TD61-7158A

ApresiaLightGM シリーズ

Ver. 1.13

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
-	2020 年 1 月 28 日	・Ver. 1.12 CLI マニュアル(TD61-6840)より新規作成 ・全章を対象に誤字・脱字・体裁を修正
A	2020 年 3 月 23 日	・全章を対象に誤字・脱字・体裁を修正、および内容の見直しを実施 ・3.39.3 config ssl cachetimeout timeout、および 3.39.6 show ssl cachetimeout コマンドの対応バージョンを変更(Ver. 1.13.01 以降は非対応)。また、関連する既知問題の情報を注意事項に追加。

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
ApresiaLightGM シリーズ	ApresiaLightGM110GT-SS	APLGM110GTSS
	ApresiaLightGM118GT-SS	APLGM118GTSS
	ApresiaLightGM124GT-SS	APLGM124GTSS
	ApresiaLightGM110GT-PoE	APLGM110GTPOE
	ApresiaLightGM118GT-PoE	APLGM118GTPOE
	ApresiaLightGM124GT-PoE	APLGM124GTPOE

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 ApresiaLightGM シリーズ専用です。ApresiaLightFM シリーズ及び ApresiaLightGM152GT にインストールすることはできません。
また、ApresiaLightGM シリーズに ApresiaLightFM シリーズ及び ApresiaLightGM152GT 用のファームウェア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。

Apresia は、APRESIA Systems 株式会社の登録商標です。
Ethernet/イーサネットは、富士ゼロックス株式会社の登録商標です。
その他ブランド名は、各所有者の商標もしくは登録商標です。

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	管理 IPv4 アドレス	設定あり(10.X.X.X)
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)
Medium Type	コンボポートのメディアタイプ(Fiber/Copper)	Copper(UTP)
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

設定項目	内　容	出荷時の設定値
Link Aggregation Algorithm	リンクアグリゲーションのアルゴリズム	MAC source
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※1	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(kbps)
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 認証/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 Failover	RADIUS 未応答時の Local 認証/強制認証切り替え	Disabled(非動作)
Web Auth Redirect	Web 認証画面への強制リダイレクト	Enabled(動作)
Web Auth Session Timeout	Web 認証画面のセッションタイムアウト時間	120(秒)
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 1) 802.1p 1 (Class 0) 802.1p 2 (Class 0) 802.1p 3 (Class 1) 802.1p 4 (Class 2) 802.1p 5 (Class 2) 802.1p 6 (Class 3) 802.1p 7 (Class 3)
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
DHCP Snooping State	DHCP Snooping 機能	Disabled(非動作)
DHCP Snooping DENY Mode	DHCP Snooping 動作モード(PERMIT/DENY)	Disabled(PERMIT)
DHCP Snooping Mode Timer	DHCP Snooping PERMIT モード時の移行タイマー	1800(秒)
DHCP Snooping Option 82	DHCP Snooping オプション 82 情報付加機能	Disabled(非動作)
DHCP Snooping Inspection	DHCP Snooping の検査対象(ARP/IPv4)	全て Enabled(対象)
PoE State※2	電力供給機能の動作状態	Enabled(動作)
PoE System Power_Limit	スイッチ全体の供給制限値	APLGM110GTPOE：125(W) APLGM118GTPOE：250(W) APLGM124GTPOE：375(W)
PoE Ports Power_Limit	ポート単位の供給制限値	31,200(mW)
Command Logging State※3	コマンドログ機能の動作状態	Enabled(動作)
Green Mode State※4	省電力機能の動作状態	Enabled(動作)
SFP Auto Recognition※5	コンボポートの SFP 自動認識	Enabled(動作)

※1 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。

※2 PoE機能は以下の機種で対応します。

GMシリーズ3機種：APLGM110GTPOE,APLGM124GTPOE (GM1.04.00以降のソフトウェアバージョン)

：APLGM118GTPOE (GM1.10.00以降のソフトウェアバージョン)

※3 コマンドログ機能は、ソフトウェアバージョン(GM1.03.00以降)で追加しました。

※4 省電力機能は、ソフトウェアバージョン(GM1.04.00以降)で追加しました。

※5 SFP自動認識機能は、ソフトウェアバージョン(GM1.12.00以降)で追加しました。

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	ルートテーブル数	1（Default ルート）
FDB(MAC Address Table)	MAC アドレステーブル登録数	8191 (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	1024 (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	16 (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	APLGM124：8 グループ APLGM118：8 グループ APLGM110：5 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	4（Class 0-3）
ACL※1	アクセスリストのプロファイル数	256
	全てのプロファイルに対するアクセスルール数	256（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	128
	IP ホスト数	1024
MLD Snooping	MLD マルチキャストグループ数	128
MAC Based Access Control	MAC 認証で RADIUS 認証による収容端末数	静的 VLAN:128（装置全体）
		動的 VLAN:64（装置全体）
	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	静的 VLAN:512（装置全体）
		動的 VLAN:64（装置全体）
	Web 認証で Local 認証によるエントリー数	16
	Web 認証前の同時セッション数	63
802.1X Authentication	802.1X 認証で RADIUS 認証による収容端末数	静的 VLAN:16(ポート単位)
		動的 VLAN:64（装置全体）

項　目	内　容	最大値
	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
DHCP Snooping	DHCP Snooping テーブル登録数	126(スタティック含む)
	スタティックエントリー数	126
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 倍数
Jumbo	ジャンボフレームサイズ（Un-Tag）	9212(Byte)
	ジャンボフレームサイズ（Tag）	9216(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
AAA	AAA 認証サーバーの IP エントリー数	16
	AAA 認証サーバーグループ数	4
	AAA 認証サーバー1 グループの IP エントリー数	8
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	6000(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
PoE	装置全体の供給電力制限値	APLGM110GTPOE：125(W) APLGM118GTPOE：250(W) APLGM124GTPOE：375(W)
	ポート単位の供給電力制限値	31,200(mW)

※1 装置に設定可能なアクセスリストの最大ルール数は 256 です。アクセスプロファイル全体で 256 以上のアクセスルールを割り当てることは出来ません。

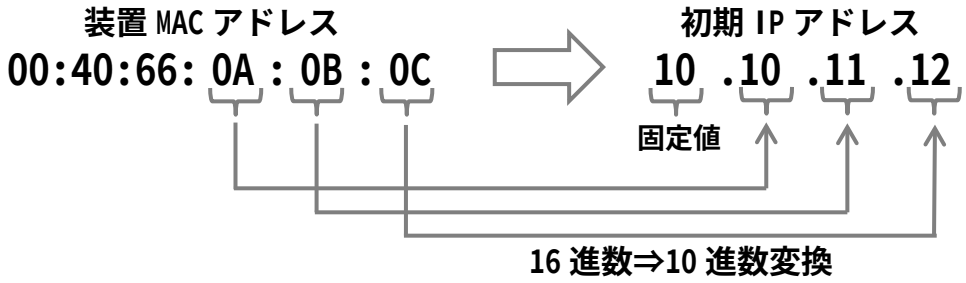
1.3 初期 IP アドレス設定

Ver.1.08.00 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。

(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。

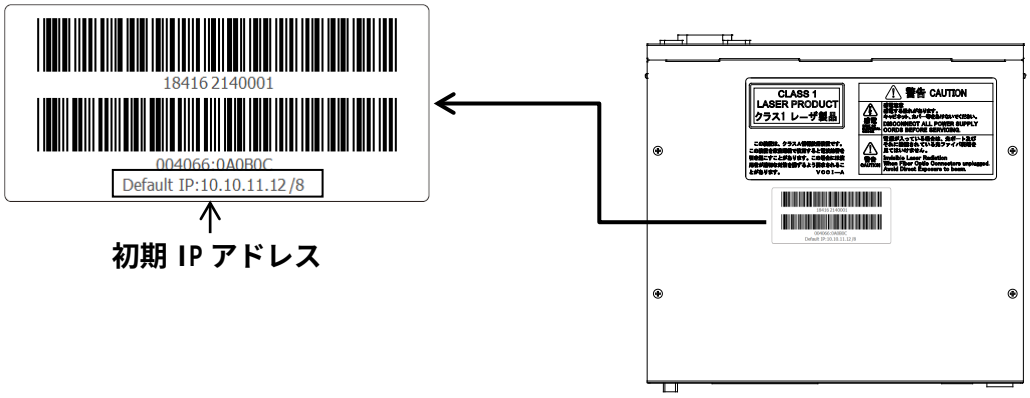


(2) サブネットマスク

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

工場出荷時の初期 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

パラメーター設定端末の準備(1.5 節参照)

↓

パラメーター設定端末の接続(1.6 節参照)

↓

パラメーター設定端末の電源 ON

↓

本装置の電源 ON

↓

LED 表示ランプの確認
PWR 表示 LED が点灯していることを確認してください。

↓

表示されたら、何かキーを押して下さい。
表示されない場合、Ctrl+R を押し、コンソール画面を更新してください。
<表示例>
Press any key to login...

↓

パラメーター設定端末の表示画面の確認
以下のように表示されていることを確認してください。
表示されない場合、Ctrl+R を押し、コンソール画面を更新してください。
<表示例>

```
ApresiaLightGM110GT-SS Gigabit Ethernet Switch
Command Line Interface


Firmware: 1.13.00
Copyright(C) 2019 APRESIA Systems, Ltd. All rights reserved.
UserName:
```

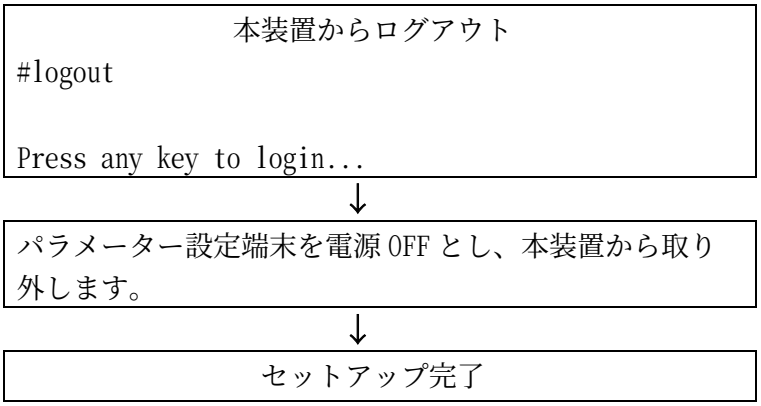
↓

システムログイン(2.2.1 項参照)

↓

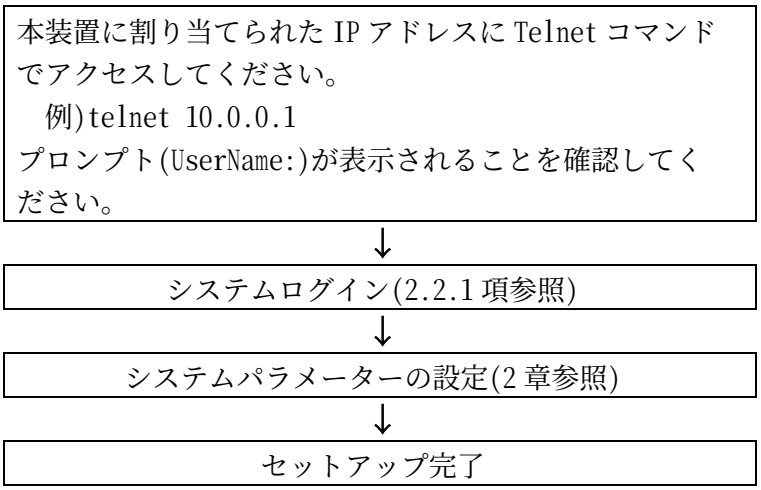
システムパラメーターの設定(2 章参照)

↓



(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(デフォルト)
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。

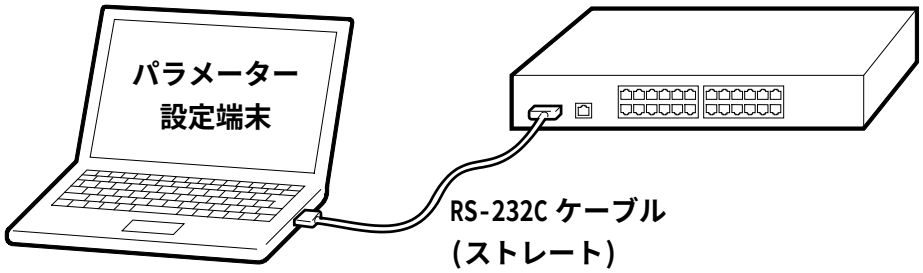


図 1-1 RS-232C ケーブルの接続

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。

```
                ApresiaLightGM110GT-SS Gigabit Ethernet Switch
                        Command Line Interface

                             Firmware: 1.13.00
          Copyright(C) 2019 APRESIA Systems, Ltd. All rights reserved.
UserName:adpro
PassWord:

#
```

2.2.2 初期化アカウント ap_recovery

Ver. 1.01.00 から実装された「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設定、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。

```
                ApresiaLightGM124GT-SS Gigabit Ethernet Switch
                        Command Line Interface

                             Firmware: 1.13.00
          Copyright(C) 2019 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	コマンド呼び出しモードに入り、現在のセッションのコマンド履歴から、前に入力したコマンドを呼び出します。以前に使用したコマンドの確認や再利用（同一コマンドの再入力、一部編集して再入力）の際に使用します。コマンド呼び出しモードでは、最初は直前に入力したコマンドが表示され、上向き矢印キーを押すたびに履歴が古いコマンドに順次切り替わります。履歴が新しいコマンドに切り替える際には下向き矢印キーを使用します。
下向き矢印キー	コマンド呼び出しモードで、履歴が新しいコマンドを呼び出します。下向き方向キーを押すたびに履歴が新しいコマンドに順次切り替わります。
Tab キー	コマンドのキーワード補完を行います。

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．1.13)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 ケーブル診断コマンド

3.1.1 cable_diag ports

目的	ツイストペアケーブルの接続をテストします。ツイストペアケーブルにエラーが確認された場合、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	ツイストペアケーブルを診断します。ケーブル診断は、各ツイストペアに診断信号を送信し、応答を見ることで行われます。診断結果では、ケーブルの各ツイストペアに対して「OK」「Open」などの診断が行われ、総合的なテスト結果を表示します。 すべてのツイストペアに対して「OK」の診断が行われた場合、該当ポートのテスト結果に「OK」と表示されます。該当ポートにケーブルが接続されていないと判断した場合、「No cable」と表示されます。リンクパートナーが接続されていない状態で短いケーブルを接続した場合にも「No cable」と表示されることがあります。いずれかのツイストペアでエラーが確認された場合、テスト結果では対応するツイストペアとその結果を表示します。代表的なエラータイプには「Open」「Short」があります。 このうち「Open」は、ツイストペアが所定の場所で電気的に切断されていることを示します。これは、ツイストペア断線などが原因の可能性もありますが、例えばリンクパートナーが接続されていない状態でケーブルを接続している場合にも表示されることがあり、「Open」の状態が必ずしもケーブルの異常を示すとは限りません。リンク状態や物理的な結線など、総合的な判断が必要です。それ以外のエラータイプ（「Short」など）が表示された場合、ケーブルや装置になんらかの問題がある疑いがあります。
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	1.00.01 以降

使用例:ポート 1～3 のツイストペアケーブル診断を行うには

```
#cable_diag ports 1-3
Command: cable_diag ports 1-3

 Perform Cable Diagnostics ...

 Port   Type      Link Status          Test Result           Cable Length (M)
 ----  -------  --------------  -------------------------  -----------------
  1     GE         Link Up       OK                                0
  2     GE         Link Down     No Cable                          -
  3     GE         Link Down     Pair1 Open      at 2   M          -
                                 Pair2 Open      at 1   M
                                 Pair3 Open      at 1   M
                                 Pair4 Open      at 2   M


#
```

注意事項

ApresiaLightGM124GT-SS 及び ApresiaLightGM124GT-PoE では、ポート 22 のケーブル診断は 1Gbps でリンクアップしている場合に限り、使用可能です。

本テストの実行時には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。

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。

光ファイバーケーブルを接続しているポートは本テストの対象にはなりません。

3.2 基本的な IP コマンド

3.2.1 config ipif

目的	IP アドレス情報を設定します。
構文	config ipif System < *ipaddress* | *vlan* | *state* | bootp | dhcp | ipv6 >> *ipaddress* =ipaddress <network_address> *vlan* = vlan <vlan_name 32> *state* = state < enable | disable > *ipv6* = ipv6 <ipv6networkaddr>
説明	本コマンドではスイッチの IP インターフェースを設定し、IP アドレス情報を登録します。IP アドレスはいずれかの VLAN に作成される IP インターフェースに設定されます。IP アドレスの指定方法は①手動(IPv4,v6)、②BOOTP、③DHCP、から選択できます。
パラメーター	ipaddress <network_address> - スイッチに設定する IPv4 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.1.11 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 IP アドレスが 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 <vlan_name 32> - IP インターフェースを作成する VLAN 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。無効にすると、IP アドレスの設定に関わらず、スイッチとの IP 通信が行えなくなります。 bootp - スイッチに IP アドレスを割り当てる方法として BOOTP プロトコルを選択します。 dhcp - スイッチに IP アドレスを割り当てる方法として 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。
制限事項	管理者アカウント「3.3.1 参照」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:スイッチに IP アドレスを設定するには

```
#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.1.08 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.1.08 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.1.08 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	IP アドレス情報を表示します。
構文	show ipif
説明	本コマンドは、スイッチの IP アドレス情報を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:スイッチの IP アドレス情報を表示するには

```
#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
Link Status     : Link DOWN
Member Ports    : 1-24
Total Entries : 1

#
```

3.3 基本的なスイッチコマンド

3.3.1 create account

目的	新規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、新規アカウントを作成します。作成するアカウントには、与える権限によって管理者アカウントとユーザーアカウントのいずれかを指定します。ユーザー名とパスワードは最大 15 文字が使用できます。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	1.00.01 以降

使用例:ユーザー名「APS」の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	アカウントのパスワードを変更します。
構文	config account <username>
説明	本コマンドは、作成済のアカウントのパスワードを変更します。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> - 登録されてい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。 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	1.00.01 以降

使用例:ユーザー名「APS」の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	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、スイッチのアカウント情報を表示します。ユーザー名と権限が表示されます。パスワードは表示されません。
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	1.00.01 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	アカウントを削除します。
構文	delete account <username>
説明	本コマンドは、登録されているアカウントを削除します。adpro も含めた全てのアカウントを削除すると任意のユーザー名、パスワードで装置にログインできることになります。
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	1.00.01 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	ログインユーザーを表示します。
構文	show session
説明	本コマンドは、現在ログイン中のユーザーをリストで表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 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	スイッチの基本情報を表示します。
構文	show switch
説明	本コマンドは、スイッチの基本情報を表示します。MAC アドレス、シリアル番号などの固有情報や機種名、その他の装置情報が表示されます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 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         : APLGM124GTSS 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   : 1.00.01
Firmware Version    : 1.13.00
System Name         :
System Location     :
System Contact      :
Serial Number       : 170892130007
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
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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、コンソールケーブル経由で行うシリアルポート通信に関する設定を表示します。
パラメーター	なし。
制限事項	なし
対応バージョン	1.00.01 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行います。
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、コンソールケーブル経由で行うシリアル通信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[bps]を指定します（1.5「パラメーター設定端末の準備」参照)。デフォルト設定は 9600 です。 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	1.00.01 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

Success.

#
```

3.3.9 enable clipaging

目的	コマンド表示情報をページ単位で表示させます。
構文	enable clipaging
説明	本コマンドは、コマンド表示情報が 1 画面以上となる場合に、自動スクロールさせずにページ単位で表示させます。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	1.00.01 以降

使用例:コマンド表示結果が 1 画面以上の場合に、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	コマンド表示情報を自動ページ送りで表示させます。
構文	disable clipaging
説明	本コマンドは、コマンド表示情報が 1 画面以上となる場合に、自動的にページ送りして表示します。
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	1.00.01 以降

使用例:コマンドの出力結果が 1 画面以上の場合に、表示を自動送りするには

```
#disable clipaging
Command: disable clipaging

Success.

#
```

3.3.11 enable telnet

目的	Telnet 管理機能を有効にします。
構文	enable telnet [<tcp_port_number 1-65535>]
説明	本コマンドは、Telnet によるスイッチの管理通信を有効にします。スイッチの Telnet 待ち受け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。省略すると 23 が使用されます。
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	1.00.01 以降

使用例:Telnet を有効にし、ポート番号「10023」を設定するには

```
#enable telnet 10023
Command: enable telnet 10023

Success.

#
```

3.3.12 disable telnet

目的	Telnet 管理機能を無効にします。
構文	disable telnet
説明	本コマンドは、Telnet によるスイッチの管理通信を無効にします。
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	1.00.01 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 で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 クライアント機能を使用してスイッチからリモートデバイスに接続します。
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。省略すると 23 を使用します。
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。 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	1.00.01 以降

使用例:Telnet で IP アドレス(10.53.13.99)のデバイスに、TCP ポート 10023 で接続するには

```
#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。Web ベース GUI では Web ブラウザを使用したスイッチの操作が可能です。Web ベース GUI で使用する 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。省略すると 80 が使用されます。
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	1.00.01 以降

使用例:HTTP を有効にし、ポート番号「10080」を設定するには

```
#enable web 10080
Command: enable web 10080

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

#
```

3.3.15 disable web

目的	Web ベース GUI を無効にします。
構文	disable web
説明	本コマンドは、スイッチの Web ベース GUI を無効にします。スイッチの操作は、コマンドラインインターフェースで実行可能になります。
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: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	設定情報を保存します。
構文	save [< config | log | all >]
説明	本コマンドは、現在の設定情報やログを NV-RAM に保存します。保存された設定情報は、スイッチが起動する際に起動時設定として使用されます。
パラメーター	config - 現在の設定情報を NV-RAM に保存します。 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 - 現在の設定情報とログの両方を NV-RAM に保存します。 パラメーターを指定しない場合、設定情報のみ保存されます。
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	1.00.01 以降

使用例:NV-RAM にスイッチの現在の設定情報を保存するには

```
#save config
Command: save config

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 に現在の設定情報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	再起動を実行します。
構文	reboot [force_agree]
説明	本コマンドは、ソフトリセットによる再起動を行います。
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	1.00.01 以降

使用例:スイッチを再起動するには

```
#reboot
Command: reboot

Are you sure you want to proceed with the system reboot?(Y|N)
Please wait, the switch is rebooting...
```

注意事項

reboot コマンドを使用せず電源を切断して機器を再起動する場合には、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	設定の初期化を行います。
構文	reset [config | system] [force_agree]
説明	本コマンドは、スイッチの初期化を行います。適用する内容や再起動有無などでいくつかのオプションを選択することができます。
パラメーター	config -現在のすべての設定(IP アドレス、アカウント)が初期値に戻り、スイッチ履歴ログがクリアされます。設定は即時反映されますが、NV-RAM には保存されません。また、再起動は行われません。 system - スイッチの設定が初期値に戻り、再起動します。設定は NV-RAM に保存されます。 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。 config、system いずれのパラメーターも指定しない場合、スイッチの IP アドレス、アカウント以外の設定が初期値に戻ります。また、スイッチ履歴ログはクリアされません。設定は即時反映されますが、設定は NV-RAM に保存されません。また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	1.00.01 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設定を初期化するには

```
#reset
Command: reset

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

#
```

使用例:すべての設定を初期値に戻すには

```
#reset config
Command: reset config

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

Success.

