TD61-8855

ApresiaNP2500 シリーズ

AEOS-NP2500 Ver. 1.13

コマンドリファレンス

APRESIA Systems 株式会社

制定・改訂来歴表

No.	年 月 日	内　　容
-	2025 年 3 月 14 日	• TD61-8455 AEOS-NP2500 Ver. 1.12 コマンドリファレンスより作成 • 全章を対象に誤字・脱字・体裁を修正 • 全章を対象に使用フォントを変更し、それに伴い構成や体裁を修正 • 全章を対象にパラメーター文字列を見直し • 全章を対象に物理ポートのみ指定可能なコマンドのコマンド書式を見直し • 全章のコマンド一覧表の記載方法を変更 • 全章を対象に「制限事項」項目と「注意事項」項目を「制限・注意」項目にまとめるよう変更、その他の項目名称も変更 • 全章を対象に show／操作コマンドで「デフォルト」項目が不要な場合は「デフォルト」項目を削除 •「エラー復旧コマンド」の記載を「10 サポート」から「4 管理」に変更 •「1 はじめに」を修正 •「1.1 本文中の表記について」を修正 •「1.2 コマンドシンタックス」を修正 •「1.5 ユーザーアカウント」を修正 •「1.7 コマンドモード」を修正 •「1.11 コマンド入力の補助機能」を修正 •「2.1 インターフェースコマンド」の以下を修正 - show interfaces transceiver の制限・注意を追加 •「2.2 ポート設定コマンド」の以下を修正 - linkup-delay enable を追加 - linkup-delay timer を追加 - show interfaces linkup-delay を追加 •「3.1 基本 CLI コマンド」の以下を修正 - enable のガイドライン、使用例を修正 - disable のガイドライン、使用例を修正 - show history のガイドライン、制限・注意を修正 •「3.5 基本 IPv4 コマンド」の以下を修正 - ip address のガイドライン、制限・注意を追加 - show ip interface の使用例を修正 •「3.7 IP ユーティリティーコマンド」の以下を修正 - traceroute の Parameter、デフォルトを修正 •「3.8 Gratuitous ARP コマンド」の以下を修正 - ip gratuitous-arps のガイドライン、制限・注意を追加 •「3.9 システムファイル管理コマンド」の以下を修正 - ip ssh source-interface を修正を追加 - show boot のガイドラインを修正 - configure replace を修正 - copy を修正 - backup を修正 - restore を修正 •「4.7 NTP コマンド」の以下を修正 - service ntp の制限・注意を修正

No.	年 月 日	内　　容
		• 「4.8 TELNET コマンド」の以下を修正 - telnet (クライアント)のガイドラインを追加 • 「4.9 SSH コマンド」の以下を修正 - ip ssh server を修正 - ip ssh timeout を修正 - ip ssh key-exchange enable のガイドライン、制限・注意を追加 - ip ssh cipher enable のガイドラインを追加 - ip ssh mac enable のガイドラインを追加 - show ssh algorithm の使用例を修正 - show ssh の制限・注意を追加 - ssh (クライアント)を追加 • 「4.12 SNMP コマンド」の以下を修正 - snmp trap link-status を修正 - snmp-server user の使用例を修正 - show snmp community の使用例を修正 - show snmp host の使用例を修正 - show snmp-server traps を修正 - show snmp user の使用例を修正 - show snmp group の使用例を修正 • 「4.13 ミラーリングコマンド」の以下を修正 - monitor session destination remote vlan の制限・注意を追加 - monitor session source interface の制限・注意を追加 • 「4.14 LLDP コマンド」の以下を修正 - lldp err-disable のガイドライン、制限・注意を修正 • 「5.6 ループ検知コマンド」の以下を修正 - loop-detection mode のガイドラインを修正 - errdisable recovery cause loop-detection のガイドラインを修正 - snmp-server enable traps loop-detection を追加 • 「5.7 ストームコントロールコマンド」の以下を修正 - storm-control を修正 - storm-control action の Parameter、制限・注意を修正 - snmp-server enable traps storm-control を追加 - show storm-control の制限・注意を追加 • 「5.13 MMRP-Plus コマンド」の以下を修正 - mmrp-plus enable の制限・注意、バージョンを修正 - mmrp-plus ring transmit-fdb-flush port を修正 - mmrp-plus ring transmit-fdb-flush retransmit enable を修正 - mmrp-plus ring fdb-flush port を修正 - mmrp-plus ring hello-timeout の制限・注意を修正 - mmrp-plus ring uplink port の制限・注意を追加 • 「5.14 スパニングツリープロトコルコマンド」の以下を修正 - spanning-tree global state の制限・注意、バージョンを修正 - spanning-tree mode の制限・注意を削除 - spanning-tree state の制限・注意、バージョンを修正

No.	年 月 日	内　　容
		• 「5.15 RPVST+コマンド」の以下を修正 - spanning-tree vlan の制限・注意、バージョンを修正 • 「5.17 VLAN コマンド」の以下を修正 - switchport access vlan の制限・注意を追加 - switchport trunk allowed vlan の制限・注意を追加 - switchport trunk native vlan の制限・注意を追加 - switchport hybrid allowed vlan のガイドラインを修正、制限・注意を追加 - switchport hybrid native vlan の制限・注意を追加 - protocol-vlan profile (Interface)の制限・注意を修正 - acceptable-frame の制限・注意を追加 - ingress-checking のガイドラインを修正、制限・注意を追加 • 「5.19 VLAN トンネルコマンド」の以下を修正 - dot1q tunneling ethertype の制限・注意を追加 - switchport vlan mapping の制限・注意を修正 - vlan mapping profile のガイドラインを追加 - switchport vlan mapping profile の制限・注意を追加 - vlan mapping miss drop の制限・注意を追加 - dot1q-tunnel trust inner-priority の制限・注意を追加 - dot1q-tunnel insert dot1q-tag の制限・注意を追加 • 「6.1 プロトコル非依存コマンド」の以下を修正 - ip route の制限・注意を追加 • 「7.1 QoS コマンド」の以下を修正 - rate-limit input の制限・注意を追加 - rate-limit output の制限・注意を追加 • 「7.2 ポリシーマップコマンド」の以下を修正 - class-map の制限・注意を追加 - set の制限・注意を追加 - police の制限・注意を追加 - police cir の制限・注意を追加 - police aggregate の制限・注意を追加 - mls qos aggregate-policer の制限・注意を追加 - service-policy のガイドラインを修正、制限・注意を追加 • 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 - expert access-group のガイドラインを修正、制限・注意を追加 - ip access-group のガイドラインを修正、制限・注意を追加 - arp access-group のガイドラインを修正、制限・注意を追加 - ipv6 access-group のガイドラインを修正、制限・注意を追加 - mac access-group のガイドラインを修正、制限・注意を追加 - action の制限・注意を追加 - vlan filter の制限・注意を修正 - show access-list resource reserved-group の制限・注意を追加 • 「9.1 AccessDefender 共通コマンド」の以下を修正 - authentication interface の制限・注意を修正 - vlan mode のガイドラインを修正

No.	年 月 日	内　　容
		- copy（AccessDefender）を修正 - 「RADIUS 属性に関する情報」を追加 • 「9.2 認証、許可、アカウンティング（AAA）コマンド」の以下を修正 - aaa new-model のガイドライン、制限・注意を修正 - aaa authentication mac-auth のガイドラインを修正 - aaa authentication dot1x のガイドラインを修正 - aaa authentication web-auth のガイドラインを修正 • 「9.4 IEEE 802.1X 認証コマンド」の以下を修正 - show access-defender dot1x の使用例を修正 - show access-defender dot1x interface の使用例を修正 • 「9.7 Web アクセス拒否通知コマンド」の以下を修正 - copy（web-deny-notify）を修正 • 「10.1 デバッグコマンド」の以下を修正 - debug copy を修正 - debug show access-defender internal-resource の使用例を修正 - show tech-support の制限・注意を追加 - debug show tech-support を追加 • 巻末の住所を修正

目次

1 はじめに 1
1.1 本文中の表記について 3
1.2 コマンドシンタックス 4
1.3 コンソールポートへの接続 6
1.4 初めての CLI への接続 8
1.5 ユーザーアカウント 9
1.6 ユーザーアカウントの作成 10
1.7 コマンドモード 11
1.8 インターフェースの表記法 12
1.9 VLAN インターフェース 13
1.10 エラーメッセージ 14
1.11 コマンド入力の補助機能 15
1.12 表示結果出力修飾子 16
1.13 本書でのコマンド説明の記載項目 17
2 インターフェースとハードウェア 18
2.1 インターフェースコマンド 18
2.2 ポート設定コマンド 43
2.3 ブザーおよびアラーム LED コマンド 53
2.4 省電力イーサネット(EEE)コマンド 60
2.5 PoE コマンド 62
2.6 PD モニタリングコマンド 73
2.7 スタックコマンド 81
3 基礎知識 98
3.1 基本 CLI コマンド 98
3.2 ファイルシステムコマンド 113
3.3 ターミナルコマンド 121
3.4 アクセス管理コマンド 125
3.5 基本 IPv4 コマンド 136
3.6 基本 IPv6 コマンド 144
3.7 IP ユーティリティーコマンド 155
3.8 Gratuitous ARP コマンド 160
3.9 システムファイル管理コマンド 162
4 管理 190
4.1 DHCP クライアントコマンド 190
4.2 DHCP サーバーコマンド 193
4.3 DHCPv6 クライアントコマンド 219
4.4 DHCPv6 サーバーコマンド 223
4.5 DHCP Auto Configuration コマンド 239
4.6 時刻および SNTP コマンド 241
4.7 NTP コマンド 247

4.8 TELNET コマンド 260
4.9 SSH コマンド 264
4.10 RMON コマンド 279
4.11 sFlow コマンド 288
4.12 SNMP コマンド 296
4.13 ミラーリングコマンド 321
4.14 LLDP コマンド 330
4.15 Ethernet OAM コマンド 360
4.16 単方向リンク検出(ULD)コマンド 374
4.17 CFM コマンド 378
4.18 エラー復旧コマンド 409
4.19 Zero Touch Provisioning(ZTP)コマンド 412
4.20 タイムレンジコマンド 416
5 レイヤー2 419
5.1 FDB コマンド 419
5.2 ジャンボフレームコマンド 426
5.3 ポートチャネルコマンド 427
5.4 ポートリダンダントコマンド 436
5.5 リンクダウン連携コマンド 443
5.6 ループ検知コマンド 446
5.7 ストームコントロールコマンド 459
5.8 Egress フィルタリングコマンド 468
5.9 マルチキャストフィルタリングモードコマンド 470
5.10 IGMP スヌーピングコマンド 472
5.11 MLD スヌーピングコマンド 493
5.12 リングプロテクション(ERPS)コマンド 513
5.13 MMRP-Plus コマンド 526
5.14 スパニングツリープロトコルコマンド 559
5.15 RPVST+コマンド 585
5.16 トラフィックセグメンテーションコマンド 593
5.17 VLAN コマンド 595
5.18 プライベート VLAN コマンド 610
5.19 VLAN トンネルコマンド 617
5.20 Voice VLAN コマンド 631
5.21 ポートセキュリティーコマンド 640

6 レイヤー3 651
6.1 プロトコル非依存コマンド 651
6.2 IPv4 マルチキャストコマンド 656
6.3 IPv6 マルチキャストコマンド 657
7 QoS 658
7.1 QoS コマンド 658
7.2 ポリシーマップコマンド 678
8 アクセスリスト(ACL) 698
8.1 アクセスリスト(ACL)コマンド 698
9 セキュリティー 744
9.1 AccessDefender 共通コマンド 744
9.2 認証、許可、アカウンティング(AAA)コマンド 777
9.3 MAC 認証コマンド 805
9.4 IEEE 802.1X 認証コマンド 809
9.5 SSL コマンド 820
9.6 Web 認証コマンド 824
9.7 Web アクセス拒否通知コマンド 836
9.8 DHCP スヌーピングコマンド 843
9.9 ARP スヌーピングコマンド 850
10 サポート 857
10.1 デバッグコマンド 857
10.2 メモリーエラー自動復旧コマンド 880
10.3 システムログコマンド 883
10.4 システムメモリー使用率監視コマンド 894
10.5 CPU 使用率監視コマンド 896
10.6 CPU 保護コマンド 901
11 付録 902
11.1 システム復旧手順(パスワードのリセット) 902

1 はじめに

■ 本書の目的

ApresiaNP2500 シリーズを設定、管理、および監視するためのコマンドラインインターフェース(CLI)を説明します。

■ 適応機種と対応バージョン

製品名称	対応バージョン
ApresiaNP2500-8MT4X-PoE	AEOS-NP2500 Ver. 1.08.02～
ApresiaNP2500-16MT4X-PoE	AEOS-NP2500 Ver. 1.08.02～

■ 対象読者

ネットワーク管理に必要な、基本的な概念や用語は十分に理解されているものとします。主にネットワーク管理者をはじめとしたネットワークの管理業務を行うユーザーを対象にしています。

■ 運用上のご注意

- 本書に未記載のコマンドは ApresiaNP2500 シリーズでは未サポートです。また、各コマンドの初回サポートバージョンは、各コマンドのバージョン項目を参照してください。
- SD LED 点滅中は SD カードの抜き差しを行わないでください。
- SD カードを再初期化する際は、FAT16 でフォーマットしてください。
- フォーマットには SD カードメーカー各社より提供されている SD カードフォーマットソフトウェアをご使用ください。
- 本装置では 4 メガバイト以上の構成情報は使用できません。構成情報が 4 メガバイト未満に収まるようにしてご使用ください。
- 大量の設定をコピー＆ペーストで入力すると、CPU 負荷の高騰や、冗長機能などに一時的に影響する可能性が考えられます。そのため、運用中は複数行の設定を一度にコピー＆ペーストで入力することは推奨しません。設定を 1 行入力したら、コマンドプロンプトの応答を待ってから次の設定を入力するようにしてください。
- ApresiaNP2500 シリーズでは、VLAN 間のレイヤー3 中継はできません。
- 本書の使用例などに用いている IP アドレス、MAC アドレスは他組織所有である場合があるため、ご使用時に留意してください。

■ 輸出する際のご注意

本製品や本資料を輸出、または再輸出する際には、日本国ならびに輸出先に適用される法令、規制に従い必要な手続きをお取りください。

ご不明な点がございましたら、販売店、または当社の営業担当にお問い合わせください。

■ 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ルーティングソフトウェアを含むすべてのソフトウェア（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。

- 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。
- 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。
- 本ソフトウェアでは、本資料に記載しているコマンドのみをサポートしています。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。

■ 商標登録

1.1 本文中の表記について

本文中の表記について以下に示します。

表記	説明
大文字	コマンドライン内の変数パラメーターを示します。コマンド実行時に、実際の値に置き換えてください。 物理ポート指定のコマンドでは、パラメーター文字列 PORT（複数指定不可）、または PORTS（複数指定可能）で表記する場合があります。物理ポートを複数指定する場合は、「1/0/1,1/0/3,1/0/5」のようにコンマで区切るか、「1/0/1-5」もしくは「1/0/1-1/0/5」のようにハイフンで範囲を指定します。
縦線 |	中括弧（{}）または角括弧（[]）内に含まれる個々のパラメーターを示します。中括弧または角括弧内で複数のパラメーターが縦線で区切られている場合、コマンド実行時に引数として使用できるパラメーターは 1 つだけです。
中括弧 { }	コマンドの必須パラメーターを示します。複数のパラメーターは中括弧で囲まれて、各パラメーターは縦線で区切られます。引数内に必須パラメーターを 1 つ以上指定した場合だけ、コマンドを実行できます。
角括弧 [ ]	コマンドで省略可能なパラメーターを示します。複数のパラメーターは角括弧で囲まれて、各パラメーターは縦線で区切られます。角括弧内のパラメーターを使用しない場合でも、コマンドを実行できます。
[,|-]	対象パラメーターを複数指定できることを示します。 対象パラメーターが物理ポートの場合は、「1/0/1,1/0/3,1/0/5」のようにコンマで区切るか、「1/0/1-5」もしくは「1/0/1-1/0/5」のようにハイフンで範囲を指定します。 対象パラメーターが VLAN、MMRP-Plus のリング ID などの場合は、「1,3,5」のようにコンマで区切るか、「1-5」のようにハイフンで範囲を指定します。 コンマとハイフンの前後には、スペースを入力しないでください。
使用例の太字斜体	説明のための番号です。装置からは出力されません。

1.2 コマンドシンタックス

コマンドシンタックスの説明で使用する記号を以下に示します。

［角括弧］	
目的	コマンド内の省略可能なパラメーターを示します。
シンタックス	command［parameter1］
説明	parameter1 パラメーターが省略可能なことを示しています。

{中括弧}	
目的	コマンドの必須パラメーターを示します。コマンドを正常に実行するためには、1 つ以上の必須パラメーターを指定する必要があります。
シンタックス	command {parameter1 | parameter2}
説明	コマンドを実行するために必要なパラメーターが parameter1、または parameter2 であることを示しています。

| 縦線	
目的	コマンドで指定可能な複数のパラメーターを区切ります。
シンタックス	command［parameter1 | parameter2 | parameter3］
説明	以下の 3 つのコマンドを個別に実行できます。 • command parameter1 • command parameter2 • command parameter3

コマンド入力で使用できる操作キーとショートカットキーを以下に示します。Ctrl キーと組み合わせて入力する文字キーは大文字小文字のいずれでも可能です。

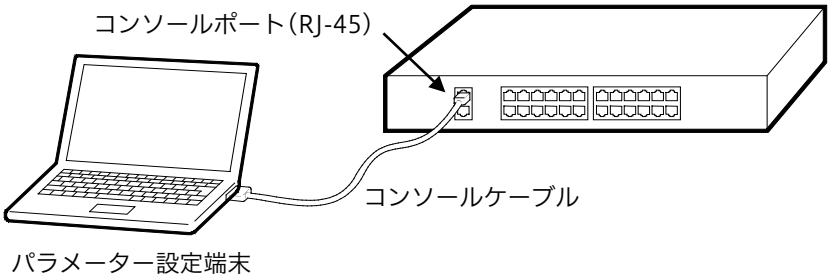
編集機能	
Enter キー	コマンドを実行します。
Delete キー	カーソル位置の文字を削除します。
Backspace キー	カーソル位置の 1 つ左の文字を削除します。
Ctrl+A	カーソルを行頭へ移動します。
Ctrl+E	カーソルを行末へ移動します。
Ctrl+K	カーソル位置の文字から行末までを削除します。
Ctrl+Z	グローバル設定モードまたはサブ設定モードの場合に、入力中の文字列を破棄して特権実行モードに戻ります。
左矢印キー	カーソルを左へ移動します。
右矢印キー	カーソルを右へ移動します。
上矢印キーまたは Ctrl+P	コマンド履歴リスト（show history で確認可能）に記録された文字列を、新しいエントリーから順番に表示します。
下矢印キーまたは Ctrl+N	コマンド履歴リスト（show history で確認可能）に記録された文字列を、古いエントリーから順番に表示します。
Ctrl+R	文字の挿入モードと上書きモードを切り替えます。挿入モードの場合は、

編集機能	
	カーソル位置に入力した文字を挿入します。上書きモードの場合は、カーソル位置の文字を入力した文字に置き換えます。
Ctrl+V	Ctrl+V の入力直後に?を入力することで、?を文字列としてコマンドラインに入力します。
ページングによる表示停止時の操作	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、以下の行が表示されて表示を一時停止します。 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All この状態では以下の操作によるスクロールが可能です。 • Ctrl+C、Esc キー、Q キー：show コマンドの実行を終了します。 • スペースキー、N キー：次のページを表示します。 • Enter キー：次の行を表示します。 • A キー：すべての情報を表示します。 スペースキーまたは N キーを押し続けると、Telnet が切断されることがあります。一時停止した表示をすべて表示させる場合は、A キーを使用してください。

1.3 コンソールポートへの接続

装置の監視や設定を行うには、コンソールポート（RJ-45 ポート）にパラメーター設定端末を接続します。パラメーター設定端末は、RS-232C シリアルポートを備えており、端末エミュレータを利用できる必要があります。

装置とパラメーター設定端末を接続するには、コンソールケーブル（一方が RJ-45 コネクターで、もう一方がメス型 DB-9 コネクター）を、装置のコンソールポートと、パラメーター設定端末の RS-232C シリアルポートに挿入します。



端末エミュレータの接続プロパティは以下のように設定してください。なお、エミュレーションモードを選択できる場合は、「VT100」に設定してください。

- ボー・レート：9600 bit/s（装置側設定により可変）
- データ長：8bit
- ストップビット：1bit
- パリティー：なし
- フロー制御：なし

パラメーター設定端末を正しく設定したら、装置の電源を入れます。起動シーケンスが端末エミュレータのウィンドウに表示されます。

```
Boot Procedure V1.00.00
  MAC Address: FC-6D-D1-F2-82-1F
  H/W Version: A

Power On Self Test: 100 %

Please Wait, Loading V1.08.02

Firmware: 100 %
UART init: 100 %

Starting firmware...

Device Discovery: 100 %
Configuration init: 100 %
〜〜省略〜〜

Switch con0 is now available
〜〜省略〜〜

Press any key to login...
```

ApresiaNP2500 シリーズでは ZTP 機能をサポートしており、以下の条件を満たす場合に ZTP 機能が動作します。

- ZTP スイッチが ON 状態（no ztp enable 設定以外）
- ZTP スイッチが OFF 状態でも、ztp enable force 設定の場合

ZTP 機能が動作する場合は、ZTP 機能の動作が完了するか、もしくは ZTP 機能が中断されると、ユーザー実行モードで CLI にアクセスが許可されます。

ZTP 機能が DHCP タイムアウト（30 秒）して中断された場合の例を示します。

```
Start ZTP, lock CLI for process!
Exit ZTP process by CTRL+C.

ZTP : DHCP connection timeout.
ZTP restore old config.
ZTP Fail: still use old image&config.

ZTP Fail: Unlock CLI.
```

また、Ctrl+C キーを入力して ZTP 機能を中断した場合の例を示します。

```
Start ZTP, lock CLI for process!
Exit ZTP process by CTRL+C.

ZTP : interrupted ZTP processing from console.

ZTP restore old config.
ZTP Fail: still use old image&config.

ZTP Fail: Unlock CLI.
```

1.4 初めての CLI への接続

設定が工場出荷状態の場合は、ユーザーアカウントは作成されていません。装置の電源を入れ、起動シーケンスが完了すると、ユーザー実行モードで CLI にアクセスが許可されます。なお、CLI のプロンプトはコマンドモードを示しており、ユーザー実行モードの場合はプロンプトが > で表示されます。

```
Ethernet Switch ApresiaNP2500-8MT4X-PoE

Firmware: Build 1.08.02

>
```

ユーザー実行モードで enable コマンドを実行すると、特権実行モードに遷移します。特権実行モードの場合はプロンプトが # で表示されます。enable password コマンド未設定時には、コンソールポート接続で装置にログインしている場合のみ、パスワードなしで特権実行モードに遷移できます。

```
> enable
#
```

特権実行モードで configure terminal コマンドを実行すると、グローバル設定モードに遷移します。グローバル設定モードの場合はプロンプトが (config)# で表示されます。

```
# configure terminal
(config)#
```

コマンドモードの詳細については、「1.7 コマンドモード」を参照してください。

IP アドレスや Telnet/SSH 関連の設定が設定されていて、装置がネットワークに接続されている場合は、Telnet/SSH でログインすることもできます。

- SSH の最大セッション数は、マネージメントポート専用が 1、それ以外が 8 です。
- ApresiaNP2500 シリーズでは、Telnet の最大セッション数は、マネージメントポート専用が 1、それ以外が 8 です。

1.5 ユーザーアカウント

セキュリティー上、装置の CLI にアクセスできるユーザーを管理・制御することは重要です。装置の CLI にアクセスできるユーザーアカウントは適切に作成してください。

ユーザーアカウントには特権レベルを割り当てることができます。各コマンドには使用できる特権レベルが設定されているため、ユーザーアカウントごとにアクセス可能なコマンドをある程度制御することができます。

特権レベルの概要を以下に示します。各コマンドの特権レベルに関しては、各コマンドの特権レベル項目を参照してください。

特権レベル	アクセス可能なコマンドモード	使用できるコマンドの概要
レベル 1	• ユーザー実行モード	• ほとんどの show コマンド（※1） • ping や telnet などの一部の操作コマンド（※2）
レベル 12	• 特権実行モード（レベル 12） • グローバル設定モード • 任意の設定モード（一部除く）	• ほとんどの show コマンド（※1） • ping や telnet、clear コマンドなどの一部の操作コマンド（※2） • セキュリティー関連の設定コマンドを除く設定コマンド
レベル 15	• 特権実行モード（レベル 15） • グローバル設定モード • 任意の設定モード	• すべてのコマンド

- ※1: 構成情報の表示コマンド(show running-config, show startup-config)や技術サポート情報の表示コマンド(show tech-support)などは、特権レベル 15 でのみ使用できます。
- ※2: 構成情報の保存コマンド(write)や装置の再起動コマンド(reboot)、その他の多くの操作コマンドは特権レベル 15 でのみ使用できます。

ユーザーが装置にログインすると、ユーザーアカウントの特権レベルによって、ログイン後のコマンドモードが決定されます。

- 特権レベル 1 のユーザーアカウントの場合は、ユーザー実行モードでログインします。
- 特権レベル 12 のユーザーアカウントの場合は、特権実行モード(レベル 12)でログインします。
- 特権レベル 15 のユーザーアカウントの場合は、特権実行モード(レベル 15)でログインします。

1.6 ユーザーアカウントの作成

ユーザーアカウントを作成する方法、および新しく作成したユーザーアカウントで CLI にログインできることを確認する方法を説明します。

ユーザーアカウントを作成するには username コマンドを使用して作成します。以下に、「ユーザー名が admin、特権レベルが 15、パスワードが pass1234」のユーザーアカウントを作成する例を示します。

```
> enable
# configure terminal
(config)# username admin privilege 15 password pass1234
(config)#
```

この例の実行内容は以下です。

- enable コマンドを実行してユーザー実行モードから特権実行モードに遷移。enable password コマンド未設定時には、コンソールポート接続で装置にログインしている場合のみ、パスワードなしで特権実行モードに遷移可能。
- configure terminal コマンドを実行して特権実行モードからグローバル設定モードに遷移。
- username コマンドを実行して、「ユーザー名が admin、特権レベルが 15、パスワードが pass1234」のユーザーアカウントを作成。

次に、新しく作成したユーザーアカウントで CLI にログインできることを確認する例を示します。

```
(config)# line console
(config-line)# login local
(config-line)# end
# logout

Switch con0 is now available




Press any key to login...


Ethernet Switch ApresiaNP2500-8MT4X-PoE

Firmware: Build 1.08.02

User Verification Access
Username:admin
Password:********

#
```

この例の実行内容は以下です。

- line console コマンドを実行してコンソールポートのライン設定モードに遷移。
- login local コマンドを実行して、コンソールポート接続で装置にログインする際に、ローカルユーザーアカウントを使用するように設定。
- end コマンドを実行して特権実行モードに遷移。
- logout コマンドを実行してログアウト。
- 新しく作成したユーザーアカウント「ユーザー名が admin、パスワードが pass1234」でログイン。特権レベルが 15 のユーザーアカウントのため、ログイン後は特権実行モード。

1.7 コマンドモード

装置の CLI では、いくつかのコマンドモードを使用できます。コマンドモードを切り替えるには、下表のような適切なコマンドを使用する必要があります。たとえば、ユーザー実行モードから特権実行モードに遷移するには enable コマンドを使用します。逆に、特権実行モードからユーザー実行モードに遷移するには disable コマンドを使用します。

特権実行モードでは configure terminal コマンドでグローバル設定モードに遷移できます。グローバル設定モードでは、対応する設定コマンドでサブ設定モードに遷移できます。サブ設定モードの例を以下に示します。

- インターフェース設定モード
- ライン設定モード
- DHCP プール設定モード

コマンドモードの概要を以下に示します。各コマンドのコマンドモードに関しては、各コマンドのモード項目を参照してください。

コマンドモード	プロンプト末尾の表示	概要
ユーザー実行モード	>	• enable コマンドで特権実行モードに遷移
特権実行モード	#	• disable コマンドでユーザー実行モードに遷移 • configure terminal コマンドでグローバル設定モードに遷移
グローバル設定モード	(config)#	• exit コマンドまたは end コマンドで特権実行モードに戻る • 対応する設定コマンドでサブ設定モードに遷移
サブ設定モード	各サブ設定モードにより異なる	• exit コマンドでグローバル設定モード、または 1 つ前の設定モードに戻る • end コマンドで特権実行モードに戻る

インターフェース設定モードの概要を以下に示します。

コマンドモード	プロンプト末尾の表示	概要
インターフェース設定モード(port)	(config-if-port)#	• 物理ポート関連の設定を、指定したポートで実施する設定モード
インターフェース設定モード(range)	(config-if-port-range)#	• 物理ポート関連の設定を、指定した範囲の複数ポートで実施する設定モード
インターフェース設定モード(port-channel)	(config-if-port-channel)#	• ポートチャネル関連の設定を、指定したポートチャネルで実施する設定モード
インターフェース設定モード(vlan)	(config-if-vlan)#	• 主にレイヤー3 関連の設定を、指定した VLAN インターフェースで実施する設定モード
インターフェース設定モード(mgmt)	(config-if-mgmt)#	• マネージメントポート関連の設定を実施する設定モード
インターフェース設定モード(l2vlan)	(config-if-l2vlan)#	• この設定モードは、description コマンドでインターフェースの説明を設定する場合にのみ使用

1.8 インターフェースの表記法

本装置で物理ポートを設定する場合のインターフェースの表記法を説明します。物理ポートは以下の表記で指定します。

- port インターフェースユニットの ID/スロットの ID/ポートの ID
  - インターフェースユニットの ID は、スタックメンバーのボックス ID です。非スタック装置の場合は、デフォルト設定では 1 です。
  - スロットの ID は、本装置の場合は常に 0 です。
  - ポートの ID は物理ポート番号です。

以下に、ポート 1/0/1 のインターフェース設定モード(port)に遷移する例を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)#
```

1.9 VLAN インターフェース

本装置で VLAN インターフェースを設定する場合の表記法を説明します。VLAN インターフェースは以下の表記で指定します。

- vlanX（X は VLAN ID で、1～4094 の範囲で指定）

なお、「vlan 10」のように vlan と VLAN ID の間に半角スペースが必要なコマンド、「vlan10」のように vlan と VLAN ID の間を空けない文字列のみ受け付けるコマンド、両方の文字列を受け付けるコマンドがあります。

以下に、VLAN 10 のインターフェース設定モード(vlan)に遷移する例を示します。

```
# configure terminal
(config)# interface vlan 10
(config-if-vlan)#
```

1.10 エラーメッセージ

装置で認識されないコマンドをユーザーが実行すると、発生したミスに関する基本的な情報を示して、エラーメッセージが生成されます。表示される可能性のあるエラーメッセージのリストを、以下の表に示します。

エラーメッセージ	意味
Ambiguous command	コマンドを認識できるパラメーターが入力されませんでした。
Incomplete command	コマンド実行に必要なすべてのパラメーターが指定されずに、コマンドが実行されました。
Invalid input detected at ^marker	コマンドが正しく入力されませんでした。

「Ambiguous command」（あいまいなコマンド）エラーメッセージが出力される例を示します。

```
# show v
Ambiguous command
```

「Incomplete command」（不完全なコマンド）エラーメッセージが出力される例を示します。

```
# show
Incomplete command
```

「Invalid input...」（無効な入力が...）エラーメッセージが出力される例を示します。

```
# show verb
        ^
Invalid input detected at ^marker
```

1.11 コマンド入力の補助機能

■ 省略形式での実行

コマンドの入力の際は、そのコマンドが認識できる最小限の文字列のみ入力することにより、コマンド文字列の入力を省略することができます。

例えば、"sh ter"と入力して実行すると、show terminal コマンドが実行されます。

```
# sh ter
Terminal Settings:
 Length: 24 lines
 Width: 80 columns
 Default Length: 24 lines
 Default Width: 80 columns
 Baud Rate: 9600 bps
```

■ [TAB]キーによるコマンド補完

コマンドの入力途中で[TAB]キーを押すと、その時点で選択できるコマンドが 1 つの場合は、残りのコマンド文字列が自動的に補完されます。

例えば、"show en"と入力した時点で[TAB]キーを押した場合は、"show environment "(末尾に半角空白) に補完されます。

```
# show en[TAB]キー押下
# show environment
```

■ [?]キーによるヘルプ機能

[?]キーを押した場合、選択可能なコマンド候補やパラメーターのヘルプが表示されます。

例えば、"show m"と入力した時点で[?]キーを押した場合は、"show m"以降で選択可能なすべてのコマンド候補が表示されます。

```
# show m[?]キー押下
mac-address-table   mls                 mmrp-plus           monitor
multicast

# show m
```

例えば、"show environment "(末尾に半角空白) と入力した時点で[?]キーを押した場合は、"show environment "(末尾に半角空白) 以降に選択可能なパラメーターとヘルプが表示されます。

```
# show environment [?]キー押下
fan                         Display fan status
health                      Display health status
memory                      Display memory status
power                       Display power status
slide-switch                Display the slide switch status
temperature                 Display temperature status
|                           Output modifiers
<cr>

# show environment
```

なお、?をヘルプ機能として使用するのではなく、文字列としてコマンドラインに入力したい場合は、Ctrl+V の入力直後に?を入力すると可能です。

1.12 表示結果出力修飾子

show コマンドで表示される結果は、以下のパラメーターでフィルタリングできます。

- begin FILTER-STRING：フィルター文字列と一致する最初の行で、表示を開始します。
- include FILTER-STRING：フィルター文字列と一致するすべての行を表示します。
- exclude FILTER-STRING：フィルター文字列と一致する行を、表示から除外します。

以下に、show running-config コマンドで begin パラメーターを使用した場合の例を示します。

```
# show running-config | begin interface port 1/0/9
interface port 1/0/9
interface port 1/0/10
interface port 1/0/11
interface port 1/0/12

# SSH

ip ssh server
ssh user user1 authentication-method password

#------------------------------------------------------------------
#              End of configuration file for ApresiaNP2500-8MT4X-PoE
#------------------------------------------------------------------
```

以下に、show running-config コマンドで include パラメーターを使用した場合の例を示します。

```
# show running-config | include ssh user
ssh user user1 authentication-method password
```

以下に、show interfaces status コマンドで exclude パラメーターを使用した場合の例を示します。

```
# show interfaces status | exclude not-connected

Port           Status         VLAN          Duplex  Speed           Type
-------------- -------------- ------------- ------- --------------- -------------
Port1/0/1      connected      1             a-full  a-1000          2500BASE-T
Port1/0/5      disabled       1             auto    auto            2500BASE-T
Port1/0/6      disabled       1             auto    auto            2500BASE-T
Port1/0/9      connected      1             a-full  a-10G           10GBASE-R
Port1/0/10     connected      1             a-full  a-10G           10GBASE-R

Total Entries: 12
```

1.13 本書でのコマンド説明の記載項目

本書では、各コマンドを以下の構成で説明しています。

見出し	内容
目的	コマンドの使用目的を示します。
Command	コマンド構文を示します。
Parameter	各パラメーターの詳細情報（省略の可否、設定範囲など）を示します。
デフォルト	設定コマンドのデフォルト設定を示します。この項目が不要な show コマンドなどではデフォルト項目は含まれません。
モード	コマンドを実行できるコマンドモードを示します。コマンドモードについては、「1.7 コマンドモード」を参照してください。
特権レベル	コマンドを実行可能な最低特権レベルを示します。
ガイドライン	コマンドの詳細な説明を示します。
制限・注意	コマンドの制限事項・注意事項を示します。
バージョン	コマンド、追加パラメーター、仕様変更などのバージョン情報を示します。記載したバージョン以降でサポートしています。

使用例：コマンドの実行例を示します。基本的には特権実行モードからの操作を示しています。

2 インターフェースとハードウェア

2.1 インターフェースコマンド

インターフェース関連の設定コマンドは以下のとおりです。

- interface
- interface range
- description
- shutdown
- default port-shutdown

インターフェース関連の show／操作コマンドは以下のとおりです。

- show interfaces
- show interfaces counters
- show interfaces status
- show interfaces utilization
- show interfaces gbic
- show interfaces description
- show interfaces auto-negotiation
- show interfaces transceiver
- show counters
- clear counters

2.1.1 interface

interface	
目的	単一インターフェースのインターフェース設定モードに遷移します。また、VLAN インターフェースなどを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	interface IF-ID no interface IF-ID
Parameter	IF-ID：インターフェース設定モードに遷移するインターフェースを、以下のパラメーターで指定します。インターフェース ID は種類と番号から構成されており、本コマンドでは種類と番号の間に半角スペースがあってもなくても実行できます。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定 • l2vlan <1-4094>：レイヤー2 VLAN インターフェース指定 各パラメーターを指定してインターフェース設定モードに遷移すると、プロンプトはそれぞれ以下に変更されます。 • port 指定時：(config-if-port)# • port-channel 指定時：(config-if-port-channel)# • vlan 指定時：(config-if-vlan)# • mgmt 指定時：(config-if-mgmt)#

interface	
	• l2vlan 指定時：(config-if-l2vlan)#
デフォルト	VLAN インターフェースは VLAN 1 インターフェースが設定済み。
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	インターフェース番号の形式は、インターフェースの種類に依存します。 物理ポートのインターフェース設定モードに遷移するには、interface port コマンドを使用します。マネージメントポートのインターフェース設定モードに遷移するには、interface mgmt コマンドを使用します。なお、物理ポートおよびマネージメントポートは削除できません。 ApresiaNP2500 シリーズでは、レイヤー3 用の VLAN インターフェースは 1 個だけ設定できます。デフォルトで VLAN 1 インターフェースが設定済みのため、別の VLAN を指定して VLAN インターフェースを作成する場合は、先に VLAN 1 インターフェースを削除 (no interface vlan 1) してから設定してください。レイヤー3 用の VLAN インターフェースを作成してインターフェース設定モードに遷移するには、interface vlan コマンドを使用します。未設定の VLAN に対しては VLAN インターフェースを作成できないため、あらかじめ vlan コマンドで VLAN を設定してから VLAN インターフェースを作成してください。作成した VLAN インターフェースには、初期値として 0.0.0.0/0 の IPv4 アドレスが割り当てられます。VLAN インターフェースを削除するには、no interface vlan コマンドを使用します。 ポートチャネルは、channel-group コマンドでメンバーポートを設定すると自動的に作成されます。ポートチャネルのインターフェース設定モードに遷移するには、interface port-channel コマンドを使用します。すべてのメンバーポートが削除されると自動的に削除されます。また、no interface port-channel コマンドを使用してポートチャネルを削除することもできます。 vlan コマンドで VLAN を作成すると、対応するレイヤー2 VLAN インターフェースも自動的に作成されます。レイヤー2 VLAN インターフェースは、description コマンドでインターフェースの説明を設定する場合にのみ使用しますが、description コマンドを設定していない状態では構成情報で interface l2vlan は表示されません。レイヤー2 VLAN インターフェースのインターフェース設定モードに遷移するには、interface l2vlan コマンドを使用します。no vlan コマンドで VLAN を削除すると、対応するレイヤー2 VLAN インターフェースも自動的に削除されます。
制限・注意	• 本コマンドはスタックポートを指定して実行できません。 • ApresiaNP2500 シリーズでは、設定できるレイヤー3 用の VLAN インターフェースは 1 個のため、VLAN 間のレイヤー3 中継はできません。 • VLAN インターフェースの削除は、削除する VLAN インターフェースに関連している設定を、あらかじめ削除してから実行してください。
バージョン	1.08.02

使用例：ポート 1/0/5 のインターフェース設定モード(port)に遷移する方法を示します。

```
# configure terminal
(config)# interface port 1/0/5
(config-if-port)#
```

使用例：VLAN 100 の VLAN インターフェースを作成し、VLAN 100 のインターフェース設定モード(vlan)に遷移する方法を示します。

```
# configure terminal
(config)# no interface vlan 1
(config)# interface vlan 100
(config-if-vlan)#
```

使用例：ポートチャネル 3 のインターフェース設定モード(port-channel)に遷移する方法を示します。

```
# configure terminal
(config)# interface port-channel 3
(config-if-port-channel)#
```

使用例：VLAN 1 のレイヤー2 VLAN インターフェースで、インターフェースの説明「control_vlan」を設定する方法を示します。

```
# configure terminal
(config)# interface l2vlan 1
(config-if-l2vlan)# description control_vlan
(config-if-l2vlan)#
```

2.1.2 interface range

interface range	
目的	複数インターフェースの範囲設定モードに遷移します。
Command	interface range IF-ID [,|-]
Parameter	IF-ID：範囲設定モードに遷移する複数のインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能（例：1/0/1,1/0/3-5） • l2vlan <1-4094>：レイヤー2 VLAN インターフェース指定（例：10,30-35） 各パラメーターを指定して複数インターフェースの範囲設定モードに遷移すると、プロンプトはそれぞれ以下に変更されます。 • port 指定時：(config-if-port-range)# • l2vlan 指定時：(config-if-l2vlan-range)#
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	複数インターフェースの範囲設定モードで設定したコマンドは、対象の複数インターフェースに適用されます。
制限・注意	• 本コマンドはスタックポートを指定して実行できません。
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/5 を指定して、複数インターフェースの範囲設定モードに遷移する方法を示します。

```
# configure terminal
(config)# interface range port 1/0/1-5
(config-if-port-range)#
```

2.1.3 description

description	
目的	インターフェースの説明を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	description STRING no description
Parameter	STRING：インターフェースの説明を最大 64 文字で指定します。ASCII コードの印字可能な文字のうち、? を除いた文字を使用可能です。スペースも使用できます。
デフォルト	なし
モード	インターフェース設定モード(port, range, port-channel, vlan, mgmt, l2vlan)
特権レベル	レベル：12
ガイドライン	設定した値は、RFC 2233 で定義されている MIB オブジェクト「ifAlias」に反映されます。
制限・注意	• ポートチャネルでの description 設定は、AEOS-NP2500 Ver. 1.10.01 以降でサポートしています。
バージョン	1.08.02 1.10.01：ポートチャネルでの設定に対応

使用例：ポート 1/0/10 で、インターフェースの説明「Physical port 10」を設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/10
(config-if-port)# description Physical port 10
(config-if-port)#
```

2.1.4 shutdown

shutdown	
目的	インターフェースを無効にします。有効にする場合は、no shutdown コマンドを使用します。
Command	shutdown no shutdown
Parameter	なし
デフォルト	有効 (no shutdown)
モード	インターフェース設定モード(port, range, vlan, mgmt)
特権レベル	レベル：12
ガイドライン	物理ポート、VLAN インターフェース、およびマネージメントポートで実行できます。ポートチャネルのメンバーポートに対しても実行できます。 無効に設定すると対象インターフェースのリンク状態もダウンし、すべてのパケットを送受信しなくなります。
制限・注意	• 本コマンドを実行した場合、1 つのポートを無効化するのに数百ミリ秒の時間を要します。そのため、同時に複数ポートに対して本コマンドを実行した場合、ポート数によっては、すべてのポートの無効化が完了するまでに数秒から数十秒程度の時間を要します。
バージョン	1.08.02

使用例：shutdown コマンドで、ポート 1/0/1 を無効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# shutdown
```

2.1.5 default port-shutdown

default port-shutdown	
目的	reset system コマンドによる構成情報リセット後の再起動時に、全ポートを強制的にリンクダウン状態にする機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	default port-shutdown no default port-shutdown
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドは、reset system コマンドによる構成情報リセット＆再起動後のレイヤー 2 ループ事象を防止するためのものです。 本コマンド設定後に以下のコマンドを実行すると、構成情報リセット＆再起動後の running-config、および startup-config 上の全ポートに shutdown コマンドが設定され、全ポートがリンクダウン状態で起動します。なお、再起動後も、default port-shutdown 設定は削除されません。 • reset system コマンド • reset system factory-default コマンド
制限・注意	• default port-shutdown 設定は、clear running-config コマンドを実行しても削除されません。
バージョン	1.08.02

使用例：reset system コマンドによる構成情報リセット後の再起動時に、全ポートを強制的にリンクダウン状態にする機能を有効にする方法を示します。

```
# configure terminal
(config)# default port-shutdown
(config)#
```

2.1.6 show interfaces

show interfaces	
目的	インターフェース情報を表示します。
Command	show interfaces [IF-ID [,|-]]
Parameter	IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード

show interfaces	
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべての物理ポートの情報が表示されます。
制限・注意	• 本コマンドではスタックポートの情報は表示されません。
バージョン	1.08.02

使用例：VLAN 1 インターフェースの情報を表示する方法を示します。

```
# show interfaces vlan 1
(1)                 (2)
vlan1 is enabled, link status is up
  Interface type: VLAN ...(3)
  Interface description: ...(4)
  MAC address: FC-6D-D1-F2-82-1F ...(5)
```

項番	説明
(1)	VLAN インターフェースの有効／無効を表示します。 enabled：有効 (no shutdown 設定時) disabled：無効 (shutdown 設定時)
(2)	VLAN インターフェースのリンク状態 (up／down) を表示します。
(3)	インターフェースの種類が VLAN インターフェースなことを示します。
(4)	VLAN インターフェースの説明を表示します。
(5)	VLAN インターフェースの MAC アドレスを表示します。

使用例：ポート 1/0/1 のインターフェース情報を表示する方法を示します。

```
# show interfaces port 1/0/1
(1)                    (2)
Port1/0/1 is enabled, link status is up
  Interface type: 2500BASE-T ...(3)
  Interface description: ...(4)
  MAC Address: FC-6D-D1-F2-82-20 ...(5)
  Auto-duplex, auto-speed, auto-mdix ...(6)
  Send flow-control: off, receive flow-control: off ...(7)
  Send flow-control oper: off, receive flow-control oper: off ...(8)
  Full-duplex, 1Gb/s ...(9)
  Maximum transmit unit: 1536 bytes ...(10)
  RX rate: 0 bits/sec, TX rate: 0 bits/sec ...(11)
  RX bytes: 0, TX bytes: 0 ...(12)
  RX rate: 0 packets/sec, TX rate: 0 packets/sec ...(13)
  RX packets: 0, TX packets: 0 ...(14)
  RX multicast: 0, RX broadcast: 0 ...(15)
  RX CRC error: 0, RX undersize: 0 ...(16)
  RX oversize: 0, RX fragment: 0 ...(17)
  RX jabber: 0, RX dropped Pkts: 0 ...(18)
  RX MTU exceeded: 0 ...(19)
  TX CRC error: 0, TX excessive deferral: 0 ...(20)
  TX single collision: 0, TX excessive collision: 0 ...(21)
  TX late collision: 0, TX collision: 0 ...(22)
```

項番	説明
(1)	ポートの有効／無効を表示します。

項番	説明
	enabled：有効（no shutdown 設定時） disabled：無効（shutdown 設定時）
(2)	ポートのリンク状態を表示します。 up：リンクアップ状態 down：リンクダウン状態 down（error disabled: 機能名称）：以下の機能による err-disabled 状態 • Loop Detection：ループ検知機能（ポートベースモード） • Storm Control：ストームコントロール機能 • OAM Unidirectional Link：単方向リンク検出機能 • Port Security：ポートセキュリティー機能 down（cause: Memory Error）：memory-error fault-action shutdown-all コマンドの機能によってポートがシャットダウンされた状態 errDis：LLDP 疑似リンクダウン状態
(3)	インターフェースの種類を表示します。 2500BASE-T：RJ-45 ポート（100BASE-TX/1000BASE-T/2.5GBASE-T） 1000BASE-T：RJ-45 ポート（10BASE-T/100BASE-TX/1000BASE-T） 10GBASE-R：SFP/SFP+ポート
(4)	ポートの説明を表示します。
(5)	ポートの MAC アドレスを表示します。
(6)	デュプレックスモード、速度、および MDIX 設定を表示します。 <デュプレックスモード> Auto-duplex ：duplex auto 設定時 Full ：全二重モード（duplex full 設定時） Half ：半二重モード（duplex half 設定時） <速度> auto-speed ：speed auto［SPEED-LIST］設定時 10G ：10Gbps（speed 10giga 設定時） 2.5G ：2.5Gbps（speed 2500 設定時） 2.5G master ：2.5Gbps（speed 2500 master 設定時） 2.5G slave ：2.5Gbps（speed 2500 slave 設定時） 1000 ：1000Mbps（speed 1000 設定時） 1000 master ：1000Mbps（speed 1000 master 設定時） 1000 slave ：1000Mbps（speed 1000 slave 設定時） 100 ：100Mbps（speed 100 設定時） 10 ：10Mbps（speed 10 設定時） <MDIX 設定> auto-mdix ：Auto MDI/MDI-X モード（mdix auto 設定時） normal-mdix ：MDI-X モード（mdix normal 設定時） cross-mdix ：MDI モード（mdix cross 設定時）
(7)	送信時および受信時のフロー制御設定（off：無効／on：有効）を表示します。

項番	説明
(8)	送信時および受信時のフロー制御の実動作（off：無効状態／on：有効状態）を表示します。
(9)	ポートのリンク状態、デュプレックスモード、および速度を表示します。 Full-duplex, 10Gb/s ：10Gbps/Full でリンクアップ状態 Full-duplex, 2.5Gb/s ：2.5Gbps/Full でリンクアップ状態 Full-duplex, 1Gb/s ：1000Mbps/Full でリンクアップ状態 Full-duplex, 100Mb/s ：100Mbps/Full でリンクアップ状態 Half-duplex, 100Mb/s ：100Mbps/Half でリンクアップ状態 Full-duplex, 10Mb/s ：10Mbps/Full でリンクアップ状態 Half-duplex, 10Mb/s ：10Mbps/Half でリンクアップ状態 Down ：リンクダウン状態
(10)	許容する最大イーサネットフレームサイズを表示します。
(11)	1 秒あたりの受信ビット数、および 1 秒あたりの送信ビット数を表示します。
(12)	受信バイト数、および送信バイト数を表示します。
(13)	1 秒あたりの受信パケット数、および 1 秒あたりの送信パケット数を表示します。
(14)	受信パケット数、および送信パケット数を表示します。
(15)	受信マルチキャストパケット数、および受信ブロードキャストパケット数を表示します。
(16)	受信 FCS エラー、および受信アンダーサイズパケットエラーのパケット数を表示します。
(17)	受信オーバーサイズパケットエラー、および受信フラグメントエラーのパケット数を表示します。
(18)	受信ジャバーパケットカウンター、および受信パケットドロップカウンターを表示します。 <受信パケットドロップカウンターのカウント対象例> • アクセスポートで、VLAN タグ付きフレームを受信した場合。（アクセスポートのデフォルトは acceptable-frame untagged-only） • トランクポートで、許可していない VID の VLAN タグ付きフレームを受信した場合。（デフォルトは ingress-checking 有効） • 非スタック装置で、中継可能なポートが存在しない場合（例：同一 VLAN の受信ポート以外のすべてのポートがリンクダウン状態）。 • 許容する最大イーサネットフレームサイズを超えるサイズのフレームを受信した場合。 • 送信元 MAC アドレスがブロードキャスト、マルチキャスト、もしくは ALL=0 のフレームを受信した場合。 • 宛先 MAC アドレスが、受信ポート宛てに学習済みの場合。もしくは、drop 指定のスタティック MAC アドレスエントリーとして設定済みの場合。 • マルチキャストフィルタリングモードが filter-unregistered モードで、未登録宛てのマルチキャストを受信した場合。 • アクセスリスト機能で、受信フレームを破棄した場合。 • 帯域制限機能（ストームコントロール、rete-limit input、もしくは受信ポートに適用したポリシーマップのポリサー）で、受信フレームを破棄した場合。 • レイヤー2 冗長機能（ポートリダンダント、STP/RSTP/MSTP/RPVST+、MMRP-Plus（Hello パケット含む）、ERPS）によって、送受信が抑制されているポートでトラフィックを受信した場合。 • 対象が自装置宛ての IP パケットで、不正な IP パケットの場合（例：IP チェックサムエラー）。

項番	説明
(19)	受信ポートの最大イーサネットフレームサイズによって破棄されたパケット数を表示します。
(20)	送信 FCS エラー、および送信過剰遅延のパケット数を表示します。
(21)	1 回のコリジョンだけで送信が成功した回数、および過度のコリジョン(16 回)によって転送が失敗した回数を表示します。
(22)	遅延コリジョンの発生回数、および送信コリジョンの発生回数を表示します。

使用例：マネージメントポートのインターフェース情報を表示する方法を示します。

```
# show interfaces mgmt 0
(1)                        (2)
mgmt_ipif 0 is enabled, link status is up
  Interface type: Management port  ...(3)
  Interface description:  ...(4)
  Auto-duplex, auto-speed, auto-mdix  ...(5)
```

項番	説明
(1)	マネージメントポートの有効／無効を表示します。 enabled：有効 (no shutdown 設定時) disabled：無効 (shutdown 設定時)
(2)	マネージメントポートのリンク状態 (up／down) を表示します。
(3)	インターフェースの種類がマネージメントポートなことを示します。
(4)	マネージメントポートの説明を表示します。
(5)	デュプレックスモード、速度、および MDIX 設定を表示します。 <デュプレックスモード、速度> Auto-duplex, auto-speed ：speed_duplex auto 設定時 Full, 100 ：100Mbps/Full (speed_duplex 100_full 設定時) Half, 100 ：100Mbps/Half (speed_duplex 100_half 設定時) Full, 10 ：10Mbps/Full (speed_duplex 10_full 設定時) Half, 10 ：10Mbps/Half (speed_duplex 10_half 設定時) <MDIX 設定> auto-mdix ：Auto MDI/MDI-X モード (mdix auto 設定時) normal-mdix ：MDI-X モード (mdix normal 設定時) cross-mdix ：MDI モード (mdix cross 設定時)

2.1.7 show interfaces counters

show interfaces counters	
目的	インターフェースカウンター（送受信オクテットカウンター、送受信パケットカウンター）を表示します。
Command	show interfaces [IF-ID [,|-]] counters [errors]
Parameter	IF-ID (省略可能)：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • mgmt 0：マネージメントポート指定、マネージメントポートの場合は errors

show interfaces counters	
	パラメーターは省略不可 errors（省略可能）：エラーカウンターを表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべての物理ポートの情報が表示されます。
制限・注意	• 本コマンドではスタックポートの情報は表示されません。
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/2 のインターフェースカウンター（送受信オクテットカウンター、送受信パケットカウンター）を表示する方法を示します。

```
# show interfaces port 1/0/1-2 counters
(1)            (2)                      (4)
Port           InOctets /               InMcastPkts /
               InUcastPkts ...(3)       InBcastPkts ...(5)
-------------- ------------------------ ------------------------
Port1/0/1                       110664                      413
                                     0                      402
Port1/0/2                            0                        0
                                     0                        0
               (6)                      (8)
Port           OutOctets /              OutMcastPkts /
               OutUcastPkts ...(7)      OutBcastPkts ...(9)
-------------- ------------------------ ------------------------
Port1/0/1                            0                        0
                                     0                        0
Port1/0/2                            0                        0
                                     0                        0

Total Entries: 2
```

項番	説明
(1)	ポート番号を表示します。
(2)	受信オクテットカウンターを表示します。
(3)	受信ユニキャストパケットカウンターを表示します。
(4)	受信マルチキャストパケットカウンターを表示します。
(5)	受信ブロードキャストパケットカウンターを表示します。
(6)	送信オクテットカウンターを表示します。
(7)	送信ユニキャストパケットカウンターを表示します。
(8)	送信マルチキャストパケットカウンターを表示します。
(9)	送信ブロードキャストパケットカウンターを表示します。

使用例：ポート 1/0/1～1/0/2 のエラーカウンターを表示する方法を示します。

```
# show interfaces port 1/0/1-2 counters errors
(1)            (2)         (3)         (4)         (5)         (6)         (7)
Port           Align-Err   Fcs-Err     Rcv-Err     Undersize   Xmit-Err    OutDiscard
-------------- ----------- ----------- ----------- ----------- ----------- -----------
Port1/0/1                0           0           0           0           0           0
```

```
Port1/0/2              0          0          0          0          0          0
               (8)        (9)        (10)       (11)       (12)       (13)
Port           Single-Col Multi-Col  Late-Col   Excess-Col Carri-Sen  Runts
-------------- ---------- ---------- ---------- ---------- ---------- ----------
Port1/0/1              0          0          0          0          0          0
Port1/0/2              0          0          0          0          0          0
               (14)       (15)       (16)       (17)       (18)       (19)
Port           Giants     Symbol-Err SQETest-Err DeferredTx IntMacTx   IntMacRx
-------------- ---------- ---------- ---------- ---------- ---------- ----------
Port1/0/1              0          0          0          0          0          0
Port1/0/2              0          0          0          0          0          0

Total Entries: 2
```

項番	説明
(1)	ポート番号を表示します。
(2)	特定のインターフェースで受信した、整数倍ではないオクテット長で、かつ FCS チェックに合格しないパケットの数を表示します。
(3)	受信 FCS エラーパケットカウンターを表示します。
(4)	上位レイヤープロトコルへの配信を妨げるエラーを含む、受信パケット数を表示します。
(5)	受信アンダーサイズパケットカウンターを表示します。
(6)	エラーのために送信できない送信パケット数を表示します。
(7)	送信を妨げるエラーが検知されていない場合に、廃棄を指定された送信パケット数を表示します。
(8)	1 回のコリジョンで送信が抑止された特定のインターフェースで、正常に送信されたパケット数を表示します。
(9)	2 回以上のコリジョンで送信が抑止された特定のインターフェースで、正常に送信されたパケット数を表示します。
(10)	パケットに割り当てられたスロットタイムが経過した後に、特定のインターフェースでコリジョンが検知された回数を表示します。
(11)	過度なコリジョンが原因で、特定のインターフェースで送信に失敗したパケット数を表示します。
(12)	特定のインターフェースでパケットを送信しようとしたときに、キャリア検知状態が失われた、またはアサートされていなかった回数を表示します。
(13)	受信フラグメントカウンターと受信アンダーサイズパケットカウンターの合計を表示します。
(14)	受信オーバーサイズパケットカウンターと受信ジャンボフレームカウンターの合計を表示します。
(15)	受信コードエラーパケットカウンターを表示します。
(16)	特定のインターフェースに対し、PLS サブレイヤーによって SQE TEST ERROR メッセージが出力された回数を表示します。
(17)	メディアがビジー状態のため、特定のインターフェースで初回の送信が遅延したパケット数を表示します。
(18)	内部 MAC サブレイヤーの送信エラーが原因で、特定のインターフェースで送信に失敗したパケット数を表示します。
(19)	内部 MAC サブレイヤーの受信エラーが原因で、特定のインターフェースで受信に失敗したパケット数を表示します。

使用例：マネージメントポートのエラーカウンターを表示する方法を示します。

```
# show interfaces mgmt 0 counters errors

 rxFCSErrorPkts            :           0 ...(1)
 rxAlignmentErrorPkts      :           0 ...(2)
 rxCodeErrorPkts           :           0 ...(3)
 rxUndersizedPkts          :           0 ...(4)
 rxOversizedPkts           :           0 ...(5)
 rxFragmentPkts            :           0 ...(6)
 rxJabbers                 :           0 ...(7)
 rxDropPkts                :           0 ...(8)
 txExcessiveDeferralPkts   :           0 ...(9)
 txFCSErrorPkts            :           0 ...(10)
 txLateCollisionPkts       :           0 ...(11)
 txExcessiveCollisionPkts  :           0 ...(12)
 txDropPkts                :           0 ...(13)
```

項番	説明
(1)	受信 FCS エラーパケットカウンターを表示します。
(2)	マネージメントポートで受信した、整数倍ではないオクテット長で、かつ FCS チェックに合格しないパケットの数を表示します。
(3)	受信コードエラーパケットカウンターを表示します。
(4)	受信アンダーサイズパケットカウンターを表示します。
(5)	受信オーバーサイズパケットカウンターを表示します。
(6)	受信フラグメントカウンターを表示します。
(7)	受信ジャバーパケットカウンターを表示します。
(8)	受信パケットドロップカウンターを表示します。
(9)	送信過剰遅延のパケットカウンターを表示します。
(10)	送信 FCS エラーパケットカウンターを表示します。
(11)	遅延コリジョンの発生回数を表示します。
(12)	過度のコリジョン(16 回)によって転送が失敗した回数を表示します。
(13)	送信パケットドロップカウンターを表示します。

2.1.8 show interfaces status

show interfaces status	
目的	ポートの接続状態を表示します。
Command	show interfaces [port PORTS] status
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	• 本コマンドではスタックポートの情報は表示されません。
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/8 のポート接続状態を表示する方法を示します。

```
# show interfaces port 1/0/1-8 status
(1)            (2)            (3)          (4)                    (5)
Port           Status         VLAN         Duplex  Speed          Type
-------------- -------------- ------------ ------- -------------- -------------
Port1/0/1      connected      1            a-full  a-1000         2500BASE-T
Port1/0/2      not-connected  1            auto    auto           2500BASE-T
Port1/0/3      not-connected  1            auto    auto           2500BASE-T
Port1/0/4      not-connected  1            auto    auto           2500BASE-T
Port1/0/5      not-connected  1            auto    auto           2500BASE-T
Port1/0/6      not-connected  1            auto    auto           2500BASE-T
Port1/0/7      connected      1            a-full  a-1000         2500BASE-T
Port1/0/8      connected      1            a-full  a-1000         2500BASE-T

Total Entries: 8
```

項番	説明
(1)	ポート番号を表示します。
(2)	ポートの状態を表示します。 connected：リンクアップ状態 not-connected：有効設定（no shutdown）で、リンクダウン状態 disabled：無効設定（shutdown）で、リンクダウン状態 err-disabled：err-disabled 状態 memory-error：memory-error fault-action shutdown-all コマンドの機能によってポートがシャットダウンされた状態
(3)	アクセス VLAN またはネイティブ VLAN の VLAN ID を表示します。 対象ポートがポートチャネルのメンバーポートの場合は trunk と表示されます。 対象ポートがプライベート VLAN プロミスキャスポートの場合はプライマリーVLAN の、プライベート VLAN ホストポートの場合はセカンダリーVLAN の VLAN ID を表示します。
(4)	デュプレックスモードと通信速度を表示します。 ■ RJ-45 ポート(100BASE-TX/1000BASE-T/2.5GBASE-T) a-full a-2500 ： オートネゴシエーション有効、2.5Gbps/Full ※1 a-full a-1000 ： オートネゴシエーション有効、1000Mbps/Full ※1 a-full a-100 ： オートネゴシエーション有効、100Mbps/Full ※1 a-half a-100 ： オートネゴシエーション有効、100Mbps/Half ※1 auto auto ： speed 設定／duplex 設定の両方、またはどちらかが auto 設定で、リンクアップしていない状態の場合 full 100 ： 100Mbps/Full 固定設定 ※2 half 100 ： 100Mbps/Half 固定設定 ※2 ■ RJ-45 ポート(10BASE-T/100BASE-TX/1000BASE-T) a-full a-1000 ： オートネゴシエーション有効、1000Mbps/Full ※1 a-full a-100 ： オートネゴシエーション有効、100Mbps/Full ※1 a-half a-100 ： オートネゴシエーション有効、100Mbps/Half ※1 a-full a-10 ： オートネゴシエーション有効、10Mbps/Full ※1 a-half a-10 ： オートネゴシエーション有効、10Mbps/Half ※1 auto auto ： speed 設定／duplex 設定の両方、またはどちらかが auto 設定

項番	説明
	で、リンクアップしていない状態の場合 full 100 : 100Mbps/Full 固定設定 ※2 half 100 : 100Mbps/Half 固定設定 ※2 full 10 : 10Mbps/Full 固定設定 ※2 half 10 : 10Mbps/Half 固定設定 ※2 ■ SFP/SFP+ポート a-full a-10G : 10Gbps/Full (speed auto, duplex auto 設定時) ※1 a-full a-1000 : オートネゴシエーション有効、1000Mbps/Full ※1 auto auto : speed 設定／duplex 設定の両方、またはどちらかが auto 設定で、リンクアップしていない状態の場合 full 10G : 10Gbps/Full (speed 10giga, duplex full 設定時) ※2 full 1000 : 1000Mbps/Full 固定設定 ※2 ※1：リンクアップ状態の場合 ※2：この設定パターンの場合は、リンク状態にかかわらず常にこの表示
(5)	インターフェースの種類を表示します。 2500BASE-T：RJ-45 ポート(100BASE-TX/1000BASE-T/2.5GBASE-T) 1000BASE-T：RJ-45 ポート(10BASE-T/100BASE-TX/1000BASE-T) 10GBASE-R：SFP/SFP+ポート

2.1.9 show interfaces utilization

show interfaces utilization	
目的	ポートの使用率を表示します。
Command	show interfaces [port PORTS] utilization
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	• 本コマンドではスタックポートの情報は表示されません。
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/2 のポートの使用率を表示する方法を示します。

```
# show interfaces port 1/0/1-2 utilization
(1)             (2)                 (3)                 (4)
Port            TX packets/sec /    TX bits/sec /       Utilization
                RX packets/sec      RX bits/sec
-------------   ------------------ ------------------ -----------
Port1/0/1                    6165           39048256           7
                            15413           97284024
Port1/0/2                       0                  0           0
                                0                  0

Total Entries: 2
```

項番	説明
(1)	ポート番号を表示します。
(2)	1 秒あたりの送信パケット数[上段]／受信パケット数[下段]を表示します。
(3)	1 秒あたりの送信ビット数[上段]／受信ビット数[下段]を表示します。
(4)	送受信あわせたポートの使用率(%)を表示します。

2.1.10 show interfaces gbic

show interfaces gbic	
目的	トランシーバーの情報を表示します。
Command	show interfaces [port PORTS] gbic
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	• 本コマンドではスタックポートの情報は表示されません。
バージョン	1.08.02

使用例：ポート 1/0/12 のトランシーバーの情報を表示する方法を示します。

```
# show interfaces port 1/0/12 gbic

Port1/0/12 ...(1)
 Type: H-SR-SFP+ ...(2)
 Vendor PN: FTLX8571D3BCL ...(3)
 Vendor SN: APC10LX ...(4)
```

項番	説明
(1)	ポート番号を表示します。
(2)	挿入されているトランシーバーの種類を表示します。
(3)	型式番号を表示します。
(4)	シリアル番号を表示します。

2.1.11 show interfaces description

show interfaces description	
目的	インターフェースの説明とリンク状態を表示します。
Command	show interfaces [IF-ID [,|-]] description
Parameter	IF-ID (省略可能)：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定 • l2vlan [<1-4094>]：レイヤー2 VLAN インターフェース指定、複数指定可能
モード	ユーザー実行モード、特権実行モード、任意の設定モード

show interfaces description	
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	• 本コマンドではスタックポートの情報は表示されません。
バージョン	1.08.02 1.10.01：port-channel パラメーター追加

使用例：インターフェースの説明とリンク状態を表示する方法を示します。

```
# show interfaces description
 (1)                  (2)       (3)             (4)
 Interface            Status    Administrative  Description
 -------------------- --------  --------------  ------------------------------
 Port1/0/1            up        enabled         TEST Port1/0/1
 Port1/0/2            up        enabled         3FN-04[1/0/2] to Conference ro
                                                om(ARENA-2F-007)
 Port1/0/3            down      enabled
 Port1/0/4            down      disabled
～～省略～～
 Port1/0/10           down      enabled
 Port1/0/11           down      enabled
 Port1/0/12           down      enabled
 Mgmt 0               up        enabled
 L2VLAN 1             up        enabled
 Interface vlan1      up        enabled         TEST VLAN 1 Interface

Total Entries: 15
```

項番	説明
(1)	ポート番号などのインターフェース ID を表示します。
(2)	インターフェースの状態を表示します。 up：アップ状態 down：ダウン状態 errDis：LLDP 疑似リンクダウン状態（物理ポートの場合のみ）
(3)	インターフェースの有効／無効設定を表示します。ポートチャネル、レイヤー2 VLAN インターフェースは常に enabled 表示です。 enabled：有効（no shutdown 設定時） disabled：無効（shutdown 設定時）
(4)	インターフェースの説明を表示します。description コマンドで設定した文字列（最大 64 文字）が 30 文字を超える場合、31 文字以降、61 文字以降は行が変更されて表示されます。

2.1.12 show interfaces auto-negotiation

show interfaces auto-negotiation	
目的	ポートのオートネゴシエーション情報の詳細を表示します。
Command	show interfaces [port PORTS] auto-negotiation
Parameter	port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1

show interfaces auto-negotiation	
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	• 本コマンドではスタックポートの情報は表示されません。 • SFP/SFP+ポートでは、本コマンドで表示される項目のうち[Auto Negotiation]以外の項目は未サポートです。 • SFP/SFP+ポートで 10GBASE-R トランシーバーを挿入して 10Gbps/Full 固定で使用する場合は、本コマンドは未サポートです。
バージョン	1.08.02

使用例：ポート 1/0/1 のオートネゴシエーション情報の詳細を表示する方法を示します。

```
# show interfaces port 1/0/1 auto-negotiation

Port1/0/1 ...(1)
 Auto Negotiation: Enabled ...(2)

 Speed auto downgrade: Disabled ...(3)
 Remote Signaling: Not detected ...(4)
 Configure Status: Complete ...(5)
 Capability Bits: 100M_Half, 100M_Full, 1000M_Full, 2500M_Full ...(6)
 Capability Advertised Bits: 100M_Half, 100M_Full, 1000M_Full, 2500M_Full ...(7)
 Capability Received Bits: 100M_Half, 100M_Full, 1000M_Full ...(8)
 RemoteFaultAdvertised: Disabled ...(9)
 RemoteFaultReceived: NoError ...(10)
```

項番	説明
(1)	ポート番号を表示します。
(2)	オートネゴシエーションの有効(Enabled)／無効(Disabled)を表示します。
(3)	speed auto-downgrade 設定の有効(Enabled)／無効(Disabled)を表示します。
(4)	リモートシグナルの状況を表示します。
(5)	オートネゴシエーションの状況を表示します。
(6)	使用可能な通信速度とデュプレックスモードを表示します。
(7)	対向装置に通知する通信速度とデュプレックスモードを表示します。
(8)	対向装置から通知された通信速度とデュプレックスモードを表示します。
(9)	本項目の表示は未サポートです。
(10)	本項目の表示は未サポートです。

2.1.13 show interfaces transceiver

show interfaces transceiver	
目的	SFP/SFP+トランシーバーの動作状況を表示します。
Command	show interfaces [port PORTS] transceiver [detail]
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。 detail (省略可能)：詳細情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、光トランシーバーが挿入されているすべてのポー

show interfaces transceiver	
	トの情報が表示されます。
制限・注意	• 本コマンドではスタックポートの情報は表示されません。 • 10Gbps の AOC（Active Optical Cable、型式：H-SFP+AOC1M/3M/5M/10M）の場合は情報は表示されません。 • 凡例にある「++ : high alarm」「+ : high warning」「- : low warning」「-- : low alarm」表示は未サポートです。表示結果で各値の右に(++)のようなこれらの記号が表示されても、未サポートのため無視してください。 • detail パラメーターを指定して実行した場合に表示される、トランシーバーモニタリング機能に関連する項目は未サポートです。
バージョン	1.08.02

使用例：すべての光トランシーバーの動作状況を表示する方法を示します。

```
# show interfaces transceiver

 ++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
 mA: milliamperes, mW: milliwatts
(1)          (2)           (3)           (4)           (5)
             Voltage       Bias Current  TX Power      RX Power
port         (V)           (mA)          (mW/dbm)      (mW/dbm)
---------- ------------ ------------ ------------ ------------
Port1/0/12 3.279         7.851         0.643         0.317
                                       -1.915        -4.995

