, Bridge

LLDP Configurations
    LLDP Status               : Disable
    LLDP Forward Status       : Disable
    Message Tx Interval       : 30
    Message Tx Hold Multiplier: 4
    ReInit Delay              : 2
    Tx Delay                  : 2
    Notification Interval     : 5
#
```

3.6.19 show lldp mgt_addr

目的	LLDP の管理アドレス情報を表示します。
構文	show lldp mgt_addr [ipv4 <ipaddr>]
説明	本コマンドは、LLDP の管理アドレス情報を表示します。
パラメーター	ipv4 - 対象の IPv4 の IP アドレスを入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:管理アドレス情報を表示するには

```
#show lldp mgt_addr ipv4 192.168.254.10
Command: show lldp mgt_addr ipv4 192.168.254.10

Address 1 :
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 192.168.254.10
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.278.1.35.106
    Advertising Ports                :

#
```

3.6.20 show lldp ports

目的	LLDP 通知オプションをポート設定ごとに表示します。
構文	show lldp ports [<portlist>]
説明	本コマンドは、LLDP 通知オプションをポート設定ごとに表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。 ポートリストを指定しない場合、すべてのポートの情報が表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポートの TLV オプション設定ごとに LLDP を表示するには

```
# show lldp ports 1
Command: show lldp ports 1

Port ID                 : 1
------------------------------------------------------------------
Admin Status            : TX_and_RX
Notification Status     : Disable
Advertised TLVs Option  :
    Port Description                                    Disable
    System Name                                         Disable
    System Description                                  Disable
    System Capabilities                                 Disable
    Enabled Management Address
        (NONE)
    Port VLAN ID                                        Disable
    Enabled Port_and_Protocol_VLAN_ID
        (NONE)
    Enabled VLAN Name
        (NONE)
    Enabled Protocol_Identity
        (NONE)
    MAC/PHY Configuration/Status                        Disable
    Link Aggregation                                    Disable
    Maximum Frame Size                                  Disable

#
```

3.6.21 show lldp local_ports

目的	出力側の LLDP 通知を組み込むためにポートごとの情報を表示します。
構文	show lldp local_ports [<portlist>] [mode < brief | normal | detailed >]
説明	本コマンドは、出力側の LLDP 通知を組み込むためにポートごとの情報を表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。 ポートリストを指定しない場合、すべてのポートの情報が表示されます。 brief - brief(簡易)モードにおける情報を表示します。 normal - normal(通常)モードの情報を表示します。これはデフォルト値の表示モードです。 detailed - detailed(詳細)モードにおける情報を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:各ポートの外出力側 LLDP 通知を detailed(詳細) モードで表示するには

```
 #show lldp local_ports 1 mode detailed
 Command: show lldp local_ports 1 mode detailed

 Port ID : 1
 ------------------------------------------------------------------------------
 Port Id Subtype                          : Local
 Port ID                                  : 1/1
 Port Description                         : APRESIA Systems ApresiaLightGM15
                                            2GT R1.03 Port 1
 Port PVID                                : 1
 Management Address Count                 : 1
         Subtype                          : IPv4
         Address                          : 192.168.70.123
         IF Type                          : IfIndex
         OID                              : 1.3.6.1.4.1.278.1.35.111

PPVID Entries Count                       : 0
    (NONE)
VLAN Name Entries Count                   : 1
    Entry 1 :
        Vlan ID                           : 1
        Vlan Name                         : default

Protocol Identity Entries Count           : 0
    (NONE)
MAC/PHY Configuration/Status              :
    Auto-negotiation Support              : Supported
    Auto-negotiation Enabled              : Enabled
    Auto-negotiation Advertised Capability : 6c01(hex)
    Auto-negotiation Operational MAU Type  : 001b(hex)

Power Via MDI                             : Not Supported

Link Aggregation                          :
    Aggregation Capability                : Aggregated
    Aggregation Status                    : Not Currently in Aggregation
    Aggregation Port ID                   : 0

Maximum Frame Size                        : 12284

#
```

使用例:特定ポートの出力側 LLDP 通知を normal（通常）モードで表示するには

```
#show lldp local_ports 1 mode normal
Command: show lldp local_ports 1 mode normal

Port ID : 1
------------------------------------------------------------------------
Port Id Subtype                          : Local
Port Id                                  : 1/1
Port Description                         : APRESIA Systems ApresiaLightGM15
                                           2GT R1.03 Port 1
Port VLAN ID                             : 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)
Power Via MDI                            : (See detail)
Link Aggregation                         : (See detail)
Maximum Frame Size                       : 12284

#
```

使用例:特定ポートの出力側 LLDP 通知を brief（簡易）モードで表示するには

```
#show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief

Port ID : 1
------------------------------------------------------------------------
Port Id Subtype                          : Local
Port Id                                  : 1/1
Port Description                         : APRESIA Systems ApresiaLightGM15
                                           2GT R1.03 Port 1
#
```

3.6.22 show lldp remote_ports

目的	ネイバーから得た情報を表示します。
構文	show lldp remote_ports [<portlist>] [mode < brief | normal | detailed >]
説明	本コマンドは、ネイバーのパラメーターから得た情報を表示します。 32 個の VLAN 名エントリーと 10 個の管理アドレスエントリーを受信できます。
パラメーター	<portlist> - 表示するポート範囲を指定します。 ポートリストを指定しない場合、すべてのポートの情報が表示されます。 brief - brief(簡易)モードにおける情報を表示します。 normal - normal(通常)モードの情報を表示します。これはデフォルト値の表示モードです。 detailed - detailed(詳細)モードにおける情報を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:リモートテーブルエントリーを brief（簡易）モードで表示するには

```
#show lldp remote_ports 1 mode brief
Command: show lldp remote_ports 1 mode brief

Port ID : 1
------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis Id Subtype                      : MAC Address
    Chassis Id                              : 00-40-66-10-27-00
    Port Id Subtype                         : Local
    Port ID                                 : 1/1
    Port Description                        :

#
```

使用例:リモートテーブルエントリーを normal（通常）モードで表示するには

```
#show lldp remote_ports ports 1 mode normal
Command: show lldp remote_ports ports 1 mode normal

Port ID : 1
------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis Id Subtype                      : MAC Address
    Chassis Id                              : 00-40-66-10-27-00
    Port Id Subtype                         : Local
    Port ID                                 : 1/1
    Port Description                        :
    System Name                             :
```

```
    System Description                      : Gigabit Ethernet Switch
    System Capabilities                     : Repeater, Bridge
    Management Address Count                : 0
    Port VLAN ID                            : 0
    PPVID Entries Count                     : 0
    VLAN Name Entries Count                 : 0
    Protocol ID Entries Count               : 0
    MAC/PHY Configuration/Status            : (None)
    Power Via MDI                           : (None)
    Link Aggregation                        : (None)
    Maximum Frame Size                      : 0
    Unknown TLVs Count                      : 0

#
```

使用例:リモートテーブルエントリーを detailed（詳細）モードで表示するには

```
#show lldp remote_ports 1 mode detailed
Command: show lldp remote_ports 1 mode detailed

Port ID : 1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis Id Subtype                      : MAC Address
    Chassis Id                              : 00-40-66-10-27-00
    Port Id Subtype                         : Local
    Port ID                                 : 1/1
    Port Description                        :
    System Name                             :
    System Description                      :
    System Capabilities                     :
    Management Address Count                : 0
        (None)

    Port PVID                               : 0
    PPVID Entries Count                     : 0
        (None)

    VLAN Name Entries Count                 : 0
        (None)

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.6.23 show lldp statistics

目的	システムの LLDP 統計情報を表示します。
構文	show lldp statistics
説明	本コマンドは、スイッチのネイバーデバイスのアクティビティ概要を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:グローバル統計情報を表示するには

```
#show lldp statistics
Command: show lldp statistics

Last Change Time           : 6094
Number of Table Insert     : 1
Number of Table Delete     : 0
Number of Table Drop       : 0
Number of Table Ageout     : 0

#
```

3.6.24 show lldp statistics ports

目的	ポートの LLDP 統計情報を表示します。
構文	show lldp statistics ports [<portlist>]
説明	本コマンドは、ポートごとの LLDP 統計を表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 1 の統計情報を表示するには

```
#show lldp statistics ports 1
Command: show lldp statistics ports 1
Port ID: 1
----------------------------------------------------------
        lldpStatsTxPortFramesTotal           : 27
        lldpStatsRxPortFramesDiscardedTotal  : 0
        lldpStatsRxPortFramesErrors          : 0
        lldpStatsRxPortFramesTotal           : 27
        lldpStatsRxPortTLVsDiscardedTotal    : 0
        lldpStatsRxPortTLVsUnrecognizedTotal : 0
        lldpStatsRxPortAgeoutsTotal          : 0
#
```

3.7 バナーとプロンプトの編集コマンド

3.7.1 config command_prompt

目的	コマンドプロンプトを設定します。
構文	config command_prompt 〈〈string 16〉	username	default 〉
説明	本コマンドを使用してコマンドプロンプトを変更します。
パラメーター	string 16 - 半角英数字 16 文字以内の新しい名前を入力することで、コマンドプロンプトを変更します。 username - コマンドプロンプトをログインユーザー名に変更します。 default - 工場出荷時コマンドプロンプトにリセットします。
制限事項	管理者アカウントのみ本コマンドを実行できます。 他の制限は以下の通りです。 「reset」コマンドが実行されると、変更されたコマンドプロンプトは変更された状態を維持します。 ただし、「reset config/reset system」コマンドが実行されると、コマンドプロンプトは工場出荷時のバナーにリセットされます。
対応バージョン	1.00.00 以降

使用例:コマンドプロンプトを「APS」に変更するには

```
#config command_prompt APS
Command: config command_prompt APS

Success.

APS#
```

3.7.2 config greeting_message

目的	ログインバナーを設定します。
構文	config greeting_message [default]
説明	本コマンドは、ログインバナーを設定します。
パラメーター	default - default を入力すると、バナーコマンドを変更し、バナーは工場出荷時設定のバナーにリセットされます。 バナーエディタを開くには、「config greeting_message」 コマンドの後で、<Enter>をクリックします。 情報を入力し、バナーエディタに記述されているコマンドを使用してバナーを表示します。 Quit without save: Ctrl+C Save and quit: Ctrl+W Move cursor: Left/Right/Up/Down Delete line: Ctrl+D Erase all setting: Ctrl+X Reload original setting: Ctrl+L
制限事項	管理者アカウントのみ本コマンドを実行できます。 他の制限は以下の通りです。 「reset」コマンドが実行されると、変更されたバナーは変更された状態を維持します。ただし、「reset config/reset system」コマンドが実行される

	と、変更されたバナーは工場出荷時のバナーにリセットされます。 バナーの最大容量は、6 行*80 文字/各行です。(1 行に 80 文字で 6 行まで)。 Ctrl+W は DRAM に変更されたバナーを保存するだけです。「save config/save all」コマンドをタイプしてフラッシュメモリーに保存する必要があります。 閾値内でのみ有効です。
対応バージョン	1.00.00 以降

使用例:バナーを編集するには

```
#config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================================

                ApresiaLightGM152GT Gigabit Ethernet Switch
                        Command Line Interface

                              Firmware: 1.03.00
        Copyright(C) 2020 APRESIA Systems, Ltd. All rights reserved.
================================================================================

   <Function Key>                  <Control Key>
   Ctrl+C     Quit without save    left/right/
   Ctrl+W     Save and quit          up/down     Move cursor
                                   Ctrl+D        Delete line
                                   Ctrl+X        Erase all setting
                                   Ctrl+L        Reload original setting
--------------------------------------------------------------------------------
```

3.7.3 show greeting_message

目的	スイッチに現在設定されているログインバナーを表示します。
構文	show greeting_message
説明	本コマンドは、スイッチに現在設定されているのログインバナーを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:現在、設定されているログインバナーを表示するには

```
#show greeting_message
Command: show greeting_message

================================================================================

                ApresiaLightGM152GT Gigabit Ethernet Switch
                        Command Line Interface

                             Firmware: 1.03.00
        Copyright(C) 2020 APRESIA Systems, Ltd. All rights reserved.
================================================================================

#
```

3.8 ネットワーク管理（SNMP）コマンド

本スイッチは、Simple Network Management Protocol（SNMP）バージョン1、2cおよび3をサポートしています。ユーザーは、SNMPのどのバージョンでスイッチを監視および制御するか指定できます。 SNMPの3つのバージョンは、管理ステーションとネットワークデバイス間に提供するセキュリティーレベルが異なります。 SNMPバージョンのセキュリティー機能は以下の表の通りです。

SNMPバージョン	認証方法	説明
v1	コミュニティー文字列	コミュニティー文字列は認証に使用されます- NoAuthNoPriv
v2c	コミュニティー文字列	コミュニティー文字列は認証に使用されます- NoAuthNoPriv
v3	ユーザー名	ユーザー名は認証に使用されます- NoAuthNoPriv
v3	MD5またはSHA	認証はHMAC-MD5またはHMAC-SHAアルゴリズムに基づいて行われます- AuthNoPriv
v3	MD5 DESまたはSHA DES	認証はHMAC-MD5またはHMAC-SHAアルゴリズムに基づいて行われます- AuthPriv DES 56ビット暗号方式がCBC-DES(DES-56)標準規格に基づいて追加されます

3.8.1 create snmp user

目的	新しいSNMPユーザーを作成し、作成したSNMPグループにユーザーを追加します。
構文	create snmp user <SNMP_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 < md5 <auth_key 32-32> | sha <auth_key 40-40> > priv < none | des <priv_key 32-32> > >]
説明	本コマンドは、新しいSNMPユーザーを作成し、作成したSNMPグループにユーザーを追加します。SNMPは以下の項目を保証します。 メッセージの保全- パケットが送信中に変更されていないことを保証します。 認証- SNMPメッセージが有効な送信元から来ているかどうかを判断します。 暗号化- 未認証の送信元に参照されることを防ぐために、メッセージの内容にスクランブルをかけます。
パラメーター	<SNMP_name 32> - 新しいSNMPユーザーを識別する半角英数字32文字以内の名前を入力します。 <groupname 32> - 新しいSNMPユーザーが対応付けされるSNMPグループを識別する半角英数字32文字以内の名前を入力します。 encrypted - SNMPを使用した認証のタイプを選択します。 ユーザーは以下の選択ができます。 by_password - 認証とプライバシーのためにSNMPユーザーにパスワードを入力するように要求します。パスワードは、以下で「auth_password」を指定することによって定義されます。セキュリティ上、この方式を推奨します。 by_key - 認証とプライバシーのためにSNMPユーザーに暗号化キーを入力するように要求します。キーは、16進形式により指定することによって定義されます。 セキュリティ上、この方式は推奨いたしません。

パラメーター	auth - SNMP ユーザーを認証するために使用される認証アルゴリズムのタイプを選択します。 以下の選択があります。 md5 - HMAC-MD5-96 認証レベルを指定します。md5 は、以下の 1 つを入力することによって、利用されます。 <auth password 8-16> - ホストに対するパケットが受信できるようエージェントを認可するために使用される半角英数字 8～16 文字列。 <auth_key 32-32> - ホストに対するパケットが受信できるようエージェントを認可するために使用される半角英数字 32 文字の文字列を 16 進数形式で入力します。 sha - HMAC-SHA-96 認証レベルを使用します。 <auth password 8-20> - ホストに対するパケットが受信できるようエージェントを認可するために使用される半角英数字 8～20 文字の文字列。 <auth_key 40-40> - ホストに対するパケットが受信できるようエージェントを認可するために使用される半角英数字 40 文字のキーを 16 進数形式で入力します。 priv - priv (プライバシー)パラメーターを追加すると、より高いセキュリティーために認証アルゴリズムに加えて、暗号化も可能になります。 ユーザーは以下の選択ができます。 des - 本パラメーターを追加すると、56 ビットの暗号化のための DES-56 標準の使用が可能となります。 <priv_password 8-16> - ホストがエージェントに送信するメッセージの内容を暗号化するために使用する半角英数字 8～16 文字の文字列。 <priv_key 32-32> - ホストがエージェントに送信するメッセージの内容を暗号化するために使用される半角英数字 32 文字のキーを 16 進数形式で入力します。 none - 本パラメーターを追加すると、暗号化を行いません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの SNMP ユーザーを作成するには

```
#create snmp user APS default encrypted by_password auth md5 knickerbockers priv none
Command: create snmp user APS default encrypted by_password auth md5 knickerbockers priv
none

Success.

#
```

3.8.2 delete snmp user

目的	SNMP グループから SNMP ユーザーを削除し、また対応付けされた SNMP グループも削除します。
構文	delete snmp user <SNMP_name 32>
説明	本コマンドは、SNMP グループから SNMP ユーザーを削除し、また対応付けされた SNMP グループも削除します。
パラメーター	<SNMP_name 32> - 削除される SNMP ユーザーを識別する半角英数字 32 文字以内の文字列を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチに入力済みの SNMP ユーザーを削除するには

```
#delete snmp user APS
Command: delete snmp user APS

Success.

#
```

3.8.3 show snmp user

目的	SNMP グループのユーザー名テーブル内の各 SNMP ユーザー名に関する情報を表示します。
構文	show snmp user
説明	本コマンドは、SNMP グループのユーザー名テーブル内の各 SNMP ユーザー名に関する情報を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている SNMP ユーザーを表示するには

```
#show snmp user
Command: show snmp user

Username         Group Name       SNMP Version Auth-Protocol PrivProtocol
---------------  ---------------  ------------ ------------- ------------
initial          initial          V3            None           None

Total Entries: 1

#
```

3.8.4 create snmp view

目的	MIB オブジェクトと SNMP マネージャーのアクセスを制限するために、コミュニティー文字列にビューを割り当てます。
構文	create snmp view <view_name 32> <oid> view_type < included | excluded >
説明	本コマンドは、MIB オブジェクトと SNMP マネージャーのアクセスを制限するために、コミュニティー文字列にビューを割り当てます。
パラメーター	<view_name 32> - 作成する SNMP ビューを識別する文字列を入力します。 <oid> - SNMP マネージャーからアクセスのオブジェクトツリー(MIB ツリー)を識別するオブジェクト ID を入力します。 view type - 以下のビュータイプを選択します。 included - SNMP マネージャーからアクセスのオブジェクトリストにこのオブジェクト ID を含めます。 excluded - SNMP マネージャーからアクセスのオブジェクトリストにこのオブジェクト ID を除外します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP ビューを作成するには

```
#create snmp view APS 1.3.6 view_type included
Command: create snmp view APS 1.3.6 view_type included

Success.

#
```

3.8.5 delete snmp view

目的	スイッチに作成済の SNMP ビューエントリーを削除します。
構文	delete snmp view <view_name 32> < all | <oid> >
説明	本コマンドは、スイッチに作成済の SNMP ビューエントリーを削除します。
パラメーター	<view_name 32> - 削除する SNMP ビューを入力します。 all - 削除するスイッチの SNMP ビューすべてが指定されます。 <oid> - 削除する MIB のオブジェクト ID を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:設定済みの SNMP ビューをスイッチから削除するには

```
#delete snmp view APS all
Command: delete snmp view APS all

Success.

#
```

3.8.6 show snmp view

目的	スイッチに作成済みの SNMP ビューを表示します。
構文	show snmp view [<view_name 32>]
説明	本コマンドは、スイッチに作成済みの SNMP ビューエントリーを表示します。
パラメーター	<view_name 32> - 表示される SNMP ビューを識別する半角英数字 32 文字以内の文字列を入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:SNMP ビュー設定を表示するには

```
#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

#
```

3.8.7 create snmp community

目的	SNMP マネージャーとエージェントとの関係を定義するために SNMP コミュニティーの文字列を作成します。コミュニティー文字列は、スイッチ上のエージェントへのアクセスを行う際のパスワードのような役割をします。 以下の特性はコミュニティー文字列に対応付けできます。 SNMP コミュニティーにアクセス可能な全 MIB オブジェクトのサブセットを定義する MIB ビュー。 SNMP コミュニティーにアクセス可能な MIB オブジェクトには、「read_write」（読み書き可能）または「read_only」(読み出しのみ)レベルがあります。
構文	create snmp community <community_string 32> view <view_name 32> < read_only | read_write >
説明	本コマンドは、SNMP コミュニティー文字列を作成し、このコミュニティー文字列にアクセス制限を行う文字列を割り当てます
パラメーター	<community_string 32> - SNMP コミュニティーのメンバーを識別する 32 文字までの半角英数文字列を入力します。 この文字列は、リモートの SNMP マネージャーが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。 view <view_name 32> - リモート SNMP マネージャーがスイッチにアクセスできる MIB オブジェクトのグループの識別に使用される 32 文字までの半角英数文字列を入力します。 read_only - 本コマンドで作成されたコミュニティー文字列を使用し、SNMP コミュニティーのメンバーはスイッチの MIB コンテンツを読み出しのみできます。 read_write - 本コマンドで作成されたコミュニティー文字列を使用し、SNMP コミュニティーメンバーはスイッチの MIB コンテンツを読み書きできます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP コミュニティー文字列「APS」を作成するには

```
#create snmp community APS view ReadView read_write
Command: create snmp community APS view ReadView read_write

Success.

#
```

3.8.8 delete snmp community

目的	スイッチから特定の SNMP コミュニティー文字列を削除します。
構文	delete snmp community <community_string 32>
説明	本コマンドは、スイッチから定義済みの SNMP コミュニティー文字列を削除します。
パラメーター	<community_string 32> - SNMP コミュニティーのメンバを識別する 32 文字までの半角英数文字列を入力します。この文字列は、リモートの SNMP マネージャーが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP コミュニティー文字列「APS」を削除するには

```
#delete snmp community APS
Command: delete snmp community APS

Success.

#
```

注意事項

工場出荷時の設定状態においては、コミュニティー名が一致する全ての SNMP マネージャーからのアクセスが許可されます。SNMP 機能を使用しない場合、delete snmp community、delete snmp user 設定を行なう必要があります。

3.8.9 show snmp community

目的	スイッチに設定されている SNMP コミュニティー文字列を表示します。
構文	show snmp community [<community_string 32>]
説明	本コマンドは、スイッチから定義済みのコミュニティー名を削除します。
パラメーター	<community_string 32> - SNMP コミュニティーのメンバを識別する 32 文字までの半角英数文字列を入力します。この文字列は、リモートの SNMP マネージャーが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:入力した SNMP コミュニティー文字列を表示するには

```
#show snmp community APS
Command: show snmp community APS

SNMP Community Table

Community Name        View Name                Access Right
------------------    --------------------     ------------
APS                   ReadView                 read_write
#
```

3.8.10 config snmp engineID

目的	スイッチの SNMP エンジンの識別子を設定します。
構文	config snmp engineID <snmp_engineID 10-64>
説明	本コマンドは、スイッチの SNMP エンジンの識別子を設定します。
パラメーター	<snmp_engineID 10-64> - スイッチの SNMP エンジンを指定する半角英数字の文字列を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの SNMP engineID に「0035636666」を付与するには

```
#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

#
```

3.8.11 show snmp engineID

目的	スイッチの SNMP エンジンの識別子を表示します。
構文	show snmp engineID
説明	本コマンドは、スイッチの SNMP エンジンの識別子を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチの SNMP engineID を表示するには

```
#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 800001160300406671fa2a

#
```

3.8.12 create snmp group

目的	新しい SNMP グループまたは SNMP ビューに SNMP ユーザーをマッピングするテーブルを作成します。
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> >
説明	本コマンドは、SNMP ビューに SNMP ユーザーをマッピングする新しい SNMP グループまたはテーブルを作成します。
パラメーター	<groupname 32> - 新しい SNMP ユーザーが対応付けされる SNMP グループを識別する半角英数字 32 文字以内の名前を入力します。 v1 - SNMP バージョン 1 を使用する場合に指定します。 Simple Network Management Protocol(SNMP)バージョン 1 は、モニタする手段と制御ネットワークデバイスを提供するネットワーク管理プロトコルです。 v2c- SNMP バージョン 2 を使用する場合に指定します。 SNMP v2c は、ネットワークマネジメント管理を中央に集結して、提供します。 SMI (Structure of Management Information) およびセキュリティー機能において強化されています。 v3 - SNMP バージョン 3 を使用する場合に指定します。 SNMP v3 は、ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。 SNMP v3 では以下のパラメーターが追加されます。 メッセージの保全- パケットが送信中に変更されていないことを保証します。 認証- SNMP メッセージが有効な送信元からのものかどうかを判断します。 暗号化- 未認証の送信元に参照されることを防ぐために、メッセージの内容にスクランブルをかけます。 noauth_nopriv - スイッチとリモート SNMP マネージャー間に送信されるパケットには認証及び暗号化は行われません。 auth_nopriv - スイッチとリモート SNMP マネージャー間には認証が必要ですが、送信パケットは暗号化されません。 auth_priv - スイッチとリモート SNMP マネージャー間には認証と送信パケットの暗号化が必要です。 read_view - 作成された SNMP グループが、SNMP メッセージを要求する場合に指定します。 write_view - 作成された SNMP グループに、書き込み権を持たせる場合に指定します。 notify_view - 作成された SNMP グループが、スイッチの SNMP エージェントによって生成された SNMP トラップメッセージを受信する場合に指定します。 view <view_name 32> - リモート SNMP マネージャーがスイッチにアクセスできる MIB オブジェクトのグループの識別に使用される 32 文字までの半角英数文字列を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP グループ名「APS」を作成するには

```
#create snmp group APS v3 noauth_nopriv read_view v1 write_view v1 notify_view v1
Command: create snmp group APS v3 noauth_nopriv read_view v1 write_view v1 notify_view v1

Success.

#
```

3.8.13 delete snmp group

目的	スイッチから SNMP グループを削除します。
構文	delete snmp group <groupname 32>
説明	本コマンドは、スイッチから SNMP グループを削除します。
パラメーター	<groupname 32> - 新しい SNMP ユーザーが対応付けされる SNMP グループを識別する半角英数字 32 文字以内の名前を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:「APS」という名前の SNMP グループを削除するには:

```
#delete snmp group APS
Command: delete snmp group APS

Success.

#
```

3.8.14 show snmp groups

目的	スイッチに現在設定されている SNMP グループのグループ名を表示します。また、各グループのセキュリティーモデル/レベルおよびステータスを表示します。
構文	show snmp groups
説明	本コマンドは、スイッチに現在設定されている SNMP グループのグループ名を表示します。 また、各グループのセキュリティーモデル/レベルおよびステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている SNMP グループを表示するには

```
#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group    Name    : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv1
Securiy Level    : NoAuthNoPriv

Group    Name    : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv2
Securiy Level    : NoAuthNoPriv

Group    Name    : initial
ReadView Name    : restricted
WriteView Name   :
Notify View Name : restricted
Securiy Model    : SNMPv3
Securiy Level    : NoAuthNoPriv

Group    Name    : private
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Securiy Model    : SNMPv1
Securiy Level    : NoAuthNoPriv

Group    Name    : private
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Securiy Model    : SNMPv2
Securiy Level    : NoAuthNoPriv

Total Entries: 5

#
```

3.8.15 create snmp host

目的	スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を作成します。
構文	create snmp < host <ipaddr> | v6host <ipv6addr > > < v1 | v2c | v3 < noauth_nopriv | auth_nopriv | auth_priv > <auth_string 32>
説明	本コマンドは、スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を作成します。
パラメーター	<ipaddr> - SNMP トラップの送信先 IP アドレスを入力します v6host <v6addr> - SNMP トラップの送信先 IPv6 アドレスを入力します v1 - SNMP バージョン 1 を使用する場合に指定します。 v2c- SNMP バージョン 2c を使用する場合に指定します。 v3 - SNMP バージョン 3 を使用する場合に指定します。 SNMP v3 は、ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。 SNMP v3 以下のパラメーターを追加します。 メッセージの保全- パケットが送信中に変更されていないことを保証します。 認証- SNMP メッセージが有効な送信元から来ているかどうかを判断します。 暗号化- 未認証の送信元に参照されることを防ぐために、メッセージの内容にスクランブルをかけます。 noauth_nopriv - スイッチとリモート SNMP マネージャー間に送信されるパケットには認証及び暗号化は行われません。 auth_nopriv - スイッチとリモート SNMP マネージャー間には認証は必要ですが、送信パケットは暗号化されません。 auth_priv - スイッチとリモート SNMP マネージャー間および送信パケットは認証と暗号化が必要です。 <auth_string 32> - スイッチの SNMP エージェントをアクセスするためにリモート SNMP マネージャーを認証する半角英数文字列を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP メッセージを受信する SNMP ホストを作成するには

```
#create snmp host 10.48.74.100 v3 auth_priv public
Command: create snmp host 10.48.74.100 v3 auth_priv public

Success.

#
```

3.8.16 delete snmp host

目的	スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を削除します。
構文	delete snmp < host <ipaddr> | v6host <ipv6addr >>
説明	本コマンドは、スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を削除します。
パラメーター	<ipaddr> - SNMP トラップの送信先 IP アドレスを入力します。 <ipv6addr > - SNMP トラップの送信先 IPv6 アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP ホストエントリーを削除するには

```
#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

#
```

3.8.17 show snmp host

目的	スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を表示します。
構文	show snmp host [<ipaddr>]
説明	本コマンドは、スイッチの SNMP エージェントによって生成される SNMP トラップの送信先として指定されたリモート SNMP マネージャーの IP アドレスおよび設定情報を表示します。
パラメーター	<ipaddr> - SNMP トラップの送信先 IP アドレスを入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている SNMP ホストを表示するには

```
#show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3 User Name
---------------  ---------------  --------------------------------
10.48.76.23      V3 noauthnopriv  initial
10.48.74.100     V2c              public

Total Entries  : 2

#
```

3.8.18 show snmp v6host

目的	スイッチの SNMP エージェントによって生成される SNMP トラップの送信先(IPv6)を表示します。
構文	show snmp v6host [<ipv6addr>]
説明	本コマンドは、スイッチの SNMP エージェントによって生成される SNMP トラップの送信先として指定されたリモート SNMP マネージャーの IPv6 アドレスおよび設定情報を表示します。
パラメーター	<ipv6addr> - SNMP トラップの送信先 IPv6 アドレスを入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている SNMP ホストを表示するには

```
#show snmp v6host
Command: show snmp v6host

SNMP Host Table
------------------------------------------------------------
Host IPv6 Address : 2001:200::2
SNMP Version      : V2c
Community Name/SNMPv3 User Name : public

Total Entries: 1

#
```

3.8.19 enable snmp

目的	SNMP トラップを有効にします。
構文	enable snmp < authenticate_traps | linkchange_traps | traps | login_trap | login_fail_trap | logout_trap >
説明	本コマンドは、スイッチの SNMP トラップを有効にします。
パラメーター	authenticate_traps - 認証失敗時のトラップ出力を有効にします。 linkchange_traps - リンクチェンジトラップ出力を有効にします。 traps - SNMP トラップ出力を有効にします。 login_trap - ログイントラップ出力を有効にします。 login_fail_trap - ログインフェイルトラップ出力を有効にします。 logout_trap - ログアウトトラップ出力を有効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの SNMP トラップを有効にするには

```
#enable snmp traps
Command: enable snmp traps

Success.

#
```

使用例:SNMP リンクチェンジトラップ出力を有効にするには

```
#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

#
```

使用例:SNMP 認証トラップ出力を有効にするには

```
#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

#
```

3.8.20 disable snmp

目的	スイッチの SNMP トラップを無効にします。
構文	disable snmp < authenticate_traps | linkchange_traps | traps | login_ trap | login_fail_trap | logout_trap >
説明	本コマンドは、スイッチの SNMP トラップを無効にします。
パラメーター	authenticate_traps - 認証失敗時のトラップ出力を無効にします。 linkchange_traps - リンクチェンジトラップ出力を無効にします。 traps - SNMP トラップ出力を無効にします。 login_trap - ログイントラップ出力を無効にします。 login_fail_trap - ログインフェイルトラップ出力を無効にします。 logout_trap - ログアウトトラップ出力を無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP 認証トラップ出力を無効にするには

```
#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

#
```

使用例:SNMP リンクチェンジトラップ出力を無効にするには

```
#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

#
```

使用例:スイッチの SNMP トラップ出力を無効にするには

```
#disable snmp traps
Command: disable snmp traps

Success.

#
```

3.8.21 config snmp linkchange_traps ports

目的	リンクチェンジトラップの対象ポートを設定します。
構文	config snmp linkchange_traps ports < all | <portlist> > < enable | disable >
説明	本コマンドは、リンクチェンジトラップの送信制御を設定します。各ポートごとに設定可能です。
パラメーター	all - すべてのポートを指定します。 <portlist> - 設定するポート範囲を指定します。 enable - 指定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 - 指定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。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1～4 の SNMP リンクチェンジトラップを設定するには

```
#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

#
```

3.8.22 show snmp traps

目的	スイッチの SNMP トラップ設定を表示します。
構文	show snmp traps [linkchange_traps [ports <portlist>]]
説明	本コマンドは、スイッチに設定した SNMP トラップステータスを表示します。
パラメーター	linkchange_traps - SNMP リンクチェンジトラップステータスを表示します。 <portlist> - 表示するポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: SNMP トラップを表示するには

```
#show snmp traps
Command: show snmp traps

SNMP Trap          : Enabled
Authenticate Traps : Enabled
Linkchange Traps   : Enabled
Login Trap         : Disabled
Logout Trap        : Disabled
Login Fail Trap    : Disabled

#
```

使用例:リンクチェンジ SNMP トラップステータスを表示するには

```
#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
```

3.8.23 config snmp system_contact

目的	スイッチを管理する連絡担当者名を入力します。
構文	config snmp system_contact [<sw_contact>]
説明	本コマンドは、スイッチの管理者などの任意情報を入力します。
パラメーター	<sw_contact> - 最大 128 文字を使用できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの連絡担当者に「APS」を設定するには

```
#config snmp system_contact APS
Command: config snmp system_contact APS

Success.

#
```

3.8.24 config snmp system_location

目的	スイッチの設置場所の説明を入力します。
構文	config snmp system_location [<sw_location>]
説明	本コマンドは、スイッチの設置場所などの任意情報を入力します。
パラメーター	<sw_location> - 最大 128 文字を使用できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:「5F」のスイッチ場所を設定するには

```
#config snmp system_location 5F
Command: config snmp system_location 5F

Success.

#
```

3.8.25 config snmp system_name

目的	スイッチの名前を設定します。
構文	config snmp system_name [<sw_name>]
説明	このコマンドは、スイッチの名称などの任意情報を入力します。
パラメーター	<sw_name> - 最大 128 文字を使用できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:「ApresiaLightGM152GT」のスイッチ名を設定するには

```
#config snmp system_name ApresiaLightGM152GT
Command: config snmp system_name ApresiaLightGM152GT

Success.

#
```

3.8.26 enable rmon

目的	スイッチの RMON を有効にします。
構文	enable rmon
説明	本コマンドは、下記の 「disable rmon」コマンドと共に使用して、スイッチのリモートモニタリング(RMON)を有効/無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：RMON を有効にするには

```
#enable rmon
Command: enable rmon

Success.

#
```

3.8.27 disable rmon

目的	スイッチの RMON を無効にします。
構文	disable rmon
説明	本コマンドは、上記の enable rmon コマンドと共に使用して、スイッチのリモートモニタリング(RMON)を有効/無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：RMON を無効にするには

```
#disable rmon
Command: disable rmon

Success.

#
```

3.8.28 create trusted_host

目的	装置への IP アクセスを許可するトラストホストを作成します。
構文	create trusted_host < <ipaddr> | <ipv6addr> | network <network_address>| ipv6_prefix <ipv6networkaddr> > <snmp | telnet | ssh | http | https | ping>
説明	本コマンドは、装置への IP アクセスを許可するトラストホストを作成します。 最大 10 個までの IP アドレスまたは IP ネットワークアドレスを指定できます。また、IP アクセスを許可するインタフェース（サービス）を指定することで、さらに信頼されたトラストホストを作成できます。トラストホストが作成されると、指定しない IP アドレスまたはインタフェースからの装置 IP アクセスはできなくなります。
パラメーター	<ipaddr> - 対象の IP アドレスを指定します。 <ipv6addr> - 対象の IPv6 アドレスを指定します。 network - 対象の IP ネットワークアドレスを指定します。(例 10.0.0.0/8) ipv6_prefix - 対象の IPv6 ネットワークアドレスを指定します。(例 10:1::/32) <snmp| telnet| ssh| http| https| ping> - 対象のインタフェースを指定します。指定しない場合、すべてのインタフェースが対象になります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.01.00 以降

使用例:IP アドレスでトラストホストを作成するには

```
#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

#
```

使用例:IPv6 ネットワークアドレスでトラストホストを作成するには

```
#create trusted_host ipv6_prefix 10:48::/32
Command: create trusted_host ipv6_prefix 10:48::/32

Success.
#
```

注意事項

インタフェース（snmp、telnet、ssh、http、https、ping）設定は、全てのトラストホストで共有します。そのため、指定されないインタフェースがある場合、そのインタフェースを使用した装置への IP アクセスは可能になります。

3.8.29 config trusted_host

目的	トラストホストのアクセスインタ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>
説明	本コマンドは、作成したトラストホストのインタフェース（サービス）を設定します。
パラメーター	<ipaddr> - 対象の IP アドレスを指定します。 <ipv6addr> - 対象の IPv6 アドレスを指定します。 network - 対象の IP ネットワークアドレスを指定します。 ipv6_prefix - 対象の IPv6 ネットワークアドレスを指定します。 add - 対象のトラストホストに指定のインタフェースを追加します。 delete -対象のトラストホストから指定のインタフェースを削除します。 <snmp| telnet| ssh| http| https| ping | all> - 対象のインタフェースを指定します。all 指定の場合、すべてのインタフェースが対象になります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.01.00 以降

使用例:対象のトラストホストにすべてのインタフェースを削除するには

```
#config trusted_host 10.48.74.121 delete all
Command: create trusted_host 10.48.74.121 delete all

Success.

#
```

使用例:対象のトラストホストに指定したインタフェースを追加するには

```
#config trusted_host 10.48.74.121 add snmp ping telnet
Command: create trusted_host 10.48.74.121 add snmp ping telnet

Success.

#
```

3.8.30 delete trusted_host

目的	トラストホストを削除します。
構文	delete trusted _host < ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr> | all> >
説明	本コマンドは、作成したトラストホストを削除します。
パラメーター	<ipaddr> - 対象の IP アドレスを指定します。 <ipv6addr> - 対象の IPv6 アドレスを指定します。 network - 対象の IP ネットワークアドレスを指定します。 ipv6_prefix - 対象の IPv6 ネットワークアドレスを指定します。 all - すべてのトラストホストを削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.01.00 以降

使用例:対象のトラストホストを削除するには

```
#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

#
```

使用例:すべてのトラストホストを削除するには

```
#delete trusted_host all
Command: delete trusted_host all

Success.

#
```

3.8.31 show trusted_host

目的	トラストホストを表示します。
構文	show trusted_host
説明	本コマンドは、作成したトラストホストを表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.01.00 以降

使用例：トラストホストを表示するには

```
#show trusted_host
Command: show trusted_host



Management Stations

IP Address                                  Access Interface
------------------------------------------------------------------
10.48.74.121/32                             SNMP Telnet Ping
10:48::/32                                  SNMP Telnet SSH HTTP HTTPs Ping

Total Entries: 2



#
```

3.9 ネットワーク監視コマンド

3.9.1 show packet ports

目的	各ポートで送受信のパケット統計情報を表示します。
構文	show packet ports <portlist>
説明	本コマンドは、各ポートで送受信されたパケットの統計情報を表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 2 のパケット統計情報を表示するには

```
#show packet ports 1
Command: show packet ports 1

Port Number : 1
================================================================
Frame Size/Type       Frame Counts                Frames/sec
---------------       ----------------------      -----------
64                    2754                        0
65-127                449                         0
128-255               20                          0
256-511               137                         0
512-1023              12                          0
1024-1518             0                           0
Unicast RX            0                           0
Multicast RX          597                         0
Broadcast RX          2775                        0

Frame Type            Total                       Total/sec
---------------       ----------------------      -----------
RX Bytes              269569                      0
RX Frames             3372                        0
TX Bytes              0                           0
TX Frames             0                           0

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

3.9.2 show error ports

目的	各ポートのエラー統計情報を表示します。
構文	show error ports <portlist>
説明	本コマンドは、スイッチが指定ポートに対して収集した、パケットエラー統計情報を表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 3 のエラー統計情報を表示するには

```
#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
```

3.9.3 config utilization notify

目的	装置の CPU およびメモリ使用率通知機能を設定します。
構文	config utilization notify <cpu | dram> [state<enable | disable>] | threshold <value 20-100> | [polling_interval <value 10-300> | trap_state <enable | disable> | log_state <enable | disable>]
説明	本コマンドは、装置の CPU およびメモリ使用率通知を設定します。 CPU&DRAM 使用率表示コマンドは、CPU および DRAM の使用状態を周期的に監視することで指定閾値を超過した場合、ログやトラップによりユーザーへ通知します。
パラメーター	<cpu | dram> - 使用率通知設定を指定します。 state<enable | disable> - 閾値の監視を有効または無効で指定します。 threshold <value 20-100> - 通知する場合の閾値を 20%から 100%の範囲で指定します。この閾値を超えた場合、"OVERLOADING utilization status"のログを出力します。 また、閾値を超えた状態から閾値より小さくなった場合、"NORMAL utilization status"のログを出力します。デフォルト値は 100%です。 polling_interval <value 10-300> - 閾値の監視間隔を 10 秒から 300 秒で指定します。デフォルト値は 60 秒です。 trap_state <enable | disable> - 閾値を超えた場合の SNMP トラップ出力を有効または無効で指定します。デフォルト値は無効(disable)です。 log_state <enable | disable> - 閾値を超えた場合のシステムログ出力を有効または無効で指定します。デフォルト値は有効(enable)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: CPU 使用率通知を閾値 100%、ポーリング間隔 10 秒で設定するには

```
#config utilization notify cpu threshold 100 polling_interval 10
Command: config utilization notify cpu threshold 100 polling_interval 10

Success.

#
```

3.9.4 clear utilization

目的	装置の CPU および DRAM 使用率統計情報をクリアします。
構文	clear <cpu | dram>
説明	本コマンドは、装置の CPU および DRAM 使用率統計情報をクリアします。
パラメーター	<cpu | dram> - クリアする使用率統計情報を指定します。 cpu - CPU 使用率に関する情報をクリアします。 dram - DRAM 使用率に関する情報をクリアします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: CPU 使用率統計情報をクリアするには

```
#clear utilization cpu
Command: clear utilization cpu

Success.

#
```

3.9.5 show utilization

目的	リアルタイムで使用率統計情報を表示します。
構文	show utilization < cpu | dram | flash | ports [<portlist>] >
説明	本コマンドは、リアルタイムでスイッチの使用率統計情報を表示します。
パラメーター	cpu - スイッチの現在の CPU 使用率を表示します。 dram - スイッチの現在の DRAM 使用率を表示します。 flash - スイッチの現在のフラッシュ使用率を表示します。 ports - スイッチの現在のポート使用率を表示します。 <portlist> - 表示するポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:現在の CPU 使用率を表示するには

```
#show utilization cpu
Command: show utilization cpu

CPU Utilization
-------------------------------------------------------------------------------
Five Seconds -  11 %         One Minute -  11 %         Five Minutes -  10 %
Maximum      -  27 %         Minimum    -   0 %

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

使用例:現在の DRAM 使用率を表示するには

```
#show utilization dram
Command: show utilization dram

DRAM Utilization :

Total DRAM       : 131,072   KB

Used DRAM        : 68,586    KB

Utilization      : 52  %

Utilization(max) : 52  %

Utilization(min) : 52  %

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

使用例:現在のフラッシュメモリー使用率を表示するには

```
#show utilization flash
Command: show utilization flash

FLASH Memory Utilization :

Total FLASH     : 16,384    KB

Used FLASH      : 7,371     KB

Utilization     : 44%


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

使用例:ポート使用統計を表示するには

```
#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         29     0           0           0
 10     0           0           0         30     0           0           0
 11     0           0           0         31     0           0           0
 12     0           0           0         32     0           0           0
 13     0           0           0         33     0           0           0
 14     0           0           0         34     0           0           0
 15     0           0           0         35     0           0           0
 16     0           0           0         36     0           0           0
 17     0           0           0         37     0           0           0
 18     0           0           0         38     0           0           0
 19     0           0           0         39     0           0           0
 20     0           0           0         40     0           0           0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

TX/sec、RX/sec の単位は packet/sec です。
Util は TX/sec、RX/sec それぞれの最大転送レートに対する割合を最大 50%とし、合計値を表示します。

3.9.6 show utilization notify

目的	CPU および DRAM 使用率通知機能の設定状態を表示します。
構文	show utilization notify <cpu | dram>
説明	本コマンドは、CPU および DRAM 使用率通知機能の設定を表示します。
パラメーター	cpu - CPU 使用率通知機能に関する設定状態を表示します。 dram - DRAM 使用率通知機能に関する設定状態を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:現在の CPU 使用率通知機能の設定を表示するには

```
#show utilization notify cpu
Command: show utilization notify cpu



CPU Utilization Notify Information
-----------------------------------
Current Status   : NORMAL
State            : Enabled
Threshold        : 100%
Polling Interval : 60 sec
Trap State       : Disabled
Log State        : Enabled

#
```

3.9.7 clear counters

目的	スイッチの統計カウンタをクリアします。
構文	clear counters [ports <portlist>]
説明	本コマンドは、スイッチの統計カウンタをクリアします。
パラメーター	<portlist> - ポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:カウンタをクリアするには

```
#clear counters ports 2-9
Command: clear counters ports 2-9

Success.

#
```

3.9.8 clear log

目的	スイッチの履歴ログをクリアします。
構文	clear log
説明	本コマンドは、スイッチの履歴ログをクリアします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ログ情報をクリアするには

```
#clear log
Command: clear log

Success.