#
```

使用例:すべての設定を初期値に戻し、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。アカウントの切り替えなどの際に使用します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 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 Telnet や SSH で接続している場合、セッションが切断されます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 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。転送処理可能なサイズは製品によって異なり、ApresiaLightGM シリーズ製品では最大 9216 バイト(タグ付き)まで中継します。
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

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、ジャンボフレーム機能を無効に設定します。1522 バイト(タグ付き)以下のフレームのみ中継処理を行います。
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設定の設定を表示します。また、ジャンボフレーム機能を有効にした場合の最大フレームサイズを表示します。
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	1.00.01 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   : 9216 Bytes

#
```

3.3.24 config default_language

目的	Web ベース GUI 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 ベース GUI の表示画面での言語モードを設定します。 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	1.00.01 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 ベース GUI 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 ベース GUI の表示画面での言語モードを表示します。
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	1.00.01 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	1.00．01 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

================================================================================
                      APLGM124GTSS Gigabit Ethernet Switch
                      Technical Information Report
================================================================================
[CPU Utilization 109089150ms]
CPU Utilization :
--------------------------------------------------------------------------------
Five Seconds -   7 %         One Minute -   3 %         Five Minutes -   4 %

[Device Information 109089350ms]
Device Type         : APLGM124GTSS 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 1.00.01
Firmware Version    : Build 1.13.00
Hardware Version    : A
Serial number       : 170892130007
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
Syslog Global State: Disabled
Dual Image          : Supported
```

```
[Connection Session Status 109089550ms]
ID   Login Time           Live Time        From          Level   Name
--  ------------------  -----------  --------------  -----  --------------
8   0/00/01  05:18:03    0:0:5.280     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	1.08.00 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_support.txt
Command: upload tech_support_toTFTP 10.0.0.66 tech_support.txt

Collect technical support information .....................
Prepare the uploaded file .....................
Connecting to server................... Done.
Upload technical support information... 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。

コンソールポートより upload tech_support_toTFTP コマンドの実行中に何かキーが入力されると、コマンド実行を中止します。

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：aplgmR11300.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 を指定することによって、2 種類のファームウェアバージ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	1.00.01 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 サーバーから設定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] >
説明	本コマンドは、TFTP サーバーから設定ファイルをダウンロードして、現在の設定に反映します。NV-RAM には保存されませんのでご注意ください。
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。
制限事項	管理者アカウン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

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切断されます。

使用例:設定ファイルを TFTP サーバーからダウンロードするには

```
#download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt
Command: download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt

Connecting to server................... Done.
Download configuration.................. Done.
Success.
#
##------------------------------------------------------------------
##                        APLGM124GTSS Configuration
##
##                        Firmware: 1.13.00
##        Copyright(C) 2019 APRESIA Systems, Ltd. All rights reserved.
##------------------------------------------------------------------
#
#
## BASIC
#
#config serial_port baud_rate 9600 auto_logout 10_minutes
Command: config serial_port baud_rate 9600 auto_logout 10_minutes
```

本コマンドによって、設定ファイルの各設定順に様々な設定のダウンロードが開始されます。ダウンロードが完了すると、「End of configuration file for APLGM124GTSS」のメッセージが表示され、コマンドプロンプトが続きます。

```
#disable authen_policy
Command: disable authen_policy

Success.

#
```

3.4.3 config firmware image_id

目的	次回起動時に展開するファームウェアの選択、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	ApresiaLightGM シリーズでは、内部に 2 つのファームウェアを格納することが可能で、それぞれセクション ID(1,2)で識別されます。 本コマンドは、次回起動時に展開するファームウェアをセクション ID で指定します。または、セクション ID を指定して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	1.00.01 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

なんらかの異常により、指定したセクション ID 番号のファームウェアで起動できない場合、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	ファームウェアの情報を表示します。
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情報を表示します。ファームウェアの情報は、保存している各セクションごとに表示されます。
パラメーター	なし。
制限事項	なし
対応バージョン	1.00.01 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情報を表示するには

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

Image ID    : 1(Boot up firmware)
Version     : 1.13.00
Size        : 3564448 Bytes
Update Time: 2019/12/28 14:54:54
User        : adpro(CONSOLE)

Image ID    : 2
Version     : 1.13.00
Size        : 3564448 Bytes
Update Time: 2019/12/28 14:43:43
User        : adpro(CONSOLE)

#
```

3.4.5 show config

目的	スイッチが現在動作している、または保存されている設定情報を表示します。	
構文	show config < current_config | config_in_nvram > [modified]	
説明	本コマンドは、スイッチが現在動作している設定情報、または NV-RAM に保存されている設定情報(起動時設定)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。 設定情報は、以下の順でカテゴリ別にリストされます。	
	# BASIC # UTILIZATION_NOTIFY # STORM # LOOP_DETECT # QOS # MIRROR # BANDWIDTH # SYSLOG # TRAF-SEGMENTATION # SSL # POE # DDM # MANAGEMENT # SNMPv3 # VLAN # PROTOCOL_VLAN # 8021X # PORT_LOCK # LACP # STP	# BPDU_PROTECTION # BANNER_PROMP # SSH # SNOOP # FDB # SMTP # ACL # SNTP # IP # MBA # LLDP # MLDSNP # ARP # AAA # DHCPSNP # Web_Authentication # ROUTE # NDP # MULTI_AUTHENTICATION # PORT
パラメーター	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。 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。	
制限事項	管理者アカウ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	

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:現在の設定情報をすべて表示するには

```
#show config config_in_nvram
Command: show config config_in_nvram
#------------------------------------------------------------------
#                       APLGM124GTSS Configuration
#
#                       Firmware: 1.13.00
#        Copyright(C) 2019 APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------


# BASIC

config serial_port baud_rate 9600 auto_logout 10_minutes
config default_language japanese
config terminal_line default
enable clipaging
enable command logging

# UTILIZATION_NOTIFY

config utilization notify cpu state enable threshold 100 polling_interval 60 trap_state disable
log_state enable

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

使用例:デフォルト状態から変更された現在の設定情報を表示するには

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



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



#
```

3.4.6 upload

目的	設定情報またはログ情報を TFTP サーバーにアップロードします。
構文	upload < cfg_toTFTP | log_toTFTP > < <ipaddr> | <ipv6addr> > <path_filename 64>
説明	本コマンドは、スイッチの設定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。テクニカルサポート情報のアップロードは「3.3.27 upload tech_support_toTFTP」を参照してください。
パラメーター	cfg_toTFTP - スイッチの設定情報を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> - アップロード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	1.00.01 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:設定情報を TFTP サーバーに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
Success.
Connecting to server................... Done.
Upload configuration...................Done.

#
```

3.4.7 ping

目的	ping を実行します。
構文	ping <ipaddr> [times <value 0-255>] [size <value 1-60000>] [timeout <sec 1-99>]
説明	ping は、リモートデバイスに Internet Control Message Protocol(ICMP)エコーメッセージを送信し、デバイスの応答を確認することで、スイッチとデバイス間の接続性をテストします。本コマンドを実行すると、ping を実行してその結果を表示します。
パラメーター	<ipaddr> - リモートホストの IP アドレスを指定します。 times <value 0-255> - 送信する各 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> - テスト用パケットの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	1.00.01 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 で ping を実行します。
構文	ping6 <ipv6addr> [times <value 1-255> | size <value 1-6000> | timeout <value 1-10>]
説明	本コマンドを実行すると、IPv6 アドレスのリモートデバイスに ping を実行してその結果を表示します。
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> - 送信する各 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 <value 1-10> - 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。1～10 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	1.00.01 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	traceroute を実行します。
構文	traceroute <ipaddr> [ttl <value 1-60>] [port <value 30000-64900>] [timeout <sec 1-65535>] [probe <value 1-9>]
説明	traceroute は UDP と ICMP によりリモートデバイスへの経路情報を取得する診断コマンドです。本コマンドは、traceroute を実行して結果を表示します。
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> - 応答待ち時間を入力します。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	1.00.01 以降

使用例:リモートデバイス(10.48.74.121)に traceroute を実行するには

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

1  <10 ms.     10.48.74.121
1  <10 ms.     10.48.74.121

#
```

3.4.10 config terminal line

目的	コマンドの表示行数を設定します。
構文	config terminal_line < default | <value 20-80> >
説明	本コマンドは、コマンドラインインターフェースでの表示行数を指定します。
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	1.00.01 以降

使用例:画面に表示されるコマンドの行数を「30」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	コマンドの表示行数を表示します。
構文	show terminal_line
説明	本コマンドは、コマンドラインインターフェースの表示行数を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:画面に表示されるコマンドの行数を表示するには

```
# show terminal_line
Command: show terminal_line

Current terminal line number : 30

#
```

3.4.12 show self-test result

目的	起動時のセルフテスト結果を表示します。
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、POE コントローラーのセルフテストの結果を表示します。
パラメーター	なし。
制限事項	POE Test の結果は、APLGM110GTPOE、APLGM118GTPOE および APLGM124GTPOE の機種で表示されます。
対応バージョン	1.04.00 以降

使用例:セルフテストの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 モジュール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、スイッチに装着した SFP モジュール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 準拠品が対象です。型式(H-FX-SFP/R) は表示されません。
対応バージョン	1.04.00 以降

使用例:トランシーバーの光入出力レベルを表示するには

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

  Port         TX Power       RX Power
                (dBm)          (dBm)
---------   ------------  ------------
   9           -4.77          -5.35
   10          -4.98          -5.30

#
```

3.4.14 show sfp info

目的	SFP モジュール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、装着した SFP モジュール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	1.04.00 以降

使用例:トランシーバーの情報を表示するには

```
#show sfp info 10
Command: show sfp info 10

SFP Auto Recognition State: Disabled

SFP Port              : 10
Vendor Name           : FINISAR CORP.
Vendor Part Number    : FTLF8519P2BNL
Serial Number         : PC80ZMP

#
```

3.5 コマンド履歴コマンド

3.5.1 ?

目的	コマンドの説明を表示します。
構文	? [<command>]
説明	本コマンドは、指定したコマンドの候補となるパラメータやコマンドの説明などの情報を表示します。
パラメーター	[<command>] - 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とコマンド機能の簡単な説明または候補となる類似のコマンドを表示します。省略した場合には、現在のログインユーザーの権限で利用可能なコマンドの一覧を表示します。
制限事項	なし。
対応バージョン	1.00.01 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

```
#?
Command: ?


..
?
cable_diag ports
clear
clear arptable
clear counters
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_failover
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config admin local_enable
 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: config user account

#
```

3.5.2 dir

目的	コマンド一覧を表示します。
構文	dir
説明	本コマンドは、ログインユーザーの権限で利用可能なコマンドを一覧で表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:すべてのコマンドを表示するには

```
#dir
Command: dir


..
?
cable_diag ports
clear
clear arptable
clear counters
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 capability ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
```

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。本コマンドを入力した時点で表示件数以上の履歴情報がある場合、設定値を超えたコマンド履歴は削除されます。
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	1.00.01 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、現在のセッションでの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	1.00.01 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	LLDP 機能を有効にします。
構文	enable lldp
説明	本コマンドは、スイッチの 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 フレームの送受信を開始し、LLDP フレームの処理を行います。各ポートの具体的な動作や通知内容は、ポートごとの LLDP 設定に依存します。スイッチは LLDP フレームにより装置の情報ネイバー装置に通知します。スイッチはネイバー装置から LLDP フレームを受信することで、LLDP ネイバーデバイス情報を学習します。 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	1.00.01 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	LLDP 機能を無効にします。
構文	disable lldp
説明	本コマンドは、スイッチの LLDP フレーム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	1.00.01 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	LLDP フレームの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、定期的に送信する LLDP フレームの送信間隔を指定します。
パラメーター	<sec 5-32768> - 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	1.00.01 以降

使用例:LLDP フレーム送信間隔を「10」に設定するには

```
# config lldp message_tx_interval 10
Command: config lldp message_tx_interval 10

Success.

#
```

3.6.4 config lldp message_tx_hold_multiplier

目的	LLDP フレームのホールド乗数を設定します。
構文	config lldp message_tx_hold_multiplier <int 2-10>
説明	LLDP の通知情報には有効期限(TTL)があり、LLDP 対応デバイスは TTL に基づき定期的に LLDP フレームを Keep-Alive として送信します。 本コマンドは、スイッチが通知する TTL の算出に使用するホールド乗数を指定します。スイッチは LLDP フレームの送信間隔とホールド乗数の乗算(もしくは 65535 秒のいずれか小さい方)を TTL として使用します。ネイバー装置は、スイッチからの LLDP フレームが途絶えた場合、通知された TTL が経過した後にその LLDP ネイバーデバイス情報を削除します。 言い換えると、ホールド乗数はネイバー装置が Keep-Alive を受信できない状況で、連続して何回まで受信失敗を許容するかを定める値です。ネイバー装置がホールド乗数と同じ回数だけ連続して Keep-Alive の受信に失敗した場合、ネイバー装置は LLDP フレーム内で通知された TTL を元に失効処理を行い、スイッチの LLDP ネイバーデバイス情報を削除します。
パラメーター	<int 2-10> - 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	1.00.01 以降

使用例:LLDP フレームのホールド乗数を「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 フレームの送信遅延時間を設定します。
構文	config lldp tx_delay <sec 1-8192>
説明	本コマンドは、LLDP フレームの送信遅延時間を設定します。送信遅延時間は、通知情報が非常に短期間に連続して変更される環境で、状態が安定するまで LLDP フレームの送信を遅らせる役割があります。 LLDP フレームの送信間隔は遅延時間の 4 倍以上である必要があります。
パラメーター	<sec 1-8192> - 範囲は 1 秒から 8192 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	1.00.01 以降

使用例:LLDP フレームの送信遅延時間を「8」に設定するには

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

Success.

#
```

3.6.6 config lldp reinit_delay

目的	装置の LLDP 再初期化遅延期間を設定します。
構文	config lldp reinit_delay <sec 1-10>
説明	本コマンドは、LLDP を無効にした後に再び LLDP を有効にする(再初期化)場合の最小待ち時間を設定します。
パラメーター	<sec 1-10> - 範囲は 1 秒から 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	1.00.01 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 ports notification

目的	LLDP 変更通知を行うポートを設定します。
構文	config lldp ports < <portlist> | all > notification < enable | disable >
説明	本コマンドでは、LLDP 変更通知を行うポートを指定します。LLDP 変更通知は、LLDP ネイバーデバイス情報が変更された場合に、SNMP トラップを送信します。変更には新規ネイバーデバイス情報の登録や、一部情報の更新/挿入/削除、失効が含まれます。
パラメーター	<portlist> | all - 設定するポート範囲を指定します。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 - 対象ポートでの LLDP 変更通知を有効または無効にします。 デフォルト設定は、すべてのポートで「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	1.00.01 以降

使用例:ポート 1-5 の LLDP 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.

#
```

3.6.8 config lldp notification_interval

目的	LLDP 変更通知の最小送信間隔を設定します。
構文	config lldp notification_interval <sec 5 - 3600>
説明	本コマンドは、LLDP 変更通知で送信する SNMP トラップの最小送信間隔を指定します。この送信間隔は、短期間に連続して LLDP ネイバーデバイス情報変更が発生した場合に、SNMP トラップの集中を緩和する役割があります。
パラメーター	<sec 5 - 3600> - 範囲は 5 秒から 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	1.00.01 以降

使用例:LLDP 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.

#
```

3.6.9 config lldp ports admin_status

目的	各ポートの LLDP 送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 送受信モードを設定します。ポート単位で LLDP フレームの送信を行うかどうか、あるいは受信した LLDP フレームを参照してネイバーデバイス情報を更新するかどうかを指定することができます。
パラメーター	<portlist> | all - 設定するポート範囲を指定します。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 | rx_only | tx_and_rx | disable > tx_only - LLDP フレームを送信しますが、受信 LLDP フレームは無視します。 rx_only - 受信 LLDP フレームを参照しますが、LLDP フレームを送信しません。 tx_and_rx - LLDP フレームの送受信処理を行います。 disable - LLDP フレームを送信せず、受信 LLDP フレームは無視します。 デフォルトではすべてのポートで「tx_and_rx」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	1.00.01 以降

使用例:ポート 1-5 の LLDP 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	LLDP 管理アドレス情報の通知に関する設定を行います。
構文	config lldp ports < <portlist> | all > mgt_addr ipv4 <ipaddr> < enable | disable >
説明	本コマンドは、管理アドレスに関する LLDP 通知の設定を行います。各ポートで通知する LLDP 情報にシステムの管理アドレスを含めるかどうかを指定することができます。管理アドレスのインターフェースは ifIndex 形式で通知します。
パラメーター	<portlist> | all - 設定するポート範囲を指定します。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。 <ipaddr> - IPv4 の IP アドレスを入力します。この IP アドレスは、システムに設定された IP アドレスと一致する必要があります。 < enable | disable > - 指定したポートで有効/無効を設定します。
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	1.00.01 以降

使用例:ポート 1-2 の LLDP 情報に管理アドレスを含めるためには

```
# 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	LLDP の基本管理 TLV 情報の通知に関する設定を行います。
構文	config lldp ports < <portlist> | all > basic_tlvs < all | < port_description | system_name | system_description | system_capabilities > > < enable | disable >
説明	LLDP 基本管理 TLV は、IEEE802.1AB で定める LLDP での基本的な通知情報です。LLDP で TLV(Type Length Value)は、LLDP フレームに含まれる通知情報を指します。基本管理 TLV には、例えば TTL のような必ず含まれる基本的な通知情報の他に、4 つのオプション通知情報(ポートの説明(Port Description)、システム名(System Name)、システムの説明(System Description)、システムサポート情報(System Capability))があります。本コマンドでは、各オプション通知情報をポート単位で通知するかどうかを設定することができます。
パラメーター	<portlist> | all - 設定するポート範囲を指定します。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。 all | <port_description | system_name | system_description | system_capabilities> - 通知する情報を指定します。すべての情報を指定する場合には「all」を使用します。 port_description - Port Description 情報の通知を指定します。 system_name - System Name 情報の通知を指定します。 system_description - System Description 情報の通知を指定します。 system_capabilities - System Capability 情報を通知します。スイッチが通知する情報は、「Repeater」「Bridge」です。 < enable | disable > - 指定したポート、通知情報の有効/無効を設定します。デフォルトでは、すべてのポートですべての通知情報が「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	1.00.01 以降

使用例:すべてのポートに対して LLDP 通知情報にシステム名を含めるには

```
# 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	LLDP の IEEE802.1 TLV(ポート VLAN ID)の通知に関する設定を行います。
構文	config lldp ports < <portlist> | all > dot1_tlv_pvid < enable | disable >
説明	LLDP では、IEEE802.1AB で定められる基本管理 TLV の他に、拡張 TLV と呼ばれるオプション情報を通知することができます。IEEE802.1 で定められる拡張 TLV の中には PVID(Port VLAN ID)が含まれます。 本コマンドでは、PVID 情報をポート単位で通知するかどうかを設定することができます。
パラメーター	<portlist> | all - 設定するポート範囲を指定します。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。 < enable | disable > - 指定したポートで有効/無効を設定します。 デフォルトでは、すべてのポートで「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	1.00.01 以降

使用例:すべてのポートに対して LLDP 通知に IEEE802.1 TLV の PVID 情報を含めるには

```
# 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	LLDP の IEEE802.1 TLV(Protocol VLAN ID)の通知に関する設定を行います。
構文	config lldp ports < <portlist> | all > dot1_tlv_protocol_vid < vlan < all | < vlan_name 32 > > | vlanid <vlanid_list> > < enable | disable >
説明	本コマンドでは、IEEE802.1 で定められる拡張 TLV のうちの Protocol VLAN ID 情報をポート単位で通知するかどうかを設定します。Protocol VLAN ID 情報は VLAN 単位で通知するかどうかを指定することができます。
パラメーター	<portlist> | all - 設定するポート範囲を指定します。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。 all | < vlan_name 32 > - 通知する VLAN を設定します。すべての VLAN を通知する場合には、「all」のパラメーターを使用します。 vlanid_list - 通知する VLAN を VLAN ID のリストで指定します。 < enable | disable > - 指定したポート、VLAN で有効/無効を設定します。 デフォルトでは、すべてのポートですべての VLAN が「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	1.00.01 以降

使用例:すべてのポートに対して LLDP 通知に IEEE802.1 TLV の Protocol VLAN ID 情報を含めるには

```
#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	LLDP の IEEE802.1 TLV(VLAN Name)の通知に関する設定を行います。
構文	config lldp ports < <portlist> | all > dot1_tlv_vlan_name < vlan < all | <vlan_name 32> > | vlanid <vidlist> > < enable | disable >
説明	本コマンドでは、IEEE802.1 で定められる拡張 TLV のうちの VLAN 名情報をポート単位で通知するかどうかを設定します。VLAN 名情報は VLAN 単位で通知するかどうかを指定することができます。
パラメーター	<portlist> | all - 設定するポート範囲を指定します。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。 all | < vlan_name 32 > - 通知する VLAN を指定します。すべての VLAN を通知する場合は、「all」を指定します。 < vlanid_list > - 通知する VLAN を VLAN ID のリストで指定します。 < enable | disable > - 指定したポート、VLAN 名で有効/無効を設定します。 デフォルトでは、すべてのポートですべての VLAN が「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	1.00.01 以降

使用例: LLDP 通知に IEEE802.1 TLV の VLAN 名情報を含めるには

```
# 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	LLDP の IEEE802.1 TLV(Protocol ID)の通知に関する設定を行います。
構文	config lldp ports < <portlist> | all > dot1_tlv_ protocol_identity < all | [eapol | lacp | gvrp | stp] > <enable | disable>
説明	本コマンドでは、IEEE802.1 で定められる拡張 TLV のうちの Protocol ID 情報をポート単位で通知するかどうかを設定します。通知するプロトコルは EAPOL、GVRP、STP、LACP で、個別に通知するかどうかを指定することができます。
パラメーター	<portlist> | all - 設定するポート範囲を指定します。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。 < all | [eapol | lacp | gvrp | stp] > - 通知するプロトコルを指定します。すべてのプロトコルを設定する場合は「all」のパラメーターを使用します。 < enable | disable > - 指定したポート、プロトコルで有効/無効を設定します。デフォルトでは、すべてのポートですべてのプロトコルが「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	1.00.01 以降

使用例:すべてのポートに対して LLDP 通知に IEEE802.1 TLV の Protocol ID 情報を含めるには

```
# 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	LLDP の IEEE802.3 TLV の通知に関する設定を行います。
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	本コマンドでは、IEEE802.3 で定められる拡張 TLV の情報をポート単位で通知するかどうかを設定します。システムが通知する IEEE802.3 TLV の情報には、MAC/PHY 設定状態(MAC/PHY Configuration/Status)、リンクアグリゲーション(Link Aggregation)、PoE 状態(Power via MDI)、最大フレームサイズ(Maximum Frame Size)があり、各情報をポート単位で通知するかどうかを設定することができます。
パラメーター	<portlist> | all - 設定するポート範囲を指定します。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。 < all | [mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size] > - 通知する情報を指定します。すべての情報を指定する場合は、「all」を使用します。 mac_phy_configuration_status - MAC/PHY 設定状態の通知を指定します。 link_aggregation - リンクアグリゲーション情報の通知を指定します。 power_via_mdi - PoE 状態の通知を指定します。 maximum_frame_size - 最大フレームサイズの通知を指定します。 < enable | disable > - 指定したポート、通知情報の有効/無効を設定します。 デフォルトでは、すべてのポートですべての通知情報が「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	1.00.01 以降

使用例:すべてのポートに対して LLDP 通知に IEEE802.3 TLV の MAC/PHY 設定状態を含めるには

```
#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 フレームの転送を設定します。
構文	config lldp forward_message < enable | disable >
説明	本コマンドでは、LLDP フレームの転送動作についての設定を行います。LLDP フレーム転送が有効の場合、LLDP 機能自体が無効であれば受信した LLDP フレームを他のポートに転送できます。LLDP フレーム転送が無効の場合は、受信した LLDP フレームはスイッチで終端され、他のポートには転送されません。 デフォルトでは「disable」(無効)です。
パラメーター	< enable | disable > - 転送する/しないを設定します。
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	1.00.01 以降

使用例:LLDP フレーム転送を有効にするには

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

Success.

#
```

3.6.18 show lldp

目的	LLDP 状態を表示します。
構文	show lldp
説明	本コマンドは、スイッチの LLDP 状態を表示します。LLDP のグローバルな設定情報の他に、基本管理 TLV で通知される情報も含まれます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:LLDP 状態を表示するには

```
#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 管理アドレス通知情報を表示します。
構文	show lldp mgt_addr [ipv4 <ipaddr>]
説明	本コマンドは、スイッチの LLDP 管理アドレスのグローバルな通知情報を表示します。
パラメーター	ipv4 - IPv4 の IP アドレスを指定します。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例: LLDP 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                          : Unknown
    OID                              : 1.3.6.1.4.1.278.1.35.106
    Advertising Ports                :

#
```

3.6.20 show lldp ports

目的	LLDP のポート設定情報を表示します。
構文	show lldp ports [<portlist>]
説明	本コマンドは、各ポートの LLDP 設定や通知設定を表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。省略した場合、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	1.00.01 以降

使用例:ポート 1 の LLDP ポート設定情報を表示するには

```
# 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
    Power Via MDI                                       Disable
    Link Aggregation                                    Disable
    Maximum Frame Size                                  Disable
#
```

3.6.21 show lldp local_ports

目的	LLDP の通知情報をポートごとに表示します。
構文	show lldp local_ports [<portlist>] [mode < brief | normal | detailed >]
説明	本コマンドは、各ポートで通知する LLDP の具体的な情報を表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。省略した場合は、すべてのポートの情報が表示されます。 < brief | normal | detailed > - 表示モードを指定します。モードによって、表示される情報量が異なります。 brief - 簡易モードで情報を表示します。 normal - 通常モードで情報を表示します。 detailed - 詳細モードで情報を表示します。 モードを省略すると、通常モードで情報を表示します。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:ポート 1 の LLDP 通知情報を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 APLGM124GTSS R1.13 Port 1

#
```

使用例:ポート 1 の LLDP 通知情報を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 APLGM124GTSS R1.13 Port 1
Port VLAN ID                             : 1
Management Address Count                 : 0
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                       : 1536

#
```

使用例:ポート 1 の LLDP 通知情報を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 APLGM124GTSS R1.13 Port 1
Port VLAN ID                             : 1
Management Address Count                 : 0
    (NONE)
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  : 0000(hex)

Power Via MDI                            : Not Supported

Link Aggregation                         :
    Aggregation Capability               : Aggregated
    Aggregation Status                   : Not Currently In Aggregation
    Aggregation Port ID                  : 1

Maximum Frame Size                       : 1536

#
```

3.6.22 show lldp remote_ports

目的	LLDP ネイバーデバイス情報を表示します。
構文	show lldp remote_ports [<portlist>] [mode < brief | normal | detailed >]
説明	本コマンドは、受信した LLDP フレームで得られたネイバーデバイス情報を表示します。ネイバーデバイス情報では、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格納できます。
パラメーター	<portlist> - 表示するポート範囲を指定します。省略した場合は、すべてのポートの情報が表示されます。 < brief | normal | detailed > - 表示モードを指定します。モードによって、表示される情報量が異なります。 brief - 簡易モードで情報を表示します。 normal - 通常モードで情報を表示します。 detailed - 詳細モードで情報を表示します。 モードを省略すると、通常モードで情報を表示します。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:ポート 1 のネイバーデバイス情報を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:ポート 1 のネイバーデバイス情報を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                      :
    System Capabilities                     :
    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

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

使用例:ポート 1 のネイバーデバイス情報を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、LLDP ネイバーデバイス情報履歴の統計を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:LLDP 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	ポートでの 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、ポートでの LLDP 情報の統計を表示します。LLDP フレームの受信件数などの情報が表示されます。
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	1.00.01 以降

使用例:ポート 1 の LLDP 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	本コマンドでは、コマンドプロンプトを変更します。また、ログインユーザー名を使用するように設定することも可能です。
パラメーター	<<string 16> | username | default> <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状態にリセットされます。
対応バージョン	1.00.01 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、ログイン時に表示されるバナーを設定します。バナーの詳細な設定はバナーエディタで行います。
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状態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	1.00.01 以降

使用例:ログインバナーを編集するには

```
#config greeting_message
Command: config greeting_message

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


                ApresiaLightGM124GT-SS Gigabit Ethernet Switch
                           Command Line Interface

                                Firmware: 1.13.00
      Copyright(C) 2019 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	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ログインバナーを表示します。バナーを変更した際に確認する場合などに使用します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:ログインバナーを表示するには