Total Entries: 1
```

項番	説明
(1)	ポート番号を表示します。
(2)	ポートの電圧を表示します。
(3)	ポートのバイアス電流を表示します。
(4)	ポートの送信パワーを表示します。
(5)	ポートの受信パワーを表示します。

2.1.14 show counters

show counters	
目的	指定したインターフェースのカウンターを表示します。
Command	show counters [interface IF-ID [,|-] | cpu-port [detail] | stack-port] show counters [interface port PORTS | cpu-port [detail] | stack-port]
Parameter	interface port PORTS（省略可能）：物理ポートのカウンターを表示する場合に指定します。複数指定できます。 cpu-port [detail]（省略可能）：CPU に送信されたレイヤー2、レイヤー3 関連の制御パケットのカウンターを表示する場合に指定します。detail パラメーターを指定すると、受信ポートごとの情報が表示されます。 stack-port（省略可能）：スタックポートのカウンターを表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード

show counters	
特権レベル	レベル：1
ガイドライン	パラメーター省略時は、物理ポートのカウンター、CPU ポートのカウンター（detail 指定は除く）、スタックポートのカウンターが表示されます。
制限・注意	• ApresiaNP2500 シリーズでは、txCoS0DropPkts～txCoS7DropPkts はカウントしません。
バージョン	1.08.02 1.10.01：cpu-port detail パラメーター追加

使用例：ポート 1/0/1 のカウンターを表示する方法を示します。

```
# show counters interface port 1/0/1

Port1/0/1 counters
rxHCTotalPkts                   :                86734 ...(1)
txHCTotalPkts                   :                   73 ...(2)
rxHCUnicastPkts                 :                  158 ...(3)
txHCUnicastPkts                 :                   73 ...(4)
rxHCMulticastPkts               :                39140 ...(5)
txHCMulticastPkts               :                    0 ...(6)
rxHCBroadcastPkts               :                47436 ...(7)
txHCBroadcastPkts               :                    0 ...(8)
rxHCOctets                      :             14420412 ...(9)
txHCOctets                      :                 4992 ...(10)
rxHCPkt64Octets                 :                38554 ...(11)
rxHCPkt65to127Octets            :                23454 ...(12)
rxHCPkt128to255Octets           :                 7531 ...(13)
rxHCPkt256to511Octets           :                12541 ...(14)
rxHCPkt512to1023Octets          :                 3228 ...(15)
rxHCPkt1024to1518Octets         :                 1426 ...(16)
rxHCPkt1519to1522Octets         :                    0 ...(17)
rxHCPkt1519to2047Octets         :                    0 ...(18)
rxHCPkt2048to4095Octets         :                    0 ...(19)
rxHCPkt4096to9216Octets         :                    0 ...(20)
txHCPkt64Octets                 :                   41 ...(21)
txHCPkt65to127Octets            :                   32 ...(22)
txHCPkt128to255Octets           :                    0 ...(23)
txHCPkt256to511Octets           :                    0 ...(24)
txHCPkt512to1023Octets          :                    0 ...(25)
txHCPkt1024to1518Octets         :                    0 ...(26)
txHCPkt1519to1522Octets         :                    0 ...(27)
txHCPkt1519to2047Octets         :                    0 ...(28)
txHCPkt2048to4095Octets         :                    0 ...(29)
txHCPkt4096to9216Octets         :                    0 ...(30)

rxCRCAlignErrors                :                    0 ...(31)
rxUndersizedPkts                :                    0 ...(32)
rxOversizedPkts                 :                    0 ...(33)
rxFragmentPkts                  :                    0 ...(34)
rxJabbers                       :                    0 ...(35)
rxSymbolErrors                  :                    0 ...(36)
rxDropPkts                      :                50256 ...(37)

txCollisions                    :                    0 ...(38)
ifInErrors                      :                    0 ...(39)
ifOutErrors                     :                    0 ...(40)
ifInDiscards                    :                50256 ...(41)
ifInUnknownProtos               :                    0 ...(42)
ifOutDiscards                   :                    0 ...(43)
txDelayExceededDiscards         :                    0 ...(44)
```

```
txCRC                                :                0 ...(45)
txDropPkts                           :                0 ...(46)
txCoS0DropPkts                       :                0 ...(47)
txCoS1DropPkts                       :                0 ...(48)
txCoS2DropPkts                       :                0 ...(49)
txCoS3DropPkts                       :                0 ...(50)
txCoS4DropPkts                       :                0 ...(51)
txCoS5DropPkts                       :                0 ...(52)
txCoS6DropPkts                       :                0 ...(53)
txCoS7DropPkts                       :                0 ...(54)

dot3StatsAlignmentErrors             :                0 ...(55)
dot3StatsFCSErrors                   :                0 ...(56)
dot3StatsSingleColFrames             :                0 ...(57)
dot3StatsMultiColFrames              :                0 ...(58)
dot3StatsSQETestErrors               :                0 ...(59)
dot3StatsDeferredTransmisions        :                0 ...(60)
dot3StatsLateCollisions              :                0 ...(61)
dot3StatsExcessiveCollisions         :                0 ...(62)
dot3StatsInternalMacTransmitErrors   :                0 ...(63)
dot3StatsCarrierSenseErrors          :                0 ...(64)
dot3StatsFrameTooLongs               :                0 ...(65)
dot3StatsInternalMacReceiveErrors    :                0 ...(66)

linkChange                           :                2 ...(67)
```

項番	説明
(1)	受信パケットカウンターを表示します。
(2)	送信パケットカウンターを表示します。
(3)	受信ユニキャストパケットカウンターを表示します。
(4)	送信ユニキャストパケットカウンターを表示します。
(5)	受信マルチキャストパケットカウンターを表示します。
(6)	送信マルチキャストパケットカウンターを表示します。
(7)	受信ブロードキャストパケットカウンターを表示します。
(8)	送信ブロードキャストパケットカウンターを表示します。
(9)	受信オクテットカウンターを表示します。
(10)	送信オクテットカウンターを表示します。
(11)	受信 64 オクテットパケットカウンターを表示します。
(12)	受信 65～127 オクテットパケットカウンターを表示します。
(13)	受信 128～255 オクテットパケットカウンターを表示します。
(14)	受信 256～511 オクテットパケットカウンターを表示します。
(15)	受信 512～1,023 オクテットパケットカウンターを表示します。
(16)	受信 1,024～1,518 オクテットパケットカウンターを表示します。
(17)	受信 1,519～1,522 オクテットパケットカウンターを表示します。
(18)	受信 1,519～2,047 オクテットパケットカウンターを表示します。
(19)	受信 2,048～4,095 オクテットパケットカウンターを表示します。
(20)	受信 4,096～9,216 オクテットパケットカウンターを表示します。
(21)	送信 64 オクテットパケットカウンターを表示します。
(22)	送信 65～127 オクテットパケットカウンターを表示します。

項番	説明
(23)	送信 128～255 オクテットパケットカウンターを表示します。
(24)	送信 256～511 オクテットパケットカウンターを表示します。
(25)	送信 512～1,023 オクテットパケットカウンターを表示します。
(26)	送信 1,024～1,518 オクテットパケットカウンターを表示します。
(27)	送信 1,519～1,522 オクテットパケットカウンターを表示します。
(28)	送信 1,519～2,047 オクテットパケットカウンターを表示します。
(29)	送信 2,048～4,095 オクテットパケットカウンターを表示します。
(30)	送信 4,096～9,216 オクテットパケットカウンターを表示します。
(31)	受信 FCS エラーパケットカウンターを表示します。
(32)	受信アンダーサイズパケットカウンターを表示します。
(33)	受信オーバーサイズパケットカウンターを表示します。
(34)	受信フラグメントカウンターを表示します。
(35)	受信ジャバーパケットカウンターを表示します。
(36)	受信コードエラーパケットカウンターを表示します。
(37)	受信パケットドロップカウンターを表示します。 <カウント対象例> • アクセスポートで、VLAN タグ付きフレームを受信した場合。(アクセスポートのデフォルトは acceptable-frame untagged-only) • トランクポートで、許可していない VID の VLAN タグ付きフレームを受信した場合。(デフォルトは ingress-checking 有効) • 非スタック装置で、中継可能なポートが存在しない場合 (例：同一 VLAN の受信ポート以外のすべてのポートがリンクダウン状態)。 • 許容する最大イーサネットフレームサイズを超えるサイズのフレームを受信した場合。 • 送信元 MAC アドレスがブロードキャスト、マルチキャスト、もしくは ALL=0 のフレームを受信した場合。 • 宛先 MAC アドレスが、受信ポート宛てに学習済みの場合。もしくは、drop 指定のスタティック MAC アドレスエントリーとして設定済みの場合。 • マルチキャストフィルタリングモードが filter-unregistered モードで、未登録宛てのマルチキャストを受信した場合。 • アクセスリスト機能で、受信フレームを破棄した場合。 • 帯域制限機能 (ストームコントロール、rete-limit input、もしくは受信ポートに適用したポリシーマップのポリサー) で、受信フレームを破棄した場合。 • レイヤー2 冗長機能 (ポートリダンダント、STP/RSTP/MSTP/RPVST+、MMRP-Plus (Hello パケット含む)、ERPS) によって、送受信が抑制されているポートでトラフィックを受信した場合。 • 対象が自装置宛ての IP パケットで、不正な IP パケットの場合 (例：IP チェックサムエラー)。
(38)	送信コリジョンカウンターを表示します。
(39)	上位レイヤープロトコルへの配信を妨げるエラーを含む、受信パケット数を表示します。
(40)	エラーのために送信できない送信パケット数を表示します。
(41)	上位レイヤープロトコルに配信できないエラーが検知されていない場合に、廃棄が選択された受信パケット数を表示します。

項番	説明
(42)	当該インターフェース経由で受信したプロトコルが不明、またはサポートされていないために廃棄されたパケット数を表示します。
(43)	送信を妨げるエラーが検知されていない場合に、廃棄を指定された送信パケット数を表示します。
(44)	送信マルチ遅延パケットカウンターを表示します。
(45)	送信 FCS エラーカウンターを表示します。
(46)	送信パケットドロップカウンターを表示します。
(47)	CoS キュー0 の送信パケットドロップカウンターを表示します。 ApresiaNP2500 シリーズでは、本項目はカウントしません。
(48)	CoS キュー1 の送信パケットドロップカウンターを表示します。 ApresiaNP2500 シリーズでは、本項目はカウントしません。
(49)	CoS キュー2 の送信パケットドロップカウンターを表示します。 ApresiaNP2500 シリーズでは、本項目はカウントしません。
(50)	CoS キュー3 の送信パケットドロップカウンターを表示します。 ApresiaNP2500 シリーズでは、本項目はカウントしません。
(51)	CoS キュー4 の送信パケットドロップカウンターを表示します。 ApresiaNP2500 シリーズでは、本項目はカウントしません。
(52)	CoS キュー5 の送信パケットドロップカウンターを表示します。 ApresiaNP2500 シリーズでは、本項目はカウントしません。
(53)	CoS キュー6 の送信パケットドロップカウンターを表示します。 ApresiaNP2500 シリーズでは、本項目はカウントしません。
(54)	CoS キュー7 の送信パケットドロップカウンターを表示します。 ApresiaNP2500 シリーズでは、本項目はカウントしません。
(55)	特定のインターフェースで受信した、整数倍ではないオクテット長で、かつ FCS チェックに合格しないパケットの数を表示します。
(56)	特定のインターフェースで受信した、整数倍のオクテット長で、かつ FCS チェックに合格にしないパケットの数を表示します。
(57)	1 回のコリジョンで送信が抑止された特定のインターフェースで、正常に送信されたパケット数を表示します。
(58)	2 回以上のコリジョンで送信が抑止された特定のインターフェースで、正常に送信されたパケット数を表示します。
(59)	特定のインターフェースに対し、PLS サブレイヤーによって SQE TEST ERROR メッセージが出力された回数を表示します。
(60)	メディアがビジー状態のため、特定のインターフェースで初回の送信が遅延したパケット数を表示します。
(61)	パケットに割り当てられたスロットタイムが経過した後に、特定のインターフェースでコリジョンが検知された回数を表示します。
(62)	過度なコリジョンが原因で、特定のインターフェースで送信に失敗したパケット数を表示します。
(63)	内部 MAC サブレイヤーの送信エラーが原因で、特定のインターフェースで送信に失敗したパケット数を表示します。
(64)	特定のインターフェースでパケットを送信しようとしたときに、キャリア検知状態が失われ

項番	説明
	た、またはアサートされていなかった回数を表示します。
(65)	特定のインターフェースで受信した、最大許容フレームサイズを超えるパケット数を表示します。
(66)	内部 MAC サブレイヤーの受信エラーが原因で、特定のインターフェースで受信に失敗したパケット数を表示します。
(67)	ポートのステータスが変化した際にカウントされる数字を表示します。

使用例：スタックポートのカウンターを表示する方法を示します。

```
# show counters stack-port

Unit 1, Stack Port 11 counters
ifInErrors                      :                       0 ...(1)
txDropPkts                      :                       0 ...(2)

Unit 1, Stack Port 12 counters
ifInErrors                      :                       0
txDropPkts                      :                       0

Unit 2, Stack Port 11 counters
ifInErrors                      :                       0
txDropPkts                      :                       0

Unit 2, Stack Port 12 counters
ifInErrors                      :                       0
txDropPkts                      :                       0
```

項番	説明
(1)	FCS エラー、アンダーサイズエラーおよびスタックポートでのみ検出可能なエラーを含む、受信パケット数を表示します。
(2)	送信パケットドロップカウンターを表示します。

使用例：CPU に送信されたレイヤー2、レイヤー3 関連の制御パケットのカウンターを表示する方法を示します。

```
# show counters cpu-port

Unit 1, CPU Port counters
txDropPkts                      :                       0 ...(1)
(2)                (3)                  (4)
CoS                cpuRxPkts            cpuTxDropPkts
--- ---------------------- ----------------------
0                         0                       0
1                         0                       0
2                         0                       0
3                         0                       0
4                         0                       0
5                         0                       0
6                         0                       0
7                         0                       0
```

項番	説明
(1)	CPU に送信されたパケットのドロップカウンターを表示します。
(2)	CoS キューを表示します。

項番	説明
(3)	CoS ごとの受信パケットカウンターを表示します。
(4)	CoS ごとの送信パケットドロップカウンターを表示します。

使用例：受信ポートごとに、CPU に送信されたレイヤー2、レイヤー3 関連の制御パケットのカウンターを表示する方法を示します。

```
# show counters cpu-port detail

cpuRxPkts:          (1)        (2)        (3)        (4)        (5)        (6)        (7)        (8)
                    CoS0       CoS1       CoS2       CoS3       CoS4       CoS5       CoS6       CoS7
          ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
port 1/0/1                 0          0          0          0          0          0          0          0
port 1/0/2                 0          0          0          0          0          0          0          0
port 1/0/3                 0          0          0          0          0          0          0          0
port 1/0/4                 0          0          0          0          0          0          0          0
port 1/0/5                 0          0          0          0          0          0          0          0
port 1/0/6                 0          0          0          0          0          0          0          0
port 1/0/7                 0          0          0          0          0          0          0          0
port 1/0/8                 0          0          0          0          0          0          0          0
port 1/0/9                 0          0          0          0          0          0          0          0
port 1/0/10                0          0          0          0          0          0          0          0
port 1/0/11                0          0          0          0          0          0          0          0
port 1/0/12                0          0          0          0          0          0          0          0
```

項番	説明
(1)	CoS キュー0 の受信パケットカウンターを表示します。
(2)	CoS キュー1 の受信パケットカウンターを表示します。
(3)	CoS キュー2 の受信パケットカウンターを表示します。
(4)	CoS キュー3 の受信パケットカウンターを表示します。
(5)	CoS キュー4 の受信パケットカウンターを表示します。
(6)	CoS キュー5 の受信パケットカウンターを表示します。
(7)	CoS キュー6 の受信パケットカウンターを表示します。
(8)	CoS キュー7 の受信パケットカウンターを表示します。

2.1.15 clear counters

clear counters	
目的	指定したインターフェースのカウンターをクリアします。
Command	clear counters {all | interface IF-ID [,|-] | cpu-port | stack-port}
Parameter	all：すべてのインターフェースのカウンターをクリアする場合に指定します。 interface IF-ID：カウンターをクリアするインターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • mgmt 0：マネージメントポート指定 cpu-port：CPU に送信されたレイヤー2、レイヤー3 関連の制御パケットのカウンターをクリアする場合に指定します。 stack-port：スタックポートのカウンターをクリアする場合に指定します。
モード	特権実行モード
特権レベル	レベル：12

clear counters	
ガイドライン	-
制限・注意	• 本コマンドでインターフェースのカウンターをクリアすると、IF-MIB などのカウンターMIB の値もクリアされます。
バージョン	1.08.02

使用例：ポート 1/0/1 のカウンターをクリアする方法を示します。

```
# clear counters interface port 1/0/1
#
```

2.2 ポート設定コマンド

ポート設定関連の設定コマンドは以下のとおりです。

- speed
- duplex
- mdix
- flowcontrol
- speed_duplex（mgmt 0）
- linkup-delay enable
- linkup-delay timer

ポート設定関連の show コマンドは以下のとおりです。

- show interfaces linkup-delay

2.2.1 speed

speed	
目的	ポートの速度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	speed {10 | 100 | 1000 [master | slave] | 2500 [master | slave] | 10giga | auto [SPEED-LIST] | auto-downgrade} no speed [auto-downgrade]
Parameter	■ RJ-45 ポート(100BASE-TX/1000BASE-T/2.5GBASE-T)の場合 100：通信速度を 100Mbps に設定する場合に指定します。 1000：通信速度を 1000Mbps に設定する場合に指定します。オプションでクロック基準を指定できます。 • master（省略可能）：マスター装置として動作させる場合 • slave（省略可能）：スレーブ装置として動作させる場合 2500：通信速度を 2.5Gbps に設定する場合に指定します。オプションでクロック基準を指定できます。 • master（省略可能）：マスター装置として動作させる場合 • slave（省略可能）：スレーブ装置として動作させる場合 auto：オートネゴシエーションを有効にする場合に指定します。 • SPEED-LIST（省略可能）：オートネゴシエーション有効時にアドバタイズする内容を、以下のパラメーターで指定します。複数指定する場合は「100,1000,2500」のようにコンマで区切ります。このパラメーターを指定しない場合は、すべての速度がアドバタイズされます。 • 100（省略可能）：100Mbps をアドバタイズする場合 • 1000（省略可能）：1000Mbps をアドバタイズする場合 • 2500（省略可能）：2.5Gbps をアドバタイズする場合 ■ RJ-45 ポート(10BASE-T/100BASE-TX/1000BASE-T)の場合 10：通信速度を 10Mbps に設定する場合に指定します。 100：通信速度を 100Mbps に設定する場合に指定します。 1000：通信速度を 1000Mbps に設定する場合に指定します。オプションでクロック

speed	
	基準を指定できます。 • master（省略可能）：マスター装置として動作させる場合 • slave（省略可能）：スレーブ装置として動作させる場合 auto：オートネゴシエーションを有効にする場合に指定します。 • SPEED-LIST（省略可能）：オートネゴシエーション有効時にアドバタイズする内容を、以下のパラメーターで指定します。複数指定する場合は「10,100,1000」のようにコンマで区切ります。このパラメーターを指定しない場合は、すべての速度がアドバタイズされます。 • 10（省略可能）：10Mbps をアドバタイズする場合 • 100（省略可能）：100Mbps をアドバタイズする場合 • 1000（省略可能）：1000Mbps をアドバタイズする場合 auto-downgrade（省略可能）：アドバタイズする速度を自動的にダウングレードする機能を有効にする場合に指定します。 ■ SFP/SFP+ポートの場合 1000：1000BASE-X トランシーバーを使用して、通信速度を 1000Mbps に設定する場合に指定します。 10giga：10GBASE-R トランシーバー使用して、通信速度を 10Gbps に設定する場合に指定します。 auto：トランシーバーの自動認識を有効にする場合に指定します。1Gbps の場合はオートネゴシエーションが有効になります。
デフォルト	RJ-45 ポート（100BASE-TX/1000BASE-T/2.5GBASE-T）：auto 100,1000,2500 （オートネゴシエーション有効, 100/1000Mbps/2.5Gbps） RJ-45 ポート（10BASE-T/100BASE-TX/1000BASE-T）：auto 10,100,1000 （オートネゴシエーション有効, 10/100/1000Mbps） SFP/SFP+ポート：auto （トランシーバー自動認識、1Gbps はオートネゴシエーション有効）
モード	インターフェース設定モード（port, range）
特権レベル	レベル：12
ガイドライン	ポートの速度／デュプレックスモードの設定可能な組み合わせは、別表のポート種別ごとの「使用方法と設定コマンド」を参照してください。 • RJ-45 ポート（100BASE-TX/1000BASE-T/2.5GBASE-T）の使用方法と設定コマンド • RJ-45 ポート（10BASE-T/100BASE-TX/1000BASE-T）の使用方法と設定コマンド • SFP/SFP+ポートの使用方法と設定コマンド オートネゴシエーションを無効にするには、デュプレックスモードおよび速度の両方を固定設定にしてください。どちらか一方が auto 設定の場合は、オートネゴシエーションは有効のままです。 1000BASE-T、2.5GBASE-T は、オートネゴシエーションが有効の場合のみ使用できます。 指定された速度とデュプレックスモードの組み合わせがハードウェアでサポートしていない場合は、エラーメッセージが表示されます。

speed	
	RJ-45 ポートでデュプレックスモードが半二重に設定されている場合は、1000、2500、またはアドバタイズする速度に 1000 や 2500 を含む auto は設定できません。 auto-downgrade は、リンク状態が不安定な場合にアドバタイズする速度を自動的にダウングレードする機能です。auto-downgrade は RJ-45 ポート（10BASE-T/100BASE-TX/1000BASE-T）でのみ設定可能で、オートネゴシエーションが有効な 1000BASE-T ポートでのみ有効です。
制限・注意	• SFP/SFP+ポートで 10GBASE-R のトランシーバーを使用する場合に、ポートの速度を 1000Mbps に設定することは未サポートです。 • SFP/SFP+ポートで 1000BASE-T トランシーバーを使用する場合は、本コマンドの設定を変更せず、デフォルト設定（auto）のまま使用してください。 • 本コマンドの 1000 または 2500 指定で、master または slave オプションを指定して設定する場合は、デュプレックスモードはデフォルト設定（duplex auto）のまま使用してください。 • オートネゴシエーションの有効／無効や、速度およびデュプレックスモードの設定は、隣接装置でも同じ設定にして使用してください。ただし、master または slave オプションでクロック基準を手動で指定して設定する場合は、自装置のポートと対向ポートが同じ役割にならないように設定してください。
バージョン	1.08.02

■ RJ-45 ポート（100BASE-TX/1000BASE-T/2.5GBASE-T）の使用方法と設定コマンド

• ApresiaNP2500-8MT4X-PoE の Port 1/0/1～1/0/8

• ApresiaNP2500-16MT4X-PoE の Port 1/0/1～1/0/8

オートネゴシエーションの有効／無効 ※()内は有効時のアドバタイズ内容	設定コマンド
有効（100M/Half, 100M/Full, 1000M/Full, 2.5G/Full）	speed auto 100,1000,2500（デフォルト） duplex auto（デフォルト）
有効（100M/Half）	speed auto 100 / duplex half
有効（100M/Full）	speed auto 100 / duplex full
有効（1000M/Full）	speed auto 1000 / duplex auto <その他の設定パターン> • speed auto 1000 / duplex full • speed 1000 [master|slave] / duplex auto
有効（2.5G/Full）	speed auto 2500 / duplex auto <その他の設定パターン> • speed auto 2500 / duplex full • speed 2500 [master|slave] / duplex auto
有効（100M/Half, 100M/Full）	speed auto 100 / duplex auto
有効（100M/Half, 100M/Full, 1000M/Full）	speed auto 100,1000 / duplex auto
有効（100M/Half, 100M/Full, 2.5G/Full）	speed auto 100,2500 / duplex auto

オートネゴシエーションの有効／無効 ※()内は有効時のアドバタイズ内容	設定コマンド
有効（100M/Full, 1000M/Full）	speed auto 100,1000 / duplex full
有効（100M/Full, 2.5G/Full）	speed auto 100,2500 / duplex full
有効（1000M/Full, 2.5G/Full）	speed auto 1000,2500 / duplex auto <その他の設定パターン> • speed auto 1000,2500 / duplex full
有効（100M/Full, 1000M/Full, 2.5G/Full）	speed auto 100,1000,2500 / duplex full
オートネゴシエーション無効、 100Mbps/Half 固定	speed 100 / duplex half
オートネゴシエーション無効、 100Mbps/Full 固定	speed 100 / duplex full

■ RJ-45 ポート（10BASE-T/100BASE-TX/1000BASE-T）の使用方法と設定コマンド

• ApresiaNP2500-16MT4X-PoE の Port 1/0/9～1/0/16

オートネゴシエーションの有効／無効 ※()内は有効時のアドバタイズ内容	設定コマンド
有効（10M/Half, 10M/Full, 100M/Half, 100M/Full, 1000M/Full）	speed auto 10,100,1000（デフォルト） duplex auto（デフォルト）
有効（10M/Half）	speed auto 10 / duplex half
有効（10M/Full）	speed auto 10 / duplex full
有効（100M/Half）	speed auto 100 / duplex half
有効（100M/Full）	speed auto 100 / duplex full
有効（1000M/Full）	speed auto 1000 / duplex auto <その他の設定パターン> • speed auto 1000 / duplex full • speed 1000 [master|slave] / duplex auto
有効（10M/Half, 10M/Full）	speed auto 10 / duplex auto <その他の設定パターン> • speed 10 / duplex auto
有効（100M/Half, 100M/Full）	speed auto 100 / duplex auto <その他の設定パターン> • speed 100 / duplex auto
有効（10M/Half, 10M/Full, 100M/Half, 100M/Full）	speed auto 10,100 / duplex auto
有効（10M/Half, 10M/Full, 1000M/Full）	speed auto 10,1000 / duplex auto
有効（100M/Half, 100M/Full, 1000M/Full）	speed auto 100,1000 / duplex auto
有効（10M/Half, 100M/Half）	speed auto 10,100 / duplex half
有効（10M/Full, 100M/Full）	speed auto 10,100 / duplex full

オートネゴシエーションの有効／無効 ※()内は有効時のアドバタイズ内容	設定コマンド
有効（10M/Full, 1000M/Full）	speed auto 10,1000 / duplex full
有効（100M/Full, 1000M/Full）	speed auto 100,1000 / duplex full
有効（10M/Full, 100M/Full, 1000M/Full）	speed auto 10,100,1000 / duplex full
オートネゴシエーション無効、 10Mbps/Half 固定	speed 10 / duplex half
オートネゴシエーション無効、 10Mbps/Full 固定	speed 10 / duplex full
オートネゴシエーション無効、 100Mbps/Half 固定	speed 100 / duplex half
オートネゴシエーション無効、 100Mbps/Full 固定	speed 100 / duplex full

■ SFP/SFP+ポートの使用方法と設定コマンド
• ApresiaNP2500-8MT4X-PoE の Port 1/0/9～1/0/12
• ApresiaNP2500-16MT4X-PoE の Port 1/0/17～1/0/20

使用方法	設定コマンド
10GBASE-R トランシーバーを挿入して 10GBASE-R で使用、 10Gbps/Full 固定	speed auto（デフォルト設定） duplex auto（デフォルト設定） または、 speed 10giga duplex full
1000BASE-X トランシーバーを挿入して 1000BASE-X で使用、 オートネゴシエーション有効（1000M/Full）	speed auto（デフォルト設定） duplex auto（デフォルト設定）
1000BASE-X トランシーバーを挿入して 1000BASE-X で使用、 オートネゴシエーション無効、1000M/Full 固定	speed 1000 duplex full
1000BASE-T トランシーバーを挿入して 1000BASE-T で使用、 オートネゴシエーション有効（1000M/Full）	speed auto（デフォルト設定） duplex auto（デフォルト設定）

2.2.2 duplex

duplex	
目的	ポートのデュプレックスモードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	duplex {full | half | auto} no duplex
Parameter	■ RJ-45 ポート(100BASE-TX/1000BASE-T/2.5GBASE-T)の場合 full：全二重モードに設定する場合に指定します。 half：半二重モードに設定する場合に指定します。半二重モードは 100BASE-TX でのみサポートしています。 auto：オートネゴシエーションを有効にする場合に指定します。

duplex	
	■ RJ-45 ポート(10BASE-T/100BASE-TX/1000BASE-T)の場合 full：全二重モードに設定する場合に指定します。 half：半二重モードに設定する場合に指定します。半二重モードは 10BASE-T/100BASE-TX でのみサポートしています。 auto：オートネゴシエーションを有効にする場合に指定します。 ■ SFP/SFP+ポートの場合 full：全二重モードに設定する場合に指定します。 auto：1Gbps のオートネゴシエーションを有効にする場合に指定します。10Gbps の場合は常に全二重モードです。
デフォルト	RJ-45 ポート、SFP/SFP+ポート：auto
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	ポートの速度／デュプレックスモードの設定可能な組み合わせは、別表のポート種別ごとの「使用方法と設定コマンド」を参照してください。 • RJ-45 ポート(100BASE-TX/1000BASE-T/2.5GBASE-T)の使用方法と設定コマンド • RJ-45 ポート(10BASE-T/100BASE-TX/1000BASE-T)の使用方法と設定コマンド • SFP/SFP+ポートの使用方法と設定コマンド オートネゴシエーションを無効にするには、デュプレックスモードおよび速度の両方を固定設定にしてください。どちらか一方が auto 設定の場合は、オートネゴシエーションは有効のままです。 1000BASE-T、2.5GBASE-T は、オートネゴシエーションが有効の場合のみ使用できます。 指定された速度とデュプレックスモードの組み合わせがハードウェアでサポートしていない場合は、エラーメッセージが表示されます。 RJ-45 ポートで速度が 1000Mbps、2.5Gbps、またはアドバタイズする速度に 1000 や 2500 を含む auto に設定されている場合は、半二重モード(half)には設定できません。 SFP/SFP+ポートでは半二重モード(half)には設定できません。
制限・注意	• SFP/SFP+ポートで 1000BASE-T トランシーバーを使用する場合は、本コマンドの設定を変更せず、デフォルト設定(auto)のまま使用してください。 • オートネゴシエーションの有効／無効や、速度およびデュプレックスモードの設定は、隣接装置でも同じ設定にして使用してください。
バージョン	1.08.02

使用例：ポート 1/0/8 を、100Mbps/Full 固定に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/8
(config-if-port)# speed 100
(config-if-port)# duplex full
(config-if-port)#
```

2.2.3 mdix

mdix	
目的	ポートの MDI/MDI-X を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	**mdix** {**auto** | **normal** | **cross**} **no mdix**
Parameter	auto：Auto MDI/MDI-X モードに設定する場合に指定します。 normal：MDIX 状態を通常のスイッチングハブのポート（MDI-X モード）に設定する場合に指定します。 cross：MDIX 状態を通常のスイッチングハブのポートとは逆（MDI モード）に設定する場合に指定します。
デフォルト	Auto MDI/MDI-X（auto）
モード	インターフェース設定モード(port, range, mgmt)
特権レベル	レベル：12
ガイドライン	UTP ポートでのみ設定できます。
制限・注意	-
バージョン	1.08.02

使用例：マネージメントポートの MDI/MDI-X を、Auto MDI/MDI-X モードに設定する方法を示します。

```
# configure terminal
(config)# interface mgmt 0
(config-if-mgmt)# mdix auto
(config-if-mgmt)#
```

2.2.4 flowcontrol

flowcontrol	
目的	ポートのフロー制御機能を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	**flowcontrol** {**on** | **off**} **no flowcontrol**
Parameter	on：PAUSE フレームの送受信を有効にする場合に指定します。 off：PAUSE フレームの送受信を無効にする場合に指定します。
デフォルト	無効（off）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	装置のソフトウェアでフロー制御機能が設定されます。
制限・注意	• リンクアップした状態で flowcontrol on コマンド、flowcontrol off コマンド、または no flowcontrol コマンドを実行するとリンクダウンが発生します。
バージョン	1.08.02

使用例：ポート 1/0/10 で、フロー制御を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/10
(config-if-port)# flowcontrol on
(config-if-port)#
```

2.2.5 speed_duplex (mgmt 0)

speed_duplex (mgmt 0)	
目的	マネージメントポートの速度とデュプレックスモードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	speed_duplex {10_half | 10_full | 100_half | 100_full | auto} no speed_duplex
Parameter	10_half：10Mbps/Half 固定に設定する場合に指定します。 10_full：10Mbps/Full 固定に設定する場合に指定します。 100_half：100Mbps/Half 固定に設定する場合に指定します。 100_full：100Mbps/Full 固定に設定する場合に指定します。 auto：オートネゴシエーション有効に設定する場合に指定します。
デフォルト	オートネゴシエーション有効 (auto)
モード	インターフェース設定モード(mgmt)
特権レベル	レベル：12
ガイドライン	ApresiaNP2500 シリーズでは、オートネゴシエーションが有効な場合のみ 1000BASE-T をサポートしています。
制限・注意	• オートネゴシエーションの有効／無効や、動作速度およびデュプレックスモードの設定は、隣接装置でも同じ設定にして使用してください。
バージョン	1.08.02

使用例：マネージメントポートを 100Mbps/Full 固定に設定する方法を示します。

```
# configure terminal
(config)# interface mgmt 0
(config-if-mgmt)# speed_duplex 100_full
(config-if-mgmt)#
```

2.2.6 linkup-delay enable

linkup-delay enable	
目的	リンクアップ抑制機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	linkup-delay enable no linkup-delay enable
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	リンクアップ抑制機能は、装置起動時またはポートのリンクダウンを契機に、対象

linkup-delay enable	
	ポートのリンクアップを設定した時間抑制する機能です。 リンクアップ抑制機能を使用する場合は、linkup-delay enable 設定と linkup-delay timer 設定の両方を設定する必要があります。 リンクアップ抑制機能が有効なポートでは、装置起動時またはポートのリンクダウン時に、リンクアップ抑制タイマーが開始されます。リンクアップ抑制タイマーが満了するまでの間は、リンクアップする条件を満たしてもリンクアップは抑制されます。リンクアップ抑制タイマーが満了した後は、リンクアップする条件を満たしているとリンクアップします。 リンクアップ抑制機能が有効でかつリンクアップ状態のポートで shutdown 設定を実施しても、リンクアップ抑制タイマーは開始されません。 リンクアップ抑制中のポートで shutdown 設定を実施すると、リンクアップ抑制タイマーはすぐに満了します。

制限・注意	• リンアップ抑制機能とリンクダウン連携機能は、同一ポートで併用できません。
	
	• 以下のような、ポートがシャットダウン（err-disabled 状態に変更）される機能を設定しているポートでは、リンクアップ抑制機能を併用することは未サポートです。
	  • ポートベースモードのループ検知機能
	  • 単方向リンク検出機能（uld action 設定が shutdown 設定）
	  • ストームコントロール機能（storm-control action 設定が shutdown 設定）
	  • ポートセキュリティー機能（switchport port-security violation 設定が shutdown 設定）
	
	• memory-error fault-action shutdown-all 設定（デフォルト設定は無効）を有効にした装置では、リンクアップ抑制機能を併用することは未サポートです。
	
	• ApresiaNP2500 シリーズでは、装置起動時のリンクアップ抑制タイマーの開始ログと満了ログの時刻差が、実際の設定値よりも約 1～2 秒短い時間で表示されることがあります。

バージョン	1.13.01

使用例：ポート 1/0/1 で、リンクアップ抑制機能を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# linkup-delay enable
(config-if-port)#
```

2.2.7 linkup-delay timer

linkup-delay timer	
目的	リンクアップを抑制する時間（リンクアップ抑制タイマー）を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	linkup-delay timer SECONDS no linkup-delay timer
Parameter	SECONDS：リンクアップ抑制タイマー値を 1～1000 秒の範囲で指定します。
デフォルト	設定なし（no linkup-delay timer）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12

linkup-delay timer	
ガイドライン	リンクアップ抑制機能を使用する場合は、linkup-delay enable 設定と linkup-delay timer 設定の両方を設定する必要があります。 リンクアップ抑制中に本設定を変更すると、変更したタイマー値でリンクアップ抑制タイマーが再度開始されます。その際には、リンクアップ抑制タイマーの満了ログと開始ログが出力されます。
制限・注意	-
バージョン	1.13.01

使用例：ポート 1/0/1 で、リンクアップを抑制する時間（リンクアップ抑制タイマー値）を 120 秒に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# linkup-delay timer 120
(config-if-port)#
```

2.2.8 show interfaces linkup-delay

show interfaces linkup-delay	
目的	リンクアップを抑制する時間（リンクアップ抑制タイマー）の設定を表示します。
Command	show interfaces [port PORTS] linkup-delay
Parameter	port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	• 本コマンドではスタックポートの情報は表示されません。
バージョン	1.13.01

使用例：リンクアップを抑制する時間（リンクアップ抑制タイマー）の設定を表示する方法を示します。

```
# show interfaces linkup-delay

Linkup-delay Time Configuration:
 Time range :    0 - 1,000 (s)
 Default value : 0 (not delay)
(1)                  (2)
Port                 Delay(s)
-------------        --------
Port1/0/1                 120
Port1/0/2                   0
Port1/0/3                   0
Port1/0/4                   0
Port1/0/5                   0
～～省略～～
```

項番	説明
(1)	ポート番号を表示します。
(2)	リンクアップを抑制する時間(秒)を表示します。

2.3 ブザーおよびアラーム LED コマンド

ブザーおよびアラーム LED 関連の設定コマンドは以下のとおりです。

- alarm global enable
- alarm duration
- alarm state enable
- alarm buzzer beep-type

ブザーおよびアラーム LED 関連の show／操作コマンドは以下のとおりです。

- show alarm
- debug alarm test

2.3.1 alarm global enable

alarm global enable	
目的	ブザーおよびアラーム LED のグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	alarm [buzzer | warn-led] global enable no alarm [buzzer | warn-led] global enable
Parameter	buzzer（省略可能）：ブザーの設定をする場合に指定します。 warn-led（省略可能）：アラーム LED の設定をする場合に指定します。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	buzzer および warn-led を指定しない場合は、両方が対象になります。
制限・注意	-
バージョン	1.08.02

使用例：ブザーおよびアラーム LED のグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# alarm global enable
(config)#
```

2.3.2 alarm duration

alarm duration	
目的	ブザーおよびアラーム LED が警告状態(Warning)になった際の、ブザーおよびアラーム LED の動作時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	alarm [buzzer | warn-led] duration {SECONDS | infinite} no alarm [buzzer | warn-led] duration
Parameter	buzzer（省略可能）：ブザーの設定をする場合に指定します。 warn-led（省略可能）：アラーム LED の設定をする場合に指定します。 SECONDS：ブザーおよびアラーム LED の動作時間を、1～60 秒の範囲で指定します。

alarm duration	
	infinite：ループ検知状態またはストーム検知状態が解除されるまで、ブザーおよびアラーム LED を動作したままにする場合に指定します。
デフォルト	60 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	buzzer および warn-led を指定しない場合は、両方が対象になります。 ブザーおよびアラーム LED が動作を開始してから指定した動作時間が経過すると、ループ検知状態またはストーム検知状態が解除されていなくても、ブザーおよびアラーム LED は動作を停止します。
制限・注意	-
バージョン	1.08.02

使用例：ブザーの動作時間を 30 秒に設定する方法を示します。

```
# configure terminal
(config)# alarm buzzer duration 30
(config)#
```

2.3.3 alarm state enable

alarm state enable	
目的	ブザーおよびアラーム LED のインターフェースごとの設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	alarm [buzzer | warn-led] state enable [cause {loop-detection | storm-control | all}] no alarm [buzzer | warn-led] state enable
Parameter	buzzer（省略可能）：ブザーの設定をする場合に指定します。 warn-led（省略可能）：アラーム LED の設定をする場合に指定します。 cause（省略可能）：ブザーおよびアラーム LED で通知する対象の機能を指定します。省略した場合は loop-detection で設定されます。 • loop-detection（省略可能）：ループ検知機能 • storm-control（省略可能）：ストームコントロール機能 • all（省略可能）：ループ検知機能、ストームコントロール機能
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	buzzer および warn-led を指定しない場合は、両方が対象になります。 ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 通知する対象の機能がループ検知機能の場合、ループ検知機能によってループを検知するとブザーおよびアラーム LED が動作します。ループ検知状態は show loop-detection コマンドで確認できます。 通知する対象の機能がストームコントロール機能の場合、ストームコントロール機能

alarm state enable	
	によってストームを検知するとブザーおよびアラーム LED が動作します。ストーム検知状態は show storm-control コマンドで確認できます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 において、通知する対象の機能をループ検知機能で指定して、ブザーのインターフェースごとの設定を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# alarm buzzer state enable cause loop-detection
(config-if-port)#
```

2.3.4 alarm buzzer beep-type

alarm buzzer beep-type	
目的	ブザーの種類を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	alarm buzzer beep-type {default | TYPE-ID} no alarm buzzer beep-type
Parameter	default：ブザーの種類をデフォルトにする場合に指定します。 TYPE-ID：ブザーの種類を以下から指定します。 • 1：2 秒鳴動、8 秒停止を繰り返す • 2：5 秒鳴動、5 秒停止を繰り返す • 3：8 秒鳴動、2 秒停止を繰り返す
デフォルト	default（2 秒鳴動、2 秒停止を繰り返す）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ブザーの種類を 1（2 秒鳴動、8 秒停止を繰り返す）に設定する方法を示します。

```
# configure terminal
(config)# alarm buzzer beep-type 1
(config)#
```

2.3.5 show alarm

show alarm	
目的	ブザーおよびアラーム LED の設定と状態を表示します。
Command	show alarm [buzzer | warn-led] [interface IF-ID [,|-]]
Parameter	buzzer（省略可能）：ブザーの情報を表示する場合に指定します。 warn-led（省略可能）：アラーム LED の情報を表示する場合に指定します。 interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。

show alarm	
	• port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	buzzer および warn-led を指定しない場合は、両方が対象になります。 特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ブザーの設定と状態を表示する方法を示します。

```
# show alarm buzzer

 Alarm Buzzer:
 ----------------------------------------------------------------------
 Global State      : Enabled ...(1)
 Duration          : 60 second(s) ...(2)
 Warning Time Left: 25 second(s) ...(3)
 Current Status    : Warning ...(4)
 (5)               (6)        (7)
 Interface         State      Cause Enabled
 ---------------   --------   --------------
 Port1/0/1         Enabled    Storm Control
 Port1/0/2         Enabled    All
 Port1/0/3         Enabled    Loop Detection
 Port1/0/4         Disabled   -
～～省略～～
 Port1/0/11        Disabled   -
 Port1/0/12        Disabled   -
 Port-channel5     Enabled    Storm Control
 Port-channel7     Disabled   -

 Alarm Events:
 Interface ...(8) Reason ...(9)
 ----------------------------------------------------------------------
 Port1/0/1         Storm(BC)
 Port1/0/2         Loop
```

項番	説明
(1)	グローバル設定モードのブザーの有効(Enabled)／無効(Disabled)を表示します。
(2)	ブザーの鳴動時間を表示します。infinite 設定の場合は infinite と表示されます。
(3)	ブザーが停止するまでの残り時間を表示します。infinite 設定の場合は infinite と表示されます。
(4)	ブザーの状態を表示します。 Inactive：ブザーが無効 Ready：ブザーが有効で、鳴動していない状態 Warning：ブザーが有効で、鳴動している状態
(5)	ポート番号またはポートチャネル番号を表示します。
(6)	ブザーの有効(Enabled)／無効(Disabled)を表示します。

項番	説明
(7)	ブザーで通知する対象の機能を表示します。 All：ループ検知機能、ストームコントロール機能 Loop Detection：ループ検知機能 Storm Control：ストームコントロール機能
(8)	ブザーおよびアラーム LED が動作する原因を検知した、ポート番号またはポートチャネル番号を表示します。
(9)	ブザーおよびアラーム LED が動作している原因を表示します。 Loop：ループ検知 Storm(BC)：ブロードキャストストームを検知 Storm(MC)：マルチキャストストームを検知 Storm(DLF)：未知のユニキャストストームを検知 Storm(BC&MC)：ブロードキャストストームおよびマルチキャストストームを検知 Storm(BC&DLF)：ブロードキャストストームおよび未知のユニキャストストームを検知 Storm(MC&DLF)：マルチキャストストームおよび未知のユニキャストストームを検知 Storm(BC&MC&DLF)：ブロードキャストストーム、マルチキャストストーム、および未知のユニキャストストームを検知 All（Storm Type: ストーム種別）：ループ検知機能が notify-only モードで、ループとストームの両方を検知している場合

使用例：アラーム LED の設定と状態を表示する方法を示します。

```
# show alarm warn-led

 Alarm Warning LEDs:
 ------------------------------------------------------------------
 Global State     : Disabled ...(1)
 Duration         : 60 second(s) ...(2)
 (3)              (4)        (5)              (6)        (7)
 Interface        State      Cause Enabled    Current    Warning
                                              Status     Time Left
 ---------------  ---------  ---------------  ---------  -------------
 Port1/0/1        Enabled    Storm Control    Ready      60 second(s)
 Port1/0/2        Enabled    All              Warning    21 second(s)
 Port1/0/3        Enabled    Loop Detection   Ready      60 second(s)
 Port1/0/4        Disabled   -                Inactive   60 second(s)
～～省略～～
 Port1/0/11       Disabled   -                Inactive   60 second(s)
 Port1/0/12       Disabled   -                Inactive   60 second(s)
 Port-channel5    Enabled    Storm Control    Ready      60 second(s)
 Port-channel7    Disabled   -                Inactive   60 second(s)

 Alarm Events:
 Interface ...(8) Reason ...(9)
 ------------------------------------------------------------------
 Port1/0/1        Storm(BC)
 Port1/0/2        Loop
```

項番	説明
(1)	グローバル設定モードのアラーム LED の有効(Enabled)／無効(Disabled)を表示します。
(2)	アラーム LED の動作時間を表示します。infinite 設定の場合は infinite と表示されます。
(3)	ポート番号またはポートチャネル番号を表示します。

項番	説明
(4)	アラーム LED の有効(Enabled)／無効(Disabled)を表示します。
(5)	アラーム LED で通知する対象の機能を表示します。 All：ループ検知機能、ストームコントロール機能 Loop Detection：ループ検知機能 Storm Control：ストームコントロール機能
(6)	アラーム LED の状態を表示します。 Inactive：アラーム LED が無効 Ready：アラーム LED が有効で、アラーム LED が消灯している状態 Warning：アラーム LED が有効で、アラーム LED が点滅している状態
(7)	アラーム LED が停止するまでの残り時間を表示します。infinite 設定の場合は infinite と表示されます。
(8)	ブザーおよびアラーム LED が動作する原因を検知した、ポート番号またはポートチャネル番号を表示します。
(9)	ブザーおよびアラーム LED が動作している原因を表示します。 Loop：ループ検知 Storm(BC)：ブロードキャストストームを検知 Storm(MC)：マルチキャストストームを検知 Storm(DLF)：未知のユニキャストストームを検知 Storm(BC&MC)：ブロードキャストストームおよびマルチキャストストームを検知 Storm(BC&DLF)：ブロードキャストストームおよび未知のユニキャストストームを検知 Storm(MC&DLF)：マルチキャストストームおよび未知のユニキャストストームを検知 Storm(BC&MC&DLF)：ブロードキャストストーム、マルチキャストストーム、および未知のユニキャストストームを検知 All（Storm Type: ストーム種別）：ループ検知機能が notify-only モードで、ループとストームの両方を検知している場合

2.3.6 debug alarm test

debug alarm test	
目的	テスト目的などで、ブザーおよびアラーム LED を手動でオン／オフします。
Command	debug alarm [buzzer | warn-led [interface IF-ID [,|-]]] test
Parameter	buzzer（省略可能）：ブザーをテストする場合に指定します。 warn-led（省略可能）：アラーム LED をテストする場合に指定します。 interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	ブザーおよびアラーム LED がオフ
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	buzzer および warn-led を指定しない場合は、両方が対象になります。 ブザーが「Ready」または「Inactive」状態のときに本コマンドを実行すると、ブザーが動作します。コマンドをもう一度実行すると、ブザーが停止します。

debug alarm test	
	ブザーが「Warning」状態のときに本コマンドを実行すると、ブザーが停止し、ブザーの状態は「Ready」になります。 ポートのアラーム LED が「Ready」または「Inactive」状態のときに本コマンドを実行すると、アラーム LED が点滅します。コマンドをもう一度実行すると、アラーム LED が消灯します。 ポートのアラーム LED が「Warning」状態のときに本コマンドを実行すると、アラーム LED が消灯し、アラーム LED の状態は「Ready」になります。 特定のインターフェースを指定しない場合は、すべてのインターフェースのアラーム LED がテストされます。
制限・注意	• 手動でオン／オフを切り替えた場合でも、各機能の監視は継続されます。そのため、再びブザーまたはアラーム LED が動作する条件を満たした場合は、各ブザーおよびアラーム LED が動作します。
バージョン	1.08.02

使用例：ブザーを手動でオン／オフする方法を示します。

```
# debug alarm buzzer test
#
```

使用例：ポート 1/0/1 のアラーム LED を手動でオン／オフする方法を示します。

```
# debug alarm warn-led interface port 1/0/1 test
#
```

2.4 省電力イーサネット(EEE)コマンド

省電力イーサネット(EEE)関連の設定コマンドは以下のとおりです。

- eee

省電力イーサネット(EEE)関連の show コマンドは以下のとおりです。

- show eee

2.4.1 eee

eee	
目的	省電力イーサネット(EEE)を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	eee no eee
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	省電力イーサネット(EEE)を有効にすると、物理ポートのリンクが確立していて、送受信されるパケット数が少ない場合に、物理ポートの消費電力を節約できます。物理ポートは、送受信されるパケットがないときに、Low Power Idle（LPI）モードに遷移します。物理ポートに消費電力は、物理ポートの実際の帯域幅使用率によって変わります。
制限・注意	• オートネゴシエーションが無効なポートでは設定できません。
バージョン	1.08.02

使用例：ポート 1/0/1 の省電力イーサネット(EEE)を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# eee
(config-if-port)#
```

2.4.2 show eee

show eee	
目的	省電力イーサネット(EEE)の有効／無効を表示します。
Command	show eee [interface PORTS]
Parameter	interface PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：省電力イーサネット(EEE)の有効／無効を表示する方法を示します。

```
# show eee
(1)             (2)
Port            State
---------       -----------
1/0/1            Disabled
1/0/2            Disabled
1/0/3            Enabled
1/0/4            Enabled
1/0/5            Disabled
1/0/6            Disabled
1/0/7            Disabled
1/0/8            Disabled
1/0/9            -
1/0/10           -
1/0/11           -
1/0/12           -
```

項番	説明
(1)	ポート番号を表示します。
(2)	省電力イーサネットの有効(Enabled)／無効(Disabled)を表示します。省電力イーサネット未対応ポートは "-" と表示されます。

2.5 PoE コマンド

PoE 関連の設定コマンドは以下のとおりです。

- poe power-inline
- poe power-inline never
- poe pd description
- poe pd priority
- poe usage-threshold
- poe fan mode poe-power-priority
- snmp-server enable traps poe
- c-poe enable

PoE 関連の show／操作コマンドは以下のとおりです。

- show poe power module
- show poe power-inline
- clear poe statistic

2.5.1 poe power-inline

poe power-inline	
目的	PoE ポートの電力管理モード、およびタイムレンジを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	poe power-inline auto [max MAX-WATTAGE] [time-range NAME] no poe power-inline [auto {max | time-range}]
Parameter	auto：PD の検出、および電力の供給を自動的に行う場合に指定します。 max MAX-WATTAGE（省略可能）：自動的に検出された PD に供給できる最大電力（ミリワット）を設定する場合に指定します。最大電力を設定しない場合、PD のクラスは自動的に供給可能な最大電力で供給します。設定可能な範囲は 1000～30000 ミリワットです。 time-range NAME（省略可能）：PoE ポートに適用するタイムレンジプロファイル名を指定します。
デフォルト	PD の検出、および電力供給は有効（poe power-inline auto）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	PoE ポートにタイムレンジプロファイルを適用した場合、そのポートではプロファイルに設定されたタイムレンジの開始時刻から終了時刻までの間のみ PoE 給電されます。タイムレンジ範囲外の間は PoE 給電を停止します。 本コマンドにより PD に供給できる最大電力を設定できます。設定された最大電力よりも多くの電力を PD が要求する場合は、PD に電力は供給されません。 poe power-inline auto max MAX-WATTAGE が設定済みの状態で、異なる値を指定して再設定した場合は上書きされます。
制限・注意	• 本コマンドは、PoE 対応ポートでのみ使用できます。 • 総電力量が既存の PD への電力供給要件を満たせない場合、PD への電力供給が切断されることがあります。

poe power-inline	
	• 同一ポートに poe power-inline never が設定されている場合は、no poe power-inline コマンドを実行すると poe power-inline never 設定も削除されます。 • poe power-inline auto max MAX-WATTAGE だけが設定されているポートで poe power-inline auto コマンドを実行しても上書き設定されませんが、同一ポートに poe power-inline never が設定されている状態で poe power-inline auto コマンドを実行すると、最大電力指定のない poe power-inline auto で上書き設定されます。
バージョン	1.08.02 1.10.01：time-range パラメーター追加

使用例：ポート 1/0/1 に接続された PD の検出、および電力の供給を自動的に行う設定にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# poe power-inline auto
(config-if-port)# no poe power-inline never
(config-if-port)#
```

使用例：ポート 1/0/1 に接続された PD に供給する最大電力を 7 ワットに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# poe power-inline auto max 7000
(config-if-port)#
```

使用例：ポート 1/0/1 にタイムレンジプロファイル「weekdays」を適用する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# poe power-inline auto time-range weekdays
(config-if-port)#
```

2.5.2 poe power-inline never

poe power-inline never	
目的	PoE ポートの PD への電力供給を無効にします。有効にする場合は、no 形式のコマンドを使用します。
Command	poe power-inline never no poe power-inline never
Parameter	never：PD への電力供給を無効にする場合に指定します。
デフォルト	PD の検出、および電力供給は有効 (no poe power-inline never)
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 本コマンドは、PoE 対応ポートでのみ使用できます。
バージョン	1.08.02

使用例：ポート 1/0/1 に接続された PD への電力供給を無効に設定にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# poe power-inline never
(config-if-port)#
```

使用例：ポート 1/0/1 の PoE 給電を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# no poe power-inline never
(config-if-port)#
```

2.5.3 poe pd description

poe pd description	
目的	PoE ポートに接続される PD の説明を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	poe pd description STRING no poe pd description
Parameter	STRING：PoE ポートに接続される PD の説明を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、？ を除いた文字を使用可能です。スペースも使用できます。
デフォルト	なし
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 本コマンドは、PoE 対応ポートでのみ使用できます。
バージョン	1.08.02

使用例：ポート 1/0/1 の PD の説明として「For VOIP usage」を設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# poe pd description For VOIP usage
(config-if-port)#
```

2.5.4 poe pd priority

poe pd priority	
目的	PoE ポートの電力供給優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	poe pd priority {critical | high | low} no poe pd priority
Parameter	critical：最も優先度が高いポートにする場合に指定します。 high：2 番目に優先度が高いポートにする場合に指定します。 low：3 番目に優先度が高いポートにする場合に指定します。
デフォルト	low
モード	インターフェース設定モード(port, range)

poe pd priority	
特権レベル	レベル：12
ガイドライン	供給電力が装置の最大電力供給量を超えた場合、優先度の低いポートから電力供給が停止されます。同じ優先度のポート同士では、小さいポート番号のポートが優先されます。 新たに PD を接続すると、「その PD のクラスの最大電力供給量」と「装置が供給できる残りの電力供給量」がいったん比較されます。残りの電力供給量が不足する場合は、新たに接続したポートも含めて、優先度の低いポートから電力供給が停止されます。
制限・注意	• 本コマンドは、PoE 対応ポートでのみ使用できます。
バージョン	1.08.02

使用例：ポート 1/0/1 において、電力供給優先度を最も高い優先度(critical)に設定にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# poe pd priority critical
(config-if-port)#
```

2.5.5 poe usage-threshold

poe usage-threshold	
目的	PoE 機能の SNMP トラップを送信するための電力使用率のしきい値を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	poe [unit UNIT-ID] usage-threshold PERCENTAGE no poe [unit UNIT-ID] usage-threshold
Parameter	unit UNIT-ID：電力使用率のしきい値を設定する装置のボックス ID を 1～4 の範囲で指定します。本パラメーターは、スタック機能が有効になっている場合にのみコマンド文字列として表示されます。 PERCENTAGE：電力使用率のしきい値を 1～99(%)の範囲で指定します。
デフォルト	99%
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	装置全体の電力使用率がしきい値を超過した場合、および下回った場合に以下の SNMP トラップが送信されます。 • 超過した場合：pethMainPowerUsageOnNotification トラップ • 下回った場合：pethMainPowerUsageOffNotification トラップ
制限・注意	• 本コマンドはスタック機能の有効／無効を変更した場合には引き継がれません。スタック機能の状態を変更した後に再設定してください。
バージョン	1.08.02

使用例：ボックス ID 1 の装置において、SNMP トラップを送信するための電力使用率のしきい値を 50%に設定にする方法を示します。

```
# configure terminal
(config)# poe unit 1 usage-threshold 50
(config)#
```

2.5.6 poe fan mode poe-power-priority

poe fan mode poe-power-priority	
目的	ApresiaNP2500-16MT4X-PoE において、最大電力供給量を 300W モードに設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	poe fan mode poe-power-priority [unit UNIT-ID] no poe fan mode poe-power-priority [unit UNIT-ID]
Parameter	unit UNIT-ID（省略可能）：最大電力供給量を 300W モードに変更する装置のボックス ID を 1～4 の範囲で指定します。本パラメーターは、スタック機能が有効になっている場合にのみコマンド文字列として表示されます。
デフォルト	245W モード（no poe fan mode poe-power-priority）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドは ApresiaNP2500-16MT4X-PoE でのみ動作します。 デフォルト設定の 245W モードの場合は、装置全体の最大電力供給量は 245W になり、動作周囲温度仕様は 0～50℃になります。 本コマンドを設定して 300W モードに変更した場合は、装置全体の最大電力供給量は 300W になり、動作周囲温度仕様は 0～45℃になります。
制限・注意	• 本コマンドはスタック機能の有効／無効を変更した場合には引き継がれません。スタック機能の状態を変更した後に再設定してください。
バージョン	1.08.02

使用例：ApresiaNP2500-16MT4X-PoE において、最大電力供給量を 300W モードに設定にする方法を示します。

```
# configure terminal
(config)# poe fan mode poe-power-priority
(config)#
```

2.5.7 snmp-server enable traps poe

snmp-server enable traps poe	
目的	PoE 機能の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps poe no snmp-server enable traps poe
Parameter	なし
デフォルト	有効（snmp-server enable traps poe）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。
制限・注意	-
バージョン	1.08.02

使用例：PoE 機能の SNMP トラップを無効に設定にする方法を示します。

```
# configure terminal
(config)# no snmp-server enable traps poe
(config)#
```

2.5.8 c-poe enable

c-poe enable	
目的	Continuous PoE 機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	c-poe enable no c-poe enable
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	本機能を有効にした場合、CLI や MIB による再起動中は PD への電源供給が継続されます。 reboot コマンドの cold オプション（AEOS-NP2500 Ver. 1.10.01 で追加）を指定して再起動した場合は、Continuous PoE 機能が有効であっても、再起動中は PD への給電が一時的に中断されます。
制限・注意	• 本コマンドは、PoE 対応ポートでのみ使用できます。 • 1 ポートでも有効に設定すると、装置のすべての PoE 対応ポートで Continuous PoE 機能は有効になります。 • 本機能を有効にする場合、装置を再起動する前に設定を保存してください。
バージョン	1.08.02

使用例：ApresiaNP2500-8MT4X-PoE において、ポート 1/0/1～1/0/8 の PoE 対応ポートで Continuous PoE 機能を有効にする方法を示します。

```
# configure terminal
(config)# interface range port 1/0/1-8
(config-if-port-range)# c-poe enable
(config-if-port-range)#
```

2.5.9 show poe power module

show poe power module	
目的	電力モジュールの設定値と実際の値を表示します。
Command	show poe power module [unit UNIT-ID] [detail]
Parameter	unit UNIT-ID（省略可能）：情報を表示する装置のボックス ID を 1～4 の範囲で指定します。本パラメーターは、スタック機能が有効になっている場合にのみコマンド文字列として表示されます。 detail（省略可能）：電力モジュールの詳細情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	スタック構成で特定のボックス ID を指定しない場合は、すべてのスタックメンバー

show poe power module	
	の情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：電力モジュールの設定値と実際の値を表示する方法を示します。

```
# show poe power module
 (1)    (2)             (3)               (4)                    (5)          (6)
Unit   Delivered(W)   Power Budget(W)   Usage-Threshold(%)    Trap State   Fan Mode
----   ------------   ---------------   -------------------   ----------   ----------
1      0              245               99                    Enabled      High Temp
2      0              300               99                    Enabled      PoE Power
```

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は 1 が表示されます。
(2)	実際の合計電力供給量（ワット）を表示します。
(3)	装置の最大電力供給量（ワット）を表示します。
(4)	PoE 機能の SNMP トラップを送信するための電力使用率のしきい値を表示します。
(5)	PoE 機能の SNMP トラップの有効(Enabled)／無効(Disabled)を表示します。
(6)	PoE 機能の FAN モードを表示します。 High Temp：最大電力供給量 245W モード（動作周囲温度仕様 0～50℃） PoE Power：最大電力供給量 300W モード（動作周囲温度仕様 0～45℃）

使用例：ボックス ID 1 の電力モジュールの詳細情報を表示する方法を示します。

```
# show poe power module unit 1 detail
 (1)    (2)             (3)               (4)                    (5)          (6)
Unit   Delivered(W)   Power Budget(W)   Usage-Threshold(%)    Trap State   Fan Mode
----   ------------   ---------------   -------------------   ----------   ----------
1      0              300               99                    Enabled      PoE Power

PoE system parameters:
 (1)    (7)          (8)          (9)
Unit   Max Ports   Device ID   SW Version
----   ---------   ---------   ----------
1      16          E121        3.0.0.B6
```

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は 1 が表示されます。
(2)	実際の合計電力供給量（ワット）を表示します。
(3)	装置の最大電力供給量（ワット）を表示します。
(4)	PoE 機能の SNMP トラップを送信するための電力使用率のしきい値を表示します。
(5)	PoE 機能の SNMP トラップの有効(Enabled)／無効(Disabled)を表示します。
(6)	PoE 機能の FAN モードを表示します。 High Temp：最大電力供給量 245W モード（動作周囲温度仕様 0～50℃） PoE Power：最大電力供給量 300W モード（動作周囲温度仕様 0～45℃）
(7)	PoE を使用可能な最大ポート数を表示します。
(8)	PoE チップのハードウェアバージョンを表示します。

項番	説明
(9)	PoE チップのファームウェアバージョンを表示します。

2.5.10 show poe power-inline

show poe power-inline	
目的	指定したポートの PoE 機能の情報を表示します。
Command	show poe power-inline [port PORTS] {status | configuration | statistics | lldp-classification}
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。 status：PoE 機能の状態を表示する場合に指定します。 configuration：PoE 機能の設定を表示する場合に指定します。 statistics：PoE 機能に関連するエラー統計情報を表示する場合に指定します。 lldp-classification：LLDP（Power via MDI TLV）経由の PoE 情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべての PoE ポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02 1.10.01：configuration パラメーター指定時にタイムレンジプロファイルの表示追加

使用例：PoE 機能の状態を表示する方法を示します。

```
# show poe power-inline status
(1)          (2)         (3)      (4)     (5)      (6)
Interface    State       Class    Max(W)  Used(W)  Description
--------------------------------------------------------------------------------
Port1/0/1    searching   n/a      10.0    0.0
Port1/0/2    searching   n/a      0.0     0.0
Port1/0/3    delivering  class-0  15.4    3.3
Port1/0/4    searching   n/a      0.0     0.0
Port1/0/5    searching   n/a      0.0     0.0
Port1/0/6    searching   n/a      0.0     0.0
Port1/0/7    disabled    n/a      0.0     0.0
Port1/0/8    searching   n/a      0.0     0.0

Faulty code
[1] MPS (Maintain Power Signature) Absent
[2] PD short
[3] Overload
[4] Power Denied
[5] Thermal Shutdown
[6] Startup Failure
[7] Classification Failure
```

項番	説明
(1)	ポート番号を表示します。
(2)	PoE 機能の状態を表示します。 disabled：PoE 機能が無効状態

項番	説明
	searching：PD が接続されていない状態 requesting：PD が接続されているが、電力を供給していない状態 delivering：電力供給状態 faulty[X]：電力供給が失敗している状態。X はエラーコード。 • [1] MPS（Maintain Power Signature）Absent：電力シグネチャの監視不可 • [2] PD short：PD ショート • [3] Overload：過負荷 • [4] Power Denied：電源拒否 • [5] Thermal Shutdown：サーマルシャットダウン • [6] Startup Failure：起動失敗 • [7] Classification Failure：電力クラス分類の失敗（IEEE 802.3at）
(3)	IEEE 規格の電力クラスを表示します。
(4)	ポートの最大電力供給量（ワット）を表示します。
(5)	実際の電力供給量（ワット）を表示します。
(6)	poe pd description コマンドで設定された、PD の説明を表示します。

使用例：PoE 機能の設定を表示する方法を示します。

```
# show poe power-inline configuration
(1)          (2)       (3)        (4)
Interface    Admin     Priority   Time-Range
-----------  -------   --------   ------------------------
Port1/0/1    auto(M)   critical   wlan-ap
Port1/0/2    auto      low
Port1/0/3    auto      low        ip-phone
Port1/0/4    auto      low        ip-phone
Port1/0/5    auto      low        ip-phone
Port1/0/6    auto      low
Port1/0/7    never     low
Port1/0/8    auto      low
```

項番	説明
(1)	ポート番号を表示します。
(2)	PoE 機能の設定を表示します。 auto：PD は自動的に検出され、最大電力供給量は検出結果に基づいて決定 auto(M)：PD は自動的に検出され、最大電力供給量は設定した値 never：PD の検出、および電力供給は無効
(3)	ポートの電力供給優先度を表示します。 critical：最も優先度が高いポート high：2 番目に優先度が高いポート low：3 番目に優先度が高いポート
(4)	適用されているタイムレンジプロファイル名を表示します。

使用例：PoE 機能に関連するエラー統計情報を表示する方法を示します。

```
# show poe power-inline statistics
(1)            (2)          (3)        (4)        (5)            (6)
Interface      MPS Absent   Overload   Short      Power Denied   Invalid Signature
-------------  -----------  --------   --------   ------------   -----------------
```

```
Port1/0/1      0              0              0              0              243
Port1/0/2      0              0              0              0              244
Port1/0/3      0              0              0              76             3
Port1/0/4      0              0              0              0              243
Port1/0/5      0              0              0              0              245
Port1/0/6      0              0              0              0              245
Port1/0/7      0              0              0              0              15
Port1/0/8      0              0              0              0              215
```

項番	説明
(1)	ポート番号を表示します。
(2)	PSE が PD の有効な MPS を監視できず、PSE が電力供給を停止した回数を表示します。
(3)	PD が過度に電力を消費し、ポートが供給できる最大出力電力を超えた回数を表示します。
(4)	PD の内部回路が短絡した回数を表示します。
(5)	PoE 機能が接続された PD への電力供給を拒否した回数を表示します。
(6)	PSE が無効な PD シグネチャを持つ PD を検出した回数を表示します。

使用例：LLDP（Power via MDI TLV）経由の PoE 情報を表示する方法を示します。

```
# show poe power-inline lldp-classification

Interface Port1/0/1 ...(1)
PSE TX information:

  Power type: type 2 PSE ...(2)
  Power source: primary power source ...(3)
  Power priority: low ...(4)
  PD requeseted power value: 25.0W ...(5)
  PSE allocated power value: 25.0W ...(6)

Information from PD:

  Power type: type 2 PD
  Power source: PSE
  Power priority: low
  PD requeseted power value: 25.0W
  PSE allocated power value: 25.0W

Interface Port1/0/2
PSE TX information:

none

Information from PD:
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

項番	説明
(1)	ポート番号を表示します。
(2)	電力のタイプを表示します。
(3)	電力の供給元を表示します。
(4)	ポートの電力供給優先度を表示します。 critical：最も優先度が高いポート high：2 番目に優先度が高いポート low：3 番目に優先度が高いポート

項番	説明
(5)	PD が要求した電力量 (ワット) を表示します。
(6)	PSE が割り当てた電力量 (ワット) を表示します。

2.5.11 clear poe statistic

clear poe statistic	
目的	PoE 機能の統計情報を消去します。
Command	clear poe statistic {all | interface port PORTS}
Parameter	all：すべてのポートの統計情報を消去する場合に指定します。 interface port PORTS：物理ポートを指定します。複数指定できます。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の PoE 機能の統計情報を消去する方法を示します。

```
# clear poe statistic interface port 1/0/1
#
```

2.6 PD モニタリングコマンド

PD モニタリング関連の設定コマンドは以下のとおりです。

- pd-monitoring global state enable
- pd-monitoring period-to-start
- pd-monitoring restart-poe retry
- pd-monitoring auto-recovery time
- pd-monitoring acl-mode
- pd-monitoring acl-mode access-list
- pd-monitoring icmp
- pd-monitoring icmp pd-ip
- pd-monitoring state

PD モニタリング関連の show コマンドは以下のとおりです。

- show pd-monitoring

2.6.1 pd-monitoring global state enable

pd-monitoring global state enable	
目的	PD モニタリングのグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	pd-monitoring global state enable no pd-monitoring global state enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：PD モニタリングを有効にする方法を示します。

```
# configure terminal
(config)# pd-monitoring global state enable
(config)#
```

2.6.2 pd-monitoring period-to-start

pd-monitoring period-to-start	
目的	給電を開始してから、PD 監視開始までの待機時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	pd-monitoring period-to-start MINUTES no pd-monitoring period-to-start
Parameter	MINUTES：PD 監視開始までの待機時間を 1～10 分の範囲で指定します。
デフォルト	3 分

pd-monitoring period-to-start	
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	妥当な設定時間は PD の起動時間によります。例えば、2 分に設定した場合、給電を開始してから 2 分後に PD 監視を開始します。
制限・注意	-
バージョン	1.08.02

使用例：PD の監視開始までの待機時間を 2 分に設定する方法を示します。

```
# configure terminal
(config)# pd-monitoring period-to-start 2
(config)#
```