#
```

3.9.9 show log

目的	スイッチの履歴ログを表示します。
構文	show log [index <value_list X-Y>]
説明	本コマンドは、スイッチの履歴ログの内容を表示します。 ログは最大 10,000 行まで表示できます。
パラメーター	index <value_list X-Y> - 本コマンドは、<value_list X-Y>フィールドでユーザーが指定した開始と終了の値間の履歴ログを表示します。 パラメーターを指定しない場合、すべての履歴ログエントリーを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチの履歴ログを表示するには

```
#show log
Command: show log

Index Data       Time     Log Text
----- ---------- -------- ------------------------------------------------------
2     2016-08-21 10:35:45 Successful login through Console (Username: adpro)
1     2016-08-21 10:34:53 System warm start (CONSOLE)

#
```

3.9.10 enable syslog

目的	システムログをリモートホストに送信する機能を有効にします。
構文	enable syslog
説明	本コマンドは、システムログをリモートホストに送信する機能を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの syslog 機能を有効にするには

```
#enable syslog
Command: enable syslog

Success.

#
```

3.9.11 disable syslog

目的	システムログをリモートホストに送信する機能を無効にします。
構文	disable syslog
説明	本コマンドは、システムログをリモートホストに送信する機能を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの syslog 機能を無効にするには

```
#disable syslog
Command: disable syslog

Success.

#
```

3.9.12 show syslog

目的	syslog のステータスが有効または無効であるか表示します。
構文	show syslog
説明	本コマンドは、syslog のステータスが有効または無効であるか表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:syslog 機能のステータスを表示するには

```
#show syslog
Command: show syslog

Syslog Global State  : Disabled

#
```

3.9.13 create syslog host

目的	新たに syslog の送信内容を設定します。
構文	create syslog host <index 1-4> [severity < informational | warning | all > | facility < local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 > | udp_port <udp_port_number> | ipaddress <ipaddr> | state < enable | disable >]
説明	本コマンドは、新たに syslog の送信内容を設定します。
パラメーター	<index 1-4> - コマンドを適用するホストのインデックスを指定します。 1～4 の番号のついた 4 つの利用可能なインデックスがあります。 severity - 重度レベルを指定します。 以下の説明を参考にしてください。
	数値 重度 コード
	4 Warning(警告)： 警告の状態 6 Informational(情報的)： 情報を伝えるメッセージ

パラメーター	数値　　ファシリティ コード
	16　　ローカル使用 0　(local0) 17　　ローカル使用 1　(local1) 18　　ローカル使用 2　(local2) 19　　ローカル使用 3　(local3) 20　　ローカル使用 4　(local4) 21　　ローカル使用 5　(local5) 22　　ローカル使用 6　(local6) 23　　ローカル使用 7　(local7) local0 - ローカル使用 0 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 16 番に対応します。 local1 - ローカル使用 1 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 17 番に対応します。 local2 - ローカル使用 2 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 18 番に対応します。 local3 - ローカル使用 3 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 19 番に対応します。 local4 - ローカル使用 4 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 20 番に対応します。 local5 - ローカル使用 5 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 21 番に対応します。 local6 - ローカル使用 6 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 22 番に対応します。 local7 - ローカル使用 7 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 23 番に対応します。 udp_port <udp_port_number> - syslog プロトコルがメッセージをリモートホストに送信するために使用する UDP ポート番号を指定します。 ipaddress <ipaddr> - syslog メッセージが送信されるリモートホストの IP アドレスを指定します。 state <enable | disable> - リモートホストへの syslog メッセージの送信を「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:syslog ホストを作成するには

```
#create syslog host 1 ipaddress 10.68.88.1 severity all facility local0
Command: create syslog host 1 ipaddress 10.68.88.1 severity all facility local0

Success.

#
```

3.9.14 config syslog

目的	syslog の送信内容を変更します。
構文	config syslog host < all | <index 1-4> > severity < informational | warning | all > [facility < local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 > | udp_port <udp_port_number> | ipaddress <ipaddr> | state < enable | disable >]
説明	本コマンドは、syslog プロトコルを設定し、システムログ情報をリモートホストに送信します。
パラメーター	all - 利用可能なすべてのインデックスを指定します。 <index 1-4> - コマンドを適用するホストのインデックスを指定します。 1～4 の番号のついた 4 つの利用可能なインデックスがあります。 severity - 重度レベルを指定します。 以下の説明を参考にしてください。
	数値 重度 コード
	4 Warning(警告)： 警告の状態 6 Informational(情報的)： 情報を伝えるメッセージ
	informational - 情報的なメッセージをリモートホストに送信する場合に指定します。 これは上記リストの 6 番に対応します。 warning - 警告的なメッセージをリモートホストに送信する場合に指定します。 これは上記リストの 4 番に対応します。 all - スイッチに生成される現在サポートしている Syslog メッセージのすべてをリモートホストに送信します。 facility - 指定できるファシリティは以下の通りです。
	数値 ファシリティ コード
	16 ローカル使用 0 (local0) 17 ローカル使用 1 (local1) 18 ローカル使用 2 (local2) 19 ローカル使用 3 (local3) 20 ローカル使用 4 (local4) 21 ローカル使用 5 (local5) 22 ローカル使用 6 (local6) 23 ローカル使用 7 (local7)
	local0 - ローカル使用 0 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 16 番に対応します。 local1 - ローカル使用 1 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 17 番に対応します。 local2 - ローカル使用 2 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 18 番に対応します。 local3 - ローカル使用 3 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 19 番に対応します。 local4 - ローカル使用 4 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 20 番に対応します。

パラメーター	local5 - ローカル使用 5 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 21 番に対応します。 local6 - ローカル使用 6 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 22 番に対応します。 local7 - ローカル使用 7 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 23 番に対応します。 udp_port <udp_port_number>- syslog プロトコルがメッセージをリモートホストに送信するために使用する UDP ポート番号を指定します。 ipaddress <ipaddr> - syslog メッセージが送信されるリモートホストの IP アドレスを指定します。 state <enable | disable> - リモートホストへの syslog メッセージの送信を「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:インデックス 1 の syslog ホストを設定するには

```
#config syslog host 1 severity all facility local0
Command: config syslog host 1 severity all facility local0

Success.

#
```

3.9.15 delete syslog host

目的	設定済みの syslog ホストをスイッチから削除します。
構文	delete syslog host < <index 1-4> | all >
説明	本コマンドは、設定済みの syslog ホストをスイッチから削除します。
パラメーター	<index 1-4> - コマンドを適用するホストのインデックスを指定します。 1～4 の番号のついた 4 つの利用可能なインデックスがあります。 all - コマンドをすべてのホストに適用する場合に指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:設定済みの syslog ホストを削除するには

```
#delete syslog host 4
Command: delete syslog host 4

Success.

#
```

3.9.16 show syslog host

目的	現在スイッチに設定されている syslog ホストを表示します。
構文	show syslog host [<index 1-4>]
説明	本コマンドは、スイッチに現在設定されている syslog ホストを表示します。
パラメーター	<index 1-4> - コマンドを適用するホストのインデックスを指定します。 1～4 の番号のついた 4 つの利用可能なインデックスがあります。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:syslog ホスト情報を表示するには

```
#show syslog host
Command: show syslog host

Syslog Global State : Enabled

Host 1
  IP Address        : 10.0.0.5
  Severity          : All
  Facility          : Local0
  UDP port          : 514
  Status            : Disabled

Total Entries : 1
#
```

3.9.17 config log_save_timing

目的	スイッチのフラッシュメモリーへ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 >
説明	本コマンドは、スイッチのフラッシュメモリーへログを保存します。
パラメーター	time_interval <min 1-65535> - ログの保存を実行する間隔を設定します。 ログは、ここで設定した時間（X 分）ごとに保存されます。 on_demand - 「save all」または「save log」コマンドを使用して、手動でスイッチにログを保存します。 log_trigger - ログイベントの発生毎にスイッチにログを保存します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ログファイルの保存を 30 分間隔に設定するには

```
#config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.

#
```

注意事項

フラッシュメモリーに保存可能なログは最大 10,000 行です。

3.9.18 show log_save_timing

目的	スイッチのフラッシュメモリーへログを保存する方法を表示します。
構文	show log_save_timing
説明	本コマンドは、スイッチのフラッシュメモリーへログを保存する方法を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ログファイルを保存する方法を表示するには

```
#show log_save_timing
Command: show log_save_timing

Saving log method: on_demand

#
```

3.9.19 delete ipif System

目的	IPv6 アドレスを削除します。
構文	delete ipif System < ipv6address <ipv6networkaddr> >
説明	本コマンドは、IPv6 アドレスを削除します。
パラメーター	<ipv6networkaddr> - IPv6 ネットワークアドレスを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:システムインターフェースの IPv6 アドレスを削除するには

```
#delete ipif System ipv6address FE80::200:1FF:FE02:303/128
Command: delete ipif System ipv6address FE80::200:1FF:FE02:303/128

Success.

#
```

3.9.20 enable ipif_ipv6_link_local_auto

目的	IPv6 アドレスが設定されていない場合、リンクローカルアドレスの自動設定を有効にします。
構文	enable ipif_ipv6_link_local_auto <System>
説明	本コマンドは、IPv6 アドレスが明確に設定されていない場合、リンクローカルアドレスの自動設定を有効にします。IPv6 アドレスが明確に設定されている場合は、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 アドレスが明確に設定されていない場合、デフォルトにより、リンクローカルアドレスは設定されず、IPv6 処理は無効になります。 この自動設定を有効にすることによって、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。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:インターフェースのリンクローカルアドレスの自動設定を有効にするには

```
#enable ipif_ipv6_link_local_auto System
Command: enable ipif_ipv6_link_local_auto System

Success.

#
```

3.9.21 disable ipif_ipv6_link_local_auto

目的	IPv6 アドレスが設定されていない場合、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 <System>
説明	本コマンドは、IPv6 アドレスが明確に設定されていない場合、リンクローカルアドレスの自動設定を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:インターフェースのリンクローカルアドレスの自動設定を無効にするには

```
#disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System

Success.

#
```

3.9.22 show ipif_ipv6_link_local_auto

目的	リンクローカルアドレス自動設定の状態を表示します。
構文	show ipif_ipv6_link_local_auto
説明	本コマンドは、リンクローカルアドレス自動設定の状態を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:インターフェース情報を表示するには

```
#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

IPIF: System         Automatic Link Local Address: Disabled
#
```

3.10 SMTP コマンド

SMTP（Simple Mail Transfer Protocol）は、電子メールのアドレスに基づき下記のコマンドを使用してスイッチのイベントをメールの受信者に送信するスイッチの機能です。スイッチは SMTP のクライアントとして設定され、一方サーバーはスイッチからのメッセージを受信し、電子メールに適切な情報を記載し、スイッチに設定した受信者に送信します。これにより小規模のワークグループや配線の管理が簡素化され、スイッチの緊急イベントで処理速度が向上し、スイッチに発生した問題イベントの記録によりセキュリティーが強化されます。

SMTP 機能におけるクライアントとしてのスイッチの重要な役割:

この機能を適切に動作させるには、SMTP サーバーの IP アドレスと TCP ポートは正しく設定されている必要があります。「server」と「server_port」のパラメーターを適切に設定することによって「config smtp」コマンドが機能します。

メール受信者をスイッチに設定しておく必要があります。サーバーに受信者の情報が送信され、情報が処理され、スイッチ情報が受信者にメールされます。 「config smtp」コマンドの「add mail_receiver」と「delete mail_receiver」のパラメーターを使用して、最大 8 人までのメール受信者をスイッチに登録できます。

管理者は、設定した受信者に送信されるメッセージの送信元アドレスを設定することができます。これによりスイッチの機能や問題などについてより詳細な情報を得ることができます。「config smtp」コマンドを使用したり、「self_mail_addr」パラメーターを設定して、プライベートの電子メールを設定することもできます。

受信者が SMTP サーバーからの電子メールを受信できるか、スイッチにテストメール送信の設定をすることができます。テストメールの設定には、まず「enable smtp」コマンドを使用して SMTP 機能を有効にし、次に「smtp send_testmsg」コマンドを入力します。 SMTP を設定したすべての受信者は、SMTP サーバーからのサンプルテストメッセージを受信し、この機能の信頼性が確認できます。

次のイベントのどれかひとつでも発生した場合、スイッチは受信者にメールを送信します。
スイッチにコールドスタートまたはウォームスタートが発生した時。
ポートがリンクダウン状態になった時。
ポートがリンクアップ状態になった時。
SNMP 認証がスイッチによって拒否された時。
スイッチ構成エントリーがスイッチによって NVRAM に保存された時。
ファームウェアのダウンロードイベント中に TFTP サーバーに異常が発生した時。
これには、TFTP サーバーからの「invalid-file（無効なファイル)」、「file-not-found（ファイルが見つかりません)」、「complete(完了)」、「time-out(j タイムアウト)」のメッセージを含みます。
スイッチにシステムリセットが発生した時。

SMTP サーバーが送信する電子メールには次のスイッチイベント情報が含まれます。
メール送信機器のモデル名と IP アドレス、SMTP サーバーとメッセージを送信したクライアントを識別するタイムスタンプとスイッチからメッセージを受信した日付も含まれます。 中継されたメッセージには各中継ごとにタイムスタンプが付きます。
電子メール送信の要因となるスイッチに発生したイベント。
ファームウェアの保存またはアップグレードなどユーザーによってイベントが処理されたとき、タスクを処理したユーザーの IP アドレス、MAC アドレス、ユーザー名がイベント発生時のシステムメッセージと共に送信されます。
複数回同じイベントが発生した時、2 通目からのメッセージはシステムエラーメッセージが件名に表

示されます。

「Delivery Process（配信中）」中に発生したイベント詳細について
優先度の高いの緊急メールは送信待ちの通常メールを差し置いて送信されます。
送信待ちの未送信メールは最大 30 件まで保存されます。 30 件まで保存されると新規メールは廃棄されます。
初期のメッセージが受信者に届いていない場合、送信待ちメールの順番に入れられ、再送信が実行されます。
再送信の最大限度は 3 回です。3 回まで 5 分毎に再送信が実行されます。 限度数に達してもメッセージが受信されない場合、メールは破棄されます。
スイッチがシャットダウンや再起動した場合、送信待ちメールは破棄されます。

3.10.1 enable smtp

目的	SMTP クライアントとしてスイッチを有効にします。
構文	enable smtp
説明	本コマンドは「disable smtp コマンド」と共に設定を変更せずに、スイッチを SMTP クライアントとして有効/無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの SMTP を有効にするには

```
#enable smtp
Command: enable smtp

Success.

#
```

3.10.2 disable smtp

目的	SMTP クライアントとしてスイッチを無効にします。
構文	disable smtp
説明	本コマンドは「enable smtp コマンド」と共に設定を変更せずに、スイッチを SMTP クライアントとして有効/無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの SMTP を無効にするには

```
#disable smtp
Command: disable smtp

Success.

#
```

3.10.3 config smtp

目的	スイッチの SMTP クライアントとして必要な設定を行います。
構文	config smtp < server <ipaddr> | server_port <tcp_port_number 1-65535> | self_mail_addr <mail_addr 64> | add mail_receiver <mail_addr 64> | delete mail_receiver <index 1-8> >
説明	本コマンドは SMTP サーバーやメール受信者の設定を行うために必要なパラメーターを設定します。 本コマンドは、スイッチの SMTP 機能が正常に作動するために、正しく全て設定する必要があります。
パラメーター	server <ipaddr> - リモートデバイス上の SMTP サーバーの IP アドレスを指定します。 server_port <tcp_port_number 1-65535> - SMTP サーバーに接続する TCP ポート番号を入力します。 SMTP の一般的なポート番号は、「25」です。 self_mail_addr <mail addr 64> - 送信元の電子メールアドレスを入力します。 このアドレスは受信者に送信された電子メールアドレスになります。 このスイッチでは、メールアドレスを 1 つだけ設定することができます。 文字列は最大 64 文字までの半角英数字が使用できます。 add mail_receiver <mail_addr 64> - このパラメーターを選択することにより、スイッチからの電子メールメッセージの受信者を追加できます。 各スイッチごとに 8 つまでの電子メールアドレスを追加できます。 delete mail_receiver <index 1-8> - このパラメーターを選択すると、設定リストからメール受信者を削除できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SMTP 設定を行うには

```
#config smtp server 10.48.74.100 server_port 25 add mail_receiver
smtp@apresiasystems.com
Command: config smtp server 10.48.74.100 server_port 25 add mail_receiver
smtp@apresiasystems.com

Success.

#
```

3.10.4 show smtp

目的	スイッチの SMTP 機能の設定パラメーターの内容について表示します。
構文	show smtp
説明	本コマンドは、「server information（サーバー情報）」「mail recipients（メール受信者）」やスイッチの SMTP 機能の状態を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている SMTP パラメーターを表示するには

```
#show smtp
Command: show smtp

SMTP Status: Disabled
SMTP Server Address : 10.48.74.100
SMTP Server Port : 25
Self Mail Address: smtp@apresiasystems.com

Index                Mail Receiver Address
--------             ---------------------------------
1                    smtp@apresiasystems.com
2
3
4
5
6
7
8

#
```

3.10.5 smtp send_testmsg

目的	スイッチで設定したメール受信者にテストメールを送信します。
構文	smtp send_testmsg
説明	本コマンドは設定された全ての受信者にテストメールを送信します。 テストメール送信はSMTPサーバーの設定内容に従い行われます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:設定したメール受信者全員にテストメールを送信するには

```
#smtp send_testmsg
Command: smtp send_testmsg

Subject: This is a SMTP test.
Content: Hello everybody!!

Sending mail, please wait…

Success.

#
```

3.11 スイッチポートコマンド

3.11.1 config ports

目的	スイッチのイーサネットポートを設定します。
構文	config ports < <portlist> | all > [medium_type] < *speed* | flow_control <enable | disable> | state <enable | disable> | learning <enable | disable> | <description <desc 32> | clear_description> | mdix < auto | normal | cross > > *medium_type* =medium_type <fiber | copper> *speed* =speed <auto | 10_half | 10_full | 100_half | 100_full | 1000_full [< master | slave >] >
説明	本コマンドは、スイッチのイーサネットポートを設定します。 <portlist> でリストされたポートのみが影響を受けます。
パラメーター	all - スイッチのすべてのポートを設定します。 <portlist> - 設定するポートまたはポート範囲を指定します。 medium_type <fiber | copper> - 省略可能です。 speed - ポートの通信速度を指定します。 ユーザーは以下の選択ができます。 auto - オートネゴシエーションに設定します。 <10 | 100 | 1000> - 通信速度 (Mbps) を固定モードに設定します。 <half | full> - 半二重または全二重に設定します。 <master | slave> - 1000BASE-T ポートの固定モード(1000M/Full)では、マスター設定またはスレーブ設定を指定します。マスター設定(1000M/Full_M)は、物理レイヤに関連する情報を通知し接続先とのタイミング制御を確立します。スレーブ設定(1000M/Full_S)は、マスターとのタイミング制御により確立されます。マスター設定(1000M/Full_M)とした場合には、接続先はスレーブ設定(1000M/Full_S)にする必要があります。それ以外の設定では両ポートにリンクダウンを引き起こします。 IEEE 802.3-2005 1000BASE-T 仕様に準拠した装置との接続が可能です。 flow_control <enable | disable> -フロー制御を有効または無効にします。 state <enable | disable> - ポートの動作を有効または無効にします。 learning <enable | disable> - MAC アドレス学習を有効または無効にします。 description <desc 32> - ポートのコメントを 32 文字以下の半角英数字の文字列で入力します。 clear_description - ポートのコメントをクリアします。
	mdix - 10/100/1000BASE-T ポートにおける MDIX を設定します。 MDIX 設定は「auto (自動)」、「normal (MDI-X)」、「cross (MDI)」から選択できます。「normal (MDI-X)」に設定した場合 、ストレートケーブルを使用して PC(MDI)に接続することが可能です。「cross (MDI)」に設定した場合、ストレートケーブルを使用して他のスイッチ(MDI-X)に接続することが可能です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 20～24 の速度を 10Mbps、フルデュプレックス、ステータスを有効にするには

```
#config ports 20-24 speed 10_full state enable
Command: config ports 20-24 speed 10_full state enable

Success.

#
```

注意事項

相手装置との通信モードは、オートネゴシエーションまたは固定に合わせて下さい。
固定モードでは、通信速度や全二重および半二重モードを合わせる必要があります。
双方で一致しないと、リンク確立されない場合やリンク確立してもエラー率の高い通信となる場合があります。

3.11.2 show ports

目的	ポートの設定を表示します。
構文	show ports [<portlist>] [description | err_disabled | media_type]
説明	本コマンドは、ポートの設定を表示します。パラメーターがない場合は、すべてのポートを表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。 description - コメント入力したポートの説明を表示します。。 err_disabled - ループ検知や BPDU ガード機能などで接続状態が無効になったポートを表示します。 media_type - ポートのメディアタイプを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:すべてのポート設定を表示するには

```
#show ports
Command: show ports

 Port      State/          Settings            Connection          Address
           MDIX      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
 -------  --------  --------------------  ---------------------  ---------
 1         Enabled   Auto/Disabled         Link Down              Enabled
           Auto
 2         Enabled   Auto/Disabled         Link Down              Enabled
           Auto
 3         Enabled   Auto/Disabled         Link Down              Enabled
           Auto
 4         Enabled   Auto/Disabled         Link Down              Enabled
           Auto
 5         Enabled   Auto/Disabled         Link Down              Enabled
           Auto
 6         Enabled   Auto/Disabled         Link Down              Enabled
           Auto
 7         Enabled   Auto/Disabled         Link Down              Enabled
           Auto
 8         Enabled   Auto/Disabled         Link Down              Enabled
           Auto
 9         Enabled   Auto/Disabled         Link Down              Enabled
           Auto

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

3.12 Time と SNTP コマンド

3.12.1 config sntp

目的	SNTP サービスを設定します。
構文	config sntp < primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999> >
説明	本コマンドは、SNTP サーバーから SNTP 情報を取得する設定をします。SNTP を使用するためには、本コマンドで SNTP を有効にする必要があります（「enable sntp」を参照してください)。
パラメーター	primary - SNTP 情報を取得するプライマリサーバーの IP アドレスを入力します。 <ipaddr> - プライマリサーバーの IP アドレスを入力します。 secondary - プライマリサーバーが使用できない場合に SNTP 情報を取得するセカンダリサーバーを指定します。 <ipaddr> - セカンダリサーバーの IP アドレスを入力します。 poll-interval <int 30-99999> - SNTP の更新情報をリクエストする間隔を指定します。ポーリング間隔は、30～99999 秒の範囲です。
制限事項	管理者アカウントのみ本コマンドを実行できます。 SNTP サーバーを使用するためには、本コマンドで SNTP を有効にする必要があります（「enable sntp」を参照してください)。
対応バージョン	1.00.00 以降

使用例:SNTP 設定を行うには

```
#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.

#
```

3.12.2 show sntp

目的	SNTP 情報を表示します。
構文	show sntp
説明	本コマンドは、SNTP 設定情報を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:SNTP 設定情報を表示するには

```
#show sntp
Command: show sntp

Current Time Source      : System Clock
SNTP                     : Disabled
SNTP Primary Server      : 10.1.1.1
SNTP Secondary Server    : 10.1.1.2
SNTP Poll Interval       : 720 sec

#
```

3.12.3 enable sntp

目的	SNTP を有効にします。
構文	enable sntp
説明	本コマンドは、SNTP を有効にします。 SNTP のパラメーターは別途設定する必要があります(「config sntp」を参照してください)。 SNTP を有効にして設定すると、手動で設定したすべてのシステム時間設定が上書きされます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。 SNTP 設定は SNTP が機能するように設定される必要があります (「config sntp」を参照してください)。
対応バージョン	1.00.00 以降

使用例:SNTP 機能を有効にするには

```
#enable sntp
Command: enable sntp

Success.

#
```

3.12.4 disable sntp

目的	SNTP を無効にします。
構文	disable sntp
説明	本コマンドは、SNTP を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNTP を無効にするには

```
#disable sntp
Command: disable sntp

Success.

#
```

3.12.5 config time

目的	手動でシステム時間と日付の設定を行います。
構文	config time <date ddmmmyyyy> <time hh:mm:ss>
説明	本コマンドは、システム時間と日付の設定を行います。
パラメーター	date - 日付は 2 桁の数字、月は 2 桁の数字または英字 3 文字、年は 4 桁の数字で設定します。 例： 29032015（月を 2 桁の数字で表した場合） 29Mar2015（月を英字 3 文字で表した場合） time - システム時間は hh:mm:ss 形式で表します。 例： 19:42:30
制限事項	管理者アカウントのみ本コマンドを実行できます。 SNTP が有効の場合、手動で設定したシステム時間と日付は上書きされます。
対応バージョン	1.00.00 以降

使用例:手動でシステム時間と日付の設定を行うには

```
#config time 01062014 19:42:30
Command: config time 01062014 19:42:30

Success.

#
```

3.12.6 config time_zone

目的	使用するタイムゾーンを決定し、システムクロックを調整します。
構文	config time_zone < operator < + | - > | hour <gmt_hour 0-13> | min <minute 0-59> >
説明	本コマンドは、タイムゾーンに従ってシステムクロック設定を調整します。 タイムゾーン設定により SNTP 情報が調整されます。
パラメーター	operator - UTC に対するタイムゾーンの調整で時間を追加(+)または減算(-)します。 hour - UTC 時間との差分(時間)を指定します。 min - UTC 時間との差分(分)を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:タイムゾーン設定を行うには

```
#config time_zone operator + hour 9 min 0
Command: config time_zone operator + hour 9 min 0

Success.

#
```

3.12.7 config dst

目的	サマータイム(DST：Daylight Savings Time)を有効にし、時間調整を設定します。
構文	config dst < disable | *repeating* | annual > *Repeating* =repeating < <s_week <start_week 1-5,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-5,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset < 30 | 60 | 90 | 120 > > 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 > >
説明	本コマンドは、DST を有効にして設定します。本コマンドを有効にする場合、どの DST 要求にも応じるようにシステムクロックの調整をします。 DST 調整は手動で設定した時間および SNTP サービスを利用して設定した時間の両方のシステム時間に作用します。
パラメーター	disable - スイッチの DST 季節時間の調整を無効にします。 repeating - リピートモードを使用すると、DST の季節の時間調整が有効になります。 リピートモードでは、計算式を使用して DST（サマータイム）の開始日と終了日を指定する必要があります。 例えば、DST（サマータイム）を 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定します。 annual - アニュアルモードを使用すると、DST(サマータイム)の季節の時間調整が有効になります。 アニュアルモードでは、DST（サマータイム）の開始日と終了日を詳細に指定する必要があります。 例えば、DST（サマータイム）を 4 月 3 日から、10 月 14 日までと指定します。 s_week - DST(サマータイム)が開始する週を設定します。 <start_week 1-5,last> - DST が開始する週の番号を設定します。1 は第 1 週目、2 は第 2 週目と続き、last は月の最終週を意味します。 e_week - DST(サマータイム)が終了する週を設定します。 <end_week 1-5,last> - DST(サマータイム)が終了する週の番号設定します。1 は第 1 週目、2 は第 2 週目と続き、last は月の最終週を意味します。 s_day - DST（サマータイム）が開始する曜日を設定します。 <start_day sun-sat> - 3 文字の英字を使用して表された DST(サマータイム)が開始する曜日を設定します。(sun, mon, tue, wed, thu, fri, sat) e_day - DST(サマータイム)が終了する曜日を設定します。 <end_day sun-sat> - 3 文字の英字を使用して表された DST(サマータイム)が終了する曜日を設定します。(sun, mon, tue, wed, thu, fri, sat)

パラメーター	s_mth - DST(サマータイム)が開始する月を設定します。 <start_mth 1-12> - DST(サマータイム)が開始する月番号を設定します。 e_mth - DST(サマータイム)が終了する月番号を設定します。 <end_mth 1-12> - DST(サマータイム)が終了する月番号を設定します。 s_time - DST（サマータイム）が開始する時刻を設定します。 <start_time hh:mm> - 24 時制で時刻（hh:時、mm:分）を表します。 e_time - DST(サマータイム)が終了する時刻を設定します。 <end_time hh:mm> - 24 時制で時刻（hh:時、mm:分）を表します。 s_date - DST(サマータイム)が開始する特定日(月日)を設定します。 <start_date 1-31> - 開始日を数字で表します。 e_date - DST(サマータイム)が開始する特定日(月日)を設定します。 <end_date 1-31> - 終了日を数字で表します。 offset <30 | 60 | 90 | 120> - サマータイム間の追加または減算分を示します。 可能なオフセット時間は、30/60/90/120 です。デフォルト値は、60 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチのサマータイムを設定するには

```
#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.

#
```

3.12.8 show time

目的	現在の時刻設定と状態を表示します。
構文	show time
説明	本コマンドは、現在のシステム時間と共に日付と時刻のコンフィグレーションを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチのシステムクロックに現在設定されている時刻を表示するには

```
#show time
Command: show time

Current Time Source : System Clock
Current Time        : 01 Jun 2014 19:42:50
Time Zone           : UTC +09:00
Daylight Saving Time: Repeating
Offset in minutes   : 30
    Repeating From  : Apr 2nd Tue 15:00
              To    : Oct 2nd Wed 15:30
    Annual    From  : 29 Apr 00:00
              To    : 12 Oct 00:00

#
```

3.13 Asymmetric VLAN コマンド

3.13.1 enable asymmetric_vlan

目的	スイッチの asymmetric VLAN を有効にします。
構文	enable asymmetric_vlan
説明	本コマンドは、スイッチの asymmetric VLAN 機能を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:asymmetric VLAN を有効にするには

```
#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

#
```

3.13.2 disable asymmetric_vlan

目的	スイッチの asymmetric VLAN を無効にします。
構文	disable asymmetric_vlan
説明	本コマンドは、スイッチの asymmetric VLAN 機能を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:asymmetric VLAN を無効にするには

```
#disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

#
```

3.13.3 show asymmetric_vlan

目的	スイッチの asymmetric VLAN 状態を表示します。
構文	show asymmetric_vlan
説明	本コマンドは、スイッチの asymmetric VLAN 状態を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている asymmetric VLAN 状態を表示するには

```
#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN: Enabled

#
```

3.14 BPDU ガードコマンド

3.14.1 enable bpdu_guard

目的	スイッチの BPDU ガード機能を有効にします。
構文	enable bpdu_guard
説明	本コマンドは、スイッチの BPDU ガード機能を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:BPDU ガード機能を有効にするには

```
#enable bpdu_guard
Command: enable bpdu_guard

Success.

#
```

3.14.2 disable bpdu_guard

目的	スイッチの BPDU ガード機能を無効にします。
構文	disable bpdu_guard
説明	本コマンドは、スイッチの BPDU ガード機能を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:BPDU ガード機能を無効にするには

```
#disable bpdu_guard
Command: disable bpdu_guard

Success.

#
```

3.14.3 config bpdu_guard ports

目的	スイッチのポートに BPDU ガード機能を設定します。
構文	config bpdu_guard ports <<portlist> | all> [state <enable | disable> | mode <shutdown>]
説明	BPDU ガードを有効にしたポートでは、BPDU パケットを受信すると err-disable 状態となりポートを shutdown します。
パラメーター	ports <<portlist> | all> - BPDU ガード機能を設定するポートまたはポートリストを入力します。all パラメーターを入力すると、スイッチのすべてのポートが対象となります。 state <enable | disable> - 指定されたポートの BPDU ガード機能を enable で有効、disable で無効にします。デフォルト設定は、「disable」(無効)です。 mode <shutdown> - BPDU パケットを受信したポートを shutdown します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポートの BPDU ガードを有効にして、状態モードを shutdown に設定するには

```
#config bpdu_guard ports 1 state enable mode shutdown
Command: config bpdu_guard ports 1 state enable mode shutdown

Success.

#
```

注意事項

BPDU ガード機能が有効なポートでは、スパニングツリー機能は設定できません。

BPDU ガード機能が対象とするパケットは、スイッチでサポートする IEEE802.1d BPDU(STP/RSTP/MSTP)となります。

3.14.4 config bpdu_guard recovery_time

目的	BPDU ガードのリカバリー時間を設定します。
構文	config bpdu_guard recovery_time <<sec 60-1000000> | infinite>
説明	BPDU ガードのリカバリー時間を設定します。
パラメーター	recovery_time <<sec 60-1000000> | infinite> - 自動復帰に関する BPDU ガードリカバリータイムを 60～1000000 秒の範囲または無限に設定します。 デフォルト値は、60 秒です。 Infinite パラメーターを指定するとリカバリータイムが無限に設定され、自動復帰をしなくなります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの BPDU ガード機能リカバリー時間を 120 秒に設定するには

```
#config bpdu_guard recovery_time 120
Command: config bpdu_guard recovery_time 120

Success.

#
```

3.14.5 config bpdu_guard log

目的	スイッチの BPDU ガードに関するログ状態を設定します。
構文	config bpdu_guard log <none | attack_detected | attack_cleared | both>
説明	スイッチの BPDU ガードに関するログ状態を設定します。
パラメーター	<none> - ログへの書き込みをしません。 <attack_detected> - BPDU パケットを検出した場合に、ログへの書き込みをします。 <attack_cleared> - リカバリー時間による自動復旧、またはコマンドによる手動復旧を行った場合に、ログへの書き込みをします。 <both> - BPDU パケット検知、復旧の両方のログを書き込みます。 デフォルトでは both が設定されています。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:BPDU ガードログ状態を both として設定するには

```
#config bpdu_guard log both
Command: config bpdu_guard log both

Success.

#
```

3.14.6 show bpdu_guard

目的	スイッチおよびポートの BPDU ガード状態を表示します。
構文	show bpdu_guard [ports [<portlist>]]
説明	スイッチおよびポートごとの BPDU ガード状態を表示します。
パラメーター	ports - ポートの BPDU ガード状態を表示させます。 <portlist> - 表示するポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチの BPDU ガード設定を表示するには

```
#show bpdu_guard
Command: show bpdu_guard

 BPDU Guard Global Settings
 ----------------------------------------
 BPDU Guard Status          : Enabled
 BPDU Guard Recovery Time   : 120 seconds
 BPDU Guard Trap Status     : Both
 BPDU Guard Log Status      : Both

#
```

使用例:ポートの BPDU ガード設定を表示するには

```
#show bpdu_guard ports
Command: show bpdu_guard ports

 Port  State        Mode       Status
------ -----------  ---------- ----------
 1     Enabled      Shutdown   Normal
 2     Disabled     Shutdown   Normal
 3     Disabled     Shutdown   Normal
 4     Disabled     Shutdown   Normal
 5     Disabled     Shutdown   Normal
 6     Disabled     Shutdown   Normal
 7     Disabled     Shutdown   Normal
 8     Disabled     Shutdown   Normal
 9     Disabled     Shutdown   Normal
 10    Disabled     Shutdown   Normal
 11    Disabled     Shutdown   Normal
 12    Disabled     Shutdown   Normal
 13    Disabled     Shutdown   Normal
 14    Disabled     Shutdown   Normal
 15    Disabled     Shutdown   Normal
 16    Disabled     Shutdown   Normal
 17    Disabled     Shutdown   Normal
 18    Disabled     Shutdown   Normal
 19    Disabled     Shutdown   Normal
 20    Disabled     Shutdown   Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.15 フォワーディングデータベースコマンド

3.15.1 create fdb

目的	ユニキャスト MAC アドレスフォワーディングテーブル（データベース）にスタティックエントリーを作成します。
構文	create fdb < <vlan_name 32> | vlanid <vidlist> > <macaddr> port <port>
説明	本コマンドは、スイッチのユニキャスト MAC アドレスフォワーディングテーブルにエントリーを作成します。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名を入力します。 vlanid <vidlist> - MAC アドレスが存在する VLAN ID を入力します。 <macaddr> - 追加するユニキャスト MAC アドレスを入力します。 port <port> - MAC 送信先アドレスに対応するポート番号を指定します。 スイッチはこのポートで指定されたデバイスにトラフィックを転送します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ユニキャスト MAC FDB エントリーを作成するには

```
#create fdb vlanid 1 00-11-22-33-44-55 port 10
Command: create fdb vlanid 1 00-11-22-33-44-55 port 10


Success.


#
```

3.15.2 create multicast_fdb

目的	マルチキャスト MAC アドレスフォワーディングテーブル（データベース）にスタティックエントリーを作成します。
構文	create multicast_fdb <vlan_name 32> <macaddr>
説明	本コマンドは、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ーを作成します。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名を入力します。 <macaddr> - 追加するマルチキャスト MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:マルチキャスト MAC フォワーディングエントリーを作成するには

```
#create multicast_fdb default 01-00-5E-00-00-01
Command: create multicast_fdb default 01-00-5E-00-00-01

Success.

#
```

3.15.3 config multicast_fdb

目的	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を設定します。
構文	config multicast_fdb <vlan_name 32> <macaddr> < add | delete > <portlist>
説明	本コマンドは、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構成します。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名を入力します。 <macaddr> - マルチキャストフォワーディングテーブルに追加される MAC アドレスを入力します。 <add | delete> - add は、ポートをテーブルに追加します。delete は、マルチキャストフォワーディングテーブルからポートを削除します。 <portlist> - 設定するポートまたはポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:マルチキャスト MAC フォワーディングを設定するには

```
#config multicast_fdb default 01-00-5E-00-00-01 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-01 add 1-5

Success.

#
```

3.15.4 config fdb aging_time

目的	フォワーディングデータベースのエージングタイムを設定します。
構文	config fdb aging_time <sec 10-1000000>
説明	エージングタイムは、スイッチの学習プロセスに影響します。送信元 MAC アドレスと対応するポート番号から構成されるダイナミックフォワーディングテーブルエントリーが、エージングタイム内にアクセスされないと、テーブルから削除されます。エージングタイムは 10～1000000 秒で指定します。デフォルトでは 300 秒に設定されています。エージングタイムが非常に長い場合、古いか既に存在しないダイナミックフォワーディングテーブルエントリーとなってします。これは、不正パケットの送信を引き起こす原因となります。しかし、 エージングタイムが短すぎると多くのエントリーが非常に早く削除されてしまいます。これは送信元アドレスがフォワーディングテーブルで見つけられないパケットを受信する高い確率をもたらし、その場合、スイッチはすべてのポートにパケットをブロードキャストするため、スイッチが持つ利点の多くを無駄にしてしまいます。
パラメーター	<sec 10-1000000> - MAC アドレスフォワーディングデータベース値のエージングタイムを入力します。10～1000000 秒の範囲で設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:fdb エージングタイムを設定するには

```
#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

#
```

注意事項

FDB に登録されたエントリーがクリアされる時間は、<入力値>÷2 から<入力値>-1 までの時間幅があります。

3.15.5 delete fdb

目的	スイッチのフォワーディングデータベースのエントリーを削除します。
構文	delete fdb 〈vlan_name 32〉〈macaddr〉
説明	本コマンドは、スイッチの MAC アドレスフォワーディングデータベースに作成したエントリーを削除します。
パラメーター	〈vlan_name 32〉- MAC アドレスが存在する VLAN 名を入力します。 〈macaddr〉- フォワーディングテーブルから削除する MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スタティックで登録した FDB エントリーを削除するには

```
#delete fdb default 00-40-66-00-00-01
Command: delete fdb default 00-40-66-00-00-01

Success.

#
```

使用例:スタティックで登録したマルチキャスト FDB エントリーを削除するには

```
#delete fdb default 01-00-5E-00-00-01
Command: delete fdb default 01-00-5E-00-00-01

Success.

#
```

3.15.6 clear fdb

目的	すべての動的に学習された MAC アドレスをスイッチのフォワーディングデータベースからクリアします。
構文	clear fdb < vlan <vlan_name 32> | port <port> | all >
説明	本コマンドは、スイッチのフォワーディングデータベースにダイナミックに学習されたエントリーをクリアします。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名を入力します。 port <port> - MAC 送信先アドレスに対応するポート番号を指定します。 all - スイッチのフォワーディングデータベースのすべてのダイナミックエントリーをクリアします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべての FDB ダイナミックエントリーをクリアするには

```
#clear fdb all
Command: clear fdb all

Success.

#
```

3.15.7 show multicast_fdb

目的	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の内容を表示します。
構文	show multicast_fdb [vlan <vlan_name 32> | vlanid <vlanlist> | mac_address <macaddr>]
説明	本コマンドは、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の内容を表示します。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名を入力します。 <vidlist> - FDB エントリーを表示する対象の VLAN ID リストを入力します。 <macaddr> - FDB エントリーを表示する対象の MAC アドレスを指定します。 パラメーターを指定しない場合、すべてのマルチキャスト FDB エントリーが表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MAC アドレステーブルを表示するには

```
#show multicast_fdb vlan default
Command: show multicast_fdb vlan default

VLAN Name       : default
MAC Address     : 01-00-5E-00-00-01
Egress Ports    : 1-5
Mode            : Static

Total Entries  : 1

#
```

3.15.8 show fdb

目的	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]
説明	本コマンドは、スイッチのフォワーディングデータベースの内容を表示します。
パラメーター	port <port> - MAC 送信先アドレスに対応するポート番号を指定します。 スイッチはこのポートで指定されたデバイスにトラフィックを転送します。 <vlan_name 32> - MAC アドレスが存在する VLAN 名を入力します。 <vidlist> - FDB テーブルの表示対象とする VLAN ID リストを入力します。 <macaddr> - FDB テーブルに存在する MAC アドレスを入力します。 static - スタティック MAC アドレスエントリーを表示します。 aging_time - MAC アドレスフォワーディングデータベースのエージングタイムを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ユニキャスト MAC アドレステーブルを表示するには

```
#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID  VLAN Name                      MAC Address       Port Type
---- ------------------------       ----------------- ---- --------
1    default                        00-40-66-00-00-01 CPU  Self

Total Entries  : 1

#
```

3.15.9 config multicast port_filtering_mode

目的	ポートの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 port_filtering_mode < <portlist> | all > < forward_unregistered_groups | filter_unregistered_groups >
説明	本コマンドは、スイッチの特定ポート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設定します。
パラメーター	<<portlist> | all> - マルチキャストポートフィルタリングモードを設定するポートまたはポートリストを入力します。all パラメーターを入力すると、スイッチのすべてのポートが対象となります。 <forward_unregistered_groups | filter_unregistered_groups> - 2 つのオプションのいずれにもフィルタリングモードを設定することができます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1～4 にマルチキャストフィルタリングモードを設定するには

```
#config multicast port_filtering_mode 1-4 forward_unregistered_groups
Command: config multicast port_filtering_mode 1-4 forward_unregistered_groups

Success.

#
```

3.15.10 show multicast port_filtering_mode

目的	ポートの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 port_filtering_mode
説明	本コマンドは、スイッチのポート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。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:すべてのポートのマルチキャストポートフィルタリングモードを表示するには

```
#show multicast port_filtering_mode
Command: show multicast port_filtering_mode

Multicast Filter Mode For Unregistered Group:
        Forwarding List: 1-52
        Filtering List:

#
```

3.16 IGMP スヌーピングコマンド

3.16.1 config igmp_snooping

目的	スイッチの IGMP スヌーピングを設定します。
構文	config igmp_snooping < vlan_name <vlan_name 32> | vlanid <vidlist> | all > < state < enable | disable > | fast_leave < enable | disable > >
説明	本コマンドは、スイッチの IGMP スヌーピングを設定します。
パラメーター	<vlan_name 32> - IGMP スヌーピングを設定する VLAN 名を入力します。 <vidlist> - 設定する VLAN のリストを指定します。 all - スイッチが設定されるすべての VLAN を指定します。 fast_leave <enable | disable> - IGMP スヌーピングの fast-leave（直ぐに離脱）機能を 「enable」(有効)または 「disable」(無効)にします。この機能を有効にすると、システムが IGMP Leave メッセージを受信し、Leave メッセージを送信するホストがグループの最後のホストである場合、メンバーは直ぐに離脱されます。 state <enable | disable> - 指定した VLAN の IGMP スヌーピングを「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:IGMP スヌーピングを設定するには

```
#config igmp_snooping vlan_name default state enable
Command: config igmp_snooping vlan_name default state enable

Success.

#
```

3.16.2 config igmp_snooping querier

目的	通常のクエリ送信の間隔（秒）、メンバーからのレポートを待つ最大時間（秒）およびIGMPスヌーピングを保証する許容パケット損失を設定します。
構文	config igmp_snooping querier < vlan_name <vlan_name 32> | vlanid <vidlist> | all > < query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state < enable | disable > | version <value 1-3> >
説明	本コマンドは、IGMPスヌーピングクエリアを設定します。
パラメーター	<vlan_name 32> - 設定するクエリアに対するVLAN名を入力します。 <vidlist> - クエリアを設定するVLAN ID範囲を入力します。 all - スイッチが設定されるすべてのVLANを指定します。 query_interval - 一般的なクエリー送信間隔を秒単位で指定します。デフォルト値は125秒です。 max_response_time - メンバーからのレポートを待つ最大時間(秒)を入力します。 デフォルト値は10秒です。 robustness_variable - 予想されるサブネット上のパケットの損失に応じてこの変数を微調整します。 robustness variable（堅牢性変数）の値は以下のIGMPメッセージ間隔を計算する場合に使用されます。 ・group membership interval - マルチキャストルーターがネットワーク上のグループにメンバーがいないと判断するまでの時間。 間隔の計算は以下の通りです。（堅牢性変数 x クエリー間隔）+（1 x クエリー応答間隔）。 ・other querier present interval-マルチキャストルーターがクエリアである他のマルチキャストルーターがないと判断するまでの時間。 間隔の計算は以下の通りです。（堅牢性変数 x クエリ間隔）+（0.5 x クエリ応答間隔）。 ・last member query count - ルーターがグループ内にローカルメンバーがいないと見なす前に送信されたGroup-Specific Query数。デフォルト値はrobustness variable（堅牢性変数）の値です。 ・robustness variable（堅牢性変数）はデフォルト「2」に設定されています。パケット損失が高くなると予想する場合には、この値を増やします。 last_member_query_interval - leave-groupメッセージの応答で送信したメッセージを含むgroup-specific queryメッセージ間の最大時間。この間隔を短くすると、ルーターがラストグループメンバー損失を早く検出します。 state - 状態がenableの場合、IGMP Querierとして選択できます(IGMPクエリーパケットを送信します)。「disable（無効）」の場合、スイッチはクエリアとして機能しません。 スイッチに接続したレイヤ3ルーターが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、この状態は無効として設定されます。 そうでない場合、レイヤ3ルーターがクエリアとして選択さないと、IGMPクエリーパケットを送信しません。マルチキャストルーティングプロトコルパケットを送信しないため、ポートはルーターポートとしてタイムアウトになります。 Version - このVLANが送信するIGMPパケットのバージョンを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:IGMP スヌーピングクエリアを設定するには

```
#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.