```
#show greeting_message
Command: show greeting_message


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

                ApresiaLightGM124GT-SS Gigabit Ethernet Switch
                        Command Line Interface

                             Firmware: 1.13.00
       Copyright(C) 2019 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	コミュニティー名	コミュニティー名は認証に使用されます- NoAuthNoPriv
v2c	コミュニティー名	コミュニティー名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	新規 SNMP ユーザーを登録します。
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。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	1.00.01 以降

使用例:新規 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 ユーザーを削除します。
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	1.00.01 以降

使用例: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 ユーザーの情報を表示します。
構文	show snmp user
説明	本コマンドは、登録されている SNMP ユーザー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	1.00.01 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	SNMP ビューエントリーを登録します。
構文	create snmp view <view_name 32> <oid> view_type < included | excluded >
説明	SNMP ビューは、スイッチの MIB に対する SNMP マネージャーのアクセスを制限するための、MIB オブジェクトの範囲を指定するものです。コミュニティ名やグループ名と紐づけられて、それぞれのアクセス範囲を指定します。 SNMP ビューは、OID とビュータイプの組み合わせによる複数エントリーで構成されます。各エントリーでは、指定した OID 以下の MIB オブジェクトに対し、included（アクセス可能）もしくは exlcuded(アクセス禁止)というルールを指定します。一つのビューの複数エントリーで競合するルールが存在する場合は、OID が長いエントリーのルールが優先されます。 本コマンドは、SNMP ビューエントリーを登録します。同じビュー名のエントリーが存在していても、OID が完全に一致していなければ、異なるエントリーとして登録されます。
パラメーター	<view_name 32> - SNMP ビュー名を入力します。 <oid> - SNMP ビューエントリーの OID を指定します。 view type - 以下のビュータイプを選択します。 included - SNMP マネージャーからのアクセスを許可します。 excluded - SNMP マネージャーからのアクセスを許可しません。
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	1.00.01 以降

使用例:OID「1.3.6」以下の MIB オブジェクトへのアクセスを許可するエントリーを作成するには

```
#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	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、登録された SNMP ビューエントリーを削除します。指定した SNMP ビューの一つのエントリー、もしくはすべてのエントリーを削除できます。
パラメーター	<view_name 32> - SNMP ビュー名を入力します。 all - 指定した SNMP ビューのすべてのエントリーを削除します。 <oid> - 指定した SNMP ビューの特定の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	1.00.01 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	SNMP ビューエントリーを表示します。
構文	show snmp view [<view_name 32>]
説明	本コマンドは、登録されている SNMP ビューエントリーを表示します。指定した SNMP ビューのエントリーのみを表示することもできます。
パラメーター	<view_name 32> - 表示する SNMP ビューを指定します。省略した場合はすべての SNMP ビュー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	1.00.01 以降

使用例:SNMP ビューエントリーをすべて表示するには

```
#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 コミュニティーを登録します。
構文	create snmp community <community_string 32> view <view_name 32> < read_only | read_write >
説明	SNMP コミュニティーは、SNMPv1 および v2c で SNMP マネージャーのユーザー識別に使用されます。 本コマンドでは、SNMP コミュニティーを登録し、そのユーザーに対する操作権限を SNMP ビューと権限レベルで指定します。権限レベルには「read_write」(読み書き可能) または「read_only」(読み出しのみ)があります。
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 SNMP コミュニティー名を 32 文字までの半角英数文字列を入力します。 view <view_name 32> - アクセス範囲を示す SNMP ビューを指定します。 read_only - 権限レベルを「読み出しのみ」に指定します。 read_write - 権限レベルを「読み書き可能」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	1.00.01 以降

使用例:SNMP コミュニティー「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	SNMP コミュニティーを削除します。
構文	delete snmp community <community_string 32>
説明	本コマンドは、登録されている SNMP コミュニティーを削除します。初期登録されている SNMP コミュニティーも削除することができます。
パラメーター	<community_string 32> - 削除する SNMP コミュニティーをコミュニティー名で指定します。
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	1.00.01 以降

使用例:SNMP コミュニティー「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	SNMP コミュニティーの情報を表示します。
構文	show snmp community [<community_string 32>]
説明	本コマンドは、登録されている SNMP コミュニティーを表示します。所定のコミュニティ名の情報のみを表示させることもできます。
パラメーター	<community_string 32> - 表示する SNMP コミュニティーをコミュニティー名で指定します。省略した場合はすべての SNMP コミュニティーが表示されます。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:SNMP コミュニティー「APS」の情報を表示するには

```
#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	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、SNMPv3 で使用される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	1.00.01 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	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	1.00.01 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 : 800001160300406645 99a6

#
```

3.8.12 create snmp group

目的	SNMP グループを作成します。
構文	create snmp group <groupname 32> < v1 | v2c | v3 < noauth_nopriv | auth_nopriv | auth_priv > > < read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32> >
説明	SNMP グループは、SNMP ユーザーや SNMP コミュニティーと紐づき、その権限を指定します。SNMP ユーザーは、所属する SNMP グループで指定された権限の範囲でアクセスが許可されます。 本コマンドは、SNMP グループを新規に登録します。なお、SNMP コミュニティー名を登録した場合は、同名の SNMP グループが自動的に登録されます。
パラメーター	<groupname 32> - SNMP グループ名を入力します。 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 2 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。SNMPv3 では SNMP アクセスにおいて認証と暗号化をサポートしており、認証と暗号化を使用するかどうかをパラメータで指定します。 noauth_nopriv - 認証、暗号化を行いません。 auth_nopriv - 認証を行いますが、暗号化は行いません。 auth_priv - 認証と暗号化を行います。 read_view - 読み出しアクセス範囲を示す SNMP ビューを選択します。 write_view - 書き込みアクセス範囲を示す SNMP ビューを選択します。 notify_view - SNMP トラップを送信する範囲を示すビューを選択します。 view <view_name 32> - 各アクセスに対する SNMP ビューを指定します。
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	1.00.01 以降

使用例:SNMP グループ「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	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。異なる SNMP バージョンで同一の SNMP グループ名のエントリーが存在する場合、すべてのエントリーが削除されます。
パラメーター	<groupname 32> - 削除する SNMP グループをグループ名で指定します。
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	1.00.01 以降

使用例:SNMP グループ「APS」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	SNMP グループを表示します。
構文	show snmp groups
説明	本コマンドは、登録されている SNMP グループの情報を表示します。複数の SNMP バージョンに対応する場合は、それぞれ別の情報にまとめて表示されます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 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         : Group3
ReadView Name      : ReadView
WriteView Name     : WriteView
Notify View Name   : NotifyView
Security Model     : SNMPv3
Security Level     : NoAuthNoPriv

Group Name         : Group4
ReadView Name      : ReadView
WriteView Name     : WriteView
Notify View Name   : NotifyView
Security Model     : SNMPv3
Security Level     : authNoPriv

Group Name         : Group5
ReadView Name      : ReadView
WriteView Name     : WriteView
Notify View Name   : NotifyView
Security Model     : SNMPv3
Security Level     : authNoPriv


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

Group Name         : ReadGroup
ReadView Name      : CommunityView
WriteView Name     :
Notify View Name   : CommunityView
Security Model     : SNMPv1
Security Level     : NoAuthNoPriv

Total Entries: 5

#
```

3.8.15 create snmp host

目的	SNMP トラップの送信先を設定します。
構文	create snmp < host <ipaddr> > < v1 | v2c | v3 < noauth_nopriv | auth_nopriv | auth_priv > <auth_string 32>
説明	本コマンドは、SNMP トラップの送信先ホストを設定します。指定した SNMP コミュニティー名もしくは SNMP ユーザーのアクセス範囲(所属するグループで指定されている SNMP ビュー)に応じて SNMP トラップを送信します。
パラメーター	<ipaddr> - SNMP トラップの送信先 IP アドレス。 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。 noauth_nopriv - 認証、暗号化を行いません。 auth_nopriv - 認証を行いますが、暗号化は行いません。 auth_priv - 認証と暗号化を行います。 <auth_string 32> - SNMP コミュニティー名もしくは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	1.00.01 以降

使用例:SNMP トラップの送信先を登録するには

```
#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	SNMP トラップの送信先を削除します。
構文	delete snmp < host <ipaddr> >
説明	本コマンドは、SNMP トラップの送信先のエントリーを削除します。
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。
制限事項	管理者アカウン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:SNMP トラップ送信先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	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、登録した SNMP トラップの送信先の情報を表示します。特定の送信先 IP アドレスに絞って表示することもできます。
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	1.00.01 以降

使用例: SNMP トラップ送信先の情報を表示するには

```
#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 create trusted_host

目的	トラストホストエントリーを作成します。
構文	create trusted_host < <ipaddr> | network <network_address> >
説明	本コマンドは、トラストホストを作成します。トラストホストが登録されると、指定した IP アドレス(もしくはネットワークアドレス範囲の IP アドレス)以外の IP アドレスからはネットワーク経由でアクセスできなくなります。トラストホストの登録は最大 10 個まで可能です。
パラメーター	<ipaddr> - トラストホストの IP アドレスを指定します。 <network_address> - トラストホストの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	1.00.01 以降

使用例: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:トラストホストネットワークを作成するには

```
#create trusted_host network 10.48.0.0/16
Command: create trusted_host network 10.48.0.0/16

Success.

#
```

3.8.19 delete trusted_host

目的	トラストホストエントリーを削除します。
構文	delete trusted _host < ipaddr <ipaddr> | network <network_address> | all >
説明	本コマンドは、トラストホストエントリーを削除します。エントリー個別、あるいはエントリーすべてを削除することができます。
パラメーター	<ipaddr> - 削除する対象の IP アドレスを指定します。 <network_address> - 削除する対象のネットワークアドレスを指定します。 all - 登録されている全てのトラストホストが削除されます。
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	1.00.01 以降

使用例:IP アドレス「10.48.74.121」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:ネットワークアドレス「10.62.0.0/16」のトラストホストネットワークを削除するには

```
#delete trusted_host network 10.62.0.0/16
Command: delete trusted_host network 10.62.0.0/16

Success.

#
```

使用例:トラストホストエントリーをすべて削除するには

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

Success.

#
```

3.8.20 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、登録されているトラストホストのリストを表示します。トラストホストを IP アドレスで指定した場合、サブネットマスクを「/32」として表示します。
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	1.00.01 以降

使用例：トラストホストのリストを表示するには

```
#show trusted_host
Command: show trusted_host

Management Stations

IP Address/Netmask
----------------------
10.53.13.94/32

Total Entries: 1

#
```

3.8.21 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 トラップの有効にします。また、所定のトラップのみ選択して有効にすることもできます。
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	1.00.01 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.

#
```

3.8.22 disable snmp

目的	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。また、特定のトラップのみ選択して無効にすることもできます。
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	1.00.01 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.

#
```

3.8.23 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> - ポート範囲を指定します。 enable - このポートのリンクチェンジトラップの送信を有効にします。 disable - このポートのリンクチェンジトラップの送信を無効にします。
制限事項	管理者アカウン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:ポート 1～4 のリンクチェンジトラップを有効に設定するには

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

Success.

#
```

3.8.24 show snmp traps

目的	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、スイッチの SNMP トラップの設定情報を表示します。
パラメーター	linkchange_traps - SNMP リンクチェンジトラップの設定情報を表示します。 <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	1.00.01 以降

使用例:SNMP トラップ設定情報を表示するには

```
#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:SNMP リンクチェンジトラップの設定情報を表示するには

```
#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
#
```

3.8.25 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。その情報は、スイッチの基本情報に「System Contect」として表示されます。
パラメーター	<sw_contact> - 最大 128 文字を使用できます。 連絡担当者を指定しない場合は、NULL 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	1.00.01 以降

使用例:スイッチの連絡担当者を「APS」に設定するには

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

Success.

#
```

3.8.26 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。その情報は、スイッチの基本情報に「System Location」として表示されます。
パラメーター	<sw_location> - 最大 128 文字を使用できます。場所を指定しない場合は、NULL 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	1.00.01 以降

使用例:スイッチ場所を「5F」に設定するには

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

Success.

#
```

3.8.27 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。その情報は、スイッチの基本情報に「System Name」として表示されます。
パラメーター	<sw_name> - 最大 128 文字を使用できます。名前を指定しない場合は、NULL 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	1.00.01 以降

使用例:スイッチ名を「ApresiaLightGM124GT-SS」に設定するには

```
#config snmp system_name ApresiaLightGM124GT-SS
Command: config snmp system_name ApresiaLightGM124GT-SS

Success.

#
```

3.8.28 enable rmon

目的	RMON を有効にします。
構文	enable rmon
説明	本コマンドは、スイッチのリモートモニタリング(RMON)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	1.00.01 以降

使用例：RMON を有効にするには

```
#enable rmon
Command: enable rmon

Success.

#
```

3.8.29 disable rmon

目的	RMON を無効にします。
構文	disable rmon
説明	本コマンドは、スイッチのリモートモニタリング(RMON)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	1.00.01 以降

使用例：RMON を無効にするには

```
#disable rmon
Command: disable rmon

Success.

#
```

3.9 ネットワーク監視コマンド

3.9.1 show packet ports

目的	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	1.00.01 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 2
Command: show packet ports 2

Port Number : 2
 Frame Size    Frame Counts  Frames/sec    Frame Type   Total      Total/sec
 ------------  ------------  ----------    ----------   ---------  ---------
 64            0             0             RX Bytes     0          0
 65-127        0             0             RX Frames    0          0
 128-255       0             0
 256-511       0             0             TX Bytes     0          0
 512-1023      0             0             TX Frames    0          0
 1024-1518     0             0

 Unicast RX    0             0
 Multicast RX  0             0
 Broadcast RX  0             0

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

3.9.2 show error ports

目的	パケットエラーの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。 なお、Drop Pkts カウンタについては、未対応のためカウントされません。
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	1.00.01 以降

使用例:ポート 3 のパケット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

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

3.9.3 config utilization notify

目的	CPU/DRAM 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 CPU/DRAM 使用率通知を設定します。 CPU/DRAM 使用率通知機能は、CPU や DRAM の使用状態を周期的に監視し、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> - CPU もしくは DRAM の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	1.03.00 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	CPU/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/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	1.03.00 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	ハードウェア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、運用中のスイッチのハードウェア使用率統計情報をリアルタイムで表示します。CPU、DRAM、FLASH、各ポートの情報を取得します。
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 FLASH 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	1.00.01 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 -   3 %          One Minute -   2 %          Five Minutes -  5 %
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 FLASH 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       148810      148810      100       22      0           0           0
 2       148810      148810      100       23      0           0           0
 3       0           148810      50        24      0           0           0
 4       0           0           0
 5       0           0           0
 6       0           0           0
 7       0           37          1
 8       0           0           0
 9       0           0           0
 10      0           0           0
 11      36          0           1
 12      0           0           0
 13      0           0           0
 14      0           0           0
 15      0           0           0
 16      0           0           0
 17      0           0           0
 18      0           0           0
 19      0           0           0
 20      0           0           0
 21      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/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/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	1.03.00 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 : 10 sec
Trap State       : Disabled
Log State        : Enabled

#
```

3.9.7 clear counters

目的	パケット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、スイッチのパケット統計カウンタをクリアします。所定のポートのカウンタのみをクリアすることもできます。
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	1.00.01 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	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。本コマンド自体の履歴は残ります。
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: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	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 6,000 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	1.00.01 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 Date       Time     Log Text
----- ---------- -------- ---------------------------------------------------
2     0000-00-00 00:00:34 Successful login through Console (Username: adpro)
1     0000-00-00 00:00:27 System warm start (CONSOLE)

#
```

3.9.10 enable syslog

目的	Syslog 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 Syslog 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	1.00.01 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	Syslog 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 Syslog 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	1.00.01 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 機能の状態を表示します。
構文	show syslog
説明	本コマンドは、syslog の設定状態を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:syslog 機能の設定状態を表示するには

```
#show syslog
Command: show syslog

Syslog Global State  : Disabled

#
```

3.9.13 create syslog host

目的	Syslog サーバを登録します。
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、システムログを送信する宛先(Syslog サーバ)を登録します。また、登録した Syslog サーバに対して、どのレベルのログを送信するか、あるいは、どの分類で送信するか、などの設定を行います。
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	1.00.01 以降

使用例:Syslog サーバーを登録するには

```
#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 サーバーの登録内容を変更します。
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、登録した Syslog サーバーの設定を変更します。そのサーバーに送信する情報の種類などの変更も行うことができます。
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	1.00.01 以降

使用例:インデックス 1 の Syslog サーバーを編集するには

```
#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	Syslog サーバーを削除します。
構文	delete syslog host < <index 1-4> | all >
説明	本コマンドは、Syslog サーバーの設定を削除します。インデックスで識別される一つのサーバー、もしくはすべての登録済み Syslog サーバーの設定を削除することができます。
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	1.00.01 以降

使用例:Syslog サーバーを削除するには

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

Success.

#
```

3.9.16 show syslog host

目的	Syslog サーバーの設定情報を表示します。
構文	show syslog host [<index 1-4>]
説明	本コマンドは、Syslog サーバーの設定を表示します。特定の Syslog サーバーの情報のみも取得できます。
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	1.00.01 以降

使用例:syslog サーバーの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	ログを FLASH に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 FLASH にログを保存する方法を指定します。定期的に書き込みを行う方法、コマンド実行時に行う方法、およびログ発生時に書き込む方法を選択します。
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	1.00.01 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 4,000 行です。

3.9.18 show log_save_timing

目的	FLASH に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にログを書き込む方法の設定状態を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 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	1.00.01 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の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、デフォルトではリンクローカルアドレスは設定されず、IPv6 処理は無効になります。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	1.00.01 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の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	1.00.01 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	1.00.01 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が、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 クライアント機能を有効にします。
構文	enable smtp
説明	本コマンドは、スイッチの SMTP クライアント機能を有効にします。実際に電子メールを送信するためには、パラメータを正しく設定する必要があります。
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:スイッチの SMTP クライアント機能を有効にするには

```
#enable smtp
Command: enable smtp

Success.

#
```

3.10.2 disable smtp

目的	SMTP クライアント機能を無効にします。
構文	disable smtp
説明	本コマンドは、スイッチの SMTP クライアント機能を無効にします。設定されたパラメータは設定情報に保持されますのでご注意ください。
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	1.00.01 以降

使用例:スイッチの SMTP クライアント機能を無効にするには

```
#disable smtp
Command: disable smtp

Success.

#
```

3.10.3 config smtp

目的	SMTP クライアントのパラメーター設定を行います。
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	1.00.01 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	SMTP 機能の設定パラメーターを表示します。
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	1.00.01 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: Enabled
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	1.00.01 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	物理ポートの設定を行います。
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、スイッチの各ポートの状態やリンク速度などの設定を行います。また、コンボポートで使用するメディアを指定することができます。
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> - コンボポートのメディアタイプを指定します。 speed - ポートのリンク速度を設定します。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_half - 10Mbps 半二重に設定します。 10_full - 10Mbps 全二重に設定します。 100_half - 100Mbps 半二重に設定します。 100_full - 100Mbps 全二重に設定します。 1000_full - 1Gbps 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	1.00.01 以降

使用例:ポート 21～24 を有効にし、リンク速度を 10Mbps 全二重にするには

```
#config ports 21-24 medium_type copper speed 10_full state enable
Command: config ports 21-24 medium_type copper 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 config sfp auto_recognition

目的	SFP 自動認識機能を設定します。
構文	config sfp auto_recognition < enable | disable >
説明	本コマンドは、SFP 自動認識機能を設定します。SFP 自動認識機能を使用すると、コンボポートのメディアタイプの設定によらず、使用するメディアが自動的に選択されます。
パラメーター	enable - SFP 自動認識機能を有効にします。 disable - SFP 自動認識機能を無効にします。
制限事項	なし
対応バージョン	1.12.00 以降

使用例:SFP 自動認識機能を有効にするには

```
#config sfp auto_recognition enable
Command: config sfp auto_recognition enable

Success.

#
```

注意事項

SFP 自動認識機能を有効にすると、全てのコンボポートの state の設定は適用されず、Fiber ポートで光信号を受信する環境では Fiber ポートが、それ以外の場合は UTP ポートが、有効な状態に変更されます。

SFP 自動認識機能の設定を切り替えると、コンボポートがリセットされます。

3.11.3 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。また、現在のリンク状態も表示することができます。
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	1.00.01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         LinkDown               Enabled
       Auto
 2      Enabled   Auto/Disabled         LinkDown               Enabled
       Auto
 3      Enabled   Auto/Disabled         LinkDown               Enabled
       Auto
 4      Enabled   Auto/Disabled         LinkDown               Enabled
       Auto
 5      Enabled   Auto/Disabled         LinkDown               Enabled
       Auto
 6      Enabled   Auto/Disabled         LinkDown               Enabled
       Auto
 7      Enabled   Auto/Disabled         LinkDown               Enabled
       Auto
 8      Enabled   Auto/Disabled         LinkDown               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 enable sntp

目的	SNTP 機能を有効にします。
構文	enable sntp
説明	本コマンドは、SNTP クライアント機能を有効にします。SNTP は時刻サーバーから時刻情報を取得するプロトコルで、時刻同期を行うには SNTP サーバーを正しく設定する必要があります。SNTP で時刻情報を取得すると、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。
対応バージョン	1.00.01 以降

使用例:SNTP 機能を有効にするには

```
#enable sntp
Command: enable sntp

Success.

#
```

3.12.2 disable sntp

目的	SNTP 機能を無効にします。
構文	disable sntp
説明	本コマンドは、SNTP クライアント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	1.00.01 以降

使用例:SNTP を無効にするには

```
#disable sntp
Command: disable sntp

Success.

#
```

3.12.3 config sntp

目的	SNTP サーバーを設定します。
構文	config sntp < primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999> >
説明	本コマンドは、SNTP で時刻情報を取得するサーバーを設定します。
パラメーター	primary <ipaddr> - プライマリ SNTP サーバーの IP アドレスを入力します。 secondary <ipaddr> - セカンダリ SNTP 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。
対応バージョン	1.00.01 以降

使用例:SNTP サーバーを設定するには

```
#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.

#
```

3.12.4 show sntp

目的	SNTP 設定の情報を表示します。
構文	show sntp
説明	本コマンドは、SNTP クライアント機能の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	1.00.01 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

#
```

3.12.5 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、手動でシステム時間と日付の設定を行います。SNTP 機能で時刻情報を取得すると、手動で設定したシステム時間と日付は上書きされます。
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。
対応バージョン	1.00.01 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 29032015 19:42:30
Command: config time 29032015 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	1.00.01 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、サマータイム (DST：Daylight Savings Time)を設定します。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。 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	1.00.01 以降

使用例: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	システム時間および時刻設定を表示します。
構文	show time
説明	本コマンドは、現在のシステム時間と時刻設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:スイッチのシステム時間を表示するには

```
#show time
Command: show time

Current Time Source : System Clock
Current Time        : 01 Apr 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	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。非対称構成を使用しない場合は有効にしないでください。
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	1.00.01 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	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	1.00.01 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	Asymmetric VLAN の設定を表示します。
構文	show asymmetric_vlan
説明	本コマンドは、スイッチの Asymmetric VLAN 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	1.00.01 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	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 ガード機能のグローバル設定を有効にします。BPDU ガードはポート単位で有効/無効を指定します。BPDU ガードが有効のポートでは、BPDU フレームを受信すると err-disable 状態となりポートを shutdown します。
パラメーター	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: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	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	1.01.00 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	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	本コマンドは、ポート単位で BPDU ガードの動作を設定します。
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。デフォルトでは無効になっています。 mode <shutdown> - BPDU パケットを受信したポートを shutdown 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	1.01.00 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 ガード機能の対象となるパケットは、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	本コマンドは、BPDU ガードでのポートの自動復旧時間を設定します。
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。 デフォルトの値は 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	1.01.00 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	BPDU ガードのログを設定します。
構文	config bpdu_guard log <none | attack_detected | attack_cleared | both>
説明	本コマンドは、BPDU ガード機能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 パケット検知および復旧した場合に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	1.01.00 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	BPDU ガード状態を表示します。
構文	show bpdu_guard [ports [<portlist>]]
説明	本コマンドは、グローバルもしくはポート単位での BPDU ガード設定を表示します。
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> - 表示させたい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	1.01.00 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 アドレスのスタティックエントリーを作成します。
構文	create fdb <vlan_name 32> <macaddr> port <port>
説明	本コマンドは、MAC アドレス転送テーブル(FDB:フォワーディングデータベース)上にスタティックエントリーを作成します。スイッチの転送テーブルは、ポートと VLAN、MAC アドレスの組み合わせのエントリーから構成され、スイッチが受信したフレームは転送テーブルの情報を元に所定のポートに転送します。通常、転送テーブルのエントリーはスイッチは受信するトラフィックから自動的に学習しますが、本コマンドでは永続的な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> - スタティックエントリーの 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	1.00.01 以降

使用例:ユニキャスト MAC アドレスのスタティックエントリーを作成するには

```
#create fdb default 00-40-66-00-00-01 port 5
Command: create fdb default 00-40-66-00-00-01 port 5

Success.

#
```

3.15.2 create multicast_fdb

目的	マルチキャスト MAC アドレスのスタティックエントリーを登録します。
構文	create multicast_fdb <vlan_name 32> <macaddr>
説明	本コマンドは、マルチキャスト MAC アドレス転送テーブル上にスタティックエントリーを登録します。実行時点では所属ポートは割り当てられません。
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> - スタティックエントリーの 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	1.00.01 以降

使用例:マルチキャスト MAC アドレスのスタティック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	マルチキャスト MAC アドレスのスタティックエントリーを編集します。
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 アドレス転送テーブル上のスタティックエントリーにポートを割り当てます。
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> - スタティックエントリーの MAC アドレスを入力します。 <add | delete> - add は、エントリーにポートを追加します。delete は、エントリー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	1.00.01 以降