2.6.3 pd-monitoring restart-poe retry

pd-monitoring restart-poe retry	
目的	PD モニタリングによるリスタートの上限回数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	pd-monitoring restart-poe retry VALUE no pd-monitoring restart-poe retry
Parameter	VALUE：上限回数を 1～3 回の範囲で指定します。
デフォルト	3 回
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	デフォルト設定(3 回)の場合は、PD モニタリングによる PD のリスタート（電力供給を一時的に停止することによる電源 OFF/ON)、PD 監視開始までの待機時間、および PD 監視のサイクルを 3 回繰り返します。 PD モニタリングによる PD のリスタートが上限回数を超過した場合、そのポートの PoE 給電が無効化されます。PoE 給電が無効化されたポートには、自動的に poe power-inline never が設定されます。 自動復旧時間が 0 以外に設定されている場合は、自動復旧時間が経過した後に PoE 給電が再開されて、自動的に poe power-inline never 設定が削除されます。 no poe power-inline never コマンドを使用して、PoE 給電を手動で有効にすることもできます。 本コマンドの設定は、pd-monitoring icmp pd-ip コマンド、または pd-monitoring acl-mode access-list で restart-poe パラメーターを設定した場合のみ有効です。
制限・注意	-
バージョン	1.08.02

使用例：PD モニタリングによるリスタートの上限回数を 2 回に設定する方法を示します。

```
# configure terminal
(config)# pd-monitoring restart-poe retry 2
(config)#
```

2.6.4 pd-monitoring auto-recovery time

pd-monitoring auto-recovery time	
目的	PoE 給電の自動復旧時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	pd-monitoring auto-recovery time MINUTES no pd-monitoring auto-recovery time
Parameter	MINUTES：自動復旧時間を 0～60 分の範囲で指定します。
デフォルト	0 分（自動復旧しない）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	PD モニタリングによる PD のリスタートが上限回数を超過した場合、そのポートの PoE 給電が無効化されます。自動復旧時間を 0 以外に設定すると、設定時間経過後に自動的に PoE 給電が復旧します。 自動復旧時間がデフォルト設定の 0 分の場合、PoE 給電は自動復旧しません。
制限・注意	• 本コマンドは、PoE 対応ポートでのみ使用できます。
バージョン	1.08.02

使用例：ポート 1/0/1 において、PoE 給電の自動復旧時間を 5 分に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# pd-monitoring auto-recovery time 5
(config-if-port)#
```

2.6.5 pd-monitoring acl-mode

pd-monitoring acl-mode	
目的	ACL モードの場合の、トラフィックレートの監視間隔としきい値を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	pd-monitoring acl-mode interval SECONDS threshold pps RATE no pd-monitoring acl-mode [interval | threshold]
Parameter	interval SECONDS：監視間隔を 5～30 秒の範囲で指定します。 threshold pps RATE：下限しきい値を 5～1000 パケット/秒の範囲で指定します。
デフォルト	interval は 10 秒、threshold pps は 100 パケット/秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ACL モードの場合のトラフィックレートの監視間隔を 5 秒、下限しきい値を 800 パケット/秒に設定する方法を示します。

```
# configure terminal
(config)# pd-monitoring acl-mode interval 5 threshold pps 800
(config)#
```

2.6.6 pd-monitoring acl-mode access-list

pd-monitoring acl-mode access-list	
目的	ACL モードで監視するアクセスリスト、およびアクションを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	pd-monitoring acl-mode access-list ACL-NAME action {restart-poe | notify-only} no pd-monitoring acl-mode access-list
Parameter	ACL-NAME：監視するアクセスリストを指定します。 action：アクセスリストに一致するトラフィックのレートが、設定したしきい値を下回った場合に実行するアクションを指定します。 • restart-poe：PD のリスタートを促すために一時的にポートへの電力供給を停止します。ログ出力も行います。 • notify-only：ログ出力のみを行います。
デフォルト	設定なし
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	アクセスリストが PD モニタリングに適用されている場合、このアクセスリストは別のアクセスグループ、および同じインターフェース上の同様のアクセスリストには適用されません。
制限・注意	• 本コマンドは、PoE 対応ポートでのみ使用できます。 • 本コマンドで ARP アクセスリストを指定することは未サポートです。 • 本コマンドで指定されているアクセスリストとマッチ条件が同じアクセスリストを、以下のコマンドで同一インターフェースに設定しないでください。この場合、本コマンドの動作優先度が低いため、PD モニタリングによる監視が動作しません。 • expert access-group コマンド • ip access-group コマンド • ipv6 access-group コマンド • mac access-group コマンド • 未定義のアクセスリストを指定して設定した場合は、WARNING メッセージが表示されます。
バージョン	1.08.02

使用例：ポート 1/0/1 において、ACL モードで監視するアクセスリストを acl2、アクションをログ出力のみに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# pd-monitoring acl-mode access-list acl2 action notify-only
(config-if-port)#
```

2.6.7 pd-monitoring icmp

pd-monitoring icmp	
目的	ICMP モードの場合の、PD 監視間隔、応答タイムアウト時間、および再送信回数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。

pd-monitoring icmp	
Command	**pd-monitoring icmp interval** SECONDS **timeout** MILLISECONDS **count** VALUE **no pd-monitoring icmp** [**interval** | **timeout** | **count**]
Parameter	interval SECONDS：PD 監視間隔を 1～60 秒の範囲で指定します。 timeout MILLISECONDS：応答タイムアウト時間を 500～3000 ミリ秒の範囲で指定します。 count VALUE：再送信回数を 3～10 回の範囲で指定します。
デフォルト	interval は 5 秒、timeout は 1000 ミリ秒、count は 3 回
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ICMP モードの場合の PD 監視間隔を 3 秒、応答タイムアウト時間を 2000 ミリ秒、再送信回数を 5 回に設定する方法を示します。

```
# configure terminal
(config)# pd-monitoring icmp interval 3 timeout 2000 count 5
(config)#
```

2.6.8 pd-monitoring icmp pd-ip

pd-monitoring icmp pd-ip	
目的	ICMP モードで監視する PD の IP アドレス、およびアクションを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	**pd-monitoring icmp pd-ip** IP-ADDRESS **action** {**restart-poe** | **notify-only**} **no pd-monitoring icmp pd-ip**
Parameter	IP-ADDRESS：監視する PD の IP アドレスを指定します。 action：ICMP による PD 監視において、PD からの応答がないと判断された場合に実行するアクションを指定します。 • restart-poe：PD のリスタートを促すために一時的にポートへの電力供給を停止します。ログ出力も行います。 • notify-only：ログ出力のみを行います。
デフォルト	設定なし
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	ICMP モードを使用する場合は、ポートが所属する VLAN に IP アドレスを設定してください。
制限・注意	• 本コマンドは、PoE 対応ポートでのみ使用できます。
バージョン	1.08.02

使用例：ポート 1/0/1 において、ICMP モードで監視する PD の IP アドレスを 192.168.1.1、アクションをログ出力のみに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# pd-monitoring icmp pd-ip 192.168.1.1 action notify-only
(config-if-port)#
```

2.6.9 pd-monitoring state

pd-monitoring state	
目的	PD モニタリングのインターフェースごとの設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	pd-monitoring {icmp | acl-mode} state enable no pd-monitoring state enable
Parameter	icmp：ICMP モードで PD モニタリングを有効にする場合に指定します。 acl-mode：ACL モードで PD モニタリングを有効にする場合に指定します。
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 本コマンドは、PoE 対応ポートでのみ使用できます。
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/2 で、ICMP モードで PD モニタリングを有効にする方法を示します。

```
# configure terminal
(config)# interface range port1/0/1-2
(config-if-port-range)# pd-monitoring icmp state enable
(config-if-port-range)#
```

2.6.10 show pd-monitoring

show pd-monitoring	
目的	PD モニタリングの設定を表示します。
Command	show pd-monitoring [port PORTS]
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、グローバル設定モードの設定を表示します。
制限・注意	-
バージョン	1.08.02

使用例：グローバル設定モードの PD モニタリングの設定を表示する方法を示します。

```
# show pd-monitoring

[Global configuration]
    Global state                    : Disabled ...(1)
    Period-to-start(minutes)        : 3 ...(2)
```

```
    Restart-PoE retry(times)          : 3 ...(3)
    ICMP interval(seconds)            : 5 ...(4)
    ICMP timeout(milliseconds)        : 1000 ...(5)
    ICMP count(times)                 : 3 ...(6)
    ACL interval(sec)                 : 10 ...(7)
    ACL threshold(pps)                : 100 ...(8)
```

項番	説明
(1)	PD モニタリングの有効(Enabled)／無効(Disabled)を表示します。
(2)	給電を開始してから、PD 監視開始までの待機時間 (分) を表示します。
(3)	PD モニタリングによるリスタートの上限回数を表示します。
(4)	ICMP モードの PD 監視間隔 (秒) を表示します。
(5)	ICMP モードの応答タイムアウト時間 (ミリ秒) を表示します。
(6)	ICMP モードの再送信回数を表示します。
(7)	ACL モードのトラフィックレートの監視間隔 (秒) を表示します。
(8)	ACL モードのトラフィックレートのしきい値 (pps) を表示します。

使用例：ポート 1/0/1 の PD モニタリングの設定を表示する方法を示します。

```
# show pd-monitoring port 1/0/1

Port1/0/1 ...(1)
-------------------------------------------
    PoE port status                 : PoE Power supply in progress ...(2)
    Auto-recovery time(min)         : 0 ...(3)
[ICMP mode]
    State                           : Disabled ...(4)
    IP address                      : 0.0.0.0 ...(5)
    Action                          : Restart-PoE ...(6)
[ACL mode]
    State                           : Disabled ...(7)
    access-list                     : Test-Monitor-IP-ACL ...(8)
    Action                          : Restart-PoE ...(9)
```

項番	説明
(1)	ポート番号を表示します。
(2)	PoE ポートの給電状態（PoE Power supply in progress：給電中／PoE Power supply disable：給電停止中）を表示します。
(3)	リスタートの上限回数に達して電源供給を停止している状態からの自動復旧時間 (分) を表示します。自動復旧が無効の場合は「0」と表示されます。
(4)	ICMP モードの有効(Enabled)／無効(Disabled)を表示します。
(5)	ICMP モードの監視 IP アドレスを表示します。
(6)	ICMP モードのアクション設定を表示します。 Restart-PoE：電力供給を一時的に停止してリスタートを促すモード Notify-only：電力供給を停止せずに、ログの出力だけを行うモード
(7)	ACL モードの有効(Enabled)／無効(Disabled)を表示します。
(8)	ACL モードの監視アクセスリストを表示します。
(9)	ACL モードのアクション設定を表示します。 Restart-PoE：電力供給を一時的に停止してリスタートを促すモード

項番	説明
	Notify-only：電力供給を停止せずに、ログの出力だけを行うモード

2.7 スタックコマンド

スタック関連の設定コマンドは以下のとおりです。

- stack bandwidth
- stack renumber
- stack priority
- stack my_box_id
- stack my_box_priority
- stack preempt
- stack stack-port load-balance
- stack port-channel mode partial
- stack version check ignore
- snmp-server enable traps stack

スタック関連の show／操作コマンドは以下のとおりです。

- show stack
- show stack detail
- stack remove

2.7.1 stack bandwidth

stack bandwidth	
目的	スタック機能を有効にし、スタックポートの帯域幅を変更します。無効にする場合は、no stack コマンドを使用します。
Command	stack bandwidth 10G {2-port | 4-port} [chain] no stack
Parameter	10G 2-port：SFP+ポート(10GBASE-R)の 2 ポートをスタックポートとして使用する場合に指定します。 10G 4-port：SFP+ポート(10GBASE-R)の 4 ポートをスタックポートとして使用する場合に指定します。 chain（省略可能）：常にチェーントポロジーでスタックを構成します。
デフォルト	無効
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	スタックを構成する場合は、他のスタックメンバーと接続する前に、本コマンドを設定してスタックを有効にする必要があります。 スタック機能を有効にすると、以下のポートがスタックポート 1、およびスタックポート 2 として動作します。スタックポートは通常のポートとは異なり、スタック専用ポートになります。なお、帯域幅の設定によってスタックポートとして動作するポートは異なります。

装置	帯域幅の設定	スタックポート 1	スタックポート 2
ApresiaNP 2500-8MT4X -PoE	10G 2-port	1/0/11	1/0/12
	10G 4-port	1/0/9, 1/0/10	1/0/11, 1/0/12
	10G 2-port chain	1/0/11, 1/0/12	-

stack bandwidth

	10G 4-port chain	1/0/9, 1/0/10, 1/0/11, 1/0/12	-
ApresiaNP 2500-16MT4X -PoE	10G 2-port	1/0/19	1/0/20
	10G 4-port	1/0/17, 1/0/18	1/0/19, 1/0/20
	10G 2-port chain	1/0/19, 1/0/20	-
	10G 4-port chain	1/0/17, 1/0/18, 1/0/19, 1/0/20	-

スタックポート 1 が複数のポートから構成される場合、スタックポート 1 を構成するすべてのポートは同じスタックメンバーに接続する必要があります。スタックポート 2 も同様です。

本コマンドは、構成情報を保存し、装置を再起動するまで反映されません。本コマンドを設定してスタック機能を有効にした場合、またはデフォルト設定に戻してスタック機能を無効にした場合は、構成情報を保存して装置を再起動してください。

本コマンドが反映されてスタック機能が有効になると、スタックポートに設定した物理ポートはスタック専用ポートになり、通常の物理ポートのような使用はできなくなります。主な違いを以下に示します。

- 構成情報では、スタックポートに設定した物理ポートの interface port 設定は表示されなくなります。
- 物理ポートを指定して設定する各種設定では、スタックポートに設定した物理ポートを指定して実行できなくなります。
- interface コマンドもスタックポートに設定した物理ポートを指定して実行できなくなるため、インターフェース設定モードの各種設定も使用できません。
- show interfaces コマンドなどでも、スタックポートに設定した物理ポートは表示されなくなります。スタックポートの情報は、show stack コマンドを参照してください。

chain パラメーターを指定した場合、スタックポートの状態によらず、常にチェーントポロジーで動作します。このとき、スタックポートのすべてのポートがスタックポート 1 となり、これらのポートはポートチャネルで動作します。

制限・注意

- スタックメンバーのファームウェアのバージョンを同じにしてください。ファームウェアのバージョンが異なるスタックメンバー同士では、スタックを構成できません。
- 本コマンドは、スタック構成に接続されている状態では設定できません。
- ボックス ID が、他のスタックメンバーと競合した場合に使用できるコマンドは以下になります。なお、省略形式では実行できません。
  - login
  - logout
  - reboot
  - enable
  - copy running-config startup-config
  - [no] stack renumber
  - stack my_box_id
  - write memory
- chain パラメーターは、2 つの装置でスタックを構成した場合のみ有効となります。

stack bandwidth	
	3 台以上でスタックを構成する場合は、本パラメーターを指定しないでください。 • スタック機能を利用する際には、リングトポロジー、または chain オプションを使用したチェーントポロジーで構成することを推奨します。 • すべてのスタックポートがリンクダウンした場合、同じ設定の装置がネットワーク内に複数存在することになります。スタックポートのリンクダウンが発生した場合は、速やかにスタックポートを復旧してください。 • スタック構成では、各スタックメンバー装置が個々に MAC アドレスを学習します。そして、その学習した MAC アドレスは CPU を介してスタックメンバー装置間で同期を行います。そのため、スタック構成全体で FDB 同期が完了するまでには、非スタック装置の場合よりも多くの時間を要します。 • スタック構成において、スタックメンバー装置をまたぐポート間でステーションムーブが発生（学習済みの MAC アドレスが登録状態のまま、別のスタックメンバー装置のポートでフレームを受信して再学習）した場合、初回フレーム受信時には再学習されないことがあります。また、FDB 同期の仕組みの制限により、再学習されずに該当 MAC アドレスが MAC アドレステーブルから削除されることがあります。このような場合でも、移動先のポートで再度フレームを受信することで正常に再学習されます。 • プリエンプトモード無効時のスタック構成において、stack preempt コマンド未設定でスタック機能が有効な装置をスタックメンバーに追加する際、その装置を稼働状態でスタック構成に追加すると MAC アドレスの比較によるマスターの選出が行われます。マスターの切り替わりは、追加した装置の MAC アドレスがマスターの MAC アドレスより小さい場合に発生します。マスターの切り替わりを防止するためには、スタックメンバーとして追加する装置の電源を切った状態でスタック構成へ接続し、その後電源を投入してください。
バージョン	1.08.02

使用例：スタックポートの帯域幅を 10G 4-port に設定する方法を示します。

```
# stack bandwidth 10G 4-port

 WARNING: The command does not take effect until the next reboot.
```

2.7.2 stack renumber

stack renumber	
目的	手動でボックス ID を装置に割り当てます。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	stack CURRENT-ID renumber NEW-ID no stack CURRENT-ID renumber
Parameter	CURRENT-ID：ボックス ID を手動で設定する装置の、今のボックス ID を 1～4 の範囲で指定します。 NEW-ID：新たに設定するボックス ID を 1～4 の範囲で指定します。
デフォルト	ボックス ID は自動割り当て（no stack my_box_id） 自動割り当て・手動設定をしていない初期状態ではボックス ID は 1
モード	特権実行モード
特権レベル	レベル：12

stack renumber	
ガイドライン	デフォルトではボックス ID は自動割り当てになっていますが、本コマンドにより手動で明示的にボックス ID を割り当てることができます。同じスタックを構成する他のスタックメンバーとボックス ID が競合しないように注意して設定してください。 本コマンドは、スタック構成のままでもスタックメンバーのボックス ID を変更できます。 本コマンドを実行すると、ボックス ID を変更した対象装置の stack my_box_id 設定が変更されます。変更したボックス ID は、構成情報を保存し、対象装置を再起動するまで反映されません。
制限・注意	-
バージョン	1.08.02

使用例：今のボックス ID が 2 の装置のボックス ID を、3 に変更する方法を示します。

```
# stack 2 renumber 3

 WARNING: The command does not take effect until the next reboot.
```

2.7.3 stack priority

stack priority	
目的	装置の優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	stack CURRENT-ID priority PRIORITY no stack CURRENT-ID priority
Parameter	CURRENT-ID：優先度を設定する装置のボックス ID を 1～4 の範囲で指定します。 PRIORITY：優先度の値を 1～63 の範囲で指定します。
デフォルト	32（stack my_box_priority 32）
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	スタックの優先度は、値が小さいほど優先度が高くなります。また、同じ優先度の場合は MAC アドレスが比較され、MAC アドレスの値が小さい方が優先度が高くなります。 本コマンドは、スタック構成のままでもスタックメンバーの優先度を変更できます。 本コマンドを実行すると、優先度を変更した対象装置の stack my_box_priority 設定が変更されます。 優先度を変更した場合は、次回起動時にも反映されるように構成情報を保存してください。
制限・注意	-
バージョン	1.08.02

使用例：ボックス ID 2 の装置の優先度を、10 に設定する方法を示します。

```
# stack 2 priority 10
#
```

2.7.4 stack my_box_id

stack my_box_id	
目的	手動で自装置のボックス ID を割り当てます。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	stack my_box_id NEW-ID no stack my_box_id
Parameter	NEW-ID：新たに設定するボックス ID を 1～4 の範囲で指定します。
デフォルト	ボックス ID は自動割り当て（no stack my_box_id） 自動割り当て・手動設定をしていない初期状態ではボックス ID は 1
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドは、CURRENT-ID に自装置の今のボックス ID を指定して、stack CURRENT-ID renumber NEW-ID コマンドを実行した場合と同じです。 デフォルトではボックス ID は自動割り当てになっていますが、本コマンドにより手動で明示的に自装置のボックス ID を割り当てることができます。同じスタックを構成する他のスタックメンバーとボックス ID が競合しないように注意して設定してください。 スタック構成で本コマンドを実行した場合は、マスター装置が対象になります。 本コマンドは、構成情報を保存し、装置を再起動するまで反映されません。
制限・注意	-
バージョン	1.08.02

使用例：自装置のボックス ID を 3 に変更する方法を示します。

```
# stack my_box_id 3

 WARNING: The command does not take effect until the next reboot.
```

2.7.5 stack my_box_priority

stack my_box_priority	
目的	自装置の優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	stack my_box_priority PRIORITY no stack my_box_priority
Parameter	PRIORITY：優先度の値を 1～63 の範囲で指定します。
デフォルト	32
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドは、CURRENT-ID に自装置の今のボックス ID を指定して、stack CURRENT-ID priority PRIORITY コマンドを実行した場合と同じです。 スタックの優先度は、値が小さいほど優先度が高くなります。また、同じ優先度の場合は MAC アドレスが比較され、MAC アドレスの値が小さい方が優先度が高くなります。

stack my_box_priority	
	スタック構成で本コマンドを実行した場合は、マスター装置が対象になります。 優先度を変更した場合は、次回起動時にも反映されるように構成情報を保存してください。
制限・注意	-
バージョン	1.08.02

使用例：自装置の優先度を 10 に設定する方法を示します。

```
# stack my_box_priority 10
#
```

2.7.6 stack preempt

stack preempt	
目的	スタックのプリエンプトモードを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	stack preempt no stack preempt
Parameter	なし
デフォルト	無効
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	プリエンプトモードは、「マスター装置がダウンして復旧した際に、マスターを元の装置に切り戻す運用」を行う場合などに有効にします。 プリエンプトモードが無効の場合、マスターの優先度は設定値ではなく 0（最も高い優先度）で動作します。そのため、優先度比較において常に現状のマスターの優先度が最も高くなるため、スタックメンバーの復旧や、新規追加時（スタック構成に接続してから電源 ON）に、マスターの切り替わりが発生するのを抑制できます。 プリエンプトモードが有効の場合、マスターの優先度も設定値で動作します。そのため、以下のような状況でマスターが切り替わります。 • マスター装置(A)がダウンしてマスターが切り替わり、その後装置(A)が復旧した場合に、優先度比較において装置(A)が最も高い優先度と判定されると、マスターが装置(A)に切り替わる。 • スタックメンバーを新規に追加した場合に、優先度比較において新規に追加した装置が最も高い優先度と判定されると、マスターが新規に追加した装置に切り替わる。 本コマンドを実行してプリエンプトモードの設定を変更した場合は、次回起動時にも反映されるように構成情報を保存してください。
制限・注意	• プリエンプトモードでより高い優先度の装置がマスターに切り替わる場合には、ポート閉塞を伴うマスター再選出プロセスが動作するため一定の通信断時間が発生します。 • プリエンプトモードでは、マスターがダウン後に復旧すると、AccessDefender の認証済み端末情報が引き継がれません。その場合は再認証を行ってください。
バージョン	1.08.02

使用例：プリエンプトモードを有効にする方法を示します。

```
# stack preempt
#
```

2.7.7 stack stack-port load-balance

stack stack-port load-balance	
目的	1 つのスタックポートが複数のポートで構成されているポートチャネル構成の場合の、負荷分散アルゴリズムを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	stack stack-port load-balance {src-dst-mac | dst-mac | src-mac | src-dst-ip | dst-ip | src-ip} no stack stack-port load-balance
Parameter	使用する負荷分散アルゴリズムを、以下のパラメーターで指定します。 • src-dst-mac：宛先 MAC アドレスと送信元 MAC アドレスで負荷分散 • dst-mac：宛先 MAC アドレスで負荷分散 • src-mac：送信元 MAC アドレスで負荷分散 • src-dst-ip：送信元 IP アドレスと宛先 IP アドレスで負荷分散 • dst-ip：宛先 IP アドレスで負荷分散 • src-ip：送信元 IP アドレスで負荷分散
デフォルト	設定なし（no stack stack-port load-balance）
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドを設定しないデフォルト設定の場合は、宛先 MAC アドレス、送信元 MAC アドレス、VLAN ID、イーサタイプに基づいて負荷分散されます。その他の場合に関しては「スタックポート（ポートチャネル構成）の負荷分散」を参照してください。 本コマンドは、構成情報を保存し、装置を再起動するまで反映されません。
制限・注意	-
バージョン	1.08.02

■ スタックポート（ポートチャネル構成）の負荷分散

設定	対象	負荷分散の基になる情報
デフォルト	すべて	宛先 MAC アドレス、送信元 MAC アドレス、VLAN ID、イーサタイプ
src-dst-mac	すべて	宛先 MAC アドレス、送信元 MAC アドレス、VLAN ID、イーサタイプ
dst-mac	すべて	宛先 MAC アドレス、VLAN ID、イーサタイプ
src-mac	すべて	送信元 MAC アドレス、VLAN ID、イーサタイプ
src-dst-ip	IP パケット	送信元 IPv4/IPv6 アドレス、宛先 IPv4/IPv6 アドレス
	非 IP パケット	宛先 MAC アドレス、送信元 MAC アドレス、VLAN ID、イーサタイプ
dst-ip	IP パケット	宛先 IPv4/IPv6 アドレス

設定	対象	負荷分散の基になる情報
	非 IP パケット	宛先 MAC アドレス、VLAN ID、イーサタイプ
src-ip	IP パケット	送信元 IPv4/IPv6 アドレス
	非 IP パケット	送信元 MAC アドレス、VLAN ID、イーサタイプ

使用例：1 つのスタックポートが複数のポートで構成されているポートチャネル構成の場合の負荷分散アルゴリズムを、src-ip に設定する方法を示します。

```
# stack stack-port load-balance src-ip

 WARNING: The command does not take effect until the next reboot.
```

2.7.8 stack port-channel mode partial

stack port-channel mode partial	
目的	スタック跨ぎのポートチャネルの負荷分散を、ローカル装置のメンバーポートの中から選択されるように変更します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	stack port-channel mode partial no stack port-channel mode partial
Parameter	なし
デフォルト	無効（スタック跨ぎのポートチャネルにおいて、すべてのメンバーポートの中から分散アルゴリズムに従って出力ポートが選択される）
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドを有効にした場合は、スタック跨ぎのポートチャネルにおいて、入力ポートと同じ装置のメンバーポートの中から分散アルゴリズムに従って出力ポートが選択されるようになります。これにより、ユーザートラフィックによるスタックポートの帯域消費を抑制できます。なお、リンクダウンなどで同じ装置に送信可能なメンバーポートが 1 つも残っていない場合は、別装置のメンバーポートから選択されます。 本コマンドは、構成情報を保存し、装置を再起動するまで反映されません。
制限・注意	• 本コマンドは、2 つの装置でスタックを構成し、かつ stack bandwidth コマンドで chain パラメーターを指定した場合のみ有効となります。 • 本コマンドは、スタック構成に接続されている状態では設定できません。 • スタックを構成する際は、両方の装置で本設定が同一となるようにしてください。本設定が装置間で異なる場合、ポートチャネルを使用した通信が停止することがあります。
バージョン	1.08.02

使用例：スタックを跨いだポートチャネルでの装置跨ぎの負荷分散を無効にする方法を示します。

```
# stack port-channel mode partial

 WARNING: The command does not take effect until the next reboot.
```

2.7.9 stack version check ignore

stack version check ignore	
目的	2 台スタック構成でのファームウェアのアップデート時に、一時的にスタックメンバーのバージョンチェック処理を無視する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	stack version check ignore no stack version check ignore
Parameter	なし
デフォルト	無効（no stack version check ignore）
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	スタックを構成するすべての装置は、同一バージョンのファームウェアである必要があります。そのため、スタック構成でのファームウェアのアップデート時は、通常はスタック構成全体を再起動して、スタックを構成するすべての装置のファームウェアを同時にアップデートする必要があります。 2 台スタック構成でのファームウェアのアップデート時に本コマンドを有効にすると、一時的にスタックメンバーのバージョンチェック処理を無視し、スタックメンバー装置を 1 台づつ再起動してアップデートすることができるようになります。 これにより、主にレイヤー2 利用のスタック構成において、ファームウェアのアップデート作業時のロス時間を少なくすることが期待されます。 本コマンドは 2 台スタック構成の場合にサポートしています。 プリエンプトモードが有効なスタック構成で本コマンドを使用する際は、プリエンプトモードによるマスター切り替わり時のポート閉塞を伴うロスを避けるために、一旦プリエンプトモードを無効に変更してから使用してください。 本コマンドの使用手順例については、以下を参照してください。 • 手順例(1) プリエンプトモード無効、2 台スタック構成(その 1) • 手順例(2) プリエンプトモード無効、2 台スタック構成(その 2) • 手順例(3) プリエンプトモード有効、2 台スタック構成
制限・注意	• 本コマンドはファームウェアのアップデート作業時に一時的に有効（stack version check ignore）にして、アップデート作業が完了したら無効（デフォルト設定）に戻すことを想定しています。そのため、本コマンドを有効設定のまま定常的に運用することは未サポートです。 • 3 台スタック構成、または 4 台スタック構成で本コマンドを使用することは未サポートです。 • 本コマンドを使用するには、ファームウェアのアップデート前とアップデート後の両方のバージョンでサポートされている必要があります。そのため、本コマンドが未実装のバージョン（AEOS-NP2500 Ver. 1.12.01 より前のバージョン）に変更する際は、本コマンドは使用しないでください。
バージョン	1.12.01

■ 手順例(1) プリエンプトモード無効、2 台スタック構成(その 1)

この手順例ではスタックマスターの切り替わりは 1 回ですが、ファームウェアのアップデート前とアップデート後で、マスターの役割になる装置が変更されます。

<手順例の前提条件>
- プリエンプトモード無効。
- 実施前は、装置 1（優先度 10）がスタックマスター、装置 2（優先度 20）がバックアップマスターになっているとする。
- ファームウェアのアップデートにおける事前作業（新ファームウェアのダウンロード、boot image コマンドによる次回起動時のブートイメージファイルの設定など）は完了済みとする。

（1）ファームウェアのアップデート前の状態を確認する。

装置 1	装置 2
マスター	バックアップ

（2）stack version check ignore コマンドで、一時的にスタックメンバーのバージョンチェック処理を無視するように変更する。その後、設定を保存して、show stack コマンドで確認する。

```
# stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

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

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Disabled      ※スタックメンバーのバージョンチェック処理を無視
～～省略～～
```

（3）バックアップマスター（装置 2）を再起動、もしくは電源 OFF/ON して、新ファームウェアにアップデートする。装置 2 が起動してスタック構成に取り込まれるのを待つ。

装置 1	装置 2
マスター	バックアップ → バックアップ

（4）スタックマスター（装置 1）を再起動、もしくは電源 OFF/ON して、新ファームウェアにアップデートする。装置 1 が起動してスタック構成に取り込まれるのを待つ。この手順時にはスタックマスターの切り替わりが発生する。

装置 1	装置 2
マスター → バックアップ	バックアップ → マスター

（5）no stack version check ignore コマンドで、スタックメンバーのバージョンチェック処理を有効に戻す。その後、設定を保存して、show stack コマンドで確認する。

```
# no stack version check ignore
#
# write memory
```

```
Destination filename startup-config? [y/n]:  y

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

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Enabled      ※スタックメンバーのバージョンチェック処理は有効
～～省略～～
```

■ 手順例(2) プリエンプトモード無効、2 台スタック構成(その 2)

この手順例ではスタックマスターの切り替わりは 2 回ですが、ファームウェアのアップデート前とアップデート後で、同じ装置がマスターになります。

<手順例の前提条件>

- プリエンプトモード無効。
- 実施前は、装置 1 (優先度 10) がスタックマスター、装置 2 (優先度 20) がバックアップマスターになっているとする。
- ファームウェアのアップデートにおける事前作業 (新ファームウェアのダウンロード、boot image コマンドによる次回起動時のブートイメージファイルの設定など) は完了済みとする。

(1) ファームウェアのアップデート前の状態を確認する。

装置 1	装置 2
マスター	バックアップ

(2) stack version check ignore コマンドで、一時的にスタックメンバーのバージョンチェック処理を無視するように変更する。その後、設定を保存して、show stack コマンドで確認する。

```
# stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

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

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Disabled     ※スタックメンバーのバージョンチェック処理を無視
～～省略～～
```

(3) スタックマスター（装置 1）を再起動、もしくは電源 OFF/ON して、新ファームウェアにアップデートする。装置 1 が起動してスタック構成に取り込まれるのを待つ。この手順時にはスタックマスターの切り替わりが発生する。

装置 1	装置 2
マスター → バックアップ	バックアップ → マスター

(4) スタックマスター（装置 2）を再起動、もしくは電源 OFF/ON して、新ファームウェアにアップデートする。装置 2 が起動してスタック構成に取り込まれるのを待つ。この手順時にはスタックマスターの切り替わりが発生する。

装置 1	装置 2
バックアップ → マスター	マスター → バックアップ

(5) no stack version check ignore コマンドで、スタックメンバーのバージョンチェック処理を有効に戻す。その後、設定を保存して、show stack コマンドで確認する。

```
# no stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

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

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Enabled      ※スタックメンバーのバージョンチェック処理は有効
～～省略～～
```

■ 手順例(3) プリエンプトモード有効、2 台スタック構成

この手順例ではスタックマスターの切り替わりは 2 回ですが、ファームウェアのアップデート前とアップデート後で、同じ装置がマスターになります。また、プリエンプトモードによるマスター切り替わり時のポート閉塞を伴うロスを避けるために、アップデート前に一時的にプリエンプトモードを無効に変更し、アップデート後にプリエンプトモードを有効に戻します。

<手順例の前提条件>

- プリエンプトモード有効。
- 実施前は、装置 1 (優先度 10) がスタックマスター、装置 2 (優先度 20) がバックアップマスターになっているとする。
- ファームウェアのアップデートにおける事前作業 (新ファームウェアのダウンロード、boot image コマンドによる次回起動時のブートイメージファイルの設定など) は完了済みとする。

(1) ファームウェアのアップデート前の状態を確認する。

装置 1	装置 2
マスター	バックアップ

(2) no stack preempt コマンドで、一時的にプリエンプトモードを無効に変更する。stack version check ignore コマンドで、一時的にスタックメンバーのバージョンチェック処理を無視するように変更する。その後、設定を保存して、show stack コマンドで確認する。

```
# no stack preempt
#
# stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

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

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled      ※プリエンプトモード無効
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Disabled      ※スタックメンバーのバージョンチェック処理を無視
～～省略～～
```

(3) スタックマスター（装置 1）を再起動、もしくは電源 OFF/ON して、新ファームウェアにアップデートする。装置 1 が起動してスタック構成に取り込まれるのを待つ。この手順時にはスタックマスターの切り替わりが発生する。

装置 1	装置 2
マスター → バックアップ	バックアップ → マスター

(4) スタックマスター（装置 2）を再起動、もしくは電源 OFF/ON して、新ファームウェアにアップデートする。装置 2 が起動してスタック構成に取り込まれるのを待つ。この手順時にはスタックマスターの切り替わりが発生する。

装置 1	装置 2
バックアップ → マスター	マスター → バックアップ

(5) stack preempt コマンドで、プリエンプトモードを有効に戻す。no stack version check ignore コマンドで、スタックメンバーのバージョンチェック処理を有効に戻す。その後、設定を保存して、show stack コマンドで確認する。

```
# stack preempt
#
# no stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

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

#
# show stack

Stacking Mode        : Enabled
```

```
Stack Preempt        : Enabled      ※プリエンプトモード有効
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Enabled      ※スタックメンバーのバージョンチェック処理は有効
～～省略～～
```

2.7.10 snmp-server enable traps stack

snmp-server enable traps stack	
目的	スタック機能の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps stack no snmp-server enable traps stack
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。
制限・注意	-
バージョン	1.08.02

使用例：スタック機能の SNMP トラップを有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps stack
(config)#
```

2.7.11 show stack

show stack	
目的	スタック情報を表示します。
Command	show stack
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	マスターに障害が発生した場合、バックアップマスターがマスターになりますがスタックの MAC アドレスは変更されません。スタックのマスターから引き継いだ MAC アドレスを確認するには、show version コマンドを使用してください。
制限・注意	• Unit Status 項目は AEOS-NP2500 Ver. 1.12.01 以降で表示されます。それより前のバージョンでは表示されません。
バージョン	1.08.02 1.12.01：表示項目の仕様変更

使用例：スタック情報を表示する方法を示します。

```
# show stack
```

```
Stacking Mode       : Enabled ...(1)
Stack Preempt       : Disabled ...(2)
Trap State          : Disabled ...(3)
Port-channel mode   : All ...(4)
Stack-port load-balance: default ...(5)
Version check       : Enabled ...(6)

Topology            : Duplex_Ring ...(7)
My Box ID           : 1 ...(8)
Master ID           : 1 ...(9)
BK Master ID        : 2 ...(10)
Box Count           : 2 ...(11)
(12) (13)  (14)                        (15)   (16)   (17)               (18)       (19)       (20)
Box User Module                              Prio-                      Prom       Runtime    H/W
ID  Set  Name                        Exist  rity  MAC                  Version    Version    Version
--- ---- ------------------------- ------ ----- ------------------ --------- --------- -------
1   User ApresiaNP2500-8MT4X-PoE  Exist 0     FC-6D-D1-F2-82-1F 1.00.00   1.12.01   A
2   User ApresiaNP2500-8MT4X-PoE  Exist 20    FC-6D-D1-F2-81-F8 1.00.00   1.12.01   A
3   -    NOT_EXIST                No
4   -    NOT_EXIST                No

 Stack Bandwidth and Unit Status:
 (12)    (21)         (22)           (23)           (24)
 Box     User Set     SIO1 Active    SIO2 Active    Unit
 ID      Bandwidth    Bandwidth      Bandwidth      Status
 ----    ---------    ---------      ---------      ---------
 1       2-port(10G)  1-port         1-port         Stable
 2       2-port(10G)  1-port         1-port         Stable
 3
 4
```

項番	説明
(1)	スタックの有効(Enabled)／無効(Disabled)を表示します。
(2)	プリエンプトモードの有効(Enabled)／無効(Disabled)を表示します。
(3)	トラップの有効(Enabled)／無効(Disabled)を表示します。
(4)	ポートチャネルモードを表示します。 All：スタック跨ぎのポートチャネルにおいて、装置跨ぎの負荷分散が有効 Partial：スタック跨ぎのポートチャネルにおいて、装置跨ぎの負荷分散が無効
(5)	スタックポートの負荷分散アルゴリズムを表示します。
(6)	スタックメンバーのバージョンチェック処理の設定を表示します。 Enabled：バージョンチェック処理は有効（デフォルト設定） Disabled：バージョンチェック処理を無視する設定時（stack version check ignore）
(7)	スタックトポロジーを表示します。 Duplex_Chain：チェーントポロジー Duplex_Ring：リングトポロジー
(8)	装置のボックス ID を表示します。
(9)	マスターのボックス ID を表示します。
(10)	バックアップマスターのボックス ID を表示します。
(11)	スタックを構成している装置の数を表示します。
(12)	ボックス ID を表示します。
(13)	ボックス ID の設定状況を表示します。 Auto：自動割り当て User：手動割り当て

項番	説明
(14)	装置の名称を表示します。
(15)	スタック構成の中に存在しているかどうかを表示します。
(16)	優先度を表示します。
(17)	スタックメンバーの MAC アドレスを表示します。
(18)	ブートローダーバージョンを表示します。
(19)	ファームウェアバージョンを表示します。
(20)	ハードウェアリビジョンを表示します。
(21)	スタックポート構成を表示します。 4-port(10G)：stack bandwidth 10G 4-port 設定時 2-port(10G)：stack bandwidth 10G 2-port 設定時
(22)	スタックポート 1 の状態を表示します。 4-port：スタックポート 1 の 4 ポートがリンクアップ状態 (4-port chain 設定時) 3-port：スタックポート 1 の 3 ポートがリンクアップ状態 (4-port chain 設定時) 2-port：スタックポート 1 の 2 ポートがリンクアップ状態 1-port：スタックポート 1 の 1 ポートがリンクアップ状態 Down：スタックポート 1 の全ポートがリンクダウン状態
(23)	スタックポート 2 の状態を表示します。 2-port：スタックポート 2 の 2 ポートがリンクアップ状態 1-port：スタックポート 2 の 1 ポートがリンクアップ状態 Down：スタックポート 2 の全ポートがリンクダウン状態 -：chain オプションが有効なスタック構成の場合
(24)	装置の状態を表示します。 Stable：安定状態 *Unstable：不安定状態

2.7.12 show stack detail

show stack detail	
目的	スタックポートの情報を表示します。
Command	show stack detail
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.12.01

使用例：スタックポートの情報を表示する方法を示します。

```
# show stack detail

Unit 1, Stack Port 11 link status is up ...(1)
 Type: H-SFP+AOC1M ...(2)
 Vendor PN: FCBG110SD1C01 ...(3)
```

```
 Vendor SN: WZ90FLU ...(4)

Unit 1, Stack Port 12 link status is up
 Type: H-SFP+AOC1M
 Vendor PN: FCBG110SD1C01
 Vendor SN: WZ90FP6

Unit 2, Stack Port 11 link status is up
 Type: H-SFP+AOC1M
 Vendor PN: FCBG110SD1C01
 Vendor SN: WZ90FP6

Unit 2, Stack Port 12 link status is up
 Type: H-SFP+AOC1M
 Vendor PN: FCBG110SD1C01
 Vendor SN: WZ90FLU
```

項番	説明
(1)	ボックス ID、スタックポートのポート番号、リンク状態 (up／down) を表示します。
(2)	挿入されているトランシーバーの種類を表示します。
(3)	型式番号を表示します。
(4)	シリアル番号を表示します。

2.7.13 stack remove

stack remove	
目的	存在しないスタックメンバーの情報を削除します。
Command	stack remove UNIT-ID
Parameter	UNIT-ID：情報を削除する装置のボックス ID を 1～4 の範囲で指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドを実行することで、show stack コマンドで表示されるスタック情報、および構成情報（running-config）から、指定されたボックス ID の装置に関する情報が削除されます。 本コマンドを実行して存在しないスタックメンバーの情報を削除した場合は、次回起動時にも反映されるように構成情報を保存してください。
制限・注意	• 指定したボックス ID の装置が存在する場合は実行できません。
バージョン	1.08.02

使用例：ボックス ID 3 の装置の情報を削除する方法を示します。

```
# stack remove 3
#
```

3 基礎知識

3.1 基本 CLI コマンド

基本 CLI 関連のコマンドは以下のとおりです。

- help
- enable
- disable
- login（EXEC）
- logout
- configure terminal
- exit
- end

装置の基本的な状態を確認するための show／操作コマンドは以下のとおりです。

- show version
- show environment
- show unit
- show cpu utilization
- clear cpu utilization history
- show history

3.1.1 help

help	
目的	ヘルプシステムの簡単な説明を表示します。
Command	help
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のコマンドラインで使用できるすべてのコマンドをリスト表示する場合、システムプロンプトでクエスチョンマーク(?)を入力します。 特定の文字列で始まるコマンドのリストを表示する場合、コマンドの一部を入力した後にクエスチョンマーク(?)を入力します。入力した文字列で始まるパラメーター、または引数がリスト表示されます。ワードヘルプと呼ばれる機能です。 コマンドのパラメーターと引数のリストを表示する場合、コマンドラインで、パラメーターまたは引数の代わりにクエスチョンマーク(?)を入力します。すでに入力したコマンド、パラメーター、および引数に基づいて、該当するパラメーターや引数がリスト表示されます。コマンドシンタックスヘルプと呼ばれる機能です。 本コマンドは、任意のコマンドモードで使用できます。
制限・注意	-
バージョン	1.08.02

使用例：help コマンドを使用して、ヘルプシステムの簡単な説明を表示する方法を示します。

```
# help

The switch CLI provides advanced help feature.
1. Help is available when you are ready to enter a command
   argument (e.g. 'show ?') and want to know each possible
   available options.
2. Help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input(e.g. 'show ve?'.).
   If nothing matches, the help list will be empty and you must backup
   until entering a '?' shows the available options.
3. For completing a partial command name could enter the abbreviated
   command name immediately followed by a <Tab> key.

Note:
Since the character '?' is used for help purpose, to enter
the character '?' in a string argument, press ctrl+v immediately
followed by the character '?'.
```

使用例：ワードヘルプを使用して、"re"で始まるすべての特権実行モードコマンドを表示する方法を示します。クエスチョンマーク(?)の前に入力した文字は、ユーザーがコマンドの入力を続行できるように、次のコマンドラインに再表示されます。

```
# re?
reboot              rename              reset               restore

# re
```

使用例：コマンドシンタックスヘルプを使用して、部分的に入力した ip access-list の次の引数を表示する方法を示します。クエスチョンマーク(?)の前に入力された文字は、ユーザーがコマンドの入力を続行できるように、次のコマンドラインに再表示されます。

```
# configure terminal
(config)# ip access-list ?
extended                  Extended Access List
WORD                      Access-list name (the first character must be a letter)

(config)# ip access-list
```

3.1.2 enable

enable	
目的	特権実行モードに遷移します。主に遷移する特権レベルを指定しない形式で実行して、特権実行モード（レベル 15）に遷移するコマンドとして使用します。
Command	enable [PRIVILEGE-LEVEL]
Parameter	PRIVILEGE-LEVEL（省略可能）：遷移する特権レベルを 1～15 の範囲で指定します。指定しない場合はレベル 15 指定になります。
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	ユーザー実行モード（レベル 1）では、プロンプト末尾は > で表示されます。 特権実行モード（レベル 2～15）では、プロンプト末尾は # で表示されます。 本コマンド実行時にパスワードが必要な場合は、enable パスワードの入力を促す「Password:」プロンプトが表示されます。パスワードの入力に 3 回失敗すると、コマンド実行失敗と判断されて通常のプロンプトに戻ります。

enable	
制限・注意	-
バージョン	1.08.02

使用例：ユーザー実行モード（レベル 1）から特権実行モード（レベル 15）に遷移する方法を示します。

```
> show privilege

Current privilege level is 1

> enable

Password:********
#
# show privilege

Current privilege level is 15
```

3.1.3 disable

disable	
目的	現在の特権レベルより低い特権レベルに遷移します。主に遷移する特権レベルを指定しない形式で実行して、ユーザー実行モード（レベル 1）に遷移するコマンドとして使用します。
Command	disable [PRIVILEGE-LEVEL]
Parameter	PRIVILEGE-LEVEL（省略可能）：遷移する特権レベルを 1～15 の範囲で指定します。指定しない場合はレベル 1 指定になります。
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	ユーザー実行モード（レベル 1）では、プロンプト末尾は > で表示されます。 特権実行モード（レベル 2～15）では、プロンプト末尾は # で表示されます。 現在の特権レベルより低い特権レベルに遷移する場合は、enable パスワードの入力は不要です。
制限・注意	-
バージョン	1.08.02

使用例：特権実行モード（レベル 15）からユーザー実行モード（レベル 1）に遷移する方法を示します。

```
# show privilege

Current privilege level is 15

# disable
>
> show privilege

Current privilege level is 1
```

3.1.4 login (EXEC)

login (EXEC)	
目的	CLI でログイン処理を実施します。

login (EXEC)	
Command	login
Parameter	なし
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	CLI で login コマンドを実行すると、ログイン処理が実施され、別のユーザーアカウントでログインしなおすことができます。
制限・注意	-
バージョン	1.08.02

使用例：ユーザー名「user1」でログインする方法を示します。

```
# login
Username:user1
Password:******
```

3.1.5 logout

logout	
目的	装置からログアウトして、アクティブな端末セッションを閉じます。
Command	logout
Parameter	なし
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ログアウトする方法を示します。

```
# logout
```

3.1.6 configure terminal

configure terminal	
目的	グローバル設定モードに遷移します。
Command	configure terminal
Parameter	なし
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	グローバル設定モードでは、プロンプト末尾は (config)# で表示されます。-
制限・注意	• 装置に複数セッションでログインしている状態で、複数セッションから同時に設定を変更しないでください。 • そのため、複数セッションでログインしている状態では、グローバル設定モードに遷移するのは 1 つのセッションだけにしてください。

configure terminal	
バージョン	1.08.02

使用例：グローバル設定モードに遷移する方法を示します。

```
# configure terminal
(config)#
```

3.1.7 exit

exit	
目的	任意の設定モードから 1 つ前の設定モードに戻ります。
Command	exit
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	現在のモードがユーザー実行モード、または特権実行モードの場合、現在のセッションからログアウトします。
制限・注意	-
バージョン	1.08.02

使用例：インターフェース設定モード(port)からグローバル設定モードに戻る方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# exit
(config)#
```

3.1.8 end

end	
目的	現在の設定モードを終了して特権実行モードに戻ります。
Command	end
Parameter	なし
モード	任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：インターフェース設定モード(port)を終了して、特権実行モードに戻る方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# end
#
```

3.1.9 show version

show version	
目的	装置のソフトウェアバージョン情報を表示します。
Command	show version
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：装置のバージョン情報を表示する方法を示します。

```
# show version

System MAC Address: FC-6D-D1-F2-82-1F ...(1)
(2)          (3)                              (4)
Unit ID     Module Name                      Versions
-------  ---------------------------  ---------------------
   1       ApresiaNP2500-8MT4X-PoE       H/W:A
                                         Bootloader:1.00.00
                                         Runtime:1.08.02
                                         CPLD:08
```

項番	説明
(1)	システム MAC アドレスを表示します。 非スタック装置の場合は、自装置の MAC アドレスを表示します。 スタック構成の場合は、「そのスタック構成が最初に起動したときのマスター装置の MAC アドレス」を表示します。
(2)	装置のボックス ID を表示します。スタックを構成していない場合は 1 が表示されます。
(3)	装置名を表示します。
(4)	バージョン情報を表示します。

3.1.10 show environment

show environment	
目的	ファン、メモリー、温度、電源の可用性、装置の状態の情報、および ZTP スイッチの OFF/ON 状態を表示します。
Command	show environment [fan | memory | power | temperature | health | slide-switch]
Parameter	fan（省略可能）：装置のファンの状態を表示する場合に指定します。 memory（省略可能）：装置の SW-LSI メモリーの状態を表示する場合に指定します。 power（省略可能）：装置の電源の状態を表示する場合に指定します。 temperature（省略可能）：装置の温度の状態を表示する場合に指定します。 health（省略可能）：装置の正常性を表示する場合に指定します。

show environment	
	slide-switch（省略可能）：ZTP スイッチの状態を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	パラメーターを指定しない場合は、すべてのパラメーターが対象になります。
制限・注意	-
バージョン	1.08.02

使用例：単体装置の状態を表示する方法を示します。

```
# show environment

Detail Temperature Status:
(1)      (2)          (3)
Unit     Status       Current Temperature
-----    ---------    --------------------
1        Normal       26C

Detail Fan Status: ...(4)
------------------------------------------------------------------
Unit 1:
  Back Fan  1 (OK)      Back Fan  2 (OK)      Back Fan  3 (OK)

Detail Power Status:
(1)      (5)                 (6)
Unit     Power Module        Power Status
-----    ----------------    -------------
1        Power 1             in-operation

Detail Memory-Error Auto-Recovery Status:
------------------------------------------------------------------
Auto Recovery Mode          : Enabled ...(7)
Auto Recovery Notification : Enabled ...(8)
Fault Action Configuration : - ...(9)
(1)      (10)         (11)                (12)
Unit     Status       Recovery Count      ECC Uncorrectable Error Count
-----    ---------    ---------------     -----------------------------
1        Normal       0                   0

Health Status:
(1)      (13)         (14)
Unit     Status       Failure Code
-----    ---------    --------------------
1        Normal       0x00000

Slide Switch Status:
(1)      (15)
Unit     Status
-----    ---------
1        Off
```

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は 1 が表示されます。
(2)	装置の温度状態を表示します。 Normal：装置の温度が正常範囲 Abnormal：装置の温度が正常範囲外

項番	説明
(3)	現在の温度を表示します。
(4)	ファンの状態を表示します。 OK：正常状態 Fault：異常あり
(5)	電源ユニットを表示します。
(6)	電源の状態を表示します。 in-operation：通常動作中 failed：異常あり
(7)	メモリーエラー自動復旧機能の有効(Enabled)／無効(Disabled)を表示します。
(8)	メモリーエラー自動復旧機能に関連する通知（ログ, SNMP トラップ）の有効(Enabled)／無効(Disabled)を表示します。
(9)	SW-LSI メモリーの状態が「異常」になった場合に、すべてのポートをシャットダウンする機能の有効(Shutdown-all)／無効(-)を表示します。
(10)	SW-LSI メモリーの状態を表示します。 Normal：正常 Abnormal：メモリーエラー発生状態（メモリーエラー自動復旧機能無効：メモリーエラーの発生を検知、メモリーエラー自動復旧機能有効：メモリーエラーの多発を検知）
(11)	メモリーエラーが検出されたときに、実行された復旧アクションの回数を表示します。
(12)	復旧不能なメモリーエラーが検出された回数を表示します。
(13)	装置の正常性を表示します。 Normal：正常 Abnormal：1 つ以上のコンポーネントでエラーを検出
(14)	装置によって検出された障害コードを表示します。 すべての bit=0 (0x00000)：正常状態 bit[8]=1 (0x00100)：電源の障害 bit[10]=1 (0x00400)：ファンの障害 bit[11]=1 (0x00800)：温度異常 bit[14]=1 (0x04000)：SW-LSI のメモリーエラー bit[15]=1 (0x08000)：SW-LSI の復旧不能なメモリーエラー bit[16]=1 (0x10000)：SW-LSI のメモリーエラー（ハードエラー） bit[17]=1 (0x20000)：SW-LSI の復旧不能なメモリーエラー（ハードエラー） ※メモリーエラー自動復旧機能が無効で、「復旧可能なメモリーエラーを検出した場合」は、bit[14]=1 (0x04000)を表示します。 ※メモリーエラー自動復旧機能が無効で、「復旧不能なメモリーエラーを検出した場合」は、bit[15]=1 (0x08000)を表示します。 ※メモリーエラー自動復旧機能が有効で、「SW-LSI の同じメモリー領域で、メモリーエラーの検出および復旧アクションが 10 回以上動作して、監視対象外になった場合」は、bit[16]=1 (0x10000)を表示します。 ※メモリーエラー自動復旧機能が有効で、「復旧不能なメモリーエラーを検出した場合」は、bit[17]=1 (0x20000)を表示します。
(15)	ZTP スイッチの状態を表示します。 On：ZTP スイッチが ON 状態

項番	説明
	Off：ZTP スイッチが OFF 状態

使用例：スタックを構成する装置の状態を表示する方法を示します。

```
# show environment

Detail Temperature Status:
(1)      (2)          (3)
Unit     Status       Current Temperature
-----    ---------    --------------------
1        Normal       28C
2        Normal       26C

Detail Fan Status: ...(4)
------------------------------------------------------------
Unit 1:
  Back Fan  1 (OK)      Back Fan  2 (OK)      Back Fan  3 (OK)
Unit 2:
  Back Fan  1 (OK)      Back Fan  2 (OK)      Back Fan  3 (OK)

Detail Power Status:
(1)      (5)                (6)
Unit     Power Module       Power Status
-----    ----------------   -------------
1        Power 1            in-operation
2        Power 1            in-operation

Detail Memory-Error Auto-Recovery Status:
------------------------------------------------------------
Auto Recovery Mode          : Enabled ...(7)
Auto Recovery Notification : Enabled ...(8)
Fault Action Configuration : - ...(9)
(1)      (10)         (11)                (12)
Unit     Status       Recovery Count      ECC Uncorrectable Error Count
-----    ---------    ---------------     -----------------------------
1        Normal       0                   0
2        Normal       0                   0

Health Status:
(1)      (13)         (14)
Unit     Status       Failure Code
-----    ---------    --------------------
1        Normal       0x00000
2        Normal       0x00000

Slide Switch Status:
(1)      (15)
Unit     Status
-----    ---------
1        Off
2        Off
```

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は 1 が表示されます。
(2)	装置の温度状態を表示します。 Normal：装置の温度が正常範囲 Abnormal：装置の温度が正常範囲外
(3)	現在の温度を表示します。

項番	説明
(4)	ファンの状態を表示します。 OK：正常状態 Fault：異常あり
(5)	電源ユニットを表示します。
(6)	電源の状態を表示します。 in-operation：通常動作中 failed：異常あり
(7)	メモリーエラー自動復旧機能の有効(Enabled)／無効(Disabled)を表示します。
(8)	メモリーエラー自動復旧機能に関連する通知（ログ, SNMP トラップ）の有効(Enabled)／無効(Disabled)を表示します。
(9)	SW-LSI メモリーの状態が「異常」になった場合に、すべてのポートをシャットダウンする機能の有効(Shutdown-all)／無効(-)を表示します。
(10)	SW-LSI メモリーの状態を表示します。 Normal：正常 Abnormal：メモリーエラー発生状態（メモリーエラー自動復旧機能無効：メモリーエラーの発生を検知、メモリーエラー自動復旧機能有効：メモリーエラーの多発を検知）
(11)	メモリーエラーが検出されたときに、実行された復旧アクションの回数を表示します。
(12)	復旧不能なメモリーエラーが検出された回数を表示します。
(13)	装置の正常性を表示します。 Normal：正常 Abnormal：1 つ以上のコンポーネントでエラーを検出
(14)	装置によって検出された障害コードを表示します。 すべての bit=0 (0x00000)：正常状態 bit[8]=1 (0x00100)：電源の障害 bit[10]=1 (0x00400)：ファンの障害 bit[11]=1 (0x00800)：温度異常 bit[14]=1 (0x04000)：SW-LSI のメモリーエラー bit[15]=1 (0x08000)：SW-LSI の復旧不能なメモリーエラー bit[16]=1 (0x10000)：SW-LSI のメモリーエラー (ハードエラー) bit[17]=1 (0x20000)：SW-LSI の復旧不能なメモリーエラー (ハードエラー) ※メモリーエラー自動復旧機能が無効で、「復旧可能なメモリーエラーを検出した場合」は、bit[14]=1 (0x04000)を表示します。 ※メモリーエラー自動復旧機能が無効で、「復旧不能なメモリーエラーを検出した場合」は、bit[15]=1 (0x08000)を表示します。 ※メモリーエラー自動復旧機能が有効で、「SW-LSI の同じメモリー領域で、メモリーエラーの検出および復旧アクションが 10 回以上動作して、監視対象外になった場合」は、bit[16]=1 (0x10000)を表示します。 ※メモリーエラー自動復旧機能が有効で、「復旧不能なメモリーエラーを検出した場合」は、bit[17]=1 (0x20000)を表示します。
(15)	ZTP スイッチの状態を表示します。 On：ZTP スイッチが ON 状態 Off：ZTP スイッチが OFF 状態

使用例：メモリーの詳細状態を表示する方法を示します。

```
# show environment memory

Detail Memory-Error Auto-Recovery Status:
-----------------------------------------------------------
Auto Recovery Mode          : Enabled ...(1)
Auto Recovery Notification : Enabled ...(2)
Fault Action Configuration : - ...(3)
(4)      (5)          (6)                (7)
Unit     Status       Recovery Count     ECC Uncorrectable Error Count
-----    ---------    ---------------    -----------------------------
1        Normal       0                  0
2        Normal       0                  0
```

項番	説明
(1)	メモリーエラー自動復旧機能の有効(Enabled)／無効(Disabled)を表示します。
(2)	メモリーエラー自動復旧機能に関連する通知（ログ, SNMP トラップ）の有効(Enabled)／無効(Disabled)を表示します。
(3)	SW-LSI メモリーの状態が「異常」になった場合に、すべてのポートをシャットダウンする機能の有効(Shutdown-all)／無効(-)を表示します。
(4)	装置のボックス ID を表示します。スタックを構成していない場合は 1 が表示されます。
(5)	SW-LSI メモリーの状態を表示します。 Normal：正常 Abnormal：メモリーエラー発生状態（メモリーエラー自動復旧機能無効：メモリーエラーの発生を検知、メモリーエラー自動復旧機能有効：メモリーエラーの多発を検知）
(6)	メモリーエラーが検出されたときに、実行された復旧アクションの回数を表示します。
(7)	復旧不能なメモリーエラーが検出された回数を表示します。

3.1.11 show unit

show unit	
目的	システムユニットの情報を表示します。
Command	show unit [UNIT-ID]
Parameter	UNIT-ID（省略可能）：装置のボックス ID を 1～4 の範囲で指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	SD カードを挿入した場合、メモリー種別"NVRAM"として SD カードの情報が表示されます。 スタック構成で特定のボックス ID を指定しない場合は、すべてのスタックメンバーの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：システム上のユニットの情報を表示する方法を示します。

```
# show unit
(1)            (2)
```

```
Unit          Model Name
----  ----------------------------
 1     ApresiaNP2500-8MT4X-PoE
 2     ApresiaNP2500-8MT4X-PoE
(1)           (3)                              (4)           (5)
Unit          Serial-Number                    Status        Up Time
----  ---------------------------------  ---------  -----------------
 1     304210000053                       ok          0DT0H31M35S
 2     304210000050                       ok          0DT0H30M58S
(1)    (6)          (7)          (8)          (9)
Unit   Memory       Total        Used         Free
----  --------  -----------  -----------  -----------
 1     DRAM       524288 K     152146 K     372142 K
 1     FLASH      125937 K      25278 K     100659 K
 2     DRAM       524288 K     151620 K     372668 K
 2     FLASH      125937 K      35768 K      90169 K
```

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は 1 が表示されます。
(2)	装置名を表示します。
(3)	シリアル番号を表示します。
(4)	ステータスを表示します。
(5)	連続稼働時間(sysUpTime)を、(日)DT(時)H(分)M(秒)S 形式で表示します。
(6)	メモリー種別を表示します。
(7)	メモリー容量を表示します。
(8)	使用中のメモリー容量を表示します。
(9)	未使用のメモリー容量を表示します。

3.1.12 show cpu utilization

show cpu utilization	
目的	CPU 使用率を表示します。
Command	show cpu utilization [unit [UNIT-ID]]
Parameter	unit（省略可能）：スタック構成で、すべてのスタックメンバーの CPU 使用率を表示する場合に指定します。 UNIT-ID（省略可能）：スタックメンバーを指定して CPU 使用率を表示する場合に、装置のボックス ID を 1～4 の範囲で指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	スタック構成で、unit パラメーターを指定して特定のボックス ID を指定しない場合は、すべてのスタックメンバーの情報が表示されます。 Maximum 項目と Minimum 項目の値をリセットする場合は clear cpu utilization history コマンドを使用します。
制限・注意	-
バージョン	1.08.02

使用例：CPU 使用率を表示する方法を示します。

```
# show cpu utilization

CPU Utilization
(1)                             (2)                             (3)
Five seconds -  14 %            One minute -  13 %              Five minutes -  13 %
Maximum -  28 %                 Minimum -  10 %
(4)                             (5)
```

項番	説明
(1)	5 秒間の平均の CPU 使用率を表示します。
(2)	1 分間の平均の CPU 使用率を表示します。
(3)	5 分間の平均の CPU 使用率を表示します。
(4)	CPU 使用率の最大値を表示します。
(5)	CPU 使用率の最小値を表示します。

使用例：すべてのスタックメンバーの CPU 使用率を表示する方法を示します。

```
# show cpu utilization unit

CPU Utilization
(1)         (2)       (3)       (4)       (5)    (6)
          5 sec     1 min     5 min     Max    Min
-----------------------------------------------
Unit 1:     15%       13%       13%    28%    10%
Unit 2:     12%       11%       11%    54%    11%
Unit 3:       -         -         -      -      -
Unit 4:       -         -         -      -      -
```

項番	説明
(1)	ボックス ID を表示します。
(2)	5 秒間の平均の CPU 使用率を表示します。
(3)	1 分間の平均の CPU 使用率を表示します。
(4)	5 分間の平均の CPU 使用率を表示します。
(5)	CPU 使用率の最大値を表示します。
(6)	CPU 使用率の最小値を表示します。

使用例：ボックス ID 2 のスタックメンバーの CPU 使用率を表示する方法を示します。

```
# show cpu utilization unit 2

CPU Utilization
(1)         (2)       (3)       (4)       (5)    (6)
          5 sec     1 min     5 min     Max    Min
-----------------------------------------------
Unit 2:     12%       11%       11%    54%    11%
```

項番	説明
(1)	ボックス ID を表示します。
(2)	5 秒間の平均の CPU 使用率を表示します。
(3)	1 分間の平均の CPU 使用率を表示します。

項番	説明
(4)	5 分間の平均の CPU 使用率を表示します。
(5)	CPU 使用率の最大値を表示します。
(6)	CPU 使用率の最小値を表示します。

3.1.13 clear cpu utilization history

clear cpu utilization history	
目的	CPU 使用率をクリアします。
Command	clear cpu utilization history
Parameter	なし
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	clear cpu utilization history を実行すると、show cpu utilization の Maximum 項目と Minimum 項目がリセットされます。
制限・注意	-
バージョン	1.08.02

使用例：CPU 使用率をクリアする方法を示します。

```
# clear cpu utilization history
#
```

3.1.14 show history

show history	
目的	現在のセッションで入力したコマンド履歴のリストを表示します。
Command	show history
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	コマンド履歴のリストはセッションごとに記録されます。過去に入力して実行したコマンド文字列が最大 20 個まで記録されます。 コマンド履歴のリストが 20 個を超えた場合は、一番古いコマンド履歴から削除されて、新しく入力したコマンド文字列が記録されます。 「上矢印キー」または「Ctrl+P」を入力すると、コマンド履歴リストの新しいエントリーから順番に CLI に表示されます。 「下矢印キー」または「Ctrl+N」を入力すると、コマンド履歴リストの古いエントリーから順番に CLI に表示されます。
制限・注意	• コマンド文字列として正しく入力できなかった文字列の場合でも記録されます。 • 同じ文字列を連続して 2 回以上入力した場合は、2 回目以降は記録されません。
バージョン	1.08.02

使用例：現在のセッションで入力したコマンド履歴のリストを表示する方法を示します。

```
# show history

 en
 help
 show history
```

3.2 ファイルシステムコマンド

ファイルシステム関連の設定コマンドは以下のとおりです。

- cd
- delete
- dir
- mkdir
- more
- rename
- rmdir

ファイルシステム関連の show コマンドは以下のとおりです。

- show storage media-info

3.2.1 cd

cd	
目的	現在のディレクトリーを変更します。
Command	cd [URL]
Parameter	URL（省略可能）：ディレクトリーの URL を指定します。URL を指定しない場合は、現在のディレクトリーが表示されます。
デフォルト	ローカルフラッシュのファイルシステム上のルートディレクトリー
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	非スタック装置およびスタックマスター装置の場合、ローカルフラッシュのルートディレクトリーは「c:」になります。外部ストレージ（SD カード）のルートディレクトリーは「d:」になります。 スタックマスター以外の装置の場合は、先頭に「unitX:/（X はボックス ID）」を付加したパスを指定します。例えば、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのルートディレクトリーは「unit2:/c:」です。
制限・注意	-
バージョン	1.08.02

使用例：現在のディレクトリーを「c:/log」に変更する方法を示します。

```
# dir

Directory of /c:
1   d--              0 Dec 18 2020 14:32:04  log
2   -rw       11774704 Dec 18 2020 12:54:14  image.had
3   -rw       11774704 Dec 18 2020 12:55:23  image_sec.had
4   -rw           1228 Dec 18 2020 14:25:49  secondary.cfg
5   -rw           1228 Dec 18 2020 14:25:45  primary.cfg
6   d--              0 Dec 18 2020 05:26:31  system

128960000 bytes total (104067584 bytes free)

# cd log
# dir
```

```
Directory of /c:/log
No files in directory
128960000 bytes total (104067584 bytes free)
```

使用例：現在のディレクトリーを表示する方法を示します。

```
# cd
Current directory is /c:/log ...(1)
```

項番	説明
(1)	現在のディレクトリーを表示します。

3.2.2 delete

delete	
目的	ファイルを削除します。
Command	delete FILE
Parameter	FILE：ファイルパス名を指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	非スタック装置およびスタックマスター装置の場合、ローカルフラッシュのルートディレクトリーは「c:」になります。外部ストレージ（SD カード）のルートディレクトリーは「d:」になります。 スタックマスター以外の装置の場合は、先頭に「unitX:/（X はボックス ID)」を付加したパスを指定します。例えば、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのルートディレクトリーは「unit2:/c:」です。
制限・注意	• boot image コマンドで指定したブートイメージファイル、および boot config コマンドで指定した構成情報として使用するファイルは、削除できません。
バージョン	1.08.02

使用例：現在のディレクトリーのファイル「test.txt」を削除する方法を示します。

```
# delete test.txt
Delete test.txt? (y/n) [n]  y
File is deleted.
```

使用例：スタック構成において、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのファイル「test.txt」を削除する方法を示します。

```
# delete unit2:/c:/test.txt
Delete unit2:/c:/test.txt? (y/n) [n]  y
File is deleted.
```

3.2.3 dir

dir	
目的	指定したディレクトリーのファイル一覧などの情報を表示します。
Command	dir [URL]
Parameter	URL（省略可能）：ディレクトリーまたはファイルの URL を指定します。
モード	ユーザー実行モード、特権実行モード

dir	
特権レベル	レベル：1
ガイドライン	URL を指定しない場合は現在のディレクトリーの情報を表示します。デフォルト状態では、ローカルフラッシュ(c:)の情報を表示します。 非スタック装置およびスタックマスター装置の場合、ローカルフラッシュのルートディレクトリーは「c:」になります。外部ストレージ（SD カード）のルートディレクトリーは「d:」になります。 スタックマスター以外の装置の場合は、先頭に「unitX:/（X はボックス ID)」を付加したパスを指定します。例えば、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのルートディレクトリーは「unit2:/c:」です。
制限・注意	-
バージョン	1.08.02

使用例：現在のディレクトリーの情報を表示する方法を示します。

```
# dir

Directory of /c: ...(1)
(2)  (3)       (4)       (5)                    (6)
1    -rw      11774704 Dec 18 2020 12:54:14  image.had
2    -rw      11774704 Dec 18 2020 12:55:23  image_sec.had
3    -rw          1228 Dec 18 2020 14:25:49  secondary.cfg
4    -rw          1228 Dec 18 2020 14:25:45  primary.cfg
5    d--             0 Dec 18 2020 05:26:31  system

128960000 bytes total (104068096 bytes free) ...(7)
```

項番	説明
(1)	ディレクトリー情報を表示するパスを表示します。
(2)	ディレクトリーまたはファイルの通し番号を表示します。
(3)	ディレクトリーまたはファイルの種別、およびアクセス権を表示します。 d：ディレクトリー r：読み出し可能 w：書き込み可能
(4)	ファイルサイズを表示します。ディレクトリーの場合は「0」を表示します。
(5)	ディレクトリーまたはファイルの更新日時を表示します。
(6)	ディレクトリーまたはファイルの名前を表示します。
(7)	ファイルが使用している容量および未使用容量を表示します。

使用例：スタック構成において、ボックス ID 2 の装置（スタックマスター以外）のディレクトリー「c:」の情報を表示する方法を示します。

```
# dir unit2:/c:

Directory of /unit2:/c: ...(1)
(2)  (3)       (4)       (5)                    (6)
1    -rw      11774704 Dec 18 2020 12:54:14  image.had
2    -rw      11774704 Dec 18 2020 12:55:23  image_sec.had
3    -rw          1228 Dec 18 2020 14:25:49  secondary.cfg
4    -rw          1228 Dec 18 2020 14:25:45  primary.cfg
5    d--             0 Dec 18 2020 05:26:31  system
```

```
128960000 bytes total (104068096 bytes free) ...(7)
```

項番	説明
(1)	ディレクトリー情報を表示するパスを表示します。
(2)	ディレクトリーまたはファイルの通し番号を表示します。
(3)	ディレクトリーまたはファイルの種別、およびアクセス権を表示します。 d：ディレクトリー r：読み出し可能 w：書き込み可能
(4)	ファイルサイズを表示します。ディレクトリーの場合は「0」を表示します。
(5)	ディレクトリーまたはファイルの更新日時を表示します。
(6)	ディレクトリーまたはファイルの名前を表示します。
(7)	ファイルが使用している容量および未使用容量を表示します。

3.2.4 mkdir

mkdir	
目的	ディレクトリーを作成します。
Command	mkdir DIRECTORY-NAME
Parameter	DIRECTORY-NAME：ディレクトリー名を指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	非スタック装置およびスタックマスター装置の場合、ローカルフラッシュのルートディレクトリーは「c:」になります。外部ストレージ（SD カード）のルートディレクトリーは「d:」になります。 スタックマスター以外の装置の場合は、先頭に「unitX:/（X はボックス ID)」を付加したパスを指定します。例えば、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのルートディレクトリーは「unit2:/c:」です。
制限・注意	-
バージョン	1.08.02