#
```

3.16.3 config router_ports

目的	ポートをルーターポートとして設定します。
構文	config router_ports < <vlan_name 32> | vlanid <vidlist> > < add | delete > <portlist>
説明	本コマンドは、マルチキャストイネーブルのルーターに接続するポート範囲を指定します。これは、プロトコルの種類にかかわらず送信先としてルーターが持つすべてのパケットをマルチキャストイネーブルのルーターに到達するように設定します。
パラメーター	<vlan_name 32> - ルーターポートが存在する VLAN 名を入力します。 <vidlist> - 設定するルーターポートの VID 範囲を入力します。 <add|delete> - 設定するルーターポートの追加または削除を指定します。 <portlist> - 設定するポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スタティックルーターポートを設定するには

```
#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

#
```

3.16.4 config router_ports_forbidden

目的	ポートを forbidden (禁止)ルーターポートとして設定します。
構文	config router_ports_forbidden < <vlan_name 32> | vlanid <vidlist> > < add | delete > <portlist>
説明	本コマンドは、マルチキャストイネーブルのルーターへの接続を禁止するポート範囲を指定します。 これは、禁止ルーターポートがルーティングパケットを伝播しないようにします。
パラメーター	<vlan_name 32> - ルーターポートが存在する VLAN 名を入力します。 <vidlist> - 禁止ポートとして設定するポートの VID 範囲を入力します。 <add | delete> - 指定した VLAN の禁止ポートの追加または削除を指定します。 <portlist> - 禁止ルーターポートとして設定されるポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:禁止ルーターポートを設定するには

```
#config router_ports_forbidden default add 2-10
Command: config router_ports_forbidden default add 2-10

Success.

#
```

3.16.5 enable igmp_snooping

目的	スイッチの IGMP スヌーピングを有効にします。
構文	enable igmp_snooping [forward_mcrouter_only]
説明	本コマンドは、スイッチの IGMP スヌーピングを有効にします。 「forward_mcrouter_only」が指定されると、スイッチはマルチキャストルーティングプロトコルパケットと IGMP 制御パケットの識別に基づいたルーターポートを学習します。
パラメーター	forward_mcrouter_only - 本コマンドにこのパラメーターを追加すると、スイッチはマルチキャストルーティングプロトコルパケットと IGMP 制御パケットの識別に基づいたルーターポートを学習します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの IGMP スヌーピングを有効にするには

```
#enable igmp_snooping
Command: enable igmp_snooping

Success.

#
```

3.16.6 disable igmp_snooping

目的	スイッチの IGMP スヌーピングを無効にします。
構文	disable igmp_snooping [forward_mcrouter_only]
説明	本コマンドは、スイッチの IGMP スヌーピングを無効にします。 「forward_mcrouter_only」 が指定されると、スイッチはユニキャストルーティングプロトコルパケット、マルチキャストルーティングプロトコルパケット、および IGMP 制御パケットの識別に基づいたルーターポートを学習します。 コマンドの上位互換性について、本コマンドは CLI でサポートされますがルーターポート学習のシステム動作は無効になります。
パラメーター	Forward_mcrouter_only - このパラメーターを本コマンドに追加すると、スイッチはユニキャストルーティングプロトコルパケット、マルチキャストルーティングプロトコルパケット、および IGMP 制御パケットの識別に基づいたルーターポートを学習し、disable igmp_snooping forward_mcrouter_only コマンドは無効になります。スイッチはマルチキャストルーティングプロトコルパケットと IGMP 制御パケットの識別に基づいたルーターポートを学習します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの IGMP スヌーピングを無効にするには

```
#disable igmp_snooping
Command: disable igmp_snooping

Success.

#
```

3.16.7 show igmp_snooping

目的	スイッチ上の IGMP スヌーピングのステータスを表示します。
構文	show igmp_snooping [vlan <vlan_name 32> | vlanid <vidlist>]
説明	本コマンドは、スイッチの IGMP スヌーピングステータスとコンフィグレーションを表示します。
パラメーター	<vlan_name 32> - IGMP スヌーピングコンフィグレーションを表示する VLAN 名を入力します。 <vidlist> - 表示するコンフィグレーションの VID 範囲を入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:IGMP スヌーピングを表示するには

```
#show igmp_snooping
Command: show igmp_snooping

 IGMP Snooping Global State            : Disabled
 Multicast Router Only                 : Disabled

 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                         : Disabled
 Fast Leave                    : Disabled
 Version                       : 3

Total Entries : 1

#
```

3.16.8 show router_ports

目的	現在スイッチで設定されているルーターポートを表示します。
構文	show router_ports [< vlan <vlan_name 32> | vlanid <vidlist> >] [<static | dynamic | forbidden >]
説明	本コマンドは、スイッチに現在設定されているルーターポートを表示します。
パラメーター	<vlan_name 32> - ルーターポートが存在する VLAN 名を入力します。 <vidlist> - 表示するルーターポートの VID 範囲を入力します。 static - 静的に設定されているルーターポートを表示します。 dynamic - 動的に設定されているルーターポートを表示します。 forbidden - 静的に設定されている forbidden (禁止)ルーターポートを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ルーターポートを表示するには

```
#show router_ports
Command: show router_ports

VLAN Name          : default
Static Router Port :
Dynamic Router Port:
Forbidden Router Port:

Total Entries: 1

#
```

3.16.9 show igmp_snooping group

目的	スイッチ上の IGMP スヌーピンググループのコンフィグレーションを表示します。
構文	show igmp_snooping group [< vlan <vlan_name 32> | vlanid <vidlist> >]
説明	本コマンドはスイッチ上の IGMP スヌーピンググループのコンフィグレーションを表示します。
パラメーター	<vlan_name 32> - IGMP スヌーピンググループ情報を表示する VLAN 名を入力します。 <vidlist> - IGMP スヌーピンググループ情報を表示する VID リストを入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: IGMP スヌーピンググループを表示するには

```
#show igmp_snooping group
Command: show igmp_snooping group

Source/Group       : NULL/239.255.255.255
VLAN Name/VID      : default/1
Reports            : 1
Member Ports       : 4
Router Ports       : 8
Up time            : 122
Expire Time        : 260
Filter Mode        : EXCLUDE

Total Entries      : 1

#
```

3.16.10 show igmp_snooping host

目的	特定のポートまたはVLANにグループを登録したIGMPホストを表示します。
構文	show igmp_snooping host [<vlan_name <vlan_name 32> | vlanid <vidlist> | ports <portlist> | group <ipaddr>>]
説明	本コマンドは、特定のポートまたは特定のVLANにグループを登録したIGMPホストを表示します。
パラメーター	<vlan_name 32> -VLANを指定してホスト情報を表示します。VLANまたはポートを指定しない場合、すべての登録ホストが表示されます。 <vlanid>- VLAN IDを指定します。 <portlist>- ポートのリストを指定してホスト情報を表示します。VLANまたはポートを指定しない場合、すべての登録ホストが表示されます。 <ipaddr> - グループのIPアドレスを指定してホスト情報を表示します。
制限事項	なし。
対応バージョン	1.00.00以降

使用例:IGMPスヌーピング高速脱退（Fast Leave）機能を表示するには

```
# show igmp_snooping host
Command: show igmp_snooping host

VLAN ID       Group             Port No        IGMP Host
 --------  -----------------    ---------      ------------
 1             225.0.1.0            2           10.0.0.1
 1             225.0.1.0            2           10.0.0.2
 1             225.0.1.0            3           10.0.0.3
 1             225.0.1.2            2           10.0.0.4
 1             225.0.2.3            3           10.0.0.5
 1             225.0.3.4            3           10.0.0.6
 1             225.0.4.5            5           10.0.0.7
 1             225.0.5.6            5           10.0.0.8
 1             225.0.6.7            4           10.0.0.9
 1             225.0.7.8            4           10.0.0.10
 1             239.255.255.250      7           10.0.0.11

Total Entries : 11

#
```

3.17 リンクアグリゲーションコマンド

3.17.1 create link_aggregation

目的	スイッチの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> [type <lacp | static>]
説明	本コマンドは、固有の識別子を有するリンクアグリゲーショングループを作成します。
パラメーター	<value> - グループ ID を指定します。最大 26 までのリンクアグリゲーショングループを設定できます。グループ ID によって各グループを識別します。 type - グループに使用するリンクアグリゲーションのタイプを指定します。タイプを指定しない場合は、デフォルトタイプは「static」になります。 lacp - ポートグループを LACP 準拠として指定します。LACP は接続されたデバイスと動的なネゴシエーションが行われます。(config lacp_ports を参照のこと)。 LACP 準拠のポートは LACP 準拠のデバイスに接続する必要があります。 static - ポートグループをスタティックとして指定します。 スタティックポートグループを変更した場合、リンク接続の両デバイスで設定を確認してください。 リンクアグリゲーションでは、接続の両デバイスが適切に設定され、ポートグループの設定が同一の速度/デュプレックスである必要があります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:リンクアグリゲーショングループを作成するには

```
#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.
#
```

注意事項

APLGM152GT のリンクアグリゲーショングループ数の最大は、製品搭載ポート数÷2 となります。

メンバーポートは、UTP ポートと Fiber ポートを組み合わせることは出来ません。

認証機能（802.1X 認証、MAC 認証、WEB 認証）とのポート併用はできません。

3.17.2 delete link_aggregation group_id

目的	設定済みの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>
説明	本コマンドは、設定済みのリンクアグリゲーショングループを削除します。
パラメーター	<value> - グループ ID を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:リンクアグリゲーショングループを削除するには

```
#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

#
```

3.17.3 config link_aggregation group_id

目的	作成済みのリンクアグリゲーショングループを設定します。
構文	config link_aggregation group_id <value> < master_port <port> | ports <portlist> | state < enable | disable > >
説明	本コマンドは、上記の create link_aggregation コマンドと併せて作成されたリンクアグリゲーショングループを設定します。
パラメーター	group_id <value> - グループ ID を指定します。各グループはグループ ID によって識別されます。 master_port <port> - マスタポートを指定します。リンクアグリゲーショングループごとに 1 つのマスターポートを設定する必要があります。 ports <portlist> - リンクアグリゲーショングループに所属するすべてのポートを指定します。指定のポートにはマスターポートも含める必要があります。 state <enable | disable> - 指定したリンクアグリゲーショングループを「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。 リンクアグリゲーションの所属ポートと認証機能（802.1X 認証、MAC 認証、WEB 認証）のポート併用はできません。
対応バージョン	1.00.00 以降

使用例:ポート 1-4 でリンクアグリゲーショングループ 1 を設定するには

```
#config link_aggregation group_id 1 master_port 1 ports 1-4
Command: config link_aggregation group_id 1 master_port 1 ports 1-4

Success.

#
```

3.17.4 config link_aggregation

目的	リンクアグリゲーションアルゴリズムと LACP の装置優先度を設定します。
構文	config link_aggregation < algorithm < mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest > | system_priority <value> >
説明	アルゴリズム設定は、負荷分散データを送信ポートに転送する際、参照するパケットの部分を指定します。 LACP の装置優先度設定は、数値が小さいほど優先度が高くなります。
パラメーター	algorithm - リンクアグリゲーションの負荷分散アルゴリズムを設定します。 mac_source - スイッチは送信元 MAC アドレスを検証します。 mac_destination - スイッチは送信先 MAC アドレスを検証します。 mac_source_dest - スイッチは送信元および送信先 MAC アドレスを検証します。 ip_source - スイッチは送信元 IP アドレスを検証します。 ip_destination - スイッチは送信先 IP アドレスを検証します。 ip_source_dest - スイッチは送信元および送信先 IP アドレスを検証します。 system_priority - LACP の装置優先度を 1～65535 の範囲で設定します。値が小さいほど優先度が高くなります。デフォルト値は、32768 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降 1.01.00 以降(system_priority パラメーターをサポート)

使用例:送信先および送信元 MAC のリンクアグリゲーションアルゴリズムを設定するには

```
#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

#
```

注意事項

Unknown unicast/Broadcast/Multicast の分散動作は下記を KEY としたアルゴリズムで振り分けられます。
Unknown unicast、Broadcast、L2 Multicast：MAC_DA、MAC_SA、SRC_PORT
IP Multicast：SIP、DIP、SRC_PORT
MAC_DA：宛先 MAC アドレス
MAC_SA：送信元 MAC アドレス
SRC_PORT：送信元 TCP/UDP ポート番号
SIP：送信元 IP アドレス
DIP：宛先 IP アドレス

3.17.5 show link_aggregation

目的	リンクアグリゲーションのコンフィグレーションを表示します。
構文	show link_aggregation [group_id <value> | algorithm | system_priority]
説明	本コマンドは、スイッチ上のリンクアグリゲーションのコンフィグレーションを表示します。
パラメーター	<value> - グループ ID を指定します。 algorithm - リンクアグリゲーションのアルゴリズムを表示します。 system_priority - LACP の装置優先度を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降 1.01.00 以降(system_priority パラメーターをサポート)

使用例:リンクアグリゲーションのコンフィグレーションを表示するには

```
#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source
Link Aggregation System Priority : 32768

Group ID      : 1
Type:         : Static
Master Port   : 1
Member Port   : 1-4
Active Port   : 1
Status        : Enabled
Flooding Port : 1

Total Entries : 1

#
```

3.17.6 config lacp_ports

目的	LACP 準拠のポートを設定します。
構文	config lacp_ports <portlist> < mode < active | passive > | lacp_timeout <short | long> | port_priority <value> >
説明	本コマンドは、指定された LACP ポートを設定します。 （create link_aggregation コマンドで LACP モードが指定されている場合）
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 mode - LACP 制御フレームの処理モードを active、passive から選択します。 active - Active LACP ポートは、接続されたデバイスに LACP 制御フレームを送信します。これにより LACP 準拠のデバイス間でリンク状態をネゴシエートし、必要に応じて動的に変更されます。ポートグループの変更を行う場合、ネゴシエートのため、いずれかのデバイスで LACP ポートを「Active」に設定する必要があります。 passive - Passive LACP ポートは、接続されたデバイスからの LACP 制御フレームを待ちます。LACP 制御フレームの受信によりリンク状態のネゴシエートが開始されます。 接続するデバイスは両方とも LACP をサポートしている必要があります。 lacp_timeout - 対向装置から受信する LACP 制御フレームの受信タイムアウト時間を設定します。デフォルト設定は、short です。 short - LACP の受信タイムアウト時間を 3 秒に設定します。 long - LACP の受信タイムアウト時間を 90 秒に設定します。 port_priority - LACP のポート優先度を 1～65535 の範囲で設定します。値が小さいほど優先度が高くなります。デフォルト値は、32768 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降 1.01.00 以降(lacp_timeout 及び port_priority パラメーターをサポート)

使用例:LACP ポートモード設定を行うには

```
#config lacp_ports 1-12 mode active
Command: config lacp_ports 1-12 mode active

Success.

#
```

3.17.7 show lacp_ports

目的	LACP ポートモード設定を表示します。
構文	show lacp_ports [<portlist>]
説明	本コマンドは、LACP モード設定を表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。 パラメーターを指定しない場合、すべてのポートの LACP 設定を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降 1.01.00 以降(port_priority パラメーター表示をサポート)

使用例:LACP ポートモード設定を表示するには

```
#show lacp_ports 1-10
Command: show lacp_ports 1-10

Port     Activity    LACP_Timeout    Port_Priority

 -----    --------    ------------    -------------
 1        Active      Short           32768
 2        Active      Short           32768
 3        Active      Short           32768
 4        Active      Long            32768
 5        Active      Long            32768
 6        Passive     Long            10000
 7        Passive     Long            10000
 8        Passive     Long            10000
 9        Passive     Short           10000
 10       Passive     Short           10000

#
```

3.18 ループ防止コマンド

3.18.1 config loopdetect

目的	ループ検知パケットの送信間隔およびループ検知状態の復旧時間を設定します。
構文	config loopdetect 〈 recover_timer 〈 value 0 ｜〈sec 60-1000000〉 〉｜ interval〈sec 1-32767〉 〉
説明	本コマンドは、ループ防止機能の有効ポートから送信されるループ検知パケットの送信間隔およびループ検知状態からの自動復旧時間を設定します。
パラメーター	recover_timer - ループ発生状態から自動復旧までの時間(秒)を設定します。 [0]を設定した場合、自動復旧が無効になるため手動による復旧が必要になります。 手動復旧には以下コマンドを使用します。 「config loopdetect ports〈portlist〉 state disable」 「config loopdetect ports〈portlist〉 state enable」 自動復旧タイマーのデフォルト値は 60 秒です。 interval - ループ防止機能が有効なポートから送信されるループ検知パケット(CTP：Configuration Test Protocol)パケットの送信間隔(秒)を設定します。 デフォルト値は 10 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:復旧タイマーを 0、検知パケットの送信間隔を 20 に設定するには

```
#config loopdetect recover_timer 0 interval 20
Command: config loopdetect recover_timer 0 interval 20

Success.

#
```

注意事項

ループ防止機能によりループ検知の場合、速やかにループ原因を取り除いて下さい。ループ検知状態からリカバリー時間(デフォルト 60 秒)経過すると自動復旧が行われます。ループ状態である場合、次のループ検知まで一時的なループ再発となり、ネットワーク全体が不安定な状態になります。ループ発生源を早期に特定できない場合には、自動復旧を無効とするリカバリー時間(0 秒)を設定とする、手動復旧を設定されることを推奨します。

3.18.2 config loopdetect ports

目的	ループ防止機能をポートに設定します。
構文	config loopdetect ports < <portlist> | all > state < enable | disable > method < shutdown | drop >
説明	本コマンドは、スイッチのポートにループ防止機能を設定します。有効ポートでループ検知した場合の動作モードとして、ポート閉塞(shutdown)または検知のみ(drop)のどちらかを選択できます。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - すべてのポートに設定を適用します。 state - ポートリストに指定されたポートにループ防止機能を「enable」(有効)または「disable」(無効)にします。 デフォルト設定は、「disable」(無効)です。 enable - ループ防止機能のステータスを「enable」(有効)に設定します。 disable - ループ防止機能のステータスを「disable」(無効)に設定します。 method - ループ防止機能設定をしたポートに対して、shutdown 動作または drop 動作のどちらかを定義します。デフォルト値は、「shutdown」です。 shutdown - ポートに shutdown 設定を適用します。 drop - ポートに drop 設定を適用します。Drop 設定ではループ検知しパケット転送は行われます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポートのループ防止機能を有効にするには

```
# config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

#
```

注意事項

ループ防止機能は、機器毎に識別されたループ監視専用フレームを自装置内ポートで受信することでループ検知と判断します。
このループ監視専用フレームは、Tag VLAN には対応しておりません。
（Tag ポートでも Tag 付与されずに送出されます）
そのため、対向機器で転送するには Native VLAN を設定する必要があります。

3.18.3 enable loopdetect

目的	ループ防止機能をスイッチで有効にします。
構文	enable loopdetect
説明	本コマンドは、ループ防止機能をスイッチで「enable」(有効)にします。 デフォルト設定は、「disable」(無効)です。 ループ防止機能は、ループ検知している状態において、LED 可視化機能により本装置の console LED が点滅します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

注意事項

ループ検知状態では、LED 可視化機能により本装置の console LED が点滅します。
なお、ループ検知状態が解除された場合には LED 点滅も同時に解除されます。

使用例:スイッチのループ防止機能を有効にするには

```
# enable loopdetect
Command: enable loopdetect

Success.

#
```

3.18.4 disable loopdetect

目的	ループ防止機能をスイッチで無効にします。
構文	disable loopdetect
説明	本コマンドは、ループ防止機能をスイッチで無効にします。 デフォルト設定は、「disable」(無効)です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチのループ防止機能を無効にするには

```
# disable loopdetect
Command: disable loopdetect

#
```

3.18.5 show loopdetect

目的	ループ防止機能のスイッチ設定を表示します。
構文	show loopdetect
説明	本コマンドは、ループ防止機能のスイッチ設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ループ防止機能のスイッチ設定を表示するには

```
#show loopdetect
Command: show loopdetect

 Loopdetect Global Settings
 --------------------------
 Loopdetect Status         : Enabled
 Loopdetect Interval       : 20
 Recover Time              : 0

#
```

3.18.6 show loopdetect ports

目的	ループ防止機能のポート設定を表示します。
構文	show loopdetect ports < <portlist> | all >
説明	本コマンドは、ループ防止機能のポート設定と検知状態を表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。 all - すべてのポートが対象になります。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 1～5 のループ防止機能のステータスを表示するには

```
#show loopdetect ports 1-5
Command: show loopdetect ports 1-5

Port   Loopdetect State   Method     Loop Status
------ ----------------- ---------- ------------
1      Enabled            Shutdown   Normal
2      Enabled            Shutdown   Normal
3      Enabled            Shutdown   Normal
4      Enabled            Shutdown   Normal
5      Enabled            Shutdown   Normal
```

3.19 MAC ベース VLAN コマンド

3.19.1 create mac_based_vlan

目的	スタティック MAC ベース VLAN エントリーを作成します。
構文	create mac_based_vlan mac_address <macaddr> < vlan <vlan_name 32> | vlanid <vlanid 1-4094 > >
説明	本コマンドは、スタティック MAC ベース VLAN エントリーを作成します。 スタティック MAC ベース VLAN エントリーが作成されると、このユーザーからのトラフィックはこのポートで動作する PVID に関係なく指定した VLAN の下で、実行されます。
パラメーター	<macaddr> - VLAN を作成する対象の MAC アドレスを入力します。 <vlan_name 32> - MAC アドレスに対応付けされる VLAN 名を入力します。 <vlanid 1-4094 > - VLAN に対応付けされる VLAN ID を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベース VLAN ローカルエントリーを作成するには

```
# create mac_based_vlan mac_address 00-40-66-00-00-01 vlan default
Command: create mac_based_vlan mac_address 00-40-66-00-00-01 vlan default

Success.

#
```

3.19.2 delete mac_based_vlan

目的	スタティック MAC ベース VLAN エントリーを削除します。
構文	delete mac_based_vlan [mac_address <macaddr> vlan <vlan_name 32> vlanid <vlanid 1-4094 >]
説明	本コマンドは、データベースエントリーを削除します。 MAC アドレスおよび VLAN を指定しない場合、ポートに対応付けされたスタティックエントリーのすべてが削除されます。
パラメーター	<macaddr> - エントリーを削除する対象の MAC アドレスを入力します。 <vlan_name 32> - MAC アドレスに対応付けされる VLAN 名を入力します。 <vlanid 1-4094 > - VLAN に対応付けされる VLAN ID を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スタティック MAC ベース VLAN エントリーを削除するには

```
#delete mac_based_vlan mac_address 00-40-66-00-00-01 vlan default
Command: delete mac_based_vlan mac_address 00-40-66-00-00-01 vlan default

Success.
```

3.19.3 show mac_based_vlan

目的	スタティック MAC ベース VLAN エントリーを表示します。
構文	show mac_based_vlan [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094 >]
説明	本コマンドは、スタティック MAC ベース VLAN エントリーを表示します。
パラメーター	mac <macaddr> - 表示するエントリーの MAC アドレスを入力します。 vlan <vlan_name 32> - 表示するエントリーの VLAN 名を入力します。 vlanid <vlanid 1-4094> - VLAN に対応付けされる VLAN ID を入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: MAC ベース VLAN エントリーを表示するには

```
# show mac_based_vlan
Command: show mac_based_vlan

  MAC Address       VLAN    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    802.1X

Total Entries: 3

#
```

3.20 MLD スヌーピングコマンド

3.20.1 config mld_snooping

目的	スイッチに MLD スヌーピングを設定します。
構文	config mld_snooping < vlan <vlan_name 32> | vlanid <vidlist> | all > < state <enable | disable> | fast_done < enable | disable > >
説明	本コマンドは、スイッチに MLD スヌーピングを設定します。
パラメーター	<vlan_name 32> - MLD スヌーピングを設定する VLAN 名を入力します。 <vidlist> - 設定される VLAN ID の範囲を入力します。 all- スイッチのすべての VLAN を設定します。 state - 選択した VLAN の MLD スヌーピング機能を「enable」(有効)または「disable」(無効)にします。 fast_done - MLD スヌーピング Fast done 機能を「enable」(有効)または「disable」(無効)にします。 この機能を「enable」（有効）にするとメンバーは MLD の完了メッセージがシステムに受信されるとすぐにグループから抜けることができます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MLD スヌーピングのステートを有効にしてデフォルトの VLAN に設定するには

```
#config mld_snooping vlan default state enable
Command: config mld_snooping vlan default state enable

Success.

#
```

3.20.2 config mld_snooping querier

目的	MLD スヌーピングクエリアのタイマーと属性を設定します。
構文	config mld_snooping querier < vlan <vlan_name 32> | vlanid <vidlist> | all > < query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_listener_query_interval <sec 1-25> >
説明	本コマンドは、一般的なクエリー送信の間隔（秒）、リスナーからのレポートを待つ最大時間(秒)を設定し、MLD スヌーピングによって保証されるパケットの損失を許容します。
パラメーター	<vlan_name 32> - MLD スヌーピングを設定する VLAN 名を入力します。 <vidlist>- VLAN ID リストを入力します。 all- スイッチのすべての VLAN を設定します。 query_interval - 一般的なクエリー送信間隔を秒単位で指定します。 デフォルト値は、125 秒です。 max_reponse_time - リスナーからのレポートを待つ最大時間（秒)です。 デフォルト値は、10 秒です。

パラメーター	robustness_variable - 予想されるサブネット上のパケットの損失に応じてこの変数を微調整します。Robustness Variable（堅牢性変数）の値は以下の MLD メッセージ間隔を計算する場合に使用されます。 Group listener interval - マルチキャストルーターがネットワーク上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。間隔の計算は以下の通りです。(堅牢性変数 x クエリ間隔) + (1 x クエリ応答間隔) Other querier present interval - マルチキャストルーターがクエリアである他のマルチキャストルーターがないと判断するまでの時間です。間隔の計算は以下の通りです。（堅牢性変数 x クエリ間隔）+ (0.5 x クエリ応答間隔) Last listener query count - ルーターがグループ内にローカルリスナーがいないと見なす前に送信されたグループに固有なクエリ数です。デフォルト値は Robustness Variable (堅牢性変数)の値です。 デフォルトでは robustness variable (堅牢性変数)は「2」に設定されています。パケット損失が高くなると予想する場合には、この値を増やします。 last_listener_query_interval - Done-group メッセージへの応答として送信したメッセージを含む group-specific query メッセージ間の最大時間です。この間隔を短くして、ルーターがラストグループリスナー損失の検出時間を減少させることができます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:クエリ間隔を 125 秒、状態を有効にして MLD スヌーピングクエリアを設定するには

```
#config mld_snooping querier vlan default query_interval 125
Command: config mld_snooping querier vlan default query_interval 125 state enable

Success.

#
```

3.20.3 config mld_snooping mrouter_ports

目的	ポートをルーターポートとして設定します。
構文	config mld_snooping mrouter_ports <vlan_name 32> < add | delete > <portlist>
説明	本コマンドは、マルチキャストイネーブルのルーターに接続するポート範囲を指定します。これは、プロトコルの種類にかかわらず送信先としてルーターが持つすべてのパケットをマルチキャストイネーブルのルーターに到達するように設定します。
パラメーター	<vlan_name 32> - ルーターポートが存在する VLAN 名を入力します。 <add | delete> - ルーターポートを追加または削除します。 <portlist> - 設定するポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ルーターポートに 1～10 のポート範囲を設定するには

```
# config mld_snooping mrouter_ports default add 1-10
Command: config mld_snooping mrouter_ports default add 1-10

Success.

#
```

3.20.4 config mld_snooping mrouter_ports_forbidden

目的	ポートを forbidden（禁止）ルーターポートとして設定します。
構文	config mld_snooping mrouter_ports_forbidden <vlan_name 32> < add | delete > <portlist>
説明	本コマンドは、マルチキャストイネーブルのルーターに接続しないポート範囲を指定します。 これは、禁止ルーターポートがルーティングパケットを伝播しないようにします。
パラメーター	<vlan_name 32> - 禁止ルーターポートが存在する VLAN 名を入力します。 <add | delete> - 禁止ルーターポートを追加または削除します。 <portlist> - 設定するポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:禁止ルーターポートに 1～10 のポート範囲を設定するには

```
#config mld_snooping mrouter_ports_forbidden default add 1-10
Command: config mld_snooping mrouter_ports_forbidden default add 1-10

Success.

#
```

3.20.5 enable mld_snooping

目的	スイッチの MLD スヌーピングを有効にします。
構文	enable mld_snooping
説明	本コマンドは、スイッチの MLD スヌーピングを有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

注意事項

MLD スヌーピングバージョン 2 のソースフィルタリング機能は未サポートです。

使用例:スイッチの MLD スヌーピングを有効にするには

```
# enable mld_snooping
Command: enable mld_snooping

Success.

#
```

3.20.6 disable mld_snooping

目的	スイッチの MLD スヌーピングを無効にします。
構文	disable mld_snooping
説明	本コマンドは、スイッチの MLD スヌーピングを無効にします。 MLD スヌーピングを無効にすると、デフォルトによりすべての MLD と IPv6 マルチキャストトラフィックがスイッチ内でフラッドします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの MLD スヌーピングを無効にするには

```
# disable mld_snooping
Command: disable mld_snooping

Success.

#
```

3.20.7 show mld_snooping

目的	スイッチ上の MLD スヌーピングコンフィグレーションを表示します。
構文	show mld_snooping [vlan <vlan_name 32> | vlanid <vidlist>]
説明	本コマンドは、スイッチの MLD スヌーピングコンフィグレーションを表示します。
パラメーター	<vlan_name 32> - MLD スヌーピングコンフィグレーションを表示する VLAN 名を入力します。 <vidlist> - VLAN ID リストを入力します。 パラメーターを指定しない場合、システムはすべての MLD スヌーピングのコンフィグレーションを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MLD スヌーピングを表示するには

```
# show mld_snooping
Command: show mld_snooping

MLD Snooping Global State    : Enabled

VLAN  Name                   : default
Query Interval               : 125
Max Response Time            : 10
Robustness Value             : 2
Last Listener Query Interval : 1
Querier Router Behavior      : Non-Querier
State                        : Disabled
Fast Done                    : Disabled
Receive Query Count          : 0

Total Entries: 1

#
```

3.20.8 show mld_snooping group

目的	スイッチ上の MLD スヌーピンググループコンフィグレーションを表示します。
構文	show mld_snooping group [vlan <vlan_name 32> | vlanid <vidlist>]
説明	本コマンドは、スイッチの MLD スヌーピングコンフィグレーションを表示します。
パラメーター	<vlan_name 32> - MLD スヌーピンググループコンフィグレーション情報を表示する VLAN 名を入力します。 <vidlist> - MLD スヌーピンググループコンフィグレーション情報を表示する VLAN ID を入力します。 パラメーターを指定しない場合、システムはすべての MLD グループスヌーピングコンフィグレーションを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MLD スヌーピングを表示するには

```
#show mld_snooping group
Command: show mld_snooping group

Source/Group     : 2000::100:10:10:5/FF0E::100:0:0:20
VLAN Name/VID    : default/1
Member Ports     : 24
Router Ports     :
UP Time          : 5
Expiry Time      : 260
Filter Mode      : INCLUDE

Source/Group     : 2000::100:10:10:5/FF0E::100:0:0:20
VLAN Name/VID    : default/1
Member Ports     : 24
Router Ports     :
UP Time          : 5
Expiry Time      : 260
Filter Mode      : EXCLUDE

Source/Group     : NULL/FF0E::100:0:0:21
VLAN Name/VID    : default/1
Member Ports     : 24
Router Ports     :
UP Time          : 5
Expiry Time      : 260
Filter Mode      : EXCLUDE

#
```

3.20.9 show mld_snooping mrouter_ports

目的	現在スイッチで設定されているルーターポートを表示します。
構文	show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vidlist>] [static | dynamic | forbidden]
説明	本コマンドは、スイッチに現在設定されているルーターポートを表示します。
パラメーター	<vlan_name 32> - 情報を表示するルーターポートが存在する VLAN 名を入力します。 <vidlist> - 情報を表示する設定済みルーターの VLAN ID 範囲を入力します。 static -静的に設定されているルーターポートを表示します。 dynamic - 動的に設定されているルーターポートを表示します。 forbidden - 静的に設定されている forbidden (禁止)ルーターポートを表示します。 パラメーターを指定しない場合、システムはスイッチに現在設定されているすべてのルーターポートを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ルーターポートを表示するには

```
# show mld_snooping mrouter_ports
Command: show mld_snooping mrouter_ports

VLAN Name               : default
Static Router Port      : 1-10
Dynamic Router Port     :
Forbidden Router Port   :

VLAN Name               : vlan2
Static Router Port      :
Dynamic Router Port     :
Forbidden Router Port   :

Total Entries : 2

#
```

3.21 マルチプルスパニングツリープロトコル（MSTP）コマンド

本スイッチは3種類のバージョンのスパニングツリープロトコル（802.1D STP、802.1w Rapid STP、802.1s MSTP）をサポートしています。 マルチプルスパニングツリープロトコル（MSTP）はIEEE委員会により定義された標準規格で、複数のVLANを1つのスパニングツリーインスタンスにマッピングし、ネットワーク中に複数の経路を提供します。従って、これらのMSTPコンフィグレーションはトラフィックロードのバランシングを行い、単一のスパニングツリーインスタンスに障害が発生した場合でも、広い範囲で影響を与えないようにすることができます。これにより、障害が発生したインスタンスに代わって新しいトポロジーを素早く収束します。これらVLAN用のフレームは、これらの3つのスパニングツリープロトコル（STP、RSTP、MSTP）のいずれかを使用して、素早く適切に相互接続されたブリッジを通して処理されます。本プロトコルでは、BPDU（Bridge Protocol Data Unit）パケットにタグ付けを行い、受信するデバイスが、スパニングツリーインスタンス、スパニングツリーリージョン、およびそれらに対応づけられたVLANを区別できるようにしています。これらのインスタンスはInstance_IDによって分類されます。MSTPでは、複数のスパニングツリーをCIST（Common and Internal Spanning Tree）で接続します。 CISTは自動的に各MSTPリージョンとその最大範囲を決定し、1つのスパニングツリーを構成する1つの仮想ブリッジのように見せかけます。 そのため、異なるVLANを割り当てられたフレームは、ネットワーク上の管理用に設定されたリージョン中の異なるデータ経路を通ります。

ネットワーク上のMSTPを使用しているスイッチは、以下の3つの属性を持つ1つのMSTPコンフィグレーションを持ちます。

(1) 32文字までの半角英数字で定義された「コンフィグレーション名」（「config stp mst_config_id」コマンドでのname <string>として設定済み）。
(2) 「コンフィグレーションリビジョン番号」（「revision_level」として設定済み）。
(3) 4094件のエレメントテーブル(「VID range」として設定済み)。
(4) スイッチがサポートする4094件までのVLANとインスタンスとの対応づけです。

スイッチでMSTP機能を利用するためには、以下の手順を実行します。
スイッチにMSTP設定を行います（「config stp version」コマンド）。
MSTPインスタンスに適切なスパニングツリープライオリティを設定します（「config stp priority」コマンド）。
共有するVLANをMSTP Instance IDに追加する必要があります（config stp instance_idコマンド）。

3.21.1 enable stp

目的	スイッチのスパニングツリープロトコルをグローバルで有効にします。
構文	enable stp
説明	本コマンドは、スイッチのスパニングツリープロトコルをグローバルで有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:スイッチのスパニングツリープロトコルをグローバルで有効にするには

```
#enable stp
Command: enable stp

Success.

#
```

注意事項

認証機能（MAC 認証、WEB 認証、802.1X 認証）とのポート併用はできません。

3.21.2 disable stp

目的	スイッチのスパニングツリープロトコルをグローバルで無効にします。
構文	disable stp
説明	本コマンドは、スイッチのスパニングツリープロトコルをグローバルで無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチのスパニングツリープロトコルを無効にするには

```
#disable stp
Command: disable stp

Success.

#
```

3.21.3 config stp version

目的	スイッチのスパニングツリーのバージョンをグローバルに設定します。
構文	config stp version〈 mstp	rstp	stp 〉
説明	本コマンドは、スイッチのスパニングツリーのバージョンを選択します。
パラメーター	mstp - 本パラメーターを選択すると、スイッチのマルチプルスパニングツリープロトコル(MSTP)をグローバルに設定します。 rstp - 本パラメーターを選択すると、スイッチのラピッドスパニングツリープロトコル(RSTP)をグローバルに設定します。 stp - 本パラメーターを選択すると、スイッチのスパニングツリープロトコル(STP)をグローバルに設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチをマルチプルスパニングツリープロトコル（MSTP）用にグローバルに設定するには

```
#config stp version mstp
Command: config stp version mstp

Success.

#
```

3.21.4 config stp

目的	スイッチに STP、RSTP、および MSTP を設定します。
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)
説明	本コマンドは、スイッチ全体にスパニングツリープロトコル（STP）を設定します。 STP バージョン用に実行される以下のすべてのコマンドは、現在スイッチに設定されています。
パラメーター	maxage <value 6-40> - 本値は古い情報がネットワークにある冗長パスを永遠に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。 ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリーコンフィグレーション値が矛盾していないかを確認するための値です。 本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。 この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。 6～40 秒の範囲で時間を選択できます。 デフォルト値は 20 です。 maxhops <value 6-40> - スイッチが送信した BPDU（bridge protocol data unit）パケットが破棄される前のスパニングツリー範囲内のデバイス間のホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。スイッチは、その後 BPDU パケットを破棄し、ポートに保持していた情報を解放します。ホップカウントは 6～40 で指定します。デフォルト値は 20 です。 hellotime <value 1-2> - ルートデバイスによるコンフィグレーションメッセージの送信間隔を設定し、スイッチがまだ機能していることを知らせます。1 秒または 2 秒の時間を選択します。デフォルト値は、2 秒です。 forwarddelay <value 4-30> - 状態を変更する前にルートデバイスが待機する最大時間(秒)を設定します。4～30 秒の範囲で時間を選択できます。デフォルト値は 15 秒です。 txholdcount <value 1-10> - 間隔ごとに送信される BPDU Hello パケットの最大数を設定します。デフォルト値は 6 です。 fbpdu <enable | disable> - STP を無効にすると、BPDU パケットが他のネットワークデバイスから送信されます。デフォルト値は「enable」(有効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Maxage を 18、Maxhops を 15 にして STP を設定するには

```
#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

#
```

注意事項

マルチプルスパニングツリープロトコル (MSTP) では、スパニングツリーがポートごとに設定されるため、MSTP を使用するスイッチには「configure stp ports」コマンドを使用して「hellotime」を設定する必要があります。

3.21.5 config stp ports

目的	ポートレベルで STP 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 > | restricted_role < true | false > | restricted_tcn < true | false > | p2p < true | false | auto > | state < enable | disable > | fbpdu < enable | disable > >
説明	本コマンドは、ポートグループに対して STP を作成および設定します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 externalCost - 指定したポートリストに対し、パケットの転送にかかるコストを表すメトリックを定義します。 ポートコストは、自動的に設定するかメトリック値を設定できます。 デフォルト値は、「auto」(自動)です。 auto - 本パラメーターを設定すると、リストに指定したポートに対して、最適な効率でパケット転送スピードを自動的に設定します。 Default port cost: 100Mbps port = 200000. Gigabit port = 20000. <value 1-200000000> - 1～200000000 の範囲で外部コストを指定します。小さい値を指定すると、パケット転送を選択するポートの優先度が高くなります。 hellotime <value 1-2> - 指定ポートがブリッジ接続される LAN 上の他のスイッチに BPDU パケットを送信する間隔を設定します。ルートブリッジであるスイッチは BPDU パケットを送信することで他のスイッチへ通知します。1 秒または 2 秒で時間を選択できます。 デフォルト値は 2 秒です。 migrate <yes | no> - 「Yes」設定では、STP 設定に関する情報をリクエストする他のブリッジに BPDU パケットを送信する場合に設定します。スイッチが RSTP に設定されると、ポートは 802.1D STP から 802.1w RSTP まで移行することができます。 スイッチが MSTP に設定されると、ポートは 802.1D STP から 802.1s MSTP まで移行することができます。 RSTP と MSTP は標準の STP と共存できますが、802.1D ネットワークが 802.1w または 802.1s が有効なネットワークに接続するポート上では、実現されません。 セグメントのすべてまたは一部において 802.1w RSTP または 802.1s にアップグレード可能なネットワークステ

	ーションまたはセグメントに接続したポートでは本パラメーターを「Yes」とします。 edge <true | false | auto> - true を選択するとポートはエッジポートとして指定されます。 ただし、トポロジーの変更によってループ発生の可能性が生じると、エッジポートとしての資格を失います。 また、エッジポートで BPDU パケットを受信すると、そのポートはエッジポートの資格を失います。false は、エッジポートとして指定されていないことを示します。auto は、BPDU パケットを受信しない場合などで自動的にエッジポートとなります。 p2p <true | false | auto> - true は、選択ポートを P2P ポートとして指定します。P2P ポートはエッジポートと似ていますが、P2P ポートは全二重モードでのみ動作する点で異なります。RSTP の特長として、エッジポート同様、P2P ポートは迅速にフォワーディング状態に遷移します。P2P の値が false の場合は、そのポートに P2P ポートの資格がないことを示しています。Auto にすると、ポートはいつでも可能な時に（「true」を指定した時と同様に）P2P ポートとして動作します。ポートの資格を失う時（例えば、半二重モードを指定された時など）、自動的に「false」を指定した時と同様になります。本パラメーターのデフォルト値は、「auto」です。 state <enable | disable> - 指定されたポートで STP を「enable」(有効)または「disable」(無効)にします。デフォルト値は「enable」です。 restricted_role - ルートポートとして選択するかどうかを決定します。 デフォルト値は「false」(偽)です。 restricted_tcn - このポートがトポロジーの変更を伝播するかどうかを決定します。 デフォルト値は「false」(偽)です。 fbpdu <enable | disable> - 有効にすると、STP が指定したポートで無効になっている場合に STP BPDU パケットが他のネットワークデバイスから転送されます。 ユーザーがポートごとに BPDU パケットの転送を有効にしたい場合、最初に次の設定を有効にする必要があります。 1. STP をグローバルに無効にする必要があります。2. BPDU の転送をグローバルで有効にする必要があります。グローバルに STP を無効化するには、「disable stp」コマンドを使用します。「fbpdu」をグローバルに有効化するには、「config stp」コマンドを使用します。 デフォルト値は「enable」 (有効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

注意事項

STP モードにおいては edge の値を true に設定しても機能しません。

使用例:Path cost auto、hellotime 2秒、migration enable、ポート1～2のstate enableでSTPを設定するには

```
#config stp ports 1-2 externalCost auto hellotime 2 migrate yes state enable
Command: config stp ports 1-2 externalCost auto hellotime 2 migrate yes state enable

#
```

3.21.6 create stp instance_id

目的	MSTPにSTPインスタンスIDを作成します。
構文	create stp instance_id <value 1-4>
説明	本コマンドは、マルチプルスパニングツリープロトコル（MSTP）のSTPインスタンスIDを作成します。 スイッチには5個のインスタンス（1つはCISTで変更できません。）があり、4個のインスタンスIDを作成することができます。
パラメーター	<value 1-4> - スイッチにSTPインスタンスを指定するために1～4の範囲から指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:スパニングツリーインスタンス2を作成するには

```
#create stp instance_id 2
Command: create stp instance_id 2

Success.

#
```

3.21.7 config stp instance_id

目的	STPインスタンスIDを追加または削除します。
構文	config stp instance_id <value 1-4> < add_vlan | remove_vlan > <vidlist>
説明	本コマンドは、スイッチに「instance_id」を作成することによって、VLAN ID を設定済みのSTPインスタンスにマップします。 STPインスタンスは、同じMSTPコンフィグレーションを持つ複数メンバーを持っています。 ネットワークにおける、STP範囲の数には制限はありませんが、各範囲は、最大5個のSTPインスタンス（1つは変更できないデフォルトエントリー）をサポートしています。 VLAN IDは一度に1つのSTPインスタンスにだけ所属することができます。
パラメーター	<value 1-4> - スイッチにinstance_idを指定するために1～4の範囲から指定します。 スイッチは「0」として設定されている変更できないデフォルトインスタンスID1個を含め5個のSTP範囲をサポートしています。 add_vlan - vid_range <vidlist>パラメーターと共に、設定済みのSTPinstance_idにVLAN IDを追加します。

パラメーター	remove_vlan - vid_range <vidlist>パラメーターと共に、設定済みのSTPinstance_id から VLAN ID を削除します。 <vidlist> - スイッチに設定済みの VLAN の中から、VLAN ID の範囲を指定します。 ID 番号が 1～4094 の範囲でスイッチの VLAN ID をサポートします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:インスタンス ID 2 を設定して VLAN ID 10 を追加するには

```
#config stp instance_id 2 add_vlan 10
Command: config stp instance_id 2 add_vlan 10

Success.

#
```

使用例:インスタンス ID 2 から VLAN ID 10 を削除するには

```
#config stp instance_id 2 remove_vlan 10
Command: config stp instance_id 2 remove_vlan 10

Success.