使用例:マルチキャスト MAC アドレスのスタティックエントリーにポート 1-5 を割り当てるには

```
#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	MAC アドレス転送テーブルのエージング時間を設定します。
構文	config fdb aging_time <sec 10-1000000>
説明	本コマンドは、MAC アドレス転送テーブルのダイナミックエントリーのエージング時間を設定します。デフォルトでは 300 秒です。 スイッチは、受信するフレームの送信元 MAC アドレスから学習し、MAC アドレス転送テーブル上にダイナミックエントリーを自動的に作成します。スイッチは、受信したフレームの宛先 MAC アドレスを MAC アドレス転送テーブルに照会し、その情報を元に所定のポートに転送します。MAC アドレス転送テーブル上で見つからない場合は、対象 VLAN のすべてのメンバーポートに転送されます（フラッディング）。ダイナミックエントリーは、一定期間そのポートから送信元 MAC アドレスのフレームを受信しない場合に削除されます。 エージング時間が非常に長い場合、既にそのホストが存在しないダイナミックエントリーにより、不適切なフレームの転送が行われることがあります。一方、エージングタイムが短すぎるとエントリーの削除が短期間に行われるため、フラッディングが多発する可能性があります。
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。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	1.00.01 以降

使用例:FDB の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	ユニキャスト/マルチキャスト MAC アドレスのスタティック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、スイッチのユニキャスト MAC アドレス転送テーブルやマルチキャスト MAC アドレス転送テーブルに登録したスタティック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> - スタティック 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	1.00.01 以降

使用例:ユニキャスト MAC アドレス転送テーブルのスタティック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:マルチキャスト MAC アドレス転送テーブルのスタティック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	MAC アドレス転送テーブルのダイナミックエントリーを削除します。
構文	clear fdb < vlan <vlan_name 32> | port <port> | all >
説明	本コマンドは、スイッチの MAC アドレス転送テーブルのダイナミックエントリーをクリアします。スイッチ全体、VLAN 単位、もしくはポート単位で指定することができます。
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入力します。 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	1.00.01 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	マルチキャスト MAC アドレス転送テーブルの情報を表示します。
構文	show multicast_fdb [vlan <vlan_name 32> | mac_address <macaddr>]
説明	本コマンドは、スイッチのマルチキャスト MAC アドレス転送テーブルの内容を表示します。表示内容は、スタティックとダイナミックの両方のエントリーが含まれます。
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> - 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	1.00.01 以降

使用例:マルチキャスト MAC アドレス転送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 アドレス転送テーブルの情報を表示します。
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、スイッチのユニキャスト MAC アドレス転送テーブルの情報を表示します。表示内容は、スタティックとダイナミックの両方のエントリーが含まれますが、スタティックエントリーだけを表示することもできます。また。ポート、VLAN、MAC アドレスを指定して表示することもできます。
パラメーター	port <port> - 表示するポートを指定します。 vlan <vlan_name 32> - 表示する VLAN を VLAN 名で指定します。 vlanid <vidlist> -表示する VLAN を VLAN ID のリストで指定します。 mac_addredd <macaddr> - 表示する MAC アドレスを指定します。 static - スタティックエントリーのみを表示します。 aging_time - MAC アドレス転送テーブルのエージング時間を表示します。
制限事項	なし。
対応バージョン	1.00.01 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、マルチキャスト MAC アドレス転送テーブルに登録されていないマルチキャストトラフィックを各ポートに転送するかどうかを定めるマルチキャス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> forward_unregistered_groups - このモードでは未登録のマルチキャストトラフィックは対象ポートに転送されます。 filter_unregistered_groups - このモードでは未登録のマルチキャストトラフィックは対象ポートに転送されません。
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	1.00.01 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	マルチキャス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、ポートのマルチキャス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	1.00.01 以降

使用例: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: 1-24
        Filtering List:

#
```

3.16 IGMP スヌーピングコマンド

3.16.1 enable igmp_snooping

目的	IGMP スヌーピング機能を有効にします。
構文	enable igmp_snooping [forward_mcrouter_only]
説明	本コマンドは、スイッチの IGMP スヌーピング機能をグローバルで有効にします。IGMP スヌーピング機能を使用すると、マルチキャストホストの IGMP パケットをモニタリングしてマルチキャスト転送テーブルのダイナミックエントリーを自動的に更新します。
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	1.00.01 以降

使用例:IGMP スヌーピング機能を有効にするには

```
#enable igmp_snooping
Command: enable igmp_snooping

Success.

#
```

3.16.2 disable igmp_snooping

目的	IGMP スヌーピング機能を無効にします。
構文	disable igmp_snooping [forward_mcrouter_only]
説明	本コマンドは、スイッチの IGMP スヌーピング機能をグローバルで無効にします。IGMP スヌーピング機能が無効の場合、マルチキャスト転送テーブルは自動的に学習されず、エントリーはスタティック登録に限定されます。
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	1.00.01 以降

使用例:IGMP スヌーピング機能を無効にするには

```
#disable igmp_snooping
Command: disable igmp_snooping

Success.

#
```

3.16.3 config igmp_snooping

目的	IGMP スヌーピング機能の動作を設定します。
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 スヌーピング機能の動作を設定します。IGMP スヌーピングを適用する VLAN などの設定を行います。
パラメーター	vlan_name <vlan_name 32> - 対象の VLAN を VLAN 名で指定します。 vlanid <vidlist> - 対象の VLAN を VLAN ID のリストで指定します。 all - すべての VLAN を対象とします。 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。 fast_leave <enable | disable> - IGMP スヌーピングの fast-leave(即時離脱)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た場合に、メンバーはただちにグループから削除されます。
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	1.00.01 以降

使用例:IGMP スヌーピング機能の動作を設定するには

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

Success.

#
```

3.16.4 config igmp_snooping querier

目的	IGMP クエリアの設定を行います。
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 クエリア設定を行います。クエリアは、使用するマルチキャスト環境でマルチキャストルーターが存在しない場合に、IGMP クエリの処理を代行します。クエリアでは、以下の 3 種類の通知パラメーターがあります。 - クエリ間隔(query_interval): ジェネラルクエリの送信間隔(秒)。 - 最大応答時間(max_response_time): メンバーシップレポートの待ち時間(秒)。 - ロバストネス変数(robustness_variable): IGMP Leave メッセージを受信することなくメンバーシップレポートが途絶えた場合の、メンバーを除外するまでのジェネラルクエリ送信回数。これはパケットロスが多い環境で、何回まで連続してクエリとメンバーシップレポートのロスを許容するかを定めるパラメーターとしても使用されます。 これらは送信する IGMP クエリの中で通知され、マルチキャストネットワーク内でのマルチキャスト MAC アドレス転送テーブルの管理に適用されます。例えば、IGMP スヌーピング機能で学習したメンバーポートのエージング時間は、(クエリ間隔 x ロバストネス変数) + (最大応答時間)で算出されます。
パラメーター	vlan_name <vlan_name 32> - 対象となる VLAN を VLAN 名で指定します。 vlanid <vidlist> - 対象となる VLAN を VLAN ID のリストで指定します。 all - すべての VLAN を対象とします。 query_interval - クエリ間隔を指定します。デフォルト値は 125 です。 max_response_time - 最大応答時間を指定します。デフォルト値は 10 です。 robustness_variable - ロバストネス変数を指定します。デフォルト値は 2 です。 last_member_query_interval - IGMP グループスペシフィッククエリの送信間隔を秒単位で指定します。グループスペシフィッククエリは IGMP Leave メッセージを受信した場合にマルチキャストルーター(もしくはクエリア)が、他のメンバーの存在を確認するために送信します。応答がない場合、学習したグループのエントリーが削除されます。 state - IGMP クエリア機能を「enable」(有効)、または「disable」(無効)にします。有効の場合、ネットワーク内に他にクエリアとして動作するデバイスが存在しない場合には、クエリアとして動作し、クエリを送信します。クエリア候補となる他のデバイスが存在する場合は、代表クエリアとして選定された場合にクエリアとして動作します。 version - IGMP 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	1.00.01 以降

使用例:IGMP 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.

#
```

3.16.5 config router_ports

目的	ルーターポートを設定します。
構文	config router_ports < <vlan_name 32> | vlanid <vidlist> > < add | delete > <portlist>
説明	本コマンドは、ルーターポートを指定します。例えばマルチキャストパケットフィルタリングを行う複数のスイッチを経由する場合の通信などで明示的に指定しなければならないことがあります。
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を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	1.00.01 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.

#
```

3.16.6 config router_ports_forbidden

目的	forbidden (禁止)ルーターポートを設定します。
構文	config router_ports_forbidden < <vlan_name 32> | vlanid <vidlist> > < add | delete > <portlist>
説明	本コマンドは、禁止ルーターポートを指定します。これは、指定した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> - 対象となる VLAN を VLAN 名で指定します。 vlanid <vidlist> - 対象となる VLAN を VLAN ID で指定します。 <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> - 追加もしくは削除の対象とな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	1.00.01 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.

#
```

3.16.7 show igmp_snooping

目的	IGMP スヌーピング機能の状態を表示します。
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 スヌーピングの状態や設定を表示します。
パラメーター	vlan <vlan_name 32> - 表示する対象の VLAN を VLAN 名で指定します。 vlanid <vidlist> - 表示する対象の VLAN を VLAN ID で指定します。 省略すると、すべての VLAN での状態が表示されます。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:IGMP スヌーピングの状態を表示するには

```
#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	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、現在のルーターポートを表示します。学習したルーターポートとスタティックエントリーの両方を表示することができます。
パラメーター	vlan <vlan_name 32> - 対象の VLAN を VLAN 名で指定します。 vlanid <vidlist> - 対象の VLAN を VLAN ID で指定します。 static - スタティック登録のルーターポートを表示します。 dynamic - 学習したルーターポートを表示します。 forbidden - 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	1.00.01 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	マルチキャストグループの情報を表示します。
構文	show igmp_snooping group [< vlan <vlan_name 32> | vlanid <vidlist> >]
説明	本コマンドは、IGMP スヌーピングで検出されたマルチキャストグループの情報を表示します。
パラメーター	<vlan_name 32> - 表示する VLAN を VLAN 名で指定します。 <vidlist> - 表示する VLAN を VID ID で指定します。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:マルチキャスト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	マルチキャストホストを表示します。
構文	show igmp_snooping host [<vlan <vlan_name 32> | vlanid <vidlist> | ports <portlist> | group <ipaddr>>]
説明	本コマンドは、IGMP スヌーピングで検知されたマルチキャスト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	1.00.01 以降

使用例:マルチキャストホストを表示するには

```
# 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             225.0.3.4           3           10.0.0.6

Total Entries : 2

#
```

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	リンクアグリゲーショングループを登録します。
構文	create link_aggregation group_id <value> [type <lacp | static>]
説明	本コマンドは、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。リンクアグリゲーションには、固定でポートを指定するスタティックと、LACP フレームを使用して隣接デバイスとネゴシエーションを行うダイナミック(LACP)の 2 種類のタイプがあり、グループごとにいずれを使用するか指定します。
パラメーター	<value> - グループ ID を指定します。最大 8(各装置で最大ポート数の半分)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、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	1.00.01 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

GM シリーズのリンクアグリゲーショングループ数の最大は、APLGM118GTSS と APLGM124GTSS のみ最大 8、それ以外は製品搭載ポート数÷2 となります。

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	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	1.00.01 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	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 コマンドで作成されたリンクアグリゲーショングループのポート割り当てなどの設定を行います。
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	1.00.01 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 algorithm

目的	リンクアグリゲーションアルゴリズムを設定します。
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	本コマンドは、負荷分散データの送信に対し、egress ポートを選択する際、スイッチによって検証されるパケットの部分を設定します。また、LACP のシステム優先度を設定します。LACP では、対向するデバイス間で LACP システム優先度を比較し、システム優先度が小さいデバイスがアクティブ/スタンバイポートを決定します。システム優先度が同値の場合は、同様に MAC アドレスの比較を行います。
パラメーター	mac_source - 送信元 MAC アドレスベースで負荷分散します。 mac_destination - 送信先 MAC アドレスベースで負荷分散します。 mac_source_dest - 送信元および送信先 MAC アドレスベースで負荷分散します。 ip_source - 送信元 IP アドレスベースで負荷分散します。 ip_destination - 送信先 IP アドレスベースで負荷分散します。 ip_source_dest - 送信元および送信先 IP アドレスベースで負荷分散します system_priority - LACP のシステム優先度を 1～65535 の範囲で設定します。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	1.00.01 以降 1.07.00 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 アドレスベースの負荷分散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

アルゴリズムが ip_source または ip_destination の場合、Unknown unicast、Broadcast、及び Multicast のフレームはロードシェアされません。

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設定情報を表示します。
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設定情報を表示します。
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 のシステム優先度を表示します。
制限事項	なし。
対応バージョン	1.00.01 以降 1.07.00 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 ポートのモード設定を行います。
構文	config lacp_ports <portlist> < mode < active | passive > | lacp_timeout <short | long> | port_priority <value> >
説明	本コマンドは、LACP ポートの処理モードを設定します。処理モードには、LACP フレームを送信する Active と、受信専用の Passive の 2 種類のモードがあります。また、ポートのアクティブ/スタンバイの選定に使用するポート優先度をポート単位で設定します。ポート優先度が小さい方がアクティブに選択されやすくなります。
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。 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 - 処理モードが Active の場合、対向デバイスに 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 - 処理モードが Passive の場合、対向デバイスからの 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。 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 <value> - LACP のポート優先度を 1～65535 の範囲で設定します。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	1.00.01 以降 1.07.00 以降(lacp_timeout 及び port_priority パラメーターをサポート)

使用例:LACP ポートの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 ポートの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 ポートの処理モードや設定情報を表示します。
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。 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	1.00.01 以降 1.07.00 以降(port_priority パラメーター表示をサポート)

使用例:LACP ポートの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

ループ防止コマンドでは、ネットワークでループ構成が発生した場合に検知するループ検知機能を設定します。
ループ検知機能が有効のポートでは、スイッチが一定間隔でループ検知フレームを送信します。自身が送信したループ検知フレームを受信した場合に、ループ構成が発生したとみなします。
ループを検知した場合の対象ポート（ループ検知フレームの送信ポートや受信ポート）のアクションは、各ポートの method パラメーターで選択することができます。shutdown を指定した場合、対象ポートはループ検知時に閉塞されます。drop を指定した場合は、ループ検知時でもブロックしません。

注意事項

ループ検知機能で使用するループ検知フレームは、タグなしで送信されます。（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。
- **ver.1.00.01 までは、ループ検知フレームを「自送出のポートで受信」することでループを検知します。**
- **ver.1.01.00 以降は、ループ検知フレームを「自装置内ポートで受信」することでループを検知します。**

ループ検知フレームの送信可否は、論理的なポートの状態（例えば、リンクアグリゲーションの論理リンクや、スパニングツリーのステータスなど）の影響を受けます。リンクアップしたポートでも必ずしも送信されるとは限りません。

ループ検知機能は、スイッチ単体でも効果が見込める機能ですが、動作は極めてシンプルであり、併用する機能やネットワーク環境によっては有効に動作しないこともありますので、導入の際にはご留意ください。

3.18.1 enable loopdetect

目的	ループ検知機能を有効にします。
構文	enable loopdetect
説明	本コマンドは、ループ検知機能をグローバルで有効にします。 デフォルト設定は無効(disable)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	1.00.01 以降

使用例:ループ検知機能を有効にするには

```
# enable loopdetect
Command: enable loopdetect

Success.

#
```

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。
・ver.1.03.00 以降では、ループ検知している状態で console LED が点滅します。
（ループ検知が解除された場合には LED 点滅も同時に解除されます。）
・ver.1.02.00 以前では、ループ検知しても console LED は点滅しません。

3.18.2 disable loopdetect

目的	ループ検知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、ループ防止機能をグローバルで無効にします。 デフォルト設定は無効(disable)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	1.00.01 以降

使用例:ループ検知機能を無効にするには

```
# disable loopdetect
Command: disable loopdetect

#
```

3.18.3 config loopdetect

目的	ループ検知機能のパラメーターを設定します。
構文	config loopdetect < recover_timer < 0 | <value 60-1000000> > | interval <value 1-32767> >
説明	本コマンドは、ループ検知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フレーム(CTP(Configuration Test Protocol)フレーム)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	1.00.01 以降

使用例:復旧タイマーを 0、検知フレームの送信間隔を 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

ループ検知機能でループを検知した場合、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)を設定し、手動復旧を設定されることを推奨します。

3.18.4 config loopdetect ports

目的	ループ検知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検知機能を設定します。ループを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。drop では、ループの検知は行いますが、ポートに対するアクションは行いません(主にアップリンクポートで使用されます)。
パラメーター	<portlist> - ループ検知機能を設定するポートを指定します。 all - すべてのポートに設定を適用します。 state - ループ検知機能を有効または無効にします。デフォルトでは無効です。 enable - ポートのループ検知機能を「enable」(有効)に設定します。 disable - ポートのループ検知機能を「disable」(無効)に設定します。 method - 動作モードを指定します。デフォルトは shutdown です。 shutdown - 動作モードを shutdown に設定します。 drop - 動作モードを drop 設定に適用します。
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	1.01.00 以降

使用例:ポート 1-5 のループ検知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.

#
```

3.18.5 show loopdetect

目的	ループ検知機能の設定を表示します。
構文	show loopdetect
説明	本コマンドは、ループ検知機能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	1.00.01 以降

使用例:ループ検知機能の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	ループ検知機能のポート情報を表示します。
構文	show loopdetect ports < <portlist> | all >
説明	本コマンドは、各ポートのループ検知機能の設定情報や検知状態を表示します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - 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	1.00.01 以降

使用例:ポート 1～5 のループ防止機能の状態を表示するには

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

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

3.19 MAC ベース VLAN コマンド

3.19.1 create mac_based_vlan

目的	MAC ベース VLAN のエントリーを作成します。
構文	create mac_based_vlan mac_address <macaddr> vlan <vlan_name 32>
説明	本コマンドは、MAC ベース VLAN のスタティックエントリーを作成します。 MAC ベース VLAN は､該当する MAC アドレスを送信元とする通信が入力された場合、ポートの PVID を参照せず、エントリー内で指定された VLAN に所属するものとしてトラフィック処理を行います。
パラメーター	<macaddr> - 対応する MAC アドレスを指定します。 <vlan_name 32> - MAC アドレスに対応付けされる VLAN を VLAN 名で指定します。
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	1.00.01 以降

使用例:MAC ベース VLAN の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.

#
```

注意事項

MAC ベース VLAN を管理するテーブルは、処理の高速化のためハッシュテーブルを使用しています。ハッシュ値の衝突により、MAC ベース VLAN テーブルのエントリーを登録できない場合があります。

MAC ベース VLAN では、実装しているハッシュ計算アルゴリズムの関係上、所定の条件を満たすと完全にランダムな場合と比べて衝突が発生しやすいことがあります。例えば、同一の OID の MAC アドレスを多数登録する場合が該当します。

3.19.2 delete mac_based_vlan

目的	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>]
説明	本コマンドは､登録した MAC ベース LAN のスタティックエントリーを削除します。MAC アドレスと VLAN を指定しない場合、すべてのスタティックエントリーを削除します。ダイナミックなエントリー(ポート認証でホストベース認証を使用し、ダイナミック VLAN で自動作成されるエントリー)は削除されません。
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。
制限事項	管理者アカウン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:MAC ベース VLAN の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	MAC ベース VLAN のエントリーを表示します。
構文	show mac_based_vlan [mac <macaddr> | vlan <vlan_name 32>]
説明	本コマンドは、MAC ベース VLAN のエントリーを表示します。スタティック、ダイナミック両方のエントリーが表示されます。
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。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:MAC ベース VLAN の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 enable mld_snooping

目的	MLD スヌーピング機能を有効にします。
構文	enable mld_snooping
説明	本コマンドは、スイッチの MLD スヌーピング機能をグローバルで有効にします。MLD スヌーピング機能は、IPv6 マルチキャスト通信に適用される機能で、IPv4 マルチキャスト通信での IGMP スヌーピング機能に相当します。
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

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:MLD スヌーピング機能を有効にするには

```
# enable mld_snooping
Command: enable mld_snooping

Success.

#
```

3.20.2 disable mld_snooping

目的	MLD スヌーピング機能を無効にします。
構文	disable mld_snooping
説明	本コマンドは、MLD スヌーピング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	1.00.01 以降

使用例:MLD スヌーピング機能を無効にするには

```
# disable mld_snooping
Command: disable mld_snooping

Success.

#
```

3.20.3 config mld_snooping

目的	MLD スヌーピング機能の動作を設定します。
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、スイッチの MLD スヌーピング機能の動作を設定します。IGMP スヌープを適用する VLAN などの設定を行います。
パラメーター	vlan_name <vlan_name 32> - 対象の VLAN を VLAN 名で指定します。 vlanid <vidlist> - 対象の VLAN を VLAN ID のリストで指定します。 all - すべての VLAN を対象とします。 state <enable | disable> - 指定した VLAN の MLD スヌーピングを「enable」(有効)または「disable」(無効)にします。 fast_done - MLD スヌーピングの Fast done 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、メンバーは MLD Done メッセージを受信するとただちにグループから除外されます。
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	1.00.01 以降

使用例:MLD スヌーピング機能の動作を設定するには

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

Success.

#
```

3.20.4 config mld_snooping querier

目的	MLD クエリアの設定を行います。
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、MLD クエリア設定を行います。
パラメーター	vlan_name <vlan_name 32> - 対象となる VLAN を VLAN 名で指定します。 vlanid <vidlist> - 対象となる VLAN を VLAN ID で指定します。 all - すべての VLAN を対象とします。 query_interval - クエリ間隔を指定します。デフォルト値は 125 です。 max_response_time - 最大応答時間を指定します。デフォルト値は 10 です。 robustness_variable - ロバストネス変数を指定します。デフォルト値は 2 です。 last_listener_query_interval - MLD グループスペシフィッククエリの送信間隔を秒単位で指定します。グループスペシフィッククエリは MLD Done メッセージを受信した場合にマルチキャストルーター(もしくはクエリア)が、他のメンバーの存在を確認するために送信します。応答がない場合、学習したグループのエントリーが削除されます
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	1.00.01 以降

使用例:MLD 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.

#
```

3.20.5 config mld_snooping mrouter_ports

目的	IPv6 ルーターポートを設定します。
構文	config mld_snooping mrouter_ports <vlan_name 32> < add | delete > <portlist>
説明	本コマンドは、スタティック IPv6 ルーターポートを指定します。
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	1.00.01 以降

使用例:ポート 1～10 をスタティック IPv6 ルーターポートに設定するには

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

Success.

#
```

3.20.6 config mld_snooping mrouter_ports_forbidden

目的	forbidden(禁止)IPv6 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、禁止 IPv6 ルーターポートを指定します。
パラメーター	<vlan_name 32> - 対象となる VLAN を VLAN 名で指定します。 <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> - 追加もしくは削除の対象とな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	1.00.01 以降

使用例:ポート 1～10 を禁止 IPv6 ルーターポートに設定するには

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

Success.