使用例：現在のディレクトリーに、ディレクトリー「newdir」を作成する方法を示します。

```
# mkdir newdir
# dir

Directory of /c:
1    d--              0 Dec 18 2020 13:09:20  newdir
2    -rw           4717 Dec 14 2020 13:17:48  primary.cfg
～～省略～～
```

使用例：スタック構成において、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュに、ディレクトリー「test_dir」を作成する方法を示します。

```
# mkdir unit2:/c:/test_dir
# dir unit2:/c:
```

```
Directory of /unit2:/c:
1    d--              0 Dec 18 2020 13:13:49  test_dir
2    -rw           4643 Dec 14 2020 13:17:53  primary.cfg
～～省略～～
```

3.2.5 more

more	
目的	ファイルの内容を表示します。
Command	more FILE
Parameter	FILE：ファイルパス名を指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	非スタック装置およびスタックマスター装置の場合、ローカルフラッシュのルートディレクトリーは「c:」になります。外部ストレージ（SD カード）のルートディレクトリーは「d:」になります。 スタックマスター以外の装置の場合は、先頭に「unitX:/（X はボックス ID)」を付加したパスを指定します。例えば、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのルートディレクトリーは「unit2:/c:」です。
制限・注意	• ファイル内の非標準の印刷可能文字は、読み取れない文字や空白のスペースで表示されます。
バージョン	1.08.02

使用例：現在のディレクトリーのファイル「primary.cfg」の内容を表示する方法を示します。

```
# more primary.cfg


#------------------------------------------------------------------------------
#                ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
#                              Configuration
#
#                           Firmware: Build 1.08.02
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------

# Date: Wed Dec 18 13:00:45 2020


# STACK

no stack
no stack my_box_id
stack my_box_priority 32
no stack preempt
no stack port-channel mode partial
no stack stack-port load-balance

# PORT

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

使用例：スタック構成において、ボックス ID 2 の装置（スタックマスター以外）のファイル「primary.cfg」の内容を表示する方法を示します。

```
# more unit2:/c:/primary.cfg


#------------------------------------------------------------------------------
#                ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
#                                Configuration
#
#                            Firmware: Build 1.08.02
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------

# Date: Wed Dec 18 13:53:30 2020


# STACK

##  stacking config information
##   #Box                                Prio-
##   #ID  Type                      Exist rity
##   #--- ------------------------ ----- -----
##   #  1 ApresiaNP2500-8MT4X-PoE  exist 10
##   #  2 ApresiaNP2500-8MT4X-PoE  exist 20
##   #  3 NOT_EXIST                no
##   #  4 NOT_EXIST                no
stack bandwidth 10G 2-port
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.2.6 rename

rename	
目的	ファイルの名前を変更します。
Command	rename FILE1 FILE2
Parameter	FILE1：名前を変更するファイルパス名を指定します。 FILE2：名前変更後のファイルパス名を指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	非スタック装置およびスタックマスター装置の場合、ローカルフラッシュのルートディレクトリーは「c:」になります。外部ストレージ（SD カード）のルートディレクトリーは「d:」になります。 スタックマスター以外の装置の場合は、先頭に「unitX:/（X はボックス ID）」を付加したパスを指定します。例えば、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのルートディレクトリーは「unit2:/c:」です。 変更後のファイル名として変更前とは別のディレクトリーを指定した場合は、名前が変更されて保存ディレクトリーも移動されます。
制限・注意	-
バージョン	1.08.02

使用例：現在のディレクトリーのファイル「doc1.txt」の名称を、「test.txt」に変更する方法を示します。

```
# rename doc1.txt test.txt
```

```
Rename file doc1.txt to test.txt? (y/n) [n]  y
```

使用例：スタック構成において、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのファイル「before.txt」の名称を、「after.txt」に変更する方法を示します。

```
# rename unit2:/c:/before.txt unit2:/c:/after.txt
Rename file unit2:/c:/before.txt to unit2:/c:/after.txt? (y/n) [n]  y
```

3.2.7 rmdir

rmdir	
目的	ディレクトリーを削除します。
Command	rmdir DIRECTORY-NAME
Parameter	DIRECTORY-NAME：ディレクトリー名を指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	非スタック装置およびスタックマスター装置の場合、ローカルフラッシュのルートディレクトリーは「c:」になります。外部ストレージ（SD カード）のルートディレクトリーは「d:」になります。 スタックマスター以外の装置の場合は、先頭に「unitX:/（X はボックス ID）」を付加したパスを指定します。例えば、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのルートディレクトリーは「unit2:/c:」です。
制限・注意	-
バージョン	1.08.02

使用例：現在のディレクトリー配下に存在するディレクトリー「newdir」を削除する方法を示します。

```
# rmdir newdir
Remove directory newdir? (y/n) [n]  y
The directory is removed.
```

使用例：スタック構成において、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュ配下に存在するディレクトリー「test_dir」を削除する方法を示します。

```
# rmdir unit2:/c:/test_dir
Remove directory unit2:/c:/test_dir? (y/n) [n]  y
The directory is removed.
```

3.2.8 show storage media-info

show storage media-info	
目的	ローカルフラッシュおよび外部ストレージの情報を表示します。
Command	show storage media-info [unit UNIT-ID]
Parameter	unit UNIT-ID（省略可能）：装置のボックス ID を 1～4 の範囲で指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	スタック構成で特定のボックス ID を指定しない場合は、すべてのスタックメンバーの情報が表示されます。
制限・注意	-

show storage media-info	
バージョン	1.08.02

使用例：ローカルフラッシュおよび外部ストレージの情報を表示する方法を示します。

```
# show storage media-info
 (1)    (2)     (3)          (4)        (5)       (6)
Unit   Drive   Media-Type   Size       FS-Type   Label
----   -----   ----------   --------   -------   -----------
1      c:      Flash        122 MB     FFS
1      d:      SD Card      1888 MB    FAT16
```

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は 1 が表示されます。
(2)	ドライブ文字を表示します。
(3)	メディアの種類（Flash：ローカルフラッシュ／SD Card：外部ストレージ）を表示します。
(4)	総容量を表示します。
(5)	ファイルシステムを表示します。
(6)	ラベルを表示します。

3.3 ターミナルコマンド

ターミナル関連の設定コマンドは以下のとおりです。

- terminal length default
- terminal width default
- terminal speed

ターミナル関連の show／操作コマンドは以下のとおりです。

- show terminal
- terminal length
- terminal width

3.3.1 terminal length default

terminal length default	
目的	ターミナルの 1 画面に表示される行数（ページング機能により表示を一時停止する行数）のデフォルト値を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	terminal length default VALUE no terminal length default
Parameter	VALUE：1 画面に表示する行数を 0～512 行の範囲で指定します。0 指定時はページング機能は無効になります。
デフォルト	24 行
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本設定は現在のセッションには反映されません。設定後に新しく接続したセッションから反映されます。 show コマンドなどの表示内容が 1 画面に収まらない場合は、ページング機能により以下の行が表示されて表示を一時停止します。 • CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All ページング機能により一時停止している状態では、以下の操作によるスクロールが可能です。 • Ctrl+C キー、Esc キー、または Q キーを入力すると、show コマンドの実行を終了します。 • スペースキーまたは N キーを入力すると、次の 1 ページを表示します。 • Enter キーを入力すると、次の 1 行を表示します。 • A キーを入力すると、最後まですべて表示します。 以下の方法でカウントした行数が「terminal length [default]設定の 1 画面に表示される行数」になると、ページング機能が動作します。 • 出力された 1 行の文字数が「terminal width [default]設定の 1 行の文字数」以下の場合、その行は 1 行とカウントされます。 • 出力された 1 行の文字数が「terminal width [default]設定の 1 行の文字数」より多い場合、その行は 2 行以上としてカウントされます。例えば、terminal width [default]設定が 80 文字で、出力された 1 行の文字数が 110 文字の場合、その行はページング機能としては 2 行とカウントされます。

terminal length default	
制限・注意	• 本設定は構成情報では CLI 関連（ラベル# CLI）で表示されます。
バージョン	1.08.02

使用例：ターミナルの 1 画面に表示される行数（ページング機能により表示を一時停止する行数）のデフォルト値を、50 行に設定する方法を示します。

```
(config)# terminal length default 50
(config)#
```

3.3.2 terminal width default

terminal width default	
目的	ターミナルの 1 行の文字数（コマンド入力時の動作やページング機能の動作に関係する文字数）のデフォルト値を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	terminal width default VALUE no terminal width default
Parameter	VALUE：1 行の文字数を 40～255 文字の範囲で指定します。
デフォルト	80 文字
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本設定は現在のセッションには反映されません。設定後に新しく接続したセッションから反映されます。 コマンド入力時の 1 行の文字数（プロンプト文字列を含む）が「terminal width [default]設定の 1 行の文字数」を超えた場合、それまでの入力内容が $ で省略表示されます。
制限・注意	• 本設定は構成情報では CLI 関連（ラベル# CLI）で表示されます。 • [?]キーによる「選択可能なパラメーターとヘルプ表示」の改行位置は、本コマンドで設定する 1 行の文字数に影響されます。
バージョン	1.08.02

使用例：ターミナルの 1 行の文字数（コマンド入力時の動作やページング機能の動作に関係する文字数）のデフォルト値を、100 文字に設定する方法を示します。

```
# configure terminal
(config)# terminal width default 100
(config)#
```

3.3.3 terminal speed

terminal speed	
目的	コンソールポートのボー・レートを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	terminal speed BPS no terminal speed
Parameter	BPS：コンソールポートのボー・レートを指定します。設定可能な値は 9600(bps), 19200(bps), 38400(bps), 115200(bps)です。

terminal speed	
デフォルト	9600(bps)
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 本設定は構成情報では BASIC 関連 (ラベル# BASIC) で表示されます。
バージョン	1.08.02

使用例：コンソールポートのボー・レートを 115200 に設定する方法を示します。

```
# configure terminal
(config)# terminal speed 115200
(config)#
```

3.3.4 show terminal

show terminal	
目的	ターミナル設定を表示します。
Command	show terminal
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ターミナル設定を表示する方法を示します。

```
# show terminal
Terminal Settings:
 Length: 24 lines ...(1)
 Width: 80 columns ...(2)
 Default Length: 24 lines ...(3)
 Default Width: 80 columns ...(4)
 Baud Rate: 9600 bps ...(5)
```

項番	説明
(1)	現在のセッションの、端末画面に表示される行数を表示します。
(2)	現在のセッションの、端末画面の 1 行の文字数を表示します。
(3)	端末画面に表示される行数のデフォルト値を表示します。
(4)	端末画面の 1 行の文字数のデフォルト値を表示します。
(5)	コンソールポートのボー・レートを表示します。

3.3.5 terminal length

terminal length	
目的	現在のセッションで、ターミナルの 1 画面に表示される行数（ページング機能により表示を一時停止する行数）を設定します。デフォルト設定に戻すには、no terminal

terminal length	
	length コマンドを使用します。
Command	terminal length VALUE no terminal length
Parameter	VALUE：1 画面に表示する行数を 0～512 行の範囲で指定します。0 指定時はページング機能は無効になります。
デフォルト	24 行
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	本設定は現在のセッションにのみ反映されますが、動作は terminal length default コマンドで説明している内容と同じです。terminal length コマンドの使用方法については「3.3.1 terminal length default」を参照してください。
制限・注意	-
バージョン	1.08.02

使用例：現在のセッションで、ターミナルの 1 画面に表示される行数（ページング機能により表示を一時停止する行数）を、50 行に設定する方法を示します。

```
# terminal length 50
#
```

3.3.6 terminal width

terminal width	
目的	現在のセッションで、ターミナルの 1 行の文字数（コマンド入力時の動作やページング機能の動作に関係する文字数）を設定します。デフォルト設定に戻すには、no terminal width コマンドを使用します。
Command	terminal width VALUE no terminal width
Parameter	VALUE：1 行の文字数を 40～255 文字の範囲で指定します。
デフォルト	80 文字
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	本設定は現在のセッションにのみ反映されますが、動作は terminal width default コマンドで説明している内容と同じです。terminal width コマンドの使用方法については「3.3.2 terminal width default」を参照してください。
制限・注意	• [?]キーによる「選択可能なパラメーターとヘルプ表示」の改行位置は、本コマンドで設定する 1 行の文字数に影響されます。
バージョン	1.08.02

使用例：現在のセッションで、ターミナルの 1 行の文字数（コマンド入力時の動作やページング機能の動作に関係する文字数）を 100 文字に設定する方法を示します。

```
# terminal width 100
#
```

3.4 アクセス管理コマンド

アクセス管理関連の設定コマンドは以下のとおりです。

- username
- enable password
- service user-account encryption
- prompt
- banner login
- line
- login（Line）
- password
- session-timeout
- access-class

アクセス管理関連の show／操作コマンドは以下のとおりです。

- show users
- show privilege
- clear line

3.4.1 username

username	
目的	ユーザーアカウントを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	username NAME [privilege LEVEL] [nopassword | password [0 | 7] PASS] no username [NAME]
Parameter	NAME：ユーザー名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 privilege LEVEL（省略可能）：ユーザーアカウントの特権レベルを 1～15 の範囲で指定します。省略した場合は、特権レベル 1 で設定されます。 nopassword（省略可能）：パスワードを設定しない場合に指定します。省略した場合は、nopassword で設定されます。 password [0 | 7] PASS（省略可能）：パスワードを設定する場合に指定します。省略した場合は、nopassword で設定されます。 • [0 | 7]（省略可能）：後に続くパスワードの文字列の形式を明示する場合に指定します。0 の場合は平文（最大 32 文字）を、7 の場合は暗号化された形式（最大 35 文字）を意味します。省略した場合は、平文で入力します。 • PASS：平文で入力する場合は、パスワードを最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? を除いた文字を使用可能です。スペースも使用できます。
デフォルト	ユーザーアカウントなし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	ユーザーアカウントの最大数は 256 個です。 特権レベル 1 のユーザーアカウントでログインした場合は、ユーザー実行モード（プ

username	
	ロンプト末尾が > 表示）でログインします。ユーザー実行モードから特権実行モードに遷移する場合は enable コマンドを使用します。 特権レベル 2 以上のユーザーアカウントでログインした場合は、設定したレベルの特権実行モード（プロンプト末尾が # 表示）でログインします。 ユーザー名を指定せずに no username コマンドを実行すると、すべてのユーザーアカウント設定が削除されます。 本コマンドでユーザーアカウントを設定すると、そのユーザーアカウントに対応した ssh user authentication-method 設定も自動的に作成されます。また、ユーザーアカウントを削除すると、対応する ssh user authentication-method 設定も自動的に削除されます。
制限・注意	• ユーザー名として、装置のパスワード・設定の初期化が実行される特別なアカウント文字列「ap_recovery」を指定することはできません。 • 構成情報では、username NAME privilege LEVEL 設定は別行で表示されます。特権レベル 1（デフォルト設定）の場合は表示されません。
バージョン	1.08.02

使用例：「ユーザー名が admin、特権レベルが 15、パスワードが mypassword」のユーザーアカウントを設定する方法を示します。

```
# configure terminal
(config)# username admin privilege 15 password mypassword
(config)#
```

3.4.2 enable password

enable password	
目的	異なる特権レベルに遷移する enable パスワードを設定します。空の文字列にパスワードを戻す場合は、no enable password コマンドを使用します。
Command	enable password [level PRIVILEGE-LEVEL] [0 | 7] PASS no enable password [level PRIVILEGE-LEVEL]
Parameter	level PRIVILEGE-LEVEL（省略可能）：特権レベルを 1～15 の範囲で指定します。省略した場合は、特権レベル 15 で設定されます。 [0 | 7]（省略可能）：後に続くパスワードの文字列の形式を明示する場合に指定します。0 の場合は平文（最大 32 文字）を、7 の場合は暗号化された形式（最大 35 文字）を意味します。省略した場合は、平文で入力します。 PASS：平文で入力する場合は、パスワードを最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、？ を除いた文字を使用可能です。スペースも使用できます。
デフォルト	パスワードの設定なし（空の文字列）
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	• enable パスワードとして、装置のパスワード・設定の初期化が実行される特別なアカウント文字列「ap_recovery」を指定することはできません。 • enable パスワード未設定時には、コンソールポート接続で装置にログインしている

enable password	
	場合のみ、パスワードなしで特権レベル 15 に遷移できます。
バージョン	1.08.02

使用例：特権レベル 15 の enable パスワード「MyEnablePassword」を設定する方法を示します。

```
# configure terminal
(config)# enable password MyEnablePassword
(config)# exit
# disable
> enable

Password:****************
#
```

3.4.3 service user-account encryption

service user-account encryption	
目的	パスワード文字列などの暗号化を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	service user-account encryption no service user-account encryption
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	本設定を有効にすると、以下のコマンドで設定されたパスワード文字列、SNMP コミュニティー名、SNMP グループ名、共有鍵が暗号化されます。また、本設定が有効な状態では、以下のコマンドでパスワード文字列などを平文で指定して新たに設定した場合でも、暗号化されて設定されます。 • username コマンド • enable password コマンド • password コマンド • aaa-local-db user コマンド • mac-authentication password コマンド • snmp-server community コマンド • snmp-server host コマンド • snmp-server user コマンド • snmp-server group コマンド • radius-server host コマンド • tacacs-server host コマンド 本設定を有効にして暗号化したパスワード文字列などの設定は、本設定を無効にしても平文の文字列の設定には戻りません。
制限・注意	-
バージョン	1.08.02

使用例：パスワード文字列などの暗号化を有効にする方法を示します。

```
# configure terminal
```

```
(config)# service user-account encryption
(config)#
```

3.4.4 prompt

prompt	
目的	CLI に表示されるプロンプト文字列を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	prompt STRING no prompt
Parameter	STRING：プロンプト文字列を最大 35 文字で指定します。なお、最初の 15 文字のみ表示されます。ASCII コードの印字可能な文字のうち、？ 空白文字 を除いた文字と、以下の制御文字を使用可能です。 • %h：snmp-server name コマンドで設定したシステム名（sysName） • %s：スペース • %%：h または s の前に%を入力したい場合の指定方法（例：a%%sa と設定すると a%sa と表示される）
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	プロンプト文字列の最大表示文字数は 15 文字です。また、以下が特権レベルを表す文字として、プロンプトの末尾に表示されます。 • >：ユーザー実行モード（レベル 1） • #：特権実行モード（レベル 2～15）
制限・注意	-
バージョン	1.08.02

使用例：CLI に表示されるプロンプト文字列を「BRANCH A」に設定する方法を示します。

```
# configure terminal
(config)# prompt BRANCH%sA
BRANCH A(config)#
```

3.4.5 banner login

banner login	
目的	ログイン画面で表示されるログインバナーメッセージを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	banner login cMESSAGEc no banner login
Parameter	c：区切り文字を指定します。区切り文字には、ログインバナーメッセージで使用しない文字を指定します。スペースおよび？は指定できません。 MESSAGE：ログインバナーメッセージを指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ログインバナーメッセージが 1 行の場合、メッセージの前後に区切り文字を挿入して

banner login	
	コマンドを実行します。 ログインバナーメッセージが複数行の場合も同様ですが、メッセージを複数行入力する場合に Enter キーで改行して入力します。 "banner login 区切り文字" のみを指定して実行した場合は、ログインバナーメッセージの入力モードになります。Enter キーで改行して複数行のメッセージを入力できます。メッセージをすべて入力したら、最後に区切り文字を入力して Enter キーを実行します。 区切り文字には、ログインバナーメッセージで使用しない文字を指定する必要があります。設定後の構成情報では、区切り文字は自動的に適切な文字に変更されます。
制限・注意	-
バージョン	1.08.02

使用例：1 行のログインバナーメッセージを設定する方法を示します。この例では入力時の区切り文字は「#」、メッセージは「Apresia Systems LAN」とします。

```
# configure terminal
(config)# banner login #Apresia Systems LAN#
(config)#

～～設定後の構成情報の表示～～
banner login bApresia Systems LANb
```

使用例：複数行のログインバナーメッセージを設定する方法を示します。この例では入力時の区切り文字は「%」、メッセージは以下とします。

- メッセージ 1 行目「####################################」
- メッセージ 2 行目「### 2F-L2-05, Apresia Systems LAN ###」
- メッセージ 3 行目「###   Location: TNTC-2Fb01 ###」

```
# configure terminal
(config)# banner login %
LINE c banner-text c, where 'c' is a delimiting character
####################################
### 2F-L2-05, Apresia Systems LAN ###
###          Location: TNTC-2Fb01 ###%
(config)#

～～設定後の構成情報の表示～～
banner login d####################################
### 2F-L2-05, Apresia Systems LAN ###
###          Location: TNTC-2Fb01 ###d
```

3.4.6 line

line	
目的	設定対象のセッション種別を指定して、それぞれのライン設定モードに遷移します。遷移後のプロンプトは (config-line)# に変更されます。
Command	line {console | telnet | ssh}
Parameter	console：装置のコンソールポートにコンソールケーブルを接続して、装置にアクセスする際の設定を変更する場合に指定します。 telnet：Telnet で装置にアクセスする際の設定を変更する場合に指定します。

line	
	ssh：SSH で装置にアクセスする際の設定を変更する場合に指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ラインセッション(SSH)のライン設定モードに遷移する方法を示します。

```
# configure terminal
(config)# line ssh
(config-line)#
```

3.4.7 login (Line)

login (Line)	
目的	AAA が無効な場合の、各ラインセッション(コンソール、Telnet、SSH)へのログイン方法を設定します。ログイン方法を無効にする場合は、no login コマンドを使用します。
Command	login [local] no login
Parameter	local（省略可能）：ラインセッションへのログイン方法をローカルのユーザーアカウント（username コマンドで設定したユーザー名とパスワード）にする場合に指定します。
デフォルト	ラインセッション(コンソール)：no login (無効) ラインセッション(Telnet)：login (パスワードの入力が必要) ラインセッション(SSH)：login (ユーザー名とパスワードの入力が必要)
モード	ライン設定モード
特権レベル	レベル：15
ガイドライン	コンソールおよび Telnet アクセスでは、AAA が有効な場合、AAA モジュールによって設定されたルールが適用されます。AAA が無効な場合、以下の認証ルールが適用されます。 • ログイン方法が無効 no login 設定の場合、ユーザー名とパスワードの入力無しでレベル 1 の特権レベルでログインします。 • ログイン方法が login 設定で password コマンドでパスワードが設定されている場合は、パスワードを入力するとレベル 1 の特権レベルでログインします。パスワードが設定されていない場合は、エラーメッセージが表示されセッションが閉じられます。 • ログイン方法が login local 設定の場合は、ローカルのユーザーアカウント（username コマンドで設定したユーザー名とパスワード）でログインできるようになります。 SSH アクセスでは、AAA が有効な場合、AAA モジュールによって設定されたルールが適用されます。また、SSH の認証方式は以下の 3 種類の認証方式が使用できますが、SSH 公開鍵またはホストベース認証の場合は、本コマンドの設定に影響を受けません。

login (Line)	
	• SSH 公開鍵 • ホストベース認証 • パスワード認証 AAA が無効で SSH の認証方式がパスワード認証の場合は、SSH サーバーと SSH クライアントの間の認証方式を確認するために、あらかじめ username コマンドでユーザー名を設定する必要があります。認証方式が一致した場合、以下の認証ルールが適用されます。 • ログイン方法が no login 設定の場合、認証時にパスワードが無視されます。username コマンドで設定したユーザー名と、パスワードとして任意の文字列を入力すると、レベル 1 の特権レベルでログインします。 • ログイン方法が login 設定の場合は password コマンドでパスワードの設定が必要です。username コマンドで設定したユーザー名と、password コマンドで設定したパスワードを入力すると、レベル 1 の特権レベルでログインします。 • ログイン方法が login local 設定の場合は、ローカルのユーザーアカウント (username コマンドで設定したユーザー名とパスワード) でログインできるようになります。
制限・注意	• 本コマンドは、AAA が無効 (no aaa new-model (デフォルト設定)) の場合に設定できます。
バージョン	1.08.02

使用例：ラインセッション(コンソール)でのログイン用のパスワードを「loginpassword」に設定し、ログイン方法を login に設定する方法を示します。

```
# configure terminal
(config)# line console
(config-line)# password loginpassword
(config-line)# login
(config-line)#
```

使用例：ラインセッション(Telnet)でのログイン方法を login local に設定する方法を示します。

```
# configure terminal
(config)# line telnet
(config-line)# login local
(config-line)#
```

3.4.8 password

password	
目的	各ラインセッション(コンソール、Telnet、SSH)のパスワードを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	password [0 | 7] PASS no password
Parameter	[0 | 7] (省略可能)：後に続くパスワードの文字列の形式を明示する場合に指定します。0 の場合は平文 (最大 32 文字) を、7 の場合は暗号化された形式 (最大 35 文字) を意味します。省略した場合は、平文で入力します。 PASS：平文で入力する場合は、パスワードを最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? を除いた文字を使用可能です。スペースも使用できます。

password	
デフォルト	パスワードなし
モード	ライン設定モード
特権レベル	レベル：15
ガイドライン	各ラインセッション(コンソール、Telnet、SSH)ごとに 1 つのパスワードを設定できます。
制限・注意	• パスワードとして、装置のパスワード・設定の初期化が実行される特別なアカウント文字列「ap_recovery」を指定することはできません。
バージョン	1.08.02

使用例：ラインセッション(コンソール)のパスワードを設定する方法を示します。

```
# configure terminal
(config)# line console
(config-line)# password 123
(config-line)#
```

3.4.9 session-timeout

session-timeout	
目的	各ラインセッション(コンソール、Telnet、SSH)のタイムアウト時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	session-timeout MINUTES no session-timeout
Parameter	MINUTES：タイムアウト時間を 0～1439 分の範囲で指定します。0 指定時はタイムアウト処理は無効になります。
デフォルト	3 分
モード	ライン設定モード
特権レベル	レベル：12
ガイドライン	AAA が無効で、コンソールおよび Telnet アクセスのログイン方法が login local に設定されている場合、ラインセッション(コンソール、Telnet)のログイン処理のリトライ回数は以下になります。 • session-timeout 0 or 1 設定時：リトライ回数は 1 回 • session-timeout 2 設定時：リトライ回数は 2 回 • session-timeout 3 以上に設定時：リトライ回数は 3 回 ラインセッション(SSH)のログイン処理のリトライ回数は、ip ssh authentication-retries コマンドで設定します。
制限・注意	-
バージョン	1.08.02

使用例：ラインセッション(コンソール)のタイムアウト処理を無効にする方法を示します。

```
# configure terminal
(config)# line console
(config-line)# session-timeout 0
(config-line)#
```

3.4.10 access-class

access-class	
目的	各ラインセッション(Telnet、SSH)経由のアクセス制限を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	access-class ACL-NAME no access-class ACL-NAME
Parameter	ACL-NAME：アクセス制限で使用する標準 IP アクセスリスト、または標準 IPv6 アクセスリストを指定します。
デフォルト	アクセス制限の設定なし
モード	ライン設定モード
特権レベル	レベル：15
ガイドライン	本コマンドを設定すると、装置宛てアクセス(Telnet、SSH)の送信元 IPv4/IPv6 アドレスが、指定したアクセスリストを基にチェックされるようになります。各ラインセッション(Telnet、SSH)ごとに、IPv4 アドレス用に 1 個、IPv6 アドレス用に 1 個の、最大 2 個まで設定できます。 <標準 IP アクセスリスト指定の場合> • 装置宛てアクセスを許可する IPv4 アドレスを permit ルールの「送信元 IP アドレス」条件で、拒否する IPv4 アドレスを deny ルールの「送信元 IP アドレス」条件で指定します。 • いずれのルールにもマッチしない場合は、拒否されます。 <標準 IPv6 アクセスリスト指定の場合> • 装置宛てアクセスを許可する IPv6 アドレスを permit ルールの「送信元 IPv6 アドレス」条件で、拒否する IPv6 アドレスを deny ルールの「送信元 IPv6 アドレス」条件で指定します。 • いずれのルールにもマッチしない場合は、拒否されます。 いずれの場合も、「宛先 IP アドレス」「宛先 IPv6 アドレス」条件は、any で設定する必要があります。any 以外で設定した場合は、そのルールは無効になります。なお、入力を省略した場合は any で設定されます。
制限・注意	• 説明に記載されている種別以外のアクセスリストを指定して使用できません。 • IPv4 アドレス用の標準 IP アクセスリストを 2 つ設定した場合は、最初の 1 つのみが有効となります。同様に、IPv6 アドレス用の標準 IPv6 アクセスリストを 2 つ設定した場合は、最初の 1 つのみが有効となります。 • すでに 2 つのアクセスリストを適用している状態では、新しいアクセスリストを指定して設定できません。 • 本コマンドは、ラインセッション(コンソール)では対応していません。設定しても構成情報には表示されません。 • 本設定で指定する標準 IP アクセスリスト、または標準 IPv6 アクセスリストでは、装置のハードウェアリソースを使用しません。
バージョン	1.08.02

使用例：以下の内容で Telnet によるアクセス制限を有効にする方法を示します。アクセス制限用の標準 IP アクセスリスト名は「TELNET-LIST」とします。

- 192.0.2.0/24 からの Telnet アクセスを許可

- 10.0.0.100/32 からの Telnet アクセスを許可
- それ以外からの Telnet アクセスを拒否

```
# configure terminal
(config)# ip access-list TELNET-LIST
(config-ip-acl)# permit 192.0.2.0 0.0.0.255
(config-ip-acl)# permit host 10.0.0.100
(config-ip-acl)# exit
(config)#
(config)# line telnet
(config-line)# access-class TELNET-LIST
(config-line)#
```

使用例：以下の内容で SSH によるアクセス制限を有効にする方法を示します。アクセス制限用の標準 IP アクセスリスト名は「SSH-LIST」とします。

- ルール 10：192.0.2.100/32 からの SSH アクセスを許可
- ルール 20：192.0.2.100 以外の 192.0.2.0/24 からの SSH アクセスを拒否
- ルール 100：それ以外からの SSH アクセスを許可

```
# configure terminal
(config)# ip access-list SSH-LIST
(config-ip-acl)# 10 permit host 192.0.2.100
(config-ip-acl)# 20 deny 192.0.2.0 0.0.0.255
(config-ip-acl)# 100 permit any
(config-ip-acl)# exit
(config)#
(config)# line ssh
(config-line)# access-class SSH-LIST
(config-line)#
```

3.4.11 show users

show users	
目的	ラインセッション情報を表示します。
Command	show users
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべてのラインセッション情報を表示する方法を示します。

```
# show users
 (1)   (2)       (3)             (4)       (5)                 (6)
ID    Type      User-Name       Privilege Login-Time          IP address
------------------------------------------------------------------------------
0       console Anonymous       1         16H9M36S
1     * telnet  example         1         11M48S              192.0.2.100
10      SSH     test            15        4M54S               10.250.21.112

Total Entries: 3
```

項番	説明
(1)	ラインセッション ID を表示します。
(2)	ラインセッションのタイプを表示します。自セッションの場合はアスタリスク(*)が表示されます。 console：コンソール経由のログイン telnet：Telnet 経由のログイン SSH：SSH 経由のログイン
(3)	ユーザー名を表示します。
(4)	特権レベルを表示します。
(5)	ログインしてからの経過時間を表示します。
(6)	クライアントの IP アドレスを表示します。

3.4.12 show privilege

show privilege	
目的	現在の特権レベルを表示します。
Command	show privilege
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：現在の特権レベルを表示する方法を示します。

```
# show privilege

Current privilege level is 15
```

3.4.13 clear line

clear line	
目的	ラインセッションを手動で切断します。
Command	clear line ID
Parameter	ID：切断するラインセッション ID を 1～18 の範囲で指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	ラインセッション ID は、show users コマンドで確認できます。
制限・注意	• ラインセッション(コンソール)は手動で切断できません。
バージョン	1.08.02

使用例：ラインセッション ID=1 を手動で切断する方法を示します。

```
# clear line 1
#
```

3.5 基本 IPv4 コマンド

基本 IPv4 関連の設定コマンドは以下のとおりです。

- ip address
- ip default-gateway（mgmt 0）
- arp
- arp timeout

基本 IPv4 関連の show／操作コマンドは以下のとおりです。

- show ip interface
- show arp
- show arp cache
- show arp timeout
- clear arp-cache

3.5.1 ip address

ip address	
目的	VLAN インターフェース、またはマネージメントポートの IPv4 アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip address {{IP-ADDRESS MASK | IP-ADDRESS/LEN} | dhcp} no ip address [IP-ADDRESS MASK | IP-ADDRESS/LEN | dhcp]
Parameter	IP-ADDRESS MASK：IPv4 アドレスとサブネットマスクを指定します。（例：192.0.2.100 255.255.255.0） IP-ADDRESS/LEN：IPv4 アドレスとプレフィックス長を指定します。（例：192.0.2.100/24） dhcp：DHCP で IPv4 アドレスを取得する場合に指定します。マネージメントポートでは指定できません。
デフォルト	0.0.0.0/0
モード	インターフェース設定モード(vlan, mgmt)
特権レベル	レベル：12
ガイドライン	ApresiaNP2500 シリーズでは、レイヤー3 用の VLAN インターフェースは 1 個だけ設定できます。デフォルトで VLAN 1 インターフェースが設定済みのため、別の VLAN を指定して VLAN インターフェースを作成する場合は、先に VLAN 1 インターフェースを削除（no interface vlan 1）してから設定してください。 ip address dhcp 設定時に DHCP サーバーからデフォルトゲートウェイアドレスを取得した場合は、自動的に対応するデフォルトスタティックルート設定が追加されます。ip address dhcp 設定を削除すると、自動的に追加されたデフォルトスタティックルート設定も削除されます。
制限・注意	• ApresiaNP2500 シリーズでは、設定できるレイヤー3 用の VLAN インターフェースは 1 個のため、VLAN 間のレイヤー3 中継はできません。 • ip address dhcp 設定と「ユーザーによるデフォルトスタティックルート設定」は、同一装置で併用できません。例えば、「ユーザーによるデフォルトスタティックルート設定」がある状態で ip address dhcp を設定すると、そのデフォルトスタティックルート設定は削除されます。

ip address	
	• IPv4 アドレスとサブネットマスクを指定して設定した場合でも、構成情報では IPv4 アドレスとプレフィックス長で表示されます。
バージョン	1.08.02

使用例：VLAN 1 インターフェースの IPv4 アドレスを 192.0.2.254/24 に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.0.2.254/24
(config-if-vlan)#
```

3.5.2 ip default-gateway（mgmt 0）

ip default-gateway（mgmt 0）	
目的	マネージメントポートのデフォルトゲートウェイの IPv4 アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip default-gateway IP-ADDRESS no ip default-gateway IP-ADDRESS
Parameter	IP-ADDRESS：IPv4 アドレスを指定します。
デフォルト	0.0.0.0
モード	インターフェース設定モード(mgmt)
特権レベル	レベル：12
ガイドライン	マネージメントポートから送信する他の IP サブネット宛ての通信は、デフォルトゲートウェイ宛てに送信されます。
制限・注意	-
バージョン	1.08.02

使用例：マネージメントポートのデフォルトゲートウェイの IPv4 アドレスを 192.0.2.1 に設定する方法を示します。

```
# configure terminal
(config)# interface mgmt 0
(config-if-mgmt)# ip default-gateway 192.0.2.1
(config-if-mgmt)#
```

3.5.3 arp

arp	
目的	ARP テーブルに、スタティックエントリーを追加します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	arp IP-ADDRESS MAC-ADDRESS no arp IP-ADDRESS MAC-ADDRESS
Parameter	IP-ADDRESS：スタティックエントリーの IPv4 アドレスを指定します。 MAC-ADDRESS：スタティックエントリーのユニキャスト MAC アドレスを、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX）

arp	
	• 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX）
デフォルト	スタティックエントリーの設定なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• スタティック ARP エントリーを設定する場合は、mac-address-table static コマンドで対応するスタティック MAC アドレスエントリーも設定してください。 • ApresiaNP2500 シリーズでは、スタティック ARP エントリーは最大 128 個まで設定できます。 • マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、ALL=0 の MAC アドレスを指定してスタティック ARP エントリーを設定することはできません。また、224.0.0.0/4（マルチキャスト）, 127.0.0.0/8（ループバックアドレス）, 0.0.0.0/8, 240.0.0.0/4 の IPv4 アドレスを指定してスタティック ARP エントリーを設定することはできません。
バージョン	1.08.02

使用例：スタティック ARP エントリー「IP=192.0.2.101、MAC=00:00:5E:00:53:11」を設定する方法を示します。

```
# configure terminal
(config)# arp 192.0.2.101 0000.5e00.5311
(config)#
```

3.5.4 arp timeout

arp timeout	
目的	ARP テーブルの ARP エージングタイムを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	arp timeout MINUTES no arp timeout
Parameter	MINUTES：ARP エージングタイムを 0～65,535 の範囲で指定します。
デフォルト	240 分
モード	インターフェース設定モード（vlan）
特権レベル	レベル：12
ガイドライン	ARP エージングタイム期間内にトラフィックがない場合、動的に登録された ARP エントリーはエージングタイムアウトすると削除されます。 ルートのネクストホップの ARP エントリーは、タイムアウトしても削除されません。ルートのネクストホップの ARP エントリーを削除するには、clear arp-cache コマンドを使用します。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 インターフェースの ARP エージングタイムを 60 分に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# arp timeout 60
(config-if-vlan)#
```

3.5.5 show ip interface

show ip interface	
目的	IPv4 インターフェース情報を表示します。
Command	show ip interface [IF-ID] [brief]
Parameter	IF-ID（省略可能）：IPv4 インターフェースを以下のパラメーターで指定します。 • mgmt 0：マネージメントポート指定 • vlan <1-4094>：VLAN インターフェース指定 brief（省略可能）：IPv4 インターフェースの概要情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定の IPv4 インターフェースを指定しない場合は、すべての IPv4 インターフェースの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：IPv4 インターフェースの概要情報を表示する方法を示します。

```
# show ip interface brief

(1)          (2)               (3)
Interface    IP Address        Link Status
-----------  ----------------  -----------
vlan1        192.0.2.100       up
mgmt_ipif    0.0.0.0           down

Total Entries: 2
```

項番	説明
(1)	IPv4 インターフェースを表示します。
(2)	IPv4 アドレスを表示します。
(3)	リンク状態（up／down）を表示します。

使用例：VLAN 1 の IPv4 インターフェース情報を表示する方法を示します。

```
# show ip interface vlan 1
(1)                          (2)
Interface vlan1 is enabled, link status is up
  IP address is 192.0.2.100/24 (Manual) ...(3)
  ARP timeout is 240 minutes ...(4)
  Gratuitous-send is disabled, interval is 0 seconds ...(5)
```

項番	説明
(1)	VLAN インターフェースの有効／無効を表示します。

項番	説明
	enabled：有効（no shutdown 設定時） disabled：無効（shutdown 設定時）
(2)	VLAN インターフェースのリンク状態（up／down）を表示します。
(3)	IPv4 アドレスを表示します。コマンドで設定した場合は（Manual）が、DHCP で取得した場合は（DHCP）が IPv4 アドレスの後ろに表示されます。
(4)	ARP エージングタイムを表示します。
(5)	GARP リクエスト送信の有効(enabled)／無効(disabled)、および送信間隔を表示します。

3.5.6 show arp

show arp	
目的	ARP テーブルのエントリーを表示します。
Command	show arp [ARP-TYPE | IP-ADDRESS [MASK] | interface IF-ID | MAC-ADDRESS]
Parameter	ARP-TYPE（省略可能）：表示するエントリーの種類を、以下のパラメーターで指定します。 • dynamic：ダイナミックエントリーを指定します。 • static：スタティックエントリーを指定します。 IP-ADDRESS［MASK］（省略可能）：表示するエントリーの IPv4 アドレスを指定します。サブネットマスクを指定することにより、ネットワークアドレスを指定することも可能です。 interface IF-ID（省略可能）：エントリーを表示する IPv4 インターフェースを、以下のパラメーターで指定します。 • mgmt 0：マネージメントポート指定 • vlan <1-4094>：VLAN インターフェース指定 MAC-ADDRESS（省略可能）：表示するエントリーの MAC アドレスを、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX）
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	パラメーター省略時は、すべてのエントリーが表示されます。
制限・注意	• オプションパラメーター未指定の show arp コマンドでは、以下のような「利用できないスタティック ARP エントリー」は表示されません。 • IPv4 インターフェースがダウンしているスタティック ARP エントリー • 自装置に直接接続されていないセグメントの IPv4 アドレスを指定して登録されたスタティック ARP エントリー • show arp static コマンドでは「利用できないスタティック ARP エントリー」も表示されますが、対象エントリーの IPv4 インターフェースは非表示になります。
バージョン	1.08.02

使用例：ARP テーブルを表示する方法を示します。

```
# show arp

S - Static Entry
(1)                (2)                (3)            (4)
IP Address         Hardware Addr      IP Interface   Age (min)
-----------------  -----------------  -------------  ---------------
  192.0.2.100      00-00-5E-00-53-11  vlan10         240
S 192.0.2.201      00-00-5E-00-53-22  vlan10         forever
  192.0.2.253      00-00-5E-00-53-BB  vlan10         240
  192.0.2.254      FC-6D-D1-F2-82-1F  vlan10         forever

Total Entries: 4
```

項番	説明
(1)	IPv4 アドレスを表示します。
(2)	MAC アドレスを表示します。
(3)	エントリーを学習した IPv4 インターフェースを表示します。
(4)	ARP エージングタイムの設定値を表示します。自装置のエントリー、またはスタティックエントリーの場合は forever と表示されます。マネージメントポートで学習したダイナミックエントリーの場合は 0 と表示されます。

3.5.7 show arp cache

show arp cache	
目的	ARP キャッシュテーブルを表示します。
Command	show arp cache [IP-ADDRESS [MASK] | interface IF-ID]
Parameter	IP-ADDRESS [MASK]（省略可能）：表示するエントリーの IPv4 アドレスを指定します。サブネットマスクを指定することにより、ネットワークアドレスを指定することも可能です。 interface IF-ID（省略可能）：エントリーを表示するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 • vlan <1-4094>：VLAN インターフェース指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	パラメーター省略時は、すべてのエントリーが表示されます。
制限・注意	• 登録済みの ARP キャッシュエントリーにおいて、リンクダウンを伴わないポート間移動が発生した場合、MAC アドレスを再学習してから数秒後に ARP キャッシュエントリーの送信先インターフェースの更新が行われます。なお、MAC アドレスや ARP キャッシュエントリーの登録数が多い環境では、この更新時間がより長くなることがあります。 • 以下のエントリーは本コマンドでは表示されません。 • マネージメントポートに登録されるエントリー • 対応する MAC アドレスが MAC アドレステーブルに登録されていないスタティック ARP エントリー
バージョン	1.08.02

使用例：ARP キャッシュテーブルを表示する方法を示します。

```
# show arp cache
(1)               (2)    (3)                 (4)            (5)
IP Address        VID    Hardware Addr       Interface      Age
---------------   ----   -----------------   ------------   --------
192.0.2.100         10   00-00-5E-00-53-11   C/5            240
192.0.2.201         10   00-00-5E-00-53-22   C/5            forever
192.0.2.253         10   00-00-5E-00-53-BB   1/0/11         240
192.0.2.254         10   FC-6D-D1-F2-82-1F   CPU            forever

Total Entries: 4
```

項番	説明
(1)	IPv4 アドレスを表示します。
(2)	VLAN ID を表示します。
(3)	MAC アドレスを表示します。
(4)	エントリーを学習したインターフェース ID（物理ポート、ポートチャネル）を表示します。自装置のエントリーの場合は CPU と表示されます。
(5)	ARP エージングタイムの設定値を表示します。自装置のエントリー、またはスタティックエントリーの場合は forever と表示されます。

3.5.8 show arp timeout

show arp timeout	
目的	ARP エージングタイムの設定値を表示します。
Command	show arp timeout [interface vlan VLAN-ID]
Parameter	interface vlan VLAN-ID（省略可能）：ARP エージングタイムの設定値を表示する VLAN インターフェースを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定の VLAN インターフェースを指定しない場合は、すべての VLAN インターフェースの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ARP エージングタイムの設定値を表示する方法を示します。

```
# show arp timeout

(1)             (2)
Interface       Timeout (minutes)
------------ -----------------
vlan1           240
------------ -----------------
Total Entries: 1
```

項番	説明
(1)	VLAN インターフェースを表示します。

項番	説明
(2)	ARP エージングタイムの設定値を表示します。

3.5.9 clear arp-cache

clear arp-cache	
目的	ARP テーブルからダイナミックエントリーを削除します。
Command	**clear arp-cache** {**all** | **interface** IF-ID | IP-ADDRESS}
Parameter	all：すべてのダイナミックエントリーを削除する場合に指定します。 interface IF-ID：ダイナミックエントリーをすべて削除する IPv4 インターフェースを、以下のパラメーターで指定します。 • mgmt 0：マネージメントポート指定 • vlan <1-4094>：VLAN インターフェース指定 IP-ADDRESS：ダイナミックエントリーを削除する IPv4 アドレスを指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべてのダイナミックエントリーを ARP テーブルから削除する方法を示します。

```
# clear arp-cache all
#
```

3.6 基本 IPv6 コマンド

基本 IPv6 関連の設定コマンドは以下のとおりです。

- ipv6 enable
- ipv6 address
- ipv6 address eui-64
- ipv6 address dhcp
- ipv6 address autoconfig
- ipv6 nd ns-interval
- ipv6 neighbor

基本 IPv6 関連の show／操作コマンドは以下のとおりです。

- show ipv6 interface
- show ipv6 general-prefix
- show ipv6 neighbors
- show ipv6 neighbors cache
- clear ipv6 neighbors

3.6.1 ipv6 enable

ipv6 enable	
目的	IPv6 機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ipv6 enable no ipv6 enable
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	本コマンドで IPv6 機能を有効にすると、対象 VLAN インターフェースに IPv6 リンクローカルアドレスが 1 つ自動的に割り当てられます。 以下のコマンドを設定すると、本設定も自動的に有効に設定されます。 • ipv6 address • ipv6 address eui-64 • ipv6 address dhcp • ipv6 address autoconfig ApresiaNP2500 シリーズの場合、本コマンドを有効にすると、ステートレス自動構成とルートタイプが SLAAC（Stateless address autoconfiguration）のデフォルトルートの登録（ipv6 address autoconfig default 設定相当の動作）も必ず有効になります。ApresiaNP2500 シリーズでは、本コマンドが有効設定の状態でステートレス自動構成を無効にすることはできません。
制限・注意	• ipv6 address コマンドなどの IPv6 アドレス設定が残っている状態では、本設定を削除して IPv6 機能を無効にできません。
バージョン	1.08.02

使用例：VLAN 1 インターフェースで、IPv6 を有効にする方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 enable
(config-if-vlan)#
```

3.6.2 ipv6 address

ipv6 address	
目的	VLAN インターフェースの IPv6 アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 address {IPV6-ADDRESS/LEN | PREFIX-NAME SUB-BITS/LEN | IPV6-ADDRESS link-local} no ipv6 address {IPV6-ADDRESS/LEN | PREFIX-NAME SUB-BITS/LEN | IPV6-ADDRESS link-local}
Parameter	IPV6-ADDRESS/LEN：IPv6 アドレスとプレフィックス長を指定します。 PREFIX-NAME SUB-BITS/LEN：DHCPv6-PD によるプレフィックス委譲によって取得したプレフィックスを使用して、IPv6 アドレスを指定します。 • PREFIX-NAME：プレフィックス名を指定します。 • SUB-BITS：委譲されたプレフィックス部以外の値を指定します。 • LEN：プレフィックス長を指定します。 IPV6-ADDRESS link-local：リンクローカルアドレスを指定します。
デフォルト	なし
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	ApresiaNP2500 シリーズでは、レイヤー3 用の VLAN インターフェースは 1 個だけ設定できます。デフォルトで VLAN 1 インターフェースが設定済みのため、別の VLAN を指定して VLAN インターフェースを作成する場合は、先に VLAN 1 インターフェースを削除 (no interface vlan 1) してから設定してください。 VLAN インターフェースで本設定を実施すると、ipv6 enable も自動的に設定されます。
制限・注意	• ApresiaNP2500 シリーズでは、手動で設定できる IPv6 アドレスは 1 つだけです。 • マネージメントポートでは IPv6 アドレスは設定できません。 • ApresiaNP2500 シリーズでは、設定できるレイヤー3 用の VLAN インターフェースは 1 個のため、VLAN 間のレイヤー3 中継はできません。
バージョン	1.08.02

使用例：VLAN 1 インターフェースで IPv6 アドレス 2001:db8::11/64 を設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 address 2001:db8::11/64
(config-if-vlan)#
```

使用例：VLAN 1 インターフェースで IPv6 アドレス 2001:db8::11/64 を削除する方法を示します。

```
# configure terminal
(config)# interface vlan 1
```

```
(config-if-vlan)# no ipv6 address 2001:db8::11/64
(config-if-vlan)#
```

使用例：VLAN 1 インターフェースで、DHCPv6-PD で取得したプレフィックスを使用して IPv6 アドレスを設定する方法を示します。この例では、DHCPv6-PD で「プレフィックス名：test-prefix、IPv6 プレフィックス：2001:db8:aaaa:bbbb::/64」を取得しているとします。そのため、この例では最終的には IPv6 アドレスとして 2001:db8:aaaa:bbbb::1111:2222/64 が設定されます。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 address test-prefix ::1111:2222/64
(config-if-vlan)#
```

使用例：VLAN 1 インターフェースで、DHCPv6-PD で取得したプレフィックスを使用して設定した IPv6 アドレス(test-prefix ::1111:2222/64)を削除する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# no ipv6 address test-prefix ::1111:2222/64
(config-if-vlan)#
```

3.6.3 ipv6 address eui-64

ipv6 address eui-64	
目的	EUI-64 形式のインターフェース ID を使用して、IPv6 アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 address IPV6-PREFIX/LEN eui-64 no ipv6 address IPV6-PREFIX/LEN eui-64
Parameter	IPV6-PREFIX：設定する IPv6 アドレスの、IPv6 プレフィックス部を指定します。 LEN：プレフィックス長を 64 以下で指定します。
デフォルト	なし
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	ApresiaNP2500 シリーズでは、レイヤー3 用の VLAN インターフェースは 1 個だけ設定できます。デフォルトで VLAN 1 インターフェースが設定済みのため、別の VLAN を指定して VLAN インターフェースを作成する場合は、先に VLAN 1 インターフェースを削除 (no interface vlan 1) してから設定してください。 本設定を実施すると、ipv6 enable も自動的に設定されます。
制限・注意	• ApresiaNP2500 シリーズでは、手動で設定できる IPv6 アドレスは 1 つだけです。 • マネージメントポートでは IPv6 アドレスは設定できません。 • ApresiaNP2500 シリーズでは、設定できるレイヤー3 用の VLAN インターフェースは 1 個のため、VLAN 間のレイヤー3 中継はできません。
バージョン	1.08.02

使用例：VLAN 1 インターフェースで、IPv6 プレフィックス部を「2001:db8:a:b」に指定し、EUI-64 形式のインターフェース ID を使用して IPv6 アドレスを設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 address 2001:db8:a:b::/64 eui-64
```

```
(config-if-vlan)#
```

3.6.4 ipv6 address dhcp

ipv6 address dhcp	
目的	DHCPv6 を使用して、IPv6 アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 address dhcp [rapid-commit] no ipv6 address dhcp
Parameter	rapid-commit（省略可能）：DHCPv6 の Rapid Commit オプションを有効にする場合に指定します。デフォルトは無効です。
デフォルト	なし
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	ApresiaNP2500 シリーズでは、レイヤー3 用の VLAN インターフェースは 1 個だけ設定できます。デフォルトで VLAN 1 インターフェースが設定済みのため、別の VLAN を指定して VLAN インターフェースを作成する場合は、先に VLAN 1 インターフェースを削除 (no interface vlan 1) してから設定してください。 DHCPv6 の Rapid Commit オプションを使用する場合は、DHCPv6 サーバーとクライアントの両方で有効にする必要があります。 本設定を実施すると、ipv6 enable も自動的に設定されます。
制限・注意	• マネージメントポートでは IPv6 アドレスは設定できません。
バージョン	1.08.02

使用例：VLAN 1 インターフェースで、DHCPv6 で IPv6 アドレスを設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 address dhcp
(config-if-vlan)#
```

3.6.5 ipv6 address autoconfig

ipv6 address autoconfig	
目的	ステートレス自動構成を使用して、IPv6 アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 address autoconfig [default] no ipv6 address autoconfig
Parameter	default（省略可能）：Router Advertisement に基づいてデフォルトルートを登録する場合に指定します。
デフォルト	なし
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	ApresiaNP2500 シリーズでは、レイヤー3 用の VLAN インターフェースは 1 個だけ設定できます。デフォルトで VLAN 1 インターフェースが設定済みのため、別の VLAN を指定して VLAN インターフェースを作成する場合は、先に VLAN 1 インターフェースを削除 (no interface vlan 1) してから設定してください。

ipv6 address autoconfig	
	ApresiaNP2500 シリーズの場合、本コマンドの有無にかかわらず、ipv6 enable コマンドを有効にすると、ステートレス自動構成とルートタイプが SLAAC（Stateless address autoconfiguration）のデフォルトルートの登録（ipv6 address autoconfig default 設定相当の動作）も必ず有効になります。ApresiaNP2500 シリーズでは、ipv6 enable コマンドが有効設定の状態でステートレス自動構成を無効にすることはできません。 本設定を実施すると、ipv6 enable も自動的に設定されます。
制限・注意	• マネージメントポートでは IPv6 アドレスは設定できません。
バージョン	1.08.02

使用例：VLAN 1 インターフェースで、ステートレス自動構成で IPv6 アドレスを設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 address autoconfig
(config-if-vlan)#
```

3.6.6 ipv6 nd ns-interval

ipv6 nd ns-interval	
目的	NS メッセージを再送信する間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 nd ns-interval MILLISECONDS no ipv6 nd ns-interval
Parameter	MILLISECONDS：NS メッセージを再送信する間隔を、0～3,600,000 ミリ秒（1000 ミリ秒単位）の範囲で指定します。
デフォルト	設定値は 0 で、実動作は 1000 ミリ秒（1 秒）
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	設定値は show ipv6 interface コマンドの"NS messages retransmit interval"項目で確認できます。デフォルトの場合は"0 milliseconds"と表示されますが、実動作は 1000 ミリ秒（1 秒）で動作します。
制限・注意	• ipv6 address コマンドと ipv6 nd ns-interval コマンドを同時に設定する場合は、5 秒あけてから設定してください。
バージョン	1.08.02

使用例：IPv6 NS メッセージの再送信間隔を、6 秒に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 nd ns-interval 6000
(config-if-vlan)#
```

3.6.7 ipv6 neighbor

ipv6 neighbor	
目的	スタティック IPv6 ネイバーキャッシュエントリーを作成します。設定を削除する場

ipv6 neighbor	
	合は、no 形式のコマンドを使用します。
Command	ipv6 neighbor IPV6-ADDRESS IF-NAME MAC-ADDRESS no ipv6 neighbor IPV6-ADDRESS IF-NAME
Parameter	IPV6-ADDRESS：スタティック IPv6 ネイバーキャッシュエントリーの IPv6 アドレスを指定します。 IF-NAME：スタティック IPv6 ネイバーキャッシュエントリーの VLAN インターフェース（vlan と VLAN ID の間を空けない形式）を指定します。 MAC-ADDRESS：スタティック IPv6 ネイバーキャッシュエントリーの MAC アドレスを、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX）
デフォルト	スタティックエントリーの設定なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	到達可能な検出プロセスは、スタティック IPv6 ネイバーキャッシュエントリーには適用されません。
制限・注意	• スタティック IPv6 ネイバーキャッシュエントリーは最大 64 個設定できます。設定する場合は mac-address-table static コマンドで対応するスタティック MAC アドレスエントリーも設定してください。 • スタティック IPv6 ネイバーキャッシュエントリーを登録した VLAN インターフェースがダウン状態でも、show コマンドでエントリーは表示されます。
バージョン	1.08.02

使用例：スタティック IPv6 ネイバーキャッシュエントリー「IPv6=2001:db8::101、VLAN 1 インターフェース、MAC=00:00:5E:00:53:11」を設定する方法を示します。

```
# configure terminal
(config)# ipv6 neighbor 2001:db8::101 vlan1 00-00-5e-00-53-11
(config)#
```

3.6.8 show ipv6 interface

show ipv6 interface	
目的	IPv6 インターフェース情報を表示します。
Command	show ipv6 interface [IF-ID] [brief]
Parameter	IF-ID（省略可能）：IPv6 インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定 brief（省略可能）：IPv6 インターフェースの概要情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定の IPv6 インターフェースを指定しない場合は、すべての IPv6 インターフェース

show ipv6 interface	
	の情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：IPv6 インターフェースの概要情報を表示する方法を示します。

```
# show ipv6 interface brief
 (1)           (2)
vlan1 is up, link status is up
    fe80::240:66ff:fef2:821f  ...(3)
    2001:db8:1:1::1001

Total Entries: 1
```

項番	説明
(1)	VLAN インターフェースの有効／無効を表示します。 up：有効 (no shutdown 設定時) down：無効 (shutdown 設定時)
(2)	VLAN インターフェースのリンク状態 (up／down) を表示します。
(3)	IPv6 アドレスを表示します。

使用例：IPv6 インターフェース情報を表示する方法を示します。

```
# show ipv6 interface
 (1)           (2)
vlan1 is up, link status is up
  IPv6 is enabled,  ...(3)
  Link-local address:  ...(4)
      fe80::240:66ff:fef2:821f
  Global unicast address:  ...(5)
      2001:db8:1:1::1001/64 (Manual)
  NS messages retransmit interval is 0 milliseconds  ...(6)

Total Entries: 1
```

項番	説明
(1)	VLAN インターフェースの有効／無効を表示します。 up：有効 (no shutdown 設定時) down：無効 (shutdown 設定時)
(2)	VLAN インターフェースのリンク状態 (up／down) を表示します。
(3)	IPv6 が有効(enabled)なことを示します。
(4)	リンクローカルアドレスを表示します。
(5)	グローバルユニキャストアドレスを表示します。 (Manual)：手動設定 (Manual-EUI)：eui-64 オプションを使用して設定 (Stateless)：ステートレスアドレス自動設定 (DHCPv6)：DHCPv6 によるアドレス設定 (DHCPv6 PD)：DHCPv6 プレフィックス委譲によるアドレス設定
(6)	IPv6 インターフェースの NS 再送信間隔を表示します。

3.6.9 show ipv6 general-prefix

show ipv6 general-prefix	
目的	DHCPv6-PD によるプレフィックス委譲によって取得したプレフィックス情報を表示します。
Command	show ipv6 general-prefix [PREFIX-NAME]
Parameter	PREFIX-NAME（省略可能）：表示するプレフィックス名を指定します。指定しない場合は、すべてのプレフィックスが表示されます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCPv6-PD によるプレフィックス委譲によって取得したプレフィックス情報を表示する方法を示します。

```
# show ipv6 general-prefix

IPv6 prefix test-pd ...(1)
 Acquired via DHCPv6 PD ...(2)
   vlan1: 2001:db8:1111:1::/64
       Valid lifetime 2592000, preferred lifetime 604800
   Apply to interfaces ...(3)
     vlan1: ::1:2:3:4/64


Total Entries: 1
```

項番	説明
(1)	プレフィックス名を表示します。
(2)	DHCPv6-PD によって委譲されたプレフィックス情報を表示します。
(3)	DHCPv6-PD によって委譲されたプレフィックスを使用して設定した IPv6 アドレス情報を表示します。

3.6.10 show ipv6 neighbors

show ipv6 neighbors	
目的	IPv6 ネイバー情報を表示します。
Command	show ipv6 neighbors [IF-NAME] [IPV6-ADDRESS]
Parameter	IF-NAME（省略可能）：IPv6 ネイバーキャッシュエントリーを表示する VLAN インターフェース（vlan と VLAN ID の間を空けない形式）を指定します。 IPV6-ADDRESS（省略可能）：IPv6 ネイバーキャッシュエントリーを表示する IPv6 アドレスを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	パラメーター省略時は、すべてのエントリーが表示されます。

show ipv6 neighbors	
制限・注意	-
バージョン	1.08.02

使用例：IPv6 ネイバーキャッシュエントリーを表示する方法を示します。

```
# show ipv6 neighbors
 (1)                                    (2)                (3)        (4)   (5)
IPv6 Address                            Link-Layer Addr    Interface  Type  State
--------------------------------------- ------------------ ---------- ----- -----
2001:db8:11:0:a:a:a:a                   00-00-11-11-22-22  vlan11     D     REACH
fe80::200:11ff:fe11:2222                00-00-11-11-22-22  vlan11     D     REACH

Total Entries: 2
```

項番	説明
(1)	IPv6 アドレスを表示します。
(2)	MAC アドレスを表示します。
(3)	エントリーを学習した IPv6 インターフェースを表示します。
(4)	エントリーの種類（D：ダイナミック／S：スタティック）を表示します。
(5)	エントリーの状態を表示します。 INCMP（Incomplete/未完了）：エントリーに対してアドレス解決を実行中だが、対応するネイバーアドバタイズメッセージを受信していない REACH（Reachable/到達可能）：対応するネイバーアドバタイズメッセージを受信したが、到達可能時間（ミリ秒単位）が経過していない（ネイバーが正常に機能していた） STALE：最後の確認を受信した後に経過した時間が、到達可能時間（ミリ秒単位）を超過 PROBE：到達可能性を確認するための、近隣要請メッセージの送信中 DELAY：到達可能であることが知られていないネイバーに、最近トラフィックが送信された。上位レイヤープロトコルがネイバーの到達可能性を確認している間は、ネイバーを調査しない

3.6.11 show ipv6 neighbors cache

show ipv6 neighbors cache	
目的	IPv6 ネイバーキャッシュテーブルを表示します。
Command	show ipv6 neighbors cache [IPV6-ADDRESS | interface IF-ID]
Parameter	IPV6-ADDRESS（省略可能）：IPv6 ネイバーキャッシュエントリーを表示する IPv6 アドレスを指定します。 interface IF-ID（省略可能）：エントリーを表示するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 • vlan <1-4094>：VLAN インターフェース指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	パラメーター省略時は、すべてのエントリーが表示されます。
制限・注意	• 登録済みの IPv6 ネイバーキャッシュエントリーにおいて、リンクダウンを伴わない

show ipv6 neighbors cache	
	ポート間移動が発生した場合、MAC アドレスを再学習してから数秒後に IPv6 ネイバーキャッシュエントリーの送信先インターフェースの更新が行われます。なお、MAC アドレスや IPv6 ネイバーキャッシュエントリーの登録数が多い環境では、この更新時間がより長くなることがあります。 • 以下のエントリーは本コマンドでは表示されません。 • リンクローカルアドレスのエントリー • 状態が到達可能（Reachable）以外のエントリー • 対応する MAC アドレスが MAC アドレステーブルに登録されていないスタティック IPv6 ネイバーキャッシュエントリー
バージョン	1.08.02

使用例：IPv6 ネイバーキャッシュエントリーを表示する方法を示します。

```
# show ipv6 neighbors cache
(1)                                     (2)   (3)                 (4)      (5)
IPv6 Address                            VID   Link-Layer Addr     I/F      State
--------------------------------------- ----- ------------------ -------- -----
2001:db8:11:0:a:a:a:a                     11  00-00-11-11-22-22 1/0/1    REACH
2001:db8:11:0:1:2:3:4                     11  FC-6D-D1-F2-82-1F CPU

Total Entries: 2
```

項番	説明
(1)	IPv6 アドレスを表示します。
(2)	VLAN ID を表示します。
(3)	MAC アドレスを表示します。
(4)	エントリーを学習したインターフェース ID（物理ポート、ポートチャネル）を表示します。自装置のエントリーの場合は CPU と表示されます。
(5)	エントリーの状態を表示します。

3.6.12 clear ipv6 neighbors

clear ipv6 neighbors	
目的	IPv6 ネイバーキャッシュのダイナミックエントリーを削除します。
Command	clear ipv6 neighbors {all | interface IF-ID}
Parameter	all：インターフェースに関連付けられているすべての IPv6 ネイバーキャッシュのダイナミックエントリーを削除する場合に指定します。 interface IF-ID：ダイナミックエントリーをすべて削除する IPv6 インターフェースを、以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 インターフェースに関連付けられている、IPv6 ネイバーキャッシュのダイナミックエントリーを削除する方法を示します。

```
# clear ipv6 neighbors interface vlan 1
#
```

3.7 IP ユーティリティーコマンド

IP ユーティリティー関連のコマンドは以下のとおりです。

- ping access-class
- ping
- traceroute

3.7.1 ping access-class

ping access-class	
目的	自装置宛ての ping のアクセス制限を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ping access-class ACL-NAME no ping access-class ACL-NAME
Parameter	ACL-NAME：アクセス制限で使用する標準 IP アクセスリスト、または標準 IPv6 アクセスリストを指定します。
デフォルト	アクセス制限の設定なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを設定すると、自装置宛て ICMP リクエストパケットの送信元 IPv4/IPv6 アドレスが、指定したアクセスリストを基にチェックされるようになります。IPv4 アドレス用に 1 個、IPv6 アドレス用に 1 個の、最大 2 個まで設定できます。 <標準 IP アクセスリスト指定の場合> • 自装置宛て ICMP リクエストパケットを許可する IPv4 アドレスを permit ルールの「送信元 IP アドレス」条件で、拒否する IPv4 アドレスを deny ルールの「送信元 IP アドレス」条件で指定します。 • いずれのルールにもマッチしない場合は、拒否されます。 <標準 IPv6 アクセスリスト指定の場合> • 自装置宛て ICMP リクエストパケットを許可する IPv6 アドレスを permit ルールの「送信元 IPv6 アドレス」条件で、拒否する IPv6 アドレスを deny ルールの「送信元 IPv6 アドレス」条件で指定します。 • いずれのルールにもマッチしない場合は、拒否されます。 いずれの場合も、「宛先 IP アドレス」「宛先 IPv6 アドレス」条件は、any で設定する必要があります。any 以外で設定した場合は、そのルールは無効になります。なお、入力を省略した場合は any で設定されます。
制限・注意	• 説明に記載されている種別以外のアクセスリストを指定して使用できません。 • IPv4 アドレス用の標準 IP アクセスリストを 2 つ設定した場合は、最初の 1 つのみが有効となります。同様に、IPv6 アドレス用の標準 IPv6 アクセスリストを 2 つ設定した場合は、最初の 1 つのみが有効となります。 • すでに 2 つのアクセスリストを適用している状態では、新しいアクセスリストを指定して設定できません。 • 本設定で指定する標準 IP アクセスリスト、または標準 IPv6 アクセスリストでは、装置のハードウェアリソースを使用しません。
バージョン	1.08.02

使用例：以下の内容で自装置宛ての ping のアクセス制限を有効にする方法を示します。アクセス制限用の標準 IP アクセスリスト名は「ping-permit-list」とします。

- 192.0.2.0/24 からの ping を許可
- 10.0.0.100/32 からの ping を許可
- それ以外からの ping を拒否

```
# configure terminal
(config)# ip access-list ping-permit-list
(config-ip-acl)# permit 192.0.2.0 0.0.0.255
(config-ip-acl)# permit host 10.0.0.100
(config-ip-acl)# exit
(config)#
(config)# ping access-class ping-permit-list
(config)#
```

使用例：以下の内容で自装置宛ての ping のアクセス制限を有効にする方法を示します。アクセス制限用の標準 IP アクセスリスト名は「ping-list」とします。

- ルール 10：192.0.2.100/32 からの ping を許可
- ルール 20：192.0.2.100 以外の 192.0.2.0/24 からの ping を拒否
- ルール 100：それ以外からの ping を許可

```
# configure terminal
(config)# ip access-list ping-list
(config-ip-acl)# 10 permit host 192.0.2.100
(config-ip-acl)# 20 deny 192.0.2.0 0.0.0.255
(config-ip-acl)# 100 permit any
(config-ip-acl)# exit
(config)#
(config)# ping access-class ping-list
(config)#
```

3.7.2 ping

ping	
目的	指定した宛先に対して ping を実施し、宛先への到達性を確認します。
Command	**ping** {[**ip**] IP-ADDRESS | [**ipv6**] IPV6-ADDRESS} [**count** VALUE] [**timeout** SECONDS] [**source** {IP-ADDRESS | IPV6-ADDRESS}] [**size** LENGTH] [**interval** SECONDS]
Parameter	[ip] IP-ADDRESS：宛先 IPv4 アドレスを指定します。 [ipv6] IPV6-ADDRESS：宛先 IPv6 アドレスを指定します。リンクローカルアドレスまたはマルチキャストアドレスの場合は、「IPV6-ADDRESS%IF-NAME」のように VLAN インターフェース（vlan と VLAN ID の間を空けない形式）を付加して指定します。 count VALUE（省略可能）：送信回数を 1～255 回の範囲で指定します。 timeout SECONDS（省略可能）：応答タイムアウト時間を 1～99 秒の範囲で指定します。 source {IP-ADDRESS | IPV6-ADDRESS}（省略可能）：ping パケットの送信元 IPv4 アドレス、または送信元 IPv6 アドレスを指定します。設定済みの IP アドレスを指定する必要があります。 size LENGTH（省略可能）：ping パケットのデータ部のサイズを 32～1500 バイトの

ping	
	範囲で指定します。 interval SECONDS（省略可能）：送信間隔を 1～3600 秒の範囲で指定します。
デフォルト	送信回数：5 回 応答タイムアウト時間：1 秒 データ部のサイズ：IPv4 の場合は 32 バイト、IPv6 の場合は 100 バイト 送信間隔：1 秒
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	ping を中断する場合は、Ctrl+C キーを押してください。

制限・注意	• VLAN インターフェース、またはマネージメントポートからルーター越えでアクセス可能なネットワークに対して directed broadcast アドレス宛ての ping を実施しても、応答を表示できません。そのため、そのような宛先に対しては実施しないでください。
	• マネージメントポートに直接接続されたネットワークに対して directed broadcast アドレス宛ての ping を実施しても、すべての応答を表示できません。一部の応答のみ表示されます。
	• デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在する端末を指定して本コマンドを実施すると、ping パケットは VLAN インターフェースとマネージメントポートの両方から送信されます。どちらか一方のみから送信する場合は、source オプションで送信元 IPv4 アドレスを指定してください。
	  • 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク
	  • 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク
	• コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。

バージョン	1.08.02

使用例：IPv4 アドレス 192.0.2.200 宛てに ping を実施する方法を示します。

```
# ping 192.0.2.200

Reply from 192.0.2.200, bytes=32, time=10ms
Reply from 192.0.2.200, bytes=32, time<10ms
Reply from 192.0.2.200, bytes=32, time<10ms
Reply from 192.0.2.200, bytes=32, time<10ms
Reply from 192.0.2.200, bytes=32, time<10ms

 Ping Statistics for 192.0.2.200
 Packets: Sent =5, Received =5, Lost =0
```