#
```

注意事項

同じ STP instance_id を持つ同じ STP 範囲にあるスイッチがマップされ、同じコンフィグレーションの revision_level 番号と同じ name（名前）を持つ必要があります。

3.21.8 delete stp instance_id

目的	スイッチから STP インスタンス ID を削除します。
構文	delete stp instance_id <value 1-4>
説明	本コマンドは、スイッチから設定済みの STP インスタンス ID を削除します。
パラメーター	<value 1-4> - スイッチにスパニングツリーインスタンスを指定するために 1～4 の範囲から指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチから STP インスタンス ID 2 を削除するには

```
#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

#
```

3.21.9 config stp priority

目的	STP インスタンスコンフィグレーションを更新します。
構文	config stp priority 〈value 0-61440〉 instance_id 〈value 0-4〉
説明	本コマンドは、スイッチの STP インスタンスコンフィグレーション設定を更新します。 MSTP は、ルートブリッジ、ルートポート、指定ポートの選択に優先度を使用します。 STP 領域に高い優先度を割り当てることにより、スイッチに転送パケット用として選択した instance_id に優先権を与えます。 優先度の設定値が低いほど、優先度は高くなります。
パラメーター	priority 〈value 0-61440〉 - 0～61440 の値を選択し、転送パケットに対して指定されたインスタンス ID に優先度を指定します。数字が低いほど、優先度は高くなります。このエントリーは 4096 の倍数とする必要があります。 instance_id 〈value 0-4〉 - 設定済みのインスタンス ID に対応する優先度の値を入力します。0 のインスタンス ID は、スイッチに内部設定されたデフォルトの instance_id (CIST) であることを示します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Instance_id 2 に対する優先度値に 4096 を設定するには

```
#config stp priority 4096 instance_id 2
Command: config stp priority 4096 instance_id 2

Success.

#
```

3.21.10 config stp mst_config_id

目的	MSTP コンフィグレーション ID を更新します。
構文	config stp mst_config_id ｛ revision_level 〈int 0-65535〉	name 〈string〉 ｝
説明	本コマンドは、スイッチに現在設定されている MSTP コンフィグレーションを一意に識別します。ここに入力された情報は、それが属する MSTP 範囲の識別子として BPDU パケットに添付されます。 同じ revision_level と名前を持つスイッチは、同じ MSTP 範囲の一部であると見なされます。
パラメーター	revision_level 〈int 0-65535〉 - 0～65535 の値を入力し、MSTP 領域を識別します。この値は名前と共に、スイッチに設定した MSTP 領域を識別します。デフォルト値は、0 です。 name 〈string〉 - 32 文字以内の半角英数字の文字列を入力して、スイッチの MSTP 領域を一意に識別します。 この name（名前）は、revision_level の値と共に、スイッチに設定した MSTP 領域を識別します。name（名前)が入力されないと、デフォルト名はデバイスの MAC アドレスになります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:リビジョンレベルを 10 にし、名前を「APS」にしてスイッチの MSTP 領域を設定するには

```
#config stp mst_config_id revision_level 10 name APS
Command: config stp mst_config_id revision_level 10 name APS

Success.

#
```

3.21.11 config stp mst_ports

目的	MSTP インスタンスのポートコンフィグレーションを更新します。
構文	config stp mst_ports <portlist> instance_id <value 0-4> < internalCost < auto | <value 1-200000000> > | priority <value 0-240> >
説明	本コマンドは、STP instance_id のポートコンフィグレーションを更新します。ループが発生すると、MSTP 機能はポートの優先度を使用して、フォワーディング状態に遷移させるインターフェースを選択します。 最初に転送させるために選択するインターフェースには高い優先度を付与します。 優先値が同じインスタンスでは、MSTP 機能は最小のポート番号をフォワーディング状態にし、他のインターフェースをブロックします。 低優先度値が転送パケットのために、より高い優先度を意味することにご注意ください。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 instance_id <value 0-4> - スイッチに設定済みの instance_id を指定するために 0～4 の範囲から数値を入力します。0 のエントリーは CIST (Common and Internal Spanning Tree) を示します。 internalCost - 本パラメーターは、インターフェースが STP インスタンス内で選択される場合、指定ポートへの転送パケットの相対的なコストを設定します。 デフォルト値は「auto」です。次の 2 つのオプションがあります： auto - internalCost に本パラメーターを選択すると、インターフェースに自動的に最適な最速ルートを設定します。 デフォルト値はインターフェースのメディアスピードに基づきます。 value 1-200000000 - ループが発生した場合、1～200000000 の範囲の値を持つコストを使用して最速ルートを設定します。internalCost の値が低いほど、高速で伝送されます。 priority <value 0-240> - ポートインターフェースの優先値を 0～240 の範囲から指定します。 最初に転送させたいインターフェースには高い優先度 (小さい数値) を与え、 最後に転送させたいインターフェースには低い優先度(大きい数値)を与えます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: インスタンス ID 2、自動 internalCost、優先度 16 でポート 1～5 を指定するには

```
#config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16
Command : config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16

Success.

#
```

3.21.12 show stp

目的	スイッチに現在設定されている STP コンフィグレーションを表示します。
構文	show stp
説明	本コマンドは、スイッチの STP コンフィグレーションを表示します。
パラメーター	なし
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチの STP のステータスを表示するには
ステータス 1: STP 互換バージョンで有効にされた STP

```
#show stp
Command: show stp

STP Bridge Global Settings
 ---------------------------
 STP Status          : Enabled
 STP Version         : STP compatible
 Max Age             : 20
 Hello Time          : 2
 Forward Delay       : 15
 Max Hops            : 20
 TX Hold Count       : 6
 Forwarding BPDU     : Enabled

#
```

ステータス 2: RSTP に対し有効にされた STP

```
#show stp
Command: show stp

STP Bridge Global Settings
 --------------------------
STP Status          : Enabled
STP Version         : RSTP
Max Age             : 20
Hello Time          : 2
Forward Delay       : 15
Max Hops            : 20
TX Hold Count       : 6
Forwarding BPDU     : Enabled

#
```

ステータス 3: MSTP に対し有効にされた STP

```
#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

#
```

3.21.13 show stp ports

目的	スイッチ現在設定されている STP ポートコンフィグレーションを表示します。
構文	show stp ports [<portlist>] [instance <value 0-4>]
説明	本コマンドは、特定のポートまたはポートグループに対する STP ポート設定を表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。 1 つのポート情報が表示されます。 ポートを指定しない場合、ポート 1 の STP 情報が表示されます。 スペースバー、「p」および「n」キーを使用して、残りのポートの情報を表示します。 instance <value 0-4> - 事前に設定した instance_id に対応する ID を 0～4 の間で入力します。 0 のインスタンスは、スイッチの内部に設定したデフォルトの instance_id (CIST) を示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 1 の STP ポート情報を表示するには（スイッチに有効な STP）

```
#show stp ports
Command: show stp ports

MSTP Port Information
 ---------------------
 Port Index     : 1     , Hello Time: 2 /2 , Port STP Enabled  ,
 Restricted role   : False,  Restricted TCN : False
 External PathCost : Auto/200000   , Edge Port : Auto /No , P2P : Auto /Yes
 Port Forward BPDU : Enabled
 MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
 -----  ------------------  ----------------  ----  ----------  ----------
 0      N/A                 200000            128   Disabled    Disabled

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

3.21.14 show stp instance

目的	スイッチの STP インスタンスコンフィグレーションを表示します。
構文	show stp instance [<value 0-4>]
説明	本コマンドは、スイッチの STP インスタンス設定と STP インスタンスの動作状態を表示します。
パラメーター	<value 0-4> - スイッチに設定済みの instance_id を入力します。 0 のエントリーは、スイッチの内部に設定されている CIST の STP コンフィグレーションを表示します。
制限事項	なし
対応バージョン	1.00.00 以降

使用例:スイッチのインスタンス 0（内部 CIST）に対する STP インスタンスコンフィグレーションを表示するには

```
#show stp instance 0
Command: show stp instance 0

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      : 32766/00-40-66-39-78-E2
 External Root Cost          : 200012
 Regional Root Bridge        : 32768/00-40-66-1A-33-24
 Internal Root Cost          : 0
 Designated Bridge           : 32768/00-40-66-71-20-D6
 Root Port                   : None
 Max Age                     : 20
 Forward Delay               : 15
 Time Since Topology Change  : 0 day(s) 0:00:27
 Topology Changes Count      : 1

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

3.21.15 show stp mst_config_id

目的	MSTP コンフィグレーション ID を表示します。
構文	show stp mst_config_id
説明	本コマンドは、スイッチの MSTP コンフィグレーション ID を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに現在設定されている MSTP コンフィグレーション ID を表示するには

```
#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
---------------------------------------

Configuration Name : 00:40:66:1A:33:24           Revision Level :0
MSTI ID           VID list
-------           ------------------------------------------------
   CIST           1-4094

#
```

3.22 パケットストーム制御コマンド

コンピュータネットワーク上にはマルチキャストやブロードキャストなどのパケットが絶えずあふれています。このトラフィックはネットワーク上の端末の不良や、故障したネットワークカードなどの誤動作によって増加することもあります。その結果、スイッチの処理能力問題が発生し、ネットワーク全体のパフォーマンスに影響を与えることがあります。本スイッチではこのパケットストーム状況を監視し制御することが可能です。

パケットストーム制御では、スイッチに入力されたパケットのスキャンを行い、ユーザーが指定した閾値を監視し制御します。動作モードには「drop」または「shutdown」を指定することが出来ます。

「drop」オプションでは、スイッチ内のカウンタをインターバル時間毎に監視し、閾値を超えた分のパケットは次に監視する間まで破棄されます。監視の対象となるパケットストームは、ブロードキャストとマルチキャスト、宛先不明のユニキャストパケットです。

「shutdown」オプションでは、ブロードキャストとマルチキャストを対象にスイッチ内のカウンタをインターバル時間毎に監視し、「countdown」オプションで指定した時間内（0 秒～1800 秒）にパケットストームが継続すると、ポート閉塞し、警告メッセージを出力します。

閉塞したポートの復旧には、(1)10 秒から 300 秒後の自動リカバリーを待つか、(2) 手動コマンドにより復旧させる方法があります。手動コマンドで復旧するには、対象ポートのステータスを無効、有効に切り替える必要があります。

3.22.1 config traffic control

目的	ブロードキャスト/マルチキャスト/宛先不明のユニキャストパケットストーム制御を設定します。 ハードウェアストーム制御に加え、ソフトウェアメカニズムがトラフィックレートのモニタリングをします。
構文	config traffic control ＜〈portlist〉｜ all ＞＜ broadcast ＜ enable ｜ disable ＞｜ multicast ＜ enable ｜ disable ＞｜ unicast ＜ enable ｜ disable ＞｜ action ＜ drop ｜ shutdown ＞｜ threshold 〈value 64-1000000〉｜ countdown ＜ sec 0-1800〉｜ time_interval 〈sec 5-30〉｜ recover_time〈sec 10-300〉＞
説明	本コマンドは、ブロードキャスト/マルチキャスト/宛先不明のユニキャストパケットストーム制御を設定します。 ソフトウェアトラフィック制御メカニズムを追加することで、ハードウェアとソフトウェアの両メカニズムが使用できます。ソフトウェアの制御により、シャットダウン機能とスイッチのリカバリーを提供します。
パラメーター	〈portlist〉- トラフィック制御のために設定するポート範囲を指定します。 all - スイッチのトラフィック制御のためにすべてのポートを設定するよう指定します。 broadcast 〈enable ｜ disable〉- ブロードキャストストーム制御を「enable」(有効)または「disable」(無効)にします。 multicast 〈enable ｜ disable〉- マルチキャストストーム制御を「enable」(有効)または「disable」(無効)にします。 unicast 〈enable ｜ disable〉- 宛先不明のユニキャストトラフィック制御を「enable」(有効)または「disable」(無効)にします。 action － スイッチでパケットストームを検知した際の動作モードを設定します。 動作モードには、「drop」または「shutdown」を指定することが出来ま

	す。 drop - スイッチのハードウェアによるトラフィック制御により、パケットストームの発生を検知します。パケットストームが検知されると、状態が改善するまで閾値を超えた分のパケットを廃棄します。 shutdown - スイッチのソフトウェアによるトラフィック制御により、パケットストームの発生を検知します。パケットストームが検出されると、ブロードキャストとマルチキャストを対象にスイッチ内のカウンタをカウントダウン時間監視します。さらにカウントダウンタイマー経過後もパケットストームが続く場合には、そのポートを閉塞します。閉塞したポートの復旧には、(1) 指定時間後の自動リカバリーを待つか、(2) 「config ports 1 state disable」および「config ports 1 state enable」コマンドを使用して手動でポートをリセットすることで復旧できます。 threshold <value 64-1000000> - 指定されたトラフィックを制御する閾値です。 drop モードの単位は Kbit/秒です。shutdown モードでの単位は packets/秒です。デフォルト値は drop モードで 64Kbit/秒です。 time_interval - スイッチのチップ情報からトラフィック制御機能に送られるマルチキャストおよびブロードキャストパケットのカウンタ監視間隔を設定します。 このパケットカウンタを監視することで、入力トラフィックが閾値を超過したことを検出します。 <sec 5-30> - Interval を 5～30 秒間隔に設定します。デフォルト値は 5 秒です。 countdown - パケットストームが継続しているポートをシャットダウンするまでの時間(秒)を指定します。本パラメーターは、action フィールドで shutdown を指定し、ソフトウェアによるトラフィック制御を行う場合に有効です。 <sec 0-1800> - デフォルト値は 0 で、ポートはシャットダウンされません。シャットダウンするまでのスイッチが待機する時間を 1～1800 秒で指定します。 recover_time - shutdown モードにおけるストームの検知により閉塞されたポートを自動的に復旧するまでの待機時間を設定します。 <sec 10-300> - 自動復旧待機時間を 10～300 秒に設定します。デフォルト値は、300 です。action パラメータで drop モードを指定した場合には適用できません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1～12 に対してブロードキャストストーム閾値 64Kbit/秒・監視間隔 10 秒・カウントダウン時間 0 秒・自動復旧時間 60 秒のトラフィック制御を設定するには

```
#config traffic control 1-12 broadcast enable action shutdown threshold 64 countdown 0
time_interval 10 recover_time 60
Command: config traffic control 1-12 broadcast enable action shutdown threshold 64
countdown 0 time_interval 10 recover_time 60

Success.

#
```

3.22.2 show traffic control

目的	トラフィック制御設定を表示します。
構文	show traffic control [<portlist>]
説明	本コマンドは、スイッチのストームトラフィック制御の設定を表示します。
パラメーター	<portlist> - トラフィック制御を表示するポートまたはポートリストを指定します。ポートリスト範囲の最初と最後の間に - を使用します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 1～4 のトラフィック制御設定を表示するには

```
#show traffic control 1-4
Command: show traffic control 1-4

Port Thres   Broadcast Multicast Unicast  Action   Count Time     Recover
     hold    Storm     Storm     Storm              down  Interval time
---- ------- --------- --------- -------- -------- ----- -------- -------
1    64      Enabled   Disabled  Disabled shutdown 0     10       60
2    64      Enabled   Disabled  Disabled shutdown 0     10       60
3    64      Enabled   Disabled  Disabled shutdown 0     10       60
4    64      Enabled   Disabled  Disabled shutdown 0     10       60

Total Entries  : 4

#
```

3.23 ポートミラーリングコマンド

3.23.1 config mirror port

目的	スイッチにミラーポートを設定し、指定したポートを通過するトラフィックをネットワークスニファーなどのデバイスを接続して監視することができます。
構文	config mirror port <port> [<add | delete> source ports <portlist> < rx | tx | both >]
説明	本コマンドは、指定したポートを透過するトラフィックをネットワークスニファーなどのデバイスを接続してネットワークトラフィックのモニタリングができます。オプション指定により、1 方向または両方向で送受信されるトラフィックを指定するミラーリングも可能です。
パラメーター	<port> - Target ポート(ミラー先ポート)を指定します。 <add | delete> - source ports でミラー元ポートを追加または削除します。 source ports - ミラー元ポートを指定します。Target ポートは含めません。 <portlist> - ミラー元ポートを指定します。複数ポートの指定可能です。 rx - ミラー元ポートで受信するパケットのみをミラーリングします。 tx - ミラー元ポートで送信するパケットのみをミラーリングします。 both - ミラー元ポートで送受信するパケットをミラーリングします。
制限事項	管理者アカウントのみ本コマンドを実行できます。 Target ポートはミラー元ポートとして指定できません。
対応バージョン	1.00.00 以降

使用例:ミラーリングポートを追加するには

```
#config mirror port 1 add source ports 2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

#
```

注意事項

リンクアグリゲーションポートをミラーリングする場合、LAG 所属ポートの全てをミラー元として設定してください。

送信フレームのミラーリングでは、タグなしフレームの場合も送信フレームの VLAN タグ付きフレームでミラーリングします。

Target ポートに VLAN がアサインされている場合、Target ポートに接続したデバイスからのフレームは VLAN 内に送出されます。アサイン VLAN を削除することにより Target ポートからのフレーム送出を回避することができます。

3.23.2 enable mirror

目的	指定済みポートミラーリングコンフィグレーションを有効にします。
構文	enable mirror
説明	本コマンドは以下の 「disable mirror」 と組み合わせて、スイッチにポートミラーリングコンフィグレーションを入力した後に、ポートミラーリングコンフィグレーションを変更せずにミラーリングを有効または無効にすることができます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例ミラーリングコンフィグレーションを有効にするには

```
#enable mirror
Command: enable mirror

Success.

#
```

3.23.3 disable mirror

目的	指定済みポートミラーリングコンフィグレーションを無効にします。
構文	disable mirror
説明	本コマンドは上記の 「enable mirror」 と組み合わせて、スイッチにポートミラーリング設定コンフィグレーションを入力した後に、ポートミラーリングコンフィグレーションを変更せずにミラーリングを有効または無効にすることができます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ミラーリングコンフィグレーションを無効にするには

```
#disable mirror
Command: disable mirror

Success.

#
```

3.23.4 show mirror

目的	スイッチ上のポートミラーリングコンフィグレーションを表示します。
構文	show mirror
説明	本コマンドは、スイッチ上のポートミラーリングコンフィグレーションを表示します。
パラメーター	なし
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ミラーリングコンフィグレーションを表示するには

```
#show mirror
Command: show mirror

Current Settings
Mirror Status  : Enabled
Target Port    : 1
Mirrored Port  :
                 RX :
                 TX : 5-7

#
```

3.24 ポートセキュリティーコマンド

3.24.1 config port_security ports

目的	ポートのセキュリティー機能を設定します。
構文	config port_security ports < <auth_portlist> | all > < admin_state < enable | disable > | max_learning_addr <max_lock_no 0-64> | lock_address_mode < DeleteOnTimeout | DeleteOnReset | Permanent> >
説明	指定したポートで FDB テーブルへ動的に学習される MAC アドレスエントリー数を制限します。エントリー数を超えた MAC アドレスは FDB テーブルに登録されずポートを介した通信を制限します。FDB テーブルの学習方法は、3 つのロックモードから選択できます。
パラメーター	<auth_portlist> - 設定するポートまたはポート範囲を指定します。 all - スイッチのすべてのポートに対しポートセキュリティーを設定します。 admin_state <enable | disable> - 指定したポートのポートセキュリティー機能を「enable」(有効)または「disable」(無効)にします。 max_learning_addr <max_lock_no 0-64> - 指定したポートで動的に学習される MAC アドレスの制限値を設定します。 lock_address_mode <DeleteOnTimout | DeleteOnReset | Permanent> - アドレスをロックする方法を以下の 3 つのオプションから指定します : DeleteOnTimeout - FDB テーブルのエージアウト時間までアドレスをロックします。 DeleteOnReset - 再設定または装置の再起動までアドレスをロックします。 Permanent - ポートセキュリティー機能の無効化までアドレスをロックします。 （装置の再起動後もロックされたアドレスは保持されます）
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポートセキュリティーを設定するには

```
#config port_security ports 1-5 admin_state enable max_learning_addr 5 lock_address_mode
DeleteOnReset
Command: config port_security ports 1-5 admin_state enable max_learning_addr 5
lock_address_mode DeleteOnReset

Success.

#
```

注意事項

認証機能（MAC 認証、WEB 認証、802.1X 認証）とのポート併用はできません。

3.24.2 delete port_security_entry vlan_name

目的	VLAN 名および MAC アドレスよりポートセキュリティーエントリーを削除します。
構文	delete port_security_entry vlan_name <vlan_name 32> mac_address <macaddr>
説明	学習したポートセキュリティーエントリーを VLAN 名および MAC アドレスで削除します。
パラメーター	vlan name <vlan_name 32> - エントリーに対応する VLAN 名を入力します。 mac_address <macaddr> - エントリーに対応する MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポートセキュリティーを削除するには

```
#delete port_security_entry vlan_name default mac_address 00-04-66-10-2C-C7
Command: delete port_security_entry vlan_name default mac_address 00-04-66-10-2C-C7

Success.

#
```

3.24.3 clear port_security_entry port

目的	学習したポートセキュリティーエントリーを指定ポートからクリアーします。
構文	clear port_security_entry port <auth_portlist>
説明	本コマンドは、指定ポートで学習した MAC アドレスエントリーをクリアーします。本コマンドは、ポートのセキュリティー機能のみに関係します。
パラメーター	<auth_portlist> - クリアーするポートまたはポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポートで学習したポートセキュリティーエントリーをクリアーするには

```
# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

#
```

3.24.4 show port_security

目的	ポートセキュリティー情報を表示します。
構文	show port_security [ports <auth_portlist>]
説明	本コマンドは、スイッチのポートのポートセキュリティー情報を表示します。 表示される情報は、ポートセキュリティー、管理者の状態、学習するアドレスの最大数、およびロックモードを含みます。
パラメーター	<auth_portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポートセキュリティー情報を表示するには

```
#show port_security ports 1-10
Command: show port_security ports 1-10

Port_security Trap/Log : Disabled

Port   Admin State   Max. Learning Addr.  Lock Address Mode
----   -----------   -------------------  -----------------
1      Disabled      1                    DeleteOnTimeout
2      Disabled      1                    DeleteOnTimeout
3      Disabled      1                    DeleteOnTimeout
4      Disabled      1                    DeleteOnTimeout
5      Disabled      1                    DeleteOnTimeout
6      Disabled      1                    DeleteOnTimeout
7      Disabled      1                    DeleteOnTimeout
8      Disabled      1                    DeleteOnTimeout
9      Disabled      1                    DeleteOnTimeout
10     Disabled      1                    DeleteOnTimeout

#
```

3.25 プロトコル VLAN コマンド

3.25.1 create dot1v_protocol_group

目的	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 <int 1-16> [group_name <name 32>]
説明	本コマンドは、プロトコル VLAN 機能のプロトコルグループを作成します。
パラメーター	group_id - プロトコルのセットを他のセットと識別するために使用するプロトコルグループの ID を指定します。 group_name - プロトコルグループ名を入力します。最大長は、半角英数字 32 文字です。グループ名が指定されない場合、「ProtocolGroup+group_id」というグループ名が自動的に生成されます。例えば、group_id が 2 の場合に自動生成される名前は、「ProtocolGroup2」となります。自動生成された名前が既存のグループと重複した場合、「ProtocolGroup+group_id+ALT+num」という代替名が使用されます。「num」は 1 から開始します。さらに重複すると、その次の数が代わりに使用されます。 例： Group ID が 1 の場合、自動生成される名前は、「ProtocolGroup1」となります。 この名前が既に存在していると、「ProtocolGroup1ALT1」が代わりに使用されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:プロトコルグループを作成するには

```
# create dot1v_protocol_group group_id 1 group_name General_Group
Command: create dot1v_protocol_group group_id 1 group_name General_Group

Success.

#
```

3.25.2 config dot1v_protocol_group

目的	プロトコルグループにプロトコルを追加します。
構文	config dot1v_protocol_group < group_id <int 1-16> | group_name <name 32> > < add protocol <ethernet_2 | ieee802.3_snap> <hex> | delete protocol < ethernet_2 | ieee802.3_snap > <hex> >
説明	本コマンドは、プロトコルグループにプロトコルを追加します。
パラメーター	group_id - プロトコルのセットを他のセットと識別するために使用するプロトコルグループの ID を指定します。 Group_name - プロトコルグループ名を入力します。 protocol - フレームタイプおよびプロトコル値を指定します。 フレームタイプは、ethernet_2 または ieee802.3_snap を選択できます。 （フレームタイプ ieee802.3_llc には対応しておりません） プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。入力形式は16 ビット(2オクテット)の16進法で、0x0 から 0xFFFF です。 例： IPv4 は 0x0800、IPv6 は 0x86DD、ARP は 0x0806 など。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:プロトコルグループ 1 にプロトコル IPv6 を追加するには

```
#config dot1v_protocol_group group_id 1 add protocol ethernet_2 0x86DD
Command: config dot1v_protocol_group group_id 1 add protocol ethernet_2 0x86DD

The protocol value configured to add will take effect on both frame types ethernet_2 and
ieee802.3_snap.

Success.

#
```

使用例:プロトコルグループ 1 のプロトコル IPv6 を削除するには

```
#config dot1v_protocol_group group_id 1 delete protocol ethernet_2 0x86DD
Command: config dot1v_protocol_group group_id 1 delete protocol ethernet_2 0x86DD

 The protocol value configured to delete will take effect on both frame types ethernet_2
and ieee802.3_snap.

Success.

#
```

3.25.3 delete dot1v_protocol_group

目的	プロトコルグループを削除します。
構文	delete dot1v_protocol_group < group_id <int 1-16> | group_name <name 32> | all >
説明	本コマンドは、プロトコルグループを削除します。
パラメーター	group_id - 削除するグループ ID を指定します。 group_name - 削除するグループ名を指定します。 all - 全グループを削除選択します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:プロトコルグループ 1 を削除するには

```
# delete dot1v_protocol_group group_id 1
Command: delete dot1v_protocol_group group_id 1

Success.

#
```

3.25.4 show dot1v_protocol_group

目的	プロトコルグループで定義されたプロトコルを表示します。
構文	show dot1v_protocol_group <group_id <int 1-16> | group_name <name 32> >
説明	本コマンドは、プロトコルグループで定義されたプロトコルを表示します。
パラメーター	Group_id - 表示するグループ ID を指定します。 グループ ID を指定しない場合、設定したすべてのプロトコルグループが表示されます。 Group_name - プロトコルグループ名を入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:プロトコルグループ ID 1 を表示するには

```
# show dot1v_protocol_group group_id 1
Command: show dot1v_protocol_group group_id 1

Protocol Group ID Protocol Group Name              Frame Type     Protocol Value
----------------- -------------------------------- -------------- --------------
1                 General_Group                    EthernetII     86dd
1                 General_Group                    IEEE802.3 SNAP 86dd



Total Entries: 1
#
```

3.25.5 config port dot1v ports

目的	設定されているプロトコルグループに基づきポートリストから入力するタグなしパケットのために VLAN を割り当てます。
構文	config port dot1v ports 〈all〉〈 add protocol_group 〈 group_id 〈int 1-16〉	group_name 〈name 32〉 〉〈 vlan 〈vlan_name 32〉	vlanid 〈int〉 〉 [priority 〈value 0-7〉]	delete protocol_group 〈 group_id 〈int 1-16〉	all 〉〉
説明	本コマンドは、設定されているプロトコルグループに基づきポートリストから入力するタグなしパケットのための VLAN を割り当てます。この割り当ては、「delete protocol_group」オプションを使用して削除できます。 優先度をコマンドで指定しない場合、デフォルトのポート優先度は、プロトコル VLAN によって分類されるタグなしパケットの優先度になります。
パラメーター	Group_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名を入力します。 Vlan - ポートに本プロトコルグループを対応づける VLAN 名を入力します。 Vlan_id - VLAN ID を指定します。 Priority - プロトコルによって指定される VLAN に分類されたパケットに対応づけられる優先度を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: VLAN marketing-1 を割り当てた全ポートにグループ ID 1 を設定するには

```
# config port dot1v ports all add protocol_group group_id 1 vlan marketing-1
Command: config port dot1v ports all add protocol_group group_id 1 vlan marketing-1

Success.

#
```

3.25.6 show port dot1v

目的	プロトコルグループに基づいたポートから入力するタグなしパケットに対応づけられる VLAN を表示します。
構文	show port dot1v [ports <portlist>]
説明	本コマンドは、プロトコルグループに基づいたポートから入力するタグなしパケットに対応付けられる VLAN を表示します。
パラメーター	Portlist - 表示するポート範囲を指定します。 指定しない場合、すべてのポートの情報が表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 1～2 のプロトコル VLAN 情報を表示するには

```
# show port dot1v ports 1-2
Command: show port dot1v ports 1-2

Port: 1
 Protocol Group ID     VLAN Name                        Protocol Priority
 ------------------    --------------------------------  ----------------
 3                     default                                  -
 4                     VLAN300                                  -
 5                     marketing-1                              -

 Port: 2
 Protocol Group ID     VLAN Name                        Protocol Priority
 ------------------    --------------------------------  ----------------
 3                     default                                  -
 4                     VLAN300                                  -
 5                     marketing-1                              -


Total Entries: 6
#
```

3.26 Q-in-Q コマンド

3.26.1 enable qinq

目的	本コマンドは、Q-in-Q モードを有効にします。
構文	enable qinq
説明	本コマンドは、Q-in-Q モードを有効にします。 Q-in-Q を有効にすると、すべてのネットワークポートの役割が NNI ポートとなり、外部 TPID が 88a8 に設定されます。 既存のスタティック VLAN はすべて SP-VLAN となります。 動的に学習したすべての L2 アドレスは、クリアされます。 GVRP および STP は手動で無効にする必要があります。 スイッチの GVRP を実行する必要がある場合は、先ず最初に、手動で GVRP を有効にします。 Q-in-Q のデフォルト値は、「disable」(無効)です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Q-in-Q を有効にするには

```
#enable qinq
Command: enable qinq

Success.

#
```

3.26.2 disable qinq

目的	本コマンドは、Q-in-Q モードを無効にします。
構文	disable qinq
説明	本コマンドは、Q-in-Q モードを無効にします。 動的に学習したすべての L2 アドレスは、クリアされます。 動的に登録したすべての VLAN エントリーはクリアされ、GVRP は「disable」(無効)になります。 スイッチの GVRP を実行する必要がある場合は、先ず最初に、手動で GVRP を有効にします。既存の SP-VLAN はすべてスタティック IQ VLAN として実行します。 Q-in-Q のデフォルト値は、「disable」(無効)です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Q-in-Q を無効にするには

```
#disable qinq
Command: disable qinq

Success.

#
```

3.26.3 show qinq

目的	グローバル Q-in-Q を表示します。
構文	show qinq
説明	本コマンドは、グローバル Q-in-Q ステータスを表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:グローバル Q-in-Q のステータスを表示するには

```
#show qinq
Command: show qinq

QinQ Status: Enabled

#
```

3.26.4 show qinq ports

目的	グローバル Q-in-Q およびポート Q-in-Q モードのステータスを表示します。
構文	show qinq ports [<portlist>]
説明	本コマンドは、以下を含むグローバル Q-in-Q ステータスを表示します。 Q-in-Q モードでのポートロールおよびポート外部 TPID を含みます。
パラメーター	<portlist> - 表示するポート範囲を指定します。 パラメーターを指定しない場合、システムはすべての Q-in-Q ポート情報を表示します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1～4 の Q-in-Q ステータスを表示するには

```
#show qinq ports 1-4
Command: show qinq ports 1-4

Port Role Outer TPID VLAN Translation
---- ---- ---------- ----------------
1    NNI  0x88a8     Disabled
2    NNI  0x88a8     Disabled
3    NNI  0x88a8     Disabled
4    NNI  0x88a8     Disabled

Total Entries  : 4

#
```

3.26.5 config qinq ports

目的	Q-in-Q ポートを設定します。
構文	config qinq ports ＜ <portlist> ｜ all ＞ [role ＜ nni ｜ uni ＞ ｜ outer_tpid <hex 0x1 - 0xffff> ｜ vlan_translation ＜ enable ｜ disable ＞ ＞
説明	本コマンドは、VLAN 機能のポートレベル設定を行います。Q-in-Q モードが無効であるとき、本設定は有効ではありません。
パラメーター	<portlist> - 設定するポート範囲を入力します。 role - UNI ポートまたは NNI ポートのいずれかを選択します。 outer_tpid - SP-VLAN タグの TPID を入力します。 vlan_translation - 有効と指定された場合、VLAN トランスレーションがそのポートで実行されます。デフォルト設定は、「disable」(無効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1～4 を NNI ポートとして設定し、アウターTPID を 0x88a8 に設定するには

```
#config qinq ports 1-4 role nni outer_tpid 0x88a8
Command: config qinq ports 1-4 role nni outer_tpid 0x88a8

Warning: The outer TPID will be globally applied to all ports!

Success.

#
```

3.26.6 create vlan_translation

目的	新しいルールとして追加される VLAN トランスレーションルールの作成、または現在のルールを置換します。
構文	create vlan_translation [ports <portlist>]< add cvid <vidlist> svid <vlanid 1-4094> ｜ replace cvid <vlanid 1-4094> svid <vlanid 1-4094> > [priority <priority 0-7>]
説明	本コマンドは、VLAN トランスレーションルールを作成して単一 S タグの送信パケットを追加または置換します(C-VID は S-VID に変更し、パケットの TPID はアウターTPID に変更します)。
パラメーター	<portlist> - 設定するポート範囲を指定します。 cvid - UNI ポートからイングレスするパケットの C-VLAN ID を入力します。 svid - C-VLAN ID を置換する、またはパケットに挿入される S-VLAN ID を入力します。 <vlanid 1-4094> - 1～4094 の範囲の VLAN ID を入力します。 priority - プロトコル指定の VLAN で分類したパケットの優先度を設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:S-VLAN 100 を C-VLAN 1-10 に追加の割り当てをする VLAN トランスレーションルールを作成するには

```
#create vlan_translation add cvid 1-10 svid 100
Command: create vlan_translation add cvid 1-10 svid 100

Success.

#
```

3.26.7 delete vlan_translation

目的	VLAN トランスレーションルールを削除します。
構文	delete vlan_translation [ports <portlist> | cvid <vidlist>]
説明	本コマンドは、VLAN トランスレーションルールを削除します。
パラメーター	<portlist> - 削除するポート範囲を指定します。 cvid - VLAN トランスレーションの C-VID ルールを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべての C-VID VLAN トランスレーションルールを削除するには

```
#delete vlan_translation cvid all

Command: delete vlan_translation cvid all

Success.

#
```

3.26.8 show vlan_translation

目的	VLAN トランスレーションルールを表示します。
構文	show vlan_translation [< ports <portlist> | cvid <vidlist> >]
説明	本コマンドは、設定済み VLAN トランスレーションコンフィグレーションを表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。 cvid - 指定した C-VID リストの Q-in-Q トランスレーションルール。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:C-VID 10～C-VID 40 の VLAN トランスレーションルールを表示するには

```
#show vlan_translation
Command: show vlan_translation

Port    CVID       SPVID      Action    Priority
-----   --------   --------   -------   ---------
10      1          1          Add       0

 Total Entries: 1

#
```

3.27 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、細分化した VLAN をさらに小さいポートグループに分割することで VLAN のトラフィックを軽減します。VLAN ルールが優先され、次に、トラフィックセグメンテーションルールが適用されます。

3.27.1 config traffic_segmentation

目的	スイッチの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> forward_list < null | <portlist> >
説明	本コマンドは、スイッチにトラフィックセグメンテーションを設定します。
パラメーター	<portlist> - トラフィックセグメンテーションを設定するポートまたはポート範囲を指定します。 forward_list - 上で指定されたポートから転送されたフレームを受信するポートまたはポート範囲を指定します。 null - ポートは指定されません。 <portlist> - 転送リストのポート範囲を指定します。 このリストはトラフィックセグメンテーション用として指定済みの同一スイッチ上にある必要があります（例：上の config traffic_segmentation で指定した<portlist>)。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 11～15 にフレームを転送するために、ポート 1～10 を設定するには

```
#config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

#
```

3.27.2 show traffic_segmentation

目的	スイッチ上のトラフィックセグメンテーションのコンフィグレーションを表示します。
構文	show traffic_segmentation [<portlist>]
説明	本コマンドは、スイッチのトラフィックセグメンテーションのコンフィグレーションを表示します。
パラメーター	<portlist> - スイッチのトラフィックセグメンテーションコンフィグレーションが表示されるポートまたはポート範囲を指定します。
制限事項	セグメンテーション用ポートリストおよび転送リストは同一スイッチ上になければなりません。
対応バージョン	1.00.00 以降

使用例: ポート 1～10 のトラフィックセグメンテーションのコンフィグレーションを表示するには

```
#show traffic_segmentation 1-10
Command: show traffic_segmentation 1-10

Traffic Segmentation Table

Port  Forward Portlist
----  ------------------------------------------------------------------------

1      1-52
2      1-52
3      1-52
4      1-52
5      1-52
6      1-52
7      1-52
8      1-52
9      1-52
10     1-52

#
```

3.28 VLAN コマンド

3.28.1 create vlan

目的	スイッチの VLAN を作成します。
構文	create vlan <vlan_name 32> tag <vlanid 1-4094> [advertisement]
説明	本コマンドは、スイッチに VLAN を作成します。
パラメーター	<vlan_name 32> - 作成する VLAN 名を入力します。 <vlanid 1-4094> - 作成する VLAN の VLAN ID(1-4094)を入力します。 advertisement - VLAN が GVRP に連携できるように指定します。本パラメーターが設定されないと、スイッチは VLAN に関するすべての GVRP メッセージを送信することができません。
制限事項	管理者アカウントのみ本コマンドを実行できます。 各 VLAN 名は 32 文字以内で指定します。コンフィグレーションごとに最大 4094 まで VLAN を作成できます。
対応バージョン	1.00.00 以降

使用例:VLAN「v1」、「tag 2」を作成するには

```
#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

#
```

3.28.2 delete vlan

目的	スイッチに設定済みの VLAN を削除します。
構文	delete vlan <vlan_name 32> | vlanid <vidlist>
説明	本コマンドは、スイッチに設定済みの VLAN を削除します。
パラメーター	<vlan_name 32> - 削除する VLAN の VLAN 名を入力します。 <vidlist> - 削除する複数の VLAN ID 範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:VLAN「v1」を削除するには

```
#delete vlan v1
Command: delete vlan v1

Success.

#
```

3.28.3 config vlan

目的	設定済みの VLAN にポートを追加します。
構文	config vlan <vlan_name 32> < < add < tagged | untagged | forbidden > | delete > <portlist> | advertisement < enable | disable > >
説明	本コマンドは、設定済み VLAN のポートリストにポートを追加します。 追加ポートに「tagging」(タグ付き)、「untagging」(タグなし)、「forbidden」(禁止)の指定ができます。 デフォルトによりポートは「untagging」(タグなし)として割り当てられます。
パラメーター	<vlan_name 32> - ポートを追加する VLAN 名を入力します。 add - 「add」パラメーターを入力すると、VLAN にポートを追加します。 追加するポートには 3 つのタイプがあります。 tagged - 追加ポートをタグ付きとして指定します。 untagged - 追加ポートをタグなしとして指定します。 forbidden - 追加ポートを禁止ポートとして指定します。 delete - 指定した VLAN からポートを削除します。 <portlist> - 指定した VLAN に追加する、または削除するポートまたはポート範囲を指定します。 advertisement <enable | disable> - 指定した VLAN 上の GVRP を「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:4～8 のポートをタグ付きポートとして VLAN「v1」に追加するには

```
#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

#
```

使用例:VLAN からポートを削除するには

```
#config vlan v1 delete 6-8
Command: config vlan v1 delete 6-8

Success.

#
```

注意事項

ポートには複数のタグなし VLAN を割り当てることができます。複数の VLAN がアサインされたポートでは、タグなしフレームを受信した場合にポート VLAN ID(PVID)により送信する VLAN を決めます。

3.28.4 create vlan vlanid

目的	スイッチに複数の VLAN ID を作成して VLAN を作成します。
構文	create vlan vlanid <vidlist> [advertisement]
説明	本コマンドは、スイッチに複数の VLAN を作成します。
パラメーター	<vidlist> - 作成する複数の VLAN ID 範囲を指定します。 advertisement - GVRP に連携するかしないか指定します。連携しない場合、VLAN は動的に連携できません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチに VLAN ID を作成するには

```
#create vlan vlanid 5-6 advertisement
Command: create vlan vlanid 5-6 advertisement

Success

#
```

3.28.5 delete vlan vlanid

目的	スイッチに設定された複数の VLAN を VLAN ID によって削除します。
構文	delete vlan vlanid <vidlist>
説明	本コマンドは、スイッチに設定済みの複数の VLAN を削除します。
パラメーター	<vidlist> - 削除する複数の VLAN ID 範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの VLAN ID を削除するには

```
#delete vlan vlanid 5-6
Command: delete vlan vlanid 5-6

Success

#
```

3.28.6 config vlan vlanid

目的	設定済みの VLAN にポートを追加します。
構文	config vlan vlanid <vidlist> < <add < tagged | untagged | forbidden > | delete > <portlist> | advertisement < enable | disable > | name <vlan_name 32> >
説明	本コマンドは、設定済み VLAN のポートリストにポートを追加または削除します。追加ポートに「tagged」（タグ付き）、「untagged」（タグなし)、「forbidden」(禁止)の指定をします。 同一ポートを「untagged」（タグなし）として複数の VLAN のメンバポートにすることもできます。 advertisement パラメーターを使用してポートが GVRP に連携するかどうかも指定できます。「name」パラメーターで変更の必要のある VLAN の名前を設定します。
パラメーター	<vidlist> - 設定する複数 VLAN ID の範囲を設定します。 tagged - 追加ポートをタグ付きとして指定します。 untagged - 追加ポートをタグなしとして指定します。 forbidden - 追加ポートを禁止ポートとして指定します。 <portlist> - VLAN に追加するポート範囲を指定します。 advertisement - ポートを GVRP に連携させる場合、「advertisement」パラメーターを入力します。次の 2 つのパラメーターがあります： enable - ポートを GVRP に連携させます。 disable - ポートを GVRP に連携させません。 name - 「name」のパラメーターを入力し、変更する VLAN の名前を設定します。 <vlan_name 32> - VLAN の名前を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチに設定済みの VLAN にポートを追加するには

```
#config vlan vlanid 5 add tagged 7 advertisement enable name APS
Command: config vlan vlanid 5 add tagged 7 advertisement enable name APS

Success.

#
```

注意事項

同一ポートにアサインするタグなし VLAN が 1 つだけの場合、PVID を意識する必要はありません。明示的に 1 つのアサインをお勧めします。非対称 VLAN やプロトコル VLAN などの機能においては、複数のタグなし VLAN をアサインするため、PVID を意識する必要があります。

3.28.7 enable pvid auto_assign

目的	PVID の自動割り当てを有効にします。
構文	enable pvid auto_assign
説明	本コマンドは、PVID の自動割り当てを有効にします。
パラメーター	なし。 デフォルト値は、「enable」(有効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:PVID の自動割り当てを有効にするには

```
#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

#
```

3.28.8 disable pvid auto_assign

目的	PVID の自動割り当てを無効にします。
構文	disable pvid auto_assign
説明	本コマンドは、PVID の自動割り当てを無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:PVID の自動割り当てを無効にするには

```
#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

#
```

3.28.9 show pvid auto_assign

目的	PVID の自動割り当てステータスを表示します。
構文	show pvid auto_assign
説明	本コマンドは、PVID の自動割り当てステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:PVID の自動割り当てステータスを表示するには

```
#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

#
```

3.28.10 config gvrp

目的	スイッチに GVRP を設定します。
構文	config gvrp < <portlist> | all > < state < enable | disable > | ingress_checking < enable | disable > | acceptable_frame < tagged_only | admit_all > | pvid <vlanid 1-4094> >
説明	本コマンドは、スイッチに Group VLAN Registration Protocol を設定します。 イングレスチェック、GVRP 情報の送受信、およびポート VLAN ID (PVID) を設定できます。
パラメーター	<portlist> - GVRP を有効にするポートまたはポート範囲を指定します。 all - スイッチのすべてのポートを設定します。 state <enable | disable> - ポートリストで指定したポートに GVRP 機能を「enable」有効または「disable」無効にします。 ingress_checking <enable | disable> - Ingress チェックを有効にすると本装置の全ポートにおいて、受信パケットのVLAN IDと受信ポートのVLAN IDが異なる場合に、パケットが破棄されます。デフォルト設定は「enable」有効です。 acceptable_frame <tagged_only | admit_all> - 本機能のためにスイッチが受け入れるフレームタイプを示します。tagged_only は、タグ付きの VLAN フレームだけを受け入れることを示します。一方、admit_all は、タグ付きおよびタグなしフレームを受け入れることを示します。 pvid <vlanid 1-4094> - ポートに関連するデフォルト VLAN ID を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:イングレスチェック状態および GVRP 情報の送受信を設定するには

```
#config gvrp 1-4 state enable ingress_checking enable acceptable_frame tagged_only pvid 2
Command: config gvrp 1-4 state enable ingress_checking enable acceptable_frame tagged_only
pvid 2

Success.

#
```

3.28.11 enable gvrp

目的	スイッチの GVRP を有効にします。
構文	enable gvrp
説明	disable gvrp を併せた本コマンドは、スイッチの GVRP コンフィグレーションを変更せずに、スイッチの GVRP を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:一般的な VLAN Registration Protocol (GVRP) を有効にするには

```
#enable gvrp
Command: enable gvrp

Success.

#
```

3.28.12 disable gvrp

目的	スイッチの GVRP を無効にします。
構文	disable gvrp
説明	enable gvrp を併せた本コマンドは、スイッチの GVRP コンフィグレーションを変更せずに、スイッチの GVRP を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:一般的な VLAN Registration Protocol (GVRP) を無効にするには

```
#disable gvrp
Command: disable gvrp

Success.