#
```

3.20.7 show mld_snooping

目的	MLD スヌーピング機能の状態を表示します。
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 スヌーピングの状態や設定を表示します。
パラメーター	vlan <vlan_name 32> - 表示する対象の VLAN を VLAN 名で指定します。 vlanid <vidlist> - 表示する対象の VLAN を VLAN ID で指定します。 省略すると、すべての VLAN での状態が表示されます。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:MLD スヌーピングの状態を表示するには

```
# 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 mrouter_ports

目的	IPv6 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、現在の IPv6 ルーターポートを表示します。学習した IPv6 ルーターポートとスタティックエントリーの両方を表示することができます。
パラメーター	vlan <vlan_name 32> - 対象の VLAN を VLAN 名で指定します。 vlanid <vidlist> - 対象の VLAN を VLAN ID で指定します。 static - スタティック登録の IPv6 ルーターポートを表示します。 dynamic - 学習した IPv6 ルーターポートを表示します。 forbidden - forbidden(禁止)IPv6 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	1.00.01 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

#
```

3.20.9 show mld_snooping group

目的	IPv6 マルチキャストグループの情報を表示します。
構文	show mld_snooping group [vlan <vlan_name 32> | vlanid <vidlist>]
説明	本コマンドは、MLD スヌーピングで検出された IPv6 マルチキャストグループの情報を表示します。
パラメーター	<vlan_name 32> - 表示する VLAN を VLAN 名で指定します。 <vidlist> - 表示する VLAN を VID ID で指定します。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:IPv6 マルチキャストグループの情報を表示するには

```
#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
Port Member       :   1-2
Mode              :   INCLUDE

Source/Group      :   2000::100:10:10:5/FF0E::100:0:0:20
VLAN Name/VID     :   default/1
Port Member       :   3
Mode              :   EXCLUDE

#
```

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	スパニングツリープロトコルを有効にします。
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	1.00.01以降

使用例:スパニングツリープロトコルを有効にするには

```
#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	スパニングツリープロトコルを無効にします。
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	1.00.01 以降

使用例: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	スパニングツリーのバージョンを設定します。
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設定します。マルチプルスパニングツリープロトコル(MSTP)、ラピッドスパニングツリープロトコル(RSTP)、スパニングツリープロトコル(STP)から選択します。
パラメーター	mstp - MSTP を使用します。 rstp - RSTP を使用します。 stp - STP を使用します。
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	1.00.01 以降

使用例:マルチプルスパニングツリープロトコル(MSTP)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>]
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、STP 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」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	1.00.01 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 の範囲で値を定義し、外部コストを決定します。 小さい数字を指定すると、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。 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。 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> - ポートリストに指定されたポートに 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。 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	1.00.01 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	1.00.01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、VID (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。VID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VID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 VID を削除します。 <vidlist> -スイッチに設定済みの VLAN の中から、VID の範囲を指定します。ID 番号が 1～4094 の範囲でスイッチの VID 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	1.00.01 以降

使用例:インスタンス ID 2 を設定して VID 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 VID 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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                : 1
 Max Age                  : 20
 Forward Delay            : 15
 Last Topology Change     : 856
 Topology Changes Count   : 2987

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	1.00.01 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、インターバル時間毎に監視対象のトラフィックが閾値を超えた場合、閾値を超えた分の監視対象トラフィックを破棄します。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、インターバル時間毎にブロードキャストとマルチキャストの監視対象パケットが閾値を超え、「countdown」オプションで指定した時間内（0 秒～1800 秒）も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	パケットストーム制御を設定します。
構文	config traffic control < <portlist> | all > < broadcast < enable | disable > | multicast < enable | disable > | unicast < enable | disable > | action < drop | shutdown > | threshold <value 64-1000000> | countdown < secs 0-1800> | time_interval <secs 5-30> | recover_time <secs 10-300> >
説明	本コマンドは、パケットストーム制御機能を設定します。パケットストーム制御機能で制御されるパケットには、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があり、それぞれに対して動作を設定することができます。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。 <secs 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。 <secs 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(秒)を 1～1800 で指定します。1.03 以降から指定可能な時間が分から秒に変更されました。 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。 <secs 10-300> - 自動復旧待機時間を 10 秒～300 秒に設定します。デフォルト値は「300」です。action パラメーターで drop モードを指定した場合には適用できません。 1.03 以降から自動復旧待機時間を 10 秒～300 秒の範囲でユーザーが設定できるように変更されました。
制限事項	管理者アカウン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: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。 1.03以降からRecover timeのパラメーター追加により表示が追加されました。
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	1.00.01 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	ミラーポートを設定します。
構文	config mirror port <port> [<add | delete> source ports <portlist> < rx | tx | both >]
説明	本コマンドは、ミラーポートを設定します。ポートミラーリングでは、指定したポート(ミラー元ポート)を透過するトラフィックをコピーして、ターゲットポート（ミラー先ポート）に転送します。ターゲットポートにネットワークスニファーなどのデバイスを接続することで、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	1.00.01 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	ポートミラーリングを有効にします。
構文	enable mirror
説明	本コマンドは、ポートミラーリングを有効にします。有効にすると、ミラーポート設定に従ってトラフィックがミラーリングされます。
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	1.00.01 以降

使用例:ポートミラーリングを有効にするには

```
#enable mirror
Command: enable mirror

Success.

#
```

3.23.3 disable mirror

目的	ポートミラーリングを無効にします。
構文	disable mirror
説明	本コマンドは、ポートミラーリングを無効にします。ミラーポートが設定されていても、トラフィックはミラーリングされません。
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	1.00.01 以降

使用例:ポートミラーリングを無効にするには

```
#disable mirror
Command: disable mirror

Success.

#
```

3.23.4 show mirror

目的	ポートミラーリングの設定情報を表示します。
構文	show mirror
説明	本コマンドは、ポートミラーリングやミラーポート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	1.00.01 以降

使用例:ポートミラーリングの設定情報を表示するには

```
#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	本コマンドは、ポートセキュリティー機能を設定します。ポートセキュリティー機能は、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	1.00.01 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	ポートセキュリティーの特定の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> port <auth_port>
説明	本コマンドは、学習したポートセキュリティーエントリーを VLAN 名、MAC アドレス、ポート番号を指定して削除します。
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。 port <auth_port> - エントリーに対応するポート番号を入力します。
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	1.00.01 以降

使用例:ポートセキュリティーのエントリーを削除するには

```
#delete port_security_entry vlan_name default mac_address 00-04-66-10-2C-C7 port 6
Command: delete port_security_entry vlan_name default mac_address 00-04-66-10-2C-C7 port 6

Success.

#
```

3.24.3 clear port_security_entry port

目的	指定ポートのポートセキュリティーエントリーをクリアーします。
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	1.00.01 以降

使用例:ポート 6 で学習したポートセキュリティーの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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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 <int 1-16> - プロトコルグループのグループ ID を指定します。 group_name <name 32> - プロトコルグループ名を入力します。 vlan <vlan_name 32> - 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 <int> - VLAN ID を指定します。 priority <value 0-7> - 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	1.00.01 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	1.00.01 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	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	1.00.01 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	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	1.00.01 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	1.00.01 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 モードでのポートの役割およびポート外部 TPID。
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	1.00.01 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、無効(disable) 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	1.00.01 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を作成するか、現在のルールを置換します。
構文	create vlan_translation < add cvid <vidlist> svid <vlanid 1-4094> | replace cvid <vlanid 1-4094> svid <vlanid 1-4094> >
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	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。
制限事項	管理者アカウン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: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 cvid

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 cvid < <vidlist> | all >
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	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	1.00.01 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 cvid

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 cvid [<vidlist>]
説明	本コマンドは、設定済み VLAN トランスレーションルールを表示します。
パラメーター	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	1.00.01 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 cvid 10-40
Command: show vlan_translation cvid 10-40

CVID   SVID   Action
----   ----   ------
10     100    Add
20     100    Add
30     200    Add
40     400    Replace

Total Entries: 4

#
```

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	トラフィックセグメンテーションルールを設定します。
構文	config traffic_segmentation <portlist> forward_list < null | <portlist> >
説明	本コマンドは、トラフィックセグメンテーションルールを設定します。トラフィックセグメンテーションでは、入力ポートと転送先ポートリストの組み合わせによるルールを作成します。指定した入力ポートで受信したフレームは、ルールに従って転送先ポートリストに登録されているポートに転送されます。デフォルトでは、すべてのポートに対して転送先ポートリストをすべてのポートに設定されており、トラフィックセグメンテーションによる転送制限が行われません。
パラメーター	<portlist> - 入力ポートを指定します。 forward_list - 入力ポートで受信したフレームの転送先ポートを指定します。 null - ポートは指定されません。 <portlist> - 転送ポート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	1.00.01 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	トラフィックセグメンテーションの設定を表示します。
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設定を表示します。
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設定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	1.00.01 以降

使用例:スイッチ上のトラフィックセグメンテーションの設定を表示するには

```
#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port  Forward Portlist
----  ------------------------------------------------
1     1-24
2     1-24
3     1-24
4     1-24
5     1-24
6     1-24
7     1-24
8     1-24
9     1-24
10    1-24
11    1-24
12    1-24
13    1-24
14    1-24
15    1-24
16    1-24
17    1-24
18    1-24
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.28 VLAN コマンド

3.28.1 create vlan

目的	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、スイッチ上に VLAN を作成します。
パラメーター	<vlan_name 32> - VLAN 名を入力します。 <vlanid 1-4094> - 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	1.00.01 以降

使用例:VLAN ID が 2 の VLAN 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	VLAN を削除します。
構文	delete vlan <vlan_name 32> | vlanid <vidlist>
説明	本コマンドは、登録されている VLAN を削除します。VLAN 名もしくは VLAN ID で削除する VLAN を指定します。
パラメーター	<vlan_name 32> - 削除する VLAN を VLAN 名で指定します。 <vidlist> - 削除する VLAN を VLAN ID 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	1.00.01 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	VLAN をポートに割り当てます。
構文	config vlan <vlan_name 32> < < add < tagged | untagged | forbidden > | delete > <portlist> | advertisement < enable | disable > >
説明	本コマンドは、VLAN をポートに割り当てるか、割り当ての解除を行います。割り当てる場合は、「tagging」(タグ付き)、「untagging」(タグなし)、「forbidden」(禁止)のいずれかのタイプを指定します。デフォルトではすべてのポートに VLAN ID が 1 の「default」VLAN がタグなしで割り当てられています。
パラメーター	<vidlist> - 対象 VLAN を VLAN 名で指定します。 add - VLAN にポートを追加で割り当てます。VLAN の割り当てには以下の 3 つのタイプのいずれかを指定します。 tagged - タグ付きとして指定します。 untagged - タグなしとして指定します。 forbidden - 禁止ポートとして指定します。 delete - VLAN の割り当てを削除します。 <portlist> - 対象ポートを指定します。 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	1.00.01 以降

使用例:ポート 4～8 に VLAN「v1」をタグ付きで割り当てるには

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

Success.

#
```

使用例:ポート 6～8 から VLAN「v1」の割り当てを削除するには

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

Success.

#
```

注意事項

1 つの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。複数のタグなし 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は原則としてポート VLAN ID(PVID)を参照して所属する VLAN を決定します。

3.28.4 create vlan vlanid

目的	複数の VLAN を作成します。
構文	create vlan vlanid <vidlist> [advertisement]
説明	本コマンドは、VLAN ID を指定して複数の VLAN を作成します。
パラメーター	<vidlist> - 作成する VLAN を VLAN ID のリストで指定します。 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	1.00.01 以降

使用例:スイッチに VLAN ID 5,6 の VLAN 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	複数の VLAN を削除します。
構文	delete vlan vlanid <vidlist>
説明	本コマンドは、VLAN ID を指定して複数の VLAN を削除します。
パラメーター	<vidlist> - 対象の VLAN を VLAN ID のリストで指定します。
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	1.00.01 以降

使用例:スイッチの VLAN ID 5,6 の VLAN 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	複数の VLAN をポートに割り当てます。
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、VLAN ID を指定して複数の VLAN をポートに割り当てるか、割り当ての解除を行います。また、VLAN ID を一つだけ指定している場合は、VLAN 名の変更も行うことができます。
パラメーター	<vidlist> - 対象 VLAN を VLAN ID のリストで指定します。 add - VLAN にポートを追加で割り当てます。VLAN の割り当てには以下の 3 つのタイプのいずれかを指定します。 tagged - タグ付きとして指定します。 untagged - タグなしとして指定します。 forbidden - 禁止ポートとして指定します。 delete - VLAN の割り当てを削除します。 <portlist> - 対象ポートを指定します。 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。 name - VLAN 名を変更します。 <vlan_name 32> - 新たな VLAN 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	1.00.01 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。 デフォルト値は有効(enable)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	1.00.01 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	1.00.01 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	1.00.01 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	ポートに GVRP 設定や PVID を割り当てます。
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(GVRP)をポート単位で設定します。また、イングレスチェックやポート VLAN ID(PVID)を設定できます。PVID は、該当ポートにタグなしフレームを受信した場合のデフォルト VLAN を指し、MAC ベース VLAN などの動作により他の VLAN に動的に割り当てられない限り、PVID で指定された VLAN ID の VLAN として処理されます。
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 VLAN ID(PVID)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	1.00.01 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	GVRP を有効にします。
構文	enable gvrp
説明	本コマンドは、スイッチの GVRP 設定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	1.00.01 以降

使用例:GVRP をグローバルで有効にするには

```
#enable gvrp
Command: enable gvrp

Success.

#
```

3.28.12 disable gvrp

目的	GVRP を無効にします。
構文	disable gvrp
説明	本コマンドは、スイッチの GVRP 設定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	1.00.01 以降

使用例:GVRP をグローバルで無効にするには

```
#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	1.00.01 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    : 1-24
Static Ports    : 1-24
Current Tagged Ports   :
Current Untagged Ports : 1-24
Static Tagged Ports    :
Static Untagged Ports  : 1-24
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 port 1
Command: show vlan ports 1

Port 1
VLAN ID  Untagged  Tagged  Forbidden  Dynamic
-------  --------  ------  ---------  -------
 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	1.00.01 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、ARP テーブルのスタティックエントリーを作成します。ARP テーブルは、ホストの IP アドレスと MAC アドレスの対応を示すデータベースで、TCP/IP 通信を行う際に参照されます。
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	1.00.01 以降

使用例:IP アドレス「10.48.74.121」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 10.48.74.121 00-40-66-00-07-36
Command: create arpentry 10.48.74.121 00-40-66-00-07-36

Success.

#
```

3.29.2 config arpentry

目的	ARP テーブルのスタティックエントリーを編集します。
構文	config arpentry <ipaddr> <macaddr>
説明	本コマンドは、ARP テーブルに登録されているスタティックエントリーを編集します。本コマンドで編集可能なエントリーは、既に設定で登録されていて、かつ ARP テーブルに実際に登録されているものに限られます。
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	1.00.01 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 エントリーを編集するには

```
#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 テーブルの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	本コマンドは、設定されている ARP テーブルのスタティックエントリーを削除します。
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	1.00.01 以降

使用例：IP アドレス「10.48.74.121」を ARP テーブルから削除するには

```
#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

#
```

3.29.4 config arp_aging time

目的	ARP テーブルのエージング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	1.00.01 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	1.00.01 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       00-1D-60-E7-B5-CD  Dynamic
System          10.73.21.11      00-19-5B-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	1.00.01 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	デフォルトルートを設定します。
構文	create iproute default <ipaddr> [<metric 1-65535>]
説明	本コマンドは、デフォルトルートのエントリーを作成します。
パラメーター	<ipaddr> - ネクストホップルーターのゲートウェイ 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。
制限事項	管理者アカウン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:ゲートウェイ「10.0.0.254」のデフォルトルートを設定するには

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

Success.

#
```

3.30.2 delete iproute

目的	デフォルトルートを削除します。
構文	delete iproute default
説明	本コマンドは、デフォルトルートエントリーを削除します。
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:デフォルトルートを削除するには

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

Success.

#
```

3.30.3 show iproute

目的	IP ルート情報を表示します。
構文	show iproute [<network_address> | static]
説明	本コマンドは、スイッチの IP ルート情報を表示します。アクティブなコネクテッドルートやデフォルトルートを表示することができます。
パラメーター	<network_address> - 表示対象の宛先ネットワーク IP アドレスを指定します。 static - 設定したデフォルトルートを表示します。 パラメーターを指定しない場合、すべての有効な IP ルート情報を表示します。
制限事項	なし。
対応バージョン	1.00.01 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    Hops    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 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	1.00.01 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::20b:6aff:fecf:7ec6 00-40-66-03-04-05
Command: create ipv6 neighbor_cache ipif System fe80::20b:6aff:fecf:7ec6 00-40-66-03-04-05

Success.

#
```

3.30.5 delete ipv6 neighbor_cache ipif

目的	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 12> | all> - IPv6 インターフェース名を入力します。 all - 全ての IPv6 インターフェースを示します。 <ipv6addr> - ネイバーのアドレスを入力します。 static - スタティックエントリーを示します。 dynamic - ダイナミックエントリーを示します。 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	1.00.01 以降

使用例:IPv6 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> | all> - IPv6 インターフェース名を入力します。 all - 全ての IPv6 インターフェースを示します。 <ipv6addr> - ネイバーのアドレスを入力します。 static - スタティックエントリーを示します。 dynamic - ダイナミックエントリーを示します。 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を示します。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:IPv6 ネイバーを表示するには

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

Neighbor                                 Link Layer Address Interface    State
---------------------------------------  ----------------- ----------- -----
FE80::240:66FF:FE00:3                    00-11-22-33-44-55  System       T

Total Entries: 1

State:
(I) means Incomplete state. (R) means Reachable state.
(S) means Stale state.      (D) means Delay state.
(P) means Probe state.      (T) means Static state.

#
```

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	<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	1.00.01 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。 <ipif_name 12> - ルートのインターフェース名を指定します。 <ipv6addr> -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	1.00.01 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	IPv6 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 12> - 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	1.00.01 以降

使用例:IPv6 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 ルート情報を表示します。
構文	show ipv6route
説明	本コマンドは、IPv6 ルート情報を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 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: 1
Next Hop   : 3FFC::1                IPIF    : System


Total Entries: 1

#
```

3.30.11 config ipv6 nd ns ipif

目的	IPv6 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、IPv6 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 12> - 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	1.00.01 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 4 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 3 番キュー (クラス 3) 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 Q1 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 Q0 キューに割り当てられます。
優先度 3 は、スイッチの Q1 キューに割り当てられます。
優先度 4 は、スイッチの Q2 キューに割り当てられます。
優先度 5 は、スイッチの Q2 キューに割り当てられます。
優先度 6 は、スイッチの Q3 キューに割り当てられます。
優先度 7 は、スイッチの Q3 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 4 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 3 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	ポートでの帯域制御を設定します。
構文	config bandwidth_control <portlist> < rx_rate < no_limit | <value 64-1024000> > | tx_rate < no_limit <value 64-1024000> > >
説明	本コマンドは、ポート単位で帯域制御を設定します。帯域制御は受信(rx)、送信(tx)のそれぞれに対して帯域を指定し、指定帯域以上のトラフィックは制限されます。
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。 rx_rate - 対象ポートで受信するパケットの帯域制御を設定します。 no_limit - 受信帯域制御を行いません。 <value 64-1024000> - 受信帯域の制限値を[Kbps]で指定します。 tx_rate - 対象ポートから送信するパケットの帯域制御を設定します。 no_limit - 送信帯域制御を行いません。 <value 64-1024000> - 送信帯域の制限値を[Kbps]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	1.00.01 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

Note: To perform precise bandwidth control, it is required to enable the flow
control to mitigate the retransmission of TCP traffic.

The specified RX rate is not a multiple of 64, thus the closest
smaller multiple 64 is chosen.

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	帯域制御設定を表示します。
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	1.00.01 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	QoS の各キューの重み付けを設定します。
構文	config scheduling <class_id 0-3> weight <value 1-55>
説明	スイッチには 4 つのハードウェア優先キュー(Q0/Q1/Q2/Q3)があります。入力パケットは、これらのキューのうちのいずれかにマッピングされ、バッファに保管されます。本コマンドは、これらの 4 つのハードウェア優先キューに設定する重み付け(weight)を指定します。重み付けは、各キューのバッファに送信パケットが格納されているときに、どのキューからパケットの送信を開始するかを決定する際に参照されることがあります。 デフォルト値では、Q0<Q1<Q2<Q3 で重み付けが設定されており、送信時には Q3 が最も優先されます。実際のパケット送信順番は、各キューのバッファ状態と重み付けの値、およびスケジューリングメカニズムによって決定します。
パラメーター	<class_id 0-3> - 設定するハードウェア優先キューを指定します。 weight <value 1-55> - キューに設定する重み付けの値を指定します。1～55 の範囲で値を指定できます。
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	1.00.01 以降

使用例:キュー0 に重み付け値「55」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	QoS の各キューの重み付けを表示します。
構文	show scheduling
説明	本コマンドは、各ハードウェア優先キュー(Q0/Q1/Q2/Q3)に設定されている重み付けを表示じます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:各キューに設定されている重み付けを表示するには

```
#show scheduling
Command: show scheduling

QOS Output Scheduling

Class ID     Weight
---------   -------------
Class-0        1
Class-1        2
Class-2        4
Class-3        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 機能のスケジューリングメカニズムを設定します。スケジューリングメカニズムは、各キューのバッファに格納されたパケットを送信する順番を決定する方式で、weight fair と strict から選択します。strict の場合、を選択すると、優先度の高いキューからパケットを送信します。より優先度の低いキューのバッファに格納されたパケットは、優先度の高いキューのバッファが空になるまで、送信を開始しません。weight fair を選択すると、重み付けの大きいキューから順番にパケット送信を行い、均一に処理されます。
パラメーター	strict - スケジューリングメカニズムに strict を指定します。 weight_fair - スケジューリングメカニズムに weight fair 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	1.00.01 以降

使用例: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	QoS 機能のスケジューリングメカニズムを表示します。
構文	show scheduling_mechanism
説明	本コマンドは、QoS 機能の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	1.00.01 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

#
```

3.31.7 config 802.1p user_priority

目的	802.1p ユーザー優先度と優先キューをマップします。
構文	config 802.1p user_priority <priority 0-7> <class_id 0-3>
説明	本コマンドは、入力パケットの 802.1p ユーザー優先度とハードウェア優先キューのマッピングを設定します。スイッチは、入力したタグつきパケットを転送する際に、マッピングに従って各キューのバッファに格納します。 スイッチの初期状態では、以下の通り入力パケットの 802.1p ユーザー優先度の値に対して優先キューがマッピングされています。 802.1p　ハードウェアキュー　備考 0　1　中低 1　0　最低 2　0　最低 3　1　中低 4　2　中高 5　2　中高 6　3　最高 7　3　最高
パラメーター	<priority 0-7> - 802.1p ユーザー優先度を指定します。 <class_id 0-3> - マッピングする優先キュ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	1.00.01 以降

使用例:802.1p ユーザー優先度「1」に対して優先キューQ3 をマッピングするには

```
#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	802.1p ユーザー優先値と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 優先値とハードウェア優先キュー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	1.00.01 以降

使用例:802.1p ユーザー優先度と優先キューのマッピングを表示するには

```
#show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

Priority-0  ->  <Class-1>
Priority-1  ->  <Class-0>
Priority-2  ->  <Class-0>
Priority-3  ->  <Class-1>
Priority-4  ->  <Class-2>
Priority-5  ->  <Class-2>
Priority-6  ->  <Class-3>
Priority-7  ->  <Class-3>

#
```

3.31.9 config 802.1p default_priority

目的	802.1p デフォルト優先度を設定します。
構文	config 802.1p default_priority <<portlist> | all> <priority 0-7>
説明	本コマンドは、優先度情報がないタグなしパケットを受信した場合に割り当てる 802.1p 優先度をポート単位で設定します。
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 - スイッチのすべてのポートに適用します。 <priority 0-7> - 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	1.00.01 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	802.1p デフォルト優先度を表示します。
構文	show 802.1p default_priority [<portlist>]
説明	本コマンドは、802.1p デフォルト優先度を表示します。
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	1.00.01 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 <tos | dscp> - IP パケット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	1.00.01 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	1.00.01 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	ToS 値のトラフィッククラスマッピングを設定します。
構文	config cos tos value <value 0-7> <class <class_id 0-3>>
説明	本コマンドは、ToS 値とハードウェア優先キューのマッピングを設定します。
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 0-3> - 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、4 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 3(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	1.00.01 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	Tos 値のトラフィッククラスマッピングを表示します。
構文	show cos tos [value <value 0-7>]
説明	本コマンドは、ToS 値のトラフィッククラスマッピングを表示します。
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	1.00.01 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	DSCP 値のトラフィッククラスマッピングを設定します。
構文	config dscp_mapping dscp_value <value 0-63> < class <class_id 0-3> >
説明	本コマンドは、DSCP 値とハードウェア優先キューのマッピングを設定します。
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 0-3> - 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、4 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 3(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	1.00.01 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	DSCP 値のトラフィッククラスマッピングを表示します。
構文	show dscp_mapping [dscp_value <value 0-63>]
説明	本コマンドは、DSCP 値のトラフィッククラスマッピングを表示します。
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	1.00.01 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
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。

注意事項

APLGM シリーズでは ethernet、ip、ipv6、packet_content_mask の各タイプに対してルールを書き込むグループが装置内部に割り当てられ、独立して動作します。受信パケットが同一グループ内の複数ルールに該当する場合、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が、該当するルールが複数のグループに存在する場合、対象となる全てのグループに対して調査し、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。

ACL タイプ ipv6 と packet_content_mask、及び DHCP Snooping 機能は、最大でも 2 個までしか併用できません。また、2 個併用した場合は、一つのタイプに対して設定可能な ACL の最大ルール数が、最大合計登録数の約半分に制限されます。

APLGM シリーズで設定可能なルール数は ethernet、ip、ipv6、packet_content_mask の全てのタイプの合計で最大 256 です。一つのタイプに対して設定可能なルール数は、最大合計登録数を超えない範囲内では原則として制限はありませんが、以下の場合に登録数が制限されることがあります。

- **DCHP スヌーピング機能を有効にしている場合**
- **ACL タイプ ipv6 もしくは packet_content_mask のルールを使用している場合**

3.32.1 create access_profile

目的	ACL アクセスプロファイルを作成します。
構文	create access_profile < *ethernet* | *ip* | *ipv6* | *packet_content_mask* > profile_id <value 1-256> *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> > > *ipv6* =ipv6 < class | flowlabel | source_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>] > > *packet_content_mask* = packet_content_mask < offset1 <value 2-126> <hex 0x0-0xffffffff> | offset2 <value 2-126> <hex 0x0-0xffffffff> | offset3 <value 2-126> <hex 0x0-0xffffffff> | offset4 <value 2-126> <hex 0x0-0xffffffff> >
説明	本コマンドは、ACL のアクセスプロファイルを作成します。アクセスプロファイルは、入力するフレームのどの部分を調査するかを定義します。プロファイルでは最初にタイプの指定を行います。タイプは ethernet、ip、ipv6、packet_content_mask の 4 種類から選択可能で、調査するフレームの種類や調査箇所の分類を行います。ethernet タイプでは、イーサネットフレーム全般を調査対象とし、主にイーサネットヘッダ(送信元 MAC アドレスや宛先 MAC アドレスなどの情報が含まれる)を調査するルールを定めることができます。ip タイプ、ipv6 タイプは、それぞれ IPv4、IPv6 パケットを調査対象とし、IP ヘッダ/IPv6 ヘッダ(IP アドレス/IPv6 アドレス情報などが含まれる)や、その直後に続く上位プロトコルの情報を調査するルールを定めることができます。packet_content_mask は、ユーザー定義のプロファイルで、すべてのフレームを調査対象とし、調査箇所はユーザーが指定する箇所から始まる最大 4 バイトのフィールドを最大 4 個まで指定することができます。タイプを指定した後、調査するフィールドを指定します。調査対象となるフィールドはタイプによって異なり、例えば ethernet タイプを選択した場合、VLAN タグを調査する「vlan」、送信元 MAC アドレスを調査する「source_mac」、宛先 MAC アドレスを調査する「destination_mac」、EtherType を調査する「ethernet_type」、802.1p 優先度値を調査する「802.1p」から 1 個以上のフィールドを選択します。フィールドによっては、マスクを指定するものがあります。指定したフィールドのうち、どの箇所を参照するかを、マスクで指定することができます。アクセスプロファイルは、ルールを定めるための調査箇所の型を定義するもので、具体的にどのように処理を行うかは、プロファイル上に作成するアクセスルールによって定められます。