使用例：IPv6 マルチキャストアドレス ff02::1（VLAN 110 インターフェース経由）宛てに ping（送信回数=2 回指定）を実施する方法を示します。

```
# ping ipv6 ff02::1%vlan110 count 2

Reply to request 1 from fe80::240:66ff:fea8:cfa2, bytes=100, time<10 ms
Reply to request 1 from fe80::201:2ff:fe03:400, bytes=100, time<10 ms
```

```
  Request 1  received 2  replies.
Reply to request 2 from fe80::240:66ff:fea8:cfa2, bytes=100, time<10 ms
Reply to request 2 from fe80::201:2ff:fe03:400, bytes=100, time<10 ms
  Request 2  received 2  replies.

 Ping Statistics for ff02::1
 Packets: Sent =2, Received =4, Lost =0
```

3.7.3 traceroute

traceroute	
目的	指定した宛先に対して traceroute を実施し、宛先までの IP ネットワークの通信経路を確認します。
Command	**traceroute** {[**ip**] IP-ADDRESS | [**ipv6**] IPV6-ADDRESS} [**probe** VALUE] [**timeout** SECONDS] [**max-ttl** VALUE] [**port** UDP-PORT]
Parameter	[ip] IP-ADDRESS：宛先 IPv4 アドレスを指定します。 [ipv6] IPV6-ADDRESS：宛先 IPv6 アドレスを指定します。 probe VALUE（省略可能）：同一 TTL 値(IPv4)または同一ホップリミット値(IPv6)あたりのプローブ数を 1～1000 回の範囲で指定します。 timeout SECONDS（省略可能）：応答タイムアウト時間を 1～65,535 秒の範囲で指定します。 max-ttl VALUE（省略可能）：送信する UDP パケットの最大 TTL 値(IPv4)または最大ホップリミット値(IPv6)を 1～255 の範囲で指定します。指定した最大値まで実行しても宛先に到達しない場合は、traceroute は終了します。 port UDP-PORT（省略可能）：送信する UDP パケットの宛先 UDP ポート番号のベース値を 1～65535 の範囲で指定します。宛先 UDP ポート番号は traceroute を実行すると指定したポート番号がセットされます。同一 traceroute の実行内で UDP パケットを送信するたびに、加算したポート番号がセットされます。
デフォルト	同一 TTL 値(IPv4)または同一ホップリミット値(IPv6)あたりのプローブ数：3 回 応答タイムアウト時間：5 秒 最大 TTL 値(IPv4)または最大ホップリミット値(IPv6)：30 宛先 UDP ポート番号のベースの値：33434
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	traceroute の実行を中断する場合は、Ctrl+C キーを押します。
制限・注意	• traceroute を同時に使用できる最大セッション数は 3 個です。 • デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在する端末を指定して本コマンドを実施する場合、宛先判定にはデフォルトルートよりもデフォルトゲートウェイ設定が優先され、宛先(1)(2)のいずれの場合も traceroute パケットはマネージメントポートから送信されます。 　• 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク 　• 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク • そのため、このような状況では宛先(1)への実施が失敗します。ApresiaNP2500 シ

traceroute	
	リーズでは、このような状況にならないように、VLAN インターフェース経由、もしくはマネージメントポート経由のどちらかのみで管理することを推奨します。 • コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。
バージョン	1.08.02

使用例：IPv4 アドレス 192.0.2.100 宛てに traceroute を実施する方法を示します。

```
# traceroute 192.0.2.100

 <10 ms  172.16.10.253
 <10 ms  172.16.10.253
 <10 ms  172.16.10.253
 <10 ms  192.168.20.254
 <10 ms  192.168.20.254
 <10 ms  192.168.20.254
 <10 ms  192.0.2.100

Trace complete.
```

使用例：IPv6 アドレス 2001:db8:4::5555 宛てに traceroute を実施する方法を示します。

```
# traceroute 2001:db8:4::5555

 <10 ms  2001:db8:2::2222
 <10 ms  2001:db8:2::2222
 <10 ms  2001:db8:2::2222
 <10 ms  2001:db8:3::abcd
 <10 ms  2001:db8:3::abcd
 <10 ms  2001:db8:3::abcd
 <10 ms  2001:db8:4::5555

Trace complete.
```

3.8 Gratuitous ARP コマンド

Gratuitous ARP 関連のコマンドは以下のとおりです。

- ip arp gratuitous
- ip gratuitous-arps
- arp gratuitous-send

3.8.1 ip arp gratuitous

ip arp gratuitous	
目的	ARP テーブルでの Gratuitous ARP（GARP）パケットの学習を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip arp gratuitous no ip arp gratuitous
Parameter	なし
デフォルト	有効（ip arp gratuitous）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ARP テーブルでの GARP パケットの学習を無効にする方法を示します。

```
# configure terminal
(config)# no ip arp gratuitous
(config)#
```

3.8.2 ip gratuitous-arps

ip gratuitous-arps	
目的	GARP リクエストの送信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip gratuitous-arps [dad-reply] no ip gratuitous-arps [dad-reply]
Parameter	dad-reply（省略可能）：IP アドレスの重複が検出されたときに GARP リクエストを送信する場合に指定します。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	GARP リクエストは、Sender Protocol Address フィールドと Target Protocol Address フィールドの両方が、送信装置の IP アドレスに設定されている ARP リクエストパケットです。宛先 MAC アドレスはブロードキャストアドレスです。 GARP リクエスト送信の有効／無効は、ip gratuitous-arps コマンドで設定します。GARP リクエストの送信を有効にすると、IP インターフェースのリンクアップ時、または IP アドレスの設定／変更時に、GARP リクエストが送信されます。

ip gratuitous-arps	
	さらに、重複 IP アドレスからの ARP リクエストを検知した場合に GARP リクエストの送信を有効にするには、ip gratuitous-arps dad-reply コマンドを設定します。 なお、ip gratuitous-arps dad-reply だけを設定した状態では動作しないため、dad-reply オプションを使用する場合は ip gratuitous-arps コマンドで GARP リクエストの送信も有効にしてください。
制限・注意	• dad-reply オプションを使用している場合で重複 IP アドレスからの ARP リクエストを受信し続けている状況では、本装置が送信するその重複 IP アドレスの GARP リクエストは 1 秒ごとに送信されます。 • 構成情報では、ip gratuitous-arps と ip gratuitous-arps dad-reply は別に表示されます。設定を削除する場合は、それぞれの no 形式のコマンドを使用して削除する必要があります。
バージョン	1.08.02

使用例：GARP リクエストの送信を有効にする方法を示します。

```
# configure terminal
(config)# ip gratuitous-arps
(config)#
```

3.8.3 arp gratuitous-send

arp gratuitous-send	
目的	GARP リクエストを定期的に送信する間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	arp gratuitous-send interval SECONDS no arp gratuitous-send
Parameter	SECONDS：GARP リクエストの送信間隔を 1～3,600 秒の範囲で指定します。
デフォルト	定期的に送信する間隔は未設定
モード	インターフェース設定モード（vlan, mgmt）
特権レベル	レベル：12
ガイドライン	本設定を使用する場合は、ip gratuitous-arps コマンドで GARP リクエストの送信を有効にする必要があります。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 100 インターフェースから GARP リクエストを定期的に送信する間隔を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# arp gratuitous-send interval 300
(config-if-vlan)#
```

3.9 システムファイル管理コマンド

ポート設定関連の設定コマンドは以下のとおりです。

- boot image
- boot config
- ip tftp source-interface
- ip ftp source-interface
- ip ssh source-interface

システムファイル管理関連の show／操作コマンドは以下のとおりです。

- show boot
- show running-config
- show startup-config
- show config differences
- backup clone
- write
- copy primary-config secondary-config
- reboot
- copy boot
- erase boot
- configure replace
- copy
- backup
- restore
- clear running-config
- reset system

3.9.1 boot image

boot image	
目的	次回起動時に、ブートイメージファイルとして使用するファイルを指定します。
Command	boot image [check] URL [primary | secondary]
Parameter	check（省略可能）：指定したブートイメージファイルのファームウェア情報を表示する場合に指定します。情報には、バージョン番号とモデルの説明が含まれます。 URL：ブートイメージファイルとして使用するファイルの URL を指定します。以下のいずれかの書式を使用します。 <対象が非スタック装置、およびスタックマスター装置の場合> • c:/URL：ローカルフラッシュ上のファイル指定（例：c:/switch-image.had） • d:/URL：SD カード上のファイル指定（例：d:/switch-image.had） <対象がスタックマスター以外の装置の場合> • unitX:/c:/URL（X はボックス ID）：ローカルフラッシュ上のファイル指定（例：ボックス ID が 2 の場合は unit2:/c:/switch-image.had） • unitX:/d:/URL（X はボックス ID）：SD カード上のファイル指定（例：ボックス ID が 2 の場合は unit2:/d:/switch-image.had） primary（省略可能）：プライマリーブートイメージファイルとして使用する場合に指

boot image	
	定します。 secondary（省略可能）：セカンダリーブートイメージファイルとして使用する場合に指定します。
デフォルト	ブートイメージファイルあり
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	primary および secondary のいずれも指定しない場合、プライマリーブートイメージファイルとして使用されます。 プライマリーブートイメージファイルまたはセカンダリーブートイメージファイルとしてファイルを設定すると、モデルとチェックサムが検証され、ファイルが有効なイメージファイルであることが確認されます。 check パラメーターを指定して実行すると、有効なイメージファイルの場合はファームウェア情報を表示して設定されます。 boot image コマンドを実行するとすぐに、指定したファイルが装置の NVRAM に格納されます。これは startup-config とは別の領域です。 装置が起動すると、最初にプライマリーブートイメージファイルが読み込まれます。プライマリーブートイメージファイルが読み込めない場合は、セカンダリーブートイメージファイルが読み込まれます。セカンダリーブートイメージファイルも読み込めない場合、ローカルフラッシュ内で有効なブートイメージファイルと判定されており、かつ最新の日時であるファイルが使用されます。
制限・注意	• ローカルフラッシュには、有効なブートイメージファイルを必ず 1 つは残しておいてください。 • ローカルフラッシュのブートスクリプトで、SD カード上のブートイメージファイルを指定する場合は、SD カードを取り外さないでください。この状態で SD カードを取り外すと、ブートイメージファイルにはローカルフラッシュ内で有効なブートイメージファイルと判定されたファイルのうち、最新日時のファイルが適用されます。
バージョン	1.08.02

使用例：装置のローカルフラッシュ上の「switch-image.had」を、プライマリーブートイメージファイルとして使用する方法を示します。

```
# configure terminal
(config)# boot image c:/switch-image.had primary
(config)#
```

使用例：SD カード上の「switch-image.had」を、プライマリーブートイメージファイルとして使用する方法を示します。

```
# configure terminal
(config)# boot image d:/switch-image.had primary
(config)#
```

使用例：スタック構成において、対象がボックス ID 2 の装置（スタックマスター以外）で、その装置のローカルフラッシュ上の「switch-image.had」を、プライマリーブートイメージファイルとして使用する方法を示します。

```
# configure terminal
```

```
(config)# boot image unit2:/c:/switch-image.had primary
(config)#
```

使用例：check パラメーター指定で本コマンドを実行する方法を示します。この例では「c:/switch-image.had」が有効なイメージファイルで、ファームウェア情報が表示されて、プライマリーブートイメージファイルとして設定されます。

```
# configure terminal
(config)# boot image check c:/switch-image.had

----------------------
Image information
----------------------
Version: 1.08.02
Description: APRESIA Systems, Ltd Gigabit Ethernet Switch

(config)#
```

使用例：check パラメーター指定で本コマンドを実行する方法を示します。この例では「c:/switch-image.had」が無効なイメージファイルで、エラーメッセージが表示されています。

```
# configure terminal
(config)# boot image check c:/switch-image.had

 ERROR:Invalid firmware image.
(config)#
```

3.9.2 boot config

boot config	
目的	次回起動時に、構成情報として使用するファイルを指定します。
Command	boot config URL [primary | secondary]
Parameter	URL：startup-config として使用するファイルの URL を指定します。以下のいずれかの書式を使用します。 <対象が非スタック装置、およびスタックマスター装置の場合> • c:/URL：ローカルフラッシュ上のファイル指定（例：c:/switch-config.cfg） • d:/URL：SD カード上のファイル指定（例：d:/switch-config.cfg） <対象がスタックマスター以外の装置の場合> • unitX:/c:/URL（X はボックス ID）：ローカルフラッシュ上のファイル指定（例：ボックス ID が 2 の場合は unit2:/c:/switch-config.cfg） • unitX:/d:/URL（X はボックス ID）：SD カード上のファイル指定（例：ボックス ID が 2 の場合は unit2:/d:/switch-config.cfg） primary（省略可能）：プライマリー構成情報として使用する場合に指定します。 secondary（省略可能）：セカンダリー構成情報として使用する場合に指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	primary および secondary のいずれも指定しない場合、プライマリー構成情報として使用されます。 boot config コマンドを実行するとすぐに、指定したファイルが装置の NVRAM に格納されます。これは startup-config とは別の領域です。

boot config	
	装置が起動すると、最初にプライマリー構成情報が読み込まれます。プライマリー構成情報が読み込めない場合は、セカンダリー構成情報が読み込まれます。セカンダリー構成情報も読み込めない場合、ローカルフラッシュ内で有効な構成情報と判定されており、かつ最新の日時であるファイルが使用されます。 工場出荷状態では以下のように指定されています。 • プライマリー構成情報のファイル：c:/primary.cfg • セカンダリー構成情報のファイル：c:/secondary.cfg
制限・注意	• 運用中の装置が工場出荷時の構成情報で起動した場合、ループを含む重大な障害につながる恐れがあるため、構成情報はプライマリーとセカンダリーの双方を指定し、保存してください。 • ローカルフラッシュのブートスクリプトで、SD カード上の構成情報ファイルを指定する場合は、SD カードを取り外さないでください。この状態で SD カードを取り外すと、startup-config にはローカルフラッシュ内で有効な構成情報と判定されたファイルのうち、最新日時のファイルが適用されます。
バージョン	1.08.02

使用例：startup-config ファイルとしてファイル「switch-config.cfg」を設定する方法を示します。

```
# configure terminal
(config)# boot config c:/switch-config.cfg
(config)#
```

使用例：装置のローカルフラッシュ上の「switch-config.cfg」を、プライマリー構成情報として使用する方法を示します。

```
# configure terminal
(config)# boot config c:/switch-config.cfg primary
(config)#
```

使用例：SD カード上の「switch-config.cfg」を、プライマリー構成情報として使用する方法を示します。

```
# configure terminal
(config)# boot config d:/switch-config.cfg primary
(config)#
```

使用例：スタック構成において、対象がボックス ID 2 の装置（スタックマスター以外）で、その装置のローカルフラッシュ上の「switch-config.cfg」を、プライマリー構成情報として使用する方法を示します。

```
# configure terminal
(config)# boot config unit2:/c:/switch-config.cfg primary
(config)#
```

3.9.3 ip tftp source-interface

ip tftp source-interface	
目的	TFTP パケットの送信元 IP アドレスとして使用するインターフェースを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip tftp source-interface IF-ID no ip tftp source-interface

ip tftp source-interface	
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定
デフォルト	最も近いインターフェースの IP アドレスを使用
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• マネージメントポート経由で管理する場合は、vlan パラメーターを指定して本コマンドを設定しないでください。 • VLAN インターフェース経由で管理する場合は、mgmt パラメーターを指定して本コマンドを設定しないでください。
バージョン	1.08.02

使用例：TFTP パケットの送信元 IP アドレスとして、VLAN 1 インターフェースの IP アドレスを設定する方法を示します。

```
# configure terminal
(config)# ip tftp source-interface vlan 1
(config)#
```

3.9.4 ip ftp source-interface

ip ftp source-interface	
目的	FTP パケットの送信元 IP アドレスとして使用するインターフェースを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip ftp source-interface IF-ID no ip ftp source-interface
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定
デフォルト	最も近いインターフェースの IP アドレスを使用
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• マネージメントポート経由で管理する場合は、vlan パラメーターを指定して本コマンドを設定しないでください。 • VLAN インターフェース経由で管理する場合は、mgmt パラメーターを指定して本コマンドを設定しないでください。
バージョン	1.08.02

使用例：FTP パケットの送信元 IP アドレスとして、VLAN 1 インターフェースの IP アドレスを設定する方法を示します。

```
# configure terminal
(config)# ip ftp source-interface vlan 1
(config)#
```

3.9.5 ip ssh source-interface

ip ssh source-interface	
目的	SFTP または SSH クライアント使用時に、SSH パケットの送信元 IP アドレスとして使用するインターフェースを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip ssh source-interface IF-ID no ip ssh source-interface
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定
デフォルト	最も近いインターフェースの IP アドレスを使用
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 本コマンドは IPv6 アドレスに対しては未サポートです。IPv6 アドレスを指定して SFTP または SSH クライアントを使用する場合に、本コマンドを設定しても送信元 IPv6 アドレスは変更されません。 • マネージメントポート経由で管理する場合は、vlan パラメーターを指定して本コマンドを設定しないでください。 • VLAN インターフェース経由で管理する場合は、mgmt パラメーターを指定して本コマンドを設定しないでください。
バージョン	1.13.01

使用例：SFTP または SSH クライアント使用時に、SSH パケットの送信元 IP アドレスとして、VLAN 1 インターフェースの IP アドレスを設定する方法を示します。

```
# configure terminal
(config)# ip ssh source-interface vlan 1
(config)#
```

3.9.6 show boot

show boot	
目的	起動時に使用する構成情報、およびブートイメージファイルを表示します。
Command	show boot [unit UNIT-ID]
Parameter	unit UNIT-ID（省略可能）：装置のボックス ID を 1～4 の範囲で指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	SD カードブート利用時（ブートスクリプト「apresia-loader.conf」が保存されている SD カードを挿入している場合）には、SD カードブート用のブートスクリプト情報も表示されます。 (Configured)または(SD Card)の前に付与されて表示されるアスタリスク(*)は、どのブートイメージファイル設定で起動したのかを示します。 • boot image コマンドで指定した Primary boot image または Secondary

show boot	
	boot image で起動した場合は、(Configured)の前にアスタリスク(*)が付与されて表示されます。 • SD カードブート用の Primary boot image (通常は SD カードに保存される apresia-software.had) で起動した場合は、(SD Card)の前にアスタリスク(*)が付与されて表示されます。 スタック構成で特定のボックス ID を指定しない場合は、すべてのスタックメンバーの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：起動時に使用する構成情報、およびブートイメージファイルを表示する方法を示します。この例では「apresia-loader.conf」が保存されている SD カードが挿入されています。

```
# show boot

Unit 1 ...(1)
(Configured)
 Primary boot image: /c:/AEOS-NP2500_R11301.had ...(2)
 Primary boot config: /c:/primary.cfg ...(3)
 Secondary boot image: /c:/AEOS-NP2500_R11301_sec.had ...(4)
 Secondary boot config: /c:/secondary.cfg ...(5)
*(SD Card)
 Primary boot image: /d:/apresia-software.had ...(6)
 Primary boot config: /d:/apresia-startup-config.txt ...(7)


Note: * indicates the used boot information.
```

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は 1 が表示されます。
(2)	プライマリーブートイメージファイルとして使用するファイルのパスを表示します。
(3)	プライマリー構成情報として使用するファイルのパスを表示します。
(4)	セカンダリーブートイメージファイルとして使用するファイルのパスを表示します。
(5)	セカンダリー構成情報として使用するファイルのパスを表示します。
(6)	SD カードブート利用時の、プライマリーブートイメージファイルとして使用するファイルのパスを表示します。
(7)	SD カードブート利用時の、プライマリー構成情報として使用するファイルのパスを表示します。

3.9.7 show running-config

show running-config	
目的	running-config (現在動作中の構成情報) を表示します。
Command	show running-config [effective | all] [interface IF-ID | function [NAME]]
Parameter	effective (省略可能)：装置の動作に影響を与えるコマンド設定のみを表示する場合に指定します。 all (省略可能)：すべての設定 (デフォルト設定含む) を表示する場合に指定します。 interface IF-ID (省略可能)：指定したインターフェースに関連する設定のみを表示す

show running-config	
	る場合に、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定 function［NAME］（省略可能）：特定機能に関連する設定のみを表示する場合に指定します。機能名称を省略した場合は、入力可能な機能名称（大文字文字列）の一覧が表示されます。機能名称を指定する場合は、一覧で確認できる大文字文字列を省略せずに入力する必要があります。なお、機能名称の入力には[TAB]キーによるコマンド補完は利用できません。 • NAME（省略可能）：機能名称（例：VLAN）
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	オプションパラメーターを省略した場合は、デフォルトから変更された設定のみが表示されます。ただし、スタック機能（ラベル# STACK）やポート番号など、一部の設定は常に表示されます。 effective を指定して実施すると、例えばスパニングツリープロトコルが無効の場合、スパニングツリープロトコルに関連する設定は spanning-tree global state disable 設定だけが表示され、それ以外は表示されない動作になります。 interface を指定して実施した場合は、指定したインターフェースに関連する設定のみが表示されます。例えば interface port 1/0/5 を指定して実施した場合は、running-config の interface port 1/0/5 行の次行から字下げ表示されている設定がすべて表示されます。
制限・注意	• 本装置では 4 メガバイト以上の構成情報（自動的に付加される製品名称やバージョン番号が記載された先頭のヘッダー行、末尾のフッダー行を含む）は使用できません。超過した状態で本コマンドを実行すると、先頭から約 4 メガバイトまでの構成情報は表示されますが、超過した以降の部分は表示されません。ヘッダーに表示される running-config のサイズも、超過分が削除された後のサイズが表示されます。 • 構成情報が 4 メガバイト未満の場合でも、all 指定で本コマンドを実行するとデフォルト設定も含めて表示されるため、超過した以降の部分が表示されないことがあります。例えば、VLAN を 4094 個設定した状態で all 指定で本コマンドを実行すると、VLAN に関連するデフォルト設定も大量に表示されることになるため、その結果、超過した以降の部分が表示されません。
バージョン	1.08.02

使用例：running-config（現在動作中の構成情報）を表示する方法を示します。

```
# show running-config
Building configuration...

Current configuration : 1804 bytes ...(1)

#------------------------------------------------------------------------------
#               ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
#                                Configuration
#
#                             Firmware: Build 1.08.02
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------
```

```
# Date: Wed Dec 18 15:40:21 2020


# STACK

no stack
no stack my_box_id
stack my_box_priority 32
no stack preempt
no stack port-channel mode partial
no stack stack-port load-balance

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

項番	説明
(1)	running-config のサイズを表示します。

使用例：機能名称「IP」を指定して、running-config を表示する方法を示します。

```
# show running-config function IP
Building configuration...

Current configuration : 58 bytes


# IP

interface vlan 1
 ip address 192.168.1.200/24
```

3.9.8 show startup-config

show startup-config	
目的	startup-config (起動時に使用する構成情報) を表示します。
Command	show startup-config
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	• 本装置では 4 メガバイト以上の構成情報 (自動的に付加される製品名称やバージョン番号が記載された先頭のヘッダー行、末尾のフッダー行を含む) は使用できません。超過した状態で本コマンドを実行すると、先頭から約 4 メガバイトまでの構成情報は表示されますが、超過した以降の部分は表示されません。
バージョン	1.08.02

使用例：startup-config (起動時に使用する構成情報) を表示する方法を示します。

```
# show startup-config

#------------------------------------------------------------------------------
#               ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
#                              Configuration
#
#                          Firmware: Build 1.08.02
```

```
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------

# Date: Wed Dec 18 15:40:47 2020


# STACK

no stack
no stack my_box_id
stack my_box_priority 32
no stack preempt
no stack port-channel mode partial
no stack stack-port load-balance

# PRIVMGMT

enable password level 15 pass15
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.9.9 show config differences

show config differences	
目的	指定した 2 つの構成情報を比較し、その差分を表示します。
Command	show config differences {flash: URL | running-config | startup-config} {flash: URL | running-config | startup-config}
Parameter	flash: URL：比較対象として、構成情報ファイルの URL を指定します。以下のいずれかの書式を使用します。 • c:/URL：装置のローカルフラッシュ上のファイル指定（例：c:/config.cfg） • d:/URL：SD カード上のファイル指定（例：d:/config.cfg） • unitX:/c:/URL（X はボックス ID）：スタックメンバーのローカルフラッシュ上のファイル指定（例：ボックス ID が 2 の場合は unit2:/c:/config.cfg） • unitX:/d:/URL（X はボックス ID）：スタックメンバーの SD カード上のファイル指定（例：ボックス ID が 2 の場合は unit2:/d:/config.cfg） running-config：比較対象として、本装置の running-config を指定します。 startup-config：比較対象として、本装置の startup-config を指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SD カード上の「config.cfg」と本装置の running-config の差分を表示する方法を示します。

```
# show config differences flash: d:/config.cfg running-config

Config Differences: ...(1)
+vlan 10,20,500
+interface port 1/0/12
+ switchport access vlan 500
-vlan 10,20
-logging server 10.249.234.112 severity debugging facility 23 port 514
```

項番	説明
(1)	show config differences A B と実行した場合、差分は以下のように表示されます。 • A に含まれていて、B に含まれていない設定：先頭に "+" が付与されて表示 • A に含まれず、B に含まれている設定：先頭に "-" が付与されて表示

3.9.10 backup clone

backup clone	
目的	SD カードブートのために、装置が動作するのに必要なファイルを、装置のローカルフラッシュから SD カードにバックアップします。
Command	backup clone
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15

ガイドライン	動作に必要なファイルを SD カードにコピーし、他の装置に挿入して使用できます。現在の装置と同じ設定で動作する装置を作成するために使用します。
	
	以下のファイルがバックアップされます。
	• ブートスクリプト：apresia-loader.conf
	• ブートイメージファイル：apresia-software.had
	• startup-config：apresia-startup-config.txt
	• ランタイムバージョンテキストファイル：apresia-system-name.txt
	• SSHv2 RSA 鍵対ファイル：apresia-rsa-key
	• SSHv2 DSA 鍵対ファイル：apresia-dsa-key
	• 以下の Web 認証ページ
	  • ログイン認証ページ：apresia-login-page
	  • 認証成功ページ：apresia-login-success-page
	  • 認証失敗ページ：apresia-login-failure-page
	  • ログアウト成功ページ：apresia-logout-success-page
	  • ログアウト失敗ページ：apresia-logout-failure-page
	  • リダイレクト失敗ページ：apresia-redirect-error-page
	• Web アクセス拒否通知ページ：web-access-deny-page
	• AccessDefender のローカルデータベース：apresia-aaa-local-db
	• SSL サーバー証明書：apresia-https-certificate
	• SSL サーバーの秘密鍵：apresia-https-private-key
	• Web ページ画像 01～10：apresia-webpage-image01～apresia-webpage-image10
	
	ブートスクリプト（apresia-loader.conf）は以下の内容で設定されています。
	• プライマリーブートイメージファイル：/d:/apresia-software.had
	• プライマリー構成情報：/d:/apresia-startup-config.txt
	
	ブートイメージファイル（apresia-software.had）は、boot image コマンドでプライマリーブートイメージファイルとして指定したファームウェアファイルが、バックアップ対象になります。
	
	ランタイムバージョンテキストファイル（apresia-system-name.txt）には、backup clone 実行時に SD カードに保存されたブートイメージファイル（apresia-

backup clone	
	software.had）のバージョン情報が保存されます。 各ファイルのバックアップはそれぞれ独立して実行されます。1 つのファイルのバックアップに失敗した場合でも、その他のファイルのバックアップは行われます。 スタック機能を有効にしている場合は、マスターを含むすべてのスタックメンバーでそれぞれの装置に挿入された SD カードにバックアップが行われます。 装置に挿入された SD カードに「apresia-loader.conf」が存在する場合は、装置が起動する際に「apresia-loader.conf」のブート情報が参照されます。 装置に挿入された SD カードに「apresia-rsa-key」または「apresia-dsa-key」が存在する場合は、装置の SSH サーバーではそれらのファイルに含まれる RSA/DSA 鍵対が使用されます。 装置に挿入された SD カードに Web 認証ページが存在する場合は、装置に自動的に復元されます。 装置に挿入された SD カードに「apresia-https-certificate」および「apresia-https-private-key」が存在する場合は、SSL サーバー証明書および SSL サーバーの秘密鍵として、各ファイルがインポートされます。 したがって、backup clone コマンドを実行して動作に必要なファイルを SD カードにバックアップし、その SD カードを代替装置に挿入すると、簡単に複製を再現できます。 write memory コマンドおよび copy running-config startup-config コマンドは、現在の設定を SD カードに「apresia-startup-config.txt」として保存します。その際、「apresia-startup-config.txt」が存在している場合は、上書きされます。 装置は、構成情報から AccessDefender のローカルデータベース情報を取得します。複製した「apresia-aaa-local-db」を直接参照することはありません。
制限・注意	• 本装置では 4 メガバイト以上の構成情報は使用できません。超過した状態で本コマンドを実行すると、先頭から約 4 メガバイトまでの構成情報は保存されますが、超過した以降の部分は保存されません。 • 本コマンドでバックアップした構成情報ファイル「apresia-startup-config.txt」は、先頭にバイナリの制御データが付与された形式の構成情報ファイルになります。 • 先頭にバイナリの制御データが付与された形式の構成情報ファイルを編集することは推奨しませんが、編集する場合にはバイナリの制御データが崩れるような編集は行わないでください。例えば、Null を自動的にスペースに変換するような編集や、改行コードを統一することにより制御データ部が崩れるような編集は行わないでください。 • テキスト形式の構成情報ファイルを編集する場合には、改行コードは CRLF で編集してください。 • SD カードブートで代替装置が起動した後も、代替装置のローカルフラッシュの構成情報とブートイメージファイルは更新されません。SD メモリーカードのファイル読み込み失敗に備えてローカルフラッシュのファイルを更新する場合は、以下のような手順例で更新してください。 　• write memory コマンドなどで設定を保存すれば、ローカルフラッシュのプライマリーで指定した構成情報も running-config の内容に更新されます。 　• copy コマンドでブートイメージファイルをコピーし、boot image コマンドで

backup clone	
	ブートイメージファイルを指定できます。 • スタック構成の装置で backup clone を実施した場合、実行中に"DEBG(7) Unit <unit-id> fails to send a stacking message. (Type: <msg-type>[, Sub type: <sub-type>])"ログが出力されますが、backup clone 実行中の一時的なものであり動作に問題はありません。backup clone 終了後には出力されなくなります。 • 対象ファイルのサイズが大きい場合はバックアップに時間がかかります。ブートイメージファイル(apresia-software.had)の場合、バックアップが完了するまでに約1～2 分程度の時間がかかることがあります。
バージョン	1.08.02 1.10.01：バックアップ対象ファイル追加 (Web アクセス拒否通知ページ)

使用例：装置のローカルフラッシュから SD カードに、動作に必要なファイルをバックアップする方法を示します。

```
# backup clone

 Uploading boot information (apresia-loader.conf)..... Done.
 Uploading firmware image file (apresia-software.had)..... Done.
 Uploading start-up configuration file (apresia-startup-config.txt)..... Done.
 Uploading system name file (apresia-system-name.txt)..... Done.
 Uploading SSH RSA key file (apresia-rsa-key)..... Fail.
 Uploading SSH DSA key file (apresia-dsa-key)..... Done.
 Uploading web authentication login-page file (apresia-login-page)..... Done.
 Uploading web authentication login-success-page file (apresia-login-success-page)..... Done.
 Uploading web authentication login-failure-page file (apresia-login-failure-page)..... Done.
 Uploading web authentication logout-success-page file (apresia-logout-success-page)..... Done.
 Uploading web authentication logout-failure-page file (apresia-logout-failure-page)..... Done.
 Uploading web authentication redirect-error-page file (apresia-redirect-error-page)..... Done.
 Uploading access defender local database settings file (apresia-aaa-local-db)..... Done.
 Uploading SSL server certificate file (apresia-https-certificate)..... Done.
 Uploading SSL server private key file (apresia-https-private-key)..... Done.
 Uploading web authentication webpage-image01 file (apresia-webpage-image01)..... Done.
 Uploading web authentication webpage-image02 file (apresia-webpage-image02)..... Done.
 Uploading web authentication webpage-image03 file (apresia-webpage-image03)..... Done.
 Uploading web authentication webpage-image04 file (apresia-webpage-image04)..... Done.
 Uploading web authentication webpage-image05 file (apresia-webpage-image05)..... Done.
 Uploading web authentication webpage-image06 file (apresia-webpage-image06)..... Done.
 Uploading web authentication webpage-image07 file (apresia-webpage-image07)..... Done.
 Uploading web authentication webpage-image08 file (apresia-webpage-image08)..... Done.
 Uploading web authentication webpage-image09 file (apresia-webpage-image09)..... Done.
 Uploading web authentication webpage-image10 file (apresia-webpage-image10)..... Done.
```

3.9.11 write

write	
目的	running-config（現在動作中の構成情報）を startup-config（起動時に使用する構成情報）に保存します。
Command	write [memory [secondary]]
Parameter	memory（省略可能）：現在動作中の構成情報を、プライマリー構成情報に保存する場合に指定します。SD カードが挿入されている場合は、SD カードにも保存します。 secondary（省略可能）：現在動作中の構成情報を、セカンダリー構成情報に保存する場合に指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	write［memory］コマンドは、running-config（現在動作中の構成情報）をプライマリー構成情報にのみ上書き保存します。

write	
	セカンダリー構成情報に上書き保存する場合は、write memory secondary コマンドを使用してください。
制限・注意	• boot config コマンドでセカンダリー構成情報を指定していない場合は、write memory secondary コマンドを実行できません。 • 本装置では 4 メガバイト以上の構成情報は使用できません。超過した状態で本コマンドを実行すると、先頭から約 4 メガバイトまでの構成情報は保存されますが、超過した以降の部分は保存されません。 • 一部のスタックメンバーに SD カードが未挿入の状態で write memory コマンドを実行すると、以下のメッセージが表示されません。 　• "Saving all configurations to SD-Card" • 本コマンドで SD カードに保存した構成情報ファイルは、先頭にバイナリの制御データが付与された形式の構成情報ファイルになります。
バージョン	1.08.02

使用例：running-config（現在動作中の構成情報）を startup-config（起動時に使用する構成情報）に保存する方法を示します。

```
# write memory

Destination filename startup-config? [y/n]:  y

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

3.9.12 copy primary-config secondary-config

copy primary-config secondary-config	
目的	プライマリー構成情報をセカンダー構成情報にコピーします。
Command	copy primary-config secondary-config
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	boot config コマンドでプライマリー構成情報に指定したファイルの内容を、セカンダリー構成情報に指定したファイルにコピーします。
制限・注意	• プライマリー構成情報、またはセカンダリー構成情報が指定されていない場合は実行できません。
バージョン	1.08.02

使用例：プライマリー構成情報をセカンダー構成情報にコピーする方法を示します。

```
# copy primary-config secondary-config

Success
```

3.9.13 reboot

reboot	
目的	装置を再起動します。

reboot	
Command	reboot [unit UNIT-ID] [force_agree] [cold]
Parameter	unit UNIT-ID（省略可能）：装置のボックス ID を 1～4 の範囲で指定します。 force_agree（省略可能）：確認メッセージを表示せずに、強制的に装置を再起動する場合に指定します。 cold（省略可能）：Continuous PoE 機能が有効でも、PoE コントローラーを再起動する場合に指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	スタック構成で特定のボックス ID を指定しない場合は、スタック構成全体が再起動されます。 cold オプションは、Continuous PoE 機能が有効設定の装置で、PoE コントローラーのファームウェアをバージョンアップする場合に使用します。cold オプションを指定して再起動した場合は、Continuous PoE 機能が有効であっても、再起動中は PD への給電が一時的に中断されます。
制限・注意	• 本コマンド実行時は保存確認を行いません。設定の保存を行ったうえで、本コマンドを実行してください。 • backup clone コマンドなどのファイルアクセス操作中は、本コマンドで装置を再起動したり、装置の電源を落としたりしないでください。本コマンドで再起動をする際は、他セッションなどでコマンド操作を行っていないことを確認してから実施してください。
バージョン	1.08.02 1.10.01：cold パラメーター追加

使用例：装置を再起動する方法を示します。

```
# reboot

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

使用例：確認メッセージを表示せずに、強制的に装置を再起動する方法を示します。

```
# reboot force_agree

Please wait, the switch is rebooting...
```

3.9.14 copy boot

copy boot	
目的	装置のローカルフラッシュから SD カードにブートスクリプトを保存します。
Command	copy boot
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	ブートスクリプトは、「d:/apresia-loader.conf」に保存されます。 装置に挿入された SD カードに「apresia-loader.conf」が存在する場合は、装置が起

copy boot	
	動する際に「apresia-loader.conf」のブートスクリプトが参照されます。
制限・注意	• 本コマンドの実行完了までに、約 10 秒程度の時間がかかることがあります。
バージョン	1.08.02

使用例：装置のローカルフラッシュから SD カードにブートスクリプトを保存する方法を示します。

```
# copy boot

 Writing the boot information to SD card.......... Done.
```

3.9.15 erase boot

erase boot	
目的	装置のローカルフラッシュからブート情報を消去します。
Command	erase boot
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	本コマンドでブート情報を消去した後は、boot image コマンドと boot config コマンドで、必ずブート情報を再設定してください。
制限・注意	• 正しく使用できるブートスクリプトが保存されている SD カードを挿入しない限り、本コマンドでブート情報を消去した後に再設定しないで装置を再起動すると、装置起動時にブート情報の読み込みに失敗します。
バージョン	1.08.02

使用例：装置のローカルフラッシュからブート情報を消去する方法を示します。

```
# erase boot

 Erasing the boot information in FLASH..........  Done.

# show boot

Unit 1
*(Configured)
 Primary boot image: No valid boot image.
 Primary boot config: No valid boot config.
 Secondary boot image: No valid boot image.
 Secondary boot config: No valid boot config.


Note: * indicates the used boot information.
```

3.9.16 configure replace

configure replace	
目的	現在の running-config を、指定した構成情報で置き換えます。
Command	configure replace tftp: //IP/FILE [force] configure replace ftp: //USER:PASS@IP:TCP/FILE [force] configure replace sftp: //USER:PASS@IP:TCP/FILE [force] configure replace flash: FILE [force]

configure replace	
Parameter	tftp: //IP/FILE：TFTP サーバーをコピー元に指定します。 • IP：TFTP サーバーの IP アドレス • FILE：ファイルパス名 ftp: //USER:PASS@IP:TCP/FILE：FTP サーバーをコピー元に指定します。 sftp: //USER:PASS@IP:TCP/FILE：SFTP サーバーをコピー元に指定します。 • USER：ユーザー名 • PASS：パスワード • IP：FTP/SFTP サーバーの IP アドレス • TCP：TCP ポート番号、省略可能 • FILE：ファイルパス名 flash: FILE：装置のローカルフラッシュ(c:)または SD カード(d:)をコピー元に指定します。 force（省略可能）：確認メッセージを表示せずに、強制的にコマンドを実行する場合に指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	• デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在するサーバーを指定して本コマンドを実施する場合、TFTP と FTP/SFTP で動作が異なります。詳細については copy コマンドの制限事項と同等のため、そちらを参照してください。 • 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク • 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク • 本コマンドを SFTP で使用する場合は、IPv6 アドレスでの使用は未サポートです。SFTP を使用する場合は IPv4 アドレスで使用してください。 • 本コマンドを使用すると、装置の再起動を伴わずに running-config の置き換えが発生します。指定した構成情報は、完全な設定であるとみなされます。装置設定の置き換えの際に通信断やループが発生する可能性がありますので、運用中の使用は避けてください。 • SIZE コマンド（RFC 3659 参照）に対応する FTP サーバーのみ指定できます。 • スタック機能が無効の装置で、本コマンドを使用して、スタック機能を設定した構成情報に置き換えないでください。 • 置き換える構成情報の設定量が多いほど、設定反映時間が長くなります。設定量が多い場合は、本コマンドの実行完了までに数分～十数分程度の時間がかかることがあります。
バージョン	1.08.02 1.13.01：sftp:パラメーター追加

使用例：TFTP サーバー(192.0.2.100)に保存されている構成情報ファイル(config.cfg)を指定して、現在の running-config を置き換える方法を示します。

```
# configure replace tftp: //192.0.2.100/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]:  y

 Accessing tftp://192.0.2.100/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done
```

使用例：FTP サーバー(192.0.2.100, ユーザー名：test, パスワード：12test34)に保存されている構成情報ファイル(config.cfg)を指定し、force オプションを使用して現在の running-config を置き換える方法を示します。

```
# configure replace ftp: //test:12test34@192.0.2.100/config.cfg force

 Accessing ftp://192.0.2.100/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done
```

使用例：ローカルフラッシュ(c:)に保存されている構成情報ファイル(config.cfg)を指定し、force オプションを使用して現在の running-config を置き換える方法を示します。

```
# configure replace flash: config.cfg force

 Executing script file config.cfg ......
 Executing done
```

3.9.17 copy

copy	
目的	ファイルをコピーします。
Command	**copy** SOURCE DESTINATION **copy** SOURCE {**flash:** [URL] | **tftp:** [URL] | **ftp:** [URL] | **sftp:** [URL]} **copy** {**flash:** [URL] | **tftp:** [URL] | **ftp:** [URL] | **sftp:** [URL]} DESTINATION
Parameter	SOURCE：コピー元を指定します。 • startup-config：startup-config をコピー(アップロード)する場合に指定 • running-config：running-config をコピー(アップロード)する場合に指定 • log：システムログをコピー(アップロード)する場合に指定 • flash: [URL]：装置のローカルフラッシュまたは SD カードを使用する場合に指定、URL は省略可能 • {tftp: | ftp: | sftp:} [URL]：TFTP/FTP/SFTP サーバーを使用する場合に指定、URL は省略可能 DESTINATION：コピー先を指定します。 • startup-config [secondary]：startup-config へ適用する場合に指定 • secondary パラメーターは、セカンダリー構成情報を指定している場合

copy	
	に copy running-config startup-config コマンドでのみ使用可能 • running-config：running-config へ適用する場合に指定 • flash: [URL]：装置のローカルフラッシュまたは SD カードを使用する場合に指定、URL は省略可能 • {tftp: | ftp: | sftp:} [URL]：TFTP/FTP/SFTP サーバーを使用する場合に指定、URL は省略可能 URL（省略可能）：コピー元ファイル、またはコピー先ファイルを指定します。省略可能ですが、指定した場合は、コマンド実行後の入力ダイアログがあらかじめ入力された状態になります。以下に入力書式例を示します。 • flash: c:/FILE：装置のローカルフラッシュ上(c:)のファイルパス指定 • flash: d:/FILE：SD カード上(d:)のファイルパス指定 • tftp: //IP/FILE：TFTP サーバー上のファイルパス指定 • IP：TFTP サーバーの IP アドレス • FILE：ファイルパス名 • ftp: //USER:PASS@IP:TCP/FILE：FTP サーバー上のファイルパス指定 • sftp: //USER:PASS@IP:TCP/FILE：SFTP サーバー上のファイルパス指定 • USER：ユーザー名 • PASS：パスワード • IP：FTP/SFTP サーバーの IP アドレス • TCP：TCP ポート番号、省略可能 • FILE：ファイルパス名
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	コピー先として startup-config を指定した場合は、コピー元ファイルが保存されている場所によって動作が異なります。コピー元が flash の場合は、boot config コマンドで設定したファイル名がコピー元ファイル名に変更されます。コピー元が flash 以外の場合は、boot config コマンドで設定したファイルの内容が上書きされます。 コピー先として running-config を指定した場合は、現在動作中の設定（running-config）に、コピー元に指定した構成情報ファイルの内容が流し込みされます。そのため、上書き可能な設定は上書きされますが、上書き不可の設定は設定されません。 スタック構成において、コピー元として TFTP/FTP/SFTP サーバーを使用し、コピー先として flash を使用する場合に、コピー先を相対パスで指定するとファイルはスタック内のすべてのユニットにダウンロードされます。 flash:パラメーター指定時のパス情報を以下に示します。 • 非スタック装置およびスタックマスター装置の場合、ローカルフラッシュのルートディレクトリーは「c:」になります。外部ストレージ（SD カード）のルートディレクトリーは「d:」になります。 • スタックマスター以外の装置の場合は、先頭に「unitX:/（X はボックス ID）」を付加したパスを指定します。例えば、ボックス ID 2 の装置（スタックマスター以外）のローカルフラッシュのルートディレクトリーは「unit2:/c:」です。 コピー元として log を指定した場合は、コピー先には TFTP/SFTP サーバーのみ指定できます。 ブートイメージファイルを装置にダウンロードするには、本コマンドでコピー先に

copy	
	ローカルフラッシュ（flash:）を指定して実施します。ダウンロードしたブートイメージファイルを次回起動時に使用する場合は、boot image コマンドで指定します。
制限・注意	• copy {tftp:｜ftp:｜sftp:} startup-config コマンドは、指定した構成情報のスタック設定を含めてコピーします。そのため、本コマンドはスタック構成の装置に対しては実行しないでください。 • 本装置では 4 メガバイト以上の構成情報は使用できません。超過した状態で本コマンドを実行すると、先頭から約 4 メガバイトまでの構成情報は保存されますが、超過した以降の部分は保存されません。 • デフォルトルート情報（0.0.0.0/0）とマネージメントポートのデフォルトゲートウェイ設定（ip default-gateway）の両方が存在する装置において、以下の宛先に存在するサーバーを指定して本コマンドを実施する場合、TFTP と FTP/SFTP で動作が異なります。 　• 宛先（1）：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク 　• 宛先（2）：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク • この状況で本コマンドを TFTP で使用する場合、宛先判定にはデフォルトルートよりもデフォルトゲートウェイ設定が優先され、宛先（1）（2）のいずれの場合も TFTP パケットはマネージメントポートから送信されます。そのため、宛先（1）への実施が失敗します。VLAN インターフェース経由でのみ管理する場合は、送信元 IP アドレス設定（ip tftp source-interface）を VLAN インターフェース指定で設定することにより、このような状況でも宛先（1）への実施が成功するようになりますが、この設定をするとマネージメントポート経由での実施が失敗するようになることに注意してください。 • この状況で本コマンドを FTP/SFTP で使用する場合、宛先判定にはデフォルトゲートウェイ設定よりもデフォルトルートが優先され、宛先（1）（2）のいずれの場合も FTP/SFTP パケットは VLAN インターフェースから送信されます。そのため、宛先（2）への実施が失敗します。マネージメントポート経由でのみ管理する場合は、送信元 IP アドレス設定（ip ftp source-interface, ip ssh source-interface）をマネージメントポート指定で設定することにより、このような状況でも宛先（2）への実施が成功するようになりますが、この設定をすると VLAN インターフェース経由での実施が失敗するようになることに注意してください。 • SIZE コマンド（RFC 3659 参照）に対応する FTP サーバーのみ指定できます。 • コピー先として flash を指定して SD カードに構成情報をアップロードした場合は、先頭にバイナリの制御データが付与された形式の構成情報ファイルになります。 • 先頭にバイナリの制御データが付与された形式の構成情報ファイルを編集することは推奨しませんが、編集する場合にはバイナリの制御データが崩れるような編集は行わないでください。例えば、Null を自動的にスペースに変換するような編集や、改行コードを統一することにより制御データ部が崩れるような編集は行わないでください。 • テキスト形式の構成情報ファイルを編集する場合には、改行コードは CRLF で編集してください。
バージョン	1.08.02 1.13.01：sftp:パラメーター追加

使用例：running-config に、TFTP サーバー10.1.1.254 の「switch-config.cfg」の内容を流し込む方法を示します。

```
# copy tftp: //10.1.1.254/switch-config.cfg running-config

Address of remote host [10.1.1.254]?
Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]:  y

 Accessing tftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 45421 bytes.
 Executing script file switch-config.cfg ......
 Executing done
```

使用例：running-config を、TFTP サーバー10.1.1.254 にファイル名「switch-config.cfg」でアップロードする方法を示します。

```
# copy running-config tftp: //10.1.1.254/switch-config.cfg

Address of remote host [10.1.1.254]?
Destination filename [switch-config.cfg]?
 Accessing tftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 45421 bytes.
```

使用例：running-config を startup-config にコピーする方法を示します。

```
# copy running-config startup-config

Destination filename startup-config? [y/n]:  y

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

使用例：running-config に、フラッシュメモリーに保存された「switch-config.cfg」の内容を流し込む方法を示します。

```
# copy flash: switch-config.cfg running-config

Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]:  y

 Executing script file switch-config.cfg ......
 Executing done
```

使用例：TFTP サーバーからスタック内のすべてのユニットに、ブートイメージファイルをダウンロードする方法を示します。

```
# copy tftp: //10.1.1.254/image.had flash: image.had

Address of remote host [10.1.1.254]?
Source filename [image.had]?
Destination filename [image.had]?
 Accessing tftp://10.1.1.254/image.had...
 Transmission start...
 Transmission finished, file length 8315060 bytes.
 Transmission to slave start.................   Done.
 Transmission to slave finished, file length 8315060 bytes.
 Please wait, programming flash.............. Done.
 Wait slave programming flash complete...
 Done.
```

3.9.18 backup

backup	
目的	動作に必要なファイルを、TFTP/FTP/SFTP サーバーまたは SD カードにバックアップします。
Command	**backup tftp:** [//IP/PATH] **prefix** BASENAME [OPTION] **backup ftp:** [//USER:PASS@IP:TCP/PATH] **prefix** BASENAME [OPTION] **backup sftp:** [//USER:PASS@IP:TCP/PATH] **prefix** BASENAME [OPTION] **backup memory-card:** [/PATH] **prefix** BASENAME [OPTION]
Parameter	※バックアップ先の情報は省略可能で、指定した場合はコマンド実行後の入力ダイアログがあらかじめ入力された状態になります。 tftp: [//IP/PATH]：TFTP サーバーにバックアップする場合に指定します。 • IP（省略可能）：TFTP サーバーの IP アドレス • PATH（省略可能）：バックアップ先のパス ftp: [//USER:PASS@IP:TCP/PATH]：FTP サーバーにバックアップする場合に指定します。 sftp: [//USER:PASS@IP:TCP/PATH]：SFTP サーバーにバックアップする場合に指定します。 • USER（省略可能）：ユーザー名 • PASS（省略可能）：パスワード • IP（省略可能）：FTP/SFTP サーバーの IP アドレス • TCP（省略可能）：TCP ポート番号、省略可能 • PATH（省略可能）：バックアップ先のパス memory-card: [/PATH]：SD カードにバックアップする場合に指定します。 • PATH（省略可能）：バックアップ先のパス prefix BASENAME：バックアップファイル名のプレフィックス文字列を最大 12 文字で指定します。\ / : * ? " < > | およびスペースは使用できません。 OPTION（省略可能）：オプションを指定します。 • no-software：ブートイメージファイルのバックアップを省略する場合に指定 • no-access-defender：AccessDefender の Web 認証ページ(6 ファイル)、Web アクセス拒否通知ページ、AccessDefender のローカルデータベース、AccessDefender の Web ページ画像(10 ファイル)のバックアップを省略する場合に指定
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	backup コマンドで動作に必要なファイルをバックアップし、restore コマンドで他の装置にリストアできます。現在の装置と同じ設定で動作する装置を作成するために使用します。 以下のファイルがバックアップされます。 • ブートイメージファイル：BASENAME-software.had • startup-config：BASENAME-startup-config.txt • running-config：BASENAME-running-config.txt • ランタイムバージョンテキストファイル：BASENAME-system-name.txt • SSHv2 RSA 鍵対ファイル：BASENAME-rsa-key

backup	
	• SSHv2 DSA 鍵対ファイル：BASENAME-dsa-key • 以下の Web 認証ページ • ログイン認証ページ：BASENAME-login-page • 認証成功ページ：BASENAME-login-success-page • 認証失敗ページ：BASENAME-login-failure-page • ログアウト成功ページ：BASENAME-logout-success-page • ログアウト失敗ページ：BASENAME-logout-failure-page • リダイレクト失敗ページ：BASENAME-redirect-error-page • Web アクセス拒否通知ページ：BASENAME-web-access-deny-page • AccessDefender のローカルデータベース：BASENAME-aaa-local-db • SSL サーバー証明書：BASENAME-https-certificate • SSL サーバーの秘密鍵：BASENAME-https-private-key • Web ページ画像 01～10：BASENAME-webpage-image01～BASENAME-webpage-image10 ブートイメージファイル（BASENAME-software.had）は、boot image コマンドでプライマリーブートイメージファイルとして指定したファームウェアファイルが、バックアップ対象になります。 各ファイルのバックアップはそれぞれ独立して実行されます。1 つのファイルのバックアップに失敗した場合でも、その他のファイルのバックアップは行われます。
制限・注意	• スタックを構成している場合、マスター以外のスタックメンバーは、動作に必要なファイルをバックアップできません。 • IPv6 アドレスで TFTP/FTP サーバーを指定して backup コマンドを使用する場合、および IPv4 アドレスで FTP サーバーを指定して backup ftp:コマンドを使用する場合は、「AccessDefender のローカルデータベース」「SSL サーバー証明書」「SSL サーバーの秘密鍵」はバックアップ処理の対象外になります。これらを含めて実施する場合は、IPv4 アドレスで TFTP/SFTP サーバーを指定して backup コマンドを使用するか、SD カードを利用して backup memory-card:コマンドを使用してください。 • 本装置では 4 メガバイト以上の構成情報は使用できません。超過した状態で本コマンドを実行すると、先頭から約 4 メガバイトまでの構成情報は保存されますが、超過した以降の部分は保存されません。 • デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在するサーバーを指定して本コマンドを実施する場合、TFTP と FTP/SFTP で動作が異なります。詳細については copy コマンドの制限事項と同等のため、そちらを参照してください。 • 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク • 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク • 本コマンドを SFTP で使用する場合は、IPv6 アドレスでの使用は未サポートです。SFTP を使用する場合は IPv4 アドレスで使用してください。 • 本コマンドでバックアップした構成情報ファイル「BASENAME-startup-config.txt」は、先頭にバイナリの制御データが付与された形式の構成情報ファイルになります。

backup	
	• 先頭にバイナリの制御データが付与された形式の構成情報ファイルを編集することは推奨しませんが、編集する場合にはバイナリの制御データが崩れるような編集は行わないでください。例えば、Null を自動的にスペースに変換するような編集や、改行コードを統一することにより制御データ部が崩れるような編集は行わないでください。 • テキスト形式の構成情報ファイルを編集する場合には、改行コードは CRLF で編集してください。 • 対象ファイルのサイズが大きい場合はバックアップに時間がかかります。ブートイメージファイル(BASENAME-software.had)の場合、バックアップが完了するまでに約 1〜2 分程度の時間がかかることがあります。
バージョン	1.08.02 1.10.01：バックアップ対象ファイル追加（Web アクセス拒否通知ページ） 1.13.01：sftp:パラメーター追加

使用例：プレフィックス文字列を「backup1」として、動作に必要なファイルを装置のローカルフラッシュから SD カードにバックアップする方法を示します。

```
# backup memory-card: prefix backup1

 Uploading firmware image file (backup1-software.had)..... Done.
 Uploading start-up configuration file (backup1-startup-config.txt)..... Done.
 Uploading running configuration file (backup1-running-config.txt)..... Done.
 Uploading system name file (backup1-system-name.txt)..... Done.
 Uploading SSH RSA key file (backup1-rsa-key)..... Done.
 Uploading SSH DSA key file (backup1-dsa-key)..... Done.
 Uploading web authentication login-page file (backup1-login-page)..... Done.
 Uploading web authentication login-success-page file (backup1-login-success-page)..... Done.
 Uploading web authentication login-failure-page file (backup1-login-failure-page)..... Done.
 Uploading web authentication logout-success-page file (backup1-logout-success-page)..... Done.
 Uploading web authentication logout-failure-page file (backup1-logout-failure-page)..... Done.
 Uploading web authentication redirect-error-page file (backup1-redirect-error-page)..... Done.
 Uploading access defender local database settings file (backup1-aaa-local-db)..... Done.
 Uploading SSL server certificate file (backup1-https-certificate)..... Done.
 Uploading SSL server private key file (backup1-https-private-key)..... Done.
 Uploading web authentication webpage-image01 file (backup1-webpage-image01)..... Done.
 Uploading web authentication webpage-image02 file (backup1-webpage-image02)..... Done.
 Uploading web authentication webpage-image03 file (backup1-webpage-image03)..... Done.
 Uploading web authentication webpage-image04 file (backup1-webpage-image04)..... Done.
 Uploading web authentication webpage-image05 file (backup1-webpage-image05)..... Done.
 Uploading web authentication webpage-image06 file (backup1-webpage-image06)..... Done.
 Uploading web authentication webpage-image07 file (backup1-webpage-image07)..... Done.
 Uploading web authentication webpage-image08 file (backup1-webpage-image08)..... Done.
 Uploading web authentication webpage-image09 file (backup1-webpage-image09)..... Done.
 Uploading web authentication webpage-image10 file (backup1-webpage-image10)..... Done.
```

3.9.19 restore

restore	
目的	TFTP/FTP/SFTP サーバーまたは SD カードにバックアップした動作に必要なファイルを、装置のローカルフラッシュにリストアします。
Command	restore tftp: [//IP/PATH] prefix BASENAME [OPTION] restore ftp: [//USER:PASS@IP:TCP/PATH] prefix BASENAME [OPTION] restore sftp: [//USER:PASS@IP:TCP/PATH] prefix BASENAME [OPTION] restore memory-card: [/PATH] prefix BASENAME [OPTION]
Parameter	※バックアップ元の情報は省略可能で、指定した場合はコマンド実行後の入力ダイアログがあらかじめ入力された状態になります。

restore	
	tftp: [//IP/PATH]：TFTP サーバーからリストアする場合に指定します。 • IP（省略可能）：TFTP サーバーの IP アドレス • PATH（省略可能）：バックアップ元のパス ftp: [//USER:PASS@IP:TCP/PATH]：FTP サーバーからリストアする場合に指定します。 sftp: [//USER:PASS@IP:TCP/PATH]：SFTP サーバーからリストアする場合に指定します。 • USER（省略可能）：ユーザー名 • PASS（省略可能）：パスワード • IP（省略可能）：FTP/SFTP サーバーの IP アドレス • TCP（省略可能）：TCP ポート番号、省略可能 • PATH（省略可能）：バックアップ元のパス memory-card: [/PATH]：SD カードからリストアする場合に指定します。 • PATH（省略可能）：バックアップ元のパス prefix BASENAME：バックアップファイル名のプレフィックス文字列を最大 12 文字で指定します。\ / : * ? " < > | およびスペースは使用できません。 OPTION（省略可能）：オプションを指定します。 • no-software：ブートイメージファイルのリストアを省略する場合に指定 • no-access-defender：AccessDefender の Web 認証ページ(6 ファイル)、Web アクセス拒否通知ページ、AccessDefender のローカルデータベース、AccessDefender の Web ページ画像(10 ファイル)のリストアを省略する場合に指定 • reboot：リストア終了後に自動的に装置を再起動する場合に指定、ただし 1 つでもリストアに失敗したファイルがある場合は再起動されない
モード	特権実行モード
特権レベル	レベル：15

ガイドライン	backup コマンドで動作に必要なファイルをバックアップし、restore コマンドで他の装置にリストアできます。現在の装置と同じ設定で動作する装置を作成するために使用します。
	
	restore コマンドを実行した後は、ファームウェアや設定などを反映させるために、装置を再起動、または電源 OFF/ON を実施して起動しなおしてください。
	
	以下のファイルがリストアされます。
	• ブートイメージファイル：BASENAME-software.had
	• startup-config：BASENAME-startup-config.txt
	• ランタイムバージョンテキストファイル：BASENAME-system-name.txt
	• SSHv2 RSA 鍵対ファイル：BASENAME-rsa-key
	• SSHv2 DSA 鍵対ファイル：BASENAME-dsa-key
	• 以下の Web 認証ページ
	  • ログイン認証ページ：BASENAME-login-page
	  • 認証成功ページ：BASENAME-login-success-page
	  • 認証失敗ページ：BASENAME-login-failure-page
	  • ログアウト成功ページ：BASENAME-logout-success-page

restore	
	• ログアウト失敗ページ：BASENAME-logout-failure-page • リダイレクト失敗ページ：BASENAME-redirect-error-page • Web アクセス拒否通知ページ：BASENAME-web-access-deny-page • AccessDefender のローカルデータベース：BASENAME-aaa-local-db • SSL サーバー証明書：BASENAME-https-certificate • SSL サーバーの秘密鍵：BASENAME-https-private-key • Web ページ画像 01～10：BASENAME-webpage-image01～BASENAME-webpage-image10 動作に必要なファイルをリストアすると、プライマリー構成情報はリストアされた startup-config に置き換わり、プライマリーブートイメージファイルはリストアされたブートイメージファイルに置き換わります。装置に同じ名前のファイルが存在した場合は、既存のファイルは上書きされます。 RSA/DSA 鍵対は、装置を起動しなおした後にリストアされたファイルに置き換わります。RSA/DSA 鍵対は、show crypto key mypubkey コマンドで表示できます。 SSL サーバー証明書、SSL サーバーの秘密鍵、および AccessDefender のローカルデータベースは、装置にインポートされます。各ファイルを表示するには、show ssl https-certificate コマンド、show ssl https-private-key コマンド、および show access-defender aaa-local-db コマンドを使用します。
制限・注意	• スタックを構成している場合、マスター以外のスタックメンバーは、動作に必要なファイルをリストアできません。 • IPv6 アドレスで TFTP/FTP サーバーを指定して restore コマンドを使用する場合、および IPv4 アドレスで FTP サーバーを指定して restore ftp:コマンドを使用する場合は、「AccessDefender のローカルデータベース」「SSL サーバー証明書」「SSL サーバーの秘密鍵」はリストア処理の対象外になります。これらを含めて実施する場合は、IPv4 アドレスで TFTP/SFTP サーバーを指定して restore コマンドを使用するか、SD カードを利用して restore memory-card:コマンドを使用してください。 • デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在するサーバーを指定して本コマンドを実施する場合、TFTP と FTP/SFTP で動作が異なります。詳細については copy コマンドの制限事項と同等のため、そちらを参照してください。 • 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク • 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク • 本コマンドを SFTP で使用する場合は、IPv6 アドレスでの使用は未サポートです。SFTP を使用する場合は IPv4 アドレスで使用してください。 • 対象ファイルのサイズが大きい場合はリストアに時間がかかります。ブートイメージファイル(BASENAME-software.had)の場合、リストアが完了するまでに約 1～2 分程度の時間がかかることがあります。
バージョン	1.08.02 1.10.01：リストア対象ファイル追加 (Web アクセス拒否通知ページ) 1.13.01：sftp:パラメーター追加

使用例：プレフィックス文字列を「backup1」としてバックアップした動作に必要なファイルを、SD カードから装置のローカルフラッシュにリストアする方法を示します。

```
# restore memory-card: prefix backup1

 Downloading firmware image file (backup1-software.had)..... Done.
 Downloading start-up configuration file (backup1-startup-config.txt)..... Done.
 Downloading system name file (backup1-system-name.txt)..... Done.
 Downloading SSH RSA key file (backup1-rsa-key)..... Done.
 Downloading SSH DSA key file (backup1-dsa-key)..... Done.
 Downloading web authentication login-page file (backup1-login-page)..... Done.
 Downloading web authentication login-success-page file (backup1-login-success-page)..... Done.
 Downloading web authentication login-failure-page file (backup1-login-failure-page)..... Done.
 Downloading web authentication logout-success-page file (backup1-logout-success-page)..... Done.
 Downloading web authentication logout-failure-page file (backup1-logout-failure-page)..... Done.
 Downloading web authentication redirect-error-page file (backup1-redirect-error-page)..... Done.
 Downloading access defender local database settings file (backup1-aaa-local-db)..... Done.
 Downloading SSL server certificate file (backup1-https-certificate)..... Done.
 Downloading SSL server private key file (backup1-https-private-key)..... Done.
 Downloading web authentication webpage-image01 file (backup1-webpage-image01)..... Done.
 Downloading web authentication webpage-image02 file (backup1-webpage-image02)..... Done.
 Downloading web authentication webpage-image03 file (backup1-webpage-image03)..... Done.
 Downloading web authentication webpage-image04 file (backup1-webpage-image04)..... Done.
 Downloading web authentication webpage-image05 file (backup1-webpage-image05)..... Done.
 Downloading web authentication webpage-image06 file (backup1-webpage-image06)..... Done.
 Downloading web authentication webpage-image07 file (backup1-webpage-image07)..... Done.
 Downloading web authentication webpage-image08 file (backup1-webpage-image08)..... Done.
 Downloading web authentication webpage-image09 file (backup1-webpage-image09)..... Done.
 Downloading web authentication webpage-image10 file (backup1-webpage-image10)..... Done.
```

3.9.20 clear running-config

clear running-config	
目的	running-config（現在動作中の構成情報）を消去します。
Command	clear running-config
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	本コマンドにより、スタックに関する設定以外の現在動作中の構成情報が消去されます。IP アドレス設定なども消去されるため、接続済みのリモート接続はすべて切断されます。 なお、本コマンドを実行すると、装置に保存されているログも削除されます。
制限・注意	• default port-shutdown 設定は、clear running-config コマンドを実行しても削除されません。 • 本コマンドで running-config を消去した装置を運用環境で使用する際は、設定を実施して構成情報を保存した後、念のため運用前に一度起動しなおしてから使用することを推奨します。
バージョン	1.08.02

使用例：running-config（現在動作中の構成情報）を消去する方法を示します。

```
# clear running-config

This command will clear the system's configuration to the factory default
settings, including the IP address.
Clear running configuration? (y/n) [n]  y
```

3.9.21 reset system

reset system	
目的	システムのリセット、構成情報の初期化、および装置の再起動を行います。
Command	reset system [factory-default]
Parameter	factory-default（省略可能）：工場出荷時のデフォルト状態に戻す場合に指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	スタックに関する設定を含む構成情報を初期化します。factory-default パラメーターを指定すると、セカンダリー構成情報、および構成情報に関連するブート情報も初期化され、以下のファイルは削除されます。 • すべてのローカルフラッシュに保存されたファイル（セキュリティー認証ファイルを含む。）（ただし、boot image コマンドにより指定されたブートイメージファイルは削除されません。） • すべてのログおよびエラーログエントリー
制限・注意	-
バージョン	1.08.02

使用例：装置をデフォルト設定に戻す方法を示します。

```
# reset system

This command will clear the system's configuration to the factory
default settings, including the IP address and stacking settings.
Clear system configuration, save, reboot? (y/n) [n]  y

Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

4 管理

4.1 DHCP クライアントコマンド

DHCP クライアント関連の設定コマンドは以下のとおりです。

- ip dhcp client class-id
- ip dhcp client client-id
- ip dhcp client hostname
- ip dhcp client lease

4.1.1 ip dhcp client class-id

ip dhcp client class-id	
目的	DHCP クライアントが送信する DISCOVER メッセージなどに付与する、オプション 60 のベンダークラス識別子を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip dhcp client class-id {STRING | hex HEX-STRING} no ip dhcp client class-id
Parameter	STRING：ベンダークラス識別子を ASCII 文字列で設定する場合に、最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? を除いた文字を使用可能です。なお、スペースを使用する場合は、指定する文字列全体をダブルクォーテーションで囲んで指定します。 hex HEX-STRING：ベンダークラス識別子を 16 進文字列で設定する場合に、最大 64 文字で指定します。
デフォルト	"APRESIA Systems, Ltd" + 製品名称 (例：APRESIA Systems, LtdApresiaNP2500-8MT4X-PoE)
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 構成情報では、指定した文字列全体をダブルクォーテーションで囲んだ形式で表示されます。
バージョン	1.08.02

使用例：VLAN100 インターフェースにおいて、ベンダークラス識別子を Verndor-A に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# ip dhcp client class-id Verndor-A
(config-if-vlan)#
```

4.1.2 ip dhcp client client-id

ip dhcp client client-id	
目的	DHCP クライアントが送信する DISCOVER メッセージなどに付与する、オプション 61 のクライアント ID を設定します。設定を削除する場合は、no 形式のコマンドを使用します。

ip dhcp client client-id	
Command	ip dhcp client client-id IF-ID no ip dhcp client client-id
Parameter	IF-ID：クライアント ID として使用する MAC アドレスのインターフェースを、以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定
デフォルト	対象 VLAN インターフェースの MAC アドレス
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	ApresiaNP シリーズでは各 VLAN インターフェースの MAC アドレスは共通のため、本コマンドをデフォルト以外に設定しても動作に違いはありません。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 100 インターフェースのクライアント ID を、VLAN 200 インターフェースの MAC アドレスに設定する方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# ip dhcp client client-id vlan 200
(config-if-vlan)#
```

4.1.3 ip dhcp client hostname

ip dhcp client hostname	
目的	DHCP クライアントが送信する DISCOVER メッセージなどに付与する、オプション 12 のホストネームを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip dhcp client hostname NAME no ip dhcp client hostname
Parameter	NAME：ホストネームを最大 64 文字で指定します。英数字とハイフンのみ使用可能です。ただし、先頭は英字のみ、末尾は英数字のみ指定可能です。
デフォルト	なし
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	本コマンドが未設定（デフォルト設定）の場合は、DISCOVER メッセージにオプション 12 は付与されません。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 100 インターフェースにおいて、オプション 12 のホストネームを Site-A-Switch に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# ip dhcp client hostname Site-A-Switch
(config-if-vlan)#
```

4.1.4 ip dhcp client lease

ip dhcp client lease	
目的	クライアントが要求するリース期間（DHCP クライアントが送信する DISCOVER メッセージなどに付与する、オプション 51 の IP アドレスリースタイム）を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip dhcp client lease DAYS [HOURS [MINUTES]] no ip dhcp client lease
Parameter	DAYS [HOURS [MINUTES]]：クライアントが要求するリース期間を指定します。 • DAYS：0～10000 日の範囲で指定します。 • HOURS（省略可能）：0～23 時間の範囲で指定します。 • MINUTES（省略可能）：0～59 分の範囲で指定します。
デフォルト	なし
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	本コマンドが未設定（デフォルト設定）の場合は、DISCOVER メッセージにオプション 51 は付与されません。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 100 インターフェースにおいて、クライアントが要求するリース期間を 5 日に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# ip dhcp client lease 5
(config-if-vlan)#
```

4.2 DHCP サーバーコマンド

DHCP サーバー関連の設定コマンドは以下のとおりです。

- ip dhcp pool
- network
- class（DHCP Server）
- address range
- host
- hardware-address
- client-identifier
- lease
- default-router
- domain-name（DHCP Server）
- dns-server（DHCP Server）
- netbios-node-type
- netbios-name-server
- next-server
- bootfile
- option
- ip dhcp class
- option hex
- ip dhcp use class
- ip dhcp excluded-address
- ip dhcp ping packets
- ip dhcp ping timeout
- service dhcp

DHCP サーバー関連の show／操作コマンドは以下のとおりです。

- show ip dhcp binding
- show ip dhcp conflict
- show ip dhcp pool
- show ip dhcp server
- show ip dhcp server statistics
- clear ip dhcp binding
- clear ip dhcp conflict
- clear ip dhcp server statistics

4.2.1 ip dhcp pool

ip dhcp pool	
目的	DHCP サーバーで DHCP アドレスプールを設定します。また、DHCP プール設定モードに遷移します。遷移後のプロンプトは（config-dhcp-pool)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip dhcp pool NAME no ip dhcp pool NAME
Parameter	NAME：DHCP アドレスプール名を最大 32 文字で指定します。ASCII コードの印字

ip dhcp pool	
	可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	DHCP サーバーは、DHCP クライアントから要求を受信した後、アドレスプールから IP アドレスを割り当てて、クライアントにアドレスを返信します。アドレスプールには、IP アドレスのネットワークまたは単一の IP アドレスのいずれかを含めることができます。アドレスプールのネットワークを指定する場合は、DHCP プール設定モードで network コマンドを実行してください。DHCP アドレスプールで手動バインディングエントリーを指定する場合は、client-identifier または hardware-address コマンドと host コマンドを実行してください。
制限・注意	• 動的割り当てのための DHCP アドレスプールは最大 23 個までサポートしており、1 つのプールあたり最大 1024 個のアドレスをリースできます。また、手動バインディングエントリーのための DHCP アドレスプールは最大 64 個設定でき、1 つのプールあたり 1 個の手動バインディングエントリーを設定できます。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP アドレスプール「pool1」を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)#
```