#
```

3.28.13 show vlan

目的	スイッチに設定された VLAN 設定を表示します。
構文	show vlan < <vlan_name 32> | vlanid <vidlist> | ports <portlist> >
説明	本コマンドは、VLAN ID/VLAN 名/VLAN タイプ、タグ付き/タグなしステータス、および VLAN のメンバである各ポートの Member/Non-member/Forbidden ステータスを含む各 VLAN に関するサマリー情報を表示します。
パラメーター	<vlan_name 32> - サマリ設定を表示する VLAN 名を入力します。 vlanid <vidlist> - 表示する複数の VLAN ID 範囲を指定します。 ports <portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチの VLAN 設定を表示するには

```
#show vlan
Command: show vlan
VID             : 1           VLAN Name       : default
VLAN Type       : Static      Advertisement   : Enabled
Member Ports    : 1-52
Static Ports    : 1-52
Current Tagged Ports   :
Current Untagged Ports : 1-52
Static Tagged Ports    :
Static Untagged Ports  : 1-52
Forbidden Ports        :


Total Entries  : 1

#
```

使用例:スイッチの VLAN 設定を表示するには

```
#show vlan ports 6
Command: show vlan ports 6

 Port   VID   Untagged  Tagged  Dynamic  Forbidden
-----   ----  --------  ------  -------  ---------
 6      1       X         -       -        -

#
```

3.28.14 show gvrp

目的	スイッチのポートリストの GVRP ステータスを表示します。
構文	show gvrp [<portlist>]
説明	本コマンドは、スイッチのポートリストの GVRP ステータスを表示します。
パラメーター	<portlist> - GVRP ステータスを表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:GVRP ポートステータスを表示するには

```
#show gvrp 1-10
Command: show gvrp 1-10

Global GVRP  : Disabled

Port  PVID  Reassigned   GVRP      Ingress   Acceptable Frame Type
            PVID         State     Checking
----  ----  ----------   --------  --------  ----------------------
1     1     -            Disabled    Enabled     All Frames
2     1     -            Disabled    Enabled     All Frames
3     1     -            Disabled    Enabled     All Frames
4     1     -            Disabled    Enabled     All Frames
5     1     -            Disabled    Enabled     All Frames
6     1     -            Disabled    Enabled     All Frames
7     1     -            Disabled    Enabled     All Frames
8     1     -            Disabled    Enabled     All Frames
9     1     -            Disabled    Enabled     All Frames
10    1     -            Disabled    Enabled     All Frames

Total Entries  : 10
```

3.29 ARP コマンド

3.29.1 create arpentry

目的	ARP テーブルにスタティックエントリーを作成します。
構文	create arpentry <ipaddr> <macaddr>
説明	本コマンドは、スイッチの ARP テーブルに IP アドレスと対応する MAC アドレスを入力します。
パラメーター	<ipaddr> - ARP テーブルに登録する IP アドレスを入力します。 <macaddr> - 上記 IP アドレスに対応する MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。 スイッチは、255 までのスタティック ARP エントリーをサポートします。
対応バージョン	1.00.00 以降

使用例:IP アドレス「10.48.74.12」と MAC アドレス「00-40-66-00-07-36」 のスタティック ARP エントリーを作成するには

```
#create arpentry 10.48.74.12 00-40-66-00-07-36
Command: create arpentry 10.48.74.12 00-40-66-00-07-36

Success.

#
```

3.29.2 config arpentry

目的	ARP テーブルにスタティックエントリーを設定します。
構文	config arpentry <ipaddr> <macaddr>
説明	本コマンドは、ARP テーブルにスタティックエントリーを設定します。 スイッチの ARP テーブルのエントリーに IP アドレスと対応する MAC アドレスを指定できます。
パラメーター	<ipaddr> - ARP テーブルに登録する IP アドレスを入力します。 <macaddr> - 上記 IP アドレスに対応する MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:IP アドレス「10.48.74.12」と MAC アドレス「00-40-66-00-07-36」 のスタティック ARP エントリーを設定するには

```
#config arpentry 10.48.74.12 00-40-66-00-07-36
Command: config arpentry 10.48.74.12 00-40-66-00-07-36

Success.

#
```

3.29.3 delete arpentry

目的	ARP テーブルからスタティックエントリーを削除します。
構文	delete arpentry < <ipaddr> | all >
説明	上記「create arpentry」コマンドで作成したスタティック ARP エントリーを、エントリーの IP アドレスまたは「all」を指定することにより削除します。 「all」を指定すると、スイッチの ARP テーブルはすべてクリアされます。
パラメーター	<ipaddr> - ARP テーブルから削除する IP アドレスを入力します。 all - ARP エントリーをすべて削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：IP アドレス「10.48.74.12」を ARP テーブルから削除するには

```
#delete arpentry 10.48.74.12
Command: delete arpentry 10.48.74.12

Success.

#
```

3.29.4 config arp_aging time

目的	スイッチの ARP テーブルエントリーにエージアウトタイマーを設定します。
構文	config arp_aging time <value 0-65535>
説明	本コマンドは、ARP エントリーがアクセスされない状態で、スイッチの ARP テーブルに保存される最大時間(分)を設定します。
パラメーター	time <value 0-65535> - ARP エージングタイム(分)を入力します。値は 0～65535 の範囲から指定できます。デフォルト値は、20 分です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：ARP エージングアウトタイマーを設定するには

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

Success.

#
```

3.29.5 show arpentry

目的	ARP テーブルを表示します。
構文	show arpentry ipif System [ipaddress <ipaddr> | static]
説明	本コマンドは、スイッチの ARP テーブルの内容を表示します。
パラメーター	ipaddress <ipaddr> - 上記 IP インターフェースに対応するネットワークアドレスを入力します。 static - ARP テーブルのスタティックエントリーを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例：ARP テーブルを表示するには

```
#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          10.6.51.15        00-40-66-E7-B5-CD   Dynamic
System          10.73.21.11       00-40-66-EF-78-B5   Local
System          10.255.255.255    FF-FF-FF-FF-FF-FF   Local/Broadcast

Total Entries  : 4

#
```

3.29.6 clear arptable

目的	ダイナミック ARP テーブルエントリーをすべて削除します。
構文	clear arptable
説明	本コマンドは、スイッチの ARP テーブルからダイナミックエントリーを削除します。スタティック ARP テーブルエントリーは影響を受けません。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：ARP テーブルからダイナミックエントリーを削除するには

```
#clear arptable
Command: clear arptable

Success.

#
```

3.30 ルーティングテーブルコマンド

3.30.1 create iproute

目的	スイッチの IP ルートエントリーを作成します。
構文	create iproute < default | <network_address> > <ipaddr> [<metric 1-65535>] [<primary | backup>]
説明	本コマンドは、IP ルートエントリーを作成します。
パラメーター	default - デフォルトの IP ルートを作成します。 <network_address> - 指定した宛先ネットワークの IP ルートを作成します。 例：10.0.0.0/255.0.0.0 または 10.0.0.0/8 の CIDR 形式 <ipaddr> - ネクストホップルーターの IP アドレスを指定します。 <metric 1-65535> - ネクストホップルーターまでのルーター数を指定します。デフォルト値は 1 です。 <primary> - 宛先までのルートとしてプライマリルートを指定します。 <backup> - 宛先までのルートとしてバックアップルートを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:デフォルトルート、ゲートウェイ「10.0.0.254」の IP ルートを作成するには

```
#create iproute default 10.0.0.254
Command: create iproute default 10.0.0.254

Success.

#
```

3.30.2 delete iproute

目的	スイッチの IP ルートエントリーを削除します。
構文	delete iproute < default | <network_address> > <ipaddr>
説明	本コマンドは、指定した IP ルートエントリーを削除します。
パラメーター	default - デフォルトの IP ルートを削除します。 <network_address> - 指定した宛先ネットワークの IP ルートを削除します。 例：10.0.0.0/255.0.0.0 または 10.0.0.0/8 の CIDR 形式 <ipaddr> - 削除するゲートウェイ IP アドレスを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:デフォルトルート、ゲートウェイ「10.0.0.254」の IP ルートを削除するには

```
#delete iproute default 10.0.0.254
Command: delete iproute default 10.0.0.254

Success.

#
```

3.30.3 show iproute

目的	スイッチの IP ルートエントリーを表示します。
構文	show iproute [<network_address> | <ipaddr>] [static]
説明	本コマンドは、スイッチの IP ルートエントリーを表示します。
パラメーター	<network_address> - 宛先ネットワークアドレスを指定します。 <ipaddr> - 宛先 IP アドレスを指定します。 static - 作成した全ての IP ルートを表示します。指定しない場合、ネクストホップルーターが動作状態にある IP ルートのみ表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:IP ルートテーブルの内容を表示するには

```
#show iproute
Command: show iproute

Routing Table

IP Address/Netmask     Gateway      Interface    Cost    Protocol
---------------        ---------    ----------   ----    ----------
0.0.0.0/0              10.0.0.254    System       1       Default
10.0.0.0/8             0.0.0.0       System       1       Local

Total Entries: 2

#
```

3.30.4 create ipv6 neighbor_cache ipif

目的	IPv6 インターフェースにスタティックネイバーを追加します。
構文	create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
説明	本コマンドは、IPv6 インターフェースにスタティックネイバーを追加します。
パラメーター	<ipif_name> - インターフェース名を入力します。 <ipv6addr> - ネイバーのアドレスを入力します。 <macaddr> - ネイバーの MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:IPv6 インターフェースにスタティックネイバーを追加するには

```
#create ipv6 neighbor_cache ipif System fe80::fecf:7ec6 00-40-66-03-04-05
Command: create ipv6 neighbor_cache ipif System FE80::FECF:7EC6 00-40-66-03-04-05
Success.

#
```

3.30.5 delete ipv6 neighbor_cache ipif

目的	インターフェースネイバーアドレスキャッシュから IPv6 ネイバーを削除します。
構文	delete ipv6 neighbor_cache ipif < <ipif_name 12> | all > < <ipv6addr> | static | dynamic | all >
説明	本コマンドは、IPv6 インターフェースのネイバーキャッシュエントリー、もしくはスタティックネイバーキャッシュエントリーを削除します。スタティックもダイナミックも削除することができます。
パラメーター	<ipif_name> - IPv6 インターフェース名を入力します。 <ipv6addr> - ネイバーのアドレスを入力します。 all - スタティックおよびダイナミックエントリーを含むすべてのエントリーが削除されます。 static - スタティックエントリーを削除します。 dynamic - ダイナミックエントリーを削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ネイバーキャッシュを削除するには

```
#delete ipv6 neighbor_cache ipif System fe80::20b:6aff:fecf:7ec6
Command: delete ipv6 neighbor_cache ipif System fe80::20b:6aff:fecf:7ec6

Success.

#
```

3.30.6 show ipv6 neighbor_cache ipif

目的	IPv6 ネイバーキャッシュを表示します。
構文	show ipv6 neighbor_cache ipif < <ipif_name 12> | all > <ipv6address <ipv6addr> | static | dynamic | all >
説明	本コマンドは、指定したインターフェースのネイバーキャッシュエントリーを表示します。指定したエントリー、すべてのエントリー、およびすべてのスタティックエントリーを表示します。
パラメーター	<ipif_name 12> - インターフェース名を入力します。 <ipv6addr> - アドレスを入力します。 static -スタティックエントリーを表示します。 dynamic - ダイナミックエントリーを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:インターフェースシステムのネイバーを表示するには

```
#show ipv6 neighbor_cache ipif all all
Command: show ipv6 neighbor_cache ipif all all

3FFC::1                                 State: Static
MAC Address : 00-40-66-00-00-01         Port : NA
Interface   : System                   VID  : 2

FE80::F092:7EBC:D6A:B43A                State: Stale
MAC Address : 00-40-66-E0-09-35         Port : 44
Interface   : System                   VID  : 2

Total Entries: 2

#
```

3.30.7 create ipv6route

目的	IPv6 スタティックルートを作成します。
構文	create ipv6route <default> < <ipif_name 12> <ipv6addr> > [<metric 1-65535>]
説明	本コマンドは、IPv6 スタティックルートに使用します。ネクストホップがグローバルアドレスの場合、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、インターフェース名を指定する必要があります。
パラメーター	default - デフォルトルートを指定します。 <ipif_name 12> - ルートのインターフェースを指定します。 <ipv6addr> - 本ルートのネクストホップアドレスを指定します。 <metric 1-65535> - スイッチと上記 IP アドレス間のルーターの数を表すルーティングプロトコルのメトリックエントリーを入力します。 デフォルト値は、1 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スタティックルート「fe80::20b:6aff:fecf:7ec6」を作成するには

```
#create ipv6route default System fe80::20b:6aff:fecf:7ec6
Command: create ipv6route default System fe80::20b:6aff:fecf:7ec6

Success.

#
```

3.30.8 delete ipv6route

目的	IPv6 ルートを削除します。
構文	delete ipv6route < <default> < <ipif_name 12> <ipv6addr>| all >
説明	本コマンドは、IPv6 スタティックルートに使用します。ネクストホップがグローバルアドレスの場合、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、インターフェース名を指定する必要があります。
パラメーター	default - デフォルトルートを指定します。 <ipv6addr> - デフォルトルートのネクストホップアドレスを指定します。 all - 作成されたスタティックルートをすべて削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:IPv6 スタティックルートを削除するには

```
#delete ipv6route default fe80::20b:6aff:fecf:7ec6
Command: delete ipv6route default fe80::20b:6aff:fecf:7ec6

Success.

#
```

3.30.9 show ipv6 nd

目的	インターフェースの情報を表示します。
構文	show ipv6 nd [ipif <ipif_name 12>]
説明	本コマンドは、IPv6 ND に関連した情報を表示します。
パラメーター	<ipif_name> - インターフェースの名前を入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:インターフェースの情報を表示するには

```
#show ipv6 nd ipif System
Command: show ipv6 nd ipif System

Interface Name        : System
NS Retransmit Time    : 0(ms)

#
```

3.30.10 show ipv6route

目的	IPv6 ルートを表示します。
構文	show ipv6route
説明	本コマンドは、IPv6 ルートを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:すべての IPv6 ルートを表示するには

```
#show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                          Protocol: Static  Metric: 10
Next Hop   : 2014::1                       IPIF    : System
Status  : Inactive

Total Entries: 1

#
```

3.30.11 config ipv6 nd ns ipif

目的	ネイバーのソリシエーションに関連した引数を設定します。
構文	config ipv6 nd ns ipif <ipif name 12> retrans_time <uint 0-4294967295>
説明	本コマンドは、ネイバーのソリシエーションに関連した引数を設定します。
パラメーター	<ipif_name> - インターフェースの名前を入力します。 retrans_timer - ネイバーのソリシテーションを再送するまでの遅延時間(ミリ秒)を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: IPv6 nd ns インターフェースを設定するには

```
#config ipv6 nd ns ipif System retrans_time 10000
Command: config ipv6 nd ns ipif System retrans_time 100000

Success.

#
```

3.31 QoS コマンド

スイッチは、802.1p 優先キューをサポートします。 スイッチには 8 つの優先キューがあります。これらの優先キューには、最高レベルの 7 番キュー（クラス 7）から最低レベルの 0 番キュー（クラス 0）までがあります。IEEE 802.1p（p0 から p7）に規定される 8 つの優先度タグはスイッチの優先度タグと以下のように関連付けされます。
優先度 0 は、スイッチの Q2 キューに割り当てられます。
優先度 1 は、スイッチの Q0 キューに割り当てられます。
優先度 2 は、スイッチの Q1 キューに割り当てられます。
優先度 3 は、スイッチの Q3 キューに割り当てられます。
優先度 4 は、スイッチの Q4 キューに割り当てられます。
優先度 5 は、スイッチの Q5 キューに割り当てられます。
優先度 6 は、スイッチの Q6 キューに割り当てられます。
優先度 7 は、スイッチの Q7 キューに割り当てられます。

優先度スケジューリングは上記の優先キューによって実装されます。 スイッチは 8 個の優先キューを空にします。その順番は、最も高い優先キューの 7 から最も低い優先キューの 0 となります。各ハードウェアキューは次に低い優先度にパケットを送信する前にバッファのすべてのパケットを送信します。 最も低いハードウェア優先キューがすべてのパケットの送信を完了すると、最も高いハードウェア優先キューは、受信しているすべてのパケットを再送信できるようになります。

3.31.1 config bandwidth_control

目的	ポートベースで帯域幅制御を設定します。
構文	config bandwidth_control < <portlist> | all > [rx_rate < no_limit | <value 64-1024000> > | tx_rate < no_limit <value 64-1024000> >]
説明	本 コマンドは、ポートベースで帯域幅制御を設定します。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - 全てのポートに設定する場合に選択します。 rx_rate - 下のパラーメーター(no_limit または<value 64-1024000>)を指定し、上で指定したポートがパケットを受信できる速度に適用させます。 no_limit - 指定ポートが受信するパケットの速度を制限しません。 <value 64-1024000> - 上記ポートで受信するトラフィック制限(Kbps)を指定します。 tx_rate - 下のパラーメーター(no_limit または<value 64-1024000>)を指定し、上で指定したポートがパケットを送信できる速度に適用させます。 no_limit - 指定ポートが受信するパケットの速度を制限しません。 <value 64-1024000> - 上記ポートで受信するトラフィック制限(Kbps)を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:帯域幅制御を設定するには

```
#config bandwidth_control 1 rx_rate 66
Command: config bandwidth_control 1 rx_rate 66

 Granularity: RX: 64, TX: 64. Actual Rate: RX: 64.

Success.

#
```

注意事項

設定範囲は 64-1024000Kbps となりますが、実際に設定される値は 64Kbps の倍数となるように自動的に調整されます。
rx_rate パラメーターの forwarding rate が一定にならないときがあります。

3.31.2 show bandwidth_control

目的	帯域幅制御テーブルを表示します。
構文	show bandwidth_control [<portlist>]
説明	本コマンドは、スイッチの帯域幅制御の設定をポート別に表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:帯域幅制御設定を表示するには

```
#show bandwidth_control 1-3
Command: show bandwidth_control 1-3

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
3     no_limit      no_limit      no_limit            no_limit

#
```

3.31.3 config scheduling

目的	各 COS キューにトラフィックスケジューリングメカニズムを設定します。
構文	config scheduling <class_id 0-7> weight <value 1-127>
説明	スイッチには 8 つのハードウェア優先キューがあります。これら 8 つのキューのうち 1 つに入力パケットをマッピングする必要があります。本コマンドは、これらの 8 つのハードウェア優先キューが空にされている順番を指定します。 スイッチのデフォルト値（「config scheduling」コマンドが使用されない場合）では、最も高い優先キュー(ハードウェアキュー8) から最も低い優先キュー(ハードウェアキュー0)まで順番にハードウェア優先キューを空にしていきます。各ハードウェアキューは、次に低い優先キューがパケット送信を許可するまで、バッファにすべてのパケットを送信します。最も低いハードウェア優先キューがすべてのパケットの転送を完了すると、最も高いハードウェア優先キューは、受信しているすべてのパケットの送信を開始します。
パラメーター	<class_id 0-7> - 8 つのハードウェア優先キューのどれに適用されるかを指定します。 8 つのハードウェア優先キューは、最も低い優先度である 0 キューを持つ 0 から 7 の番号によって識別されます。 weight <value 1-127> - 重み付けされた COS キューのウェイトを指定します。 1 ～127 の範囲で設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:各キューにトラフィックスケジューリングメカニズムを設定するには

```
#config scheduling 0 weight 55
Command: config scheduling 0 weight 55

Success.

#
```

3.31.4 show scheduling

目的	スイッチに現在設定されているトラフィックスケジューリングを表示します。
構文	show scheduling
説明	本コマンドは、スイッチのトラフィックスケジューリングメカニズムを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スケジューリング設定を表示するには

```
#show scheduling
Command: show scheduling

QOS Output Scheduling

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

#
```

3.31.5 config scheduling_mechanism

目的	QoS 機能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 < strict | weight_fair >
説明	本コマンドは、QoS 機能サービスの優先度クラスを空にするために weight fair と strict メカニズムから選択します。 スイッチには 8 つのハードウェア優先度 CoS を含みます。これら 8 つのハードウェア優先度 CoS の 1 つに入力パケットをマップする必要があります。このコマンドは、これらの 8 つのハードウェア優先度 CoS が送信されるという循環を指定します。 スイッチのデフォルト値は、最も高い優先キュー（キュー7）から-最も低い優先キュー（キュー0)まで順番にハードウェア優先度 CoS を送信していきます。各キューは、次に低い優先度 CoS がパケット送信を許可するまで、バッファにすべてのパケットを送信します。
パラメーター	strict - strict パラメーターを指定すると、上位の CoS キューからトラフィックを処理します。上位キューの送信が完了するまで下位キューからはパケットは送信されません。 weight_fair - 「Weight fair」パラメーターを入力すると、優先度 CoS が重み付けされた順でパケットを処理します。パケットは均一に処理されることになります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:各 QoS キューにトラフィックスケジューリングメカニズムを設定するには

```
#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

#
```

3.31.6 show scheduling_mechanism

目的	スイッチのトラフィックスケジューリングメカニズムを表示します。
構文	show scheduling_mechanism
説明	本コマンドは、スイッチのトラフィックスケジューリングメカニズムを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スケジューリングメカニズムを表示するには

```
#show scheduling_mechanism
Command: show scheduling_mechanism

QOS Scheduling mechanism
CLASS ID  Mechanism
--------  -----------
Class-0   strict
Class-1   strict
Class-2   strict
Class-3   strict
Class-4   strict
Class-5   strict
Class-6   strict
Class-7   strict

#
```

3.31.7 config 802.1p user_priority

目的	スイッチで利用可能な 8 個のハードウェアキューの 1 つに入力パケットの 802.1p ユーザー優先度をマップします。
構文	config 802.1p user_priority <priority 0-7> <class_id 0-7>
説明	本コマンドは、802.1p ユーザー優先度に基づいて、入力パケットを 8 つの有効なハードウェア優先キューの 1 つにマップする方法を設定します。 スイッチの初期状態では、以下の通り入力する 802.1p ユーザー優先度の値を 8 つのハードウェア優先キューにマップします。 802.1p　ハードウェアキュー　備考 0　2 1　0　最低 2　1 3　3 4　4 5　5 6　6 7　7　最高 このマッピングスキーマは、IEEE 802.1D に含まれる勧告に基づいています。 このマッピングは、<class_id 0-7>（ハードウェアキューの番号）に対して 802.1p ユーザー優先度を指定することで変更できます。
パラメーター	<priority 0-7> - class_id（ハードウェアキューの番号)に連携させる 802.1p ユーザー優先度を指定します。 <class_id 0-7> - スイッチのハードウェア優先キューの番号を指定します。 本スイッチには、8 個のハードウェア優先キューがあります。 これらのキューは 0（最も低い優先度）と 7(最も高い優先度)の間で番号を付与されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチに 802.1p ユーザー優先度を設定するには

```
#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

#
```

3.31.8 show 802.1p user_priority

目的	入力パケットの 802.1p ユーザー優先値とスイッチの 8 個のハードウェア優先キューとのマッピングを表示します。
構文	show 802.1p user_priority
説明	本コマンドは、入力パケットの 802.1p 優先値とスイッチの 8 個のハードウェア優先キューの 1 つとのマッピングを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:802.1p ユーザー優先度を表示するには

```
#show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

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>

#
```

3.31.9 config 802.1p default_priority

目的	スイッチに 802.1p デフォルトの優先度を設定します。 タグなしパケットをスイッチが受信すると、本コマンドで設定した優先度は、パケットの優先度フィールドに記載されます。
構文	config 802.1p default_priority <<portlist> | all> <priority 0-7>
説明	本コマンドは、スイッチが受信したタグなしパケットのデフォルトの優先度処理に関する指定をします。本コマンドで入力された優先値は、パケットが 8 個のハードウェア優先キューのうちのどれに転送されるかを決定するために使用されます。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - スイッチのすべてのポートに適用します。 <priority 0-7> - スイッチまたはスイッチのポート範囲が受信したタグなしパケットに割り当てる優先値を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチに 802.1p デフォルトの優先度を設定するには

```
#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

#
```

3.31.10 show 802.1p default_priority

目的	送信先に転送される前に入力するタグなしパケットに割り当てられている 802.1p 優先値を表示します。
構文	show 802.1p default_priority [<portlist>]
説明	本コマンドは、送信先に転送される前に入力するタグなしパケットに割り当てられている 802.1p 優先値を表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 1-16 の 802.1p デフォルトの優先度コンフィグレーションを表示するには

```
#show 802.1p default_priority 1-16
Command: show 802.1p default_priority 1-16

 Port   Priority
 -----  --------
 1      0
 2      0
 3      0
 4      0
 5      0
 6      0
 7      0
 8      0
 9      0
 10     0
 11     0
 12     0
 13     0
 14     0
 15     0
 16     0

#
```

3.31.11 config cos mapping

目的	スイッチに適用する CoS ポートマッピング方法を設定します。
構文	config cos mapping ports < <portlist> | all > < none | < ethernet <802.1p> | ip < tos | dscp > > >
説明	本コマンドは、スイッチの Cos とポートのマッピング機能に対し、入力パケットが識別される方法を設定します。識別されたパケットは、適切な CoS キューに転送されます。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - すべてのポートを設定する場合に指定します。 none - 優先度ベースの CoS 機能をすべて無効にします。 ethernet - イーサネットフレームベースの優先度を有効にします。 802.1p - 「802.1p CoS」を有効にします。 ip - イーサネットフレームベースの優先度を有効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1 を CoS イネーブルとして設定するには

```
#config cos mapping ports 1 ethernet 802.1p
Command: config cos mapping ports 1 ethernet 802.1p

Success.

#
```

3.31.12 show cos mapping

目的	CoS マッピングを表示します。
構文	show cos mapping [ports < <portlist> | all >]
説明	本コマンドは、CoS マッピングの有効ポートと方法について表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。 パラメーターを省略した場合、すべてのポートの優先度設定を表示します。 all - すべてのポートを表示する場合に指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:CoS マッピング情報を表示するには

```
#show cos mapping
Command: show cos mapping

Port  Ethernet_priority  IP_priority
----  ----------------  -----------
1     802.1p            off
2     802.1p            off
3     802.1p            off
4     802.1p            off
5     802.1p            off
6     802.1p            off
7     802.1p            off
8     802.1p            off
9     802.1p            off
10    802.1p            off
11    802.1p            off
12    802.1p            off
13    802.1p            off
14    802.1p            off
15    802.1p            off
16    802.1p            off
17    802.1p            off
18    802.1p            off
19    802.1p            off
20    802.1p            off
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.31.13 config cos tos value

目的	スイッチで利用可能な 8 つのハードウェアキューの 1 つに入力パケットの IP ヘッダの ToS 値をマップします。
構文	config cos tos value <value 0-7> <class <class_id 0-7>>
説明	本コマンドは、ToS をトラフィッククラスマッピングに設定します。
パラメーター	<value 0-7> - トラフィッククラスに関連付けする入力パケットの ToS 値を指定します。 <class_id 0-7> - スイッチのハードウェア優先キューの番号を指定します。 本スイッチには、8 個のハードウェア優先キューがあります。これらのキューは 0（最も低い優先度）と 7(最も高い優先度)の間で番号を付与されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:TOS 5 をトラフィッククラス 1 マッピングに設定するには

```
#config cos tos value 5 class 1
Command: config cos tos value 5 class 1

Success.

#
```

注意事項

本コマンドには「cos」の記載がありますが、「cos」に関する設定は出来ません。

3.31.14 show cos tos

目的	トラフィッククラスマッピングをする TOS の値を表示します。
構文	show cos tos [value <value 0-7>]
説明	本コマンドは、ToS とトラフィッククラス マッピングの情報を表示します。
パラメーター	<value 0-7> - 入力パケットの TOS 値を指定します。パラメーターの指定が無い場合、すべてのトライフィッククラスマッピングが表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:TOS 5 の TOS トラフィッククラスマッピングを表示するには

```
#show cos tos value 5
Command: show cos tos value 5

TOS value             Class
-----------------------------------------
5                           2

#
```

3.31.15 config dscp_mapping

目的	スイッチで利用可能な 8 個のハードウェアキューの 1 つに入力パケットの IP ヘッダの DSCP 値をマップします。
構文	config dscp_mapping dscp_value <value 0-63> < class <class_id 0-7> >
説明	本コマンドは、DSCP マッピングをトラフィッククラスに設定します。
パラメーター	<value 0-63> - クラス ID と関連付けする DSCP 値を指定します。 <class_id 0-7> - スイッチのハードウェア優先キューの番号を指定します。本スイッチには 8 個のハードウェア優先キューがあります。これらのキューは 0(最も低い優先度)と 7(最も高い優先度)間で番号を付与されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:DSCP のトラフィッククラスマッピングを設定するには

```
#config dscp_mapping dscp_value 8 class 1
Command: config dscp_mapping dscp_value 8 class 1

Success.

#
```

3.31.16 show dscp_mapping

目的	トラフィッククラスマッピングをする DSCP の値を表示します。
構文	show dscp_mapping [dscp_value <value 0-63>]
説明	本コマンドは、DSCP トラフィッククラスマッピングの設定を表示します。
パラメーター	<value 0-63> - 入力パケットの DSCP 値を指定します。パラメーターの設定がされていない場合、トラフィッククラスへに全ての DSCP マッピングが表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:DSCP のトラフィッククラスマッピングを表示するには

```
#show dscp_mapping
Command: show dscp_mapping

DSCP    Class
--------------------
0          0
1          0
2          0
3          0
4          0
5          0
6          0
7          0
8          0
9          0
10         0
11         0
12         0
13         0
14         0
15         0
16         0
17         0
18         0
19         0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.32 アクセス制御リスト (ACL)コマンド

スイッチはアクセス制御リストを使用して、IPアドレスおよびMACアドレスに基づき特定のデバイスやデバイスグループへのネットワークアクセスを拒否できるようにします。

アクセスプロファイルを作成すると、各パケットヘッダの中の情報に従い、スイッチがパケット転送を決定するための基準を設定できるようになります。

アクセスプロファイルの作成は基本的に2 つの部分に分かれます。最初に「create access_profile」コマンドを使用してアクセスプロファイルを作成します。例えば、サブネット10.42.73.0 ～ 10.42.73.255 に対して全トラフィックを制限したい場合、はじめにスイッチに対して各フレームの関連フィールドすべてを調査するアクセスプロファイルを作成します。

最初に調査の基準としてIPアドレスを使用するアクセスプロファイルを作成します。

```
create access_profile ip source_ip_mask 255.255.255.0 profile_id 1
```

上記の例では、スイッチが受信した各フレームのIP フィールドを調査するアクセスプロファイルを作成しました。スイッチが検出した各送信元IP アドレスを論理積により source_ip_mask と照合します。profile_idパラメーターを使用してアクセスプロファイルに識別番号を設定します。ここでは1を設定します。これは競合が生じたとき優先度を割り当てるために使用します。profile_idは、プロファイルリスト内で優先度を設定します。数字の小さいaccess_id ほど高い優先度が付与されます。アクセスプロファイルに登録したルー ル内に競合がある場合、最も高い優先度（最も低いaccess_id)のルールが優先されます。アクセスプロファイルとアクセスルールの制限に関する情報は下記を参照してください。

スイッチ はdenyパラメーターを使用して規準に合うフレームを廃棄します。ここでは、次のステップで指定するIP アドレスとip_source_mask照合のAND オペレーションです。

スイッチのアクセスプロファイルの初期値は、トラフィックフローをpermit(許可)しています。トラフィックを制限するためには、deny（拒否)パラメーターを使用する必要があります。

アクセスプロファイルの作成後、スイッチがある特定フレームの転送またはフィルタリングを決定するために基準を追加する必要があります。config access_profile コマンドを使用して、希望する基準を定義する新しいルールを作成します。さらに新しいルールで各ポートからあるIPアドレスの範囲にアクセスを拒否するように指定する例を見てみましょう。この例では、10.42.73.0～10.42.73.255 のIP送信先アドレスを持つパケットをフィルタリングし、許可しないポートを指定します。

```
config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny
```

アクセスプロファイルを作成したときに指定した「profile_id 1」を使用します。「add」パラメーターはアクセスプロファイル1と関連付けられるルールリストに従う基準をスイッチに追加します。アクセスプロファイルに登録した各ルールに、ルールを識別し、ルールリスト内に優先度を設定するaccess_id を割り当てることができます。access_idはインデックス番号のみを意図し、profile_id内での優先度に影響を与えません。access_idはユーザーがプロファイルから個々のルールを解除する場合に、後で使用できます。

ipパラメーターはこの新しいルールが各フレームヘッダ内のIPアドレスに適用されるようにします。source_ipはこのルールを各フレームヘッダの送信元IPアドレスに適用するようにスイッチに指示します。最後に、IPアドレス10.42.73.1はsource_ip_mask 255.255.255.0に統合し、10.42.73.0と10.42.73.255の間の送信元IPアドレスにIPアドレス10.42.73.0を与えます。最後に制限付きポート（ポート番号7)が指定されます。

3.32.1 create access_profile

目的	スイッチにアクセスプロファイルを作成し、入力するフレームの各ヘッダのどの部分をスイッチが調査するか定義します。スイッチが特定のフレームヘッダフィールドで見つける値と組み合わせてマスクを入力することができます。ルールに対する具体的な値は、下記の「config access_profile」コマンドを入力して指定します。
構文	create access_profile < *ethernet* | *ip* | *ipv6* | *packet_content_mask* > profile_id <value 1-4> *ethernet* =ethernet < vlan [<hex 0x0-0x0fff>] | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type > *ip* =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 <0x0-0xff> > > [user_define_mask <hex 0x0-0xffffffff>] *ipv6* =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] > *packet_content_mask* = 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>]
説明	本コマンドはスイッチにアクセスプロファイルを作成し、入力するフレームの各ヘッダのどの部分をスイッチが調査するか定義します。スイッチが特定のフレームヘッダフィールドで見つける値と組み合わせてマスクを入力することができます。 ルールに対する具体的な値は、下記の「config access_profile」コマンドを入力して指定します。

パラメーター	ethernet - スイッチが各パケットヘッダのレイヤ 2 の部分を調査する場合に指定します。 vlan - VLAN マスクを調査指定します。マスクの最後の 12 ビットのみが対象になります。 source_mac <macmask> - 送信元 MAC アドレスの MAC アドレスマスクを指定します。このマスクは 16 進数形式入力されます。 destination_mac <macmask> - 送信先 MAC アドレスの MAC アドレスマスクを指定します。 802.1p - スイッチがフレームヘッダの 802.1p 優先値を調査する場合に指定します。 ethernet_type - スイッチが各フレームヘッダのイーサネットタイプ値を調査する場合に指定します。 ip - スイッチが各フレームヘッダの IP フィールドを調査する場合に指定します。 vlan - LAN マスクを調査指定します。マスクの最後の 12 ビットのみが対象になります。 source_ip_mask <netmask> - 送信元 IP アドレスの IP アドレスマスクを指定します。 destination_ip_mask <netmask> - 送信先 IP アドレスの IP アドレスマスクを指定します。 dscp - スイッチが各フレームヘッダの DiffServ Code Point (DSCP)フィールドを調査する場合に指定します。 icmp - スイッチが各フレームヘッダの Internet Control Message Protocol(ICMP)フィールドを調査する場合に指定します。 type - スイッチが各フレームの ICMP タイプフィールドを調査する場合に指定します。 code - スイッチが各フレームの ICMP Code フィールドを調査する場合に指定します。 igmp - スイッチが 各フレームの Internet Group Management Protocol (IGMP)フィールドを調査する場合に指定します。 type - スイッチが各フレームの IGMP タイプフィールドを調査する場合に指定します。 tcp - スイッチが各フレームの Transport Control Protocol (TCP)フィールドを調査する場合に指定します。 src_port_mask <hex 0x0-0xffff> - 送信元ポートの TCP ポートマスクを指定します。 dst_port_mask <hex 0x0-0xffff> - 送信先ポートの TCP ポートマスクを指定します。 flag_mask - 適切な flag_mask パラメーターを入力します。すべての入力パケットは転送基準として TCP ポート番号を持っており、これらの番号はパケットをどうするかを決定するパケットの一部分に関連する flag bit を持っています。パケット内の特定の flag bit を調査して、パケットを拒否します。all、urg (urgent)、ack (acknowledgement)、psh (push)、rst (reset)、syn (synchronize)、および fin (finish)から選択できます。

	udp - スイッチが各フレームの Universal Datagram Protocol(UDP)フィールドを調査する場合に指定します。 src_port_mask <hex 0x0-0xffff> - 送信元ポートの UDP ポートマスクを指定します。 dst_port_mask <hex 0x0-0xffff> - 送信先ポートの UDP ポートマスクを指定します。 protocol_id_mask - スイッチが各パケットのプロトコル ID フィールドを調査する場合に指定します。このフィールドにここで入力した値が含まれている場合は、以下のルールを適応します。 user_define_mask - IP ヘッダ内の IP プロトコル ID を指定します。対象となる IP ヘッダ長は 20byte です。 ipv6 - IPv6 フィルタリングマスクを指定します。 class - IPv6 クラスを指定します。 flowlabel - IPv6 フローラベルを指定します。 source_ipv6_mask - IPv6 送信元サブマスクを指定します。 destination_ipv6_mask - IPv6 送信先サブマスクを指定します。 tcp - TCP のポートマスクを指定します。 udp - UDP のポートマスクを指定します。 src_port_mask - IPv6 L4(TCP/UDP)送信元ポートサブマスクを指定します。 dst_port_mask - IPv6 L4(TCP/UDP)送信先ポートサブマスクを指定します。 icmp - ICMP フィルタリングマスクを指定します。 type - ICMP フィルタリングマスクにタイプフィールドが含まれるときに指定します。 code - ICMP フィルタリングマスクにコードフィールドが含まれるときに指定します。 packet_content_mask - デバイスがフィルタリングする対象に UDF フィールドを定義します。 offset_chunk_1～offset_chunk_4 - それぞれの UDF フィールドは 4 バイトのデータであり、オフセットリファレンスからｎバイト（このｎの数値がオフセット値です。）離れています。合計で 4 つの packet content フィールドを一パケットの先頭の 128 バイトから選ぶことが可能です。 最初のオフセットは 2 から始まり、packet content フィールドがオーバーラップせず、そしてそれぞれのフィールドが 4 バイトならば、有効なオフセット値は、2、6、10、14、18、22、26、30、34、・・・・、126 となります。オフセット 126 に関して、その値は 126、127、0、1 バイトのパケットで構成されます。 profile_id <value 1-4> - プロファイルに対応する優先度を設定します。優先度は他のプロファイルと比較して設定され、最も低いプロファイル ID が最も高い優先度を持ちます。1～4 の範囲で設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:アクセスプロファイルを作成するには

```
#create access_profile ethernet vlan source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type profile_id 1
Command: create access_profile ethernet vlan source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type profile_id 1

Success.

#create access_profile ip vlan source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code profile_id 2
Command: create access_profile ip vlan source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code profile_id 2

Success.

#create access_profile packet_content_mask offset_chunk_1 2 0xFFFFFFFF profile_id 3
Command: create access_profile packet_content_mask offset_chunk_1 2 0xFFFFFFFF profile_id 3

Success.
#
```

3.32.2 delete access_profile

目的	作成済みのアクセスプロファイルを削除します。
構文	delete access_profile < profile_id <value 1-4> | all >
説明	本コマンドは、スイッチに作成済みのアクセスプロファイルを削除します。
パラメーター	profile_id <value 1-4> - 本コマンドで削除するアクセスプロファイルを識別する番号を 1～4 の範囲で設定します。この値はアクセスプロファイルが「create access_profile 」コマンドで作成される時に割り当てられます。 all - 削除するすべてのアクセスリストプロファイルを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:プロファイル ID が 1 のアクセスプロファイルを削除するには

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

Success.

#
```

3.32.3 config access_profile

目的	スイッチにアクセスプロファイルを設定し、受信パケットを転送するか、フィルタリングするかを決めるためにスイッチが使用する値を定義します。 「create access_profile」コマンドで入力したマスクは論理積を使用し、指定したフレームのヘッダフィールド内にスイッチが検出した値と統合します。
構文	config access_profile profile_id <value 1-4> < add access_id < auto_assign | <value 1-256> > < *ethernet* | *ip* | *ipv6* | *packet_content* > > | delete access_id <value 1-256> > *ethernet* =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> > *ip* =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* | *udp* | protocol_id <value 0-255> > >] *tcp* =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* =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>]] *ipv6* =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>]]] *packet_content* =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 >] | port < <portlist> | all > > < permit [priority <value 0-7> [replace_priority] | replace_dscp_with <value0-63> | counter < enable | disable >] | deny | mirror >]
説明	本コマンドは、スイッチにアクセスプロファイルを設定し、上の「create access_profile」コマンドを使用して入力したマスク値は論理積を使用し、特定値を組み合わせて入力します。

パラメーター	profile_id <value 1-4> - 設定するアクセスプロファイルを識別する値を入力します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。プロファイル ID は、他のプロファイルと比較した相対的な優先度を設定し、インデックス番号を指定します。このインデックス番号は本コマンドと共に作成され、アクセスプロファイルを識別します。優先度は他のプロファイルと比較して設定され、最も低いプロファイル ID が最も高い優先度を持ちます。1～4 の範囲で設定します。 add access_id <value 1-256> - 上で指定したアクセスプロファイルにルールを追加します。値は作成したルールのインデックスに使用されます。ポートに作成できるルールの数についての詳細は、本章のイントロダクションの項を参照してください。 auto_assign - 本パラメーターは、設定するルールに自動的に数字（1～256 の範囲）を割り当てます。 ethernet - 以下のパラメーターに基づきパケットの廃棄または送信を決定するために各パケットのレイヤ 2 部分をスイッチが調査します。 vlan <vlan_name 32> - 既に作成しているこの VLAN だけにアクセスプロファイルを適用します。 vlan_id <vid> - 既に作成しているこの VLAN だけにアクセスプロファイルを適用します。 source_mac <macaddr> - 送信元 MAC アドレスを持つパケットだけにアクセスプロファイルを適用します。 destination_mac <macaddr> - 送信元 MAC アドレスを持つパケットだけにアクセスプロファイルを適用します。 802.1p <value 0-7> - 802.1p 優先値を持つパケットだけにアクセスプロファイルを適用します。 ethernet_type <hex 0x0-0xffff> - パケットヘッダ内に 16 進数の 802.1Q イーサネットタイプを持つパケットだけにアクセスプロファイルを適用します。 ip - スイッチが各パケットの IP フィールドを調査する場合に指定します。 vlan <vlan_name 32> - 既に作成しているこの VLAN だけにアクセスプロファイルを適用します。 vlan_id <vid> - 本 VLAN ID を持つ VLAN だけにアクセスプロファイルを適用します。 source_ip <ipaddr> - 送信元 IP アドレスを持つパケットだけにアクセスプロファイルを適用する場合に指定します。 destination_ip <ipaddr> - アクセスプロファイルをこの送信先 IP アドレスを持つパケットにだけ適用します。 dscp <value 0-63> - アクセスプロファイルが IP パケット中の type-of-Service(DiffServ コードポイント、DSCP)フィールドにこの値を有するパケットに対してのみ適用する場合に指定します。 icmp - スイッチが各パケットのインターネットコントールメッセージプロトコル(ICMP)フィールドを調査する場合に指定します。 type<0-255> - スイッチが各パケットの ICMP タイプフィールドを調査する場合に指定します。

	code<0-255> - スイッチが各パケットの ICMP コードフィールドを調査する場合に指定します。 igmp -スイッチが各パケットのインターネットグループマネージメントプロトコル(IGMP)フィールドを 調査する場合に指定します。 type<0-255> - スイッチが各パケットの IGMP タイプフィールドを調査する場合に指定します。 tcp - 各パケット内の Transmission Control Protocol(TCP)フィールドを調査する場合に指定します。 src_port <value 0-65535> - アクセスプロファイルはヘッダ内に本 TCP 送信元ポートを持つパケットにだけ適用します。 dst_port <value 0-65535> - アクセスプロファイルはヘッダ内に本 TCP 送信先ポートを持つパケットにだけ適用します。 flag - 対応する TCP フラグのタイプを入力します。 all： すべてのフラグが選択されます。 urg： TCP 制御フラグ(urgent： 緊急) ack: TCP 制御フラグ(acknowledgement： 承認) psh: TCP 制御フラグ(push： プッシュ) rst: TCP 制御フラグ(reset： リセット) syn: TCP 制御フラグ(synchronize： 同期化) fin: TCP 制御フラグ(finish： 終了) udp - 各パケットの Universal Datagram Protocol(UDP)フィールドを調査します。 src_port <value 0-65535> - アクセスプロファイルはヘッダ内に本 UDP 送信元ポートを持つパケットにだけ適用します。 dst_port <value 0-65535> - アクセスプロファイルはヘッダ内に本 UDP 送信先ポートを持つパケットにだけ適用します。 protocol_id <value 0-255> - スイッチが各パケットのプロトコル ID フィールドを調査するように指定し、このフィールドにここで入力した値が含まれている場合、以下のルールを適用します。 user_define - 追加するルールの IP プロトコル ID と IP ペイロードの最初の 4 バイトを指定します。 ipv6 - IPv6 フィルタリングマスクを指定します。 class - IPv6 クラスを指定します。 flowlabel - IPv6 フローラベルを指定します。 source_ipv6 - IPv6 送信元アドレスを指定します。 destination_ipv6 - IPv6 送信先アドレスを指定します。 tcp - TCP ポートサブマスクを指定します。 udp - UDP ポートサブマスクを指定します。 src_port - IPv6 L4 (TCP/UDP) 送信元ポートのサブマスクを指定します。 dst_port - IPv6 L4 (TCP/UDP) 送信先ポートのサブマスクを指定します。 icmp - スイッチが各パケットのインターネットコントールメッセージプロトコル(ICMP)フィールドを調査する場合に指定します。 type<0-255> - スイッチが各パケットの ICMPv6 タイプフィールドを調査する場合に指定します。 code<0-255> - スイッチが各パケットの ICMP コードフィールドを調査する場合

	に指定します。 packet_content - 最大 4 のオフセットを指定できます。単一の UDF フィールドとして認識される 4 バイトのデータが各オフセットで設定できます。オフセットリファレンスも同様に設定可能です。 offset_chunk_1 - offset_chunk_4 - プロファイルで定義した各 UDF フィールドデータにマッチするデータを指定します。 port <portlist> - スイッチのポート番号を指定し、ルールに従ってアクセスを許容または拒否します。「all」はすべてのポートを指定します。 permit - スイッチによる転送を許可するアクセスプロファイルに適合するパケットを指定します。 priority <value 0-7> - スイッチに既に設定している 802.1p デフォルトの優先度を書き換えたい場合に、このパラメーターを指定します。本フィールドを指定すると、スイッチが受信したパケットの中のこの優先度に一致するパケットは、既に指定した CoS キューに転送されます。 replace_priority <value 0-7> - 指定した CoS キューにパケットを転送する前に、このコマンドで既に指定している基準に適合するパケットの 802.1p デフォルトの優先度を優先度フィールドに入力した値に書き換えたい場合に、このパラメーターを入力します。 指定しない場合は、パケットは転送される前に、入力用の 802.1p ユーザー優先度を元の値に書き換えられます。 replace_dscp_with <value 0-63>- コマンドの最初の部分で指定した基準に適合する入力パケットの「DSCP」フィールドに記述される値を指定します。 counter - カウンター機能を有効または無効にします。これはオプションです。デフォルト値は「disable」 (無効)です。ルールがフローメーターに拘束されない場合、適合するパケットがカウントされます。ルールがフローメーターに拘束される場合、カウンターは上書きされます。 deny - アクセスプロファイルに適合しないパケットはスイッチによって転送することを許可されずフィルタリングされます。 mirror - アクセスプロファイルに一致するパケットをポートにミラーリングします。 delete access_id <value 1-256> - 本コマンドを使用して、イーサネットプロファイル、IP プロファイル、または packet_content プロファイルから指定 ACL ルールを削除します。最大 256 のルールがすべてのアクセスプロファイルに指定できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:10.42.73.0～10.42.73.255 の範囲内で IP アドレスを持つポート 7 のフレームをフィルタリングするためにプロファイル ID が 1 のアクセスプロファイルを設定するには

```
#config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny
Command: config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7
deny

Success.