パラメーター	ethernet - イーサネットフレームを調査対象にします。 vlan - VLAN 情報を調査します。16 進数の 12 ビットマスクを指定します。 source_mac <macmask> - 送信元 MAC アドレスを調査します。MAC アドレス形式の 48 ビットマスクを指定します。 destination_mac <macmask> - 宛先 MAC アドレスを調査します。MAC アドレス形式の 48 ビットマスクを指定します。 802.1p - 802.1p 優先値を調査します。 ethernet_type - EtherType 値を調査します。 ip - IP パケットを調査対象にします。 vlan - VLAN 情報を調査します。12 ビットのマスクを指定します。 source_ip_mask <netmask> - 送信元 IP アドレスを調査します。IP アドレス形式の 32 ビットマスクを指定します。 destination_ip_mask <netmask> - 宛先 IP アドレスを調査します。IP アドレス形式の 32 ビットマスクを指定します。 dscp - DiffServ Code Point (DSCP)値を調査します。 icmp - Internet Control Message Protocol(ICMP)パケットであるかどうかを調査します。以下のオプションにより ICMP メッセージ内の一部を調査対象に含めることができます。 type - ICMP タイプフィールドを調査します。 code - ICMP コードフィールドを調査します。 igmp - Internet Group Management Protocol (IGMP)パケットであるかどうかを調査します。以下のオプションにより IGMP メッセージの一部を調査対象に含めることができます。 type - IGMP タイプフィールドを調査します。 tcp - Transport Control Protocol (TCP)パケットであるかどうかを調査します。以下のオプションにより TCP ヘッダの一部を調査対象に含めることができます。 src_port_mask <hex 0x0-0xffff> - 送信元 TCP ポートを調査します。16 進数の 16 ビットマスクを指定します。 dst_port_mask <hex 0x0-0xffff> - 宛先 TCP ポートを調査します。16 進数の 16 ビットマスクを指定します。 flag_mask - TCP ヘッダのコントロールフラグを調査します。コントロールフラグは 6 ビットの情報で、URG、ACK、PSH、RST、SYN、FIN のビットマップで構成されます。それぞれのビットに対して調査対象とするかどうかを指定します。all を選択した場合、すべてのビットが調査対象になります。 udp - Universal Datagram Protocol(UDP)パケットであるかどうかを調査します。以下のオプションにより UDP ヘッダの一部を調査対象に含めることができます。 src_port_mask <hex 0x0-0xffff> - 送信元 UDP ポートを調査します。16 進数の 16 ビットマスクを指定します。 dst_port_mask <hex 0x0-0xffff> - 宛先 UDP ポートを調査します。16 進数の 16 ビットのマスクを指定します。 protocol_id_mask - プロトコル ID フィールドを調査します。16 進数の 8 ビットマスクを指定します。

	ipv6 - IPv6 パケットを調査対象にします。 class - IPv6 クラスを調査します。 flowlabel - IPv6 フローラベルを調査します。 source_ipv6_mask - IPv6 送信元アドレスを調査対象にします。IPv6 アドレス形式の 64 ビットマスクを指定します。 tcp - TCP パケットであるかどうかを調査します。以下のオプションにより TCP ヘッダの一部を調査対象に含めることができます。 src_port_mask - 送信元 TCP ポート番号を調査します。16 進数の 16 ビットマスクを指定します。 dst_port_mask - 宛先 TCP ポート番号を調査します。16 進数の 16 ビットマスクを指定します。 udp - UDP パケットであるかどうかを調査します。以下のオプションにより UDP ヘッダの一部を調査対象に含めることができます。 src_port_mask - 送信元 UDP ポート番号を調査します。16 進数の 16 ビットマスクを指定します。 dst_port_mask - 宛先 UDP ポート番号を調査します。16 進数の 16 ビットマスクを指定します。 packet_content_mask - すべてのフレームを調査対象にします。offset1～offset4 で定義される任意の 4 箇所を調査対象とすることができます。 offset1～offset4 - ユーザー指定の箇所を調査します。調査箇所は offset1～offset4 で定義され、オフセット値 n で指定されます。指定したオフセット値に対して、入力フレームの先頭から n バイト目から開始する 4 バイトが調査対象になります。指定できるオフセット値は、2 から始まる 4 離れた離散値のみで、2、6、10、14、18、22、・・・・、126 となります。オフセット値 126 を指定すると、先頭から 126、127、0、1 バイトが調査対象になります。 profile_id <value 1-256> - アクセスプロファイルの識別子を指定します。この識別子はプロファイルの優先度にも使用されます。本製品の ACL では、タイプごとに独立して動作しますが、タイプが同一の複数のプロファイルが存在する場合は、最も低いプロファイル ID のルールから順番に調査します。プロファイル ID は 1～256 の範囲で指定します。
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	1.00.01 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 offset1 2 0xFFFFFFFF profile_id 3
Command: create access_profile packet_content_mask offset1 2 0xFFFFFFFF profile_id 3

Success.
#
```

3.32.2 delete access_profile

目的	ACL アクセスプロファイルを削除します。
構文	delete access_profile < profile_id <value 1-256> | all >
説明	本コマンドは、ACL 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 1-256> -削除するアクセスプロファイルをプロファイル ID で指定します。 all - すべてのアクセス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	1.00.01 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	ACL アクセスプロファイル上にアクセスルールを作成します。
構文	config access_profile profile_id <value 1-256> < add access_id < auto_assign | <value 1-65535> > < *ethernet* | *ip* | *ipv6* | *packet_content* > < port < <portlist> | all > > < permit [priority <value 0-7> [replace_priority] | replace_dscp_with <value 0-63> | counter < enable | disable >] | deny | mirror > | delete access_id <value 1-65535> > *ethernet* =ethernet < < vlan <vlan_name 32> | vlan_id <vid> [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 <vid> [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>]] *ipv6* =ipv6 [class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_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>]] *packet_content* =packet_content [offset1 <hex 0x0-0xffffffff> [mask <hex 0x0-0xffffffff >] | offset2 <hex 0x0-0xffffffff > [mask <hex 0x0-0xffffffff >] | offset3 <hex 0x0-0xffffffff > [mask <hex 0x0-0xffffffff >] | offset4 <hex 0x0-0xffffffff > [mask <hex 0x0-0xffffffff >]]
説明	本コマンドは、ACL アクセスプロファイル上にアクセスルールを設定します。設定するルールは、プロファイルで定義されたタイプに合致し、調査フィールドに含まれている必要があります。例えば、タイプ ethernet で定義されたプロファイル上にタイプ ip で設定するルールを設定することはできません。また、送信元 IP アドレスのみを調査対象とするプロファイル上では、宛先 IP アドレスを調査するルールを設定することはできません。設定するルールでは、プロファイルに含まれるすべての調査箇所を設定する必要はありません。調査箇所によってはマスクを設定できるものがありますが、プロファイル上のマスクと同一である必要はありません。例えば、プロファイル上で宛先 IP アドレスに対して 255.255.255.255（すべての宛

	先 IP アドレス情報を調査対象とする）というマスクが指定されていても、ルールでは 255.255.255.0 というマスクを適用することができます。この場合、該当する IP アドレスに対して 24 ビットのサブネットマスクを適用したネットワークアドレスのノード全体を指定します。 入力フレームが設定したルールに合致した場合の処理（アクション）は、permit、deny、mirror の 3 種類から選択します。permit では、入力フレームを許可します。このとき、優先度に関する処理などを指定することができます。deny は、入力フレームを許可せず破棄します。mirror は、ミラーリングポートに入力フレームを転送します。
パラメーター	profile_id <value 1-256> - アクセスプロファイルの ID を指定します。 add access_id <value 1-65535> - アクセスプロファイルにアクセスルールを追加します。設定する数値には作成するルールの識別子を指定します。この識別子は、同一プロファイルでの優先度にも使用され、最も低いアクセスルール ID を持つルールから順番に調査します。 auto_assign - アクセスルールの ID を自動的に割り当てます。同一プロファイル内で使用されていない最も小さい数字が割り当てられます。 ethernet - ethernet タイプのアクセスプロファイルのルールで使用します。以下の設定により調査対象やルールの合致条件を指定します。 vlan <vlan_name 32> - VLAN 情報を調査します。合致条件は VLAN 名で指定します。 vlan_id <vid> - VLAN 情報の調査します。合致条件は VLAN ID で指定します。mask オプションで 12 ビットマスクを指定することができます。 source_mac <macaddr> - 送信元 MAC アドレスを調査します。合致条件は MAC アドレス形式で指定します。mask オプションで MAC アドレス形式の 48 ビットマスクを指定できます。 destination_mac <macaddr> - 宛先 MAC アドレスを調査します。合致条件は MAC アドレス形式で指定します。mask オプションで MAC アドレス形式の 48 ビットマスクを指定できます。 802.1p <value 0-7> - 802.1p 優先値を調査します。合致条件は数値(0～7)で指定します。 ethernet_type <hex 0x0-0xffff> - EtherType を調査します。合致条件は 16 進数 16 ビットの情報で指定します。 ip - ip タイプのアクセスプロファイルのルールで使用します。以下の設定により調査対象やルールの合致条件を指定します。 vlan <vlan_name 32> - VLAN 情報を調査します。合致条件は VLAN 名で指定します。 vlan_id <vid> - VLAN 情報の調査します。合致条件は VLAN ID で指定します。mask オプションで 12 ビットマスクを指定することができます。 source_ip <ipaddr> - 送信元 IP アドレスを調査します。合致条件は IP アドレス形式で指定します。mask オプションで IP アドレス形式の 32 ビットマスクを指定できます。 destination_ip <ipaddr> - 宛先 IP アドレスを調査します。合致条件は IP アドレス形式で指定します。mask オプションで IP アドレス形式の 32 ビットマスクを指定できます。 dscp <value 0-63> - DSCP 値を調査します。合致条件は数値(0～63)で指定します。

	icmp - ICMP パケットを合致条件とします。以下のオプションにより ICMP メッセージ内の情報を調査対象に含めることができます。 type <0-255> - ICMP タイプフィールドを調査します。合致条件は数値(0～255)で指定します。 code <0-255> - ICMP コードフィールドを調査します。合致条件は数値(0～255)で指定します。 igmp - IGMP パケットを合致条件とします。以下のオプションにより IGMP メッセージ内の情報を調査対象に含めることができます。 type <0-255> - IGMP タイプフィールドを調査します。合致条件は数値(0～255)で指定します。 tcp - TCP パケットを合致条件とします。以下のオプションにより TCP ヘッダの情報を調査対象に含めることができます。 src_port <value 0-65535> - 送信元 TCP ポート番号を調査します。合致条件は数値(0～65535)で指定します。mask オプションで 16 進数の 16 ビットマスクを指定できます。 dst_port <value 0-65535> - 宛先 TCP ポート番号を調査します。合致条件は数値(0～65535)で指定します。mask オプションで 16 進数の 16 ビットマスクを指定できます。 flag - TCP ヘッダのコントロールフラグを調査します。合致条件は各フラグ(urg/ack/psh/rst/syn/fin)で指定します。all の場合はすべてのフラグが選択された状態で指定されます。 udp - UDP パケットを合致条件とします。以下のオプションにより UDP ヘッダの情報を調査対象に含めることができます。 src_port <value 0-65535> - 送信元 UDP ポート番号を調査します。合致条件は数値(0～65535)で指定します。mask オプションで 16 進数の 16 ビットマスクを指定できます。 dst_port <value 0-65535> - 宛先 UDP ポート番号を調査します。合致条件は数値(0～65535)で指定します。mask オプションで 16 進数の 16 ビットマスクを指定できます。 protocol_id <value 0-255> - プロトコル ID フィールドを調査します。合致条件は数値(0～255)で指定します。 ipv6 - ipv6 タイプのアクセスプロファイルのルールで使用します。以下の設定により調査対象やルールの合致条件を指定します。 class - IPv6 クラスを調査します。合致条件は数値(0～255)で指定します。 flowlabel - IPv6 フローラベルを調査します。合致条件は 16 進数 20 ビットで指定します。 source_ipv6_mask - IPv6 送信元アドレスを調査します。合致条件は IPv6 アドレス形式で指定します。 tcp - TCP パケットを合致条件とします。以下のオプションにより TCP ヘッダの情報を調査対象に含めることができます。 src_port - 送信元 TCP ポート番号を調査します。合致条件は数値(0～65535)で指定します。mask オプションで 16 進数の 16 ビットマスクを指定できます。 dst_port - 宛先 TCP ポート番号を調査します。合致条件は数値(0～65535)で指定します。mask オプションで 16 進数の 16 ビットマスクを指定できます。

	udp - UDP パケットを合致条件とします。以下のオプションにより UDP ヘッダの情報を調査対象に含めることができます。 src_port - 送信元 UDP ポート番号を調査します。合致条件は数値(0～65535)で指定します。mask オプションで 16 進数の 16 ビットマスクを指定できます。 dst_port - 宛先 UDP ポート番号を調査します。合致条件は数値(0～65535)で指定します。mask オプションで 16 進数の 16 ビットマスクを指定できます。 packet_content - packet_content_mask タイプのアクセスプロファイルで使用します。以下の設定により調査対象やルールの合致条件を指定します。 offset1 - offset4 - アクセスプロファイルで定義した箇所を調査します。合致条件は 16 進数 32 ビットで指定します。 port <portlist> - ルールを適用するスイッチのポート番号を指定します。設定したポートに入力するパケットがアクセスルールの調査対象になります。all はすべてのポートが対象になります。 permit - ルールに合致するパケットを許可します。以下のオプションにより、転送時の処理を行うことができます。 priority <value 0-7> - 入力したパケットを、指定した値(0～7)の 802.1p 優先度を持つパケットとみなして処理し、所定のハードウェア優先キューに転送します。replace_priority オプションを追加すると、パケットの 802.1p 優先度自体を書き換えることができます。 replace_dscp_with <value 0-63> - 入力パケットの DSCP 値を指定した値(0-63)に書き換えます。 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。デフォルトでは無効になっています。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 - ルールに合致するパケットをフィルタリングします。 mirror - ルールに合致するパケットをミラーリングします。 delete access_id <value 1-65535> - 指定したアクセスルールを削除します。
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	1.00.01 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.

#
```

3.32.4 show access_profile

目的	ACL アクセスプロファイルとアクセスルールを表示します。
構文	show access_profile [profile_id <value 1-256>]
説明	本コマンドは、ACL アクセスプロファイルと登録されているアクセスルールを表示します。
パラメーター	profile_id <value 1-256> - プロファイル ID を指定して 1 つのプロファイル ID に対するアクセスルールのみを表示します。プロファイル ID 番号を 1～256 の範囲で入力します。
制限事項	なし。
対応バージョン	1.00.01 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

================================================================================
Profile ID: 1                          Type: Ethernet Frame Filter
================================================================================
Owner: ACL
Masks  Option
VLAN             Source MAC        Destination MAC   802.1P Eth Type
---------------- ----------------- ----------------- ------ --------
0xFFF            00-00-00-00-00-01 00-00-00-00-00-02

================================================================================
Profile ID: 2                          Type: IPv4 Frame Filter - ICMP
================================================================================
Owner: ACL
Masks  Option
VLAN             Source IP       Dest. IP        DSCP Prot Type Code
---------------- --------------- --------------- ---- ---- ---- ----
0xFFF            20.0.0.0        10.0.0.0             ICMP

================================================================================
Total Profile Entries: 2

Total Used Rule Entries: 0

Total Unused Rule Entries: 256

#
```

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 1-256> access_id <access_id> < < rate <value 64-1024000> burst_size <value 4-16384> 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 - プロファイル ID 番号を指定します。 access_id - アクセス ID 番号を指定します。 rate - シングルレート 2 カラーモードのレートを指定します。フローの認定帯域幅を Kbps で指定します。最小レートは 64 Kbps で、設定可能な最大レートは 1,024,000 です。 burst_size - 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 4 K バイトで、最大値は 16384 K バイトです。バーストサイズの有効値は 4K バイトの倍数です。 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	1.00.01 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 1-256> [access_id <access_id>]]
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 1-256> - プロファイル ID 番号を指定します。 access_id <access_id> - 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	1.00.01 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

本スイッチは、IEEE 802.1X ポートベースおよびホストベースアクセス制御機能が搭載されています。このメカニズムは、ポートがフレームを送受信する前に満たさなければならない各ポートの条件を各ポートに設定することにより、認証ユーザーまたは他のネットワークデバイスがネットワークリソースにアクセスできる許可を与えることを意図します。

3.34.1 enable 802.1x

目的	802.1X 認証機能を有効にします。
構文	enable 802.1x
説明	本コマンドは、802.1X 認証機能のグローバル設定を有効にします。
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	1.00.01 以降

使用例:802.1X 認証機能を有効にするには

```
#enable 802.1x
Command: enable 802.1x

Success.

#
```

注意事項

動的 VLAN を使用する場合、割り当て可能な最大収容数は 64 端末です。
最大数 64 には、MAC/Web/802.1X の各認証で使用する動的 VLAN の端末数を含みます。
（動的 VLAN を使用しない端末は、この最大収容数には含まれません）

端末の認証情報は VLAN とバインドして登録されます。そのため、認証端末が既に当該 VLAN に存在しないと装置が判定すると、端末の認証を解除します。

3.34.2 disable 802.1x

目的	802.1X 認証機能を無効にします。
構文	disable 802.1x
説明	本コマンドは、802.1X 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	1.00.01 以降

使用例:802.1X 認証機能を無効にするには

```
#disable 802.1x
Command: disable 802.1x

Success.

#
```

3.34.3 config 802.1x auth_protocol

目的	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、802.1X 認証プロトコルを指定します。ローカル認証、もしくは RADIUS プロトコルを使用した認証を選択します。
パラメーター	local | radius_eap - 使用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	1.00.01 以降

使用例:認証プロトコルを RADIUS 方式に設定するには

```
#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。

3.34.4 config 802.1x auth_failover

目的	802.1X 認証の failover を設定します。
構文	config 802.1x auth_failover < enable [mode < permit [vlanid <vlanid 1-4094 >] > | local] | disable >
説明	本コマンドは、802.1X 認証で RADIUS サーバーの認証応答がない場合、ローカルデータベース認証、または強制的に認証許可を行う failover 機能を設定します。
パラメーター	enable - 認証サーバーから応答がない時、failover 機能を使用します。 permit - 認証サーバーから応答がない時、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 - 認証から応答がない時、ローカルデータベースによる認証を行います。 disable - 認証サーバーから応答がない時に、failover 機能を使用しません。
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	1.09.00 以降

使用例: 802.1X 認証で failover 機能を有効にするには

```
#config 802.1x auth_failover enable mode permit vlanid 3
Command: config 802.1x auth_failover enable mode permit vlanid 3

Success.

#
```

注意事項

フェイルオーバー機能における強制的な認証許可(Permit)は、セキュリティ上問題となる可能性があるため、十分検討の上、使用してください。

強制的な認証許可(Permit)は、設定されている RADIUS サーバー全てがタイムアウトの時に、サプリカントに EAP-Success を返します。しかし、サプリカントの仕様によっては EAP-Success 受信後も認証成功状態にならず、通信出来ない場合や認証成功後も EAPOL-Start 送信を繰り返し、認証処理を繰り返す場合もあります。

フェイルオーバー機能は、RADIUS サーバーの認証応答がタイムアウトした際に動作する機能です。認証失敗の応答を受信した場合は動作しません。

フェイルオーバー機能設定時、RADIUS サーバーのタイムアウト時間は 30 秒以内に設定してください。デフォルト設定は 15 秒です。

3.34.5 config 802.1x capability ports

目的	ポート単位で 802.1X 認証を設定します。
構文	config 802.1x capability ports < <portlist> | all > <authenticator | none>
説明	本コマンドは、802.1X 認証を実施するポートを設定します。
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 - 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	1.00.01 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 auth_parameter ports

目的	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> | enable_reauth < enable | disable > >
説明	本コマンドは、ポート単位の 802.1X 認証パラメーターを設定します。default パラメーターは、対象ポートの 802.1X 認証設定をデフォルト値に戻します。
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 - 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、802.1X 認証を行うポートが、送受信両方(both)または受信方向だけ(in)の通信を制御するかを設定します。 port_control - 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、802.1X 認証を行うポートでは「auto」を指定します。 force_unauth - ポートを強制的に非認証状態にします。 auto - ポートで 802.1X 認証を行った結果を状態に反映します。 force_auth - ポートを強制的に認証済みの状態にします。 quiet_period <sec 0-65535> - 認証失敗後のブロック時間を設定します。サプリカントが認証に失敗すると、ブロック時間が経過するまでは再度サプリカントから認証を試行しても応答しません。 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 以外のすべての 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 <sec 1-65535> - 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。 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	1.00.01 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.

#
```

3.34.7 config 802.1x init

目的	ポートの 802.1X 認証を初期化します。
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、指定したポートの 802.1X 認証をただちに初期化します。
パラメーター	port_based - ポートベース認証で 802.1X 認証を初期化する際に指定します。 mac_based - ホストベース認証で 802.1X 認証を初期化する際に指定します。初期化を実施する対象ホストを MAC アドレスで指定することができます。 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> - 初期化するホストの 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	1.00.01 以降

使用例:すべてのポートの認証状態を初期化するには

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

Success.

#
```

3.34.8 config 802.1x reauth

目的	802.1X 認証の再認証を行います。
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、指定したポートで 802.1X 認証の再認証をただちに行います。
パラメーター	port_based - ポートベース認証で再認証を行う際に指定します。 mac_based - ホストベース認証で再認証を行う際に指定します。再認証を行う対象ホストを MAC アドレスで指定することができます。 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> - 再認証するホストの 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	1.00.01 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.

#
```

3.34.9 config radius add

目的	RADIUS サーバーを登録します。
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、認証に使用する RADIUS サーバーを設定します。
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。登録したインデックス番号の小さい順に RADIUS の応答を確認し、最初に応答した RADIUS サーバー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 <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 ポート番号を設定します。 auth_port <udp_port_number 1-65535> - 認証リクエストに対する UDP ポート番号を設定します。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 ポート番号を設定します。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	1.00.01 以降

使用例:RADIUS サーバーを登録するには

```
#config radius add 1 10.48.74.121 key APS default
Command: config radius add 1 10.48.74.121 key APS default

Success.

#
```

3.34.10 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> | acct_port <udp_port_number 1-65535>]
説明	登録した RADIUS サーバーの設定を変更します。
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> - 認証リクエストに対する UDP ポート番号を変更します。 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 ポート番号を変更します。
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	1.00.01 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.

#
```

3.34.11 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	1.00.01 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.

#
```

3.34.12 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	1.00.01 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.

#
```

3.34.13 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	1.00.01 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.

#
```

3.34.14 delete 802.1x user

目的	802.1X 認証のローカルユーザーを削除します。
構文	delete 802.1x user <username 15>
説明	本コマンドは､登録されている 802.1X 認証のローカルユーザーを削除します。
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	1.00.01 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.

#
```

3.34.15 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 auth_configuration 実行時に表示されるパラメーターの説明> 802.1X Enabled / Disabled - 802.1X 認証の現在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。 Authentication Failover - failover 機能の現在のステータスを表示します。 Failover Mode - failover 機能における認証方法を表示します。 Permit VLAN ID - failover 機能で permit 指定の所属 VLAN ID を表示します。 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 - 連続する再認証の間隔を表示します。 ReAuthenticate: Enabled / Disabled - 再認証を行うかどうかを表示します。 <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。 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	1.00.01 以降

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

802.1X                    : Enabled
Authentication Mode       : Port_based
Authentication Protocol   : Radius_EAP
Authentication Failover   : Enabled
Failover Mode             : Permit
Permit VLAN ID            : 3

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

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

Port Number : 1
Index  MAC Address        Auth PAE State  Backend State  Port Status
------ ----------------- -------------  -------------  -----------
1      00-40-66-4D-4E-0A  Connecting     Idle           Unauthorized
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

3.34.16 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	1.00.01 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

#
```

3.34.17 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	1.00.01 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

Index  UserName
 ----   ------------
 1      ctsnow

Total Entries: 1

#
```

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	1.00.01 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	1.00.01 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	1.00.01 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>]
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 - 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	1.00.01 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	1.00.01 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
```

3.35 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 3 つ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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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表示します。「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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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、その要求を認証または拒否します。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	1.00.01 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	1.00.01 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。 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。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	1.00.01 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	1.00.01 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 (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 認証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 認証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+認証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 認証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	1.00.01 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	1.00.01 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。 IP Address - サーバーの IP アドレス。 Protocol - サーバーが使用する認証プロトコル。
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	1.00.01 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	1.00.01 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	1.00.01 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を表示します。 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	1.00.01 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	1.00.01 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	1.00.01 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機能を有効にします。
構文	enable mac_based_access_control
説明	本コマンドは、MAC ベースアクセス制御機能のグローバル設定を有効にします。MAC ベースアクセス制御機能は、接続ホストの MAC アドレスを使用して認証を行い(MAC アドレス認証)、トラフィック制御を行う機能です。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	1.00.01 以降

使用例:MAC ベースアクセス制御機能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

Ver.1.05 以降のファームウェアより、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。

動的 VLAN を使用する場合、割り当て可能な最大収容数は 64 端末です。
最大数 64 には、MAC/Web/802.1X の各認証で使用する動的 VLAN の端末数を含みます。
（動的 VLAN を使用しない端末は、この最大収容数には含まれません）

端末の認証情報は VLAN とバインドして登録されます。そのため、認証端末が既に当該 VLAN に存在しないと装置が判定すると、端末の認証を解除します。

3.36.2 disable mac_based_access_control

目的	MAC ベースアクセス制御機能を無効にします。
構文	disable mac_based_access_control
説明	本コマンドは、MAC ベースアクセス制御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	1.00.01 以降

使用例:MAC ベースアクセス制御機能のグローバル設定を無効にするには

```
# disable mac_based_access_control
Command: disable mac_based_access_control

Success.

#
```

3.36.3 config mac_based_access_control 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 <no_limit | <value 1-128> > >
説明	本コマンドは、ポート単位で MAC ベースアクセス制御を実行するかを設定し、認証時のパラメーターを設定します。MAC ベースアクセス制御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 <<portlist> | all> - ポート範囲を設定します。 all - すべてのポートが対象となります。 state <enable | disable> - MAC ベースアクセス制御を有効または無効にします。 aging_time <infinite | <min 1-1440>>- 認証ホストが認証状態を保つ時間です。タイムアウトするとホストは未認証状態になります。デフォルト値は、1440 分です。 infinite - タイムアウトしません。 hold_time <infinite | <sec 1-300>> - 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しません。デフォルト値は 300 秒です。 infinite - 認証は再開しません。 max_users <no_limit | <value 1-128>> - ポート毎に収容可能な端末数を指定します。なお、ポート毎の収容数の総和は、装置全体の収容数(初期値128)設定の範囲内で制限されます。 no_limit - ポート毎の制限はありません。
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	1.00.01 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.

#
```

3.36.4 config mac_based_access_control method

目的	MAC アドレス認証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、MAC アドレス認証の認証方式を指定します。ローカル認証、もしくは RADIUS サーバーによる認証を選択します。
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	1.00.01 以降

使用例:MAC アドレス認証の方式を設定するには

```
#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

#
```

3.36.5 config mac_based_access_control mac_format

目的	MAC アドレス認証の 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 サーバーで MAC アドレス認証を行う際の MAC アドレスの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	1.06.00 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.