4.2.2 network

network	
目的	DHCP アドレスプールに対して関連付けられたマスクを使用して、ネットワークを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	network {NETWORK MASK | NETWORK/LEN} no network
Parameter	NETWORK MASK：ネットワークアドレスとサブネットマスクを指定します。（例：192.0.2.0 255.255.255.0） NETWORK/LEN：ネットワークアドレスとプレフィックス長を指定します。（例：192.0.2.0/24）
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	アドレスプールのネットワークを設定するために、DHCP プール設定モードで実行するコマンドです。 DHCP サーバーは、クライアントから要求を受信すると、アドレス割り当ての以下のルールに基づいて、アドレスプールまたはアドレスプール内のサブネットを選択します。IP アドレスがホストに割り当てられると、バインディングエントリーが作成され

network	
	ます。 • クライアントが DHCP サーバーに直接接続されていない場合、DISCOVER メッセージがリレーエージェントによって中継されます。サーバーは、パケットの GIADDR を含むサブネットが設定されたアドレスプールを選択します。アドレスプールが選択されると、サーバーはサブネットからアドレスを割り当てようとします。 • クライアントがサーバーに直接接続されている場合、サーバーは、受信インターフェースのプライマリーサブネットを含むアドレスプールのサブネット、またはそれと一致するアドレスプールのサブネットを検索します。 アドレスが特定のサブネットから割り当てられると、サブネットに関連付けられたネットワークマスクが、ネットワークマスクとしてユーザーに返信されます。DHCP アドレスプールに対して設定されたネットワークは、ナチュラルネットワークまたはサブネットワークです。設定された DHCP アドレスプールは、ツリーとして編成されます。ツリーのルートは、ナチュラルネットワークが含まれているアドレスプールです。サブネットワークが含まれているアドレスプールは、ルートの下にあるブランチです。手動バインディングエントリーが含まれているアドレスプールは、ブランチの下、またはルートの下にあるリーフです。ツリー構造に基づいて、子アドレスプールは、親アドレスプールの属性を引き継ぎます。ただし、リース属性だけは引き継がれません。
制限・注意	• セカンダリーIP アドレスで指定したサブネットでは、DHCP サーバー機能は動作しません。 • ネットワークが設定されたアドレスプールでは、手動バインディングエントリーを設定できません。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。 • 本設定を削除した場合には、そのアドレスプールの class コマンドの設定と option コマンドの設定も削除されます。 • ネットワークアドレスとサブネットマスクを指定して設定した場合でも、構成情報ではネットワークアドレスとプレフィックス長で表示されます。
バージョン	1.08.02

使用例：DHCP アドレスプール pool1 に対して、サブネット 10.1.0.0/16 を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# network 10.1.0.0/16
(config-dhcp-pool)# default-router 10.1.1.1
(config-dhcp-pool)#
```

4.2.3 class（DHCP Server）

class（DHCP Server）	
目的	DHCP アドレスプールで使用する DHCP クラスを設定します。また、DHCP プールクラス設定モードに遷移します。遷移後のプロンプトは（config-dhcp-pool-class)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	class NAME

class（DHCP Server）	
	no class NAME
Parameter	NAME：DHCP クラス名を最大 32 文字で指定します。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	DHCP サーバー機能において、DHCP クラスによるアドレス割り当てを使用する場合は、ip dhcp use class を有効に設定する必要があります。 option hex コマンドが未設定の DHCP クラスは「一致条件＝any」の扱いになり、すべての DHCP パケットが対象になります。 DHCP サーバー機能の DHCP アドレスプールで使用する場合は、address range コマンドで DHCP クラスに関連付ける割り当てる IP アドレスの範囲を設定します。受信した DHCP パケットが複数の DHCP クラスに一致する場合、一致したすべての DHCP クラスに関連付けられた IP アドレスの範囲が割り当て候補になります。
制限・注意	• DHCP クラスは最大 10 個設定できます。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP アドレスプール「Server-pool」で使用する DHCP クラスとして「Server-class」を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp class Server-class
(config-dhcp-class)# exit
(config)#
(config)# ip dhcp pool Server-pool
(config-dhcp-pool)# network 192.168.10.0/24
(config-dhcp-pool)# class Server-class
(config-dhcp-pool-class)#
```

4.2.4 address range

address range	
目的	DHCP クラスに関連付ける IP アドレスの範囲を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	address range START-IP END-IP no address range START-IP END-IP
Parameter	START-IP：IP アドレス範囲の最初の IP アドレスを指定します。 END-IP：IP アドレス範囲の最後の IP アドレスを指定します。
デフォルト	なし
モード	DHCP プールクラス設定モード
特権レベル	レベル：12
ガイドライン	DHCP サーバー機能において、DHCP クラスによるアドレス割り当てを使用する場合は、ip dhcp use class を有効に設定する必要があります。

address range	
	option hex コマンドが未設定の DHCP クラスは「一致条件＝any」の扱いになり、すべての DHCP パケットが対象になります。 DHCP クラスによるアドレス割り当てを有効にした場合は、address range コマンドで指定した範囲以外の IP アドレスは、割り当て候補から除外されます。
制限・注意	• すでに address range が設定されている DHCP クラスで address range を再設定した場合は、上書き設定されます。 • 設定済みの address range 設定から、一部の範囲だけを指定して削除することはできません。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP アドレスプール「pool1」の DHCP クラス「Customer-A」で、DHCP クラスに関連付ける IP アドレスの範囲を 192.169.10.100 から 192.168.10.200 に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp class Customer-A
(config-dhcp-class)# exit
(config)#
(config)# ip dhcp pool pool1
(config-dhcp-pool)# network 192.168.10.0/24
(config-dhcp-pool)# class Customer-A
(config-dhcp-pool-class)# address range 192.168.10.100 192.168.10.200
(config-dhcp-pool-class)#
```

4.2.5 host

host	
目的	DHCP アドレスプール内にある手動バインディングエントリーの IP アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	host {IP-ADDRESS MASK | IP-ADDRESS/LEN} no host
Parameter	IP-ADDRESS MASK：IPv4 アドレスとサブネットマスクを指定します。（例：192.0.2.100 255.255.255.0） IP-ADDRESS/LEN：IPv4 アドレスとプレフィックス長を指定します。（例：192.0.2.100/24）
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	バインディングエントリーでは、IP アドレスを、クライアント ID、またはホストの MAC アドレスとバインドできます。
制限・注意	• 手動バインディングエントリーは DHCP アドレスプールで 1 つだけ指定できます。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいっ

host	
	たん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。 • IPv4 アドレスとサブネットマスクを指定して設定した場合でも、構成情報では IPv4 アドレスとプレフィックス長で表示されます。
バージョン	1.08.02

使用例：「IP アドレス=192.0.2.201/24、MAC アドレス=00:00:5E:00:53:A1」の手動バインディングエントリー「pool1」を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# hardware-address 00:00:5E:00:53:A1
(config-dhcp-pool)# host 192.0.2.201/24
(config-dhcp-pool)#
```

4.2.6 hardware-address

hardware-address	
目的	DHCP アドレスプール内にある手動バインディングエントリーの MAC アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	hardware-address MAC-ADDRESS no hardware-address
Parameter	MAC-ADDRESS：手動バインディングエントリーとして登録したい DHCP クライアントの MAC アドレスを、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX）
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	バインディングエントリーは、IP アドレスと MAC アドレスまたはクライアント ID の間のマッピングです。手動バインディングエントリーを作成することで、IP アドレスがクライアントに手動で割り当てられます。 バインディングエントリーを使用して、IP アドレスを、クライアント ID、またはホストの MAC アドレスとバインドできます。 DHCP パケットのクライアント ID に基づいて手動バインディングエントリーを指定する場合は、client-identifier コマンドと host コマンドを実行してください。MAC アドレスに基づいて手動バインディングエントリーを指定する場合は、hardware-address コマンドと host コマンドを実行してください。
制限・注意	• 手動バインディングエントリーは DHCP アドレスプールで 1 つだけ指定できます。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：「IP アドレス=192.0.2.201/24、MAC アドレス=00:00:5E:00:53:A1」の手動バインディングエントリー「pool1」を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# hardware-address 00:00:5E:00:53:A1
(config-dhcp-pool)# host 192.0.2.201/24
(config-dhcp-pool)#
```

4.2.7 client-identifier

client-identifier	
目的	DHCP アドレスプール内の手動バインディングエントリーで、独自の DHCP クライアント ID を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	client-identifier IDENTIFIER no client-identifier
Parameter	IDENTIFIER：DHCP クライアント ID を最大 14 文字（16 進表記）で指定します。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	DHCP アドレスプール内の手動バインディングエントリーで有効なコマンドです。クライアント ID は、メディアタイプと MAC アドレス形式で設定されます。DHCP アドレスプールでは、手動バインディングエントリーを 1 つだけ指定できます。手動バインディングエントリーを使用して、IP アドレスを、クライアント ID、またはホストの MAC アドレスとバインドできます。 DHCP パケットのクライアント ID に基づいて手動バインディングエントリーを指定する場合は、client-identifier コマンドと host コマンドを実行してください。
制限・注意	• DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：「IP アドレス=192.0.2.202/24、クライアント ID=0x01524153203124」の手動バインディングエントリー「pool2」を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool2
(config-dhcp-pool)# client-identifier 01524153203124
(config-dhcp-pool)# host 192.0.2.202/24
(config-dhcp-pool)#
```

4.2.8 lease

lease	
目的	アドレスプールから割り当てられた IP アドレスのリース期間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lease {DAYS [HOURS [MINUTES [SECONDS]]] | infinite} no lease

lease	
Parameter	DAYS [HOURS [MINUTES [SECONDS]]]：リース期間を指定します。 • DAYS：0～365 日の範囲で指定します。 • HOURS（省略可能）：0～23 時間の範囲で指定します。 • MINUTES（省略可能）：0～59 分の範囲で指定します。 • SECONDS（省略可能）：0～59 秒の範囲で指定します。 infinite：リース期間を無制限に設定する場合に指定します。
デフォルト	リース期間：1 日
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	リース期間の設定は、親アドレスプールから引き継がれません。
制限・注意	• DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：アドレスプール「pool1」でのリースを 1 日に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# lease 1
(config-dhcp-pool)#
```

使用例：アドレスプール「pool1」でのリースを 1 時間に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# lease 0 1
(config-dhcp-pool)#
```

4.2.9 default-router

default-router	
目的	DHCP クライアントのデフォルトルーターを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	default-router IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8] no default-router IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]
Parameter	IP-ADDRESS：DHCP クライアントがデフォルトゲートウェイとして使用する IP アドレスを指定します。 IP-ADDRESS2...IP-ADDRESS8：複数のゲートウェイを設定する場合には、IP アドレスをスペースで区切って指定します。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	ルーターの IP アドレスは、クライアントのサブネットと同じサブネット上に存在する必要があります。ルーターは、優先順位に従って一覧表示されます。デフォルトルーターがすでに設定されている場合、後で設定したデフォルトルーターは、デフォ

default-router	
	ルトインターフェースリストに追加されます。
制限・注意	• デフォルトルーターとして使用する IP アドレスは、最大 8 個指定できます。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP アドレスプール内のデフォルトルーターの IP アドレスとして、10.1.1.1 を指定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# default-router 10.1.1.1
(config-dhcp-pool)#
```

4.2.10 domain-name（DHCP Server）

domain-name（DHCP Server）	
目的	DHCP クライアントのドメイン名を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	domain-name NAME no domain-name
Parameter	NAME：ドメイン名を最大 64 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 指定できるドメイン名は 1 つだけです。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP アドレスプール内でドメイン名に domain.com を指定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# domain-name domain.com
(config-dhcp-pool)#
```

4.2.11 dns-server（DHCP Server）

dns-server（DHCP Server）	
目的	DHCP クライアントの DNS サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	dns-server IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]

dns-server（DHCP Server）	
	no dns-server IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]
Parameter	IP-ADDRESS：DHCP クライアントが DNS サーバーとして使用する IP アドレスを指定します。 IP-ADDRESS2...IP-ADDRESS8：複数の DNS サーバーを設定する場合には、IP アドレスをスペースで区切って指定します。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	サーバーは、優先順位に従って一覧表示されます。DNS サーバーがすでに設定されている場合、後で設定された DNS サーバーは、DNS サーバーリストに追加されます。
制限・注意	• DNS サーバーとして使用する IP アドレスは、最大 8 個指定できます。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP アドレスプール内の DNS サーバーの IP アドレスとして、10.1.1.1 を指定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# dns-server 10.1.1.1
(config-dhcp-pool)#
```

4.2.12 netbios-node-type

netbios-node-type	
目的	Microsoft DHCP クライアントの NetBIOS ノードタイプを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	netbios-node-type {b-node | h-node | m-node | p-node} no netbios-node-type
Parameter	b-node：NetBIOS ノードタイプがブロードキャストの場合に指定します。 p-node：NetBIOS ノードタイプがピアツーピアでの場合に指定します。 m-node：NetBIOS ノードタイプが混合の場合に指定します。 h-node：NetBIOS ノードタイプがハイブリッドの場合に指定します。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	推奨のタイプは、ノードタイプ h-node（ハイブリッド）です。ノードタイプは、NetBIOS が名前を登録して解決するために使用する方式を決定します。ブロードキャストシステムではブロードキャストが使用されます。p ノードシステムでは、ネームサーバー（WINS）へのポイントツーポイントの名前クエリーだけが使用されます。m ノードシステムでは、最初にブロードキャストが使用され、次にネームサーバーのクエリーが行われます。ハイブリッドシステムでは、最初にネームサーバーの

netbios-node-type	
	クエリーが行われ、次にブロードキャストが使用されます。
制限・注意	• DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：NetBIOS ノードタイプを h-node として設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# netbios-node-type h-node
(config-dhcp-pool)#
```

4.2.13 netbios-name-server

netbios-name-server	
目的	Microsoft DHCP クライアントに WINS サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	netbios-name-server IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8] no netbios-name-server IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]
Parameter	IP-ADDRESS：DHCP クライアントが WINS サーバーとして使用する IP アドレスを指定します。 IP-ADDRESS2...IP-ADDRESS8：複数の WINS サーバーを設定する場合には、IP アドレスをスペースで区切って指定します。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	サーバーは、優先順位に従って一覧表示されます。ネームサーバーがすでに設定されている場合、後で設定されたネームサーバーは、デフォルトインターフェースリストに追加されます。
制限・注意	• WINS サーバーとして使用する IP アドレスは、最大 8 個指定できます。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：アドレスプール「pool1」の WINS サーバーとして、10.1.1.100 と 10.1.1.200 を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# netbios-name-server 10.1.1.100 10.1.1.200
(config-dhcp-pool)#
```

4.2.14 next-server

next-server	
目的	DHCP クライアントのブートサーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	next-server IP-ADDRESS no next-server
Parameter	IP-ADDRESS：DHCP クライアントがブートイメージファイルを取得するためのブートサーバーの IP アドレスを指定します。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 指定できるブートサーバーは 1 つだけです。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP アドレスプール pool1 で、ブートサーバー10.1.1.1 を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# next-server 10.1.1.1
(config-dhcp-pool)#
```

4.2.15 bootfile

bootfile	
目的	装置をブートするための DHCP クライアントの構成情報、またはブートイメージファイルを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	bootfile URL no bootfile
Parameter	URL：ブートファイルのファイルパス名を最大 64 文字で指定します。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP アドレスプール pool1 で、ブートファイルのファイルパス名を「dhcpbootfile.bin」に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# bootfile dhcpbootfile.bin
(config-dhcp-pool)#
```

4.2.16 option

option	
目的	DHCP サーバーオプションを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	option CODE {ascii STRING | hex {HEX-STRING | none} | ip IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]} no option CODE
Parameter	CODE：オプション番号を 1～254 の範囲で指定します。 ascii STRING：オプションの値を ASCII 文字列で設定する場合に、最大 255 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 hex HEX-STRING：オプションの値を 16 進文字列で設定する場合に、最大 254 文字で指定します。 hex none：オプションの値を、長さ 0（Length フィールドが 0 指定）に設定する場合に指定します。 ip IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]：オプションの値を IP アドレスで設定する場合に指定します。最大 8 個指定できます。
デフォルト	なし
モード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	DHCP プールで DHCP オプションを設定するコマンドです。DHCP オプションは、default-router コマンドなどの他のコマンドを、DHCP プール設定モードで実行することによっても設定できます。DHCP サーバーは、設定されたすべての DHCP オプションを、応答パケットで伝送します。設定されたすべての DHCP オプションは、サーバーが応答する DHCP パケットで伝送されます。 以下のオプションは、他の DHCP プール設定モードのコマンドで設定できます。ただし、option コマンドでは設定できません。 • オプション 1（ネットワークによって設定される Subnet Mask） • オプション 3（デフォルトルーターによって設定される Router Option） • オプション 6（DNS サーバーによって設定される Domain Name Server） • オプション 15（ドメイン名によって設定される Domain Name） • オプション 44（NetBIOS ネームサーバーによって設定される NetBIOS Name Server） • オプション 46（NetBIOS ノードタイプによって設定される NetBIOS Node Type） • オプション 51（リースによって設定される IP Address Lease Time） • オプション 58（リースによって設定される Renewal（T1）Time Value） • オプション 59（リースによって設定される Rebinding（T2）Time Value）

option	
	以下のオプションは、本コマンドの実行では設定できません。 • オプション 12（Host Name、デフォルトオプション） • オプション 50（Requested Address、デフォルトオプション） • オプション 53（DHCP Message Type、デフォルトオプション） • オプション 54（Server Identifier、デフォルトオプション） • オプション 55（Parameter Request List、デフォルトオプション） • オプション 61（Client Identifier、デフォルトオプション） • オプション 82（Relay Agent Information Option、デフォルトオプション）
制限・注意	• 設定される 16 進文字列の長さは偶数です（例：001100 は可、11223 は不可）。同じオプション番号に指定できる文字列は 1 つだけです。 • DHCP オプションの合計長には制限があります。制限はクライアントが指定しますが、クライアントが指定しない場合、サーバーによって決定されることもあります。制限の指定がない場合、最大長は 312 です。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP アドレスプール test で、オプション 40（NIS Domain）を ASCII 文字列 example.com で設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool test
(config-dhcp-pool)# option 40 ascii example.com
(config-dhcp-pool)#
```

使用例：DHCP アドレスプール test で、オプション 72（WWW Server）を IP アドレス 192.0.2.100 と 192.0.2.200 で設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool test
(config-dhcp-pool)# option 72 ip 192.0.2.100 192.0.2.200
(config-dhcp-pool)#
```

4.2.17 ip dhcp class

ip dhcp class	
目的	DHCP クラスを設定します。また、DHCP クラス設定モードに遷移します。遷移後のプロンプトは（config-dhcp-class)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip dhcp class NAME no ip dhcp class NAME
Parameter	NAME：DHCP クラス名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12

ip dhcp class	
ガイドライン	DHCP サーバー機能において、DHCP クラスによるアドレス割り当てを使用する場合は、ip dhcp use class を有効に設定する必要があります。 option hex コマンドが未設定の DHCP クラスは「一致条件＝any」の扱いになり、すべての DHCP パケットが対象になります。
制限・注意	• DHCP クラスは最大 10 個設定できます。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP クラス「Service-A」で、DHCP オプション 60 の一致パターンを 0x616263 に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp class Service-A
(config-dhcp-class)# option 60 hex 616263
(config-dhcp-class)#
```

4.2.18 option hex

option hex	
目的	DHCP クラスの DHCP オプション一致条件を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	option CODE hex PATTERN [*] [bitmask MASK] no option CODE hex PATTERN [*] [bitmask MASK]
Parameter	CODE：比較対象の DHCP オプション番号を指定します。 hex PATTERN：比較対象の DHCP オプションの値、またはパターンを 16 進数で、オクテット単位で指定します。*や bitmask を指定しない場合は比較対象の DHCP オプションの値をすべて指定します。 * (省略可能)：パターンの残りのビットを比較しない場合に指定します。 bitmask MASK（省略可能）：指定したパターンのうち、比較するビットのマスクを FF(大文字)で、比較しないビットのマスクを 00 で、オクテット単位で指定します。マスクは FF(大文字)または 00 のみ指定できます。
デフォルト	なし
モード	DHCP クラス設定モード
特権レベル	レベル：12
ガイドライン	DHCP サーバー機能において、DHCP クラスによるアドレス割り当てを使用する場合は、ip dhcp use class を有効に設定する必要があります。 option hex コマンドが未設定の DHCP クラスは「一致条件＝any」の扱いになり、すべての DHCP パケットが対象になります。 1 つの DHCP クラスに複数の一致条件を設定できます。 1 つの DHCP クラスに同じ DHCP オプション番号の一致条件を複数設定した場合は OR 条件動作になり、同じ DHCP オプション番号のいずれかの条件に一致すると、その DHCP クラスの対象になります。

option hex	
	1 つの DHCP クラスに異なる DHCP オプション番号の一致条件を複数設定した場合は AND 条件動作になり、異なる DHCP オプション番号のすべての条件に一致すると、その DHCP クラスの対象になります。 一般的に使用される DHCP オプションは以下のとおりです。 • オプション 60（Vendor Class Identifier） • オプション 61（Client Identifier） • オプション 77（User Class） • オプション 82（Relay Agent Information Option）（DHCP サーバーのみ） • オプション 124（Vendor-identifying Vendor Class） • オプション 125（Vendor-identifying Vendor-specific Information）
制限・注意	• DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP クラス「Service-A」で、DHCP オプション 60 の一致パターンを 0x616263 と 0x414243 に設定する方法を示します。また、DHCP クラス「Service-B」で、DHCP オプション 60 の一致パターンを 0x4150*と 0x6170*に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp class Service-A
(config-dhcp-class)# option 60 hex 616263
(config-dhcp-class)# option 60 hex 414243
(config-dhcp-class)# exit
(config)# ip dhcp class Service-B
(config-dhcp-class)# option 60 hex 4150 *
(config-dhcp-class)# option 60 hex 6170 *
(config-dhcp-class)# exit
(config)#
```

4.2.19 ip dhcp use class

ip dhcp use class	
目的	DHCP サーバー機能において、DHCP クラスによるアドレス割り当てを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip dhcp use class no ip dhcp use class
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	DHCP サーバー機能において、DHCP クラスによるアドレス割り当てを使用する場合は、ip dhcp use class を有効に設定する必要があります。 option hex コマンドが未設定の DHCP クラスは「一致条件＝any」の扱いになり、すべての DHCP パケットが対象になります。 DHCP クラスによるアドレス割り当てを有効にした場合は、network コマンド以外に address range コマンドで割り当てる IPv4 アドレスの範囲を設定します。

ip dhcp use class	
	address range コマンドで指定した範囲以外の IPv4 アドレスは、割り当て候補から除外されます。 同一プールに複数の DHCP クラスを設定していて、受信した DHCP パケットが複数の DHCP クラスに一致する場合、一致したすべての DHCP クラスに関連付けられた IP アドレスの範囲が割り当て候補になります。
制限・注意	• DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP サーバー機能において、DHCP クラスによるアドレス割り当てを有効にする方法を示します。

```
# configure terminal
(config)# ip dhcp use class
(config)#
```

4.2.20 ip dhcp excluded-address

ip dhcp excluded-address	
目的	IP アドレスの範囲をクライアントへの割り当てから除外します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip dhcp excluded-address START-IP END-IP no ip dhcp excluded-address START-IP END-IP
Parameter	START-IP：除外する IP アドレス、または除外する IP アドレス範囲の最初の IP アドレスを指定します。 END-IP：除外する IP アドレス範囲の最後の IP アドレスを指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	DHCP サーバーは、DHCP アドレスプール内のアドレスを自動的に DHCP クライアントに割り当てます。割り当てができないのは、ルーター上のインターフェースの IP アドレスと、ip dhcp excluded-address コマンドで指定した除外対象アドレスだけです。複数のアドレス範囲を除外できます。除外対象のアドレスの範囲を削除する場合は、以前に設定したアドレスの範囲を正確に指定してください。
制限・注意	• 除外対象の IP アドレスの範囲は最大 5 個設定できます。 • DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：アドレス範囲 10.1.1.1～10.1.1.255 と 10.2.1.1～10.2.1.255 を除外する方法を示します。

```
# configure terminal
(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.255
(config)# ip dhcp excluded-address 10.2.1.1 10.2.1.255
(config)#
```

4.2.21 ip dhcp ping packets

ip dhcp ping packets	
目的	割り当て候補の IP アドレスに対して、DHCP サーバーが ping による事前確認で送信する ping パケットの数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip dhcp ping packets VALUE no ip dhcp ping packets
Parameter	VALUE：ping パケットの送信回数を 0～10 回の範囲で指定します。
デフォルト	2
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	DHCP サーバーは、DHCP クライアントに IP アドレスを割り当てる前に、その IP アドレスがすでに使用されていないかどうかを ping によって確認します。ping による事前確認で応答がない場合、その IP アドレスは割り当て可能と判断されて、DHCP クライアントに割り当てられます。ping による事前確認で応答があった場合は、その IP アドレスは割り当て候補から除外され、DHCP 競合エントリーとして登録されます。 送信回数を 0 回に設定すると、ping による事前確認は無効になります。
制限・注意	• DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：ping による事前確認で送信する ping パケットの数を、3 に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp ping packets 3
(config)#
```

4.2.22 ip dhcp ping timeout

ip dhcp ping timeout	
目的	ping による事前確認の応答タイムアウト時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip dhcp ping timeout MILLISECONDS no ip dhcp ping timeout
Parameter	MILLISECONDS：ping 応答タイムアウト時間を 100～10,000 ミリ秒の範囲で、100 ミリ秒単位で指定します。
デフォルト	500 ミリ秒 (0.5 秒)
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	DHCP サーバーは、DHCP クライアントに IP アドレスを割り当てる前に、その IP アドレスがすでに使用されていないかどうかを ping によって確認します。ping による事前確認で応答がない場合、その IP アドレスは割り当て可能と判断されて、DHCP クライアントに割り当てられます。ping による事前確認で応答があった場合

ip dhcp ping timeout	
	は、その IP アドレスは割り当て候補から除外され、DHCP 競合エントリーとして登録されます。
制限・注意	• DHCP サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：ping による事前確認の応答タイムアウト時間を、800 ミリ秒に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp ping timeout 800
(config)#
```

4.2.23 service dhcp

service dhcp	
目的	DHCP サーバー機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	service dhcp no service dhcp
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• DHCP サーバーが有効状態では DHCP 関連の設定を変更しても即反映されません。設定変更を反映するには、no service dhcp コマンドにて DHCP サーバー機能をいったん無効状態にした後、再度 DHCP サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCP サーバー機能を有効にする方法を示します。

```
# configure terminal
(config)# service dhcp
(config)#
```

4.2.24 show ip dhcp binding

show ip dhcp binding	
目的	DHCP サーバーでアドレスバインディングエントリーを表示します。
Command	show ip dhcp binding [IP-ADDRESS]
Parameter	IP-ADDRESS（省略可能）：表示するアドレスバインディングエントリーの IP アドレスを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	IP アドレスを指定しない場合、すべてのアドレスバインディングエントリーが表示されます。

show ip dhcp binding	
制限・注意	-
バージョン	1.08.02

使用例：すべてのバインディングエントリーを表示する方法を示します。

```
# show ip dhcp binding
 (1)                (2)                (3)                    (4)
 IP address         Client-ID/         Lease expiration       Type
                   Hardware address
 ---------------- ------------------ -------------------- ---------
 10.1.1.1         0100B810863212     Mar 10 2016 09:12 AM Automatic
 10.1.9.1         0100B7443DC224     Mar 10 2016 10:12 AM Automatic
 10.1.11.10       0100B22291226D     Infinite             Manual
```

項番	説明
(1)	DHCP クライアントに割り当てた IP アドレスを表示します。
(2)	DHCP クライアント ID または MAC アドレスを表示します。
(3)	リース満了日時を表示します。
(4)	IP アドレスの割り当て方法（Automatic：自動／Manual：固定）を表示します。

使用例：IP アドレス 10.1.1.1 を指定して、バインディングエントリーを表示する方法を示します。

```
# show ip dhcp binding 10.1.1.1
 (1)                (2)                (3)                    (4)
 IP address         Client-ID/         Lease expiration       Type
                   Hardware address
 ---------------- ------------------ -------------------- ---------
 10.1.1.1         0100B810863212     Mar 10 2016 09:12 AM Automatic
```

項番	説明
(1)	DHCP クライアントに割り当てた IP アドレスを表示します。
(2)	DHCP クライアント ID または MAC アドレスを表示します。
(3)	リース満了日時を表示します。
(4)	IP アドレスの割り当て方法（Automatic：自動／Manual：固定）を表示します。

4.2.25 show ip dhcp conflict

show ip dhcp conflict	
目的	DHCP サーバーの割り当て候補から除外された IP アドレス（DHCP 競合エントリー）を表示します。
Command	show ip dhcp conflict [IP-ADDRESS]
Parameter	IP-ADDRESS（省略可能）：表示する DHCP 競合エントリーの IP アドレスを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	DHCP サーバーは、DHCP クライアントに IP アドレスを割り当てる前に、その IP アドレスがすでに使用されていないかどうかを ping によって確認します。ping による事前確認で応答があった場合は、その IP アドレスは割り当て候補から除外され、

show ip dhcp conflict	
	DHCP 競合エントリーとして登録されます。 DHCP 競合エントリーとして登録された IP アドレスは、clear ip dhcp conflict コマンドで手動でクリアされるまで割り当て候補にはなりません。 IP アドレスを指定しない場合、すべての DHCP 競合エントリーが表示されます。
制限・注意	-
バージョン	1.08.02

使用例：すべての DHCP 競合エントリーを表示する方法を示します。

```
# show ip dhcp conflict
 (1)              (2)              (3)
 IP address       Detected Method  Detection time
 ---------------  ---------------  --------------------
 10.1.1.1         Ping             Mar 15 2017 05:15 PM
```

項番	説明
(1)	DHCP 競合エントリーとして登録された IP アドレスを表示します。
(2)	競合の検出方法を表示します。 Gratuitous ARP：DHCP クライアントからの DHCP Decline メッセージで検出した場合 Ping：DHCP サーバーが送信する ping による事前確認で検出した場合
(3)	競合の検出日時を表示します。

4.2.26 show ip dhcp pool

show ip dhcp pool	
目的	DHCP アドレスプールに関する設定を表示します。
Command	show ip dhcp pool [NAME]
Parameter	NAME (省略可能)：表示する DHCP アドレスプールを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	DHCP アドレスプールを指定しない場合は、すべての DHCP アドレスプールの設定が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：すべての DHCP アドレスプールの設定を表示する方法を示します。

```
# show ip dhcp pool

 Pool name: server-v10 ...(1)
   Network: 192.0.2.0/24 ...(2)
   Boot file: ...(3)
   Default router: 192.0.2.254 ...(4)
   DNS server: 192.168.0.11 ...(5)
   NetBIOS server: ...(6)
   Domain name: ...(7)
   Lease: 1 days 0 hours 0 minutes 0 seconds ...(8)
   NetBIOS node type: ...(9)
   Next server: 0.0.0.0 ...(10)
```

```
   Class c1 ...(11)
     address-range 192.0.2.101 192.0.2.130 ...(12)
   Remaining unallocated address number: 252 ...(13)
   Number of leased addresses: 2 ...(14)
```

項番	説明
(1)	DHCP アドレスプール名を表示します。
(2)	サブネットを表示します。
(3)	ブートイメージファイルのパスを表示します。
(4)	デフォルトゲートウェイの IP アドレスを表示します。
(5)	DNS サーバーの IP アドレスを表示します。
(6)	WINS サーバーの IP アドレスを表示します。
(7)	ドメイン名を表示します。
(8)	IP アドレスのリース期間を表示します。
(9)	NetBIOS ノードタイプを表示します。
(10)	ブートイメージファイルを取得するためのブートサーバーの IP アドレスを表示します。
(11)	関連付けられた DHCP クラスを表示します。
(12)	DHCP クラスに関連付ける IP アドレスの範囲を表示します。
(13)	リースされていない IP アドレスの個数を表示します。
(14)	リースされた IP アドレスの個数を表示します。

4.2.27 show ip dhcp server

show ip dhcp server	
目的	DHCP サーバーの設定を表示します。
Command	show ip dhcp server
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCP サーバーの設定を表示する方法を示します。

```
# show ip dhcp server

 DHCP Service: Disabled ...(1)
 Ping packets number: 3 ...(2)
 Ping timeout: 500 ms ...(3)
 Excluded Addresses ...(4)
  10.1.1.1 - 10.1.1.255

 List of DHCP server configured address pool ...(5)
  pool1  pool2  pool3  pool4
  pool5  pool6  pool7  pool8
  pool9
```

項番	説明
(1)	DHCP サーバーの有効(Enabled)／無効(Disabled)を表示します。
(2)	ping による事前確認の送信回数を表示します。
(3)	ping による事前確認の応答タイムアウト時間を表示します。
(4)	除外 IP アドレスの範囲を表示します。
(5)	DHCP プール（動的割り当てのための DHCP アドレスプール、手動バインディングエントリーのための DHCP アドレスプール）を表示します。

4.2.28 show ip dhcp server statistics

show ip dhcp server statistics	
目的	DHCP サーバーの統計情報を表示します。
Command	show ip dhcp server statistics
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	すべてのカウンターが累積されます。
制限・注意	-
バージョン	1.08.02

使用例：DHCP サーバーの統計情報を表示する方法を示します。

```
# show ip dhcp server statistics

 Address pools           3 ...(1)
 Automatic bindings      100 ...(2)
 Manual bindings         2 ...(3)
 Malformed messages      0 ...(4)
 Renew messages          0 ...(5)

 Messages                Received ...(6)
 BOOTREQUEST             12
 DHCPDISCOVER            200
 DHCPREQUEST             178
 DHCPDECLINE             0
 DHCPRELEASE             0
 DHCPINFORM              0

 Messages                Sent ...(7)
 BOOTREPLY               12
 DHCPOFFER               190
 DHCPACK                 172
 DHCPNAK                 6
```

項番	説明
(1)	DHCP プール（動的割り当てのための DHCP アドレスプール、手動バインディングエントリーのための DHCP アドレスプール）の個数を表示します。
(2)	動的に割り当てられた IP アドレスの個数を表示します。
(3)	手動バインディングエントリーの個数を表示します。

項番	説明
(4)	DHCP サーバーが受信した不正な DHCP メッセージの個数を表示します。
(5)	リースされた IP アドレスを更新する DHCP メッセージの個数を表示します。
(6)	受信した DHCP メッセージの個数を、DHCP メッセージの種類ごとに表示します。
(7)	送信した DHCP メッセージの個数を、DHCP メッセージの種類ごとに表示します。

4.2.29 clear ip dhcp binding

clear ip dhcp binding	
目的	DHCP サーバーデータベースから、アドレスバインディングエントリーを削除します。
Command	clear ip dhcp {all | pool NAME} binding {* | IP-ADDRESS}
Parameter	all：すべての DHCP アドレスプールを対象にする場合に指定します。 pool NAME：特定の DHCP アドレスプールを対象にする場合に指定します。 *：対象の DHCP アドレスプールからすべてのアドレスバインディングエントリーを削除する場合に指定します。 IP-ADDRESS：削除するアドレスバインディングエントリーの IP アドレスを指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	DHCP アドレスプールに all を指定して、IP アドレスに*を指定した場合、すべての自動バインディングエントリーが削除されます。 DHCP アドレスプールに all を指定して、特定の IP アドレスを指定した場合、指定した IP アドレスの自動バインディングエントリーが削除されます。 特定の DHCP アドレスプールを指定して、IP アドレスに*を指定した場合、その DHCP アドレスプールのすべての自動バインディングエントリーが削除されます。 特定の DHCP アドレスプールを指定して、特定の IP アドレスを指定した場合、その DHCP アドレスプールの指定した IP アドレスの自動バインディングエントリーが削除されます。
制限・注意	-
バージョン	1.08.02

使用例：IP アドレスが 10.12.1.99 の自動バインディングエントリーを削除する方法を示します。

```
# clear ip dhcp all binding 10.12.1.99
#
```

使用例：すべての自動バインディングエントリーを削除する方法を示します。

```
# clear ip dhcp all binding *
#
```

使用例：DHCP アドレスプール「pool1」のすべての自動バインディングエントリーを削除する方法を示します。

```
# clear ip dhcp pool pool1 binding *
#
```

使用例：DHCP アドレスプール「pool2」の、IP アドレスが 10.13.2.99 の自動バインディングエントリーを削除する方法を示します。

```
# clear ip dhcp pool pool2 binding 10.13.2.99
#
```

4.2.30 clear ip dhcp conflict

clear ip dhcp conflict	
目的	DHCP サーバーデータベースから、DHCP 競合エントリーを削除します。
Command	clear ip dhcp {all | pool NAME} conflict {* | IP-ADDRESS}
Parameter	all：すべての DHCP アドレスプールを対象にする場合に指定します。 pool NAME：特定の DHCP アドレスプールを対象にする場合に指定します。 *：対象の DHCP アドレスプールからすべての DHCP 競合エントリーを削除する場合に指定します。 IP-ADDRESS：削除する DHCP 競合エントリーの IP アドレスを指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	DHCP アドレスプールに all を指定して、IP アドレスに*を指定した場合、すべての DHCP 競合エントリーが削除されます。 DHCP アドレスプールに all を指定して、特定の IP アドレスを指定した場合、指定した IP アドレスの DHCP 競合エントリーが削除されます。 特定の DHCP アドレスプールを指定して、IP アドレスに*を指定した場合、その DHCP アドレスプールのすべての DHCP 競合エントリーが削除されます。 特定の DHCP アドレスプールを指定して、特定の IP アドレスを指定した場合、その DHCP アドレスプールの指定した IP アドレスの DHCP 競合エントリーが削除されます。
制限・注意	-
バージョン	1.08.02

使用例：IP アドレスが 10.12.1.99 の DHCP 競合エントリーを削除する方法を示します。

```
# clear ip dhcp all conflict 10.12.1.99
#
```

使用例：すべての DHCP 競合エントリーを削除する方法を示します。

```
# clear ip dhcp all conflict *
#
```

使用例：DHCP アドレスプール「pool1」のすべての DHCP 競合エントリーを削除する方法を示します。

```
# clear ip dhcp pool pool1 conflict *
#
```

使用例：DHCP アドレスプール「pool2」の、IP アドレスが 10.13.2.99 の DHCP 競合エントリーを削除する方法を示します。

```
# clear ip dhcp pool pool2 conflict 10.13.2.99
#
```

4.2.31 clear ip dhcp server statistics

clear ip dhcp server statistics	
目的	DHCP サーバーの統計情報を消去します。
Command	clear ip dhcp server statistics
Parameter	なし
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCP サーバーの統計情報を消去する方法を示します。

```
# clear ip dhcp server statistics
#
```

4.3 DHCPv6 クライアントコマンド

DHCPv6 クライアント関連の設定コマンドは以下のとおりです。

- ipv6 dhcp client pd

DHCPv6 クライアント関連の show／操作コマンドは以下のとおりです。

- show ipv6 dhcp
- show ipv6 dhcp interface
- clear ipv6 dhcp client

4.3.1 ipv6 dhcp client pd

ipv6 dhcp client pd	
目的	DHCPv6-PD によるプレフィックス委譲を要求する DHCPv6 クライアント機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	**ipv6 dhcp client pd** {PREFIX-NAME [**rapid-commit**] | **hint** IPV6-PREFIX} **no ipv6 dhcp client pd**
Parameter	PREFIX-NAME：プレフィックス名を最大 12 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 rapid-commit（省略可能）：DHCPv6 の Rapid Commit オプションを有効にする場合に指定します。デフォルトは無効です。 hint IPV6-PREFIX：ヒントとして、メッセージで送信される IPv6 プレフィックスを指定します。
デフォルト	無効
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	DHCPv6 サーバーから委譲されたプレフィックスは、本設定で指定したプレフィックス名に関連付けられます。このプレフィックス名を使用して、IPv6 アドレスを設定することもできます。 hint パラメーターを指定した場合、指定したヒントプレフィックスは、プレフィックス委譲サーバーへの要求メッセージに含まれます。指定できるヒントプレフィックスは、1 つだけです。 DHCPv6 の Rapid Commit オプションを使用する場合は、DHCPv6 サーバーとクライアントの両方で有効にする必要があります。 クライアントが複数のサーバーからアドバタイズメントを受信すると、クライアントは最も優先度の高いサーバーを使用します。クライアントはサーバーから委譲された複数のプレフィックスを受け入れます。
制限・注意	• 同一 VLAN インターフェースでは、DHCPv6 サーバー機能と DHCPv6 クライアント機能を同時に有効にすることはできません。
バージョン	1.08.02

使用例：VLAN 1 インターフェースで、プレフィックス名「test-prefix」を指定して、DHCPv6-PD によるプレフィックス委譲を要求する DHCPv6 クライアント機能を有効にする方法を示します。

```
# configure terminal
(config)# interface vlan 1
```

```
(config-if-vlan)# ipv6 dhcp client pd test-prefix
(config-if-vlan)#
```

4.3.2 show ipv6 dhcp

show ipv6 dhcp	
目的	自装置の DUID（DHCP Unique Identifier）を表示します。
Command	show ipv6 dhcp
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：自装置の DUID（DHCP Unique Identifier）を表示する方法を示します。

```
# show ipv6 dhcp

This device's DUID is 00030006fc6dd1f2821f ...(1)
```

項番	説明
(1)	DUID（DHCP Unique Identifier）を表示します。

4.3.3 show ipv6 dhcp interface

show ipv6 dhcp interface	
目的	インターフェースの DHCPv6 関連の設定を表示します。
Command	show ipv6 dhcp interface [IF-NAME]
Parameter	IF-NAME（省略可能）：DHCPv6 関連の設定を表示する VLAN インターフェース名（vlan と VLAN ID の間を空けない形式）を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	インターフェースを指定しない場合、DHCPv6 機能が有効化されているすべてのインターフェースが表示されます。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 インターフェースで、DHCPv6 サーバーが動作している場合の表示例を示します。

```
# show ipv6 dhcp interface vlan1

vlan1 is in server mode ...(1)
  IPv6 DHCP pool is pool1 ...(2)
  Preference value: 0 ...(3)
  Hint from client: ignored ...(4)
  Rapid-Commit is disabled ...(5)
```

項番	説明
(1)	インターフェースの DHCPv6 関連の設定を表示します。 <IF-NAME> is not in DHCPv6 mode：DHCPv6 関連の設定が未設定 <IF-NAME> is in server mode：DHCPv6 サーバーモード
(2)	DHCPv6 プレフィックスプール名を表示します。
(3)	アドバタイズメントメッセージ内のプリファレンス（優先度）を表示します。
(4)	DHCP SOLICIT メッセージ内のクライアントからのヒントの扱い（allowed：利用する／ignored：無視する）を表示します。
(5)	DHCPv6 の Rapid Commit オプションの有効(enabled)／無効(disabled)を表示します。

使用例：VLAN 1 インターフェースが DHCPv6 クライアントとして動作し、DHCPv6-PD でプレフィックス委譲された場合の表示例を示します。

```
# show ipv6 dhcp interface

vlan1 is in client mode ...(1)
  State is OPEN
  List of known servers:
    Reachable via address: fe80::240:66ff:feac:31e9 ...(2)
    Configuration parameters:
        IA PD: IA ID 2, T1 302400, T2 483840 ...(3)
          Prefix: fd00:10:10:10:10::/96 ...(4)
                (5)                          (6)
                preferred lifetime 604800, valid lifetime 2592000
  Prefix name: test-001 ...(7)
  Rapid-Commit: disabled ...(8)
```

使用例：VLAN 1 インターフェースが DHCPv6 クライアントとして動作し、DHCPv6 で IPv6 アドレスを割り当てられた場合の表示例を示します。

```
# show ipv6 dhcp interface

vlan1 is in client mode ...(1)
  State is OPEN
  List of known servers:
    Reachable via address: fe80::240:66ff:feac:31e9 ...(2)
    Configuration parameters:
        IA NA: IA ID 2, T1 302400, T2 483840 ...(9)
          Address: fd00:192:168:10::1001/64 ...(10)
                  (5)                          (6)
                  preferred lifetime 604800, valid lifetime 2592000
  Rapid-Commit: disabled ...(8)
```

項番	説明
(1)	インターフェースの DHCPv6 関連の設定を表示します。 <IF-NAME> is not in DHCPv6 mode：DHCPv6 関連の設定が未設定 <IF-NAME> is in client mode：DHCPv6 クライアントモード
(2)	DHCPv6 サーバーのリンクローカルアドレスを表示します。
(3)	DHCPv6-PD で委譲された IPv6 アドレスプレフィックスの情報を表示します。
(4)	IPv6 アドレスプレフィックスを表示します。
(5)	IPv6 アドレスプレフィックス、または IPv6 アドレスの推奨期間を表示します。
(6)	IPv6 アドレスプレフィックス、または IPv6 アドレスの有効期間を表示します。

項番	説明
(7)	IPv6 アドレスプレフィックス名を表示します。
(8)	DHCPv6 の Rapid Commit オプションの有効(enabled)／無効(disabled)を表示します。
(9)	割り当てられた IPv6 アドレスの情報を表示します。
(10)	IPv6 アドレスを表示します。

4.3.4 clear ipv6 dhcp client

clear ipv6 dhcp client	
目的	VLAN インターフェースの DHCPv6 クライアントを再起動します。
Command	clear ipv6 dhcp client IF-NAME
Parameter	IF-NAME：DHCPv6 クライアントを再起動する VLAN インターフェース（vlan と VLAN ID の間を空けない形式）を指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 インターフェースの DHCPv6 クライアントを再起動する方法を示します。

```
# clear ipv6 dhcp client vlan1
#
```

4.4 DHCPv6 サーバーコマンド

DHCPv6 サーバー関連の設定コマンドは以下のとおりです。

- ipv6 dhcp pool
- address prefix
- address-assignment
- domain-name（DHCPv6 Server）
- dns-server（DHCPv6 Server）
- prefix-delegation pool
- prefix-delegation
- ipv6 dhcp excluded-address
- ipv6 local pool
- ipv6 dhcp server
- service ipv6 dhcp

DHCPv6 サーバー関連の show／操作コマンドは以下のとおりです。

- show ipv6 dhcp binding
- show ipv6 dhcp pool
- show ipv6 excluded-address
- show ipv6 local pool
- show ipv6 dhcp operation
- clear ipv6 dhcp binding

4.4.1 ipv6 dhcp pool

ipv6 dhcp pool	
目的	DHCPv6 サーバーで DHCPv6 プレフィックスプールを設定します。また、DHCPv6 プール設定モードに遷移します。遷移後のプロンプトは（config-dhcp)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 dhcp pool NAME no ipv6 dhcp pool NAME
Parameter	NAME：DHCPv6 プレフィックスプール名を最大 12 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドで設定した DHCPv6 プレフィックスプールは、ipv6 dhcp server コマンドで適用するインターフェースと関連付けます。
制限・注意	• IPv6 アドレスを割り当てるための DHCPv6 プレフィックスプールと、プレフィックス委譲のための DHCPv6 プレフィックスプールを、装置全体で合わせて最大 16 個まで設定できます。 • 手動エントリーは、DHCPv6 手動バインディングエントリーと手動プレフィックス委譲エントリーを、装置全体で合わせて最大 64 個まで設定できます。 • DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能

ipv6 dhcp pool	
	をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCPv6 プレフィックスプール「pool1」を設定する方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool1
(config-dhcp)#
```

4.4.2 address prefix

address prefix	
目的	IPv6 アドレスを割り当てるための DHCPv6 プレフィックスプールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	address prefix IPV6-PREFIX/LEN [lifetime VALID-LT PREFERRED-LT] no address prefix
Parameter	IPV6-PREFIX/LEN：DHCPv6 クライアントに割り当てる IPv6 アドレスプレフィックスとプレフィックス長を指定します。 lifetime VALID-LT PREFERRED-LT（省略可能）：VALID-LT（有効期間）と PREFERRED-LT（推奨期間）を、60～4,294,967,295 秒の範囲で指定します。有効期間は推奨期間より長くなるように指定してください。
デフォルト	VALID-LT（有効期間）未指定時：2,592,000 秒（30 日） PREFERRED-LT（推奨期間）未指定時：604,800 秒（7 日）
モード	DHCPv6 プール設定モード
特権レベル	レベル：12
ガイドライン	DHCPv6 クライアントから要求を受信すると、受信したインターフェースに関連付けられた DHCPv6 プレフィックスプールをチェックします。 対象の DHCPv6 プレフィックスプールに、要求元クライアントに一致する DHCPv6 手動バインディングエントリー（address-assignment）が設定されている場合は、その IPv6 アドレスが割り当てられます。一致する DHCPv6 手動バインディングエントリーが存在しない場合は、指定した IPv6 アドレスプレフィックスから IPv6 アドレスが割り当てられます。 設定済みの状態で本コマンドを新たに設定すると、上書き設定されます。
制限・注意	• 1 つの DHCPv6 プレフィックスプールにおいて、設定できる IPv6 アドレスプレフィックスは 1 つだけです。 • 本設定を削除すると、対象の DHCPv6 プレフィックスプールに設定されている address-assignment 設定も削除されます。 • DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCPv6 プレフィックスプール「v6-pool-1」において、IPv6 アドレスプレフィックス「2001:db8:10:10::/64」を設定する方法を示します。

```
# configure terminal
```

```
(config)# ipv6 dhcp pool v6-pool-1
(config-dhcp)# address prefix 2001:db8:10:10::/64
(config-dhcp)#
```

4.4.3 address-assignment

address-assignment	
目的	DHCPv6 手動バインディングエントリーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	address-assignment IPV6-ADDRESS DUID [iaid IAID] [lifetime VALID-LT PREFERRED-LT] no address-assignment IPV6-ADDRESS DUID [iaid IAID]
Parameter	IPV6-ADDRESS：DHCPv6 手動バインディングエントリーで割り当てる IPv6 アドレスを指定します。 DUID：DHCPv6 クライアントの DUID（DHCP Unique Identifier）を指定します。 iaid IAID（省略可能）：DHCPv6 クライアントの IAID（Identity Association Identifier）を指定します。 lifetime VALID-LT PREFERRED-LT（省略可能）：VALID-LT（有効期間）と PREFERRED-LT（推奨期間）を、60～4,294,967,295 秒の範囲で指定します。有効期間は推奨期間より長くなるように指定してください。
デフォルト	VALID-LT（有効期間）未指定時：2,592,000 秒（30 日） PREFERRED-LT（推奨期間）未指定時：604,800 秒（7 日）
モード	DHCPv6 プール設定モード
特権レベル	レベル：12
ガイドライン	DHCPv6 クライアントから要求を受信すると、受信したインターフェースに関連付けられた DHCPv6 プレフィックスプールをチェックします。 DUID と IAID を指定した DHCPv6 手動バインディングエントリーの場合、DHCPv6 クライアントからのリクエストメッセージに IANA オプションが含まれていて、DUID と IAID の両方が一致した DHCPv6 クライアントに、指定した IPv6 アドレスが割り当てられます。 DUID のみを指定した DHCPv6 手動バインディングエントリーの場合、DUID が一致した DHCPv6 クライアントに、指定した IPv6 アドレスが割り当てられます。 一致する DHCPv6 手動バインディングエントリーが存在しない場合は、対象の DHCPv6 プレフィックスプールに設定した IPv6 アドレスプレフィックス（address prefix）から IPv6 アドレスが割り当てられます。 IAID は 16 進文字列で、設定される 16 進文字列の長さは偶数です（例：001100 は可、11223 は不可）。
制限・注意	• 対象の DHCPv6 プレフィックスプールに設定されている address prefix 設定を削除すると、address-assignment 設定も削除されます。 • DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。 • コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の

address-assignment	
	順序はコマンド構文に記載の順序で指定してください。
バージョン	1.08.02

使用例：DHCPv6 プレフィックスプール「v6-pool-1」において、DHCPv6 手動バインディングエントリー「割り当てる IPv6 アドレス=2001:db8:10:10::aaaa、DUID=000300010506bbccddee」を設定する方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool v6-pool-1
(config-dhcp)# address prefix 2001:db8:10:10::/64
(config-dhcp)# address-assignment 2001:db8:10:10::aaaa 000300010506bbccddee
(config-dhcp)#
```

4.4.4 domain-name（DHCPv6 Server）

domain-name（DHCPv6 Server）	
目的	DHCPv6 クライアントに割り当てるドメイン名を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	domain-name NAME no domain-name
Parameter	NAME：ドメイン名を最大 253 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	DHCPv6 プール設定モード
特権レベル	レベル：12
ガイドライン	設定済みの状態で本コマンドを新たに設定すると、上書き設定されます。
制限・注意	• ドメイン名は 1 つだけ設定できます。 • DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCPv6 プレフィックスプール「pool1」において、DHCPv6 クライアントに割り当てるドメイン名「v6domain」を設定する方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool1
(config-dhcp)# domain-name v6domain
(config-dhcp)#
```

4.4.5 dns-server（DHCPv6 Server）

dns-server（DHCPv6 Server）	
目的	DHCPv6 クライアントに割り当てる DNS サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	dns-server IPV6-ADDRESS no dns-server IPV6-ADDRESS
Parameter	IPV6-ADDRESS：DNS サーバーの IPv6 アドレスを指定します。

dns-server（DHCPv6 Server）	
デフォルト	なし
モード	DHCPv6 プール設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• DNS サーバーは最大 2 個設定できます。 • DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCPv6 プレフィックスプール「pool1」において、DHCPv6 クライアントに割り当てる DNS サーバー「2001:db8:3000:3000::42」を設定する方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool1
(config-dhcp)# dns-server 2001:db8:3000:3000::42
(config-dhcp)#
```

4.4.6 prefix-delegation pool

prefix-delegation pool	
目的	プレフィックス委譲のための DHCPv6 プレフィックスプールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	prefix-delegation pool LOCAL-POOL [lifetime VALID-LT PREFERRED-LT] no prefix-delegation pool LOCAL-POOL
Parameter	LOCAL-POOL：ローカル IPv6 プレフィックスプール名を指定します。 lifetime VALID-LT PREFERRED-LT（省略可能）：VALID-LT（有効期間）と PREFERRED-LT（推奨期間）を、60～4,294,967,295 秒の範囲で指定します。有効期間は推奨期間より長くなるように指定してください。
デフォルト	VALID-LT（有効期間）未指定時：2,592,000 秒（30 日） PREFERRED-LT（推奨期間）未指定時：604,800 秒（7 日）
モード	DHCPv6 プール設定モード
特権レベル	レベル：12
ガイドライン	DHCPv6 クライアントから要求を受信すると、受信したインターフェースに関連付けられた DHCPv6 プレフィックスプールをチェックします。 対象の DHCPv6 プレフィックスプールに、要求元クライアントに一致する手動プレフィックス委譲エントリー（prefix-delegation）が設定されている場合は、そのプレフィックスが委譲されます。一致する手動プレフィックス委譲エントリーが存在しない場合は、指定したローカル IPv6 プレフィックスプールからプレフィックスが委譲されます。 設定済みの状態で本コマンドを新たに設定すると、上書き設定されます。
制限・注意	• 1 つの DHCPv6 プレフィックスプールにおいて、設定できるローカル IPv6 プレフィックスプールは 1 つだけです。 • 本設定を削除すると、対象の DHCPv6 プレフィックスプールに設定されている

prefix-delegation pool	
	prefix-delegation 設定も削除されます。 • DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：DHCPv6 プレフィックスプール「prefix-1」において、ローカル IPv6 プレフィックスプール「v6-local-1」を指定して、DHCPv6-PD によるプレフィックス委譲を設定する方法を示します。

```
# configure terminal
(config)# ipv6 local pool v6-local-1 2001:db8:ffff::/48 64
(config)# ipv6 dhcp pool prefix-1
(config-dhcp)# prefix-delegation pool v6-local-1
(config-dhcp)#
```

4.4.7 prefix-delegation

prefix-delegation	
目的	手動プレフィックス委譲エントリーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	prefix-delegation IPV6-PREFIX/LEN DUID [iaid IAID] [lifetime VALID-LT PREFERRED-LT] no prefix-delegation IPV6-PREFIX/LEN DUID [iaid IAID]
Parameter	IPV6-PREFIX/LEN：手動プレフィックス委譲エントリーで委譲する IPv6 アドレスプレフィックスとプレフィックス長を指定します。 DUID：DHCPv6 クライアントの DUID（DHCP Unique Identifier）を指定します。 iaid IAID（省略可能）：DHCPv6 クライアントの IAID（Identity Association Identifier）を指定します。 lifetime VALID-LT PREFERRED-LT（省略可能）：VALID-LT（有効期間）と PREFERRED-LT（推奨期間）を、60～4,294,967,295 秒の範囲で指定します。有効期間は推奨期間より長くなるように指定してください。
デフォルト	VALID-LT（有効期間）未指定時：2,592,000 秒（30 日） PREFERRED-LT（推奨期間）未指定時：604,800 秒（7 日）
モード	DHCPv6 プール設定モード
特権レベル	レベル：12
ガイドライン	DHCPv6 クライアントから要求を受信すると、受信したインターフェースに関連付けられた DHCPv6 プレフィックスプールをチェックします。 DUID と IAID を指定した手動プレフィックス委譲エントリーの場合、DHCPv6 クライアントからのリクエストメッセージに IANA オプションが含まれていて、DUID と IAID の両方が一致した DHCPv6 クライアントに、指定したプレフィックスが委譲されます。 DUID のみを指定した手動プレフィックス委譲エントリーの場合、DUID が一致した DHCPv6 クライアントに、指定したプレフィックスが委譲されます。 一致する手動プレフィックス委譲エントリーが存在しない場合は、対象の DHCPv6

prefix-delegation	
	プレフィックスプールに設定したローカル IPv6 プレフィックスプールからプレフィックスが委譲されます。 IAID は 16 進文字列で、設定される 16 進文字列の長さは偶数です（例：001100 は可、11223 は不可）。
制限・注意	• 対象の DHCPv6 プレフィックスプールに設定されている prefix-delegation pool 設定を削除すると、prefix-delegation 設定も削除されます。 • DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。 • コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。
バージョン	1.08.02

使用例：DHCPv6 プレフィックスプール「prefix-1」において、手動プレフィックス委譲エントリー「割り当てるプレフィックス=2001:db8:ffff:100::/64、DUID=000300010506bbccddee」を設定する方法を示します。

```
# configure terminal
(config)# ipv6 local pool v6-local-1 2001:db8:ffff::/48 64
(config)# ipv6 dhcp pool prefix-1
(config-dhcp)# prefix-delegation pool v6-local-1
(config-dhcp)# prefix-delegation 2001:db8:ffff:100::/64 000300010506bbccddee
(config-dhcp)#
```

4.4.8 ipv6 dhcp excluded-address

ipv6 dhcp excluded-address	
目的	割り当てから除外する IPv6 アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 dhcp excluded-address START-IPV6 [END-IPV6] no ipv6 dhcp excluded-address START-IPV6 [END-IPV6]
Parameter	START-IPV6：除外する IPv6 アドレス、または除外する IPv6 アドレス範囲の最初の IPv6 アドレスを指定します。 END-IPV6（省略可能）：除外する IPv6 アドレス範囲の最後の IPv6 アドレスを指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドは、IPv6 アドレスを割り当てるための DHCPv6 プレフィックスプールにのみ適用されます。 DHCPv6 サーバーは、装置に設定した IPv6 アドレスを除いた、指定した IPv6 アドレスプレフィックス（address prefix）の IPv6 アドレスを割り当て対象として扱います。本コマンドを使用すると、特定の IPv6 アドレスまたは IPv6 アドレスの範囲を、割り当て対象から除外できます。
制限・注意	• 除外対象の IPv6 アドレスは、1 つの DHCPv6 プレフィックスプールにつき最大 4 個設定でき、装置全体で最大 64 個設定できます。

ipv6 dhcp excluded-address	
	• DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：IPv6 アドレス「2001:db8:10::1000～2001:db8:10::1fff」を除外対象として設定する方法を示します。

```
# configure terminal
(config)# ipv6 dhcp excluded-address 2001:db8:10::1000 2001:db8:10::1fff
(config)#
```

4.4.9 ipv6 local pool

ipv6 local pool	
目的	ローカル IPv6 プレフィックスプールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 local pool NAME IPV6-PREFIX/LEN ASSIGNED-LENGTH no ipv6 local pool NAME
Parameter	NAME：ローカル IPv6 プレフィックスプール名を最大 12 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 IPV6-PREFIX/LEN：ローカル IPv6 プレフィックスプールの IPv6 アドレスプレフィックスとプレフィックス長を指定します。 ASSIGNED-LENGTH：委譲プレフィックス長を指定します。元のプレフィックス長より長いプレフィックス長を指定する必要があります。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ローカル IPv6 プレフィックスプールは、プレフィックスのブロックを定義します。他のプールとのオーバーレイプレフィックスを使用してプールを定義します。ローカルプールのプレフィックスを変更する場合は、ローカルプールを削除した後、プールを再作成します。すでに割り当てられているプレフィックスは、すべて解放されます。
制限・注意	• ローカル IPv6 プレフィックスプールは最大 16 個設定できます。 • DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：ローカル IPv6 プレフィックスプール「v6-local-1」を、「IPv6 アドレスプレフィックス 2001:db8:ffff::/48、委譲プレフィックス長=64」で設定する方法を示します。

```
# configure terminal
(config)# ipv6 local pool v6-local-1 2001:db8:ffff::/48 64
(config)#
```

4.4.10 ipv6 dhcp server

ipv6 dhcp server	
目的	DHCPv6 サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 dhcp server NAME [rapid-commit] [preference VALUE] [allow-hint] no ipv6 dhcp server
Parameter	NAME：関連付ける DHCPv6 プレフィックスプール名を指定します。 rapid-commit（省略可能）：DHCPv6 の Rapid Commit オプションを有効にする場合に指定します。デフォルトは無効です。 preference VALUE（省略可能）：サーバーによってアドバタイズされるプリファレンス（優先度）を、0～255 の範囲で指定します。デフォルトは 0 です。値が大きいほど優先度が高くなります。 allow-hint（省略可能）：クライアントによるプレフィックスヒントに基づいて、プレフィックスを委譲する場合に指定します。デフォルトでは、クライアントによるプレフィックスヒントは無視されます。
デフォルト	なし
モード	インターフェース設定モード(vlan)
特権レベル	レベル：12
ガイドライン	1 つのインターフェースには、設定済みの DHCPv6 プレフィックスプールを 1 つだけ関連付けらます。 DHCPv6 の Rapid Commit オプションを使用する場合は、DHCPv6 サーバーとクライアントの両方で有効にする必要があります。 preference パラメーターに 0 以外の値を指定した場合は、優先度はアドバタイズメッセージにオプションとして設定されます。優先度オプションが設定されていないアドバタイズメッセージは、優先度が 0 として扱われます。値が大きいほど優先度が高くなります。 allow-hint パラメーターを指定した場合は、DHCP サーバーはクライアントによるプレフィックスヒントに基づいて、プレフィックスを委譲します。指定しない場合は、クライアントによるプレフィックスヒントは無視されます。
制限・注意	• 1 つのインターフェースでは、DHCPv6 クライアント機能、DHCPv6 サーバー機能のいずれか 1 つのみ有効にできます。 • DHCPv6 サーバーが有効状態では、設定内容が反映されません。 • 本設定を反映するには、no service ipv6 dhcp コマンドにて DHCPv6 サーバー機能をいったん無効にした後、再度 DHCPv6 サーバー機能を有効にしてください。
バージョン	1.08.02

使用例：VLAN 100 インターフェースにおいて、設定済みの DHCPv6 プレフィックスプール「pool1」を指定して、DHCPv6 サーバーを設定する方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool1
(config-dhcp)# exit
(config)# interface vlan 100
(config-if-vlan)# ipv6 dhcp server pool1
(config-if-vlan)#
```

4.4.11 service ipv6 dhcp

service ipv6 dhcp	
目的	DHCPv6 サーバー機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	service ipv6 dhcp no service ipv6 dhcp
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCPv6 サーバー機能を有効にする方法を示します。

```
# configure terminal
(config)# service ipv6 dhcp
(config)#
```

4.4.12 show ipv6 dhcp binding

show ipv6 dhcp binding	
目的	DHCPv6 サーバーでアドレスバインディングエントリーを表示します。
Command	show ipv6 dhcp binding [IPV6-ADDRESS]
Parameter	IPV6-ADDRESS（省略可能）：表示するアドレスバインディングエントリーの IPv6 アドレス、またはプレフィックスを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	IPv6 アドレス、またはプレフィックスを指定しない場合、すべてのアドレスバインディングエントリーが表示されます。
制限・注意	-
バージョン	1.08.02

使用例：すべてのバインディングエントリーを表示する方法を示します。

```
# show ipv6 dhcp binding

Client DUID : 00030006004066ac2c90 ...(1)
                address: 2001:db8:200::100 ...(2)
                         (3)                          (4)
                         preferred lifetime 604800 ,valid lifetime 2592000

Client DUID : 00030006004066ac31e9
                prefix: 2001:db8:aaaa::/64 ...(5)
                         preferred lifetime 604800 ,valid lifetime 2592000

Total Entries: 2
```

項番	説明
(1)	DHCPv6 クライアントの DUID (DHCP Unique Identifier) を表示します。
(2)	リースした IPv6 アドレスを表示します。
(3)	IPv6 アドレス、またはプレフィックスの推奨期間を表示します。
(4)	IPv6 アドレス、またはプレフィックスの有効期間を表示します。
(5)	委譲したプレフィックスを表示します。

4.4.13 show ipv6 dhcp pool

show ipv6 dhcp pool	
目的	DHCPv6 プレフィックスプールに関する設定を表示します。
Command	show ipv6 dhcp pool [NAME]
Parameter	NAME (省略可能)：表示する DHCPv6 プレフィックスプールを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	DHCPv6 プレフィックスプールを指定しない場合は、すべての DHCPv6 プレフィックスプールの設定が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：IPv6 アドレスを割り当てるための DHCPv6 プレフィックスプールの場合の表示例を示します。

```
# show ipv6 dhcp pool

DHCPv6 pool: address-pool ...(1)
        Static bindings:
           Binding for client 00030006004066aaaaaa ...(2)
           IA NA: IA ID not specified ...(3)
              Address: 2001:db8:200::aaaa ...(4)
                (5)                          (6)
                preferred lifetime 604800, valid lifetime 2592000
           Binding for client 00030006004066bbbbbb
           IA NA: IA ID not specified
              Address: 2001:db8:200::bbbb
               preferred lifetime 604800, valid lifetime 2592000
        Address prefix: 2001:db8:200::/64 ...(7)
              (8)                         (9)
              preferred lifetime 604800, valid lifetime 2592000
        DNS server: 1:db8:3000:3000::42 ...(10)
        Domain name: v6domain ...(11)
        Active clients: 0 ...(12)
```

項番	説明
(1)	DHCPv6 プレフィックスプール名を表示します。
(2)	DHCPv6 手動バインディングエントリーの DUID（DHCP Unique Identifier）を表示します。
(3)	DHCPv6 手動バインディングエントリーの IAID（Identity Association Identifier）を表示します。

項番	説明
(4)	DHCPv6 手動バインディングエントリーに割り当てる IPv6 アドレスを表示します。
(5)	DHCPv6 手動バインディングエントリーの推奨期間を表示します。
(6)	DHCPv6 手動バインディングエントリーの有効期間を表示します。
(7)	DHCPv6 クライアントに IPv6 アドレスを割り当てるプレフィックスを表示します。
(8)	IPv6 アドレスの推奨期間を表示します。
(9)	IPv6 アドレスの有効期間を表示します。
(10)	DNS サーバーの IPv6 アドレスを表示します。
(11)	ドメイン名を表示します。
(12)	アクティブな DHCPv6 クライアントの個数を表示します。

使用例：プレフィックス委譲のための DHCPv6 プレフィックスプールの場合の表示例を示します。

```
# show ipv6 dhcp pool

DHCPv6 pool: pd-pool ...(1)
        Static bindings:
           Binding for client 00030006004066aabbcc ...(2)
           IA PD: IA ID not specified ...(3)
              Prefix: 2001:db8:aaaa:ff11::/64 ...(4)
                (5)                              (6)
               preferred lifetime 604800, valid lifetime 2592000
           Binding for client 00030006004066ddeeff
           IA PD: IA ID 0x1001
              Prefix: 2001:db8:aaaa:ff22::/64
               preferred lifetime 604800, valid lifetime 2592000
        Prefix delegation pool: pd01 ...(7)
              (8)                              (9)
             preferred lifetime 604800, valid lifetime 2592000
        DNS server:
        Domain name:
        Active clients: 0
```

項番	説明
(1)	DHCPv6 プレフィックスプール名を表示します。
(2)	手動プレフィックス委譲エントリーの DUID（DHCP Unique Identifier）を表示します。
(3)	手動プレフィックス委譲エントリーの IAID（Identity Association Identifier）を表示します。
(4)	手動プレフィックス委譲エントリーに割り当てるプレフィクスを表示します。
(5)	手動プレフィックス委譲エントリーの推奨期間を表示します。
(6)	手動プレフィックス委譲エントリーの有効期間を表示します。
(7)	プレフィクス委譲で使用するローカル IPv6 プレフィックスプールを表示します。
(8)	委譲するプレフィクスの推奨期間を表示します。
(9)	委譲するプレフィクスの有効期間を表示します。

4.4.14 show ipv6 excluded-address

show ipv6 excluded-address	
目的	リースする範囲から除外する IPv6 アドレスを表示します。

show ipv6 excluded-address	
Command	show ipv6 excluded-address
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：リースする範囲から除外する IPv6 アドレスを表示する方法を示します。

```
# show ipv6 excluded-address

 IPv6 excluded address: ...(1)
        1.      2001:db8:200::1 - 2001:db8:200::ff
        2.      2001:db8:200::abcd:1 - 2001:db8:200::abcd:ffff

 Total Entries: 2
```

項番	説明
(1)	リースする範囲から除外する IPv6 アドレスを表示します。

4.4.15 show ipv6 local pool

show ipv6 local pool	
目的	ローカル IPv6 プレフィックスプールの情報を表示します。
Command	show ipv6 local pool [NAME]
Parameter	NAME (省略可能)：表示するローカル IPv6 プレフィックスプールを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ローカル IPv6 プレフィックスプールの情報を表示する方法を示します。

```
# show ipv6 local pool
(1)          (2)                                          (3)    (4)
Pool         Prefix                                       Free   In use
------------ -------------------------------------------- ------ ------
pd01         2001:db8:aaaa::/48                           65535  1
pd02         2001:db8:1234:5678::/64                      256    0
------------ -------------------------------------------- ------ ------
Total Entries: 2
```