#
```

注意事項

**APLGM152GT では ethernet、ip、ipv6、packet_content_mask それぞれに ACL ルールを書き込むグループが装置内部で割り当てられています。
同一グループに共通するパケットを受信した場合、最も低いプロファイル ID 及びアクセス ID をもつ ACL が優先と判断されます。異なるグループに共通するパケットを受信した場合、最終的な優先順位は permit 及び deny（deny が上位）によって判断されます。**

**APLGM152 で設定可能な ACL ルール数は装置最大 900 です。
また、1 つのプロファイルに設定可能な最大ルール数は 256 です。**

3.32.4 show access_profile

目的	スイッチに現在設定されているアクセスプロファイルを表示します。
構文	show access_profile [profile_id <value 1-4>]
説明	本コマンドは、現在設定されているアクセスプロファイルを表示します。
パラメーター	profile_id <value 1-4> - プロファイル ID を指定して 1 つのプロファイル ID に対するアクセスフールコンフィグレーションのみを表示します。 プロファイル ID 番号を 1～4 の範囲で設定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されているすべてのアクセスプロファイルを表示するには

```
#show access_profile
Command: show access_profile

Access Profile Table

Total User Set Rule Entries : 0
Total Used HW Entries       : 124
Total Available HW Entries  : 900

================================================================================
Profile ID: 1     Type: Ethernet

MASK on
    VLAN            : 0xFFF
    Source MAC      : 00-00-00-00-00-01
    Destination MAC : 00-00-00-00-00-02
    802.1p
    Ethernet Type

Available HW Entries : 194
================================================================================


#
```

3.33 フローメーターコマンド

3.33.1 config flow_meter profile_id

目的	アクセスプロファイルとルールに基づいたパケットフローベースのメータリング機能を設定します。
構文	config flow_meter profile_id <value 1-4> access_id <value 1-256> < < rate <value 1-1048576> burst_size <value 1-262144> rate_exceed <drop_packet|remark_dscp <value 0-63> > > | delete >
説明	本コマンドは、フローベースメータリングを設定します。メータリング機能は、「シングルレート 2 カラーモード」(single-rate two-color mode)のみをサポートします。本機能のパラメーターを適用するには、アクセスルールを最初に作成する必要があります。 帯域幅を Kbps の単位で設定できますが、帯域幅を超過した場合、コンフィグレーションに従って、超過パケットは破棄、または DSCP フィールドを割り当てられます。 設定レートを遵守するために、パケットは ACL ルールに従い処理されます。 本フローメーターリング機能は ACL ルールが「permit」か「mirror」の場合のみ有効です。
パラメーター	profile_id <value 1-4> - プロファイル ID 番号を指定します。 access_id <value 1-256> - アクセス ID 番号を指定します。 rate <value 1-1048576> - シングルレート 2 カラーモードのレートを指定します。フローの認定帯域幅を Kbps で指定します。最小レートは 1 Kbps ですが、実際には 8Kbps の倍数で動作します。設定可能な最大レートは 1,048,576 Kbps です。 burst_size <value 1-262144> - 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、Kbytes です。バーストサイズの最小値は 1 K バイトで、最大値は 262,144 K バイトです。 rate_exceed - シングルレート 2 カラーモードの認定レートを超過したパケットの処理について設定します。この処理は以下の方法のいずれかを指定できます。 drop_packet: 超過パケットを破棄する。 remark_dscp: DSCP の割り当てをパケットにマークする。超過したパケットはまた破棄優先値を高く設定されます。 delete - 指定したフローメーターを削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ACL ルールに一致する入力パケットのレートとバーストを設定するには

```
# config flow_meter profile_id 1 access_id 1 rate 64 burst_size 64 rate_exceed drop_packet
Command: config flow_meter profile_id 1 access_id 1 rate 64 burst_size 64 rate_exceed
drop_packet

Success.

#
```

3.33.2 show flow_meter

目的	フローベースのメータリング設定を表示します。
構文	show flow_meter [profile_id <value 1-4> [access_id <value 1-256>]]
説明	本コマンドは、フローメーターの設定を表示します。
パラメーター	profile_id <value 1-4> - プロファイル ID 番号を指定します。 access_id <value 1-256> - アクセス ID 番号を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:フローメーターの設定を表示するには

```
# show flow_meter
Command: show flow_meter

Flow Meter information:
-----------------------
Profile ID : 1             Access ID : 1          Mode : Single-rate Two-color
Rate:   2000(Kbps)         Burst Size:1000(Kbyte)
Actions:
Conform : Permit
Violate : Drop

Profile ID : 1             Access ID : 2          Mode : Single-rate Two-color
Rate:   2000(Kbps)         Burst Size:1016(Kbyte)
Actions:
Conform : Permit
Violate : Permit           Replace_dscp : 20



Total Flow Meter Entries: 2
#
```

3.34 802.1X コマンド

3.34.1 enable 802.1x

目的	スイッチの 802.1X 認証を有効にします。
構文	enable 802.1x
説明	本コマンドは、スイッチの 802.1X 認証を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの 802.1X 認証を有効にするには

```
#enable 802.1x
Command: enable 802.1x

Success.

#
```

3.34.2 disable 802.1x

目的	スイッチの 802.1X 認証を無効にします。
構文	disable 802.1x
説明	本コマンドは、スイッチの 802.1X 認証を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの 802.1X 認証を無効にするには

```
#disable 802.1x
Command: disable 802.1x

Success.

#
```

3.34.3 config 802.1x authorization network radius

目的	RADIUS サーバーによる認証属性の割り当てを有効または無効にします。
構文	config 802.1x authorization network radius <enable | disable>
説明	本コマンドは、802.1X 認証において RADIUS サーバーで定義された認証属性の割り当てを有効または無効にします。 有効の場合、RADIUS サーバーで定義されたダイナミック VLAN の割り当てなどが許可されます。デフォルト設定は、「enable」(有効)です。
パラメーター	enable - RADIUS サーバーによる認証属性の割り当てを有効にします。 disable - RADIUS サーバーによる認証属性の割り当てを無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:RADIUS 認証属性を有効にするには

```
#config 802.1x authorization network radius enable
Command: config 802.1x authorization network radius enable

Success.

#
```

注意事項

認証属性を有効とするためには、認証属性のグローバル設定が「enable」(有効)である必要があります。この設定は「enable authorization network」コマンドで行います。

ダイナミック VLAN により動的 VLAN を割り当てる場合、ローミングするポートの VLAN ID が異なるため、ポートの Ingres checking 設定を無効にする必要があります。
この設定は「config gvrp all ingress_checking disable」コマンドで行います。

3.34.4 show 802.1x

目的	スイッチの 802.1X 認証設定および認証状態を表示します。
構文	show 802.1x 〈 auth_state | auth_configuration 〉[ports 〈portlist〉]
説明	本コマンドは、スイッチの 802.1X 認証設定および認証状態を表示します。
パラメーター	auth_state - 802.1X 認証状態を表示します。 auth_configuration - 802.1X 認証設定を表示します。 ports 〈portlist〉- 表示するポートまたはポート範囲を指定します。 以下に表示詳細を示します。 〈show 802.1x 実行時に表示されるパラメータの説明〉 802.1X: Enabled / Disabled - 802.1X 認証のステータスを表示します。 Authentication Protocol - 802.1X 認証プロトコルを表示します。 「radius_eap」または「local」を指定することができます。 Forward EAPOL PDU - EAPOL PDU の転送設定を表示します。 Max User - スイッチで可能な最大端末数を表示します。。 RADIUS Authorization: Enabled / Disabled - RADIUS 認証属性を表示します。 〈show 802.1x auth_configuration 実行時に表示されるパラメータの説明〉 Port number - スイッチのポート番号を表示します。 Capability: Authenticator/None - 各ポートの 802.1X 認証を表示します。 CtlDir: Both / In - 未認証の制御ポートが送受両方向または受信方向だけで通信に制御を行うかどうかを表示します。 Port Control: ForceAuth / ForceUnauth / Auto - ポートの認証状態の管理者制御を指定します。「ForceAuth」はポートのオーセンティケータを認証済みに強制します。「ForceUnauth」はポートを非認証に強制します。 QuietPeriod - 認証失敗後、認証再開するまでの時間を表示します。 TxPeriod - サプリカントから EAP Response/identity パケットの応答がない場合の待ち時間を表示します。 SuppTimeout - Request / Identity パケットを除くすべての EAP パケットに対するサプリカント（ユーザー）からの応答を待つ時間を表示します。 ServerTimeout - RADIUS サーバーからの応答を待つ時間の長さを表示します。 MaxReq - サプリカントへの EAP Request パケットの再送信回数を表示します。 ReAuthPeriod - 再認証の間隔時間を表示します。 ReAuthenticate: Enabled / Disabled - 再認証を行うかどうかを表示します。 Forward EAPOL PDU On Port: Enabled / Disabled - ポートにおける EAPOL PDU の転送設定を表示します。 Max User On Port - ポートの最大端末数を表示します。 〈show 802.1x auth_state コマンド実行時に表示されるパラメータの説明〉 Port number - スイッチのポート番号を表示します。 Auth PAE State: Initalize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth - Authenticator PAE の認証状態を表示します。

パラメーター	Backend State: Request / Response / Fail / Idle / Initalize / Success / Timeout - Backend Authenticator の状態を表示します。 Port Status: Authorized / Unauthorized - 認証プロセスの結果を表示します。Authorized は、ユーザーが認証され、ネットワークにアクセスできることを意味します。Unauthorized は、ユーザーが認証されず、ネットワークにアクセスできないことを意味します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチの 802.1X 認証設定を表示するには

```
#show 802.1x
Command: show 802.1x

802.1X                    : Enabled
Authentication Protocol : Local
Forward EAPOL PDU       : Enabled
Max User                  : 1000
RADIUS Authorization    : Enabled

#
```

使用例:ポート 1 の 802.1X 認証設定を表示するには

```
#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    sec
TxPeriod                  : 30    sec
SuppTimeout               : 30    sec
ServerTimeout             : 30    sec
MaxReq                    : 2     times
ReAuthPeriod              : 3600  sec
ReAuthenticate            : Disabled
Forward EAPOL PDU On Port : Enabled
Max User On Port          : 16

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

使用例:ポートの 802.1X 認証状態を表示するには

```
#show 802.1x auth_state
Command: show 802.1x auth_state

Status:  A - Authorized; U - Unauthorized; (P): Port-Based 802.1X
Port  MAC Address          PAE State      Backend State Status VID
----  -------------------- -------------- ------------- ------ ----
1     00-40-66-00-00-01    Authenticated  Idle          A      1









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

3.34.5 config 802.1x capability ports

目的	スイッチのポートごとに 802.1X 認証を設定します。
構文	config 802.1x capability ports < <portlist> | all > <authenticator | none>
説明	本コマンドには、「authenticator」と「none」の 2 つの機能があり、ポートごとに設定できます。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - スイッチのすべてのポートを設定します。 authenticator - このポートでは 802.1X 認証プロセスを実施します。 none - このポートでは 802.1X 認証により制御されません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1～10 に 802.1X 認証を設定するには

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

Success.

#
```

3.34.6 config 802.1x fwd_pdu ports

目的	各ポートの EAPOL PDU 転送機能を有効または無効に設定します。
構文	config 802.1x fwd_pdu ports < <portlist> | all > <enable | disable>
説明	本コマンドは、802.1X 認証が無効なポートにおいて EAPOL PDU を受信した場合、同一 VLAN へのフラッティングをポート単位で有効または無効に設定します。 デフォルト設定は、「enable」(有効)です。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - 全てのポートを指定する場合に選択します。 enable - 指定ポートの EAPOL PDU 転送機能を有効にします。 disable - 指定ポートの EAPOL PDU 転送機能を無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1-2 の 802.1x fwd_pdu を有効にするには

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

Success.

#
```

3.34.7 config 802.1x fwd_pdu system

目的	スイッチの EAPOL PDU 転送機能を有効または無効に設定します。
構文	config 802.1x fwd_pdu system <enable | disable>
説明	本コマンドは、802.1X 認証が無効なポートにおいて EAPOL PDU を受信した場合、同一 VLAN へのフラッティングを装置で有効または無効に設定します。 デフォルト設定は、「enable」(有効)です。
パラメーター	enable - スイッチの EAPOL PDU 転送機能を有効にします。 disable - スイッチの EAPOL PDU 転送機能を無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチで 802.1x fwd_pdu を有効にするには

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


Success.


#
```

3.34.8 config 802.1x auth_parameter ports

目的	指定ポートの 802.1X 認証パラメーターを設定します。
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 1-1000>] | enable_reauth < enable | disable > >
説明	本コマンドは、指定ポートの 802.1X 認証パラメーターを設定します。 default パラメーターは、指定ポートの 802.1X 認証設定をデフォルト値に戻します。 max_users パラメーターでは、ポート単位で最大端末数を設定できます。デフォルト値は 16 です。装置の最大端末数 1000 を超える設定はできません。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - スイッチのすべてのポートを設定します。 default - 指定したポートの 802.1X 認証設定をデフォルト値に戻します。 direction <both | in> - ポートベース認証において、制御されたポートが送受信両方または受信方向だけの通信をブロックするかどうかを設定します。 port_control - ポート範囲の認証処理における管理用の制御を設定します。以下の認証オプションがあります。 force_auth - ポートを強制的に認証済みの状態にします。スイッチを経由するネットワークアクセスは許可されます。 auto - ポートステータスに認証プロセスの結果を反映します。 force_unauth - ポートを強制的に非認証状態にします。スイッチを経由するネットワークアクセスはブロックされます。 quiet_period <sec 0-65535> - サプリカントの認証に失敗した後、新しく認証を開始するまでの間隔を設定します。 tx_period <sec 1-65535> - EAP Request/Identity パケットの送信間隔を設定します。tx_period で設定した時間、サプリカントからの応答が無かった場合、装置は EAP Request/Identity パケットを再送します。 supp_timeout <sec 1-65535> - EAP Request / Identity パケットを除くすべての EAP パケットに対するサプリカント(ユーザー)からの応答を待つ時間を設定します。 server_timeout - RADIUS サーバーからの応答を待つ時間を設定します。 max_req <value 1-10> - サプリカントに送信する EAP Request/Identity パケットの最大回数を設定します。 reauth_period <sec 1-65535> - クライアントの定期的な再認証の間隔を設定します。 max_users <value1-1000> - ポートあたりの最大端末数を指定します。 enable_reauth <enable | disable> - スイッチが再認証するかどうかを決定します。 有効にすると、「reauth_period」パラメーターで指定した間隔でユーザーを再認証します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1～20 に 802.1X 認証パラメーターをデフォルト設定にするには

```
#config 802.1x auth_parameter ports 1-20 default
Command: config 802.1x auth_parameter ports 1-20 default

Success.

#
```

3.34.9 config 802.1x auth_protocol

目的	スイッチの 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 >
説明	本コマンドは、認証プロトコルを設定します。
パラメーター	local | radius_eap - 希望する認証プロトコルのタイプを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの認証プロトコルを設定するには

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

Success.

#
```

注意事項

802.1X のローカル認証は、MD5 のみサポートします。

3.34.10 config 802.1x init

目的	ポート範囲内の 802.1X 機能を初期化します。
構文	config 802.1x init < port_based ports < <portlist> | all > | mac_based | ports <<portlist> | all > [mac_address <macaddr>] >
説明	本コマンドは、指定したポート範囲または指定したポート範囲から動作する MAC アドレスの 802.1X 機能をただちに初期化します。
パラメーター	port_based - スイッチがポート番号のみに基づいた 802.1X 機能を初期化する場合に指定します。初期化する対象のポートを指定します。 mac_based - スイッチがポート配下の特定の MAC アドレスに対して 802.1X 機能を初期化する場合に指定します。初期化する対象の MAC アドレスを指定します。 ports <portlist> - ポートまたはポート範囲を指定します。 all - スイッチのすべてのポートを指定します。 mac_address <macaddr> - 初期化する MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートの認証状態マシンを初期化するには

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

Success.

#
```

3.34.11 config 802.1x max_users

目的	スイッチの 802.1X 認証における最大端末数を設定します。
構文	config 802.1x max_users [<value 1-1000>]
説明	本コマンドは、スイッチの 802.1x 認証における最大端末数を設定します。
パラメーター	value - スイッチの最大端末数を 1-1000 の範囲で設定します。 デフォルト値は、1000 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチに 802.1X 認証の最大端末数を 100 に設定するには

```
#config 802.1x max_users 100
Command: config 802.1x max_users 100

Success.

#
```

3.34.12 config 802.1x reauth

目的	スイッチの 802.1X 再認証機能を設定します。
構文	config 802.1x reauth < port_based ports < <portlist> | all > | mac_based | ports < <portlist> | all > [mac_address <macaddr>] >
説明	本コマンドは、ポート番号に基づいて認証済みデバイスを再認証します。
パラメーター	port_based - スイッチがポート番号のみに基づいた 802.1X の再認証を行う場合に指定します。再認証する対象のポートを指定します。 mac_based - スイッチがポート配下の特定の MAC アドレスに対して 802.1X の再認証を行う場合に指定します。再認証する対象の MAC アドレスを指定します。 ports <portlist> - 再認証するポートまたはポート範囲を指定します。 all - スイッチのすべてのポートを指定します。 mac_address <macaddr> - 再認証する MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1-18 の 802.1X 認証を再認証するには

```
#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

#
```

3.34.13 config radius add

目的	スイッチが RADIUS サーバーと通信するための設定をします。
構文	config radius add < server_index 1-3> <server_ip> key <passwd 32> < default | < auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> > >
説明	本コマンドは、スイッチが RADIUS サーバーと通信するための設定をします。
パラメーター	<server_index 1-3> - RADIUS サーバーのインデックス番号を割り当てます。 最大 3 つまでの RADIUS サーバーをスイッチに登録できます。 スイッチでは登録したインデックス番号の若い順に RADIUS の応答を確認し、最初に応答した RADIUS を認証サーバーとして認識します。 <server_ip> - RADIUS サーバーの IP アドレスを入力します。 key - スイッチと RADIUS サーバー間で使用するパスワードと暗号鍵を指定します。 <passwd 32> - RADIUS サーバーとスイッチが使用する共有秘密鍵。32 文字以内で指定します。 default - 「auth_port」と「acct_port」設定の両方にデフォルト UDP ポート番号を使用します。 auth_port <udp_port_number 1-65535> - 認証リクエストに対する UDP ポート番号を入力します。デフォルト値は、1812 です。 acct_port <udp_port_number 1-65535> - アカウンティングリクエストに対する UDP ポート番号を入力します。デフォルト値は、1813 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:RADIUS サーバー通信設定を行うには

```
#config radius add 1 10.48.74.121 key APS default
Command: config radius add 1 10.48.74.121 key APS default

Success.

#
```

3.34.14 config radius delete

目的	入力済み RADIUS サーバー設定を削除します。
構文	config radius delete <server_index 1-3>
説明	本コマンドは、入力済み RADIUS サーバー設定を削除します。
パラメーター	<server_index 1-3> - 削除したい RADIUS サーバーの番号を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:設定済み RADIUS サーバー設定を削除するには

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

Success.

#
```

3.34.15 config radius

目的	登録した RADIUS サーバーの設定を変更します。
構文	config radius <server_index 1-3> < ipaddress <server_ip> | key <passwd 32> | auth_port < <udp_port_number 1-65535> | default > | acct_port < <udp_port_number 1-65535> | default > >
説明	スイッチが RADIUS サーバーと通信するための設定をします。
パラメーター	<server_index 1-3> - 登録した RADIUS サーバーのインデックス番号を指定します。 ipaddress <server_ip> - RADIUS サーバーの IP アドレスを変更します。 key <passwd 32> - RADIUS サーバーとスイッチが使用する共有秘密鍵を 32 文字以内で変更します。 auth_port < <udp_port_number 1-65535> | default > - 認証リクエストに対する UDP ポート番号を変更します。デフォルト値は、1812 です。 acct_port < <udp_port_number 1-65535> | default > - アカウンティングリクエストに対する UDP ポート番号を変更します。デフォルト値は、1813 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:RADIUS サーバー設定を変更するには

```
#config radius 1 ipaddress 10.1.1.1 key APS-1
Command: config radius 1 ipaddress 10.1.1.1 key APS-1


Success.


#
```

3.34.16 config radius parameter

目的	RADIUS サーバーのパラメーターを設定します。
構文	config radius parameter < timeout <int 1-255> | retransmit <int 1-255> >
説明	本コマンドは、RADIUS サーバーのパラメーターを設定します。
パラメーター	timeout <int 1-255> - サーバーの応答を待つ時間を入力します。 デフォルト値は 5 秒です。 retransmit <int 1-255> - 再送回数を入力します。デフォルト値は 2 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:RADIUS サーバーのタイムアウトオプションを設定するには

```
# config radius parameter timeout 3
Command: config radius parameter timeout 3

Success.

#
```

3.34.17 show radius

目的	スイッチに設定された RADIUS 設定を表示します。
構文	show radius
説明	本コマンドは、スイッチの RADIUS 設定を表示します。 Status には、RADIUS 応答状態に関係なく「Active」を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに設定された RADIUS 設定を表示するには

```
#show radius
Command: show radius

Timeout      : 5 seconds
Retransmit   : 2

Index  IP Address          Auth-Port  Acct-Port  Status          Key
                           Number     Number
-----  ------------------  ---------  ---------  --------------  ---------------
1       10.1.1.1             1812       1813       Active         APS-1
2       10.2.1.1             1800       1813       Active         APS-2

Total Entries : 2

#
```

3.34.18 show acct_client

目的	RADIUS アカウンティングクライアントを表示します。
構文	show acct_client
説明	本コマンドは、スイッチに現在設定されている RADIUS アカウンティングクライアントを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:RADIUS アカウンティングクライアントを表示するには

```
#show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier              APRESIA Systems

radiusAuthServerEntry ==>
radiusAccServerIndex : 1

radiusAccServerAddress                   10.53.13.199
radiusAccClientServerPortNumber          1813
radiusAccClientRoundTripTime             0
radiusAccClientRequests                  0
radiusAccClientRetransmissions           0
radiusAccClientResponses                 0
radiusAccClientMalformedResponses        0
radiusAccClientBadAuthenticators         0
radiusAccClientPendingRequests           0
radiusAccClientTimeouts                  0
radiusAccClientUnknownTypes              0
radiusAccClientPacketsDropped            0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.19 show auth_client

目的	RADIUS 認証クライアントを表示します。
構文	show auth_client
説明	本コマンドは、スイッチに現在設定されている RADIUS 認証クライアントを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:RADIUS 認証クライアントを表示するには

```
#show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               APRESIA Systems



radiusAuthServerEntry ==>
radiusAuthServerIndex  :1

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         0
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.20 show auth_diagnostics

目的	認証診断を表示します。
構文	show auth_diagnostics [ports <portlist>]
説明	ポートベースでスイッチの認証診断を表示します。
パラメーター	ports <portlist> - ポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 1 の認証診断を表示するには

```
#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Port number  : 1
MAC address: 00-40-66-5D-60-02

EntersConnecting                      3
EapLogoffsWhileConnecting             0
EntersAuthenticating                  2
SuccessWhileAuthenticating            2
TimeoutsWhileAuthenticating           0
FailWhileAuthenticating               0
ReauthsWhileAuthenticating            0
EapStartsWhileAuthenticating          0
EapLogoffWhileAuthenticating          0
ReauthsWhileAuthenticated             0
EapStartsWhileAuthenticated           1
EapLogoffWhileAuthenticated           0
BackendResponses                      4
BackendAccessChallenges               2
BackendOtherRequestsToSupplicant      0
BackendNonNakResponsesFromSupplicant  2
BackendAuthSuccesses                  2
BackendAuthFails                      0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.21 show auth_session_statistics

目的	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 | all>]
説明	ポートベースでのスイッチの認証セッション統計情報を表示します。
パラメーター	ports <portlist> - ポート範囲を指定します。 all - 全てのポートの統計情報を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 1 の認証セッション統計情報を表示するには

```
#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port number  : 1
MAC address: 00-40-66-5D-60-02

SessionOctetsRx                 7808
SessionOctetsTx                 469102741
SessionFramesRx                 122
SessionFramesTx                 4196211
SessionId                       ether1_2-1
SessionAuthenticMethod          Remote Authentication Server
SessionTime                     70803
SessionTerminateCause           NotTerminatedYet
SessionUserName                 456
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.22 show auth_statistics

目的	認証統計を表示します。
構文	show auth_statistics [ports <portlist>]
説明	ポートベースでのスイッチの認証統計情報を表示します。
パラメーター	ports <portlist> - ポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート 1 の認証統計を表示するには

```
#show auth_statistics ports 1
Command: show auth_statistics ports 1

Port number : 1
MAC address: 00-40-66-5D-60-02

EapolFramesRx                   6
EapolFramesTx                   7
EapolStartFramesRx              2
EapolReqIdFramesTx              3
EapolLogoffFramesRx             0
EapolReqFramesTx                2
EapolRespIdFramesRx             2
EapolRespFramesRx               2
InvalidEapolFramesRx            0
EapLengthErrorFramesRx          0

LastEapolFrameVersion           1
LastEapolFrameSource            00-40-66-5D-60-02
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.23 create 802.1x user

目的	802.1X 認証のローカルユーザーを作成します。
構文	create 802.1x user <username 15>
説明	本コマンドは、802.1X 認証のローカルユーザーを作成します。
パラメーター	<username 15> - 半角英数字 15 文字以内でユーザー名を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:802.1X 認証のローカルユーザーを作成するには

```
#create 802.1x user APS
Command: create 802.1x user APS

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

#
```

3.34.24 show 802.1x user

目的	スイッチの 802.1X 認証ローカルユーザーアカウントを表示します。
構文	show 802.1x user
説明	本コマンドは、スイッチに現在設定されている 802.1X 認証のローカルユーザーアカウントを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている 802.1X 認証のローカルユーザーを表示するには

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


 Current Accounts:
 Username         Password
 ---------------  ---------------
 user1            pass


 Total Entries:1


#
```

3.34.25 delete 802.1x user

目的	スイッチの 802.1X 認証ローカルユーザーアカウントを削除します。
構文	delete 802.1x user <username 15>
説明	本コマンドは、スイッチに現在設定されている 802.1X 認証のローカルユーザーアカウントを削除します。
パラメーター	<username 15> - ユーザー名は 15 文字までの半角英数字で指定できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:802.1X 認証のローカルユーザーを削除するには

```
#delete 802.1x user ctsnow
Command: delete 802.1x user ctsnow

Success.

#
```

3.35 アクセス認証制御コマンド

アクセス認証制御は、TACACS/XTACACS/TACACS+/RADIUS プロトコルを使用してスイッチへの安全なアクセスを可能にします。ユーザーがスイッチへのログインや、管理者レベルの特権へのアクセスを行おうとする時、パスワードの入力を求められます。TACACS/ XTACACS/ TACACS+/ RADIUS 認証がスイッチで有効になると、スイッチは TACACS/XTACACS/TACACS+/RADIUS サーバーと連絡し、ユーザーの確認をします。確認が行われたユーザーは、スイッチへのアクセスを許可されます。

現在 TACACS セキュリティープロトコルには異なるエンティティを持つ 3 つのバージョンが存在します。本スイッチのソフトウェアは TACACS の以下 のバージョンをサポートします。

TACACS(Terminal Access Controller Access Control System) - セキュリティーのためのパスワードチェック、認証、およびユーザーアクションの通知を、1 台またはそれ以上の集中型の TACACS サーバーを使用して行います。パケットの送受信には UDP プロトコルを使用します。

XTACACS(拡張型 TACACS) - TACACS プロトコルの拡張版で、TACACS プロトコルより多種類の認証リクエストとレスポンスコードに対応します。パケットの送受信には UDP プロトコルを使用します。

TACACS+(Terminal Access Controller Access Control System plus) - ネットワークデバイスの認証のために詳細なアクセス制御を提供します。TACACS+は、1 台またはそれ以上の集中型のサーバーを経由して認証コマンドを使用することができます。TACACS+プロトコルは、スイッチと TACACS+デーモンの間のすべてのトラフィックを暗号化します。また、TCP プロトコルを使用して信頼性の高い伝達を行います。

スイッチは、アクセス認証制御コマンドを使用して認証するための RADIUS プロトコルもサポートします。RADIUS (Remote Authentication Dial In User Server)は、認証用にリモートサーバーを使用し、ユーザーによる接続要求の受信、ユーザーの認証、クライアントがユーザーにサービスを提供するために必要なコンフィグレーション情報すべての提供を行う役割も持ちます。 RADIUS は本セクションにリストされたコマンドを使用してスイッチで活用できます。

TACACS/XTACACS/TACACS+/RADIUS のセキュリティー機能が正常に動作するためには、スイッチ以外の認証サーバーと呼ばれるデバイス上で 認証用のユーザー名とパスワードを含む TACACS/XTACACS/TACACS+/ RADIUS サーバーの設定を行う必要があります。スイッチがユーザーにユーザー名とパスワードの要求を行う時、スイッチは、TACACS/XTACACS/TACACS+/RADIUS サーバーにユーザー認証の問い合わせを行います。サーバーは以下の 3 つのうちの 1 つの応答を返します。

(1) サーバーは、ユーザー名とパスワードを認証し、ユーザーにスイッチへの通常のアクセス権を与えます。
(2) サーバーは、入力されたユーザー名とパスワードを受け付けず、スイッチへのアクセスを拒否します。
(3) サーバーは、認証の問い合わせに応じません。 この時点でスイッチはサーバーからタイムアウトを受け取り、メソッドリスト中に設定された次の認証 方法へと移行します。

本スイッチには TACACS、XTACACS、TACACS+、RADIUS の各プロトコル用に 4 つの認証サーバーグループがあらかじめ組み込まれています。これらのビルトインサーバーグループは、スイッチにアクセスを試みるユーザーの認証に使用されます。認証サーバーグループ内に任意の順番で認証サーバーを設定し、ユーザーがスイッチへのアクセス権を取得する場合、1 番目の認証サーバーに認証を依頼します。認証が行われなければ、リストの 2 番目のサーバーに依頼し、以下同様の処理が続きます。

実装されている認証サーバーグループには、特定のプロトコルが動作するホストのみを登録できます。 例えば TACACS 認証サーバーグループは、TACACS 認証サーバーのみを登録できます。

スイッチの管理者は、ユーザー定義のメソッドリストに 6 種類の異なる認証方法 (TACACS/XTACACS/TACACS+/RADIUS/local/none) を設定できます。これらの方法は、任意に並べ替えることが可能で、スイッチ上での通常のユーザー認証に使用されます。リストには最大 8 つの認証方法を登録できます。ユーザーがスイッチにアクセスしようとすると、スイッチはリストの 1 番目の認証方法を選択して認証を行います。1 番目の方法で認証サーバーを通過しても認証が返ってこなければ、スイッチはリストの次の方法を試みます。この手順は、認証が成功するか、拒否されるか、またはリストのすべての認証方法を試し終わるまで繰り返されます。

スイッチへのアクセス権を取得したユーザーは、通常のアクセス権を与えられていることにご注意ください。管理者特権レベルの権利を取得するためには、ユーザーは「enable admin」コマンドにアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。

注意事項

TACACS、XTACACS、TACACS+、RADIUS は独立したエンティティであり、互換性はありません。スイッチとサーバー間は、同じプロトコル を使用した全く同じ設定を行う必要があります(例えば、スイッチに TACACS 認証を設定した場合、ホストサーバーにも同様の設定を行います)。

3.35.1 enable authen_policy

目的	システムアクセス認証ポリシーを有効にします。
構文	enable authen_policy
説明	本コマンドは、管理者が定義するスイッチにアクセスするユーザーのための認証ポリシーを有効にします。有効にすると、デバイスはログインメソッドリストをチェックし、ログイン時のユーザー認証に使用する認証方法を選択します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:システムアクセス認証ポリシーを有効にするには

```
#enable authen_policy
Command: enable authen_policy

Success.

#
```

3.35.2 disable authen_policy

目的	システムアクセス認証ポリシーを無効にします。
構文	disable authen_policy
説明	本コマンドは、管理者が定義するスイッチにアクセスするユーザーのための認証ポリシーを無効にします。無効になると、スイッチはユーザー名とパスワード検証のためにローカルユーザーアカウントデータベースにアクセスします。 さらに、スイッチは、現在、管理者レベルの権限にアクセスを試みる普通のユーザーのために認証としてローカルイネーブルパスワードを受け入れます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:システムアクセス認証ポリシーを無効にするには

```
#disable authen_policy
Command: disable authen_policy

Success.

#
```

3.35.3 show authen_policy

目的	スイッチ上のシステムアクセス認証ポリシーのステータスを表示します。
構文	show authen_policy
説明	スイッチ上のアクセス認証ポリシーのステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:システムアクセス認証ポリシーを表示するには

```
#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

#
```

3.35.4 create authen_login method_list_name

目的	ユーザーがスイッチにログインする際の認証方法のユーザー定義メソッドリストを作成します。
構文	create authen_login method_list_name <string 15>
説明	本コマンドは、ユーザーがログインする際の認証方法リストを作成します。本スイッチは、最大 8 個のメソッドリストをサポートしていますが、1 つはデフォルトとして予約されているため、削除できません。複数のメソッドリストは、別々に作成および設定される必要があります。
パラメーター	<string 15> - 15 文字以内の半角英数字の文字列を入力して、メソッドリストを定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:メソッドリスト「APS」を作成するには

```
#create authen_login method_list_name APS
Command: create authen_login method_list_name APS

Success.

#
```

3.35.5 config authen_login

目的	ユーザーがログインする際の認証方法を規定するユーザー定義またはデフォルトのメソッドリストを設定します。
構文	config authen_login < default | method_list_name <string 15> > method < tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none >
説明	ユーザーがスイッチにログインする際の認証方法を規定するユーザー定義またはデフォルトのメソッドリストを設定します。 本コマンドで設定した認証方法の順番で、認証結果に影響を与えます。例えば、ログインメソッドリストに「tacacs,xtacacs,local」の順番で認証方法を入力した場合、スイッチはまずサーバーグループ内の 1 番目の「tacacs」ホストに認証リクエストを送信します。 そのサーバーから応答がない場合、2 番目の「tacacs 」ホストに認証リクエストを送信し、リストが終了するまでこの手順を続けます。スイッチは、リストの次のプロトコル xtacacs を使用して、同じシーケンスを再開します。 xtacacs リストを使用しても認証が行われない場合は、スイッチに設定された「local」アカウントのデータベースセットを使用して該当のユーザーを認証します。Local メソッドが使用される時、ユーザーの権限はスイッチに設定されたローカルアカウントの権限に依存します。 これらの方法によって、認証に成功したユーザーには「User」の権限のみが与えられます。ユーザーが管理者レベルの権限に更新したい場合、「enable admin」コマンドを実行し、スイッチに管理者により事前に設定されているパスワードの入力が必要になります（「enable admin」についての詳細は、このセクションの「enable admin」の説明を参照してください)。

パラメーター	default - ユーザー定義されたアクセス認証のデフォルトのメソッドリストを表示します。ユーザーは以下の認証方法を 1 つまたは組み合わせて最大 4 つまで選択できます。 tacacs - 本パラメーターを追加する場合、TACACS server group リストのリモートの TACACS server hosts から TACACS プロトコルを使用してユーザー認証を行う必要があります。 xtacacs - 本パラメーターを追加する場合、XTACACS server group リストのリモートの XTACACSserver hosts から XTACACS プロトコルを使用してユーザー認証を行う必要があります。 tacacs+ - 本パラメーターを追加する場合、TACACS+ server group リストのリモートの TACACS+ server hosts から TACACS+プロトコルを使用し てユーザー認証を行う必要があります。 radius - 本パラメーターを追加する場合、RADIUS server group リストのリモートの RADIUS server hosts から RADIUS プロトコルを使用してユーザー認証を行う必要があります。 server_group 〈string 15〉- 本パラメーターを追加する場合、スイッチに設定済みのユーザー定義のサーバーグループを使用してユーザー認証を行う必要があります。 local - 本パラメーターを追加する場合、スイッチ上のローカル user account データベースを使用してユーザー認証を行う必要があります。 none - 本パラメーターを追加する場合、スイッチにアクセスするための認証は必要ありません。 method_list_name - ユーザーによって定義されたメソッドリスト名を入力します。 ユーザーは以下の認証方法を 1 つまたは組み合わせて本メソッドリストに最大 4 つまで追加できます。 tacacs - 本パラメーターを追加する場合、リモートの TACACS サーバーから TACACS プロトコルを使用してユーザー認証を行う必要があります。 xtacacs - 本パラメーターを追加する場合、リモートの XTACACS サーバーから XTACACS プロトコルを使用してユーザー認証を行う必要があります。 tacacs+ - 本パラメーターを追加する場合、TACACS+サーバーから TACACS+ プロトコルを使用してユーザー認証を行う必要があります。 radius - 本パラメーターを追加する場合、リモートの RADIUS サーバーから RADIUS プロトコルを使用してユーザー認証を行う必要があります。 server_group 〈string 15〉- 本パラメーターを追加する場合、スイッチに設定済みのユーザー定義のサーバーグループを使用してユーザー認証を行う必要があります。 local - 本パラメーターを追加する場合、スイッチ上のローカル user account データベースを使用してユーザー認証を行う必要があります。 none - 本パラメーターを追加する場合、スイッチにアクセスするための認証は必要ありません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:認証メソッド TACACS、XTACACS、および local をこの順番でユーザー定義メソッドリスト「APS」に設定するには

```
#config authen_login method_list_name APS method tacacs xtacacs local
Command: config authen_login method_list_name APS method tacacs xtacacs local

Success.

#
```

使用例:デフォルトのメソッドリストを認証メソッド XTACACS、TACACS+、ローカルの順に設定するには

```
#config authen_login default method xtacacs tacacs+ local
Command: config authen_login default method xtacacs tacacs+ local

Success.

#
```

注意事項

認証プロトコルとして「none」 または「local」 を入力すると、メソッドリストまたはデフォルトのメソッドリストに別の認証が上書きされます。

3.35.6 delete authen_login method_list_name

目的	ユーザーがスイッチにログインする際の認証方法を規定するユーザー定義のログインメソッドリストを削除します。
構文	delete authen_login method_list_name <string 15>
説明	本コマンドは、ユーザーがログインする際の認証方法リストを削除します。
パラメーター	<string 15> - 15 文字以内の半角英数字の文字列を入力して、削除するメソッドリストを定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:メソッドリスト名「APS」を削除するには

```
#delete authen_login method_list_name APS
Command: delete authen_login method_list_name APS

Success.

#
```

3.35.7 show authen_login

目的	ユーザーがスイッチにログインする際の認証方法の設定済みユーザー定義メソッドリストを表示します。
構文	show authen_login < default | method_list_name <string 15> | all >
説明	本コマンドは、ユーザーがログインする際の認証メソッドリストを表示します。
パラメーター	default - 本パラメーターを入力すると、ユーザーがスイッチにログインする際のデフォルトメソッドリストを表示します。 method_list_name <string 15> - 最大 15 文字までの半角英数字文字列を入力して、表示する「method list」を定義します。 all - 本パラメーターを入力すると、現在スイッチに設定されているすべての認証ログインメソッドを表示します。 ウィンドウは次のパラメーターを表示します。 Method List Name - 設定済みメソッドリスト名。 Priority - ユーザーがスイッチにログインする際、認証のために問い合わせされるメソッドリストプロトコルの順番を定義します。1(最も高い) から 4 (最も低い)で優先順位が付けられます。 Method Name - メソッドリスト名ごとに実行されるセキュリティープロトコルを定義します。 Comment - メソッドのタイプを定義します。「User-defined Group」は、ユーザー定義されたサーバーグループを参照します。「Built-in Group」は、スイッチに普遍設定される TACACS、XTACACS、TACACS+および RADIUS セキュリティープロトコルを参照します。「Keyword」は、「local」(スイッチのユーザーアカウントを介した認証)と「none」(スイッチのすべての機能にアクセスするために認証する必要がない)という TACACS/XTACACS/TACACS+/RADIUS に代わる技術を使用した認証を参照します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:「APS」という名の認証ログインメソッドリストを表示するには

```
#show authen_login method_list_name APS
Command: show authen_login method_list_name APS

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

#
```

3.35.8 create authen_enable method_list_name

目的	スイッチでユーザーの権限を通常のユーザーレベルから管理者レベルに上げる認証メソッドのユーザー定義メソッドリストを設定します。
構文	create authen_enable method_list_name <string 15>
説明	本コマンドは、スイッチでユーザーを通常のユーザーレベル権限から管理者レベル権限に昇格する認証メソッドのユーザー定義メソッドリストを設定します。スイッチの通常のユーザーレベル権限を取得したユーザーが管理者レベル権限を得るためには、管理者が定義した方法により認証を受ける必要があります。スイッチに最大 8 件の「enable method list」が実行できます。
パラメーター	<string 15> - 15 文字以内の半角英数字の文字列を入力して、作成する「enable method list」を定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ユーザー権限を管理者権限に昇格するために「APS」という名のユーザー定義メソッドリストを作成するには

```
#create authen_enable method_list_name APS
Command: create authen_enable method_list_name APS

Success.

#
```

3.35.9 config authen_enable

目的	スイッチでユーザーの権限を通常のユーザーレベルから管理者レベル権限に昇格する認証メソッドのユーザー定義メソッドリストを作成します。
構文	config authen_enable < default | method_list_name <string 15> > method < tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none >
説明	本コマンドは、スイッチでユーザーを通常のユーザーレベル権限から管理者レベル権限に昇格する認証メソッドのユーザー定義メソッドリストを設定します。スイッチの通常のユーザーレベル権限を取得したユーザーが管理者レベル権限を得るためには、管理者が定義した方法により認証を受ける必要があります。最大 8 件の「enable method list」がスイッチに同時に実行できます。 本コマンドで設定した認証方法の順番で、認証結果に影響を与えます。例えば、ログインメソッドリストに「tacacs,xtacacs,local_enable」の順番で認証方法を入力した場合、スイッチはまずサーバーグループ内の 1 番目の「TACACS 」ホストに認証リクエストを送信します。認証が得られない場合、サーバーグループの 2 番目の「TACACS 」ホストに認証リクエストを送信し、リストが終了するまでこの手順を続けます。スイッチは、リストの次のプロトコル xtacacs を使用して、同じシーケンスを再開します。xtacacs リストを使用しても認証が行われない場合は、スイッチに設定された「local_enable 」のパスワードセットを使用して該当のユーザーを認証します。 これらの中のいずれかの方法で認証されたユーザーは、「Admin」（管理者）レベルの権限を取得することができます。
パラメーター	default - デフォルトのメソッドリスト名を指定します。 method_list_name - ユーザー定義されたメソッドリスト名を入力します (create authen_enable)。以下の認証方法を最大 4 つまで追加できます。 tacacs - 本パラメーターを追加する場合、リモートの TACACS サーバーから TACACS プロトコルを使用してユーザー認証を行う必要があります。 xtacacs - 本パラメーターを追加する場合、リモートの XTACACS サーバーから XTACACS プロトコルを使用してユーザー認証を行う必要があります。 tacacs+ - 本パラメーターを追加する場合、TACACS+サーバーから TACACS+プロトコルを使用してユーザー認証を行う必要があります。 radius - 本パラメーターを追加する場合、リモートの RADIUS サーバーから RADIUS プロトコルを使用してユーザー認証を行う必要があります。 server_group <string 15> - 本パラメーターは、スイッチに設定済みのユーザー定義のサーバーグループを使用してユーザー認証を行います。 local_enable - 本パラメーターは、スイッチ上のローカル user account データベースを使用してユーザー認証を行う必要があります。 デバイスのローカルイネーブルパスワードは、「config admin local_enable」コマンドを使用して設定できます。 none - 本パラメーターは、スイッチ上の管理者レベル権限にアクセスするための認証は必要ありません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ユーザー定義のメソッドリスト「APS」を認証メソッド TACACS、XTACACS、ローカルの順に設定するには

```
#config authen_enable method_list_name APS method tacacs xtacacs local_enable
Command: config authen_enable method_list_name APS method tacacs xtacacs local_enable

Success.

#
```

使用例:デフォルトのメソッドリストを認証メソッド XTACACS、TACACS+、ローカルの順に設定するには

```
#config authen_enable default method xtacacs tacacs+ local_enable
Command: config authen_enable default method xtacacs tacacs+ local_enable

Success.