#
```

3.36.6 config mac_based_access_control password_type

目的	MAC アドレス認証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 サーバーで MAC アドレス認証を行う際に使用するパスワードの方式を設定します。
パラメーター	manual_string - すべてのクライアントで共通パスワードを使用します。 client_mac_address - クライアントのMACアドレスをパスワードに使用します。共通パスワードは使用されません。
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	1.06.00 以降

使用例:MAC アドレス認証で共通パスワード方式に設定するには

```
# config mac_based_access_control password_type manual_string
Command: config mac_based_access_control password_type manual_string

Success.

#
```

3.36.7 config mac_based_access_control password

目的	MAC アドレス認証の共通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、MAC アドレス認証で使用する共通パスワードを設定します。
パラメーター	<passwd 16> - すべてのクライアントの MAC アドレス認証で使用される共通パスワードを設定します。
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	1.00.01 以降

使用例:MAC アドレス認証の共通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.

#
```

3.36.8 config mac_based_access_control auth_failover

目的	MAC アドレス認証の failover を設定します。
構文	config mac_based_access_control auth_failover < enable [mode < permit [vlanid <vlanid 1-4094 >] > | local] | disable >
説明	本コマンドは、MAC アドレス認証で RADIUS サーバーからの認証応答がない場合、ローカルデータベースによる認証、または強制的に認証許可を行う failover 機能を設定します。
パラメーター	enable - 認証サーバーから応答がない場合の failover 機能を有効にします。 permit - 認証サーバーからの応答がない時、強制的に認証許可を行います。 vlanid <vlanid 1-4049> - 認証許可後に所属する vlanid を設定します。 local - 認証サーバーから応答がない時、ローカルデータベースによる認証を行います。 disable - 認証サーバーから応答がない場合の failover 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	1.03.00 以降 1.09.00 以降(permit パラメーター)

使用例:MAC アドレス認証で failover 機能を有効にするには

```
#config mac_based_access_control auth_failover enable
Command: config mac_based_access_control auth_failover enable

Success.

#
```

注意事項

フェイルオーバー機能における強制的な認証許可(Permit)は、セキュリティ上問題となる可能性があるため、十分検討の上、使用してください。

フェイルオーバー機能設定時、RADIUS サーバーのタイムアウト時間は 30 秒以内に設定してください。デフォルト設定は 15 秒です。

3.36.9 config mac_based_access_control max_users

目的	MAC アドレス認証の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 < no_limit | <value 1-128> >
説明	本コマンドは、装置全体でMACアドレス認証クライアントを収容可能な最大数を指定します。
パラメーター	no_limit - ポート毎の収容数(初期値128)設定と併せてno_limit指定した場合、使用環境下によりますが、目安として512端末程度の利用が可能です。 max_users <value 1-128> - 装置全体で収容可能な端末数を 1～128 で入力します。デフォルト値は、128 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	1.00.01 以降

使用例:MAC ベースアクセス制御の最大ユーザー数を 128 に設定するには

```
#config mac_based_access_control max_users 128
Command: config mac_based_access_control max_users 128

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。

3.36.10 enable authorization network

目的	MAC アドレス認証での認証属性の割り当てを有効にします。
構文	enable authorization network
説明	本コマンドは、MAC アドレス認証時に付与される認証属性の割り当てを有効にします。有効にすると、認証ホストに付与された認証属性をポートに反映することができます。認証属性に所定の VLAN 情報が含まれると、認証ホストによって動的に VLAN を決定することができます。(ダイナミック VLAN)。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	1.00.01 以降

使用例:MAC アドレス認証による認証属性の割り当てを有効にするには

```
#enable authorization network
Command: enable authorization network

Success.

#
```

注意事項

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 Ingress 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。

3.36.11 disable authorization network

目的	MAC アドレス認証での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、MAC アドレス認証時に付与される認証属性の割り当てを無効にします。無効の場合、認証ホストに付与される認証属性はポートに反映されず、無視されます。 MAC アドレス認証の認証属性の割り当てはデフォルトで無効です。
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	1.00.01 以降

使用例:MAC アドレス認証での認証属性の割り当てを無効にするには

```
#disable authorization network
Command: disable authorization network

Success.

#
```

3.36.12 create mac_based_access_control_local mac

目的	MAC アドレス認証のローカルユーザーを登録します。
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、MAC アドレス認証のユーザーをローカルデータベースに登録します。
パラメーター	mac <macaddr> - ローカルユーザーの MAC アドレスを指定します。 vlan <vlan_name 32> - 付与する認証属性(VLAN)を VLAN 名で指定します。 vlanid <vlanid 1-4094> - 付与する認証属性(VLAN)を VLAN ID 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	1.00.01 以降

使用例:MAC アドレス認証のローカルユーザーを登録するには

```
#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.

#
```

3.36.13 config mac_based_access_control_local mac

目的	MAC アドレス認証のローカルユーザーを編集します。
構文	config 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に登録されている MAC アドレス認証のユーザー情報を編集します。
パラメーター	mac <macaddr> - ローカルユーザーの MAC アドレスを指定します。 vlan <vlan_name 32> - 付与する認証属性(VLAN)を VLAN 名で指定します。 vlanid <vlanid 1-4094> - 付与する認証属性(VLAN)を VLAN ID 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	1.00.01 以降

使用例:MAC アドレス認証のローカルユーザーを編集するには

```
# 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.

#
```

3.36.14 delete mac_based_access_control_local

目的	MAC アドレス認証のローカルユーザーを削除します。
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に登録されている MAC アドレス認証のユーザーエントリーを削除します。
パラメーター	mac <macaddr> - 削除するローカルユーザーの MAC アドレスを指定します。 vlan <vlan_name 32> - 特定の認証属性(VLAN)が付与されたローカルユーザーを削除する際に、対象となる VLAN を VLAN 名で指定します。 vlanid <vlanid 1-4094> - 特定の認証属性(VLAN)が付与されたローカルユーザーを削除する際に、対象となる VLAN を VLAN ID 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	1.00.01 以降

使用例:MAC アドレス認証のローカルユーザーを削除するには

```
#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.

#
```

3.36.15 clear mac_based_access_control auth_mac

目的	MAC ベースアクセス制御をリセットします。
構文	clear mac_based_access_control auth_mac < ports < all | <portlist> > | mac_addr <macaddr> >
説明	本コマンドは、MAC ベースアクセス制御で認証されたユーザーあるいはポートの認証状態をリセットします。指定したポートあるいはユーザーは未認証状態に戻ります。再認証はユーザートラフィックを受信した際に行われます。
パラメーター	ports <all | <portlist>> - MAC ベースアクセス制御をリセットするポート範囲を指定します。すべてのポートを設定する場合は、「all」を指定します。 mac_addr <macaddr> - MAC ベースアクセス制御をリセットするホストを MAC アドレスで指定します。
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	1.00.01 以降

使用例:MAC ベースアクセス制御をリセットするには

```
#clear mac_based_access_control auth_mac ports all
Command: clear mac_based_access_control auth_mac ports all

Success.

#
```

3.36.16 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。グローバル設定、もしくはポート単位の設定を選択して表示することができます。
パラメーター	ports - ポート単位の設定を表示する場合に指定します。 all - 全てのポートを対象とする場合に指定します。 パラメーターを指定しない場合、グローバル設定を表示します。
制限事項	なし。
対応バージョン	1.00.01 以降

使用例:MAC ベースアクセス制御の設定(グローバル)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                  : RADIUS
Authentication Failover: Enabled
Failover Mode           : Permit
Permit VLAN ID          : 3
MAC Format Case         : Uppercase
MAC Format Delimiter    : None
Password                : default
Password Type           : Manual String
Max Users               : 128

#
```

使用例:MAC ベースアクセス制御の設定(ポート単位)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   Auth Mode    Max Users
                   (mins)       (secs)
------ -------- ---------- --------- ----------- -----------
1      Enabled    100          100         Port_based   128
2      Enabled    100          200         Host_based   128
3      Enabled    50           300         Port_based   128
4      Enabled    200          100         Host_based   128
#
```

3.36.17 show mac_based_access_control_local

目的	MAC アドレス認証のローカルユーザーを表示します。
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 アドレス認証のローカルデータベースに登録されているユーザーの情報を表示します。
パラメーター	mac <macaddr> - 表示するローカルユーザーの MAC アドレスを指定します。 vlan <vlan_name 32> - 特定の認証属性(VLAN)が付与されたローカルユーザーを表示する際に、対象となる VLAN を VLAN 名で指定します。 vlanid <vlanid 1-4094> - 特定の認証属性(VLAN)が付与されたローカルユーザーを削除する際に、対象となる VLAN を VLAN ID で指定します。 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	1.00.01 以降

使用例:MAC アドレス認証のローカルユーザーをすべて表示するには

```
#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 アドレス認証の特定のローカルユーザーを表示するには

```
#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

#
```

使用例:MAC アドレス認証のローカルユーザーを認証属性(VLAN)を指定して表示するには

```
#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address              VLAN Name                      VID
----------------    ---------------------           ------
00-40-66-00-00-01    default                         1

Total Entries: 1

#
```

3.36.18 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によるポートの認証状態を表示します。
パラメーター	ports <portlist> - 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	1.00.01 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 ports 9
Command: show mac_based_access_control auth_mac ports 9

Port Number : 9
Index MAC Address       Auth State     VID  Aging Time/
                                           Hold Time
----- ---------------- ------------- ---- -----------
1     00-40-66-00-00-00 Authenticated  200  45
2     00-40-66-00-00-05 Failure        1    1

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

3.36.19 show authorization

目的	MAC ベースアクセス制御の認証属性の割り当ての設定を表示します。
構文	show authorization
説明	本コマンドは、スイッチの MAC ベースアクセス制御の認証属性の割り当て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	1.00.01 以降

使用例:MAC ベースアクセス制御の認証属性の割り当ての設定を表示するには

```
#show authorization
Command: show authorization

Authorization : Enabled

#
```

3.37 マルチプル認証コマンド

3.37.1 config authentication auth_mode

目的	ポート認証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、ポート認証(MAC/802.1X/Web 認証)の認証モードを設定します。認証モードにはポートベースとホストベースがあり、ポートベースでは各ポートで１台の認証のみを行い、認証に成功すれば同一ポートのすべてのホストでアクセスが許可されます。ホストベースでは、各ポートですべてのホストに対して個別に認証を行います。
パラメーター	port_based - ポートベース認証モードを指定します。 host_based - ホストベース認証モードを指定します。
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	1.00.01 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.

#
```

注意事項

ホストベース認証モードでダイナミック VLAN を動作させた場合、認証端末は MAC VLAN データベースにダイナミックエントリーとして登録されます。MAC VLAN データベースはハッシュテーブルを使用しており、衝突によりダイナミックエントリーを登録できず、ダイナミック VLAN が動作しない場合があります。

3.37.2 show authentication ports

目的	ポート認証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、ポート認証(MAC/802.1X/Web 認証)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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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	1.00.01 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 Authmode:
-----------------------------------------------
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 > >
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 秒の範囲で時間を設定します。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。
制限事項	管理者アカウン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：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	1.00.01 以降

使用例：SSH サーバーを表示するには

```
#show ssh server
Command: show ssh server

SSH Server Status             : Disabled
SSH Max Session               : 8
Connection Timeout            : 120 (sec)
Authenticate Failed Attempts  : 2
Rekey Timeout                 : never
Listened 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 - 認証用にリモート 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、SSH 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	1.00.01 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	1.00.01 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を 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 twofish256 - Twofish256 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 暗号化を「enable」(有効)または「disable」(無効)にします。 <enable | disable> - スイッチに本コマンドで入力したアルゴリズムを「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	1.00.01 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	1.00.01 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、128 ビット鍵の RC4 ストリーム暗号に対応します。こ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 及び 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 3 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、SSLv3.0、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	1.00.01 以降 (version オプションは 1.12.00 以降)

使用例: 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.

#
```

使用例:特定の TLS バージョン及び暗号スイートを有効にするには

```
#enable ssl version tls1.1 tls1.2 ciphersuite RSA_with_AES_128_CBC_SHA
Command: enable ssl version tls1.1 tls1.2 ciphersuite RSA_with_AES_128_CBC_SHA

Success.

#
```

注意事項

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	1.00.01 以降 (version オプションは 1.12.00 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:特定の TLS バージョン及び暗号スイートを有効にするには

```
#disable ssl version tls1.1 ciphersuite RSA_with_AES_128_CBC_SHA
Command: disable ssl version tls1.1 ciphersuite RSA_with_AES_128_CBC_SHA

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	1.00.01～1.13.00

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.

#
```

注意事項

SSL キャッシュを利用した場合に、HTTPS を使用した WEB 管理画面へのアクセスや HTTPS での WEB ブラウジングを起点とした WEB 認証アクセスといった、SSL を使用する WEB アクセスを累積して実行すると、WEB 認証や WEB 管理画面へのアクセス(HTTP/HTTPS)が一切動作しなくなる事象を確認しています。当該事象の対策として、Ver．1.13.01 以降のバージョンでは SSL キャッシュを無効にしています。

3.39.4 download ssl certificate

目的	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	1.00.01 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

ファームウェアのバージョンによってダウロード可能な証明書及び秘密鍵のファイルサイズが異なります。
Ver1.06.00 以降：証明書ファイルは 8192 バイト、秘密鍵ファイルは 4096 バイトのファイルサイズまでダウンロードが可能です。
Ver1.05.01 以前：証明書ファイルは 2048 バイト、秘密鍵ファイルは 1024 バイトのファイルサイズまでダウンロードが可能です。

3.39.5 show ssl

目的	SSL 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	1.00.01 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                                    Disabled
 TLS 1.1                                    Disabled
 TLS 1.2                                    Enabled

 Cipher Suites:
 RSA_WITH_RC4_128_MD5                0x0004 Disabled
 RSA_WITH_3DES_EDE_CBC_SHA           0x000A Disabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA       0x0013 Disabled
 RSA_WITH_AES_128_CBC_SHA            0x002F Disabled
 RSA_WITH_AES_256_CBC_SHA            0x0035 Disabled
 RSA_WITH_AES_128_CBC_SHA256         0x003C Enabled
 RSA_WITH_AES_256_CBC_SHA256         0x003D Disabled
 DHE_DSS_WITH_AES_256_CBC_SHA        0x0038 Disabled
 DHE_RSA_WITH_AES_256_CBC_SHA        0x0039 Disabled
#
```

3.39.6 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、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	1.00.01～1.13.00

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).

#
```

注意事項

Ver. 1.13.01 以降のバージョンでは SSL キャッシュは無効となっているため、本コマンドは利用できません。関連情報は「config ssl cachetimeout timeout**」もご確認ください。**

3.39.7 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	1.00.01 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!

#
```

3.40 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	1.00.01 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

Ver.1.05 以降のファームウェアより、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、新しいポートで認証状態が引き継がれます。

Web 認証で処理可能な最大同時セッション数は 63 です。

動的 VLAN を使用する場合、割り当て可能な最大収容数は 64 端末です。
最大数 64 には、MAC/Web/802.1X の各認証で使用する動的 VLAN の端末数を含みます。
（動的 VLAN を使用しない端末は、この最大収容数には含まれません）

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。

端末の認証情報は VLAN とバインドして登録されます。そのため、認証端末が既に当該 VLAN に存在しないと装置が判定すると、端末の認証を解除します。

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	1.00.01 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	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	ports <<portlist> | all> - 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。 state <enable | disable> - Web 認証のポート状態を有効(enable)/無効(disable)に指定します。 aging_time <infinite | <min 1-1440>> - 認証されたホストが認証状態を保持している間隔を指定します。デフォルトは 1440 分です。 infinite - 認証されたホストがエージアウトされないように指定します。 block_time <sec 0-300> - 認証に失敗したホストをブロックさせる時間を指定します。デフォルトは 60 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	1.00.01 以降

使用例:ポート 1-9 の Web 認証を有効にするには

```
#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	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	1.00.01 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 <tcp_port_number 1-65535> - Web 認証画面での TCP ポート番号(1～65535)を指定します。以下のオプションでプロトコルを明示できます。 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。 HTTP の場合、TCP ポート 443 番では動作しません。同様に HTTPS の場合には TCP ポート 80 番では動作しません。
対応バージョン	1.00.01 以降

使用例:Web 認証画面において HTTP で 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 | disable> 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	1.11.00 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、未認証端末が短期間に多数のセッションを確立しようとする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 認証画面の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	1.11.00 以降

使用例:Web 認証画面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 | radius> 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	1.00.01 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	本コマンドは、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	1.00.01 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 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 Ingress 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 config web_authentication auth_failover

目的	Web 認証の failover 機能を設定します。
構文	config web_authentication auth_failover < enable [mode < permit [vlanid <vlanid 1-4094 >] > | local] | disable >
説明	本コマンドは、Web 認証において RADIUS サーバーから認証応答がない場合、ローカルデータベースによる認証､または強制的に認証許可を行う failover 機能を設定します。
パラメーター	enable - failover 機能を有効にします。 [mode < permit [vlanid<vlanid 1-4094 >] | local] permit - RADIUS サーバーから応答がない時、強制的に認証許可します。 vlanid <vlanid 1-4094> -認証許可された場合の所属 vlanid を設定します。 local - RADIUS サーバーから応答がない時、ローカルデータベースで認証します。 disable - failover 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	1.00.01 以降 1.09.00 以降(permit パラメーター)

使用例:Web 認証で failover 機能を有効にするには

```
#config web_authentication auth_failover enable mode permit vlanid 3
Command: config web_authentication auth_failover enable mode permit vlanid 3

Success.

#
```

注意事項

フェイルオーバー機能における強制的な認証許可(Permit)は、セキュリティ上問題となる可能性があるため、十分検討の上、使用してください。

フェイルオーバー機能設定時、RADIUS サーバーのタイムアウト時間は 30 秒以内に設定してください。デフォルト設定は 15 秒です。

3.40.11 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	本コマンドは、Web 認証のローカルユーザーを新規作成します。認証成功時に割り当てる VLAN を付与することができます。VLAN 情報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 <username 15>- Web ベースのアクセス制御用のアカウントを作成します。半角英数字 15 文字以内でユーザー名を作成します。 [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] vlan <vlan_name 32> - 認証成功時にユーザーに割り当てる VLAN 名を指定します。 <vlanid> <vlanid 1-4094> - 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	1.00.01 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.

#
```

3.40.12 config web_authentication user

目的	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	本コマンドは、登録されている Web 認証ローカルユーザーを編集します。
パラメーター	user <username 15> - Web ベースアクセス制御用のアカウントを指定します。半角英数字 15 文字以内でユーザー名を指定します。 [mode < permit [vlanid<vlanid 1-4094 >] | local] vlan <vlan_name 32> - 認証成功時にユーザーに割り当てる VLAN 名を指定します。 vlanid <vlanid 1-4094> - 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	1.00.01 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.

#
```

3.40.13 delete web_authentication user

目的	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	本コマンドは、登録されている 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	1.00.01 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.

#
```

3.40.14 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	本コマンドは、Web 認証後のリダイレクト URL を設定します。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	1.00.01 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.

#
```

3.40.15 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	本コマンドは、設定されたリダイレクト 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	1.00.01 以降

使用例:Web 認証のリダイレクト URL をクリアするには

```
#config web_authentication clear_redir_url
Command: config web_authentication clear_redir_url

Success.

#
```

3.40.16 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 画面をカスタマイズして任意の文字列を追加することができます。
パラメーター	<login | logout> login - 設定を適用する対象を login 画面にします。 logout - 設定を適用する対象を logout 画面にします。 <default |customize_text_box line <value 1-8>> default - 対象画面を初期状態に戻します。 customize_text_box line <value 1-8>- 対象画面にテキストボックスを追加します。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 <multiword 70> - 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。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でエンコード方式を 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	1.03.00 以降

使用例:Web 認証 login 画面をカスタイマイズする場合

```
#config web_authentication auth_page login customize_textbox_line 1 content "ご利用方法がわからない方は下記へご連絡ください。"
Command: config web_authentication auth_page login customize_textbox_line 1 content "ご利用方法がわからない方は下記へご連絡ください。"

#
```

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

#
```

3.40.17 clear web_authentication auth_state

目的	Web 認証状態をクリアします。
構文	clear web_authentication auth_state <*ports*> *Ports* = ports <<portlist> | all> [authenticated | authenticating | blocked] | macaddr <macaddr>
説明	本コマンドは、Web 認証の状態をクリアします。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	ports <<portlist> | all> - 設定するポート範囲を指定します。全てのポートを指定する場合は、"all"を設定します。 [authenticated | authenticating | blocked] 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 <macaddr> - この設定に使用される 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	1.00.01 以降

使用例:ポート 1-5 の Web 認証状態をクリアするには

```
#clear web_authentication auth_state ports 1-5
Command: clear web_authentication auth_state ports 1-5

Success.

#
```

3.40.18 show web_authentication

目的	Web 認証のグローバル設定を表示します。
構文	show web_authentication
説明	本コマンドは、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	1.00.01 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 Authentication
 ------------------------------
 State                   : Enabled
 Method                  : Local
 Authentication Failover : Disabled
 Redirect Path           : http://www.website.com
 Virtual IP              : 1.1.1.1
 Switch HTTP Port        : 80 (HTTP)
 RADIUS Authorization    : Enabled
 Local Authorization     : Enabled
 Redirect Action         : Enabled
 Session Timeout         : 120 seconds

#
```

3.40.19 show web_authentication ports

目的	Web 認証ポート設定を表示します。
構文	show web_authentication ports [<portlist>]
説明	本コマンドは、Web 認証の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	1.00.01 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

#
```

3.40.20 show web_authentication auth_state ports

目的	ポートの Web 認証状態を表示します。
構文	show web_authentication auth_state ports [<portlist>]
説明	本コマンドは、ポートの Web 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	1.00.01 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
------ ------------------- -------- ------------- ---- -----------
1      00-00-00-00-00-01(H) 20       Authenticated  4004 Infinite
1      00-00-00-00-00-03(H) 100      Blocked        -    60
2      00-00-00-00-00-02(H) 20       Authenticated  1234 Infinite
2      00-00-00-00-00-04(H) 110      Authenticating -    10

Total Authenticating Hosts :1
Total Authenticated Hosts  :2
Total Blocked Hosts        :1

#
```

3.40.21 show web authentication connection

目的	Web 認証端末の接続情報と認証時の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 認証端末の接続情報と当該端末の認証時の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	1.11.00 以降

使用例:Web 認証端末の接続情報と認証時の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

#
```

3.40.22 show web_authentication user

目的	Web 認証アカウントを表示します。
構文	show web_authentication user
説明	本コマンドは、Web 認証アカウント情報を表示します。 パスワードは管理者アカウントの場合のみ表示されます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.01 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

#
```

3.40.23 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	1.03.00 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 Maneger
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 Maneger
7.TEL      : 123-4567
8.MAIL     : network.manager.ab@apresiasystems.com
------------------------------------------------------------------
#
```

3.41 DHCP Snooping コマンド

3.41.1 enable dhcp_snooping

目的	DHCP Snooping 機能のグローバル設定を有効にします。
構文	enable dhcp_snooping
説明	本コマンドは、DHCP Snooping 機能のグローバル設定を有効にします。 ポート単位で設定する場合には config dhcp_snooping port コマンドで有効無効を指定してください。
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	1.11.00 以降

使用例: DHCP Snooing 機能のグローバル設定を有効にするには

```
#enable dhcp_snooping
Command: enable dhcp snooping

Succsss.

#
```

注意事項

DHCP Snooping 機能と ACL の併用には制限があります。ACL ルールの登録状況によっては、本コマンドで DHCP Snooping 機能を有効にできない場合があります。

DHCP Snooping の最大エントリ数は 126 です。

3.41.2 disable dhcp_snooping

目的	DHCP Snooping 機能のグローバル設定を無効にします。
構文	disable dhcp_snooping
説明	本コマンドは、DHCP Snooping 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	1.11.00 以降

使用例: DHCP Snooing 機能のグローバル設定を無効にするには

```
#disable dhcp_snooping
Command: disable dhcp snooping

Succsss.

#
```

3.41.3 config dhcp_snooping ports

目的	ポート単位で DHCP Snooping 機能を設定します。
構文	config dhcp_snooping ports <<portslist> | all> [vlan <vlan_name 32> | vlanid <vidlist>] state <enable | disable>
説明	本コマンドは、ポート単位で DHCP Snooping 機能を設定します。 VLAN を設定した場合、指定した VLAN のみを対象とします。VLAN が設定されていない場合は、全ての VLAN に適用されます。
パラメーター	ports <portlist> | all - 設定するポート範囲を入力します。装置の全てのポートを対象とする場合は「all」を指定します。 vlan <vlan_name 32> - 対象となる VLAN を VLAN 名で指定します。 vlanid <vidlist> - 対象となる VLAN 範囲を VLAN ID で指定します。 state <enable|disable> - ポート単位で DHCP Snooping を有効あるいは無効にします。
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	1.11.00 以降

使用例: 装置のポート 1,3,4 の VLAN2 に対して DHCP Snooing 機能を有効にするには

```
#config dhcp_snooping ports 1,3-4 vlanid 2 state enable
Command: config dhcp snooping ports 1,3-4 vlanid 2 state enable

Succsss.

#
```