項番	説明
(1)	ローカル IPv6 プレフィックスプール名を表示します。
(2)	委譲元のプレフィックスを表示します。

項番	説明
(3)	指定したプレフィックス長で分割した、委譲可能なプレフィックスの残り数を表示します。
(4)	委譲したプレフィックス数を表示します。

4.4.16 show ipv6 dhcp operation

show ipv6 dhcp operation	
目的	DHCPv6 サーバーの設定を表示します。
Command	show ipv6 dhcp operation
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCPv6 サーバーの設定を表示する方法を示します。

```
# show ipv6 dhcp operation

DHCPv6 pool: address-pool ...(1)
        Address prefix: 2001:db8:200::/64 ...(2)
        Static bindings:
           Binding for client 00030006004066aaaaaa ...(3)
            IA NA: IA ID not specified ...(4)
              Address: 2001:db8:200::aaaa ...(5)
               (6)                          (7)
               preferred lifetime 604800, valid lifetime 2592000
           Binding for client 00030006004066bbbbbb
            IA NA: IA ID not specified
              Address: 2001:db8:200::bbbb
               preferred lifetime 604800, valid lifetime 2592000
        IPv6 excluded address: 2001:db8:200::1 - 2001:db8:200::ff ...(8)
                               2001:db8:200::abcd:1 - 2001:db8:200::abcd:ffff
        (9)                         (10)
        preferred lifetime 604800, valid lifetime 2592000
        DNS server: 1:db8:3000:3000::42 ...(11)
        Domain name: v6domain ...(12)

DHCPv6 pool: pd-pool
        Prefix delegation pool: pd01, prefix is 2001:db8:aaaa::/48 64 ...(13)
        Static bindings:
           Binding for client 00030006004066aabbcc ...(14)
             IA PD: IA ID not specified ...(15)
             Prefix: 2001:db8:aaaa:ff11::/64 ...(16)
             (17)                          (18)
             preferred lifetime 604800, valid lifetime 2592000
           Binding for client 00030006004066ddeeff
             IA PD: IA ID 0x1001
             Prefix: 2001:db8:aaaa:ff22::/64
             preferred lifetime 604800, valid lifetime 2592000
        (19)                         (20)
        preferred lifetime 604800, valid lifetime 2592000
        DNS server:
        Domain name:
```

項番	説明
(1)	DHCPv6 プレフィックスプール名を表示します。
(2)	DHCPv6 クライアントに IPv6 アドレスを割り当てるプレフィックスを表示します。
(3)	DHCPv6 手動バインディングエントリーの DUID（DHCP Unique Identifier）を表示します。
(4)	DHCPv6 手動バインディングエントリーの IAID（Identity Association Identifier）を表示します。
(5)	DHCPv6 手動バインディングエントリーに割り当てる IPv6 アドレスを表示します。
(6)	DHCPv6 手動バインディングエントリーの推奨期間を表示します。
(7)	DHCPv6 手動バインディングエントリーの有効期間を表示します。
(8)	リースする範囲から除外する IPv6 アドレスを表示します。
(9)	IPv6 アドレスの推奨期間を表示します。
(10)	IPv6 アドレスの有効期間を表示します。
(11)	DNS サーバーの IPv6 アドレスを表示します。
(12)	ドメイン名を表示します。
(13)	プレフィクス委譲で使用するローカル IPv6 プレフィックスプールの情報を表示します。
(14)	手動プレフィックス委譲エントリーの DUID（DHCP Unique Identifier）を表示します。
(15)	手動プレフィックス委譲エントリーの IAID（Identity Association Identifier）を表示します。
(16)	手動プレフィックス委譲エントリーに割り当てるプレフィクスを表示します。
(17)	手動プレフィックス委譲エントリーの推奨期間を表示します。
(18)	手動プレフィックス委譲エントリーの有効期間を表示します。
(19)	委譲するプレフィクスの推奨期間を表示します。
(20)	委譲するプレフィクスの有効期間を表示します。

4.4.17 clear ipv6 dhcp binding

clear ipv6 dhcp binding	
目的	DHCPv6 サーバーに登録されたバインディングエントリーを削除します。
Command	clear ipv6 dhcp binding {all | IPV6-ADDRESS}
Parameter	all：すべてのバインディングエントリーを削除する場合に指定します。 IPV6-ADDRESS：削除するバインディングエントリーの IPv6 アドレス、またはプレフィックスを指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCPv6 サーバーに登録されたすべてのバインディングエントリーを削除する方法を示します。

```
# clear ipv6 dhcp binding all
#
```

4.5 DHCP Auto Configuration コマンド

DHCP Auto Configuration 関連の設定コマンドは以下のとおりです。

- autoconfig enable

DHCP Auto Configuration 関連の show コマンドは以下のとおりです。

- show autoconfig

4.5.1 autoconfig enable

autoconfig enable	
目的	DHCP Auto Configuration を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	autoconfig enable no autoconfig enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	DHCP Auto Configuration を有効にして保存し装置を再起動すると、装置の VLAN 1 インターフェースは自動的に DHCP クライアントになります。DHCP Auto Configuration プロセスは以下のとおりです。 • DHCP Auto Configuration プロセスが開始されると、装置は DHCP サーバーから IP アドレスを取得する際に、TFTP サーバーの IP アドレスと構成情報ファイル名も取得します。 • 構成情報ファイル名は、DHCP メッセージに DHCP オプション 67（Bootfile name）が付与されている場合はその値が適用されます。DHCP オプション 67 が付与されていない場合は"file フィールド"の値が適用されます。"file フィールド"にも値が入っていない場合は、DHCP Auto Configuration プロセスは中断されます。 • TFTP サーバーの IP アドレスは、「DHCP オプション 150（TFTP Server Address）の IP アドレス（複数可、最大 3 個）」「"siaddr フィールド"の IP アドレス」の順番で、構成情報ファイルのダウンロードが成功するまで順次適用されます。すべての TFTP サーバーで失敗した場合は、DHCP Auto Configuration プロセスは中断されます。 構成情報ファイルを正常に取得できないで DHCP Auto Configuration プロセスが中断された場合には、startup-config として指定されていた構成情報が適用されます。 本コマンドは、設定を保存し、装置を再起動した後に有効となります。
制限・注意	-
バージョン	1.08.02

使用例：DHCP Auto Configuration を有効にする方法を示します。

```
# configure terminal
(config)# autoconfig enable
WARNING: Autoconfig State enabled now, but won't take effect until reboot.
(config)#
```

4.5.2 show autoconfig

show autoconfig	
目的	DHCP Auto Configuration の有効／無効を表示します。
Command	show autoconfig
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCP Auto Configuration の有効／無効を表示する方法を示します。

```
# show autoconfig

Autoconfig State: Disabled ...(1)
```

項番	説明
(1)	DHCP Auto Configuration の有効(Enabled)／無効(Disabled)を表示します。

4.6 時刻および SNTP コマンド

時刻および SNTP (Simple Network Time Protocol) 関連の設定コマンドは以下のとおりです。

- clock set
- clock summer-time
- clock timezone
- sntp server
- sntp interval
- sntp enable

時刻および SNTP (Simple Network Time Protocol) 関連の show コマンドは以下のとおりです。

- show clock
- show sntp

4.6.1 clock set

clock set	
目的	システムの時刻を手動で設定します。
Command	clock set HH:MM:SS DAY MONTH YEAR
Parameter	HH:MM:SS：時刻を 時:分:秒 形式で指定します。時は 24 時間表記で指定します。 DAY：日を指定します。 MONTH：月を jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec で指定します。 YEAR：西暦年を指定します。
デフォルト	なし
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドはシステムの時刻を手動で設定します。SNTP を使用している場合でも本コマンドで時刻を変更できます。 NTP を使用している場合は本コマンドを実行しても時刻を変更できません。no service ntp コマンドで NTP サービスを無効にした状態で本コマンドを実施してください。 本コマンドで時刻を設定する際は、本装置は clock timezone コマンドで設定したタイムゾーンにあると想定して設定されます。なお、タイムゾーンはデフォルトで日本標準時 (UTC +09:00) に設定されています。 本コマンドで手動で設定した時刻は、利用可能な場合はハードウェアクロック(RTC)にも適用されます。
制限・注意	• 本コマンドで時刻を設定してから NTP サービスを有効にする場合、NTP サービス有効後の時刻が直近に変更した時刻にならないことがあります。その場合は、本コマンドを数回実施してから NTP サービスを有効にしてください。
バージョン	1.08.02

使用例：システムの時刻を手動で 2016 年 3 月 1 日 18:00 に設定する方法を示します。

```
# clock set 18:00:00 1 Mar 2016
```

```
#
```

4.6.2 clock summer-time

clock summer-time	
目的	システムが自動的にサマータイムに切り替わることを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	**clock summer-time recurring** WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM [OFFSET] **clock summer-time date** DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM [OFFSET] **no clock summer-time**
Parameter	recurring：指定した月・週・曜日・時間にサマータイムを開始／終了する場合に指定します。「開始日」「終了日」の順番で指定します。 • WEEK：週を 1～4, last で指定します。 • DAY：曜日を sun, mon, tue, wed, thu, fri, sat で指定します。 • MONTH：月を jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec で指定します。 • HH:MM：時刻を 時:分 形式で指定します。時は 24 時間表記で指定します。 date：指定した日時にサマータイムを開始／終了する場合に指定します。「開始日」「終了日」の順番で指定します。 • DATE：日を指定します。 • MONTH：月を jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec で指定します。 • YEAR：西暦年を指定します。 • HH:MM：時刻を 時:分 形式で指定します。時は 24 時間表記で指定します。 OFFSET（省略可能）：サマータイムに追加する時間を指定します。30, 60, 90, 120 分のいずれかを指定します。指定しない場合は 60 分です。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：サマータイムの開始日を「4 月、第 1 週の日曜日、2:00」に、終了日を「10 月、最終週の日曜日、2:00」に指定する方法を示します。

```
# configure terminal
(config)# clock summer-time recurring 1 sun apr 2:00 last sun oct 2:00
(config)#
```

4.6.3 clock timezone

clock timezone	
目的	タイムゾーン（UTC（協定世界時）からのオフセット）を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。

clock timezone	
Command	clock timezone {+ | -} HOURS-OFFSET [MINUTES-OFFSET] no clock timezone
Parameter	+ : UTC からのオフセットが正値の場合に指定します。 - : UTC からのオフセットが負値の場合に指定します。 HOURS-OFFSET : UTC からのオフセットを 0～13 時間の範囲で指定します。 MINUTES-OFFSET（省略可能）: UTC からのオフセットを 0～59 分の範囲で指定します。
デフォルト	UTC + 9 時間 (clock timezone + 9 0)
モード	グローバル設定モード
特権レベル	レベル : 12
ガイドライン	時刻は、UTC 時間、タイムゾーン、サマータイム設定に基づいて算出されます。
制限・注意	-
バージョン	1.08.02

使用例：タイムゾーンを「UTC - 8 時間」に設定する方法を示します。

```
# configure terminal
(config)# clock timezone - 8
(config)#
```

4.6.4 sntp server

sntp server	
目的	SNTP で時刻を問い合わせる NTP/SNTP サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	sntp server {IP-ADDRESS | IPV6-ADDRESS} no sntp server {IP-ADDRESS | IPV6-ADDRESS}
Parameter	IP-ADDRESS : NTP/SNTP サーバーの IPv4 アドレスを指定します。 IPV6-ADDRESS : NTP/SNTP サーバーの IPv6 アドレスを指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル : 12
ガイドライン	SNTP クライアント機能のみ対応しています。 複数の NTP/SNTP サーバーを設定した場合は、設定順（show sntp での表示順）で時刻の問い合わせが行われます。なお、IPv4 アドレスで登録した NTP/SNTP サーバーの方が、IPv6 アドレスで登録した NTP/SNTP サーバーよりも優先されます。 1 台目の NTP/SNTP サーバーから時刻を取得できた場合は、2 台目以降の NTP/SNTP サーバーに問い合わせは行われません。 1 台目の NTP/SNTP サーバーからの応答がない場合は、2 台目の NTP/SNTP サーバーに問い合わせを行います。それ以降も同様の動作です。
制限・注意	• SNTP で時刻を問い合わせる NTP/SNTP サーバーは、IPv4 アドレスで最大 2 個、IPv6 アドレスで最大 2 個まで設定できます。

sntp server	

	• デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在する NTP/SNTP サーバーを指定して設定した場合、宛先判定にはデフォルトルートよりもデフォルトゲートウェイ設定が優先され、宛先(1)(2)のいずれの場合も SNTP パケットはマネージメントポートから送信されます。
	  • 宛先(1):デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク
	  • 宛先(2):デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク
	• そのため、このような状況では宛先(1)に存在する NTP/SNTP サーバーは使用できません。ApresiaNP2500 シリーズでは、このような状況にならないように、VLAN インターフェース経由、もしくはマネージメントポート経由のどちらかのみで管理することを推奨します。

バージョン	1.08.02

使用例:SNTP で時刻を問い合わせる NTP/SNTP サーバーとして 192.0.2.100 を設定する方法を示します。

```
# configure terminal
(config)# sntp server 192.0.2.100
(config)#
```

4.6.5 sntp interval

sntp interval	
目的	SNTP での時刻の問い合わせ間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	sntp interval SECONDS no sntp interval
Parameter	SECONDS:時刻の問い合わせ間隔を 30~99,999 秒の範囲で指定します。
デフォルト	720 秒
モード	グローバル設定モード
特権レベル	レベル:12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例:SNTP での時刻の問い合わせ間隔を 100 秒に設定する方法を示します。

```
# configure terminal
(config)# sntp interval 100
(config)#
```

4.6.6 sntp enable

sntp enable	
目的	SNTP クライアント機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。

sntp enable	
Command	sntp enable no sntp enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	SNTP クライアント機能を有効にした場合は、NTP サービスは有効にできません。逆も同様です。
制限・注意	-
バージョン	1.08.02

使用例：SNTP クライアント機能を有効にする方法を示します。

```
# configure terminal
(config)# sntp enable
(config)#
```

4.6.7 show clock

show clock	
目的	日時情報を表示します。
Command	show clock
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：現在の時刻を表示する方法を示します。

```
# show clock

     Current Time Source    : System Clock ...(1)
     Current Time           : 12:27:51, 2016-03-01 ...(2)
     Time Zone              : UTC +09:00 ...(3)
     Daylight Saving Time   : Disabled ...(4)
```

項番	説明
(1)	時刻情報の情報源を表示します。 System Clock：システムクロック SNTP：SNTP 有効、時刻が同期されている場合 NTP(Synchronized)：NTP サービス有効、時刻が同期されている場合 NTP(Unsynchronized)：NTP サービス有効、時刻が同期されていない場合
(2)	現在の時刻および年月日を表示します。
(3)	タイムゾーンを表示します。

項番	説明
(4)	サマータイムの有効／無効を表示します。有効な場合は、サマータイムの「オフセット」「開始日」「終了日」も表示されます。 Disabled：無効 Recurring：サマータイムを recurring パラメーターを指定して有効にした場合 Date：サマータイムを date パラメーターを指定して有効にした場合

4.6.8 show sntp

show sntp	
目的	SNTP の情報を表示します。
Command	show sntp
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SNTP の情報を表示する方法を示します。

```
# show sntp

SNTP Status               : Enabled ...(1)
SNTP Poll Interval        : 720 seconds ...(2)

SNTP Server Status:
(3)                                              (4)      (5)      (6)
SNTP Server                                      Stratum Version Last Receive
------------------------------------------------ ------- ------- ---------------
192.0.2.100                                      ------- ------- ---------------
172.16.10.200                                    5       3       00:10:28 Synced
2001:db8:10::100                                 ------- ------- ---------------
fe80::240:66ff:aaaa:bbbb%vlan10                  ------- ------- ---------------
------------------------------------------------ ------- ------- ---------------
Total Entries: 4
```

項番	説明
(1)	SNTP クライアント機能の有効(Enabled)／無効(Disabled)を表示します。
(2)	SNTP での時刻の問い合わせ間隔を表示します。
(3)	設定した NTP/SNTP サーバーの IP アドレスを表示します。リストの先頭に登録された NTP/SNTP サーバーから問い合わせが行われます。
(4)	NTP/SNTP サーバーの Stratum を表示します。
(5)	NTP/SNTP のバージョンを表示します。
(6)	最後に時刻を同期してから経過した時間を表示します。現在の同期対象の NTP/SNTP サーバーには Synced が表示されます。

4.7 NTP コマンド

NTP（Network Time Protocol）関連の設定コマンドは以下のとおりです。

- ntp server
- ntp peer
- ntp update-calendar
- ntp authenticate
- ntp authentication-key
- ntp trusted-key
- ntp control-key
- ntp request-key
- ntp disable
- ntp access-group
- ntp max-associations
- ntp master
- service ntp

NTP（Network Time Protocol）関連の show コマンドは以下のとおりです。

- show ntp associations
- show ntp status

4.7.1 ntp server

ntp server	
目的	クライアントモードで時刻を問い合わせる NTP サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ntp server {IP-ADDRESS | IPV6-ADDRESS} [version VALUE] [key KEY-ID] [prefer] [min-poll INTERVAL] [max-poll INTERVAL] no ntp server {IP-ADDRESS | IPV6-ADDRESS}
Parameter	IP-ADDRESS：NTP サーバーの IPv4 アドレスを指定します。 IPV6-ADDRESS：NTP サーバーの IPv6 アドレスを指定します。 version VALUE（省略可能）：NTP バージョン番号を 1～4 の範囲で指定します。指定しない場合はバージョン番号は 4 です。 key KEY-ID（省略可能）：認証キーの ID を 1～255 の範囲で指定します。 prefer（省略可能）：優先する NTP サーバーの場合に指定します。 min-poll INTERVAL（省略可能）：NTP パケットの最小ポーリング間隔を 3～16 の範囲で指定します。指定した値を n とすると、2 の n 乗が最小ポーリング間隔(秒)になります。指定しない場合は n=6（64 秒）です。 max-poll INTERVAL（省略可能）：NTP パケットの最大ポーリング間隔を 4～17 の範囲で指定します。指定した値を n とすると、2 の n 乗が最大ポーリング間隔(秒)になります。指定しない場合は n=10（1024 秒）です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12

ntp server	
ガイドライン	複数の NTP サーバーを設定する場合は、prefer パラメーターで優先する NTP サーバーを指定できます。

制限・注意	• デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在する NTP サーバーを指定して設定した場合、宛先判定にはデフォルトゲートウェイ設定よりもデフォルトルートが優先され、宛先(1)(2)のいずれの場合も NTP パケットは VLAN インターフェースから送信されます。
	  • 宛先(1):デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク
	  • 宛先(2):デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク
	• そのため、このような状況では宛先(2)に存在する NTP サーバーは使用できません。ApresiaNP2500 シリーズでは、このような状況にならないように、VLAN インターフェース経由、もしくはマネージメントポート経由のどちらかのみで管理することを推奨します。
	• コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。

バージョン	1.08.02

使用例:クライアントモードで時刻を問い合わせる NTP サーバーとして 192.0.2.100 を設定する方法を示します。

```
# configure terminal
(config)# ntp server 192.0.2.100
(config)#
```

4.7.2 ntp peer

ntp peer	
目的	Symmetric Active モードで関係付ける NTP サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ntp peer {IP-ADDRESS | IPV6-ADDRESS} [version VALUE] [key KEY-ID] [prefer] [min-poll INTERVAL] [max-poll INTERVAL] no ntp peer {IP-ADDRESS | IPV6-ADDRESS}
Parameter	IP-ADDRESS:NTP サーバーの IPv4 アドレスを指定します。 IPV6-ADDRESS:NTP サーバーの IPv6 アドレスを指定します。 version VALUE(省略可能):NTP バージョン番号を 1〜4 の範囲で指定します。指定しない場合はバージョン番号は 4 です。 key KEY-ID (省略可能):認証キーの ID を 1〜255 の範囲で指定します。 prefer (省略可能):優先する NTP サーバーの場合に指定します。 min-poll INTERVAL(省略可能):NTP パケットの最小ポーリング間隔を 3〜16 の範囲で指定します。指定した値を n とすると、2 の n 乗が最小ポーリング間隔(秒)になります。指定しない場合は n=6 (64 秒)です。 max-poll INTERVAL(省略可能):NTP パケットの最大ポーリング間隔を 4〜17 の範囲で指定します。指定した値を n とすると、2 の n 乗が最大ポーリング間隔(秒)に

ntp peer	
	なります。指定しない場合は n=10（1024 秒）です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-

制限・注意	• デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在する NTP サーバーを指定して設定した場合、宛先判定にはデフォルトゲートウェイ設定よりもデフォルトルートが優先され、宛先(1)(2)のいずれの場合も NTP パケットは VLAN インターフェースから送信されます。
	  • 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク
	  • 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク
	• そのため、このような状況では宛先(2)に存在する NTP サーバーは使用できません。ApresiaNP2500 シリーズでは、このような状況にならないように、VLAN インターフェース経由、もしくはマネージメントポート経由のどちらかのみで管理することを推奨します。
	• コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。

バージョン	1.08.02

使用例：Symmetric Active モードで関係付ける NTP サーバーとして 192.0.2.100 を設定する方法を示します。

```
# configure terminal
(config)# ntp peer 192.0.2.100
(config)#
```

4.7.3 ntp update-calendar

ntp update-calendar	
目的	NTP で取得した時刻のハードウェアクロックへの更新を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ntp update-calendar no ntp update-calendar
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本機能を有効にすると、NTP で取得した時刻を用いて、1 時間ごとにハードウェアクロックを更新します。なお、NTP で正常に時刻を取得できていない場合は、ハードウェアクロックも更新されません。
制限・注意	-
バージョン	1.08.02

使用例：NTP で取得した時刻のハードウェアクロックへの更新を有効にする方法を示します。

```
# configure terminal
(config)# ntp update-calendar
(config)#
```

4.7.4 ntp authenticate

ntp authenticate	
目的	NTP 認証を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	**ntp authenticate** **no ntp authenticate**
Parameter	なし
デフォルト	NTP 認証は有効（ntp authenticate）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	NTP 認証を有効にすると、認証キーが不一致の問い合わせに対する時刻同期を制限できます。 NTP 認証を使用する場合は、本コマンドを含めて以下を設定する必要があります。 • NTP 認証を ntp authenticate コマンドで有効にする • NTP 認証キーを ntp authentication-key コマンドで定義 • 使用する NTP 認証キーID を ntp trusted-key コマンドで指定 また、NTP 認証を使用して同期する NTP サーバーに対しては、ntp server コマンド、または ntp peer コマンドにおいて、key パラメーターで NTP 認証キーID を指定してください。
制限・注意	• NTP サーバーでは、認証なしの問い合わせを受信すると、デフォルト設定では応答します。認証なしの問い合わせに対する応答を制限するには、ntp access-group コマンドで notrust パラメーターを指定して設定してください。
バージョン	1.08.02

使用例：NTP 認証を無効にする方法を示します。

```
# configure terminal
(config)# no ntp authenticate
(config)#
```

4.7.5 ntp authentication-key

ntp authentication-key	
目的	NTP の認証キーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	**ntp authentication-key** KEY-ID **md5** VALUE **no ntp authentication-key** KEY-ID
Parameter	KEY-ID：認証キーID を 1～255 の範囲で指定します。 md5 VALUE：認証キーの文字列を最大 32 文字で指定します。
デフォルト	なし

ntp authentication-key	
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	NTP 認証を有効にすると、認証キーが不一致の問い合わせに対する時刻同期を制限できます。 NTP 認証を使用する場合は、本コマンドを含めて以下を設定する必要があります。 • NTP 認証を ntp authenticate コマンドで有効にする • NTP 認証キーを ntp authentication-key コマンドで定義 • 使用する NTP 認証キーID を ntp trusted-key コマンドで指定 また、NTP 認証を使用して同期する NTP サーバーに対しては、ntp server コマンド、または ntp peer コマンドにおいて、key パラメーターで NTP 認証キーID を指定してください。
制限・注意	-
バージョン	1.08.02

使用例：NTP の認証キーを、ID=42、文字列「aNiceKey」で設定する方法を示します。

```
# configure terminal
(config)# ntp authentication-key 42 md5 aNiceKey
(config)#
```

4.7.6 ntp trusted-key

ntp trusted-key	
目的	NTP 認証で使用する認証キーとして有効にする認証キーID を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ntp trusted-key KEY-ID no ntp trusted-key KEY-ID
Parameter	KEY-ID：NTP 認証で使用する認証キーID を 1～255 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	NTP 認証を有効にすると、認証キーが不一致の問い合わせに対する時刻同期を制限できます。 NTP 認証を使用する場合は、本コマンドを含めて以下を設定する必要があります。 • NTP 認証を ntp authenticate コマンドで有効にする • NTP 認証キーを ntp authentication-key コマンドで定義 • 使用する NTP 認証キーID を ntp trusted-key コマンドで指定 また、NTP 認証を使用して同期する NTP サーバーに対しては、ntp server コマンド、または ntp peer コマンドにおいて、key パラメーターで NTP 認証キーID を指定してください。
制限・注意	• ntp authentication-key コマンドで NTP 認証キーを設定していない認証キーID は指定できません。
バージョン	1.08.02

使用例：NTP 認証で使用する認証キーID を、ID=42 に設定する方法を示します。

```
# configure terminal
(config)# ntp trusted-key 42
(config)#
```

4.7.7 ntp control-key

ntp control-key	
目的	NTP control message（Mode=6）の認証キーID を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ntp control-key KEY-ID no ntp control-key
Parameter	KEY-ID：認証キーID を 1～255 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドは、Linux などの ntpq コマンド（モード 6 の NTP パケット）で使用する認証キーID を設定します。
制限・注意	• ntp authentication-key コマンドで NTP 認証キーを設定していない認証キーID は指定できません。
バージョン	1.08.02

使用例：NTP control message（Mode=6）で使用する認証キーID を、ID=42 に設定する方法を示します。

```
# configure terminal
(config)# ntp control-key 42
(config)#
```

4.7.8 ntp request-key

ntp request-key	
目的	モード 7 の NTP パケットの認証キーID を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ntp request-key KEY-ID no ntp request-key
Parameter	KEY-ID：認証キーID を 1～255 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドは、Linux などの ntpdc コマンド（モード 7 の NTP パケット）で使用する認証キーID を設定します。
制限・注意	• ntp authentication-key コマンドで NTP 認証キーを設定していない認証キーID は指定できません。
バージョン	1.08.02

使用例：モード 7 の NTP パケットで使用する認証キーID を、ID=42 に設定する方法を示します。

```
# configure terminal
(config)# ntp request-key 42
(config)#
```

4.7.9 ntp disable

ntp disable	
目的	対象 VLAN インターフェースの NTP サービスを無効にします。有効にする場合は、no 形式のコマンドを使用します。
Command	ntp disable no ntp disable
Parameter	なし
デフォルト	NTP サービスは有効（no ntp disable）
モード	インターフェース設定モード（vlan）
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 インターフェースの NTP サービスを無効にする方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ntp disable
(config-if-vlan)#
```

4.7.10 ntp access-group

ntp access-group	
目的	NTP サービスへのアクセス制御を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ntp access-group {default | IP-ADDRESS [MASK] | IPV6-ADDRESS | IPV6-ADDRESS/LEN} [ignore] [nomodify] [noquery] [nopeer] [noserve] [notrust] [version] no ntp access-group {default | IP-ADDRESS [MASK] | IPV6-ADDRESS | IPV6-ADDRESS/LEN}
Parameter	default：すべての IPv4 アドレス（0.0.0.0/0.0.0.0）または IPv6 アドレス（::/::）を対象にする場合に指定します。 IP-ADDRESS：特定の IPv4 アドレスを対象にする場合に指定します。 IP-ADDRESS MASK：特定の IPv4 ネットワークを対象にする場合に指定します。 IPV6-ADDRESS：特定の IPv6 アドレスを対象にする場合に指定します。 IPV6-ADDRESS/LEN：特定の IPv6 ネットワークを対象にする場合に指定します。 ignore（省略可能）：NTP 制御クエリーを含むすべての NTP パケットを拒否する場合に指定します。 nomodify（省略可能）：NTP サーバーの状態変更を行う NTP 制御クエリーを拒否す

ntp access-group	
	る場合に指定します。 noquery（省略可能）：すべての NTP 制御クエリー（モード 6、モード 7）を拒否する場合に指定します。 nopeer（省略可能）：認証なしでアソシエーションを確立しようとする可能性のあるパケットを拒否する場合に指定します。 noserve（省略可能）：NTP 制御クエリー（モード 6、モード 7）以外のすべての NTP パケットを拒否する場合に指定します。 notrust（省略可能）：認証なしの NTP パケットを拒否する場合に指定します。 version（省略可能）：動作中の NTP バージョン（バージョン 4）と異なるバージョンの NTP パケットを拒否する場合に指定します。
デフォルト	すべて許可
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	アクセス制御のエントリーは、リスト内では IP アドレスで昇順にソートされます。IP アドレスが同じ場合はマスク値で昇順にソートされます。なお、default パラメーターで指定したデフォルトエントリーは、最も低い優先度で扱われます。
制限・注意	• すでに設定済みのエントリーに対して、別のパラメーターを指定して設定した場合は、別のパラメーターが追加されます。 • すでに設定済みのエントリーに対して、特定のパラメーターだけを削除することはできません。特定のパラメーターだけを削除したい場合は、対象エントリーを一度削除してから、必要なパラメーターだけを指定して再設定してください。
バージョン	1.08.02

使用例：認証なしの NTP パケットを拒否する方法を示します。

```
# configure terminal
(config)# ntp access-group default notrust
(config)#
```

4.7.11 ntp max-associations

ntp max-associations	
目的	アソシエーション（NTP ピア、NTP クライアント）の最大数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ntp max-associations VALUE no ntp max-associations
Parameter	VALUE：アソシエーションの最大数を 1～64 の範囲で指定します。
デフォルト	32
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：アソシエーションの最大数を 20 に設定する方法を示します。

```
# configure terminal
(config)# ntp max-associations 20
(config)#
```

4.7.12 ntp master

ntp master	
目的	自装置のハードウェアクロック(RTC)を信頼できる情報源として利用することを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ntp master STRATUM no ntp master
Parameter	STRATUM：自装置の Stratum を 1～15 の範囲で指定します。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	装置を NTP サーバーとして使用するには、信頼できる情報源（上位の NTP サーバーなど）から時刻を取得し同期している必要がありますが、上位の NTP サーバーなどを利用できない場合に、本機能を有効にすることで、自装置のハードウェアクロック(RTC)を信頼できる情報源として利用することができます。
制限・注意	-
バージョン	1.08.02

使用例：自装置のハードウェアクロック(RTC)を信頼できる情報源として利用することを有効にする方法を示します。この例では、その際に自装置の Stratum が 5 になるように設定しています。

```
# configure terminal
(config)# ntp master 5
(config)#
```

4.7.13 service ntp

service ntp	
目的	NTP サービスを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	service ntp no service ntp
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	NTP サービスを有効にすると、NTP サーバーおよび NTP クライアントとしての動作が有効になります。
制限・注意	• 本装置が NTP サーバーで NTP クライアントからの問い合わせに応答する場合、応答 NTP パケットは問い合わせ元の NTP クライアントへのルート情報に従って送信されます。その際に、応答 NTP パケットの送信元 IP アドレスが送信 IP インター

service ntp	
	フェースの IP アドレスになる仕様制限があります。 • そのため、本装置を NTP サーバーとして使用する場合は、NTP クライアントごとに一番近い IP アドレスを NTP サーバーとして指定してください。それ以外の IP アドレスを指定しても時刻同期できません。
バージョン	1.08.02

使用例：NTP サービスを有効にする方法を示します。

```
# configure terminal
(config)# service ntp
(config)#
```

4.7.14 show ntp associations

show ntp associations	
目的	NTP アソシエーションの状態を表示します。
Command	show ntp associations [detail]
Parameter	detail（省略可能）：NTP アソシエーションの詳細情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• NTP 機能を IPv6 アドレスで使用している場合、show ntp associations コマンドでは IPv6 アドレスは省略されて表示されます。IPv6 アドレスを確認する場合は、detail パラメーターを指定して詳細情報を確認してください。
バージョン	1.08.02

使用例：NTP アソシエーションの状態を表示する方法を示します。

```
# show ntp associations
 (1) (2)           (3)             (4) (5)    (6)    (7)      (8)         (9)
  Remote           Local           St Poll   Reach  Delay    Offset     Disp
  ================ =============== == ===== ===== ======== ========== =======
*192.168.10.254   192.168.10.101    2    16    377 0.00003  0.002101   0.06461
+192.168.30.102   192.168.30.101    4    16    377 0.00027 -0.003163  0.11024
+ Symmetric active, - Symmetric passive, = Client, * System Peer
```

項番	説明
(1)	NTP アソシエーションのモードを表示します。 +：Symmetric active モード -：Symmetric passive モード =：クライアントモード *：同期対象
(2)	対象の IP アドレスを表示します。対象が IPv6 アドレスでアドレス文字数が 16 文字以上の場合は、15 文字目以降が省略表記になります。
(3)	自装置の IP アドレスを表示します。対象が IPv6 アドレスでアドレス文字数が 16 文字以上の場合は、15 文字目以降が省略表記になります。
(4)	対象の Stratum を表示します。

項番	説明
(5)	NTP パケットのポーリング間隔(秒)を表示します。
(6)	対象の到達可能性 (過去 8 回のポーリング結果) を 8 進数で表示します。
(7)	対象への往復遅延時間(秒)を表示します。
(8)	対象との時刻オフセット(秒)を表示します。
(9)	対象との通信における揺らぎ(秒)を表示します。

使用例：NTP アソシエーションの詳細情報を表示する方法を示します。

```
# show ntp associations detail
 (1)                    (2)
Remote 10.249.23.215, Local 10.249.24.175
 (3)              (4)               (5)         (6)
Our mode client, Peer mode server, Stratum 3, Precision -18
 (7)       (8)                    (9)                    (10)
Leap 00, RefID [10.249.45.11], RootDistance 0.03513, RootDispersion 0.09491
 (11)      (12)      (13)      (14)        (15)
PPoll 6, HPoll 6, KeyID 0, Version 4, Association 8355
 (16)        (17)        (18)          (19)        (20)
Reach 377, Unreach 0, Flash 0x0000, Timer 51s, flags  System_Peer, Config
Reference Timestamp : e34f45f6.9a3b3072  Fri, Nov  6 2020 12:48:06.60247 ... (21)
Originate Timestamp : e34f4ac8.cf9728ee  Fri, Nov  6 2020 13:08:40.81090 ... (22)
Receive Timestamp   : e34f4ac8.d97adc9e  Fri, Nov  6 2020 13:08:40.84953 ... (23)
Transmit Timestamp  : e34f4ac8.d97ada2b  Fri, Nov  6 2020 13:08:40.84953 ... (24)
Filter Delay:  0.00000  0.00032  0.00113  0.00122  ... (25)
               0.00124  0.00127  0.00127  0.00111
Filter Offset: 0.038631 0.040588 0.043037 0.045680 ... (26)
               0.049074 0.049002 0.049015 0.049231
Filter Order:  0        1        7        2        ... (27)
               3        4        5        6
 (28)              (29)            (30)                  (31)
Offset 0.038631, Delay 0.00000, Error Bound 0.04013, Filter Error 0.09238
```

項番	説明
(1)	対象の IP アドレスを表示します。
(2)	自装置の IP アドレスを表示します。
(3)	自装置の NTP アソシエーションのモードを表示します。 server：サーバーモード client：クライアントモード active：Symmetric active モード passive：Symmetric passive モード
(4)	対象の NTP アソシエーションのモードを表示します。 server：サーバーモード client：クライアントモード active：Symmetric active モード passive：Symmetric passive モード
(5)	対象の Stratum を表示します。
(6)	精度値を表示します。
(7)	対象から受信した NTP パケットの Leap Indicator フィールドの情報を表示します。
(8)	対象から受信した NTP パケットの Reference ID フィールドの情報を表示します。

項番	説明
(9)	対象から受信した NTP パケットの Root Delay フィールドの情報を表示します。
(10)	対象から受信した NTP パケットの Root Dispersion フィールドの情報を表示します。
(11)	対象のポーリング間隔の値を表示します。
(12)	自装置のポーリング間隔の値を表示します。
(13)	認証キーID を表示します。
(14)	NTP バージョンを表示します。
(15)	アソシエーション ID を表示します。
(16)	対象の到達可能性 (過去 8 回のポーリング結果) を 8 進数で表示します。
(17)	未到達カウンターを表示します。
(18)	問題点を診断するためのフラッシュステータスワードを表示します。
(19)	ピアタイマー (秒単位) を表示します。
(20)	ピアのフラグを表示します。
(21)	対象から受信した NTP パケットの Reference Timestamp フィールドの情報を表示します。
(22)	対象から受信した NTP パケットの Origin Timestamp フィールドの情報を表示します。
(23)	対象から受信した NTP パケットの Receive Timestamp フィールドの情報を表示します。
(24)	対象から受信した NTP パケットの Transmit Timestamp フィールドの情報を表示します。
(25)	各サンプルの往復遅延時間(秒)を表示します。
(26)	各サンプルの時刻オフセット(秒)を表示します。
(27)	各サンプルのフィルタリング順序を表示します。
(28)	対象との時刻オフセット(秒)を表示します。
(29)	対象への往復遅延時間(秒)を表示します。
(30)	対象との通信における揺らぎ(秒)を表示します。
(31)	各サンプルの近似誤差(秒)を表示します。

4.7.15 show ntp status

show ntp status	
目的	NTP の状態を表示します。
Command	show ntp status
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：NTP の状態を表示する方法を示します。

```
# show ntp status

Leap Indicator:        Synchronized ...(1)
```

```
Stratum:                6 ...(2)
Precision:              -7 ...(3)
Root Distance:          0.09572 s ...(4)
Root Dispersion:        0.35197 s ...(5)
Reference ID:           [10.0.0.12] ...(6)
Reference Time:         d6ef417e.74ccec52  Tue, Mar  1 2016
3:48:14.00456 ...(7)
System Flags:           Auth Monitor NTP Kernel Stats ...(8)
Jitter:                 0.007813 s ...(9)
Stability:              0.000 ppm ...(10)
Auth Delay:             0.000000 s ...(11)
```

項番	説明
(1)	Leap Indicator フィールドの情報を表示します。 Synchronized：信頼できる情報源と時刻を同期している状態 Unsynchronized：信頼できる情報源と時刻を同期できていない状態
(2)	自装置の Stratum を表示します。
(3)	精度値を表示します。
(4)	最上位の NTP サーバーへの往復遅延時間(秒)を表示します。
(5)	最上位の NTP サーバーとの通信における揺らぎ(秒)を表示します。
(6)	自装置が同期している NTP サーバーの IP アドレスを表示します。
(7)	自装置が最後に時刻同期を実施した時刻を表示します。
(8)	システムフラグを表示します。
(9)	システムジッター(秒)を表示します。
(10)	周波数の安定性を表示します。
(11)	認証遅延(秒)を表示します。

4.8 TELNET コマンド

TELNET 関連の設定コマンドは以下のとおりです。

- ip telnet server
- ip telnet service-port
- ip telnet source-interface

TELNET 関連の show／操作コマンドは以下のとおりです。

- show ip telnet server
- telnet（クライアント）

4.8.1 ip telnet server

ip telnet server	
目的	Telnet サーバー機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip telnet server no ip telnet server
Parameter	なし
デフォルト	有効（ip telnet server）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：Telnet サーバー機能を有効にする方法を示します。

```
# configure terminal
(config)# ip telnet server
(config)#
```

4.8.2 ip telnet service-port

ip telnet service-port	
目的	Telnet で使用する TCP ポート番号を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip telnet service-port TCP-PORT no ip telnet service-port
Parameter	TCP-PORT：TCP ポート番号を 1～65535 の範囲で指定します。Telnet プロトコルのウェルノウン TCP ポート番号は 23 です。番号によっては、他のプロトコルと競合する場合があります。
デフォルト	23
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-

ip telnet service-port	
制限・注意	• 以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 161(snmp), 162(snmptrap), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip ssh service-port • snmp-server service-port • snmp-server host • web-authentication http-port • web-authentication https-port • web-authentication redirect proxy-port • web-authentication snooping proxy-port • web-deny-notify http-port • web-deny-notify https-port • radius-server host • tacacs-server host
バージョン	1.08.02

使用例：Telnet で使用する TCP ポート番号を 3000 に設定する方法を示します。

```
# configure terminal
(config)# ip telnet service-port 3000
(config)#
```

4.8.3 ip telnet source-interface

ip telnet source-interface	
目的	Telnet クライアントの送信元 IP アドレスとして使用するインターフェースを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip telnet source-interface IF-ID no ip telnet source-interface
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定
デフォルト	最も近いインターフェースの IP アドレスを使用
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• マネージメントポート経由で管理する場合は、vlan パラメーターを指定して本コマンドを設定しないでください。 • VLAN インターフェース経由で管理する場合は、mgmt パラメーターを指定して本コマンドを設定しないでください。
バージョン	1.08.02

使用例：Telnet クライアントの送信元 IP アドレスとして、VLAN 1 インターフェースの IP アドレスを設定する方法を示します。

```
# configure terminal
(config)# ip telnet source-interface vlan 1
(config)#
```

4.8.4 show ip telnet server

show ip telnet server	
目的	Telnet サーバーの有効／無効を表示します。
Command	show ip telnet server
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：Telnet サーバーの有効／無効を表示する方法を示します。

```
# show ip telnet server

Server State: Enabled ...(1)
```

項番	説明
(1)	Telnet サーバーの有効(Enabled)／無効(Disabled)を表示します。

4.8.5 telnet (クライアント)

telnet (クライアント)	
目的	Telnet クライアント機能により、他装置に Telnet 接続を行います。
Command	telnet {IP-ADDRESS | IPV6-ADDRESS} [TCP-PORT]
Parameter	IP-ADDRESS：Telnet サーバーの IPv4 アドレスを指定します。 IPV6-ADDRESS：Telnet サーバーの IPv6 アドレスを指定します。 TCP-PORT（省略可能）：TCP ポート番号を 1～65535 の範囲で指定します。指定しない場合は TCP ポート番号は 23 です。
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	Telnet クライアントの送信元 IP アドレスを指定する場合は、ip telnet source-interface コマンドを使用します。
制限・注意	• デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在する Telnet サーバーを指定して本コマンドを実施する場合、宛先判定にはデフォルトゲートウェイ設定よりもデフォルトルートが優先され、宛先(1)(2)のいずれの場合も Telnet パケットは VLAN インターフェースから送信されます。 • 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク

telnet（クライアント）	
	• 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク • そのため、宛先(2)への実施が失敗します。マネージメントポート経由でのみ管理する場合は、送信元 IP アドレス設定(ip telnet source-interface)をマネージメントポート指定で設定することにより、このような状況でも宛先(2)への実施が成功するようになりますが、この設定をすると VLAN インターフェース経由での実施が失敗するようになることに注意してください。
バージョン	1.08.02

使用例：IP アドレス 192.0.2.100（ApresiaNP7000-48X6L）に Telnet する方法を示します。

```
# telnet 192.0.2.100

Ethernet Switch ApresiaNP7000-48X6L

Firmware: Build 1.11.01

User Verification Access
Username:
```

4.9 SSH コマンド

SSH（Secure Shell）関連の設定コマンドは以下のとおりです。

- ip ssh server
- ip ssh service-port
- ip ssh timeout
- ip ssh authentication-retries
- ssh user authentication-method
- ip ssh key-exchange enable
- ip ssh cipher enable
- ip ssh mac enable

SSH（Secure Shell）関連の show／操作コマンドは以下のとおりです。

- show ip ssh
- show ssh algorithm
- show ssh
- show crypto key mypubkey
- crypto key generate
- crypto key zeroize
- ssh（クライアント）

4.9.1 ip ssh server

ip ssh server	
目的	SSH サーバー機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip ssh server no ip ssh server
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ApresiaNP シリーズでは、以下の暗号化方式、鍵交換アルゴリズム、メッセージ認証符号、公開鍵アルゴリズムをサポートしています。 ■ AEOS-NP2500 Ver. 1.12.01 より前のバージョンで使用できるアルゴリズム <暗号化方式> 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, arcfour, blowfish-cbc, cast128-cbc, twofish-cbc, twofish256-cbc, twofish192-cbc, twofish128-cbc <鍵交換アルゴリズム> diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha256 <メッセージ認証符号> hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96 <公開鍵アルゴリズム> ssh-rsa, ssh-dss

ip ssh server	
	■ AEOS-NP2500 Ver. 1.12.01 以降で使用できるアルゴリズム <暗号化方式> 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, arcfour, blowfish-cbc, cast128-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, twofish-cbc, twofish256-cbc, twofish192-cbc, twofish128-cbc <鍵交換アルゴリズム> diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, curve25519-sha256, curve25519-sha256@libssh.org <メッセージ認証符号> hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, hmac-md5, hmac-md5-96, umac-64@openssh.com, umac-128@openssh.com, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-md5-etm@openssh.com, hmac-md5-96-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com <公開鍵アルゴリズム> ssh-rsa, ssh-dss
制限・注意	• 本装置に SSH 接続する場合は、本装置でサポートしている暗号化方式などに対応した SSH クライアントで接続してください。 • SSH クライアントソフトのバージョンアップなどの SSH クライアント側の変更により、本装置との SSH 接続ができなくなることがあります。そのような場合には SSH クライアント側の設定も見直して、本装置で有効にしている暗号化方式などが使用できる設定になっているか見直してください。
バージョン	1.08.02 1.12.01：サポートする各種アルゴリズムを追加

使用例：SSH サーバー機能を有効にする方法を示します。

```
# configure terminal
(config)# ip ssh server
(config)#
```

4.9.2 ip ssh service-port

ip ssh service-port	
目的	SSH で使用する TCP ポート番号を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip ssh service-port TCP-PORT no ip ssh service-port

ip ssh service-port	
Parameter	TCP-PORT：TCP ポート番号を 1～65535 の範囲で指定します。SSH プロトコルのウェルノウン TCP ポート番号は 22 です。番号によっては、他のプロトコルと競合する場合があります。
デフォルト	22
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 161(snmp), 162(snmptrap), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • snmp-server service-port • snmp-server host • web-authentication http-port • web-authentication https-port • web-authentication redirect proxy-port • web-authentication snooping proxy-port • web-deny-notify http-port • web-deny-notify https-port • radius-server host • tacacs-server host
バージョン	1.08.02

使用例：SSH で使用する TCP ポート番号を 3000 に設定する方法を示します。

```
# configure terminal
(config)# ip ssh service-port 3000
(config)#
```

4.9.3 ip ssh timeout

ip ssh timeout	
目的	SSH 接続のネゴシエーション時のクライアントからの応答待ち時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip ssh timeout SECONDS no ip ssh timeout
Parameter	SECONDS：応答待ち時間を 30～600 秒の範囲で指定します。
デフォルト	120 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-

ip ssh timeout	
バージョン	1.08.02

使用例：SSH 接続のネゴシエーション時のクライアントからの応答待ち時間を 160 秒に設定する方法を示します。

```
# configure terminal
(config)# ip ssh timeout 160
(config)#
```

4.9.4 ip ssh authentication-retries

ip ssh authentication-retries	
目的	SSH 認証の再試行回数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip ssh authentication-retries VALUE no ip ssh authentication-retries
Parameter	VALUE：SSH 認証の再試行回数を 1～32 回の範囲で指定します。
デフォルト	3
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	すべての再試行が失敗した場合はセッションが閉じられます。
制限・注意	-
バージョン	1.08.02

使用例：SSH 認証の再試行回数を 2 回に設定する方法を示します。

```
# configure terminal
(config)# ip ssh authentication-retries 2
(config)#
```

4.9.5 ssh user authentication-method

ssh user authentication-method	
目的	ユーザーアカウントの SSH 認証方式を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ssh user NAME authentication-method {password | publickey URL | hostbased URL host-name NAME [IP-ADDRESS | IPV6-ADDRESS]} no ssh user NAME authentication-method
Parameter	user NAME：ユーザー名を最大 32 文字で指定します。既存のローカルアカウントを指定してください。 password：SSH ユーザー認証にパスワード認証方式を使用する場合に指定します。パスワード認証方式がデフォルトの認証方式です。 publickey URL：SSH ユーザー認証に公開鍵認証方式を使用する場合に指定します。ユーザーの公開鍵の URL を指定してください。 hostbased URL：SSH ユーザー認証にホストベース認証方式を使用します。SSH クライアントのホスト鍵の URL を入力してください。

ssh user authentication-method	
	host-name NAME：ホストベース認証方式で許可するホスト名を 1～255 文字の範囲で指定します。認証フェーズ中に、SSH クライアントのホスト名が確認されます。 IP-ADDRESS（省略可能）：ホストベース認証方式で SSH クライアントの IPv4 アドレスを確認する場合、SSH クライアントの IPv4 アドレスを指定します。SSH クライアントの IPv4 アドレスを指定しない場合は、ホスト名のみ確認されます。 IPV6-ADDRESS（省略可能）：ホストベース認証方式で SSH クライアントの IPv6 アドレスを確認する場合、SSH クライアントの IPv6 アドレスを指定します。SSH の IPv6 アドレスを指定しない場合、ホスト名のみ確認されます。
デフォルト	パスワード認証方式（password）
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	本コマンドは未設定のユーザー名を指定して実行できません。 username コマンドでユーザーアカウントを設定すると、そのユーザーアカウントに対応した本設定が自動的に作成されます。また、no username コマンドでユーザーアカウントを削除すると、対応する本設定も自動的に削除されます。 設定済みのユーザーアカウントに対して、username 設定を残して本設定だけを削除することはできません。no 形式の本コマンドは「SSH 認証方式をデフォルト設定のパスワード認証方式に戻す」際に使用します。 SSH 公開鍵認証でユーザーを認証する場合は、ユーザーの公開鍵ファイルをファイルシステムにコピーします。 • 両方の鍵ファイルは、同じ形式にします。鍵ファイルには複数の鍵を含められます。各鍵は、1 行で定義します。1 行の最大長は 8KB です。 • 各鍵は、スペースで区切られたフィールド（鍵タイプ、base64 エンコード済み鍵、コメント）で構成されます。鍵タイプと base64 エンコード済み鍵は必須フィールドで、コメントフィールドは省略可能です。鍵タイプフィールドには、ssh-dss または ssh-rsa のどちらかを設定できます。
制限・注意	-
バージョン	1.08.02

使用例：ユーザー「user1」の認証方式を、ユーザーの公開鍵の URL「c:/user1.pub」を指定して公開鍵認証方式に設定する方法を示します。

```
# configure terminal
(config)# ssh user user1 authentication-method publickey c:/user1.pub
(config)#
```

4.9.6 ip ssh key-exchange enable

ip ssh key-exchange enable	
目的	指定した鍵交換方式（Key exchange algorithms）を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip ssh key-exchange enable ALGORITHM no ip ssh key-exchange enable ALGORITHM
Parameter	ALGORITHM：対象となる鍵交換方式を以下から指定します。 • diffie-hellman-group1-sha1

ip ssh key-exchange enable	
	• diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • diffie-hellman-group16-sha512 • diffie-hellman-group18-sha512 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • curve25519-sha256 • curve25519-sha256@libssh.org
デフォルト	すべて有効（ip ssh key-exchange enable ALGORITHM）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドで SSH サーバー機能で使用する鍵交換方式（Key exchange algorithms）の有効／無効を設定できます。 デフォルト設定ではすべての鍵交換方式が有効ですが、本コマンドで鍵交換方式ごとに無効にすることができます。
制限・注意	• 同時にすべての鍵交換方式を無効にすることはできません。少なくとも 1 つは有効にしておく必要があります。 • 本コマンドは SSH クライアント機能には適用されません。
バージョン	1.12.01

使用例：鍵交換方式「diffie-hellman-group1-sha1」を無効にする方法を示します。

```
# configure terminal
(config)# no ip ssh key-exchange enable diffie-hellman-group1-sha1
(config)#
```

4.9.7 ip ssh cipher enable

ip ssh cipher enable	
目的	指定した暗号化方式（Cipher algorithms）を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip ssh cipher enable ALGORITHM no ip ssh cipher enable ALGORITHM
Parameter	ALGORITHM：対象となる暗号化方式を以下から指定します。 • 3des-cbc • aes128-cbc • aes192-cbc • aes256-cbc • aes128-ctr • aes192-ctr • aes256-ctr • arcfour

ip ssh cipher enable	
	• blowfish-cbc • cast128-cbc • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly1305@openssh.com • twofish-cbc • twofish256-cbc • twofish192-cbc • twofish128-cbc
デフォルト	すべて有効（ip ssh cipher enable ALGORITHM）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドで SSH サーバー機能で使用する暗号化方式（Cipher algorithms）の有効／無効を設定できます。AEOS-NP2500 Ver. 1.13.01 以降では、本コマンドは SSH クライアント機能にも適用されます。 デフォルト設定ではすべての暗号化方式が有効ですが、本コマンドで暗号化方式ごとに無効にすることができます。
制限・注意	• 同時にすべての暗号化方式を無効にすることはできません。少なくとも 1 つは有効にしておく必要があります。
バージョン	1.12.01

使用例：暗号化方式「arcfour」を無効にする方法を示します。

```
# configure terminal
(config)# no ip ssh cipher enable arcfour
(config)#
```

4.9.8 ip ssh mac enable

ip ssh mac enable	
目的	指定したメッセージ認証符号（Message Authentication Code）を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip ssh mac enable ALGORITHM no ip ssh mac enable ALGORITHM
Parameter	ALGORITHM：対象となるメッセージ認証符号を以下から指定します。 • hmac-sha1 • hmac-sha1-96 • hmac-sha2-256 • hmac-sha2-512 • hmac-md5 • hmac-md5-96 • umac-64@openssh.com • umac-128@openssh.com • hmac-sha1-etm@openssh.com • hmac-sha1-96-etm@openssh.com

ip ssh mac enable	
	• hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • hmac-md5-etm@openssh.com • hmac-md5-96-etm@openssh.com • umac-64-etm@openssh.com • umac-128-etm@openssh.com
デフォルト	すべて有効（ip ssh mac enable ALGORITHM）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドで SSH サーバー機能で使用するメッセージ認証符号（Message Authentication Code）の有効／無効を設定できます。AEOS-NP2500 Ver. 1.13.01 以降では、本コマンドは SSH クライアント機能にも適用されます。 デフォルト設定ではすべてのメッセージ認証符号が有効ですが、本コマンドでメッセージ認証符号ごとに無効にすることができます。
制限・注意	• 同時にすべてのメッセージ認証符号を無効にすることはできません。少なくとも 1 つは有効にしておく必要があります。
バージョン	1.12.01

使用例：メッセージ認証符号「hmac-md5」を無効にする方法を示します。

```
# configure terminal
(config)# no ip ssh mac enable hmac-md5
(config)#
```

4.9.9 show ip ssh

show ip ssh	
目的	SSH サーバーの設定を表示します。
Command	show ip ssh
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SSH サーバーの設定を表示する方法を示します。

```
# show ip ssh

IP SSH server              : Enabled ...(1)
IP SSH service port        : 22 ...(2)
SSH server mode            : V2 ...(3)
Authentication timeout     : 120 secs ...(4)
Authentication retries     : 3 times ...(5)
```

項番	説明
(1)	SSH サーバーの有効(Enabled)／無効(Disabled)を表示します。
(2)	SSH の TCP ポート番号を表示します。
(3)	SSH サーバーのバージョンを表示します。
(4)	認証タイムアウト時間を表示します。
(5)	認証リトライ回数を表示します。

4.9.10 show ssh algorithm

show ssh algorithm	
目的	鍵交換方式、暗号化方式、メッセージ認証符号の有効／無効を表示します。
Command	show ssh algorithm
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.12.01

使用例：鍵交換方式、暗号化方式、メッセージ認証符号の有効／無効を表示する方法を示します。

```
# show ssh algorithm

Key Exchange ...(1)                       State ...(2)
----------------------------------------  --------
diffie-hellman-group1-sha1                Enabled
diffie-hellman-group14-sha1               Enabled
diffie-hellman-group14-sha256             Enabled
diffie-hellman-group16-sha512             Enabled
diffie-hellman-group18-sha512             Enabled
diffie-hellman-group-exchange-sha1        Enabled
diffie-hellman-group-exchange-sha256      Enabled
ecdh-sha2-nistp256                        Enabled
ecdh-sha2-nistp384                        Enabled
ecdh-sha2-nistp521                        Enabled
curve25519-sha256                         Enabled
curve25519-sha256@libssh.org              Enabled

Cipher ...(3)                             State ...(4)
----------------------------------------  --------
3des-cbc                                  Enabled
aes128-cbc                                Enabled
aes192-cbc                                Enabled
aes256-cbc                                Enabled
aes128-ctr                                Enabled
aes192-ctr                                Enabled
aes256-ctr                                Enabled
arcfour                                   Enabled
blowfish-cbc                              Enabled
cast128-cbc                               Enabled
aes128-gcm@openssh.com                    Enabled
aes256-gcm@openssh.com                    Enabled
chacha20-poly1305@openssh.com             Enabled
twofish-cbc                               Enabled
```

```
twofish256-cbc                          Enabled
twofish192-cbc                          Enabled
twofish128-cbc                          Enabled

Message Authentication Code ...(5)      State ...(6)
--------------------------------------  --------
hmac-sha1                               Enabled
hmac-sha1-96                            Enabled
hmac-sha2-256                           Enabled
hmac-sha2-512                           Enabled
hmac-md5                                Enabled
hmac-md5-96                             Enabled
umac-64@openssh.com                     Enabled
umac-128@openssh.com                    Enabled
hmac-sha1-etm@openssh.com               Enabled
hmac-sha1-96-etm@openssh.com            Enabled
hmac-sha2-256-etm@openssh.com           Enabled
hmac-sha2-512-etm@openssh.com           Enabled
hmac-md5-etm@openssh.com                Enabled
hmac-md5-96-etm@openssh.com             Enabled
umac-64-etm@openssh.com                 Enabled
umac-128-etm@openssh.com                Enabled

Public Key Algorithm ...(7)
--------------------------------------
ssh-rsa
ssh-dss
```

項番	説明
(1)	鍵交換方式 (Key exchange algorithms) を表示します。
(2)	各鍵交換方式の有効(Enabled)／無効(Disabled)を表示します。
(3)	暗号化方式 (Cipher algorithms) を表示します。
(4)	各暗号化方式の有効(Enabled)／無効(Disabled)を表示します。
(5)	メッセージ認証符号 (Message Authentication Code) を表示します。
(6)	各メッセージ認証符号の有効(Enabled)／無効(Disabled)を表示します。
(7)	公開鍵アルゴリズム (Public Key Algorithm) を表示します。

4.9.11 show ssh

show ssh	
目的	SSH 接続の情報を表示します。
Command	show ssh
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• Cipher 項目の表示内容が 30 文字以上になる組み合わせの場合、Cipher 項目と Userid 項目の間の半角空白が表示されなくなったり、同じ行の Userid 項目以降の表示内容が右にズレて表示される制限があります。
バージョン	1.08.02 1.12.01：サポートする各種アルゴリズムを追加

使用例：SSH 接続の情報を表示する方法を示します。

```
# show ssh
 (1)  (2)   (3)                          (4)              (5)
SID Ver. Cipher                         Userid           Client IP Address
--- ---- ------------------------------ ---------------- ----------------------
0   V2   aes256-ctr/hmac-sha2-256       user1            192.0.2.100
1   V2   3des-cbc/hmac-sha1             user2            2001:db8::243

Total Entries: 2
```

項番	説明
(1)	SSH セッションを識別する一意の番号を表示します。
(2)	SSH のバージョンを表示します。
(3)	使用している暗号化方式を表示します。また、関連するメッセージ認証符号も表示します。 <暗号化方式> 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, arcfour, blowfish-cbc, cast128-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, twofish-cbc, twofish256-cbc, twofish192-cbc, twofish128-cbc <メッセージ認証符号> hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, hmac-md5, hmac-md5-96, umac-64@openssh.com, umac-128@openssh.com, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-md5-etm@openssh.com, hmac-md5-96-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com
(4)	ログインユーザー名を表示します。
(5)	SSH クライアントの IP アドレスを表示します。

4.9.12 show crypto key mypubkey

show crypto key mypubkey	
目的	SSH サーバーの RSA 鍵、または DSA 鍵を表示します。
Command	show crypto key mypubkey {rsa | dsa}
Parameter	rsa：RSA 鍵を表示する場合に指定します。 dsa：DSA 鍵を表示する場合に指定します。
モード	特権実行モード、任意の設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SSH サーバーの RSA 鍵に関する情報を表示する方法を示します。

```
# show crypto key mypubkey rsa
```

```
% Key pair was generated at: 13:02:23, 2024-07-23 ...(1)
Key Size: 2048 bits ...(2)
Key Data: ...(3)
AAAAB3Nz aC1yc2EA AAADAQAB AAABAQD2 tE2iMT+e urUzKLjr 2xx1DENl jPdk3W4Z
6Mpg5btT haFksJfr +JRfbkq+ cMt4zOur /vO5etKR NdsTuHco czdo8M/6 kvPYQlp3
j0+uyPaU bYxRHdrY mZs+lVP9 xUZnf9IE t2CB11FF GSq9deIP mKtZsCn+ nfHo6DMf
iMAuJy4O TK/3gFY0 Qpsp8G3o PdEK5gKu n2iKnLEh F4ZXni3p OYnVJsj9 bE9jlbT1
yB5dtad+ wcy0Ko85 F2THjcJ/ 5+nKsk0Z XjHVm2m8 MVXet39h aVHj9Krz I9LU6L18
BWnyzVCc eY1Wh9Ft UkrzKnY+ XapB15aH 8UuyeTF4 PJQ6Uy15 R/cL
```

項番	説明
(1)	RSA 鍵対が生成された日時を表示します。 restore コマンドを実行して装置を起動しなおした後は、restore コマンド実行時の時刻（RSA 鍵が置き換えられた時刻）に変更されます。 SD カードブートで起動した場合は、RSA 鍵が置き換えられた起動時の時刻に変更されます。なお、この場合は UTC 時刻が記録されます。
(2)	RSA 鍵の鍵長を表示します。
(3)	RSA 鍵の情報を表示します。

使用例：SSH サーバーの DSA 鍵に関する情報を表示する方法を示します。

```
# show crypto key mypubkey dsa

% Key pair was generated at: 14:55:01, 2020-06-02 ...(1)
Key Size: 1024 bits ...(2)
Key Data: ...(3)
AAAAB3Nz aC1kc3MA AACBAL7+ Pi0IEeTE 57pUbmuy XfyUultm T1IP/vvP ebFLRMRF
57gyjM/v RUpipRs5 zz4xOuyl 5gT5Jfkm wyfhPUsJ mA3wW3U4 fMYCHoHx qzGYRey1
/uIce7wU vORSLc/o kgRDYbfu AvvvMqCh Hn72k1n/ D6ftT324 kHfVymGg 4GQ/ICwP
AAAAFQDM cz4dZV/Q Tv/QbTj8 oZTLiRpb FwAAAIEA gS1wH5Jf 8FngnwDg 21QfXRGW
40MoIO4H h+g6E1MF NdFxruOf QG3++sj0 rcEMsqpW T2lqu5zF K4n5J6tj YD1Ep7fn
2Q+vidj7 A9PFI5KQ x1aASrQA AedExUMQ zpuXA94/ jJbNR3TM MKC/YtkK S0Vd3sUF
QyiAjV8t RG7gT2mH Gp8AAACB AKBCupVR +XyOtk53 6HFqp6gZ wHygUgNq ue5m6XIn
yG6zFgln j78yf0q2 7HqfXRlh lWDjKisx d8makEme u/ecwoTN fWFfxC7j V0Qvfzdz
MrtHSca9 AFenLAw7 PX9eNieh 73D8G8PW ws9FT+C0 EkBtA7ly uJrqj4/D +FnLH7dy
PfXD
```

項番	説明
(1)	DSA 鍵対が生成された日時を表示します。 restore コマンドを実行して装置を起動しなおした後は、restore コマンド実行時の時刻（DSA 鍵が置き換えられた時刻）に変更されます。 SD カードブートで起動した場合は、DSA 鍵が置き換えられた起動時の時刻に変更されます。なお、この場合は UTC 時刻が記録されます。
(2)	DSA 鍵の鍵長を表示します。DSA の場合は 1024 ビット固定です。
(3)	DSA 鍵の情報を表示します。

4.9.13 crypto key generate

crypto key generate	
目的	SSH サーバーの RSA 鍵対または DSA 鍵対を生成します。

crypto key generate	
Command	crypto key generate {rsa [modulus SIZE] | dsa}
Parameter	rsa：RSA 鍵対を生成する場合に指定します。 modulus SIZE（省略可能）：RSA の鍵長を指定します。使用可能な鍵長は 512、768、1024、2048 ビットです。AEOS-NP2500 Ver. 1.12.01 より前のバージョンでは 360 ビットも使用可能です。 dsa：DSA 鍵対を生成する場合に指定します。DSA の鍵長は 1024 ビット固定です。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	すでに RSA 鍵対または DSA 鍵対を生成済みの装置で本コマンドを実行した場合は、鍵対を置き換えるかどうかの確認メッセージが表示されます。 SD カードブートを使用している装置で本コマンドを実行して既存の RSA 鍵対または DSA 鍵対を置き換えても、SD カードに保存されている RSA 鍵対ファイル（apresia-rsa-key）、または DSA 鍵対ファイル（apresia-dsa-key）は変更されません。
制限・注意	• AEOS-NP2500 Ver. 1.12.01 以降では、RSA の鍵長 360 ビットは未サポートに仕様変更されています。 • クライアントが要求するサーバーのホストキー優先順位が、DSA 鍵より RSA 鍵の方が高い設定のクライアントを接続する場合は、RSA 鍵は必ず作成してください。 • 同様に、クライアントが要求するサーバーのホストキー優先順位が、RSA 鍵より DSA 鍵の方が高い設定のクライアントを接続する場合は、DSA 鍵は必ず作成してください。 • RSA の鍵長が大きいほど、RSA 鍵対の生成時間が長くなります。RSA の鍵長を 2048 ビットで指定した場合は、本コマンドの実行完了までに約 2～6 分程度の時間がかかることがあります。 • AEOS-NP2500 Ver. 1.12.01 より前のバージョンで RSA 鍵対を鍵長 360 ビットで生成して使用していた装置を AEOS-NP2500 Ver. 1.12.01 以降にバージョンアップした場合、そのままでも SSH ログインは可能ですが、AEOS-NP2500 Ver. 1.12.01 以降では鍵長 360 ビットは未サポートのため、512 ビット以上の鍵長に生成しなおしてご使用ください。
バージョン	1.08.02 1.12.01：RSA の鍵長 360 ビットを未サポートに仕様変更

使用例：SSH サーバーの RSA 鍵対の生成方法を示します。

```
# crypto key generate rsa

Choose the size of the key modulus in the range of 360 to 2048. The process
may take a few minutes.
Number of bits in the modulus [768]: 2048
Generating RSA key...Done.
```

使用例：SSH サーバーの DSA 鍵対の生成方法を示します。

```
# crypto key generate dsa

Generating DSA key...Done.
```

4.9.14 crypto key zeroize

crypto key zeroize	
目的	SSH サーバーの RSA 鍵対または DSA 鍵対を削除します。
Command	crypto key zeroize {rsa | dsa}
Parameter	rsa：RSA 鍵対を削除する場合に指定します。 dsa：DSA 鍵対を削除する場合に指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	RSA 鍵対または DSA 鍵対が保存されていない装置で本コマンドを実行した場合は、鍵対を削除するかどうかの確認メッセージは表示されません。 SD カードブートを使用している装置で本コマンドを実行しても、SD カードに保存されている RSA 鍵対ファイル（apresia-rsa-key）、または DSA 鍵対ファイル（apresia-dsa-key）は削除されません。 RSA 鍵対と DSA 鍵対の両方が削除された場合、SSH サーバーとしてのサービスを実行できません。
制限・注意	-
バージョン	1.08.02

使用例：SSH サーバーの RSA 鍵対の削除方法を示します。

```
# crypto key zeroize rsa

Do you really want to remove the key? (y/n)[n]: y
```

使用例：SSH サーバーの DSA 鍵対の削除方法を示します。

```
# crypto key zeroize dsa

Do you really want to remove the key? (y/n)[n]: y
```

4.9.15 ssh（クライアント）

ssh（クライアント）	
目的	SSH クライアント機能により、他装置に SSH 接続を行います。
Command	ssh [-l NAME] {IP-ADDRESS | IPV6-ADDRESS} [TCP-PORT]
Parameter	-l NAME（省略可能）：現在ログイン中のユーザー名とは異なるユーザー名を使用する場合に指定します。指定しない場合は現在ログイン中のユーザー名で接続します。 IP-ADDRESS：SSH サーバーの IPv4 アドレスを指定します。 IPV6-ADDRESS：SSH サーバーの IPv6 アドレスを指定します。 TCP-PORT（省略可能）：TCP ポート番号を 1～65535 の範囲で指定します。指定しない場合は TCP ポート番号は 22 です。
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	パスワード入力プロンプト（ユーザー名@IP アドレス's password: ）が表示されている状態で SSH クライアント機能を中断するには「Ctrl+C」を入力します。 本機能で SSH サーバーに接続中に、途中の通信経路の障害などにより SSH サーバー

ssh（クライアント）	
	からの応答がなくなった場合は、「~.（チルダ ピリオド）」と連続して入力すると SSH 接続が強制的に中断されます。 SSH クライアントの送信元 IP アドレスを指定する場合は、ip ssh source-interface コマンドを使用します。
制限・注意	• SSH クライアント機能では公開鍵認証方式は対応していません。 • デフォルトルート情報（0.0.0.0/0）とマネージメントポートのデフォルトゲートウェイ設定（ip default-gateway）の両方が存在する装置において、以下の宛先に存在する SSH サーバーを指定して本コマンドを実施する場合、宛先判定にはデフォルトゲートウェイ設定よりもデフォルトルートが優先され、宛先（1）（2）のいずれの場合も SSH パケットは VLAN インターフェースから送信されます。 　• 宛先（1）：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク 　• 宛先（2）：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク • そのため、宛先（2）への実施が失敗します。マネージメントポート経由でのみ管理する場合は、送信元 IP アドレス設定（ip ssh source-interface）をマネージメントポート指定で設定することにより、このような状況でも宛先（2）への実施が成功するようになりますが、この設定をすると VLAN インターフェース経由での実施が失敗するようになることに注意してください。
バージョン	1.13.01

使用例：ユーザー名 test を指定して、IP アドレス 192.0.2.100（ApresiaNP7000-48X6L）に SSH 接続する方法を示します。

```
# ssh -l test 192.0.2.100

 Unknown server, Are you sure you want to continue connecting [y/n]?: y
test@192.0.2.100's password: ****


Ethernet Switch ApresiaNP7000-48X6L

Firmware: Build 1.11.01

#
```

4.10 RMON コマンド

RMON（Remote Network Monitoring）関連の設定コマンドは以下のとおりです。

- rmon collection stats
- rmon collection history
- rmon alarm
- rmon event
- snmp-server enable traps rmon

RMON（Remote Network Monitoring）関連の show コマンドは以下のとおりです。

- show rmon statistics
- show rmon history
- show rmon alarm
- show rmon events

4.10.1 rmon collection stats

rmon collection stats	
目的	RMON 統計情報を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	rmon collection stats ID [owner NAME] no rmon collection stats ID
Parameter	ID：RMON 統計情報 ID を 1～65535 の範囲で指定します。 owner NAME（省略可能）：所有者名を最大 127 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	無効
モード	インターフェース設定モード(port)
特権レベル	レベル：12
ガイドライン	RMON 統計情報 ID は、RMON MIB の statistics グループの ID（etherStatsIndex）に対応しています。
制限・注意	• 複数インターフェースの範囲設定モード(range)では本コマンドは設定できません。
バージョン	1.08.02

使用例：ポート 1/0/2 で、RMON 統計情報 ID=65、所有者名「guest」で RMON 統計情報を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/2
(config-if-port)# rmon collection stats 65 owner guest
(config-if-port)#
```