#
```

3.35.10 delete authen_enable method_list_name

目的	通常のユーザーレベル権限を管理者レベル権限に昇格するための認証方法を規定するユーザー定義のログインメソッドリストを削除します。
構文	delete authen_enable method_list_name <string 15>
説明	本コマンドは、通常のユーザーレベルの権限を管理者レベル権限に昇格するための認証方法を規定するユーザー定義のログインメソッドリストを削除します。
パラメーター	<string 15> - 15 文字以内の半角英数字の文字列を入力して、削除する「enable method list」を定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ユーザー定義のメソッドリスト「APS」を削除するには

```
#delete authen_enable method_list_name APS
Command: delete authen_enable method_list_name APS

Success.

#
```

3.35.11 show authen_enable

目的	スイッチでユーザーの権限を通常のユーザーレベル権限から管理者レベル権限に昇格する認証メソッドのメソッドリストを表示します。
構文	show authen_enable < default | method_list_name <string 15> | all >
説明	本コマンドは、通常のユーザーレベルの権限を管理者レベル権限に昇格するための認証方法を規定するユーザー定義のログインメソッドリストを表示します。
パラメーター	default - 本パラメーターを入力すると、ユーザーがスイッチの管理者レベル権限にアクセスする際のデフォルトメソッドリストを表示します。 method_list_name <string 15> - 最大 15 文字までの半角英数字文字列を入力して、表示する「method list」を定義します。 all - 本パラメーターを入力すると、現在スイッチに設定されているすべての認証ログインメソッドを表示します。 ウィンドウは次のパラメーターを表示します。 Method List Name - 設定済みメソッドリスト名。 Priority - ユーザーがスイッチにログインする際、認証のために問い合わせされるメソッドリストプロトコルの順番を定義します。1(最も高い) から 4 (最も低い) で優先順位が付けられます。 Method Name - メソッドリスト名ごとに実行されるセキュリティープロトコルを定義します。 Comment - メソッドのタイプを定義します。「User-defined Group」は、ユーザー定義されたサーバーグループを参照します。「Built-in Group」は、スイッチに普遍設定される TACACS、XTACACS、TACACS+および RADIUS セキュリティープロトコルを参照します。「 Keyword」は、「local」(スイッチの local_enable パスワードを介した認証)と「none」(スイッチのすべての機能にアクセスするために認証する必要がない)という TACACS/XTACACS/TACACS+/RADIUS に代わる技術を使用した認証を参照します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:通常のユーザーレベル権限を管理者レベル権限に昇格するためにすべてのメソッドリストを表示するには

```
#show authen_enable all
Command: show authen_enable all

Method List Name  Priority   Method Name    Comment
----------------  --------   -------------  ------------------
Permit               1        tacacs+         Built-in Group
                     2        tacacs          Built-in Group
                     3        APS             User-defined Group
                     4        local_enable    Keyword

default              1        tacacs+         Built-in Group
                     2        local_enable    Keyword

Total Entries : 2

#
```

3.35.12 config authen application

目的	設定済みのメソッドリストを使用して、認証のためにスイッチに様々なアプリケーションを設定します。
構文	config authen application < console | telnet | ssh | http | all > < login | enable > < default | method_list_name <string 15> >
説明	本コマンドは、作成済みのメソッドリストを使用して、ユーザーレベルおよび管理者レベル(authen_enable)でログインする際に使用するスイッチの設定用アプリケーション(コンソール、Telnet、SSH、Web)を設定します。
パラメーター	application - 設定するアプリケーションを選択します。 以下の 5 つのオプションの 1 つを選択します。 console - コマンドラインインターフェースログインメソッドを設定します。 telnet - Telnet ログインメソッドを設定します。 ssh - Secure Shell ログインメソッドを設定します。 http - Web インターフェースログインメソッドを設定します。 all - すべてのアプリケーション(コンソール、Telnet、SSH、Web)ログインメソッドを設定します。 login - 登録済みのメソッドリストを使用して、ユーザーレベルの通常ログインを行うアプリケーションを設定します。 enable - 登録済みのメソッドリストを使用して、通常のユーザーレベルを管理者権限に昇格させるアプリケーションを設定します。 default - デフォルトメソッドリストを使用して、ユーザー認証を行うアプリケーションを設定します。 method_list_name <string 15> - 登録済みのメソッドリストを使用して、ユーザー認証用のアプリケーションを設定します。15 文字以内の半角英数字の文字列を入力して、登録済みのメソッドリストを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Web インターフェースのためにデフォルトメソッドリストを設定するには

```
#config authen application http login default
Command: config authen application http login default

Success.

#
```

3.35.13 show authen application

目的	スイッチの様々なアプリケーションのための認証方法を表示します。
構文	show authen application
説明	本コマンドは、スイッチに現在設定されているスイッチコンフィグレーションアプリケーション(コンソール、Telnet、SSH、Web) に対するすべての認証メソッドリスト（ログイン、管理者特権の有効化など)を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチのすべてのアプリケーションに対するログインと「enable method list」を表示するには

```
#show authen application
Command: show authen application

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

#
```

3.35.14 create authen server_host

目的	認証サーバーを作成します。
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 < 1-255>]
説明	本コマンドは、スイッチに TACACS/ XTACACS/ TACACS+/ RADIUS セキュリティープロトコルに対応したユーザー定義の認証サーバーを作成します。ユーザーが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/ XTACACS/ TACACS+/ RADIUS サーバーに認証パケットを送信します。すると TACACS/XTACACS/TACACS+/RADIUS サーバーはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/XTACACS/TACACS+/RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。 サポート可能なサーバーは最大 16 台です。
パラメーター	server_host <ipaddr> - 追加するサーバーの IP アドレスを入力します。 protocol - サーバーが使用するプロトコルを以下から選択します。 tacacs - サーバーが TACACS プロトコルを使用している場合に選択します。 xtacacs - サーバーが XTACACS プロトコルを使用している場合に選択します。 tacacs+ - サーバーが TACACS+プロトコルを使用している場合に選択します。 radius - サーバーが RADIUS プロトコルを使用している場合に選択します。 port <int 1-65535> - サーバー上で認証プロトコルに使用する 1～65535 の仮想ポート番号を入力します。ポート番号の初期値は、TACACS/XTACACS/TACACS+サーバーの場合は 49、RADIUS サーバーの場合は 1812 と 1813 です。独自の番号を設定してセキュリティーを向上することも可能です。 key <key_string 254> - 設定した TACACS+または RADIUS サーバーのみと共有する認証キーを入力します。最大 254 文字までの半角英数字が使用可能です。認証キーを使用しない場合は、none を選択します。 timeout <int 1-255> - スイッチが、サーバーからの認証リクエストへの応答を待つ時間(秒)を入力します。デフォルト値は、5 秒です。 retransmit <int 1-255> - サーバーからの応答がない場合に、デバイスが認証リクエストを再送する回数を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート番号が 1234、タイムアウトの値が 10 秒、再送回数が 5 である TACACS+認証サーバーを作成するには

```
#create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10 retransmit 5
Command: create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10
retransmit 5

Success.

#
```

3.35.15 config authen server_host

目的	ユーザー定義の認証サーバーを設定します。
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 1-255> >
説明	本コマンドは、スイッチに TACACS/XTACACS/TACACS+/RADIUS セキュリティープロトコルに対応したユーザー定義の認証サーバーを設定します。ユーザーが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/XTACACS/TACACS+/RADIUS サーバーに認証パケットを送信します。すると TACACS/XTACACS/TACACS+/RADIUS サーバーはその要求を認証または拒否し、スイッチに適切なメッセージを返します。 1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/XTACACS/TACACS+/RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバーは最大 16 台です。
パラメーター	server_host <ipaddr> - 変更するサーバーの IP アドレスを入力します。 protocol - サーバーが使用するプロトコルを以下から選択します。 tacacs - サーバーが TACACS プロトコルを使用している場合に選択します。 xtacacs - サーバーが XTACACS プロトコルを使用している場合に選択します。 tacacs+ - サーバーが TACACS+プロトコルを使用している場合に選択します。 radius - サーバーが RADIUS プロトコルを使用している場合に選択します。 port <int 1-65535> - サーバー上で認証プロトコルに使用する 1～65535 の仮想ポート番号を入力します。 ポート番号の初期値は、TACACS/XTACACS/TACACS+サーバーの場合は 49、RADIUS サーバーの場合は 1812 と 1813 です。独自の番号を設定してセキュリティーを向上することも可能です。 key <key_string 254> - 設定した TACACS+または RADIUS サーバーのみと共有する認証キー。最大 254 文字までの半角英数字または「none」を指定します。 timeout <int 1-255> - スイッチが、サーバーからの認証リクエストへの応答を待つ時間(秒)を入力します。デフォルト値は、5 秒です。 retransmit <int 1-255> - サーバーからの応答がない場合に、デバイスが認証リクエストを再送する回数を入力します。本フィールドでは TACACS+プロトコルは操作できません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート番号 4321、タイムアウト値 12 秒、再送回数 4 の TACACS+認証サーバーを設定するには

```
#config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12 retransmit 4
Command: config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12
retransmit 4

Success.

#
```

3.35.16 delete authen server_host

目的	ユーザー定義の認証サーバーを削除します。
構文	delete authen server_host <ipaddr> protocol < tacacs | xtacacs | tacacs+ | radius >
説明	本コマンドは、スイッチに作成済みのユーザー定義認証サーバーホストを削除します。
パラメーター	server_host <ipaddr> - 削除するサーバーの IP アドレスを入力します。 protocol - ユーザーが削除したいサーバーに使用されるプロトコルを 以下から選択します。 tacacs - サーバーが TACACS プロトコルを使用している場合に選択します。 xtacacs - サーバーが XTACACS プロトコルを使用している場合に選択します。 tacacs+ - サーバーが TACACS+プロトコルを使用している場合に選択します。 radius - サーバーが RADIUS プロトコルを使用している場合に選択します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ユーザー定義の TACACS+認証サーバーを削除するには

```
#delete authen server_host 10.1.1.121 protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

#
```

3.35.17 show authen server_host

目的	ユーザー定義した認証サーバー情報を表示します。
構文	show authen server_host
説明	本コマンドは、ユーザー定義した認証サーバー情報を表示します。 次のパラメーターが表示されます。 IP Address - 認証サーバーの IP アドレスです。 Protocol - サーバーが使用するプロトコルです。 結果には TACACS、XTACACS、TACACS+または RADIUS が含まれる可能性が高くなります。 Port - サーバーの仮想ポート番号です。デフォルト値は、49 です。 Timeout - サーバーからの認証リクエストへの応答を待つ時間（秒）です。 Retransmit - 再送信フィールドの値は TACACS サーバーからの応答がない場合に、デバイスが認証リクエストを再送する回数を示します。 本フィールドでは TACACS+プロトコルは操作できません。 Key - 設定した TACACS+サーバーのみと共有する認証キーです。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている認証サーバーを表示するには

```
#show authen server_host
Command: show authen server_host

IP Address    Protocol    Port  Timeout  Retransmit  Key
------------ --------     ----- -------  ----------  ------------
10.53.13.94    TACACS       49     5         2       No Use

Total Entries : 1

#
```

3.35.18 create authen server_group

目的	ユーザー定義の認証サーバーグループを作成します。
構文	create authen server_group <string 15>
説明	本コマンドは、認証サーバーグループを作成します。 認証サーバーグループを作成します。サーバーグループとは、TACACS/XTACACS/TACACS+/RADIUS のサーバーを、ユーザー定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。「config authen server_group」コマンドを使用して、8 個までの認証サーバーをこのグループに追加できます。
パラメーター	<string 15> - 15 文字以内の半角英数字の文字列を入力して、新しく作成するサーバーグループを定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:サーバーグループ「group_1」を作成するには

```
#create authen server_group group_1
Command: create authen server_group group_1

Success.

#
```

3.35.19 config authen server_group

目的	ユーザー定義の認証サーバーグループを設定します。
構文	config authen server_group < tacacs | xtacacs | tacacs+ | radius | <string 15> > < add | delete > server_host <ipaddr> protocol < tacacs | xtacacs | tacacs+ | radius >
説明	本コマンドは、認証サーバーグループを設定します。 認証サーバーグループを作成します。サーバーグループとは、TACACS/XTACACS/TACACS+/RADIUS のサーバーを、ユーザー定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。ユーザーはサーバーグループのタイプをプロトコルによって、または定義済みサーバーグループによって定義できます。 本コマンドを使用して、最大 8 個までの認証サーバーをこのグループに追加することができます。
パラメーター	server_group - スイッチに実装するプロトコルグループを示します。(TACACS/XTACACS/TACACS+/RADIUS)、または「create authen server_group」コマンドで作成したユーザー定義グループによってグループを定義します。 tacacs - スイッチに実装されている TACACS サーバープロトコルを使用します。 TACACS プロトコルを使用するサーバーだけをこのグループに追加することができます。 xtacacs - スイッチに実装されている XTACACS サーバープロトコルを使用します。 XTACACS プロトコルを使用するサーバーだけをこのグループに追加することができます。 tacacs+ - スイッチに実装されている TACACS+サーバープロトコルを使用します。 TACACS+プロトコルを使用するサーバーだけをこのグループに追加することができます。 radius - スイッチに実装されている RADIUS サーバープロトコルを使用します。 RADIUS プロトコルを使用するサーバーだけをこのグループに追加することができます。 <string 15> - 15 文字以内の半角英数字の文字列を入力して、作成済みのサーバーグループを定義します。 本グループはプロトコルにかかわらずサーバーのどんな組み合わせも追加することができます。 add/delete - サーバーグループからサーバーを追加または削除します。 server_host <ipaddr> - 追加または削除するリモートサーバーの IP アドレスを入力します。 protocol - サーバーが使用するプロトコルを入力します。次の 4 つのオプションがあります： tacacs - サーバーが TACACS プロトコルを使用している場合に指定します。 xtacacs - サーバーが XTACACS プロトコルを使用している場合に指定します。 tacacs+ - サーバーが TACACS+プロトコルを使用している場合に指定します。 radius - サーバーが RADIUS プロトコルを使用している場合に指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:サーバーグループ「group_1」に認証ホストを追加するには

```
# config authen server_group group_1 add server_host 10.1.1.121 protocol tacacs+
Command: config authen server_group group_1 add server_host 10.1.1.121 protocol tacacs+

Success.

#
```

3.35.20 delete authen server_group

目的	ユーザー定義の認証サーバーグループを削除します。
構文	delete authen server_group <string 15>
説明	本コマンドは、認証サーバーグループを削除します。
パラメーター	<string 15> - 15 文字以内の半角英数字の文字列を入力して、削除する作成済みのサーバーグループを定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:サーバーグループ「group_1」を削除するには

```
#delete authen server_group group_1
Command: delete authen server_group group_1

Success.

#
```

3.35.21 show authen server_group

目的	スイッチの認証サーバーグループを表示します。
構文	show authen server_group <string 15>
説明	本コマンドは、スイッチに現在設定されている認証サーバーグループを表示します。 本コマンドは、次のフィールドを表示します。 Group Name - 実装されているグループおよびユーザー定義グループを含むスイッチに現在設定されているサーバーグループの名前です。 IP Address - サーバーの IP アドレスです。 Protocol - サーバーが使用する認証プロトコルです。
パラメーター	<string 15> - 15 文字以内の半角英数字の文字列を入力して、表示する作成済みのサーバーグループを定義します。 本コマンドを<string>パラメーターなしで入力すると、スイッチのすべての認証サーバーグループを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている認証サーバーグループを表示するには

```
#show authen server_group
Command: show authen server_group

Group Name    IP Address                          Protocol
-----------  ------------------------------    ------------
radius       ----------------------------------------------
tacacs       ----------------------------------------------
tacacs+      ----------------------------------------------
xtacacs      ----------------------------------------------

Total Entries : 4

#
```

3.35.22 config authen parameter response_timeout

目的	スイッチが、タイムアウトの前にユーザーからの認証のレスポンスを待つ時間を設定します。
構文	config authen parameter response_timeout <int 0-255>
説明	ユーザーからの認証のレスポンスに対するスイッチの待ち時間を指定します。
パラメーター	response_timeout <int 0-255> - コンソールまたは telnet からユーザーの認証レスポンスに対するスイッチの待ち時間を指定します。0 はタイムアウトにならないことを意味します。デフォルト値は、30 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:レスポンスのタイムアウトを 60 秒に設定するには

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

Success.

#
```

3.35.23 config authen parameter attempt

目的	スイッチが認証の試みを許容する最大回数を設定します。
構文	config authen parameter attempt <int 1-255>
説明	本コマンドは、スイッチが認証の試みを許容する最大回数を設定します。指定回数の認証に失敗すると、そのユーザーはスイッチへのアクセスを拒否され、さらに認証を試みることができなくなります。コンソールの場合は、再度認証を行うために 60 秒待つ必要があります。Telnet の場合は、スイッチから切断されます。
パラメーター	parameter attempt <int 1-255> - ロックされる前にスイッチによる認証のために試みることができる最大回数を設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:認証試みの最大数に 5 を設定するには

```
#config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

#
```

3.35.24 show authen parameter

目的	スイッチに現在設定されている認証パラメーターを表示します。
構文	show authen parameter
説明	本コマンドは、レスポンスタイムアウトおよびユーザー認証を試みる回数を含むスイッチに設定されている認証パラメーターを表示します。 本コマンドは、次のフィールドを表示します。 Response timeout -コンソールまたは telnet からログインを試みるユーザーの認証レスポンスに対するスイッチの待ち時間に割り当てられる設定時間 User attempts - ロックされる前にユーザーが認証を試みることができる最大回数を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定している認証パラメーターを表示するには

```
#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 5

#
```

3.35.25 enable admin

目的	ユーザーレベルから管理者レベルに権限を昇格します。
構文	enable admin
説明	本コマンドは、通常のユーザーレベルとしてスイッチにログインした後、管理者レベルに変更する場合に使用します。スイッチにログインした後のユーザーにはユーザーレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本コマンドを入力し、認証用パスワードを入力します。本機能における認証方法には、TACACS/XTACACS/TACACS+/RADIUS、ユーザー定義のサーバーグループ、local enable（スイッチのローカルアカウント）または、認証なし（none）があります。XTACACS、TACACS および RADIUS は、local enable（スイッチのローカルアカウント）をサポートしていないため、ユーザーはサーバーに特別なアカウントとして、 ユーザー名「enable」および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「disable」（無効）である場合には実行できません。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチの管理者権限を有効にするには

```
#enable admin
Password: ******

#
```

3.35.26 config admin local_enable

目的	管理者レベルの権限のためのローカルイネーブルパスワードを設定します。
構文	config admin local_enable
説明	本コマンドは、「enable admin」コマンドのローカルで有効なパスワードを設定します。「local_enable」方式を選択してユーザーレベルの権限を管理者レベルの権限に上げると、このセクションに記載されるスイッチにローカルに登録したパスワードを入力するように要求されます。
パラメーター	〈password 15〉 - 本コマンドを入力した後、ユーザーは元のパスワード、次に新しいパスワード、さらに確認のために再び新しいパスワードを入力します。パスワードは 15 文字以内の半角英数字で指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:「local_enable」認証方法のためのパスワードを設定するには

```
#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.

#
```

3.36 MAC ベースアクセス制御コマンド

3.36.1 enable mac_based_access_control

目的	MAC ベースアクセス制御を有効にします。
構文	enable mac_based_access_control
説明	本コマンドは、スイッチで MAC ベースアクセス制御を有効にします。デフォルトでは有効化されていません。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチに MAC ベースアクセス制御をグローバルで有効にするには

```
# enable mac_based_access_control
Command: enable mac_based_access_control

Success.

#
```

注意事項

APLGM152GT では、MAC ベースアクセス制御と組み合わせたローミング機能をサポートします。認証されたホストが同一装置内の別の認証ポートへローミングする場合、新しいポートで認証状態が引き継がれます。

3.36.2 disable mac_based_access_control

目的	MAC ベースアクセス制御を無効にします。
構文	disable mac_based_access_control
説明	本コマンドは、スイッチの MAC ベースアクセス制御を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの MAC ベースアクセス制御をグローバルで無効にするには

```
# disable mac_based_access_control
Command: disable mac_based_access_control

Success.

#
```

3.36.3 config mac_based_access_control password

目的	MAC ベースアクセス制御のパスワードを設定します。
構文	config mac_based_access_control password <passwd 16>
説明	本コマンドは、RADIUS サーバー経由の認証に使用されるパスワードを設定します。
パラメーター	<password 16> - RADIUS モードでは、スイッチは RADIUS サーバーとの通信にパスワードを使用します。16 文字以内で入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御のパスワードを設定するには

```
#config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

#
```

3.36.4 config mac_based_access_control method

目的	MAC ベースアクセス制御の認証方法を設定します。
構文	config mac_based_access_control method < local | radius >
説明	本コマンドは、認証方法を local または radius 経由に設定します。
パラメーター	local - ローカルデータベースを経由した認証を指定します。 radius - RADIUS サーバーを経由した認証を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御メソッドを設定するには

```
#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

#
```

3.36.5 config mac_based_access_control ports

目的	MAC ベースアクセス制御のパラメーターを設定します。
構文	config mac_based_access_control ports < <portlist> | all > [state < enable | disable > aging_time < infinite | <min 1-1440> > | hold_time < infinite | <sec 1-300> > | max_users [<value 1-1000>]]
説明	本コマンドは、MAC ベースアクセス制御設定のパラメーターを設定します。MAC アドレス認証機能が有効なポートでは、ユーザーのトラフィックは認証が成功しなければ転送されません。
パラメーター	ports - MAC アドレス認証機能を有効または無効にするポート範囲を設定します。 state - MAC アドレス認証機能を有効または無効にします。 aging_time - 認証ホストが認証状態を保つ時間です。 aging_time がタイムアウトになると、ホストは未認証状態に戻ります。デフォルト値は、1440 分です。 hold_time - ホストが認証通過に失敗した場合に認証を開始できない時間です。 ユーザーがエントリー状態を手動でクリアしない限り、次の認証はこの時間内に開始されません。デフォルト値は、300 秒です。 max_users - ポートあたりのユーザー数を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御のポートの状態を設定するには

```
#config mac_based_access_control ports 1-8 state enable
Command: config mac_based_access_control ports 1-8 state enable

Success.

#
```

3.36.6 config mac_based_access_control log state

目的	MAC ベースアクセス制御のログ出力機能を設定します。
構文	config mac_based_access_control log state [enable | disable]
説明	本コマンドは、MAC ベースアクセス制御のログ出力機能を設定します。 有効の場合、MAC ベースアクセス制御による認証結果をログ出力します。 デフォルト設定は、「enable」(有効)です。
パラメーター	enable - MAC ベースアクセス制御のログ出力機能を有効にします。 disable - MAC ベースアクセス制御のログ出力機能を無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御のログ出力を無効にするには

```
#config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable


Success.


#
```

3.36.7 config mac_based_access_control trap state

目的	MAC ベースアクセス制御のトラップ送出機能を設定します。
構文	config mac_based_access_control trap state [enable | disable]
説明	本コマンドは、MAC ベースアクセス制御のトラップ送出機能を設定します。 有効の場合、MAC ベースアクセス制御による認証結果をトラップ送出します。 デフォルト設定は、「enable」(有効)です。
パラメーター	enable - MAC ベースアクセス制御のトラップ送出機能を有効にします。 disable - MAC ベースアクセス制御のトラップ送出機能を無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御のトラップ送出を無効にするには

```
#config mac_based_access_control trap state disable
Command: config mac_based_access_control trap state disable


Success.


#
```

3.36.8 config mac_based_access_control authorization attributes

目的	RADIUS サーバー、ローカルデータベースによる認証属性の割り当てを設定します。
構文	config mac_based_access_control authorization attributes [radius [enable | disable] | local [enable | disable]]
説明	本コマンドは、MAC ベースアクセス制御において、RADIUS サーバー・ローカルデータベースで定義された認証属性の割り当てを有効または無効に設定します。 有効の場合、定義されたダイナミック VLAN の割り当てなどが許可されます。
パラメーター	radius - RADIUS サーバーにより認証属性の割り当てを有効または無効にします。 デフォルト設定は、「enable」(有効)です。 local - ローカルデータベースにより認証属性の割り当てを有効または無効にします。デフォルト設定は、「enable」(有効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:RADIUS サーバーからの認証属性を有効にするには

```
# config mac_based_access_control authorization attributes radius enable
Command: config mac_based_access_control authorization attributes radius enable

Success.

#
```

注意事項

認証属性を有効とするためには、認証属性のグローバル設定が「enable」(有効)である必要があります。この設定は「enable authorization network」コマンドで行います。

ダイナミック VLAN により動的 VLAN を割り当てる場合、ローミングするポートの VLAN ID が異なるため、ポートの Ingres checking 設定を無効にする必要があります。
この設定は「config gvrp all ingress_checking disable」コマンドで行います。

3.36.9 clear mac_based_access_control auth_mac

目的	ユーザーの認証状態をリセットします。再認証は、再度ユーザートラフィックを受信した後に開始します。
構文	clear mac_based_access_control auth_mac < ports < all | <portlist> > | mac_addr <macaddr> >
説明	本コマンドは、ユーザー（またはポート)の認証状態をクリアします。ポート(またはユーザー）は未認証状態に戻ります。ポート(またはユーザー)に関連しているすべてのタイマーがリセットされます。
パラメーター	ports - MAC を削除するポート範囲を指定します。 <macaddr> - この MAC アドレスを持つホストを削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御により処理した MAC をクリアするには

```
#clear mac_based_access_control auth_mac ports all
Command: clear mac_based_access_control auth_mac ports all

Success.
```

3.36.10 create mac_based_access_control_local mac

目的	ローカルデータベースエントリーを作成します。
構文	create mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
説明	本コマンドは、ローカルデータベースエントリーを作成します。
パラメーター	mac - ローカルモードでアクセスが許可される MAC アドレスです。 vlan - MAC アドレスが認証されると、ポートはこの VLAN に割り当てられます。 vlanid - MAC アドレスが認証されると、ポートはこの VLAN に割り当てられます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御ローカルエントリーを作成するには

```
#create mac_based_access_control_local mac 00-40-66-00-00-01 vlan default
Command: create mac_based_access_control_local mac 00-40-66-00-00-01 vlan default

Success.

#
```

3.36.11 config mac_based_access_control_local mac

目的	MAC ベースアクセス制御ローカルデータベースエントリーを設定します。
構文	config mac_based_access_control_local mac <macaddr> < vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan >
説明	本コマンドは、「mac_based_access_control_local」コマンドを使用して、作成済みの MAC ベースアクセス制御ローカルデータベースエントリーを設定します。
パラメーター	mac - 認証ホストの MAC アドレスを指定します。 vlan - VLAN 名によってターゲット VLAN を指定します。このホストが認証されると、この VLAN に割り当てられます。 vlanid - VLAN ID によってターゲット VLAN を指定します。ホストが認証されると、ターゲット VLAN が存在する場合、この VLAN に割り当てられます。 clear_vlan - クリア対象の VLAN を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御ローカルデータベースエントリー 00-40-66-00-00-01 のターゲット VLAN「default」を設定するには

```
# config mac_based_access_control_local mac 00-40-66-00-00-01 vlan default
Command: config mac_based_access_control_local mac 00-40-66-00-00-01 vlan default

Success.

#
```

3.36.12 delete mac_based_access_control_local

目的	ローカルデータベースエントリーを削除します。
構文	delete mac_based_access_control_local <mac <macaddr> | <vlan <vlan_name 32> | vlanid <vlanid 1-4094>>
説明	本コマンドは、ローカルデータベースエントリーを削除します。
パラメーター	mac - この MAC アドレスによってデータベースを削除します。 vlan - この VLAN 名のデータベースを削除します。 vlanid - この VLAN ID のデータベースを削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC アドレスによってローカルの MAC ベースアクセス制御を削除するには

```
#delete mac_based_access_control_local mac 00-40-66-00-00-01
Command: delete mac_based_access_control_local mac 00-40-66-00-00-01

Success.

#
```

3.36.13 show mac_based_access_control

目的	MAC ベースアクセス制御の設定を表示します。
構文	show mac_based_access_control [ports [<portlist | all>]]
説明	本コマンドは、MAC ベースアクセス制御の設定を表示します。
パラメーター	ports - MAC ベースアクセス制御のポートの状態を表示します。 all - 全てのポートを表示させる場合に指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御を表示するには

```
#show mac_based_access_control
Command: show mac_based_access_control


MAC-based Access Control
-----------------------------------
State                  : Enabled
Method                 : Local
MAC Format Case        : Uppercase
MAC Format Delimiter   : None
Password               : default
Password Type          : Manual String
Max Max User           : 1000
RADIUS Authorization   : Enabled
Local Authorization    : Enabled
Trap State             : Enabled
Log State              : Enabled


#
```

使用例:MAC ベースアクセス制御ポートを表示するには

```
#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4

Port    State     Aging Time   Hold Time   Max User
                    (min)        (sec)
-----  --------   ----------   ---------   --------
1      Enabled    1440         300         128
2      Enabled    1440         300         128
3      Enabled    1440         300         128
4      Enabled    1440         300         128

#
```

3.36.14 show mac_based_access_control_local

目的	MAC ベースアクセス制御ローカルデータベースを表示します。
構文	show mac_based_access_control_local [< mac <macaddr> | < vlan <vlan_name 32> | vlanid <vlanid 1-4094> >]
説明	本コマンドは、MAC ベースアクセス制御ローカルデータベースを表示します。
パラメーター	mac - 指定した MAC アドレスに該当するローカルデータベースを表示します。 vlan - 指定した VLAN 名に該当するローカルデータベースを表示します。 vlanid - 指定した VLAN ID に該当するローカルデータベースを表示します。 パラメーターを指定しない場合、すべてのローカルデータベースを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御ローカルデータベースを表示するには

```
#show mac_based_access_control_local
Command: show mac_based_access_control_local

  MAC Address             VLAN Name                    VID
-----------------    ----------------------          ------
 00-40-66-00-00-01        default                     1
 00-40-66-00-00-02        VLAN123                     123
 00-40-66-00-00-03        VLAN123                     123
 00-40-66-00-00-04        default                     1

Total Entries: 4

#
```

使用例:MAC アドレスから MAC ベースアクセス制御ローカルデータベースを表示するには

```
#show mac_based_access_control_local mac 00-40-66-00-00-01
Command: show mac_based_access_control_local mac 00-40-66-00-00-01

MAC Address           VLAN Name                      VID
----------------    ----------------------          ------
00-40-66-00-00-01    default                         1

Total Entries: 1

#
```

3.36.15 show mac_based_access_control auth_mac

目的	MAC ベースアクセス制御の認証状態を表示します。
構文	show mac_based_access_control auth_mac [ports <portlist>]
説明	本コマンドは、MAC ベースアクセス制御の認証状態を表示します。
パラメーター	ports - 指定したポート番号の認証ステータスを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御の状態を表示するには

```
#show mac_based_access_control auth_mac
Command: show mac_based_access_control auth_mac

 (P): Port-based

Port MAC Address          State          VID  Aging Time/
                                              Hold Time
---- ------------------- -------------- ---- ------------
1    00-40-66-00-00-01    Blocked        -    276
31   00-40-66-00-00-02    Authenticated  1    86291

Total Authenticating Hosts  : 0
Total Authenticated Hosts   : 1
Total Blocked Hosts         : 1

#
```

3.36.16 config mac_based_access_control max_users

目的	認証クライアントの最大数を設定します。
構文	config mac_based_access_control max_users [<value 1-1000>]
説明	本コマンドは、装置全体の収容可能な端末数を指定します。
パラメーター	<value 1-1000> - 装置全体の収容可能な端末数を指定します。 デフォルト値は、1000 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御の最大ユーザー数を 100 に設定するには

```
#config mac_based_access_control max_users 100
Command: config mac_based_access_control max_users 100

Success.

#
```

注意事項

MAC 認証の認証最大数を超えた場合、show fdb コマンドの Type 情報に BlockByMBA と表示されます。
BlockByMBA：MAC 認証許可されない場合に FDB 表示されます。
UnBlockByMBA： MAC 認証許可された場合に FDB 表示されます。

3.36.17 enable authorization network

目的	認証機能における認証属性の割り当てをグローバルで有効にします。
構文	enable authorization network
説明	本コマンドは、認証属性の割り当てを有効にします。有効の場合、認証属性(例： VLAN)が RADIUS サーバーまたはローカルデータベースによって割り当てられます。デフォルト設定は、「disable」(無効)です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:グローバル認証の状態を有効にするには

```
#enable authorization network
Command: enable authorization network

Success.

#
```

3.36.18 disable authorization network

目的	認証機能における認証属性の割り当てを無効にします。
構文	disable authorization network
説明	本コマンドは、認証属性の割り当てを無効にします。無効の場合、RADUIS サーバーまたはローカルデータベースによって割り当てられた認証済み属性（例：VLAN）は、個々のモジュール設定が有効になっていても無視されます。デフォルト設定は、「disable」（無効）です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:グローバル認証の状態を無効にするには

```
#disable authorization network
Command: disable authorization network

Success.

#
```

3.36.19 show authorization

目的	認証ステータスを表示します。
構文	show authorization
説明	認証ステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:認証ステータスを表示します。

```
#show authorization
Command: show authorization

Authorization for Attributes : Enabled

#
```

3.36.20 config mac_based_access_control mac_format

目的	MAC ベースアクセス制御の MAC アドレスフォーマットを設定します。
構文	config mac_based_access_control mac_format < case [lowercase | uppercase] | delimiter [hyphen | none] >
説明	本コマンドは、RADIUS サーバーを経由した MAC ベース認証時の MAC アドレスフォーマットを設定します。
パラメーター	case - MAC アドレスの大文字/小文字を選択するときに設定します。 lowercase - MAC アドレスを小文字に限定するときに設定します。 uppercase - MAC アドレスを大文字に限定するときに設定します。 delimiter - MAC アドレスの区切り文字を使用するときに設定します。 hyphen - MAC アドレスの区切り文字としてハイフンを使用するときに設定します。 none - MAC アドレスの区切り文字を使用しないときに設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: MAC アドレスフォーマットを大文字/区切り文字なしに設定するには

```
# config mac_based_access_control mac_format case uppercase delimiter none
Command: config mac_based_access_control mac_format case uppercase delimiter none

Success.

#
```

3.36.21 config mac_based_access_control password_type

目的	MAC ベースアクセス制御のパスワードタイプを設定します。
構文	config mac_based_access_control password_type < manual_string | client_mac_address >
説明	本コマンドは、RADIUS サーバー認証時のパスワードタイプを設定します。
パラメーター	manual_string - RADIUS認証時に装置に設定したパスワードを使用します。 client_mac_address - RADIUS認証時にクライアントのMACアドレスをパスワードとして使用します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 認証パスワードタイプを入力文字列に設定するには

```
# config mac_based_access_control password_type manual_string
Command: config mac_based_access_control password_type manual_string

Success.

#
```

3.37 マルチプル認証コマンド

3.37.1 config authentication auth_mode

目的	ポートに設定された認証方式の認証モードを設定します。
構文	config authentication auth_mode <port_based | host_based>
説明	本コマンドは、設定された MAC/802.1X/WEB 認証の認証モードを設定します。
パラメーター	auth_mode - 認証モードを指定します。 port_based -1 つのホストが認証された場合、同じポート上の全てのホストがアクセスを許可されます。認証に失敗した場合には、そのポートは次の認証の試みを継続します。 host_based - 全てのユーザーは個別に認証されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 全ポートの認証モードをポートベースに設定するには

```
#config authentication auth_mode port_based
Command: config authentication auth_mode port_based

Success.

#
```

3.37.2 config authentication server failover

目的	MAC/802.1X/WEB 認証の failover 機能を有効または無効に設定します。
構文	config authentication server failover < enable [mode [permit [vlanid <vlanid 1-4094>] | local]] | disable >
説明	本コマンドは、MAC/802.1X/WEB 認証において認証サーバーからの認証応答がない場合、認証方式をローカルデータベースの認証もしくは強制認証に切り替える failover 機能を設定します。認証サーバーから認証失敗の応答がある場合には faiiover 機能による切り替わりは行われません。
パラメーター	enable - 認証サーバーから応答がない場合に failover 機能を使用します。 mode - failover の動作を指定します。省略した場合、failover の動作としてローカルデータベースの認証が使用されます(mode local)。 permit - failover の動作として強制的に認証許可を行います。 vlanid <vlanid 1-4094> - 認証許可後に所属する vlanid を設定します。 local - failover の動作としてローカルデータベースの認証を行います。 disable - failover 機能を無効にします。 デフォルト設定は、「disable」(無効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降 1.03.00 以降(強制認証オプション)

注意事項

802.1X の強制認証は、MD5 のみサポートします。

使用例: failover 機能を有効にするには

```
#config authentication server failover enable
Command: config authentication server failover enable

Success.

#
```

3.37.3 show authentication

目的	failover 機能の設定を表示します。
構文	show authentication
説明	本コマンドは、failover 機能の設定を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: failover 機能の設定を表示するには

```
#show authentication
Command: show authentication

Authentication Server Failover: Enabled.
Failover Mode                 : Local

#
```

3.37.4 show authentication ports

目的	ポートに設定された認証方式の認証モードを表示します。
構文	show authentication ports [<portlist>]
説明	本コマンドは、ポートに設定された認証方式の認証モードを表示します。
パラメーター	<portlist> - 指定したポートの認証モードを表示します。ポートの指定が省略された場合には、全ポートの認証モードを表示します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1 から 5 の認証モードを表示するには

```
#show authentication ports 1-5
Command: show authentication ports 1-5

 Port Authorized Mode
 ---- -----------------
 1    Port_based
 2    Port_based
 3    Port_based
 4    Port_based
 5    Port_based
#
```

3.38 SSH コマンド

リモート PC（SSH クライアント）とスイッチ（SSH サーバー）間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

(1) 「create account admin」コマンドで管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザーアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。

(2) 「config ssh user authmode」コマンドを使用して、ユーザーアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザーの認証方法を指定します。この認証方法には、「password」、「publickey」、「hostbased」の 3 つがあります。

(3) SSH クライアントとサーバー間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。

(4) 「enable ssh」コマンドで、SSH を有効にします。

これらの手順が完了後、安全な帯域内の通信を使用してリモート PC からスイッチの管理を行うことができます。

3.38.1 enable ssh

目的	SSH を有効にします。
構文	enable ssh
説明	本コマンドは、スイッチの SSH を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：SSH を有効にするには

```
#enable ssh
Command: enable ssh

Success.

#
```

3.38.2 disable ssh

目的	SSH を無効にします。
構文	disable ssh
説明	本コマンドは、スイッチの SSH を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：SSH を無効にするには

```
# disable ssh
Command: disable ssh

Success.

#
```

3.38.3 config ssh authmode

目的	SSH 認証モードの設定を行います。
構文	config ssh authmode < password | publickey | hostbased > < enable | disable >
説明	本コマンドは、ユーザーがスイッチにアクセスするための SSH 認証モードを設定します。
パラメーター	password - 本パラメーターは、管理者がスイッチにおける認証にローカルに設定したパスワードを使用したいときに選択します。 publickey - 本パラメーターは、管理者が認証に SSH サーバーで設定した公開鍵のコンフィグレーションセットを使用したいときに選択します。 hostbased - 本パラメーターは、管理者が認証にホストコンピュータを使用するときに選択します。ホストコンピュータには SSH プログラムが起動している必要があります。 <enable | disable> - スイッチに指定された SSH 認証を「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:パスワードによる SSH 認証モードを有効にするには

```
#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

#
```

3.38.4 show ssh authmode

目的	SSH 認証モードの設定を表示します。
構文	show ssh authmode
説明	本コマンドは、スイッチに設定された SSH 設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに設定された認証モードを表示するには

```
#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method
-----------------------------------------------
Password   : Enabled
Publickey  : Enabled
Hostbased  : Enabled

#
```

3.38.5 config ssh server

目的	SSH サーバーを設定します。
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>]
説明	本コマンドは、SSH サーバーを設定します。
パラメーター	maxsession <int 1-8> - スイッチに同時に接続できるユーザー数を設定します。デフォルト値は、8 です。 contimeout <sec 120-600> - 接続のタイムアウト時間を指定します。120～600 秒の範囲で設定します。デフォルト値は、120 秒です。 authfail <int 2-20> - ユーザーが SSH 認証を使用してログインを試みることができる上限回数を管理者が指定します。指定した上限回数を超えるとスイッチは接続を切り、ユーザーは再度スイッチに再接続し、ログインをし直す必要があります。 rekey <10min | 30min | 60min | never> - スイッチが SSH 暗号を変更する期間を設定します。 port <tcp_port_number 1-65535> - 端末とサーバー間の SSH 通信に使用する TCP ポート番号を指定します。ポート番号のデフォルト値は、22 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：SSH サーバーを設定するには

```
#config ssh server maxsession 2 contimeout 300 authfail 2
Command: config ssh server maxsession 2 contimeout 300 authfail 2

Success.

#
```

3.38.6 show ssh server

目的	SSH サーバーの設定を表示します。
構文	show ssh server
説明	本コマンドは、SSH サーバーの設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例：SSH サーバーを表示するには

```
#show ssh server
Command: show ssh server


The SSH Server Configuration
Maximum Session              : 8
Connection Timeout           : 120
Authentication Fail Attempts : 2
Rekey Timeout                : Never
TCP Port Number              : 22


#
```

3.38.7 config ssh user

目的	SSH ユーザーを設定します。
構文	config ssh user <username 15> authmode < hostbased < hostname <domain_name 32> > < hostname_IP <domain_name 32> <ipaddr> > | password | publickey >
説明	本コマンドは、SSH ユーザー認証方法を設定します。
パラメーター	<username 15> - SSH ユーザーを識別するユーザー名を 15 文字までの半角英数字で指定します。 authmode - スイッチへのログインを希望する SSH ユーザーの認証モードを指定します。管理者は以下のパラメーターを選択することができます。 hostbased - 認証でリモート SSH サーバーを使用する場合に選択します。本パラメーターを選択すると、ユーザー識別のために以下の入力が必要になります。 hostname <domain_name 32> - リモートの SSH ユーザーを識別する 32 文字以内の半角英数字の文字列を入力します。 hostname_IP <domain_name 32> <ipaddr> - SSH ユーザーのホスト名と対応する IP アドレスを入力します。 password - 管理者定義のパスワードを使用してユーザー認証を行う場合に選択します。 publickey - SSH サーバー上の公開鍵を使用して認証を行う場合に選択します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SSHユーザーを設定するには

```
# config ssh user APS authmode password
Command: config ssh user APS authmode password

Success.

#
```

3.38.8 show ssh user authmode

目的	SSHユーザーの設定を表示します。
構文	show ssh user authmode
説明	本コマンドは、SSHユーザーの設定を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:SSHユーザーを表示するには

```
#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
Username    AuthMode   HostName                  HostIP
----------  ---------  ------------------------  ---------------
APS         Password

Total Entries : 1

#
```

注意事項

SSHユーザーを設定するには、管理者はスイッチにユーザーアカウントを作成する必要があります。 ユーザーアカウント設定に関する情報に ついては、本マニュアルの「create account」を参照してください。

3.38.9 config ssh algorithm

目的	SSH 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 >
説明	本コマンドは、認証の暗号化に使用される SSH アルゴリズムのタイプを設定します。
パラメーター	3DES - Triple_Data Encryption Standard 暗号化アルゴリズム AES128 - Advanced Encryption Standard AES128 暗号化アルゴリズム AES192 - Advanced Encryption Standard AES192 暗号化アルゴリズム AES256 - Advanced Encryption Standard AES256 暗号化アルゴリズム arcfour - Arcfour 暗号化アルゴリズム blowfish - Blowfish 暗号化アルゴリズム cast128 - Cast128 暗号化アルゴリズム twofish128 - Twofish 128 暗号化アルゴリズム twofish192 - Twofish192 暗号化アルゴリズム MD5 - MD5 Message Digest 暗号化アルゴリズム SHA1 - Secure Hash Algorithm 暗号化 RSA - RSA 暗号化アルゴリズム DSA - Digital Signature Algorithm 暗号化 <enable | disable> - スイッチに本コマンドで入力した各アルゴリズムを「enable」(有効)または「disable」(無効)に設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：SSH アルゴリズムを設定するには

```
# config ssh algorithm blowfish enable
Command: config ssh algorithm blowfish enable

Success.

#
```

3.38.10 show ssh algorithm

目的	SSH アルゴリズムの設定を表示します。
構文	show ssh algorithm
説明	本コマンドは、SSH アルゴリズムの設定ステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例：スイッチに現在設定されている SSH アルゴリズムを表示するには

```
#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
----------------------------
MD5         : Enabled
SHA1        : Enabled

Public Key Algorithm
----------------------------
RSA         : Enabled

CTRL+C ESC q QUIT SPACE n Next Page ENTER Next Entry a All
```

3.39 SSL コマンド

Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティー機能です。

このセキュリティー機能は、認証セッションに使用する厳密な暗号パラメーター、特定の暗号化アルゴリズムおよびキー長を決定する、暗号スイートと呼ばれるセキュリティー文字列により実現しています。SSL は、以下の 3 つの段階で構成されます。

(1) 鍵交換： 暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DHE ： DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。

(2) 暗号化： 暗号スイートの次の段階は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。

- ストリーム暗号 - スイッチは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。 これらの鍵はメッセージの暗号化に使用され、最適な使用のためにはクライアントとホスト間で一致させる必要があります。
- CBC ブロック暗号 - CBC（Cipher Block Chaining ： 暗号ブロック連鎖）とは、前に暗号化したブロックの暗号文を使用して現在のブロックの暗号化を行う方法です。 本スイッチは、DES（Data Encryption Standard）で定義する 3 DES_EDE 暗号化コードと AES(Advanced Encryption Standard)をサポートし、暗号文を生成します。

(3) ハッシュアルゴリズム： 暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。 このメッセージ認証コードは送信されたメッセージで暗号化され、整合性を提供し、 再送攻撃を防止します。 本スイッチは、MD5(Message Digest 5)と SHA(Secure Hash Algorithm)の 2 種類のハッシュアルゴリズムをサポートします。SHA は、SHA-1 および SHA-2 をサポートしています。