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。

DHCP Snooping 機能が適用される VLAN が 1 個増加すると、ACL のタイプ ip に設定できる最大ルール数が 2 個減少します。

3.41.4 config dhcp_snooping mode deny

目的	DHCP Snooping のモードを設定します。
構文	config dhcp_snooping mode deny <enable | disable>
説明	本コマンドは、DHCP Snooping のモードを設定します。 DENY モードの場合、検査パケットに対して DHCP Snooping の結果に基づくフィルタリングを実施し、登録されていない IP アドレスが送信元である場合にはブロックします。 PERMIT モードの場合、当面は DHCP Snooping の観察のみを実施し、パケットの検査を行いません。config dhcp_snooping mode timer コマンドで定める猶予期間を経過すると、DENY モードに遷移し、パケットの検査を行います。
パラメーター	enable - DHCP Snooping のモードを DENY にします。 disable - DHCP Snooping のモードが PERMIT 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	1.11.00 以降

使用例: DHCP Snooping のモードを DENY にするには

```
#config dhcp_snooping mode deny enable
Command: config dhcp snooping mode deny enable

Succsss.

#
```

3.41.5 config dhcp_snooping mode timer

目的	DHCP Snooping の PERMIT モードで使用されるタイマーを設定します。
構文	config dhcp_snooping mode timer <<sec 0> | <sec 30-604800>>
説明	本コマンドは、DHCP Snooping の PERMIT モードでの切替のタイマーを設定します。
パラメーター	timer <<sec 0> | <sec 30-604800>> <sec 0> - 0 を入力する。0 の場合は PERMIT から DENY への切替を行いません。 <sec 30-604800> - PERMIT から DENY への切替時間を 30～604800 間で秒単位で設定します。
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	1.11.00 以降

使用例: DHCP Snooping の PERMIT モードからの切り替え時間を 60 秒に設定するには

```
#config dhcp_snooping mode timer 60
Command: config dhcp snooping mode timer 60

Succsss.

#
```

3.41.6 config dhcp_snooping inspection

目的	DHCP Snooping の検査対象トラフィックを指定します。
構文	config dhcp_snooping inspection <arp <enable | disable> | ipv4 <enable | disable> >
説明	本コマンドは、DHCP Snooping の検査対象トラフィックを指定します。 ARP、IPv4 それぞれに対して適用するかどうかを個別で指定できます。
パラメーター	arp - enable の場合、ARP パケットが検査対象になります。 ipv4 - enable の場合、IPv4 パケットが検査対象になります。
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	1.11.00 以降

使用例: DHCP Snooping の検査対象を指定するには

```
#config dhcp_snooping mode arp enable ipv4 enable
Command: config dhcp snooping mode arp enable ipv4 enable

Succsss.

#
```

3.41.7 create dhcp_snooping static_entry

目的	DHCP Snooping のスタティックエントリーを作成します。
構文	create dhcp_snooping static_entry mac_addr <macaddr> port <port> <vlan <vlan_name 32> | vlanid <vlanid 1-4094>> <ip <ipaddr> >
説明	本コマンドは、DHCP Snooping のスタティックエントリーを作成します。
パラメーター	mac_addr <macaddr> - 対象となる端末の MAC アドレスを指定します。 port <port> - 対象ポートを指定します。 vlan <vlan_name 32> - 対象 VLAN を VLAN 名で指定します。 vlanid <vlanid 1-4094> - 対象 VLAN を VLANID で指定します。 ip <ipaddr> - 対象となる端末の 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	1.11.00 以降

使用例: DHCP Snooping のスタティックエントリーを登録するには

```
#create dhcp_snooping static_entry port 1 mac_addr 00-11-22-33-44-55 vlanid 1 ip 1.2.3.4
Command: create dhcp_snooping static_entry port 1 mac_addr 00-11-22-33-44-55 vlanid 1 ip 1.2.3.4

Succsss.

#
```

3.41.8 delete dhcp_snooping static_entry

目的	DHCP Snooping のスタティックエントリーを削除します。
構文	delete dhcp_snooping static_entry mac_addr <macaddr> port <port> <vlan <vlan_name 32> | vlanid <vlanid 1-4094>> <ip <ipaddr> >
説明	指定した DHCP Snooping のスタティックエントリーを削除します。
パラメーター	mac_addr <macaddr> - 対象となる端末の MAC アドレスを指定します。 port <port> - 対象ポートを指定します。 vlan <vlan_name 32> - 対象 VLAN を VLAN 名で指定します。 vlanid <vlanid 1-4094> - 対象 VLAN を VLANID で指定します。 ip <ipaddr> - 対象となる端末の 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	1.11.00 以降

使用例: DHCP Snooping のスタティックエントリーを削除するには

```
#delete dhcp_snooping static_entry port 1 mac_addr 00-11-22-33-44-55 vlanid 1 ip 1.2.3.4
Command: delete dhcp_snooping static_entry port 1 mac_addr 00-11-22-33-44-55 vlanid 1 ip 1.2.3.4

Succsss.

#
```

3.41.9 config dhcp_snooping option_82 state

目的	DHCP Snooping で Option82 情報付加機能を設定します。
構文	config dhcp_snooping option_82 state <enable | disable>
説明	本コマンドは、DHCP Snooping の Option82 情報付加機能を設定します。Option82 情報付加機能を使用すると、端末の DHCP パケットに対して装置は DHCP サーバーに転送する前に接続ポート番号や VLANID などの付加情報を追加することができます。
パラメーター	state <enable | disable> - enable を設定した場合、DHCP Snooping で Option 82 の情報を追加します。disable の場合、追加しません。
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	1.11.00 以降

使用例: DHCP Snooping の Option82 情報付加機能を設定するには

```
# config dhcp_snooping option_82 state enable
Command: config dhcp_snooping option_82 state enable

Success.

#
```

3.41.10 clear dhcp_snooping entry

目的	DHCP Snooping でのダイナミックエントリーをクリアします。
構文	clear dhcp_snooping entry <ports <<portlist> | all> [vlan <vlan_name 32> | vlanid <vidlist>] | mac_addr <macaddr> port <port> <vlan <vlan_name 32> | vlanid <vidlist>> <ip <ipaddr> >
説明	本コマンドは、DHCP Snooping のモニタリングにより学習したダイナミックエントリーをクリアします。
パラメーター	ports <<portlist> | all> - 設定するポート範囲を入力します。装置の全てのポートを対象とする場合は、「all」を指定します。 vlan <vlan_name 32>- 対象 VLAN を VLAN 名で指定します。 vlanid <vlanid 1-4094> - 対象 VLAN を VLANID で指定します。 mac_addr <macaddr>- クリアする対象を MAC アドレスベースで指定します。 port <port> - 対象ポートを指定します。 ip <ipaddr> - 対象となる端末の 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	1.11.00 以降

使用例: DHCP Snooping のダイナミックエントリーをクリアするには

```
#clear dhcp_snooping entry ports 1-3 vlanid 1-2
Command: clear dhcp_snooping entry ports 1-3 vlanid 1-2

Succsss.

#
```

3.41.11 show dhcp_snooping

目的	DHCP Snooping 機能のグローバル設定を表示します。
構文	show dhcp_snooping
説明	本コマンドは、DHCP Snooping 機能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	1.11.00 以降

使用例: DHCP Snooing 機能のグローバル設定を表示するには(モードが PERMIT の場合)

```
#show dhcp_snooping
Command: show dhcp snooping

DHCP/DHCPv6 Snooping
-------------------------------
State           : Enabled
ARP Inspection  : Enabled
IPv4 Inspection : Enabled
Force Deny Mode : Disabled
Current Mode    : Permit
Timer           : 60 Seconds
Remaining Time  : 51 Seconds
Option_82       : Disabled

#
```

使用例: DHCP Snooing 機能のグローバル設定を表示するには(モードが DENY になった場合)

```
#show dhcp_snooping
Command: show dhcp snooping

DHCP/DHCPv6 Snooping
-------------------------------
State           : Enabled
ARP Inspection  : Enabled
IPv4 Inspection : Enabled
Force Deny Mode : Disabled
Current Mode    : Deny
Timer           : 60 Seconds
Remaining Time  : -
Option_82       : Disabled

#
```

3.41.12 show dhcp_snooping ports

目的	DHCP Snooping 機能のポート設定を確認します。
構文	show dhcp_snooping ports <<portlist> | all>
説明	本コマンドは、DHCP Snooping 機能のポート設定を確認します。
パラメーター	ports <<portlist> | all> - 確認するポート範囲を入力します。全てのポートを確認する場合は、「all」を指定します。
制限事項	なし。
対応バージョン	1.11.00 以降

使用例: DHCP Snooing 機能のポート設定を確認するには

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

Port State    Enabled VLANs
---- -------- ------------------------
1    Disabled -
2    Enabled  2
3    Enabled  1-3,100
4    Enabled  -

#
```

3.41.13 show dhcp_snooping static_entry

目的	DHCP Snooping のスタティックエントリーを表示します。
構文	show dhcp_snooping static_entry [ports <portlist>]
説明	設定した DHCP Snooping のスタティックエントリーを表示します。ポートを指定した場合、対象ポートに紐づけられたエントリーのみを表示します。ポート指定を省略した場合は全てのエントリーを表示します。
パラメーター	ports <portlist> - 指定したポートを対象とした静的エントリーを表示します。
制限事項	なし。
対応バージョン	1.11.00 以降

使用例: DHCP Snooing のスタティックエントリーを確認するには

```
# show dhcp_snooping static_entry ports 3
Command: show dhcp_snooping static_entry ports 3

Port MAC Address       VID  IP Address
---- ---------------- ---- ---------------------------------------
3    00-11-22-33-44-55 100  1.2.3.4

Total Entries :1

#
```

3.41.14 show dhcp_snooping entry

目的	DHCP Snooping のダイナミックエントリーを表示します。
構文	show dhcp_snooping entry [ports <portlist>]
説明	DHCP Snooping のモニタリングにより生成されたエントリーを確認します。ポートを指定した場合、対象ポートに対して生成されたエントリーのみを表示します。ポート指定を省略した場合は全てのダイナミックエントリーを表示します。
パラメーター	ports <portlist> - 指定したポートを対象とした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	1.11.00 以降

使用例: DHCP Snooing のダイナミックエントリーを表示するには

```
# show dhcp_snooping entry
Command: show dhcp_snooping entry

Port MAC Address       VID  IP Address
---- ----------------- ---- ---------------------------------------
3    00-11-22-33-44-55 100  1.2.3.4
3    00-66-77-88-99-00 1    12.34.56.78
4    00-11-33-55-77-99 3    5.6.7.8

Total Entries :3

#
```

3.42 POE コマンド

POE(Power over Ethernet)は、TPケーブルの特定の組み合わせのペアに直流電圧を重畳させ、通信をしながら受電機器に電力を供給するIEEE802.3at に準拠した機能です。

この機能は APLGM110GT-POE、APLGM118GT-POE および APLGM124GT-POE の機種で対応しています。

3.42.1 config poe ports

目的	各ポートの PoE 機能を設定します。
構文	config poe ports <all | <portlist>> state <enable | disable> | priority <critical | high | low> | power_limit <class_based | user_define <value 1000-31200>>
説明	各ポートの PoE ステータスはデフォルト設定で有効(enable)です。 ポートの給電制限値はデフォルト設定で 31200(mW)です。 この給電制限値は、ユーザー指定(user_define)で 1000～31200(mW)の範囲で設定できます。また、ユーザーが接続した PD Class で給電制限値とする(class_based)に変更することも可能です。 クラスベースは受電機器が接続されると PD クラスが自動検出され、そのクラスに応じた給電上限値がポートに割り当てられます。 クラスベースでは、以下の 5 段階からポート給電上限値を自動検出します。 各クラスの給電上限値は受電電力範囲より少し大きな値となっています。これは接続ケーブルにおける電力損失等を考慮しているためです。 ＜クラス＞ ＜給電上限値＞ ＜受電電力範囲＞ Class 0: 16.2(W) 0.44～12.95(W) Class 1: 4.2(W) 0.44～ 3.84(W) Class 2: 7.4(W) 3.84～ 6.49(W) Class 3: 16.2(W) 6.49～12.95(W) Class 4: 31.2(W) 12.95～25.50(W)
パラメーター	ports <<portlist> | all>- 対象ポートを指定します。「all」設定は全ポートが対象になります。 state <enable | disable> - 指定されたポートの PoE 給電を「enable」(有効)または「disable」(無効)に設定します。「disable」に設定した場合、当該ポートから給電はされません。 priority <critical | high | low> - 給電ポートの優先順位を指定します。 優先順位は高い順から critical、high、low となります。 power_limit <class_based | user_define <value 1000-31200>> - 各ポートの給電制限値を指定します。 class_based - 各ポートに接続された PD クラスを自動検出して、そのクラスに応じた給電制限値が設定されます。 user_define <value 1000-31200> - 各ポートの給電制限値を 1000～31200mW 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	1.04.00 以降

使用例: ポート 1-4,5 の PoE 機能を設定するには

```
#config poe ports 1-4 state enable priority critical power_limit class_based
Command: config poe ports 1-4 state enable priority critical power_limit class_b
ased

Success.

#config poe ports 5 state enable priority critical power_limit user_define 1000
Command: config poe ports 5 state enable priority critical power_limit user_define 1000

Success.

#
```

注意事項

給電制限値を超過した場合、プライオリティの高いポートから電力を供給します。プライオリティレベルが同じ時には、若番ポートから優先的に電力を供給します。（新たに接続した受電機器によって給電制限値を超過した場合でも、必ずしも新たに接続した受電機器の電力供給が停止されるわけではありません）

パラメーター(state,priority,power_limit)を変更した場合、対象ポートの給電が一時的に停止した後に給電を再開します。

user_define で入力する給電制限値は、200mW 単位で動作します。

config ports コマンドにより、データ通信のポート設定を無効(disable)にしても電力供給は行われます。

ファームウェアバージョンにより、ポート給電制限値のデフォルト値が異なります。
・バージョン(Ver.1.04)のデフォルト値は(ClassBased)です。
・バージョン(Ver.1.05)以降のデフォルト値は(UserDefine:31200mW)です。

3.42.2 show poe ports

目的	各ポートの PoE 設定と給電電力値を表示します。
構文	show poe ports <portlist>
説明	本コマンドは、各ポートの PoE 設定と給電電力値を表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。 省略されたときは全ポートが対象となります。 コマンド実行時に表示される各項目の説明は下記を参照ください。 State - ポートへの PoE ステータスを示します。 Priority - ポートへの給電優先度を示します。 Power Limit - ポートの給電制限値を示します。 Class - PD のクラス(0-4)を示します。 Power - 給電電力値を示します。(単位：mW) Voltage - 給電電圧を示します。(単位：dV) Current - 給電電流を示します。(単位：mA)
制限事項	なし。
対応バージョン	1.04.00 以降

使用例: ポート 1-5 の PoE 設定を表示するには

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

Port   State     Priority     Power Limit(mW)
       Class     Power(mW)    Voltage(decivolt)    Current(mA)
       Status
================================================================================
1      Enabled   Low          ---(Class-based)
       0         14800        549                  271
       ON   : 802.3af-compliant PD was detected
2      Enabled   Low          ---(Class-based)
       1         1900         552                  35
       ON   : 802.3af-compliant PD was detected
3      Enabled   Low          ---(Class-based)
       2         4900         550                  90
       ON   : 802.3af-compliant PD was detected
4      Enabled   Low          ---(Class-based)
       3         9900         552                  182
       ON   : 802.3af-compliant PD was detected
5      Enabled   Low          ---(Class-based)
       4         15100        550                  276
       ON   : 802.3at-compliant PD was detected

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

3.42.3 config poe system

目的	スイッチの PoE 機能を設定します。
構文	config poe system power_limit <value 20-375>
説明	本コマンドはスイッチの PoE を設定します。
パラメーター	power_limit <value 20-375> - スイッチ全体の給電制限値を(W)単位で入力します。 APLGM110GTPOE/APLGM118GTPOE/APLGM124GTPOE で最大値が異なります。 <value 20-125> - APLGM110GTPOE <value 20-250> - APLGM118GTPOE <value 20-375> - APLGM124GTPOE
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.04.00 以降

使用例: スイッチ全体の給電制限値を 100W に設定するには

```
#config poe system power_limit 100
Command: config poe system power_limit 100

Success.

#
```

注意事項

スイッチ全体の給電制限値を超過する場合、deny_low_priority_port プロセスによって、新しく供給を開始するポートよりもプライオリティが低いポートから優先的に給電を停止します。この状態は過負荷が解消されるまで継続されます。

3.42.4 show poe system

目的	スイッチの PoE 状態を表示します。
構文	show poe system
説明	本コマンドはスイッチの PoE 状態を表示します。
パラメーター	本コマンドのパラメーターはございませんが、コマンド実行時に表示される各項目の説明は下記を参照ください。 Power Limit - 装置の給電電力制限値を示します。 System Total Power Consumption - 装置の合計供給電力値を示します。 System Power Remained - 装置で給電可能な残りの給電電力値を示します。 Power Disconnection Method - 給電電力制限値を超過した場合の給電停止方法を示します。Deny Low Priority Port は、config poe ports で設定した priority に従って給電を停止する方法です。
制限事項	なし。
対応バージョン	1.04.00 以降

使用例: スイッチの PoE 設定を表示するには

```
#show poe system
Command: show poe system

PoE System Information
-------------------------------------------------
Power Limit                          : 375.0(Watts)
System Total Power Consumption       : 0.0(Watts)
System Power Remained                : 375.0(Watts)
Power Disconnection Method           : Deny Low Priority Port

PoE Recover Mode                     : Auto (Delay: 180 sec)
PoE Environment Status               : Normal
#
```

注意事項

APLGM124GTPOE 装置のみ、PoE 給電総量によって FAN 回転数が動的に制御されます。給電総量が 185W 以上になると FAN 回転が高速になり、155W 以下になると FAN 回転が通常回転に戻ります。

3.42.5 config poe recover_mode

目的	PoE 給電停止状態からの給電復旧モードを設定します。
構文	config poe recover_mode [auto <delay_time <value 180-600>> | manual]
説明	本コマンドは PoE 給電停止状態からの給電復旧モードを設定します。 スイッチは FAN 異常/温度異常の検知により PoE 給電を停止します。 APLGM110GTPOE/APLGM118GTPOE の場合、FAN 異常を検知しても PoE 給電を停止しません。温度異常(65°C超過)を検知すると PoE 給電が停止されます。 APLGM124GTPOE の場合、FAN 番号(2)(3)異常の検知により PoE 給電を停止します。 また、温度異常(65°C超過)を検知しても PoE 給電を停止します。
パラメーター	[auto <delay_time <value 180-600>> | manual] auto <delay_time <value 180-600>> - 異常復帰するとオートで PoE 給電が再開されます。給電再開までの時間を 180～600(秒)で指定できます。デフォルト設定は 180(秒)です。 manual - 異常復帰しても PoE 給電は再開されません。給電再開にはコマンド入力「poe manual_recover」が必要です。
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	1.04.00 以降

使用例: 給電復旧モードを manual に設定するには

```
#config poe recover_mode manual
Command: config poe recover_mode manual

Success.

#
```

3.42.6 poe manual_recover

目的	PoE 給電停止状態から給電を再開します。
構文	poe manual_recover
説明	本コマンドは、PoE 給電停止状態から給電を再開します。 給電復旧モード「config poe recover_mode」(manual)設定時に有効です。
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	1.04.00 以降

使用例: スイッチの PoE 設定を表示するには

```
#poe manual_recover
Command: poe manual_recover

Success.

#
```

3.42.7 config poe check_mode

目的	PoE 機能のポート状態監視を設定します。
構文	config poe check_mode < state <enable | disable> | checking_times <value 1-10 > | polling_times < value 30-120 > | poe_shutdown <enable | disable> | led_alarm <enable | disable> >
説明	本コマンドは PoE 機能のポート状態監視を設定します。
パラメーター	state <enable | disable> - enable に設定するとポーリング時間毎に PoE 機能のポート状態監視を行います。デフォルト設定は、有効(enable)です。 checking_times <value 1-10 >- PoE 機能のポート状態監視の回数を設定します。指定回数の監視に失敗した場合、PoE エラーのログを出力します。デフォルト設定は、3 回です。 polling_times < value 30-120 >- PoE 機能のポート状態監視のポーリング時間を設定します。デフォルト設定は、30 秒です。 poe_shutdown <enable | disable>- enable に設定すると PoE エラー検出時に対象の PoE ブロックの給電を停止します。デフォルト設定は、無効(disable)です。 led_alarm <enable | disable>- enable に設定すると PoE エラー検出時に対象の PoE ブロックの PoE LED を橙色に点灯させます。デフォルト設定は、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	1.10.00 以降

使用例: PoE 機能のポート状態監視を設定するには

```
#config poe check_mode state enable checking_times 2 polling_times 60 poe_shutdown enable
led_alarm enable
Command: config poe check_mode state enable checking_times 2 polling_times 60 poe_shutdown
enable led_alarm enable

Success.

#
```

注意事項

本コマンドは、PoE 機能のポート給電状態を監視します。給電異常が発生した場合、ログトラップによる通知及び PoE ポートのリセットを実施します。

3.42.8 show poe check_mode

目的	PoE 機能の状態監視設定を表示します。
構文	show poe check_mode
説明	本コマンドは PoE 機能の状態監視設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.10.00 以降

使用例: PoE 機能の状態監視設定を表示するには

```
#show poe check_mode
Command: show poe check_mode

 State           : Enabled
 checking_times  : 3
 polling times   : 30
 Poe shutdown    : Enabled
 led_alarm       : Enabled

#
```

3.43 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。

3.43.1 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	1.03.00 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.

#
```

3.43.2 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	1.03.00 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.

#
```

3.43.3 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	1.03.00 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

#
```

3.44 PERIPHERALS コマンド

3.44.1 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	各ポートの green mode はデフォルト設定で有効(enable)です。 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。
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 を有効「enable」または無効「disable」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	1.04.00 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.

#
```

注意事項

APLGM124GTSS 及び APLGM124GTPOE のコンボポートにおいて、UTP ポートと Fiber ポートを混在使用している場合、以下の制限があります。
(1)UTP ポート(22T)のリンク状態遷移によって、Fiber ポート(21F、23F、24F)でリンクダウンが発生する場合があります。
(2)UTP ポート(23T、24T)のリンク状態遷移によって、Fiber ポート(21F、22F)でリンクダウンが発生する場合があります。
この制限は、コンボポート(21T～24T)の Green Mode 設定を無効(Disable)にすることで回避することができます。

3.44.2 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	1.04.00 以降

使用例: ポート 1-3 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
```

3.44.3 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	test <off | green | amber | blink_green | blink_amber> 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	1.04.00 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。

3.44.4 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。 スイッチの内部温度は外部温度より約 5℃ほど高くなります。 実装の FAN 番号は、APLGM110GTPOE(FAN1)、 APLGM118GTPOE/APLGM124GTPOE(FAN1/FAN2/FAN3)です。
パラメーター	なし。
制限事項	本コマンドは、APLGM110GTPOE/APLGM118GTPOE/APLGM124GTPOE の機種で対応しています。
対応バージョン	1.04.00 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

#
```

スイッチは温度異常(65℃超過)の検知により PoE 給電を停止します。
また、APLGM124GTPOE のみ FAN 異常(FAN2/FAN3)の検知により PoE 給電を停止します。
FAN 異常(FAN1)を検知しても PoE 給電は停止されません。

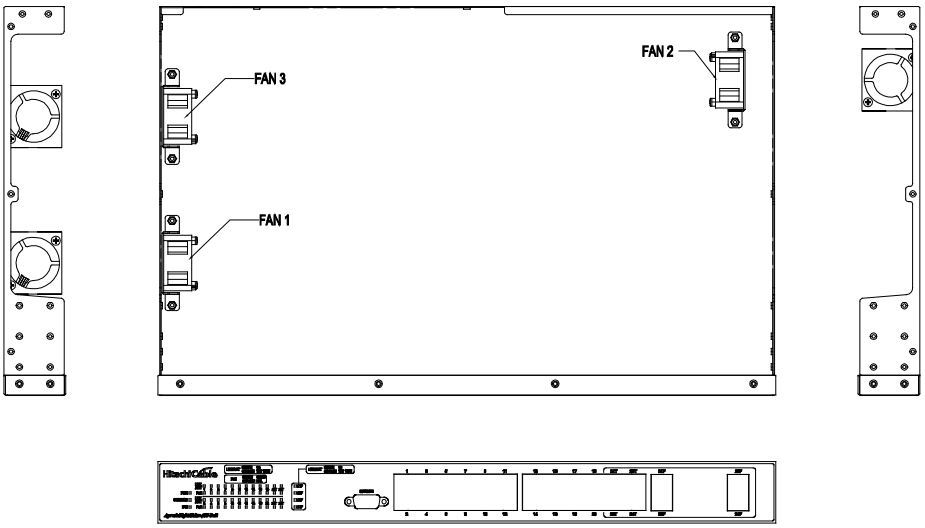


図 3-1 APLGM124GT-POE の FAN 位置図

3.45 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。

3.45.1 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、無効(disable)です。
パラメーター	< enable | disable > 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	1.06.00 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.

#
```

3.45.2 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	1.06.00 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。
ツイストペアケーブルを接続しても「LINK/ACT」 LED が点灯しない。	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、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、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。

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 接続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、ツイストペア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ペア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になっている可能性があります。SFP を再度装着し直してください。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 PoE に関連する現象と対策

現象	対策
端末へ給電されない。	給電の Status が Enable になっているかを確認してください。
	ツイストペアケーブルに異常がない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。
	端末の給電クラスと合致しているかを確認してください。
	スイッチの給電制限を超えていないかを確認してください。

5.8 内蔵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。	ファンそのものの異常が考えられます。カバーをあけることなく、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 RFC2863：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/RSTP IEEE802.1Q：MSTP IEEE802.3x：フロー制御 IEEE802.1AB：LLDP IEEE802.3at：PoE Plus

ApresiaLightGM シリーズ Ver.1.13 CLI マニュアル

Copyright(c) 2020 APRESIA Systems, Ltd.

2020 年 1 月 初版
2020 年 3 月 第 2 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/