これら 3 つのパラメーターは、スイッチ上での 4 つの選択肢として独自に組み合わされ、サーバーとホスト間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティーレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバーを使用してスイッチにダウンロードできます。本スイッチは、SSLv3 および TLSv1.0～1.2 をサポートしています。 SSL の他のバージョンは本スイッチとは互換性がないおそれがあり、クライアントからホストへの認証やメッセージ転送時に問題が発生する場合があります。

3.39.1 enable ssl

目的	スイッチの SSL 機能を有効にします。
構文	enable ssl [version < all | < tls1.0 | tls1.1 | tls1.2 >> | ciphersuite < RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_with_AES_128_CBC_SHA | RSA_with_AES_256_CBC_SHA | RSA_with_AES_128_CBC_SHA256 | RSA_with_AES_256_CBC_SHA256 | DHE_DSS_with_AES_256_CBC_SHA | DHE_RSA_with_AES_256_CBC_SHA >]
説明	本コマンドは、スイッチの SSL 機能を有効にします。 パラメーターなしで本コマンドを入力した場合、スイッチの SSL 機能のグローバル設定が有効になります。各 TLS バージョンや暗号スイートは変更されません。 パラメーターありで入力した場合は、指定した TLS バージョンや暗号スイートが有効になります。SSL 機能のグローバル設定は変更されません。
パラメーター	version - TLS バージョンを指定する場合に使用するオプションです。 ciphersuite - 暗号スイートを指定する場合に使用するオプションです。デフォルト設定では、全ての TLS バージョン及び暗号スイートが有効になっていますが、SSL 機能のグローバル設定は無効です。SSL 機能を使用する場合、オプションなしで本コマンドを入力して SSL 機能のグローバル設定を有効にし、使用しない TLS バージョン及び暗号スイートは disable ssl コマンドにより無効にしてください。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降 (version オプションは 1.03.00 以降)

使用例:すべての暗号スイートに対し、スイッチの SSL 機能を有効にするには

```
#enable ssl
Command: enable ssl

Note: Web will be disabled if SSL is enabled.
Success.

#
```

注意事項

スイッチの SSL 機能を有効にするとすべての暗号スイートが有効になります。特定の暗号スイートを使用するには、適切な暗号スイートと共に無効 SSL コマンドを使用して他の暗号スイートを無効にする必要があります。

スイッチの SSL 機能を有効にすると、スイッチは Web マネージャー用のポート(ポート 80)を無効にします。Web マネージャーにログインするためには、URL のエントリーは「https://」で始まる必要があります(例： https://10.10.10.10)。

3.39.2 disable ssl

目的	スイッチの SSL 機能を無効にします。
構文	disable ssl [version < all | < tls1.0 | tls1.1 | tls1.2 >> | ciphersuite < RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_with_AES_128_CBC_SHA | RSA_with_AES_256_CBC_SHA | RSA_with_AES_128_CBC_SHA256 | RSA_with_AES_256_CBC_SHA256 | DHE_DSS_with_AES_256_CBC_SHA | DHE_RSA_with_AES_256_CBC_SHA >]
説明	本コマンドは、スイッチの SSL 機能を無効にします。 パラメーターなしで本コマンドを入力した場合、スイッチの SSL 機能のグローバル設定が無効になります。各 TLS バージョンや暗号スイートは変更されません。 パラメーターありで入力した場合は、指定した TLS バージョンや暗号スイートが無効になります。SSL 機能のグローバル設定は変更されません。
パラメーター	version - TLS バージョンを指定する場合に使用するオプションです。 ciphersuite - 暗号スイートを指定する場合に使用するオプションです。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降 (version オプションは 1.03.00 以降)

使用例:スイッチの SSL ステータスを無効にするには

```
#disable ssl
Command: disable ssl

Success.

#
```

使用例:暗号化スイート RSA_with_RC4_128_MD5 のみを無効にするには

```
#disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

#
```

3.39.3 config ssl cachetimeout timeout

目的	SSL キャッシュタイムアウトを設定します。
構文	config ssl cachetimeout timeout <value 60-86400>
説明	本コマンドは、SSL 機能を使用してクライアントとホスト間の新しい鍵交換の間隔を設定します。クライアントとホストが鍵交換をすると常に新しい SSL セッションが確立します。この値を長くすると SSL セッションによる特定のホストとの再接続には主鍵が再利用されます。
パラメーター	timeout <value 60-86400> - 60～86400 の範囲でタイムアウト時間を入力して設定し、SSL モジュールが新しく SSL ネゴシエーションを必要となる前に SSL 鍵 ID が有効性を維持する合計時間を指定します。キャッシュタイムアウトのデフォルト値は、600 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SSL キャッシュタイムアウトを 7200 秒に設定するには

```
#config ssl cachetimeout timeout 7200
Command: config ssl cachetimeout timeout 7200

Success.

#
```

3.39.4 show ssl cachetimeout

目的	SSL キャッシュタイムアウトを表示します。
構文	show ssl cachetimeout
説明	本コマンドは、スイッチに現在設定されている SSL キャッシュタイムアウトを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに設定されている SSL キャッシュタイムアウトを表示するには

```
#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

#
```

3.39.5 show ssl

目的	スイッチ上の SSL ステータスと証明ファイルのステータスを表示します。
構文	show ssl
説明	本コマンドは、スイッチ上の SSL ステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチ上の SSL ステータスを表示するには

```
#show ssl
Command: show ssl

 SSL Status                                 Enabled
 TLS 1.0                                    Enabled
 TLS 1.1                                    Enabled
 TLS 1.2                                    Enabled

 Cipher Suites:
 RSA_WITH_RC4_128_MD5                0x0004  Enabled
 RSA_WITH_3DES_EDE_CBC_SHA           0x000A  Enabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA       0x0013  Enabled
 RSA_WITH_AES_128_CBC_SHA            0x002F  Enabled
 RSA_WITH_AES_256_CBC_SHA            0x0035  Enabled
 RSA_WITH_AES_128_CBC_SHA256         0x003C  Enabled
 RSA_WITH_AES_256_CBC_SHA256         0x003D  Enabled
 DHE_DSS_WITH_AES_256_CBC_SHA        0x0038  Enabled
 DHE_RSA_WITH_AES_256_CBC_SHA        0x0039  Enabled

#
```

3.39.6 show ssl certificate

目的	スイッチ上の SSL 証明ファイルのステータスを表示します。
構文	show ssl certificate
説明	本コマンドは、スイッチ上の SSL 証明書ファイルの情報を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチ上の証明書ファイル情報を表示するには

```
# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

#
```

3.39.7 download ssl certificate

目的	スイッチ上の SSL 機能用証明ファイルをダウンロードします。
構文	download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>
説明	本コマンドは、スイッチで SSL 機能を使用するための証明書ファイルを TFTP サーバーからダウンロードするときに使用します。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデーター記録であり、所有者の情報や認証のための鍵、またデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバーとクライアントが一致した証明書ファイルを持つ必要があります。本スイッチは、DER 形式の証明書を 1 つのみサポートします。
パラメーター	<ipaddr> - TFTP サーバーの IP アドレスを入力します。 certfilename <path_filename 64> - ダウンロードする証明書ファイルのパスとファイル名を入力します。 keyfilename <path_filename 64> - ダウンロードする秘密鍵交換ファイルのパスとファイル名を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 証明書ファイルと秘密鍵ファイルをスイッチにダウンロードするには

```
#download ssl certificate 10.53.13.94 certfilename c:/cert.der keyfilename c:/pkey.der
Command: download ssl certificate 10.53.13.94 certfilename c:/cert.der keyfilename
c:/pkey.der

Certificate Loaded Successfully!

Success.

#
```

注意事項

ダウロード可能な証明書及び秘密鍵のファイルサイズは以下の通りです。
証明書ファイル：8192 バイト
秘密鍵ファイル：4096 バイト

3.40 WEB 認証コマンド

3.40.1 enable web_authentication

目的	WEB 認証機能のグローバル設定を有効にします。
構文	enable web_authentication
説明	このコマンドは WEB 認証機能のグローバル設定を有効にします。 ポート毎に WEB 認証の有効無効を指定する場合は、本コマンドを適用した上で config web_authentication ports コマンドを用いて個別に設定します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証機能のグローバル設定を有効にするには

```
#enable web_authentication
Command: enable web_authentication

Success.

#
```

注意事項

APLGM152GT では、WEB 認証と組み合わせたローミング機能をサポートします。認証されたホストが同一装置内の別の認証ポートへローミングする場合、新しいポートでは認証状態が維持されるため、ローミング時に再認証する必要はありません。

WEB 認証ポートの最大同時セッション数は 128 です。

WEB 認証が有効なポートで認証の対象となるフレームは、イーサネットフレームタイプが IP かつ IP プロトコルタイプが TCP のフレームとなります。
認証の対象外となるフレーム（例えば ICMP,UDP など）は、認証テーブルへ登録されますが、認証による廃棄は行われませんのでご注意ください。
また、IPv6 についても認証の対象外フレームのため装置中継されます。

3.40.2 disable web_authentication

目的	WEB 認証機能のグローバル設定を無効にします。
構文	disable web_authentication
説明	このコマンドは WEB 認証機能のグローバル設定を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証機能のグローバル設定を無効にするには

```
#disable web_authentication
Command: disable web_authentication

Success.

#
```

3.40.3 config web_authentication ports

目的	装置のポート単位で WEB 認証パラメーターを設定します。
構文	config web_authentication ports <<portlist> | all> [*state*] *State* =state <enable | disable> | aging_time <infinite | <min 1-1440>> | block_time <<sec 0-300>>
説明	このコマンドはポート単位で WEB 認証パラメーターを設定します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - 装置の全てのポートを対象とします。 state - ポート単位で WEB 認証を有効あるいは無効にします。 aging_time - WEB 認証端末のタイムアウト時間を指定します。 infinite - WEB 認証端末がエージアウトされないように指定します。 block_time - 認証に失敗した端末をブロックする時間を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1-9 の WEB 認証状態を有効にするには

```
#config web_authentication ports 1-9 state enable
Command: config web_authentication ports 1-9 state enable

Success.

#
```

3.40.4 config web_authentication virtual_ip

目的	このコマンドは WEB 認証用の仮想 IP アドレスを設定します。
構文	config web_authentication virtual_ip <ipaddr>
説明	WEB 認証の仮想 IP アドレスは、未認証端末からの認証要求を受け付ける IP アドレスです。0.0.0.0 が設定されている場合、WEB 認証が動作しません。 本仮想 IP アドレスは WEB 認証を処理するための一種の内部設定値であり、ARP にも ICMP にも応答しません。仮想 IP アドレスへ到達するネットワーク経路を確保する必要はなく、任意の IP アドレスを指定することができます。ただし、未認証端末の IP アドレスと仮想 IP アドレスが同一のサブネットに設定されていると、端末が ARP を解決できず、WEB 認証を開始できませんのでご注意ください。 (例: 未認証端末が 192.168.0.1/24 で仮想 IP アドレスが 192.168.0.10 の場合)
パラメーター	virtual_ip - WEB 認証用を受け付ける仮想 IP アドレスを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。 本装置の管理 IP アドレスの同一の IP アドレスを設定した場合、WEB ベースの管理画面が使用できません。
対応バージョン	1.00.00 以降

使用例: WEB 認証用仮想 IP アドレスを設定するには

```
#config web_authentication virtual_ip 1.1.1.1
Command: config web_authentication virtual_ip 1.1.1.1

Success.

#
```

3.40.5 config web_authentication switch_http_port

目的	Web 認証画面での HTTP/HTTPS の TCP ポート番号を設定します。
構文	config web_authentication switch_http_port <tcp_port_number 1-65535> [<http | https>]
説明	WEB 認証画面での HTTP/HTTPS の TCP ポート番号を設定します。指定されない場合、各プロトコルのデフォルト TCP ポート番号を使用します。プロトコルを指定しない場合、HTTP が適用対象になります。 Web 認証を HTTPS で動作させる場合、本コマンドで https と使用ポートを指定した上で”enable ssl”コマンドで SSL 機能を有効にする必要があります。また、Web 認証を HTTPS から HTTPS に変更する場合は、”disable ssl”コマンドで SSL 機能を無効にした上で、本コマンドで http と使用ポートを設定してください。
パラメーター	switch_http_port - WEB 認証画面での TCP ポート番号(1～65535)を指定します。 http - HTTP に対して適用されます。 https - HTTPS に対して適用されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証を HTTP かつ TCP ポート番号 8888 を使用するように設定するには

```
#config web_authentication switch_http_port 8888 http
Command: config web_authentication switch_http_port 8888 http

Success.

#
```

3.40.6 config web_authentication redirect

目的	WEB 認証リダイレクト機能を設定します。
構文	config web_authentication redirect [<enable | disable>]
説明	WEB 認証リダイレクト機能は、未認証端末が WEB 認証用の仮想 IP アドレス以外のサイトにアクセスした際に、仮想 IP アドレスにリダイレクトさせて強制的に Web 認証画面に誘導する機能です。無効の場合、未認証端末は明示的に仮想 IP アドレスを指定して WEB 認証ポータルに接続する必要があります。
パラメーター	enable - WEB 認証リダイレクト機能を有効にします。 disable - WEB 認証リダイレクト機能を無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.02.00 以降

使用例: WEB 認証リダイレクト機能を有効にするには

```
#config web_authentication redirect enable
Command: config web_authentication redirect enable

Success.

#
```

3.40.7 config web_authentication session_timeout

目的	WEB 認証画面のセッションタイムアウト時間を設定します。
構文	config web_authentication session_timeout <sec 0-120>
説明	本コマンドは、WEB 認証ポートのセッションタイムアウト時間を設定します。セッションタイムアウト時間を短く設定することで、多数の未認証端末がネットワークに短期間に接続した場合の装置の負荷を緩和することができます。本パラメーターのデフォルト値は 120(秒)です。
パラメーター	session_timeout <sec 0-120> - Web 認証ポートの TCP セッションタイムアウト時間を秒単位で設定します。0 の場合はセッションタイムアウトは発生しません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.02.00 以降

使用例: WEB 認証ポートのセッションタイムアウト時間を 30 秒に設定するには

```
#config web_authentication session_timeout 30
Command: config web_authentication session_timeout 30

Success.

#
```

3.40.8 config web_authentication method

目的	WEB 認証方法を設定します。
構文	config web_authentication method <local | radius>
説明	本コマンドは、WEB 認証機能での認証をローカルデータベースを用いて実施するか RADIUS サーバーで実施するかを設定します。
パラメーター	local - ローカルデータベースを使用して認証を行います。 radius - RADIUS サーバーで認証を行います。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証方法を設定するには

```
#config web_authentication method radius
Command: config web_authentication method radius

Success.

#
```

3.40.9 config web_authentication authorization network

目的	WEB 認証成功時に認証属性を参照するかどうかを設定します。
構文	config web_authentication authorization network [radius <enable | disable> | local <enable | disable>]
説明	WEB 認証成功時に認証サーバーが保持する付加情報(VLAN 情報等)の適用方法を指定します。RADIUS サーバーを使用する場合とローカルデータベースを使用する場合でパラメーターは異なります。
パラメーター	radius <enable | disable> - enable 設定とすると RADIUS サーバーから送信される認証属性(例：VLAN)を参照します。デフォルト設定は有効です。 local <enable | disable> - enable 設定とするとローカルデータベースの認証属性を参照します。デフォルト設定は有効です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ローカルデータベースの認証属性を適用するには

```
#config web_authentication authorization network local enable
Command: config web_authentication authorization network local enable

Success.

#
```

注意事項

認証属性を適用する場合、本コマンドの他に「enable authorization network」コマンドで認証属性のグローバル設定を「enable」(有効)にする必要があります。

ダイナミック VLAN で動的に VLAN を割り当てる場合、ローミングするポートの VLAN ID が異なるため、ポートの Ingres checking 設定を無効にする必要があります。この設定は「config gvrp all ingress_checking disable」コマンドで行います。

3.40.10 create web_authentication user

目的	WEB 認証用のローカルユーザーを登録します。
構文	create web_authentication user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
説明	WEB 認証のローカルユーザーを作成する時に使用するコマンドです。 作成された WEB 認証ローカルユーザー設定は、config web_authentication user あるいは delete web_authentication user コマンドで編集、削除できます。 VLAN が指定されない場合又は割り当てられた VLAN が存在しない場合には、WEB 認証ユーザーはデフォルト VLAN が適用されます。
パラメーター	user - WEB ベースのアクセス制御用のアカウントを作成します。 <username 15> - 半角英数字 15 文字以内でユーザー名を作成します。 vlan - 認証成功時にユーザーに割り当てる VLAN を指定します。 <vlan_name 32> - VLAN 名を入力します。 <vlanid> - VLAN ID を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証のローカルユーザーを作成するには

```
#create web_authentication user webuser vlan default
Command: create web_authentication user webuser vlan default

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

#
```

3.40.11 config web_authentication user

目的	登録済みの WEB 認証ローカルユーザーを編集します。
構文	config web_authentication user <username 15> [*vlan* | clear_vlan] *Vlan* = vlan <vlan_name 32> | vlanid <vlanid 1-4094>
説明	create web_authentication user で作成された WEB 認証ローカルユーザーを編集する時に使用するコマンドです。
パラメーター	user - WEB ベースアクセス制御用のアカウントを指定します。 <username 15> - 半角英数字 15 文字以内でユーザー名を指定します。 vlan - 認証成功時にユーザーに割り当てる VLAN を指定します。 <vlan_name 32> - VLAN 名を入力します。 <vlanid> - VLAN ID を入力します。 clear vlan - このアカウントにリンクされている VLAN 情報をクリアします
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証ローカルユーザーに割り当てた認証 VLAN の設定を削除するには

```
#config web_authentication user webuser clear_vlan
Command: config web_authentication user webuser clear_vlan

Success.

#
```

3.40.12 delete web_authentication

目的	このコマンドは WEB 認証ローカルユーザーを削除します。
構文	delete web_authentication <user <username 15> | all_users>
説明	このコマンドは WEB 認証ローカルユーザーを削除します。
パラメーター	user <username 15> - 削除するユーザー名を指定します。 all users - WEB 認証ローカルユーザーを全て削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証ローカルユーザーを削除するには

```
#delete web_authentication user user1
Command: delete web_authentication user user1

Success.

#
```

3.40.13 config web_authentication redir_url

目的	WEB 認証リダイレクト URL を設定します。
構文	config web_authentication redir_url <string 128>
説明	リダイレクト URL が設定された場合、ユーザーは Web 認証が成功した後に設定した URL にリダイレクトされます。リダイレクト URL が設定されていない場合は、認証成功後にログアウト用の画面にリダイレクトされます。
パラメーター	<string 128> - WEB 認証後にユーザーがリダイレクトされる URL を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証デフォルトリダイレクト URL を設定するには

```
#config web_authentication redir_url http://www.website.com
Command: config web_authentication redir_url http://www.website.com

Success.

#
```

3.40.14 config web_authentication clear_redir_url

目的	WEB 認証のリダイレクト URL をクリアします。
構文	config web_authentication clear_redir_url
説明	config web_authentication redir_url コマンドで設定したリダイレクト URL をクリアします。リダイレクト URL がクリアされると、ユーザーは WEB 認証が成功した後にログアウト用の画面にリダイレクトされます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証のデリダイレクト URL をクリアするには

```
#config web_authentication clear_redir_url
Command: config web_authentication clear_redir_url

Success.

#
```

3.40.15 config web_authentication auth_page

目的	Web 認証画面をカスタマイズする際に使用します。
構文	config web_authentication auth_page <<login | logout> <default | customize_text_box line <value 1-8>> <content <multiword 70> | clear>>
説明	本コマンドにより管理者は WEB 認証 login または logout 画面に任意の文字列情報をカスタマイズして表示させることが可能となります。
パラメーター	login - カスタマイズする WEB 認証 login 画面を指定します。 logout - カスタマイズする WEB 認証 logout 画面を指定します。 default - WEB 認証画面を初期状態に戻します。 customize_text_box line - 対象画面にテキストボックスを追加します。 <value 1-8> - カスタマイズするテキストボックス番号を指定します。 content - 選択したテキストボックスに表示する文字列を登録します。 <multiword 70> - 選択したテキストボックスに表示する文字列（半角で 70 文字以内、全て全角文字の場合は 35 文字以内)を登録します。文字列の先頭と最後尾に「"」をおいて入力します。なお、日本語を登録する場合は、使用するターミナルソフトウェアにてエンコード方式を Shift-JIS に設定してください。 clear - 選択したテキストボックスに登録されている文字列をクリアします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証 login 画面に任意の文字列をカスタイマイズ表示設定するには

```
#config web_authentication auth_page login customize_textbox_line 8 content "MAIL    :
network.manager.ab@apresiasystems.com"
Command: config web_authentication auth_page login customize_textbox_line 8 content
"MAIL    : network.manager.ab@apresiasystems.com"

#
```

使用例: WEB 認証 login 画面のカスタイマイズ文字列をクリアするには

```
#config web_authentication auth_page login customize_textbox_line 1 clear
Command: config web_authentication auth_page login customize_textbox_line 1 clear

#
```

使用例: WEB 認証 login 画面をデフォルトに戻すには

```
#config web_authentication auth_page login default
Command: config web_authentication auth_page login default

#
```

3.40.16 clear web_authentication auth_state

目的	このコマンドは WEB 認証エントリーをクリアします。
構文	clear web_authentication auth_state 〈*ports*〉 *Ports* = ports 〈〈portlist〉	all〉 [authenticated	authenticating	blocked]	macaddr 〈macaddr〉
説明	ポートがポートベースモードに設定された場合、そのポートは認証されない状態に戻ります。そのポートに関係する全てのタイマーはリセットされます。 ポートがホストベースモードに設定された場合、そのポート上のユーザーは全てクリアされます。 ユーザーはネットワークにアクセスするために再認証される必要があります。
パラメーター	〈portlist〉 - 設定するポート範囲を指定します。 all - この設定に使用される全てのポートを指定します。 authenticated - ある 1 ポートの全ての認証されたユーザーをクリアします。 authenticating - ある 1 ポートの全ての認証中のユーザーをクリアします。 blocked - ある 1 ポートの全てのブロックされたユーザーをクリアします。 macaddr - この設定に使用される MAC アドレスを指定します。 〈macaddr〉 - この設定に使用される MAC アドレスをここに入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1-5 の WEB 認証エントリーをクリアするには

```
#clear web_authentication auth_state ports 1-5
Command: clear web_authentication auth_state ports 1-5

Success.

#
```

3.40.17 show web_authentication

目的	このコマンドはWEB認証のグローバル設定を表示します。
構文	show web_authentication
説明	このコマンドはWEB認証のグローバル設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00以降

使用例: WEB認証のグローバル設定を表示するには

```
#show web_authentication
Command: show web_authentication

 Web-Base Access Control
 --------------------------------
 State                    : Enabled
 Method                   : RADIUS
 Authentication Failover  : Enabled
 Redirect Path            : http://www.website.com
 Virtual IP               : 1.1.1.1
 Switch HTTP Port         : 8888 (HTTP)
 RADIUS Authorization     : Enabled
 Local Authorization      : Enabled
 Redirect Action          : Enabled
 Session Timeout          : 120 seconds

#
```

3.40.18 show web_authentication ports

目的	このコマンドはWEB認証ポート設定を表示します。
構文	show web_authentication ports [<portlist>]
説明	このコマンドはWEB認証ポート設定を表示します。
パラメーター	ports <portlist> - 設定を表示するポート範囲を指定します
制限事項	なし。
対応バージョン	1.00.00以降

使用例: ポート 1-3 の WEB 認証ポート設定を表示するには

```
#show web_authentication ports 1-3
Command: show web_authentication ports 1-3

 Port   State       Aging Time     Block Time     Auth Mode
                     (Minutes)      (Seconds)
 -----  --------    -------------  -------------  -------------
 1      Enabled     60             120            Host-Based
 2      Enabled     60             120            Host-Based
 3      Enabled     120            120            Host-Based

#
```

3.40.19 show web_authentication auth_state ports

目的	このコマンドはポートの認証状態を表示します。
構文	show web_authentication auth_state ports [<portlist>]
説明	このコマンドはポートの認証状態を表示します。
パラメーター	ports <portlist> - 認証状態を表示するポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ポートの認証状態を表示するには

```
#show web_authentication auth_state ports
Command: show web_authentication auth_state ports


H:Host-Based  P:Port-Based

Port   MAC Address          Original     State      VID  Aging Time/
                             RX VID                      Block Time
------ -------------------- -------- -------------- ---- -----------
10     00-40-66-00-00-01(H) 1        Authenticating -    19
10     00-40-66-00-00-02(H) 1        Authenticating -    1

 Total Authenticating Hosts  : 2
 Total Authenticated Hosts   : 0
 Total Blocked Hosts         : 0

#
```

3.40.20 show web_authentication connection

目的	WEB 認証処理中の端末接続情報とセッション情報を表示します。
構文	show web_authentication connection
説明	本コマンドは、WEB 認証処理中の端末接続情報とセッション情報を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.02.00 以降

使用例: WEB 認証処理中の端末接続情報とセッション情報を表示するには

```
#show web_authentication connection
Command: show web_authentication connection

Web Authentication Connections:
 1. 00-40-66-CC-BA-64, 192.168.10.207
  (1) l4_dst_port(host)=80, l4_src_port(host)=2195, l4_src_port(switch)=50205,
last_hit_time=1035150
 TotalNum=1

Web Authentication Sessions:
Current Time: 1056000 (ms)
 1. 00-40-66-CC-BA-64, 192.168.10.207, rx_port=1,
  l4_src_port(switch)=50205, session_start_time=1035150
TotalNum=1

#
```

3.40.21 show web_authentication user

目的	このコマンドはユーザーが WEB 認証アカウントを表示します。
構文	show web_authentication user
説明	ユーザーが WEB 認証アカウントを表示することを可能にするコマンドです パスワードは管理レベルの下に表示されます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: WEB 認証アカウントを表示するには

```
#show web_authentication user
Command: show web_authentication user

   Username           Password         VID
   -----------------  ---------------  ---------
   webuser            webuser          -

 Total Entries:1

#
```

3.40.22 show web_authentication auth_page

目的	WEB 認証で使用する認証画面に管理者がカスタマイズ登録した任意の文字列情報内容を表示します。
構文	show web_authentication auth_page
説明	本コマンドは、WEB 認証 login または logout 画面にカスタマイズ登録された文字列情報内容を表示します。日本語を表示させるには使用するターミナルソフトウェアにてエンコード方式を Shift-JIS に設定してください。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: WEB 認証カスタイマイズ文字列情報を表示するには

```
#show web_authentication auth_page
Command: show web_authentication auth_page

Login Page Customized Text Box:
------------------------------------------------------------------------
1.ご利用方法がわからない方は下記へご連絡ください。
2.
3. [問い合わせ先]
4.
5.情報システム統括部 ネットワーク運用担当
6.担当者名: Network Manager
7.TEL      : 123-4567
8.MAIL     : network.manager.ab@apresiasystems.com
------------------------------------------------------------------------

Logout Page Customized Text Box:
------------------------------------------------------------------------
1.ご利用方法がわからない方は下記へご連絡ください。
2.
3. [問い合わせ先]
4.
5.情報システム統括部ネットワーク運用担当
6.担当者名: Network Manager
7.TEL      : 123-4567
8.MAIL     : network.manager.ab@apresiasystems.com
------------------------------------------------------------------------
#
```

3.41 COMMAND LOGGING コマンド

COMMAND LOGGING コマンドは、コマンドラインインターフェース上で実行したコマンドの成功および失敗をログに出力するコマンドです。デフォルトでは「enable」有効となっています。

3.41.1 enable command logging

目的	コマンドログ機能を有効にします。
構文	enable command logging
説明	本コマンドは、コマンドログ機能を有効に設定します。 ただし、装置が起動中または設定を読み込んでいる間は動作しません。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: コマンドログ機能を有効に設定するには

```
#enable command logging
Command: enable command logging

Success.

#
```

3.41.2 disable command logging

目的	コマンドログ機能を無効にします。
構文	disable command logging
説明	本コマンドは、コマンドログ機能を無効に設定します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: コマンドログ機能を無効に設定するには

```
#disable command logging
Command: disable command logging

Success.

#
```

3.41.3 show command logging

目的	コマンドログ機能設定を表示します。
構文	show command logging
説明	本コマンドは、コマンドログ機能設定を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:コマンドログ機能設定を表示するには

```
#show command logging
Command: show command logging

Command Logging State : Enabled

#
```

3.42 PERIPHERALS コマンド

PERIPHERALS コマンドは、Green mode や EEE(Energy Efficient Ethernet)などの省電力機能及び内部温度センサによる温度検知機能、FAN の状態監視機能などをサポートします。

3.42.1 config green_mode ports

目的	各ポートの green mode を設定します。
構文	config green_mode ports <<portlist> | all> state <enable | disable>
説明	green mode が有効な場合、リンクダウンポートの省電力機能(リンクダウンしているポートの消費電力を削減)とケーブル長の省電力機能(接続されたケーブル長を判定し、短尺ケーブルが接続されたポートの消費電力を削減)が有効です。 green mode のデフォルト設定は、「disable」(無効)です。
パラメーター	ports <<portlist> | all> - green mode を設定するポートまたはポートリストを入力します。all を指定するとスイッチのすべてのポートが対象となります。 state <enable | disable> - 指定されたポートの green mode を「enable」(有効)または「disable」(無効)に設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 全ポートの green mode 機能を設定するには

```
#config green_mode ports all state enable
Command: config green_mode ports all state enable

Success.

#
```

3.42.2 show green_mode ports

目的	各ポートの green mode 状態を表示します。
構文	show green_mode ports <portlist>
説明	本コマンドは、各ポートの green mode 状態を表示します。
パラメーター	<portlist> - 表示するポートまたはポートリストを入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ポート 1-4 の green mode 状態を表示するには

```
#show green_mode ports 1-3
Command: show green_mode ports 1-3

 Port   State      Operation State
 -----  ---------  ----------------------
 1      Enabled    Normal
 2      Disabled   Normal
 3      Enabled    Power Down
```

3.42.3 port_led test

目的	全ポートの LED 表示状態を制御します。
構文	port_led test <off | green | amber | blink_green | blink_amber>
説明	本コマンドは、各ポートのリンク状態に関係なく全てのポートの LED 表示を点灯または点滅させます。
パラメーター	off - 全ポートの LED 表示を通常のリンク状態で表示します。 green - 全ポートの LED 表示を緑色点灯で表示します。 amber - 全ポートの LED 表示を橙色点灯で表示します。 blink_green - 全ポートの LED 表示を緑色点滅で表示します。 blink_amber - 全ポートの LED 表示を橙色点滅で表示します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 全ポートの LED 表示を緑色点灯で表示するには

```
#port_led test green
Command: port_led test green

Success.

#
```

使用例: 全ポートの LED 表示を通常のリンク状態で表示するには

```
#port_led test off
Command: port_led test off

Success.

#
```

注意事項

コマンド入力時にリンクアップしているポートは、一度リンクダウンが発生します。

3.42.4 show environment

目的	スイッチの内部温度と FAN 動作状態を表示します。
構文	show environment
説明	本コマンドは、スイッチの内部温度と FAN 動作状態を表示します。 FAN 動作状態の表示では、正常回転時(Normal)・回転数低下時(Abnormal slow)・回転停止時(Stop)と表示されます。 実装の FAN 番号は、図 3-1 を参照ください。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチの内部温度と FAN 動作状態を表示するには

```
#show environment
Command: show environment

 System Temperature (Celsius)   : 26
 Fan 1              : Normal
 Fan 2              : Normal
 Fan 3              : Normal
 Fan Led Error State : Enable

#
```

注意事項

装置が起動してから内部温度を検知するまで約 1 分程度かかります。その間、System Temperature は 0 表示となりますが異常ではありません。

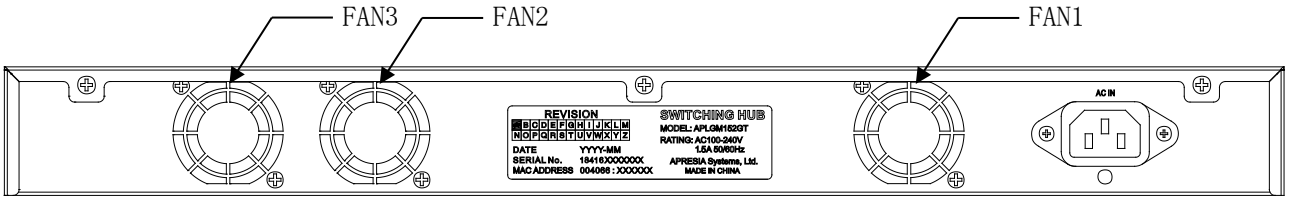


図 3-1 APLGM152GT の FAN 位置図

3.42.5 config temperature

目的	スイッチの内部温度通知機能を設定します。
構文	config temperature < polling_interval <value 10-300> | notify < high | low > [state < enable | disable > | threshold <temperature -50-85> | trap_state < enable | disable > | log_state < enable | disable >] >
説明	本コマンドは、スイッチの内部温度センサを監視し、設定した閾値の範囲を超えた場合にログ出力およびトラップ通知を行います。
パラメーター	polling_interval <value 10-300> - スイッチ内部温度の検知間隔を 10～300 秒の範囲で設定します。デフォルト値は、60 秒です。 notify < high | low > - 高温または低温の温度通知機能を設定します。 state < enable | disable > - 温度通知機能を有効または無効に設定します。 threshold <temperature -50-85> - 検知温度を-50℃から 85℃の範囲で設定します。デフォルト値は高温側が 55℃、低温側が-5℃です。 trap_state < enable | disable > - 検知温度が閾値を超えた時のトラップ通知を有効または無効に設定します。デフォルト設定は、「enable」(有効)です。 log_state < enable | disable > - 検知温度が閾値を超えた時のログ出力を有効または無効に設定します。デフォルト設定は、「enable」(有効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチ内部温度の検知間隔を 300 秒に設定するには

```
#config temperature polling_interval 300
Command: config temperature polling_interval 300


Success.


#
```

3.42.6 show temperature notify

目的	スイッチの内部温度通知機能の設定を表示します。
構文	show temperature notify <high | low>
説明	本コマンドは、スイッチの内部温度通知機能の設定を表示します。
パラメーター	notify <high | low> - 低温側または高温側の通知機能を表示させるか指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチの内部温度通知機能の高温側の設定状態を表示するには

```
#show temperature notify high
Command: show temperature notify high


High Temperature Notify Information
-----------------------------------
Current Status  :  Normal
State           :  Enabled
Threshold       :  55
Polling Interval:  60
Trap State      :  Enabled
Log State       :  Enabled


#
```

3.42.7 config eee ports

目的	各ポートに EEE(Energy Efficient Ethernet)機能を設定します。
構文	config eee ports < <portlist> | all > state < enable | disable >
説明	EEE(Energy Efficient Ethernet)機能は IEEE802.3az で標準化された省電力イーサネットの規格です。ポートに設定することでトラフィックの状態に応じて消費電力を低減する効果が得られます。デフォルト値は「disable」(無効)です。
パラメーター	ports < <portlist> | all > - EEE 機能を設定する対象ポートを指定します。All を選択した場合、1～48 番ポートに本機能を設定します。 state < enable | disable > - 上記で指定したポートで EEE 機能の有効、無効を設定します。デフォルト設定は、「disable」(無効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 8 に EEE 機能を設定するには

```
#config eee ports 8 state enable
Command: config eee ports 8 state enable


Success.


#
```

注意事項

コマンド入力時、EEE を設定する対象ポートでリンクアップしているポートは一度リンクダウンが発生します。

EEE 機能は、ポートの AutoNegotiation 設定が「Enable」(有効)の場合に使用することができます。なお、10BASE-T には対応しておりません。

接続する機器同士が EEE 機能に対応している必要があります。

3.42.8 show eee ports

目的	各ポートの EEE 設定状況を表示します。
構文	show eee ports [<portlist>]
説明	本コマンドは、各ポートの EEE 設定状況を表示します。
パラメーター	<portlist> - 表示対象のポートを指定します。指定しない場合、全てのポートの設定が表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ポート 1 から 8 の EEE 設定状況を表示するには

```
#show eee ports 1-8
Command: show eee ports 1-8

Port            State
---------     -----------
1             Disabled
2             Disabled
3             Disabled
4             Disabled
5             Disabled
6             Disabled
7             Disabled
8             Enabled

#
```

3.42.9 fan_led error

目的	ファンエラー時の LED 状態を設定します。
構文	fan_led error < enable | disable >
説明	本コマンドは、ファンエラー時の LED 状態を設定します。
パラメーター	enable - FAN エラー検知時に FAN LED が赤色に点滅または点灯します。 disable - FAN エラーを検知しても FAN LED は緑色の点灯から変化しません。 デフォルト設定は、「enable」(有効)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:FAN LED の設定を有効にするには

```
#fan_led error enable
Command: fan_led error enable


Success.


#
```

注意事項

fan_led error 設定が「enable」(有効)の場合、FAN 回転が低下時に赤点滅、FAN 回転が停止時に赤点灯の LED 状態を表示します。
FAN の動作状態は、show environment コマンドでも確認することができます。
FAN エラーが検知された場合は、装置の使用を中止し販売元に修理を依頼してください。FAN 停止のまま使用すると装置の内部温度が上昇し故障の原因となります。

3.43 保守コマンド

保守コマンドは、ポートの状態監視において異常を検出した場合、装置再起動による復旧を試みます。

注意事項

本コマンドは、ポート状態監視において異常が発生した場合の一時的な復旧を目的としております。これらの異常が発生した場合は装置故障の可能性がありますので、販売元またはサポート窓口までご連絡ください。

3.43.1 config auto_recovery_mode

目的	スイッチのポート接続状態の健全性が 2 ポート以上確認できない場合、自動再起動により復旧を試みます。
構文	config auto_recovery_mode < enable | disable >
説明	本コマンドは、ポート接続状態の健全性が 2 ポート以上確認できない場合、自動再起動により復旧を試みます。自動再起動した場合の起動ログには"System restart"ログが出力されます。デフォルト設定は、「disable」(無効)です。
パラメーター	enable - 自動再起動を「enable」(有効)に設定します。 disable - 自動再起動を「disable」(無効)に設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: オートリカバリー機能を有効にするには

```
#config auto_recovery_mode enable
Command: config auto_recovery_mode enable

Success.

#
```

3.43.2 show auto_recovery_mode

目的	オートリカバリーモード設定を表示します。
構文	show auto_recovery_mode
説明	本コマンドは、オートリカバリーモード設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:オートリカバリー設定を表示するには

```
#show auto_recovery_mode
Command: show auto_recovery_mode
Auto Recovery Mode : Enabled

Success.

#
```

4. 使用上の注意事項

(1) コンソールポートには、パラメーター設定時のみに RS-232C ケーブルを接続し、通常の運用時には接続しないでください。

(2) ポートミラーリング機能は、source ポートとして設定したポートで送受信されたフレーム等を解析するための機能です。従って、Target ポートとして設定したポートには、アナライザ等ネットワークを解析する装置以外は接続しないでください。

(3) ポート VLAN を設定する場合、ホスト(スイッチングハブ)が属していないグループのポートからホスト宛に通信を行うことはできません。またホストは複数のグループに属することはできません。

5. トラブルシューティング

5.1 表示 LED に関連する現象と対策

現象	対策
「PWR」 LED が点灯しない。	電源コードが本装置の AC インレットと電源コンセントに正常に接続されていることを確認してください。
ツイストケーブルを接続しても「LINK/ACT」 LED が点灯しない。	ツイストケーブルに異常がないかどうか確認してください。
	接続相手の端末が正常に動作しているかどうか確認してください。
	モジュラープラグ(RJ-45)の接続に異常がないかどうか確認してください。
	接続相手が NIC またはハブのカスケードポートである場合、ツイストケーブルがストレートケーブルであることを確認してください。また、接続相手がハブの MDI-X ポートの場合、ツイストケーブルがクロスケーブルであることを確認してください。
	SFP モジュールが正しく挿入されていることを確認してください。
「CONSOLE」LED が点滅している。	当該装置またはその接続先ネットワークにてループが生じていないか確認してください。
「FAN LED」が赤点滅または赤点灯している。	FAN が故障している可能性があります。装置の使用を中止して販売元に修理を依頼してください。

5.2 コンソール端末に関連する現象と対策

現象	対策
電源投入しても Login プロンプトが出力されない。	コンソール端末の通信条件の設定が正しいことを確認してください。 設定値は「通信速度 9600bps、1 キャラクタ 8 ビット、ストップビット 1 ビット、パリティなし、フロー制御なし、RS, ER は常時「ON」です。
	「CONSOLE」とコンソール端末との RS-232C ケーブルが正しいことを確認してください。
	「CONSOLE」への接続が正常かどうか確認してください。
	「POWER」 LED が点灯していることを確認してください。
設定値が正常に入力されていない。	正常な文字数であれば、内部のメモリーに異常が発生していると考えられます。サポート対応窓口にお問い合わせください。

5.3 Telnet に関連する現象と対策

現象	対策
端末から Telnet により ログインすることができない。	本装置の IP アドレス、ネットマスク、デフォルトルートの設定が正常であることを確認してください。また設定後にリセットもしくは電源再投入がされていることも確認してください。
	接続しているポートの通信設定が ENABLE 状態になっていることを確認してください。ENABLE 状態ならば、ツイストケーブルの接続を確認してください。
	Telnet しようとするアドレスが本装置のアドレスであることを確認してください。
	本装置が正常に起動し、動作していることを確認してください。

5.4 スイッチングハブ機能に関連する現象と対策

現象	対策
端末から別の端末にデータの中継ができない。	各端末が別々のポート VLAN グループに所属していないかどうか確認してください。
	各端末と本装置間のツイストケーブルの接続が正常であることを確認してください。
	各端末の接続されているポートが ENABLE 状態であるかどうか確認してください。
パケットロスが発生する。	特定のポートから出力されるフレームの負荷が 100%を超えていないかどうか確認してください。(特定のポートに 100%を超える負荷が集中した場合、別ポートにも影響を及ぼし、パケットロスが発生する場合があります。)

5.5 VLAN に関連する現象と対策

現象	対策
VID を指定するとエラーメッセージが表示される。	指定した VID が、既に他の VLAN グループで使用されているとき、エラーメッセージが表示されます。VID の設定を修正してください。

5.6 SFP に関連する現象と対策

現象	対策
SFP を認識している状態で通信しない。	SFP を認識している状態で通信しない場合は、SFP が不完全な状態で装着されている可能性があります。SFP を取り外し、再度装着してください。現象が再発する場合は SFP 又は装置の異常が考えられます。

5.7 冷却ファンに関連する現象と対策

現象	対策
電源投入しても冷却ファンが回転しない。	ファンまたは装置の異常が考えられます。カバーを開けることなく、お買い求めの販売店もしくは販売元にお問い合わせください。

6. 準拠規格

No.	項目	準拠規格
1	LAN インターフェース	IEEE802.3 ：10BASE-T IEEE802.3u ：100BASE-TX IEEE802.3u ：Auto-Negotiation IEEE802.3z ：1000BASE-X IEEE802.3ab：1000BASE-T
2	コンソール インターフェース	ITU-T 勧告 V.24/V.28
3	ネットワーク管理 プロトコル	RFC1157：Simple Network Management Protocol (SNMP) RFC1901：Introduction to Community-based SNMPv2 RFC1905：Protocol Operations for Version 2 of the Simple Network Management Protocol RFC1908：Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework RFC2570：Introduction to Version 3 of the Internet-standard Network Management Framework RFC2575：View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
4	ネットワーク管理対象	RFC1213：Internet 標準 MIB RFC1493：Bridge MIB RFC2819：RMON MIB 4 グループ RFC2021：RMON2 MIB のうち Probe config の一部 RFC2233：ifMIB ベンダー独自 MIB
5	通信プロトコル	RFC793 ：TCP(Transmission Control Protocol) RFC768 ：UDP(User Datagram Protocol) RFC1350：THE TFTP PROTOCOL (REVISION 2) RFC783 ：TFTP Client RFC791 ：IP(Internet Protocol) RFC792 ：ICMP(Internet Control Message Protocol) RFC826 ：ARP(Address Resolution Protocol) RFC854 ：TELNET RFC1769：SNTP(Simple Network Time Protocol) RFC3164：SYSLOG RFC5321：SMTP(Simple Mail Transfer Protocol) RFC951/RFC1541：BootP/DHCP Client
6	IGMP snooping	RFC1112：IGMPv1 (snooping only) RFC2236：IGMPv2 (snooping only) RFC3376：IGMPv3 (awareness only)

No.	項目	準拠規格
7	セキュリティー プロトコル	RFC2865：RADIUS (client only) RFC1492：TACACS+ Authentication For the Management Access RFC2138/RFC2139：RADIUS Auth. For Management Access RFC2866：RADIUS Accounting (802.1x only) RFC4250：The Secure Shell(SSH) Protocol Assigned Numbers RFC4251：The Secure Shell(SSH) Protocol Architecture RFC4252：The Secure Shell(SSH) Authentication Protocol RFC4253：The Secure Shell(SSH) Transport Layer Protocol RFC4254：The Secure Shell(SSH) Connection Protocol RFC4256：Generic Message Exchange Authentication for the Secure Shell Protocol(SSH)
8	その他	VCCI Class A 準拠 IEEE802.3ad ：リンクアグリゲーション IEEE802.1Q：tag group VLAN,QoS(IEEE802.1Q priority mapping/queuing) IEEE802.1D ：STP IEEE802.1W ：RSTP IEEE802.1S ：MSTP IEEE802.3x ：フロー制御 IEEE802.1AB ：LLDP IEEE802.3az ：Energy Efficient Ethernet

ApresiaLightGM152GT Ver.1.03 CLI マニュアル

2021 年 1 月 初版

APRESIA Systems 株式会社
東京都中央区築地二丁目 3 番 4 号
築地第一長岡ビル
https://www.apresiasystems.co.jp/