4.10.2 rmon collection history

rmon collection history	
目的	RMON 統計情報の履歴を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	rmon collection history ID [owner NAME] [buckets VALUE] [interval

rmon collection history	
	SECONDS] **no rmon collection history** ID
Parameter	ID：RMON 履歴 ID を 1～65535 の範囲で指定します。 owner NAME（省略可能）：所有者名を最大 127 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 buckets VALUE（省略可能）：RMON 統計情報を記録する履歴数を、1～65535 の範囲で指定します。指定しない場合は 50 に設定されます。 interval SECONDS（省略可能）：サンプリング間隔を 1～3600（秒）の範囲で指定します。指定しない場合は 1800 秒に設定されます。
デフォルト	無効
モード	インターフェース設定モード（port）
特権レベル	レベル：12
ガイドライン	RMON 履歴 ID は、RMON MIB の history グループの ID（historyControlIndex）に対応しています。 指定した履歴数を超えた後は、最も古い統計情報から削除されて新しい統計情報が記録されます。
制限・注意	• 複数インターフェースの範囲設定モード（range）では本コマンドは設定できません。
バージョン	1.08.02

使用例：ポート 1/0/8 で、RMON 履歴 ID=101、所有者名「guest」、サンプリング間隔=2000 秒で RMON 統計情報の履歴を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/8
(config-if-port)# rmon collection history 101 owner guest interval 2000
(config-if-port)#
```

4.10.3 rmon alarm

rmon alarm	
目的	RMON のアラームエントリーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	**rmon alarm** ID OID INTERVAL {**absolute** | **delta**} **rising-threshold** VALUE [RISING-EVENT-ID] **falling-threshold** VALUE [FALLING-EVENT-ID] [**owner** NAME] **no rmon alarm** ID
Parameter	ID：アラームエントリーID を 1～65535 の範囲で指定します。 OID：監視対象のオブジェクト識別子（OID）を指定します。 INTERVAL：サンプリング間隔を、1～2,147,483,647（秒）の範囲で指定します。 absolute：取得した値をそのままサンプリング値として比較対象にする場合に指定します。 delta：前回取得値と今回取得値の差分値をサンプリング値として比較対象にする場合に指定します。

rmon alarm	
	rising-threshold VALUE：上昇しきい値（上限値）を、0～2,147,483,647 の範囲で指定します。 RISING-EVENT-ID（省略可能）：サンプリング値が上昇しきい値以上になった場合に実行するイベントエントリーID を、1～65535 の範囲で指定します。指定しない場合は、イベントは実行されません。 falling-threshold VALUE：下降しきい値（下限値）を、0～2,147,483,647 の範囲で指定します。 FALLING-EVENT-ID（省略可能）：サンプリング値が下降しきい値以下になった場合に実行するイベントエントリーID を、1～65535 の範囲で指定します。指定しない場合は、イベントは実行されません。 owner NAME（省略可能）：所有者名を最大 127 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	アラームエントリーID は、RMON MIB の alarm グループの ID（alarmIndex）に対応しています。 アラームエントリーを設定すると、監視対象のオブジェクト識別子（OID）の値を指定したサンプリング間隔で取得します。absolute 方式の場合、取得した値をそのままサンプリング値として使用します。delta 方式の場合、前回取得値と今回取得値の差分値をサンプリング値として使用します。 サンプリング値が上昇しきい値（上限値）以上になった場合に、指定したイベントエントリーID の上昇しきい値イベントが実行されます。なお、上昇しきい値イベントが発生した後は、サンプリング値が上昇しきい値（上限値）を下回り、下降しきい値（下限値）に到達するまで、別のイベントは発生しません。 サンプリング値が下降しきい値（下限値）以下になった場合に、指定したイベントエントリーID の下降しきい値イベントが実行されます。なお、下降しきい値イベントが発生した後は、サンプリング値が下降しきい値（下限値）を上回り、上昇しきい値（上限値）に到達するまで、別のイベントは発生しません。
制限・注意	• Counter64 型のオブジェクト識別子（OID）は監視対象として指定できません。
バージョン	1.08.02

使用例：アラームエントリーID=783、監視対象 OID=1.3.6.1.2.1.2.2.1.12.6、サンプリング間隔=30秒、比較方式=delta 方式、上昇しきい値(上限値)=20、上昇しきい値のイベントエントリーID=1、下降しきい値(下限値)=10、下降しきい値のイベントエントリーID=2、所有者名「guest」でアラームエントリーを設定する方法を示します。

```
# configure terminal
(config)# rmon alarm 783 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1
falling-threshold 10 2 owner guest
(config)#
```

4.10.4 rmon event

rmon event	
目的	RMON のイベントエントリーを設定します。設定を削除する場合は、no 形式のコマ

rmon event	
	ンドを使用します。
Command	rmon event ID [log] [trap COMMUNITY] [owner NAME] [description STRING] no rmon event ID
Parameter	ID：イベントエントリーID を 1～65535 の範囲で指定します。 log（省略可能）：イベント発生時のログ記録（RMON MIB の logTable）を有効にする場合に指定します。 trap COMMUNITY（省略可能）：イベント発生時の SNMP トラップ送信を有効にする場合に、SNMP コミュニティー名を最大 127 文字で指定します。 owner NAME（省略可能）：所有者名を最大 127 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 description STRING（省略可能）：イベントエントリーの説明を、最大 127 文字で指定します。ASCII コードの印字可能な文字のうち、? を除いた文字を使用可能です。スペースも使用できます。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	イベントエントリーID は、RMON MIB の event グループの ID（eventIndex）に対応しています。
制限・注意	-
バージョン	1.08.02

使用例：イベントエントリーID=13、ログ記録（RMON MIB の logTable）は有効、SNMP トラップ送信は有効で SNMP コミュニティー名「public」、所有者名「guest」、イベントエントリーの説明「ifInErrors is too much」でイベントエントリーを設定する方法を示します。

```
# configure terminal
(config)# rmon event 13 log trap public owner guest description ifInErrors is
too much
(config)#
```

4.10.5 snmp-server enable traps rmon

snmp-server enable traps rmon	
目的	RMON 機能の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps rmon [rising-alarm | falling-alarm] no snmp-server enable traps rmon [rising-alarm | falling-alarm]
Parameter	rising-alarm（省略可能）：上昇しきい値イベントが発生した際の通知を有効にする場合に指定します。 falling-alarm（省略可能）：下降しきい値イベントが発生した際の通知を有効にする場合に指定します。
デフォルト	無効
モード	グローバル設定モード

snmp-server enable traps rmon	
特権レベル	レベル：12
ガイドライン	パラメーターを指定しない場合は、すべてのパラメーターが対象になります。 本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。
制限・注意	-
バージョン	1.08.02

使用例：RMON 機能の SNMP トラップを有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps rmon
(config)#
```

4.10.6 show rmon statistics

show rmon statistics	
目的	RMON 統計情報を表示します。
Command	show rmon statistics
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：RMON 統計情報を表示する方法を示します。

```
# show rmon statistics
 (1)       (2)              (3)
Index 1, owned by guest, Data source is Port1/0/1
  Received octets: 518394321, Received packets: 5228964 ...(4)
  Broadcast packets: 2559743, Multicast packets: 988945 ...(5)
  Undersized packets: 0, Oversized packets: 0 ...(6)
  Fragments: 0, Jabbers: 0 ...(7)
  CRC alignment errors: 0, Collisions: 0 ...(8)
  Drop events: 887 ...(9)
  Packets in 64 octets: 4255288, Packets in 65-127 octets: 128250 ...(10)
  Packets in 128-255 octets: 576077, Packets in 256-511 octets: 102826 ...(10)
  Packets in 512-1023 octets: 165799, Packets in 1024-1518 octets: 724 ...(10)
```

項番	説明
(1)	RMON 統計情報 ID を表示します。
(2)	所有者名を表示します。
(3)	RMON 統計情報の対象ポート番号を表示します。
(4)	受信オクテット数、および受信パケット数を表示します。
(5)	ブロードキャストパケット数、およびマルチキャストパケット数を表示します。
(6)	アンダーサイズ（フレーム長が 64 オクテットよりも小さい）パケット数、およびオーバーサイズ（フレーム長が 1,518 オクテットよりも大きい）パケット数を表示します。

項番	説明
(7)	フラグメント（フレーム長が 64 オクテットよりも小さいパケットのうち、FCS エラーを伴う）パケット数、およびジャバー（フレーム長が 1,518 オクテットよりも大きいパケットのうち、FCS エラーを伴う）パケット数を表示します。
(8)	フレーム長が 64～1,518 オクテットのパケットのうち、FCS エラーを伴うパケット数、およびコリジョンの推定値を表示します。
(9)	リソース不足のために廃棄されたイベントの検出回数を表示します。
(10)	フレーム長ごとの受信パケット数を表示します。

4.10.7 show rmon history

show rmon history	
目的	RMON 統計情報の履歴を表示します。
Command	show rmon history
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：RMON 統計情報の履歴を表示する方法を示します。

```
# show rmon history
 (1)         (2)              (3)
Index 101, owned by test, Data source is Port1/0/1
 Interval: 60 seconds ...(4)
 Requested buckets: 50, Granted buckets: 50 ...(5)
 Sample 1 ...(6)
  Received octets: 9303, Received packets: 107 ...(7)
  Broadcast packets: 37, Multicast packets: 14 ...(8)
  Estimated utilization: 100 ...(9)
  Undersized packets: 0, Oversized packets: 0 ...(10)
  Fragments: 0, Jabbers: 0 ...(11)
  CRC alignment errors: 0, Collisions: 0 ...(12)
  Drop events: 0 ...(13)
 Sample 2
  Received octets: 11027, Received packets: 110
  Broadcast packets: 32, Multicast packets: 20
  Estimated utilization: 0
  Undersized packets: 0, Oversized packets: 0
  Fragments: 0, Jabbers: 0
  CRC alignment errors: 0, Collisions: 0
  Drop events: 0
 Sample 3
  Received octets: 8762, Received packets: 103
  Broadcast packets: 29, Multicast packets: 17
  Estimated utilization: 100
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

項番	説明
(1)	RMON 履歴 ID を表示します。

項番	説明
(2)	所有者名を表示します。
(3)	RMON 履歴の対象ポート番号を表示します。
(4)	サンプリング間隔を表示します。
(5)	RMON 統計情報を記録する履歴数を表示します。
(6)	履歴番号を表示します。
(7)	受信オクテット数、および受信パケット数を表示します。
(8)	ブロードキャストパケット数、およびマルチキャストパケット数を表示します。
(9)	サンプリング間隔におけるリンクの推定利用率 (%) を表示します。
(10)	アンダーサイズ（フレーム長が 64 オクテットよりも小さい）パケット数、およびオーバーサイズ (フレーム長が 1,518 オクテットよりも大きい) パケット数を表示します。
(11)	フラグメント（フレーム長が 64 オクテットよりも小さいパケットのうち、FCS エラーを伴う）パケット数、およびジャバー（フレーム長が 1,518 オクテットよりも大きいパケットのうち、FCS エラーを伴う) パケット数を表示します。
(12)	フレーム長が 64～1,518 オクテットのパケットのうち、FCS エラーを伴うパケット数、およびコリジョンの推定値を表示します。
(13)	リソース不足のために廃棄されたイベントの検出回数を表示します。

4.10.8 show rmon alarm

show rmon alarm	
目的	アラームエントリーを表示します。
Command	show rmon alarm
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：アラームエントリーを表示する方法を示します。

```
# show rmon alarm
 (1)              (2)
Alarm Index 23, owned by IT
 Monitors OID: 1.3.6.1.2.1.2.2.1.10.1 ...(3)
 every 120 second(s) ...(4)
  (5)                    (6)
 Taking delta samples, last value was 2500
 Rising threshold is 2000, assigned to event 12 ...(7)
 Falling threshold is 1100, assigned to event 12 ...(8)
 On startup enable rising or falling alarm ...(9)
```

項番	説明
(1)	アラームエントリーID を表示します。
(2)	所有者名を表示します。

項番	説明
(3)	監視対象のオブジェクト識別子 (OID) を表示します。
(4)	サンプリング間隔を表示します。
(5)	上昇しきい値 (上限値)、および下降しきい値 (下限値) との比較方式を表示します。 Taking absolute samples：サンプリング値をそのまま比較対象にする absolute 方式 Taking delta samples：前回のサンプリング値からの差分値を比較対象にする delta 方式
(6)	最新のサンプリング値を表示します。
(7)	上昇しきい値（上限値)、および上昇しきい値イベント発生時に使用するイベントエントリー ID を表示します。
(8)	下降しきい値（下限値)、および下降しきい値イベント発生時に使用するイベントエントリー ID を表示します。
(9)	アラームエントリーが開始してから初めてのサンプリング値を、上昇しきい値（上限値)、および下降しきい値 (下限値) との判定対象として使用することを意味します。

4.10.9 show rmon events

show rmon events	
目的	イベントエントリーを表示します。
Command	show rmon events
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：イベントエントリーを表示する方法を示します。

```
# show rmon events
 (1)          (2)
Event 1001, owned by guest
 Description is Errors over 100 packets ...(3)
 Event trigger action: log & trap send to community public ...(4)
 Last triggered time: 21:59:2, 3 ...(5)
 Log: 1 ...(6)
  Log Time: 3d, 21h:57m:32s ...(7)
  Log Description: Errors over 100 packets ...(8)
 Log: 2
  Log Time: 3d, 21h:59m:2s
  Log Description: Errors over 100 packets
```

項番	説明
(1)	イベントエントリーID を表示します。
(2)	所有者名を表示します。
(3)	イベントエントリーの説明を表示します。
(4)	イベントエントリーのアクションを表示します。
(5)	直近のイベント発生時の sysUpTime の値を表示します。

項番	説明
(6)	ログ番号を表示します。ログは、イベント発生時のログ記録（RMON MIB の logTable）を有効にしている場合に表示されます。
(7)	イベント発生時の sysUpTime の値を表示します。
(8)	イベントエントリーの説明を表示します。

4.11 sFlow コマンド

sFlow 関連の設定コマンドは以下のとおりです。

- sflow receiver
- sflow sampler
- sflow poller

sFlow 関連の show コマンドは以下のとおりです。

- show sflow

4.11.1 sflow receiver

sflow receiver	
目的	sFlow エージェントのレシーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	**sflow receiver** ID **owner** NAME [**expiry** {SECONDS | **infinite**}] [**max-datagram-size** SIZE] [**host** {IP-ADDRESS | IPV6-ADDRESS}] [**udp-port** PORT] **no sflow receiver** ID
Parameter	ID：レシーバーID を 1～4 の範囲で指定します。 owner NAME：レシーバーの所有者名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 expiry（省略可能）：レシーバーの有効期限を以下のパラメーターで指定します。 • SECONDS：有効期限を 1～2,000,000 秒の範囲で指定 • infinite：有効期限を無期限にする場合に指定 max-datagram-size SIZE（省略可能）：sFlow データグラムの最大サイズを 700～1400 バイトの範囲で指定します。 host {IP-ADDRESS | IPV6-ADDRESS}（省略可能）：sFlow コレクターの IPv4 アドレスまたは IPv6 アドレスを指定します。 udp-port PORT（省略可能）：sFlow コレクターとの通信に使用する UDP ポート番号を 1～65535 の範囲で指定します。
デフォルト	レシーバーは未設定 各パラメーターを指定しないでレシーバーを設定した場合： • 有効期限：infinite • sFlow データグラムの最大サイズ：1400 バイト • sFlow コレクターの IPv4 アドレス：0.0.0.0 • UDP ポート番号：6343
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	レシーバーを設定する場合は、最初にレシーバーの所有者名を設定する必要があります。なお、設定済みの所有者名を変更することはできません。設定済みの所有者名を変更するには、一度対象のレシーバーの設定を削除してから再設定します。 有効期限を infinite 以外に設定すると、設定した時点からタイマーがカウントダウンを開始します。タイマーが満了すると、対象のレシーバーID の設定は削除されます。

sflow receiver	
	設定済みのレシーバーID で、所有者名以外の各パラメーターを指定してコマンドを実行した場合は、既存の設定内容を上書きします。 設定済みのレシーバーID で、すべてのパラメーターを指定しないでコマンドを実行しても、何も変更されません。

制限・注意	• デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在するレシーバーを指定して設定した場合、宛先判定にはデフォルトルートよりもデフォルトゲートウェイ設定が優先され、宛先(1)(2)のいずれの場合も SFLOW パケットはマネージメントポートから送信されます。
	  • 宛先(1):デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク
	  • 宛先(2):デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク
	
	• そのため、このような状況では宛先(1)に存在するレシーバーは使用できません。ApresiaNP2500 シリーズでは、このような状況にならないように、VLAN インターフェース経由、もしくはマネージメントポート経由のどちらかのみで管理することを推奨します。
	
	• レシーバーを削除すると、削除したレシーバーID に関連付けられていたサンプラーとポーラーの各パラメーターはデフォルト設定に変更されます。

バージョン	1.08.02

使用例:レシーバーID=1、所有者名を collector1、有効期限を 86,400 秒、sFlow コレクターの IP アドレスを 10.1.1.2 でレシーバーを設定する方法を示します。

```
# configure terminal
(config)# sflow receiver 1 owner collector1 expiry 86400 host 10.1.1.2
(config)#
```

4.11.2 sflow sampler

sflow sampler	
目的	sFlow エージェントのサンプラーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	sflow sampler INSTANCE [receiver ID] [inbound | outbound] [sampling-rate RATE] [max-header-size SIZE] no sflow sampler INSTANCE
Parameter	INSTANCE:サンプラーのインスタンス ID を 1～65535 の範囲で指定します。 receiver ID (省略可能):レシーバーID を 1～4 の範囲で指定します。 inbound (省略可能):受信パケットをサンプリング対象にする場合に指定します。 outbound (省略可能):送信パケットをサンプリング対象にする場合に指定します。 sampling-rate RATE (省略可能):パケットのサンプリングレートを 0～65,536 の範囲で指定します。実際のサンプリングレートは「設定値×256」で動作します。0 指定時はサンプラーが無効になります。(例:sampling-rate 60 に設定した場合、実際のサンプリングレートは 60×256=15360 パケットになる) max-header-size SIZE (省略可能):サンプリングしたパケットからコピーするデー

sflow sampler	
	タの最大バイト数を 18～256 の範囲で指定します。
デフォルト	サンプラーは未設定 各パラメーターを指定しないでサンプラーを設定した場合： • レシーバーID：0 • サンプリング対象：inbound • サンプリングレート：0 • コピーするデータの最大バイト数：128
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	実際のサンプリングレートは「設定値×256」で動作します。 サンプリングレートはシステムが過負荷になった場合に、自動的に低いサンプリングレートに調整されます。なお、変更されたサンプリングレートは自動的には元に戻りません。(例：サンプリングレートの設定値が 20 の場合、20 → 40 → 80 → 160 → 320・・・ と、システム負荷が下がるまで「設定値×2 の累乗数」に自動的に調整される) 指定したレシーバーの有効期限が満了してレシーバーが削除された場合、関連するサンプラーの各パラメーターはデフォルト設定に変更されます。 設定済みのインスタンス ID で、各パラメーターを指定してコマンドを実行した場合は、既存の設定内容を上書きします。 設定済みのインスタンス ID で、すべてのパラメーターを指定しないでコマンドを実行した場合は、そのインスタンス ID の各パラメーターの設定はデフォルト設定になります。 同一ポートに複数の同じ方向のサンプラーを設定する場合、サンプリングレートは、「対象サンプラーの中の最小サンプリングレート設定値×2 の累乗数」の値のみ設定できます。(例：同一ポートに同じ方向のサンプラーを 3 個設定し、その中の最小サンプリングレート設定値が 60 の場合、他の 2 個のサンプラーで設定できるサンプリングレートは 60, 120, 240, 480, 960, ・・・)
制限・注意	• 未設定のレシーバーID を指定して設定できません。 • 同一ポートで、設定済みのサンプラーに関連付けられたレシーバーID を指定して、新たに同じ方向のサンプラーを設定できません。 • コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。
バージョン	1.08.02

使用例：ポート 1/0/1 で、サンプラーのインスタンス ID=1、レシーバーID=1、サンプリング対象を受信パケット、サンプリングレートを 1024（1024×256＝262144 パケット)でサンプラーを設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# sflow sampler 1 receiver 1 inbound sampling-rate 1024
(config-if-port)#
```

4.11.3 sflow poller

sflow poller	
目的	sFlow エージェントのポーラーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	sflow poller INSTANCE [receiver ID] [interval SECONDS] no sflow poller INSTANCE
Parameter	INSTANCE：ポーラーのインスタンス ID を 1～65535 の範囲で指定します。 receiver ID（省略可能）：レシーバーID を 1～4 の範囲で指定します。 interval SECONDS（省略可能）：ポーリング間隔を 0～120 秒の範囲で指定します。0 指定時はポーラーが無効になります。
デフォルト	ポーラーは未設定 各パラメーターを指定しないでポーラーを設定した場合： • レシーバーID：0 • ポーリング間隔：0 秒
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	指定したレシーバーの有効期限が満了してレシーバーが削除された場合、関連するポーラーの各パラメーターはデフォルト設定に変更されます。 設定済みのインスタンス ID で、各パラメーターを指定してコマンドを実行した場合は、既存の設定内容を上書きします。 設定済みのインスタンス ID で、すべてのパラメーターを指定しないでコマンドを実行した場合は、そのインスタンス ID の各パラメーターの設定はデフォルト設定になります。
制限・注意	• 未設定のレシーバーID を指定して設定できません。 • 同一ポートで、設定済みのポーラーに関連付けられたレシーバーID を指定して、新たにポーラーを設定できません。 • コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。
バージョン	1.08.02

使用例：ポート 1/0/1 で、ポーラーのインスタンス ID=1、レシーバーID=1、ポーリング間隔を 60 秒でポーラーを設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# sflow poller 1 receiver 1 interval 60
(config-if-port)#
```

4.11.4 show sflow

show sflow	
目的	sFlow 情報を表示します。
Command	show sflow [agent | receiver | sampler | poller]
Parameter	agent（省略可能）：sFlow エージェントの情報を表示する場合に指定します。 receiver（省略可能）：レシーバーの情報を表示する場合に指定します。

show sflow	
	sampler（省略可能）：サンプラーの情報を表示する場合に指定します。 poller（省略可能）：ポーラーの情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	IPv4 アドレスが設定されている VLAN インターフェースのうち、最小 VLAN ID の VLAN インターフェースの IPv4 アドレスが、sFlow Agent Address になります。 VLAN 1 インターフェースの IPv6 リンクローカルアドレスが sFlow Agent IPv6 Address になります。sFlow Agent IPv6 Address を使用する場合には VLAN 1 インターフェースで IPv6 機能を有効にしてください。
制限・注意	-
バージョン	1.08.02

使用例：すべての sFlow 情報を表示する方法を示します。

```
# show sflow

sFlow Agent Version       : APRESIA Systems, Ltd Inc.;1.00 ...(1)
sFlow Agent Address       : 192.0.2.100 ...(2)
sFlow Agent IPv6 Address  : ...(3)

Receivers Information ...(4)
Index                     : 1 ...(5)
Owner                     : collector1 ...(6)
Expire Time               : 86400 ...(7)
Current Countdown Time    : 86395 ...(8)
Max Datagram Size         : 1400 ...(9)
Address                   : 10.1.1.2 ...(10)
Port                      : 6343 ...(11)
Datagram Version          : 5 ...(12)

Index                     : 2
～～省略～～

Index                     : 4
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Samplers Information ...(13)
(14)         (15)      (16)      (17)      (18)         (19)          (20)
Interface    Instance  Receiver  Mode      Admin Rate   Active Rate   Max Header Size
-----------  --------  --------  --------  ----------   -----------   ---------------
Port1/0/1           1         1 inbound         1024          1024               128
Port1/0/5         105         1 outbound        1024          1024               128

Pollers Information ...(21)
(22)         (23)      (24)      (25)
Interface    Instance  Receiver  Interval
-----------  --------  --------  --------
Port1/0/1           1         1        60
Port1/0/5         105         1        60
```

項番	説明
(1)	sFlow エージェントの情報（組織、sFlow ソフトウェアのリビジョン）を表示します。
(2)	sFlow エージェントの IPv4 アドレスを表示します。
(3)	sFlow エージェントの IPv6 アドレスを表示します。
(4)	sFlow レシーバーの情報を表示します。
(5)	sFlow レシーバーのインデックスを表示します。
(6)	所有者名を表示します。
(7)	レシーバーの有効期限を表示します。
(8)	サンプリングおよびポーリングが停止するまでの時間（秒）を表示します。
(9)	1 つの sFlow データグラムの最大バイト数を表示します。
(10)	sFlow コレクターの IPv4 アドレスまたは IPv6 アドレスを表示します。
(11)	sFlow コレクターとの通信に使用する UDP ポート番号を表示します。
(12)	sFlow データグラムのバージョンを表示します。
(13)	sFlow エージェントのサンプラーの情報を表示します。
(14)	サンプラーを設定したポート番号を表示します。
(15)	サンプラーのインデックスを表示します。
(16)	サンプラー用のレシーバーのインデックスを表示します。
(17)	サンプリング対象（inbound：受信パケット／outbound：送信パケット）を表示します。
(18)	設定したサンプリングレートを表示します。実際のサンプリングレートは「設定値(表示されている値)×256」パケットで動作します。
(19)	アクティブなサンプリングレートを表示します。実際のサンプリングレートは「表示されている値×256」パケットで動作します。
(20)	サンプリングしたパケットからコピーするデータの最大バイト数を表示します。
(21)	sFlow エージェントのポーラーの情報を表示します。
(22)	ポーラーを設定したポート番号を表示します。
(23)	ポーラーのインデックスを表示します。
(24)	ポーラー用のレシーバーのインデックスを表示します。
(25)	ポーリング間隔を表示します。

使用例：sFlow エージェントの情報を表示する方法を示します。

```
# show sflow agent

sFlow Agent Version        : APRESIA Systems, Ltd Inc.;1.00 ...(1)
sFlow Agent Address        : 192.0.2.100 ...(2)
sFlow Agent IPv6 Address   : ...(3)
```

項番	説明
(1)	sFlow エージェントの情報（組織、sFlow ソフトウェアのリビジョン）を表示します。
(2)	sFlow エージェントの IPv4 アドレスを表示します。
(3)	sFlow エージェントの IPv6 アドレスを表示します。

使用例：sFlow エージェントのレシーバーを表示する方法を示します。

```
# show sflow receiver

Receivers Information
Index                       : 1 ...(1)
Owner                       : collector1 ...(2)
Expire Time                 : 86400 ...(3)
Current Countdown Time      : 86390 ...(4)
Max Datagram Size           : 1400 ...(5)
Address                     : 10.1.1.2 ...(6)
Port                        : 6343 ...(7)
Datagram Version            : 5 ...(8)

Index                       : 2
～～省略～～
```

項番	説明
(1)	sFlow レシーバーのインデックスを表示します。
(2)	所有者名を表示します。
(3)	レシーバーの有効期限を表示します。
(4)	サンプリングおよびポーリングが停止するまでの時間（秒）を表示します。
(5)	1 つの sFlow データグラムの最大バイト数を表示します。
(6)	sFlow コレクターの IPv4 アドレスまたは IPv6 アドレスを表示します。
(7)	sFlow コレクターとの通信に使用する UDP ポート番号を表示します。
(8)	sFlow データグラムのバージョンを表示します。

使用例：sFlow エージェントのサンプラーを表示する方法を示します。

```
# show sflow sampler

Samplers Information
 (1)          (2)       (3)       (4)       (5)          (6)          (7)
Interface    Instance Receiver Mode     Admin Rate  Active Rate  Max Header Size
---------- -------- -------- -------- ----------  -----------  ---------------
Port1/0/1           1        1 inbound        1024         1024              128
Port1/0/5         105        1 outbound       1024         1024              128
```

項番	説明
(1)	サンプラーを設定したポート番号を表示します。
(2)	サンプラーのインデックスを表示します。
(3)	サンプラー用のレシーバーのインデックスを表示します。
(4)	サンプリング対象（inbound：受信パケット／outbound：送信パケット）を表示します。
(5)	設定したサンプリングレートを表示します。実際のサンプリングレートは「設定値(表示されている値)×256」パケットで動作します。
(6)	アクティブなサンプリングレートを表示します。実際のサンプリングレートは「表示されている値×256」パケットで動作します。
(7)	サンプリングしたパケットからコピーするデータの最大バイト数を表示します。

使用例：sFlow エージェントのポーラーを表示する方法を示します。

```
# show sflow poller

Pollers Information
(1)           (2)        (3)        (4)
Interface     Instance   Receiver   Interval
------------  --------   --------   --------
Port1/0/1            1          1         60
Port1/0/5          105          1         60
```

項番	説明
(1)	ポーラーを設定したポート番号を表示します。
(2)	ポーラーのインデックスを表示します。
(3)	ポーラー用のレシーバーのインデックスを表示します。
(4)	ポーリング間隔を表示します。

4.12 SNMP コマンド

SNMP（Simple Network Management Protocol）関連の設定コマンドは以下のとおりです。

- snmp-server
- snmp-server name
- snmp-server location
- snmp-server contact
- snmp-server service-port
- snmp-server response broadcast-request
- snmp-server community
- snmp-server host
- snmp-server enable traps
- snmp-server enable traps snmp
- snmp-server enable traps environment
- snmp-server source-interface traps
- snmp-server trap-sending disable
- snmp trap link-status
- snmp-server user
- snmp-server group
- snmp-server view
- snmp-server engineID local

SNMP（Simple Network Management Protocol）関連の show コマンドは以下のとおりです。

- show snmp-server
- show snmp community
- show snmp host
- show snmp-server traps
- show snmp-server trap-sending
- show snmp trap link-status
- show snmp user
- show snmp group
- show snmp view
- show snmp engineID

4.12.1 snmp-server

snmp-server	
目的	SNMP エージェントを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server no snmp-server
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12

snmp-server	
ガイドライン	SNMP マネージャーは SNMP リクエストを SNMP エージェントに送信し、SNMP エージェントから SNMP レスポンスと通知を受信することで、SNMP エージェントを管理します。本装置を SNMP で管理する場合は、本コマンドで SNMP エージェントを有効にします。
制限・注意	• デフォルトで設定されている Read/Write 権限の SNMP コミュニティー名「private」が存在する状態で本コマンドを設定すると、SNMP コミュニティー名の変更を促す警告メッセージが表示されます。
バージョン	1.08.02

使用例：SNMP エージェントを有効にする方法を示します。

```
# configure terminal
(config)# snmp-server
(config)#
```

4.12.2 snmp-server name

snmp-server name	
目的	システム名（sysName）を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	snmp-server name SYSTEM-NAME no snmp-server name
Parameter	SYSTEM-NAME：システム名（sysName）を最大 64 文字で指定します。英数字とハイフンのみ使用可能です。ただし、先頭と末尾は英数字のみ指定可能です。
デフォルト	Switch
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	prompt %h を設定すると、本コマンドで設定した文字列がプロンプト文字列になります。プロンプト文字列は 15 文字までしか表示されないため、prompt %h を使用する場合は、本コマンドを 15 文字以下で設定することを推奨します。
制限・注意	-
バージョン	1.08.02

使用例：システム名（sysName）を「SiteA-switch」に設定する方法を示します。

```
# configure terminal
(config)# snmp-server name SiteA-switch
(config)#
```

4.12.3 snmp-server location

snmp-server location	
目的	システムロケーション（sysLocation）を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	snmp-server location SYSTEM-LOCATION no snmp-server location
Parameter	SYSTEM-LOCATION：システムロケーション（sysLocation）を最大 255 文字で指定します。ASCII コードの印字可能な文字のうち、? を除いた文字を使用可能です。

snmp-server location	
	スペースも使用できます。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：システムロケーション（sysLocation）を「HQ 15F」に設定する方法を示します。

```
# configure terminal
(config)# snmp-server location HQ 15F
(config)#
```

4.12.4 snmp-server contact

snmp-server contact	
目的	システムコンタクト（sysContact）を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	snmp-server contact SYSTEM-CONTACT no snmp-server contact
Parameter	SYSTEM-CONTACT：システムコンタクト（sysContact）を最大 255 文字で指定します。ASCII コードの印字可能な文字のうち、？ を除いた文字を使用可能です。スペースも使用できます。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：システムコンタクト（sysContact）を「MIS Department II」に設定する方法を示します。

```
# configure terminal
(config)# snmp-server contact MIS Department II
(config)#
```

4.12.5 snmp-server service-port

snmp-server service-port	
目的	SNMP で使用する UDP ポート番号を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	snmp-server service-port UDP-PORT no snmp-server service-port
Parameter	UDP-PORT：UDP ポート番号を 1～65535 の範囲で指定します。番号によっては、他のプロトコルと競合する場合があります。

snmp-server service-port	
デフォルト	161
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 162(snmptrap), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • ip ssh service-port • snmp-server host • web-authentication http-port • web-authentication https-port • web-authentication redirect proxy-port • web-authentication snooping proxy-port • web-deny-notify http-port • web-deny-notify https-port • radius-server host • tacacs-server host
バージョン	1.08.02 1.12.01：特定番号指定時の禁則追加

使用例：SNMP で使用する UDP ポート番号を 50000 に設定する方法を示します。

```
# configure terminal
(config)# snmp-server service-port 50000
(config)#
```

4.12.6 snmp-server response broadcast-request

snmp-server response broadcast-request	
目的	ブロードキャストアドレス宛ての SNMP GetRequest パケットに対する応答を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server response broadcast-request no snmp-server response broadcast-request
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	NMS ツールはネットワーク上の装置を検知するために、ブロードキャストアドレス宛ての SNMP GetRequest パケットを送信して確認する場合があります。NMS ツールのその機能をサポートするには、本コマンドでブロードキャストアドレス宛ての SNMP GetRequest パケットに対する応答を有効にします。

snmp-server response broadcast-request	
制限・注意	-
バージョン	1.08.02

使用例：ブロードキャストアドレス宛ての SNMP GetRequest パケットに対する応答を有効にする方法を示します。

```
# configure terminal
(config)# snmp-server response broadcast-request
(config)#
```

4.12.7 snmp-server community

snmp-server community	
目的	SNMP コミュニティー名を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	snmp-server community [0 | 7] STRING [view NAME] [ro | rw] [access ACL-NAME] no snmp-server community [0 | 7] STRING
Parameter	[0 | 7]（省略可能）：後に続く SNMP コミュニティー名の文字列の形式を明示する場合に指定します。0 の場合は平文（最大 32 文字）を、7 の場合は暗号化された形式（最大 67 文字）を意味します。省略した場合は、平文で入力します。 STRING：平文で入力する場合は、SNMP コミュニティー名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 view NAME（省略可能）：関連付ける SNMP ビュー名を指定します。省略した場合は、デフォルトで設定されている「CommunityView」が適用されます。 [ro | rw]（省略可能）：MIB へのアクセス権を ro（read-only）、または rw（read-write）で指定します。省略した場合は ro が適用されます。 access ACL-NAME（省略可能）：標準 IP アクセスリスト、または標準 IPv6 アクセスリストを指定します。対象の SNMP コミュニティー名でのアクセスを許可または拒否する IPv4/IPv6 アドレスを、「送信元 IP アドレス」条件または「送信元 IPv6 アドレス」条件で指定します。
デフォルト	SNMP コミュニティー名（SNMP ビュー名, アクセス権） public（CommunityView, read-only） private（CommunityView, read-write）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドは、SNMPv1 または SNMPv2c の管理に必要な SNMP コミュニティー名を設定する簡単な方法を提供します。 本コマンドで SNMP コミュニティー名を設定すると、2 つの snmp-server group 設定が自動的に作成されます。それぞれ SNMPv1 と SNMPv2c に対応し、SNMP コミュニティー名が SNMP グループ名になります。 ro パラメーターを指定した場合、指定した view パラメーター（未指定時は CommunityView）が、自動的に作成される snmp-server group 設定の read-view, notify-view に反映されます。rw パラメーターを指定した場合、指定した view パラ

snmp-server community	
	メーター（未指定時は CommunityView）が、自動的に作成される snmp-server group 設定の read-view, write-view, notify-view に反映されます。 access パラメーターで指定するアクセスリストでは、「宛先 IP アドレス」条件または「宛先 IPv6 アドレス」条件は any で設定してください。any 以外で設定した場合は、そのルールは無効になります。また、指定したアクセスリストのどのルールにもマッチしない場合は、アクセスは拒否されます。 access パラメーターを指定した場合、対応する 2 つの snmp-server group 設定にも反映されます。 本コマンドの設定を削除すると、対応する 2 つの snmp-server group 設定も削除されます。 service user-account encryption でパスワード暗号化機能を有効にすると、SNMP コミュニティー名が暗号化されます。
制限・注意	• SNMP コミュニティー名は、デフォルトで設定済みの SNMP コミュニティー名（public, private）を含めて、最大 10 個設定できます。 • 本コマンドを設定した場合に自動的に作成される 2 つの snmp-server group 設定を、変更したり削除することはサポートしていません。 • 説明に記載されている種別以外のアクセスリストを指定して使用できません。 • 本コマンドを設定した場合には SNMPv1 と SNMPv2c の両方の SNMP コミュニティー名が設定されます。一方のみを無効にすることはできません。 • 本設定の access パラメーターで指定する標準 IP アクセスリスト、または標準 IPv6 アクセスリストでは、装置のハードウェアリソースを使用しません。
バージョン	1.08.02

使用例：SNMP コミュニティー名「test-com1」、SNMP ビュー名「interfacesMibView」（事前に設定済み想定）、アクセス権「rw（read-write）」で SNMP コミュニティー名を設定する方法を示します。

```
# configure terminal
(config)# snmp-server community test-com1 view interfacesMibView rw
(config)#
```

使用例：以下の内容で SNMP によるアクセス制限を有効にした SNMP コミュニティー名「test-com2」を、SNMP ビュー名の指定は省略、アクセス権「ro（read-only）」、アクセス制限用の標準 IP アクセスリスト名は「snmp-permit-list」で設定する方法を示します。

- 192.0.2.0/24 からの SNMP アクセスを許可
- 10.0.0.100/32 からの SNMP アクセスを許可
- それ以外からの SNMP アクセスを拒否

```
# configure terminal
(config)# ip access-list snmp-permit-list
(config-ip-acl)# permit 192.0.2.0 0.0.0.255
(config-ip-acl)# permit host 10.0.0.100
(config-ip-acl)# exit
(config)#
(config)# snmp-server community test-com2 ro access snmp-permit-list
(config)#
```

使用例：以下の内容で SNMP によるアクセス制限を有効にした SNMP コミュニティー名「test-com3」を、SNMP ビュー名の指定は省略、アクセス権「ro（read-only)」、アクセス制限用の標準 IP アクセスリスト名は「SNMP-LIST」で設定する方法を示します。

- ルール 10：192.0.2.100/32 からの SNMP アクセスを許可
- ルール 20：192.0.2.100 以外の 192.0.2.0/24 からの SNMP アクセスを拒否
- ルール 100：それ以外からの SNMP アクセスを許可

```
# configure terminal
(config)# ip access-list SNMP-LIST
(config-ip-acl)# 10 permit host 192.0.2.100
(config-ip-acl)# 20 deny 192.0.2.0 0.0.0.255
(config-ip-acl)# 100 permit any
(config-ip-acl)# exit
(config)#
(config)# snmp-server community test-com3 ro access SNMP-LIST
(config)#
```

4.12.8 snmp-server host

snmp-server host	
目的	SNMP トラップの宛先を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	**snmp-server host** {IP-ADDRESS | IPV6-ADDRESS} [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] [**0** | **7**] COMMUNITY [**port** UDP-PORT] **no snmp-server host** {IP-ADDRESS | IPV6-ADDRESS}

Parameter	IP-ADDRESS：SNMP トラップの宛先 IPv4 アドレスを指定します。
	IPV6-ADDRESS：SNMP トラップの宛先 IPv6 アドレスを指定します。
	version（省略可能）：SNMP トラップのバージョンを指定します。省略した場合は SNMPv1 が適用されます。
	• 1：SNMPv1 にする場合に指定します。
	• 2c：SNMPv2c にする場合に指定します。
	• 3 {auth | noauth | priv}：SNMPv3 にする場合に指定します。
	  • auth：パケットを認証し、暗号化しない場合に指定します。
	  • noauth：パケットの認証も暗号化もしない場合に指定します。
	  • priv：パケットを認証し、暗号化する場合に指定します。
	[0 | 7]（省略可能）：後に続く SNMP コミュニティー名またはユーザー名の文字列の形式を明示する場合に指定します。0 の場合は平文（最大 32 文字）を、7 の場合は暗号化された形式（最大 67 文字）を意味します。省略した場合は、平文で入力します。
	COMMUNITY：SNMP トラップで使用する SNMP コミュニティー名、または SNMP ユーザー名を指定します。バージョンが SNMPv1/SNMPv2c の場合は SNMP コミュニティー名を指定します。バージョンが SNMPv3 の場合は SNMP ユーザー名を指定します。
	port UDP-PORT（省略可能）：UDP ポート番号を 1～65535 の範囲で指定します。省略した場合は UDP ポート番号 162 が適用されます。番号によっては、他のプロトコルと競合する場合があります。

デフォルト	設定なし
モード	グローバル設定モード
特権レベル	レベル：12

snmp-server host	
ガイドライン	SNMP トラップのバージョンを SNMPv1 および SNMPv2c で指定する場合、指定する SNMP コミュニティー名をあらかじめ snmp-server community コマンドで設定しておく必要があります。 SNMP トラップのバージョンを SNMPv3 で指定する場合、指定するユーザー名をあらかじめ snmp-server user コマンドで設定しておく必要があります。 SNMP トラップの送信では、指定した SNMP コミュニティー名またはユーザー名に関連付けられた notify-view がチェックされます。SNMP トラップに含まれる variable-bindings フィールドの OID が notify-view に含まれない場合は、SNMP トラップは送信されません。 service user-account encryption でパスワード暗号化機能を有効にすると、SNMP コミュニティー名またはユーザー名が暗号化されます。

制限・注意	• SNMP トラップの宛先は、最大 10 個設定できます。
	
	• port パラメーターをデフォルト値(162)以外に指定する場合は、以下に示す TCP/UDP ポート番号は指定しないでください。
	  • 21(ftp), 22(ssh), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 161(snmp), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022
	  • 以下コマンドで指定した TCP/UDP ポート番号
	  • ip telnet service-port
	  • ip ssh service-port
	  • snmp-server service-port
	  • web-authentication http-port
	  • web-authentication https-port
	  • web-authentication redirect proxy-port
	  • web-authentication snooping proxy-port
	  • web-deny-notify http-port
	  • web-deny-notify https-port
	  • radius-server host
	  • tacacs-server host
	
	• デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在する SNMP マネージャーを指定して設定した場合、宛先判定にはデフォルトルートよりもデフォルトゲートウェイ設定が優先され、宛先(1)(2)のいずれの場合も SNMP トラップはマネージメントポートから送信されます。
	  • 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク
	  • 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク
	
	• VLAN インターフェース経由でのみ管理する場合は、送信元 IP アドレス設定(snmp-server source-interface traps)を VLAN インターフェース指定で設定することにより、このような状況でも宛先(1)への SNMP トラップが VLAN インターフェースから送信されるようになりますが、この設定をすると宛先(2)の場合も VLAN インターフェースから送信されるようになることに注意してください。

snmp-server host	
バージョン	1.08.02

使用例：宛先 IPv4 アドレス「192.0.2.100」、バージョンを SNMPv1、SNMP コミュニティー名「comaccess」で SNMP トラップの宛先を設定する方法を示します。

```
# configure terminal
(config)# snmp-server community comaccess rw
(config)# snmp-server host 192.0.2.100 version 1 comaccess
(config)#
```

4.12.9 snmp-server enable traps

snmp-server enable traps	
目的	SNMP トラップのグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps no snmp-server enable traps
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SNMP トラップのグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps
(config)#
```

4.12.10 snmp-server enable traps snmp

snmp-server enable traps snmp	
目的	SNMP 標準トラップの送信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps snmp [authentication | linkup | linkdown | coldstart | warmstart] no snmp-server enable traps snmp [authentication | linkup | linkdown | coldstart | warmstart]
Parameter	authentication（省略可能）：SNMP 認証失敗通知を有効にする場合に指定します。SNMPv1/SNMPv2c では不適切な SNMP コミュニティー名の場合に認証が失敗します。SNMPv3 では不適切な SHA/MD5 認証鍵の場合に認証が失敗します。 linkup（省略可能）：リンクアップ通知を有効にする場合に指定します。 linkdown（省略可能）：リンクダウン通知を有効にする場合に指定します。 coldstart（省略可能）：コールドスタート通知を有効にする場合に指定します。

snmp-server enable traps snmp	
	warmstart（省略可能）：ウォームスタート通知を有効にする場合に指定します。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	パラメーターを指定しない場合は、すべてのパラメーターが対象になります。 本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。
制限・注意	• snmp-server enable traps snmp warmstart と snmp-server enable traps snmp coldstart は、構成情報では BASIC 関連（ラベル# BASIC）で表示されます。
バージョン	1.08.02

使用例：SNMP 標準トラップの送信を有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps snmp
(config)#
```

4.12.11 snmp-server enable traps environment

snmp-server enable traps environment	
目的	環境モニタリング通知の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps environment [fan] [power] [temperature] no snmp-server enable traps environment [fan | power | temperature]
Parameter	fan（省略可能）：ファン関連の通知を有効にする場合に指定します。 power（省略可能）：電源関連の通知を有効にする場合に指定します。 temperature（省略可能）：温度関連の通知を有効にする場合に指定します。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	パラメーターを指定しない場合は、すべてのパラメーターが対象になります。 本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。
制限・注意	• 本設定は構成情報ではデバイス関連（ラベル# DEVICE）で表示されます。
バージョン	1.08.02

使用例：環境モニタリング通知の SNMP トラップを有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps environment
(config)#
```

4.12.12 snmp-server source-interface traps

snmp-server source-interface traps	
目的	SNMP トラップの送信元 IP アドレスとして使用するインターフェースを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	snmp-server source-interface traps IF-ID no snmp-server source-interface traps
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定
デフォルト	最も近いインターフェースの IP アドレスを使用
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• マネージメントポート経由で管理する場合は、vlan パラメーターを指定して本コマンドを設定しないでください。 • VLAN インターフェース経由で管理する場合は、mgmt パラメーターを指定して本コマンドを設定しないでください。
バージョン	1.08.02

使用例：SNMP トラップの送信元 IP アドレスとして、VLAN 1 インターフェースの IP アドレスを設定する方法を示します。

```
# configure terminal
(config)# snmp-server source-interface traps vlan 1
(config)#
```

4.12.13 snmp-server trap-sending disable

snmp-server trap-sending disable	
目的	設定したポートからの自装置の SNMP トラップ送信を禁止します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	snmp-server trap-sending disable no snmp-server trap-sending disable
Parameter	なし
デフォルト	自装置の SNMP トラップ送信は有効（no snmp-server trap-sending disable）
モード	インターフェース設定モード（port, range）
特権レベル	レベル：12
ガイドライン	本コマンドを設定したポートからは、自装置の SNMP トラップ送信が禁止されます。他のシステムが出力した SNMP トラップを中継する場合は対象外で禁止されません。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/8 からの自装置の SNMP トラップ送信を禁止する方法を示します。

```
# configure terminal
```

```
(config)# interface port 1/0/8
(config-if-port)# snmp-server trap-sending disable
(config-if-port)#
```

4.12.14 snmp trap link-status

snmp trap link-status	
目的	対象ポートのリンクアップ・リンクダウンの SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp trap link-status no snmp trap link-status
Parameter	なし
デフォルト	リンクアップ・リンクダウンの SNMP トラップは有効（snmp trap link-status）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	本コマンドはデフォルトで有効です。対象ポートのリンクアップ・リンクダウンの SNMP トラップを無効にするには、no snmp trap link-status を設定します。
制限・注意	• 対象ポートのリンクアップ・リンクダウンの SNMP トラップを有効にする場合は、snmp-server enable traps snmp linkup コマンドと snmp-server enable traps snmp linkdown コマンドも有効にする必要があります。
バージョン	1.08.02

使用例：ポート 1/0/1 でリンクアップ・リンクダウンの SNMP トラップを無効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# no snmp trap link-status
(config-if-port)#
```

4.12.15 snmp-server user

snmp-server user	
目的	SNMP ユーザーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	snmp-server user NAME [0 | 7] GROUP v3 [encrypted] [auth {md5 | sha} AUTH-PASS [priv PRIV-PASS]] [access ACL-NAME] no snmp-server user NAME [0 | 7] GROUP v3
Parameter	NAME：ユーザー名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 [0 | 7]（省略可能）：後に続く SNMP グループ名の文字列の形式を明示する場合に指定します。0 の場合は平文（最大 32 文字）を、7 の場合は暗号化された形式（最大 67 文字）を意味します。省略した場合は、平文で入力します。 GROUP：対象の SNMP ユーザーが所属する SNMP グループ名を指定します。 v3：SNMPv3 を使用するユーザーを設定する場合に指定します。 encrypted（省略可能）：後に続く認証パスワード／暗号化パスワードが暗号化された形式であることを示します。 auth md5（省略可能）：HMAC-MD5-96 認証を使用する場合に指定します。

snmp-server user	
	auth sha（省略可能）：HMAC-SHA-96 認証を使用する場合に指定します。 AUTH-PASS：認証に使用するパスワードを指定します。md5 指定時は 8～16 文字の範囲の平文で指定します。sha 指定時は 8～20 文字の範囲の平文で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 priv PRIV-PASS（省略可能）：パケットの暗号化パスワードを、8～16 文字の範囲の平文で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。秘密鍵はパスワードに基づいて生成されます。暗号化方式は DES（Data Encryption Standard）のみ使用可能です。 access ACL-NAME（省略可能）：標準 IP アクセスリスト、または標準 IPv6 アクセスリストを指定します。対象のユーザー名でのアクセスを許可または拒否する IPv4/IPv6 アドレスを、「送信元 IP アドレス」条件または「送信元 IPv6 アドレス」条件で指定します。
デフォルト	ユーザー名：initial、グループ名：initial
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	SNMPv3 を「認証なし」以外で使用する場合は、SNMP ユーザーを設定する前にユニークな SNMP エンジン ID を明示的に設定してください。 SNMPv3 を「認証なし」以外で使用していて運用中に SNMP エンジン ID を変更すると、既存 SNMP ユーザー設定が使用できなくなります。その場合は、既存 SNMP ユーザー設定を削除して、再設定してください。 本コマンドを認証パスワード(AUTH-PASS)、または暗号化パスワード(PRIV-PASS)を指定して設定した場合は、構成情報では encrypted パラメーターが指定された形式で表示されます。認証パスワードは md5 指定時は 16 オクテットの 16 進値、sha 指定時は 20 オクテットの 16 進値で表示されます。暗号化パスワードは 16 オクテットの 16 進値で表示されます。 access パラメーターで指定するアクセスリストでは、「宛先 IP アドレス」条件または「宛先 IPv6 アドレス」条件は any で設定してください。any 以外で設定した場合は、そのルールは無効になります。また、指定したアクセスリストのどのルールにもマッチしない場合は、アクセスは拒否されます。 service user-account encryption でパスワード暗号化機能を有効にすると、SNMP グループ名が暗号化されます。
制限・注意	• SNMP ユーザーは、デフォルトで設定済みの SNMP ユーザー名（initial）を含めて、最大 10 個設定できます。 • snmp-server host コマンドで指定済みの SNMP ユーザーは、削除できません。 • snmp-server user コマンドで v1 もしくは v2c パラメーターを指定することはサポートしていません。 • 説明に記載されている種別以外のアクセスリストを指定して使用できません。 • SNMP ユーザー設定のパスワードは、構成情報では encrypted パラメーターが指定された形式で表示されますが、この際のパスワード暗号化には SNMP エンジン ID の文字列も関係しています。SNMP エンジン ID をデフォルト設定のまま使用すると、故障などで装置を交換した場合に SNMP エンジン ID が変更されることになり、既存 SNMP ユーザー設定の削除・再設定が必要になります。これを避けるために、明示的にユニークな SNMP エンジン ID を設定して使用してください。

snmp-server user	
	• 本設定の access パラメーターで指定する標準 IP アクセスリスト、または標準 IPv6 アクセスリストでは、装置のハードウェアリソースを使用しません。
バージョン	1.08.02

使用例：SNMP ユーザー名「user1」、SNMP グループ名「test-group」（事前に設定済み想定）、バージョンを SNMPv3、md5 指定、認証パスワード「authpassword」、暗号化パスワード「privpassword」で SNMP ユーザーを設定する方法を示します。

```
# configure terminal
(config)# snmp-server user user1 test-group v3 auth md5 authpassword priv privpassword
(config)#
```

使用例：以下の内容で SNMP によるアクセス制限を有効にした SNMP ユーザー名「user2」を、SNMP グループ名「initial」（デフォルトで設定済み）、バージョンを SNMPv3、アクセス制限用の標準 IP アクセスリスト名は「snmp-permit-list」で設定する方法を示します。

- 192.0.2.0/24 からの SNMP アクセスを許可
- 10.0.0.100/32 からの SNMP アクセスを許可
- それ以外からの SNMP アクセスを拒否

```
# configure terminal
(config)# ip access-list snmp-permit-list
(config-ip-acl)# permit 192.0.2.0 0.0.0.255
(config-ip-acl)# permit host 10.0.0.100
(config-ip-acl)# exit
(config)#
(config)# snmp-server user user2 initial v3 access snmp-permit-list
(config)#
```

使用例：以下の内容で SNMP によるアクセス制限を有効にした SNMP ユーザー名「user3」を、SNMP グループ名「initial」（デフォルトで設定済み）、バージョンを SNMPv3、アクセス制限用の標準 IP アクセスリスト名は「SNMP-LIST」で設定する方法を示します。

- ルール 10：192.0.2.100/32 からの SNMP アクセスを許可
- ルール 20：192.0.2.100 以外の 192.0.2.0/24 からの SNMP アクセスを拒否
- ルール 100：それ以外からの SNMP アクセスを許可

```
# configure terminal
(config)# ip access-list SNMP-LIST
(config-ip-acl)# 10 permit host 192.0.2.100
(config-ip-acl)# 20 deny 192.0.2.0 0.0.0.255
(config-ip-acl)# 100 permit any
(config-ip-acl)# exit
(config)#
(config)# snmp-server user user3 initial v3 access SNMP-LIST
(config)#
```

4.12.16 snmp-server group

snmp-server group	
目的	SNMP グループを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	snmp-server group [0 | 7] NAME {v1 | v2c | v3 {auth | noauth | priv}} [read READ-VIEW] [write WRITE-VIEW] [notify NOTIFY-VIEW] [access ACL-NAME]

snmp-server group	
	no snmp-server group [0	7] NAME {v1	v2c	v3 {auth	noauth	priv}}
Parameter	[0	7]（省略可能）：後に続く SNMP グループ名の文字列の形式を明示する場合に指定します。0 の場合は平文（最大 32 文字）を、7 の場合は暗号化された形式（最大 67 文字）を意味します。省略した場合は、平文で入力します。 NAME：平文で入力する場合は、SNMP グループ名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 v1：SNMPv1 セキュリティーモデルを使用する場合に指定します。 v2c：SNMPv2c セキュリティーモデルを使用する場合に指定します。 v3 {auth	noauth	priv}：SNMPv3 セキュリティーモデルを使用する場合に指定します。 • auth：パケットを認証し、暗号化しない場合に指定します。 • noauth：パケットの認証も暗号化もしない場合に指定します。 • priv：パケットを認証し、暗号化する場合に指定します。 read READ-VIEW（省略可能）：read-view として使用する SNMP ビュー名を指定します。 write WRITE-VIEW（省略可能）：write-view として使用する SNMP ビュー名を指定します。 notify NOTIFY-VIEW（省略可能）：notify-view として使用する SNMP ビュー名を指定します。 access ACL-NAME（省略可能）：グループと関連付ける標準 IP アクセスリスト、または標準 IPv6 アクセスリストを指定します。
デフォルト	SNMP グループ名（バージョン, 認証, read-view, write-view, notify-view） public（SNMPv1, N/A, CommunityView, N/A, CommunityView） public（SNMPv2c, N/A, CommunityView, N/A, CommunityView） private（SNMPv1, N/A, CommunityView, CommunityView, CommunityView） private（SNMPv2c, N/A, CommunityView, CommunityView, CommunityView） initial（SNMPv3, noauth, restricted, N/A, restricted）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	SNMP グループは、セキュリティーモデル（バージョン）、read-view、write-view、nofity-view を指定して、グループユーザーへ許可する内容を定義します。 同じ SNMP グループ名をセキュリティーモデル SNMPv1、SNMPv2c、SNMPv3 で同時に設定することができます。 設定済みの SNMP グループに対して、関連付けた SNMP ビューなどを変更することはできません。変更する場合は、いったん SNMP グループを削除してから再設定してください。 read-view は、読み取りを許可する MIB オブジェクトを定義します。read-view を指定しない場合、対象のグループユーザーではすべての MIB オブジェクトの読み取りができません。 write-view は、書き込みを許可する MIB オブジェクトを定義します。write-view を指定しない場合、対象のグループユーザーではすべての MIB オブジェクトに書き込

snmp-server group	
	みができません。 notify-view は、SNMP トラップに含めることを許可する MIB オブジェクトを定義します。notify-view を指定しない場合、対象のグループユーザーでは SNMP トラップの通知はできません。 service user-account encryption でパスワード暗号化機能を有効にすると、SNMP グループ名が暗号化されます。
制限・注意	• snmp-server community コマンドを設定した場合に自動的に作成される 2 つの SNMP グループ設定を、変更したり削除することはサポートしていません。 • 説明に記載されている種別以外のアクセスリストを指定して使用できません。 • 本設定の access パラメーターで指定する標準 IP アクセスリスト、または標準 IPv6 アクセスリストでは、装置のハードウェアリソースを使用しません。
バージョン	1.08.02

使用例：SNMP グループ名「guestgroup」、セキュリティーモデル「v3 auth」、read-view「CommunityView」、write-view「CommunityView」で SNMP グループを設定する方法を示します。

```
# configure terminal
(config)# snmp-server group guestgroup v3 auth read CommunityView write CommunityView
(config)#
```

4.12.17 snmp-server view

snmp-server view	
目的	SNMP ビューを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	snmp-server view NAME OID {included | excluded} no snmp-server view NAME
Parameter	NAME：SNMP ビュー名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 OID：SNMP ビューに含める、または除外する OID ツリーのオブジェクト識別子を指定します。 • included：指定した OID ツリーを含める場合に指定します。 • excluded：指定した OID ツリーを除外する場合に指定します。
デフォルト	SNMP ビュー名 (OID, タイプ) CommunityView (1, included) CommunityView (1.3.6.1.6.3, excluded) CommunityView (1.3.6.1.6.3.1, included) 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)
モード	グローバル設定モード
特権レベル	レベル：12

snmp-server view	
ガイドライン	SNMP ビューは、snmp-server group コマンドと snmp-server community コマンドで使用します。
制限・注意	-
バージョン	1.08.02

使用例：SNMP ビュー名「interfacesMibView」、SNMP ビューに含める OID ツリーのオブジェクト識別子「1.3.6.1.2.1.2」で SNMP ビューを設定する方法を示します。

```
# configure terminal
(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
(config)#
```

4.12.18 snmp-server engineID local

snmp-server engineID local	
目的	SNMP エンジン ID を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	snmp-server engineID local STRING no snmp-server engineID local
Parameter	STRING：エンジン ID を最大 24 文字（16 進表記）で指定します。
デフォルト	"8000011603"＋装置 MAC アドレス（12 文字）＋"00"の 24 文字
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	SNMPv3 を「認証なし」以外で使用する場合は、SNMP ユーザーを設定する前にユニークな SNMP エンジン ID を明示的に設定してください。 SNMPv3 を「認証なし」以外で使用していて運用中に SNMP エンジン ID を変更すると、既存 SNMP ユーザー設定が使用できなくなります。その場合は、既存 SNMP ユーザー設定を削除して、再設定してください。 SNMP エンジン ID は、装置を識別する一意の 16 進文字列です。24 文字より少ない 16 進文字列を指定すると、24 文字になるまで末尾が 0 で埋められます。
制限・注意	• SNMP ユーザー設定のパスワードは、構成情報では encrypted パラメーターが指定された形式で表示されますが、この際のパスワード暗号化には SNMP エンジン ID の文字列も関係しています。 • SNMP エンジン ID をデフォルト設定のまま使用すると、故障などで装置を交換した場合に SNMP エンジン ID が変更されることになり、既存 SNMP ユーザー設定の削除・再設定が必要になります。これを避けるために、明示的にユニークな SNMP エンジン ID を設定して使用してください。
バージョン	1.08.02

使用例：SNMP エンジン ID を 800001160501020304050607 に設定する方法を示します。

```
# configure terminal
(config)# snmp-server engineID local 800001160501020304050607
(config)#
```

4.12.19 show snmp-server

show snmp-server	
目的	SNMP エージェントの設定を表示します。
Command	show snmp-server
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SNMP エージェントの設定を表示する方法を示します。

```
# show snmp-server

SNMP Server   : Enabled ...(1)
Name          : SiteA-Switch ...(2)
Location      : HQ 15F ...(3)
Contact       : MIS Department II ...(4)
SNMP UDP Port     : 161 ...(5)
SNMP Response Broadcast Request     : Disabled ...(6)
```

項番	説明
(1)	SNMP エージェントが有効(Enabled)なことを示します。
(2)	システム名 (sysName) を表示します。
(3)	システムロケーション (sysLocation) を表示します。
(4)	システムコンタクト (sysContact) を表示します。
(5)	SNMP で使用する UDP ポート番号を表示します。
(6)	ブロードキャストアドレス宛ての SNMP GetRequest に対する応答設定の有効(Enabled)／無効(Disabled)を表示します。

4.12.20 show snmp community

show snmp community	
目的	SNMP コミュニティー名を表示します。
Command	show snmp community
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SNMP コミュニティー名を表示する方法を示します。

```
# show snmp community
```

```
Community : public ...(1)
 Access : read-only ...(2)
 View : CommunityView ...(3)
 IP access control list : test-IPv4-ACL ...(4)

Community : private
 Access : read-write
 View : CommunityView

Total Entries: 2
```

項番	説明
(1)	SNMP コミュニティー名を表示します。
(2)	MIB へのアクセス権を表示します。
(3)	SNMP ビュー名を表示します。
(4)	SNMP コミュニティー名と関連付ける標準 IP アクセスリスト、または標準 IPv6 アクセスリストを表示します。未設定の場合は表示されません。

4.12.21 show snmp host

show snmp host	
目的	SNMP トラップの宛先ホストを表示します。
Command	show snmp host
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SNMP トラップの宛先ホストを表示する方法を示します。

```
# show snmp host

Host IP Address   : 192.0.2.100 ...(1)
SNMP Version      : V2c ...(2)
Community Name    : test-public ...(3)
UDP Port          : 162 ...(4)

Host IPv6 Address: 2001:db8::100 ...(1)
SNMP Version      : V3 noauthnopriv
SNMPv3 User Name : test-user ...(5)
UDP Port          : 162

Total Entries: 2
```

項番	説明
(1)	SNMP トラップの宛先 IP アドレスを表示します。
(2)	SNMP トラップのバージョンを表示します。 V1：SNMPv1 V2c：SNMPv2c

項番	説明
	V3 noauthnopriv：SNMPv3（認証なし、暗号化なし） V3 authnopriv：SNMPv3（認証あり、暗号化なし） V3 authpriv：SNMPv3（認証あり、暗号化あり）
(3)	SNMP トラップで通知する SNMP コミュニティー名を表示します。
(4)	UDP ポート番号を表示します。
(5)	SNMP トラップで通知する SNMP ユーザー名を表示します。

4.12.22 show snmp-server traps

show snmp-server traps	
目的	SNMP トラップの有効／無効を表示します。
Command	show snmp-server traps
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• 以下項目は、AEOS-NP2500 Ver. 1.13.01 以降で表示されます。それより前のバージョンでは表示されません。 • STORM 項目, LOOP-DETECT 項目
バージョン	1.08.02 1.13.01：表示内容を拡張

使用例：SNMP トラップの有効／無効を表示する方法を示します。

```
# show snmp-server traps

Global Trap State : Disabled ...(1)
Individual Trap State:
  STORM
    Storm-control             : Disabled ...(2)
  LOOP-DETECT
    Loop-detection            : Enabled ...(3)
  SNMP
    Authentication            : Disabled ...(4)
    Linkup                    : Disabled ...(5)
    Linkdown                  : Disabled ...(6)
    Coldstart                 : Disabled ...(7)
    Warmstart                 : Disabled ...(8)
```

項番	説明
(1)	SNMP トラップのグローバル設定の有効(Enabled)／無効(Disabled)を表示します。
(2)	ストームコントロール機能の SNMP トラップの有効(Enabled)／無効(Disabled)を表示します。
(3)	ループ検知機能の SNMP トラップの有効(Enabled)／無効(Disabled)を表示します。
(4)	SNMP 認証失敗 SNMP トラップの有効(Enabled)／無効(Disabled)を表示します。
(5)	リンクアップ SNMP トラップのグローバル設定の有効(Enabled)／無効(Disabled)を表示します。

項番	説明
(6)	リンクダウン SNMP トラップのグローバル設定の有効(Enabled)／無効(Disabled)を表示します。
(7)	コールドスタート SNMP トラップの有効(Enabled)／無効(Disabled)を表示します。
(8)	ウォームスタート SNMP トラップの有効(Enabled)／無効(Disabled)を表示します。

4.12.23 show snmp-server trap-sending

show snmp-server trap-sending	
目的	自装置の SNMP トラップの送信可能ポート／送信禁止ポートを表示します。
Command	show snmp-server trap-sending [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/5 の、自装置の SNMP トラップの送信可能ポート／送信禁止ポートを表示する方法を示します。

```
# show snmp-server trap-sending interface port 1/0/1-1/0/5
(1)                  (2)
Port                 Trap Sending
-------------        -------------
Port1/0/1            Enabled
Port1/0/2            Enabled
Port1/0/3            Enabled
Port1/0/4            Disabled
Port1/0/5            Enabled
```

項番	説明
(1)	ポート番号を表示します。
(2)	自装置の SNMP トラップの送信可能ポート(Enabled)／送信禁止ポート(Disabled)を表示します。

4.12.24 show snmp trap link-status

show snmp trap link-status	
目的	ポートのリンクアップ・リンクダウンの SNMP トラップ設定を表示します。
Command	show snmp trap link-status [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/5 の、リンクアップ・リンクダウンの SNMP トラップ設定を表示する方法を示します。

```
# show snmp trap link-status interface port 1/0/1-1/0/5
(1)                  (2)
Port                 Trap state
-------------        -------------
Port1/0/1            Enabled
Port1/0/2            Enabled
Port1/0/3            Enabled
Port1/0/4            Enabled
Port1/0/5            Enabled
```

項番	説明
(1)	ポート番号を表示します。
(2)	リンクアップ・リンクダウンの SNMP トラップの有効(Enabled)／無効(Disabled)を表示します。

4.12.25 show snmp user

show snmp user	
目的	SNMP ユーザーを表示します。
Command	show snmp user [NAME]
Parameter	NAME (省略可能)：SNMP ユーザー名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	snmp-server community コマンドで作成したコミュニティー名は、本コマンドでは表示されません。
制限・注意	-
バージョン	1.08.02

使用例：SNMP ユーザーを表示する方法を示します。

```
# show snmp user

User Name: initial ...(1)
  Security Model: 3 ...(2)
  Group Name: initial ...(3)
  Authentication Protocol: None ...(4)
  Privacy Protocol: None ...(5)
  Engine ID: 8000011603004066a8cc3600 ...(6)
  IP access control list: ...(7)

Total Entries: 1
```

項番	説明
(1)	SNMP ユーザー名を表示します。
(2)	セキュリティーモデル (3：SNMPv3) を表示します。
(3)	SNMP ユーザーが所属する SNMP グループ名を表示します。
(4)	SNMP ユーザーの認証方式を表示します。

項番	説明
	None：なし md5：HMAC-MD5-96 認証 sha：HMAC-SHA-96 認証
(5)	パケットの暗号化方式（None：暗号化なし／DES：Data Encryption Standard）を表示します。
(6)	SNMP エンジン ID を表示します。
(7)	SNMP ユーザーと関連付ける標準 IP アクセスリスト、または標準 IPv6 アクセスリストを表示します。

4.12.26 show snmp group

show snmp group	
目的	SNMP グループを表示します。
Command	show snmp group
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SNMP グループを表示する方法を示します。

```
# show snmp group

GroupName: public ...(1)
SecurityModel: v1 ...(2)
  ReadView      : CommunityView ...(3)          WriteView     : ...(4)
  NotifyView    : CommunityView ...(5)
  IP access control list: ...(6)

GroupName: public
SecurityModel: v2c
  ReadView      : CommunityView                 WriteView     :
  NotifyView    : CommunityView
  IP access control list:

GroupName: initial
SecurityModel: v3/noauth
  ReadView      : restricted                    WriteView     :
  NotifyView    : restricted
  IP access control list:

GroupName: private
SecurityModel: v1
  ReadView      : CommunityView                 WriteView     : CommunityView
  NotifyView    : CommunityView
  IP access control list:

GroupName: private
SecurityModel: v2c
  ReadView      : CommunityView                 WriteView     : CommunityView
  NotifyView    : CommunityView
```

```
  IP access control list:

Total Entries: 5
```

項番	説明
(1)	SNMP グループ名を表示します。
(2)	セキュリティーモデルを表示します。 v1：SNMPv1 v2c：SNMPv2c v3/noauth：SNMPv3（認証なし、暗号化なし） v3/auth：SNMPv3（認証あり、暗号化なし） v3/priv：SNMPv3（認証あり、暗号化あり）
(3)	グループのユーザーに読み取りを許可する SNMP ビュー（read-view）を表示します。
(4)	グループのユーザーに書き込みを許可する SNMP ビュー（write-view）を表示します。
(5)	グループのユーザーに SNMP トラップの送信を許可する SNMP ビュー（notify-view）を表示します。
(6)	SNMP グループと関連付ける標準 IP アクセスリスト、または標準 IPv6 アクセスリストを表示します。

4.12.27 show snmp view

show snmp view	
目的	SNMP ビューを表示します。
Command	show snmp view
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SNMP ビューを表示する方法を示します。

```
# show snmp view
(1)          (2)          (3)
restricted(included) 1.3.6.1.2.1.1
restricted(included) 1.3.6.1.2.1.11
restricted(included) 1.3.6.1.6.3.10.2.1
restricted(included) 1.3.6.1.6.3.11.2.1
restricted(included) 1.3.6.1.6.3.15.1.1
CommunityView(included) 1
CommunityView(excluded) 1.3.6.1.6.3
CommunityView(included) 1.3.6.1.6.3.1

Total Entries: 8
```

項番	説明
(1)	SNMP ビュー名を表示します。

項番	説明
(2)	対象の OID ツリーの条件（included：SNMP ビューに含める／excluded：SNMP ビューから除外する）を表示します。
(3)	OID ツリーの頂点のオブジェクト識別子を表示します。

4.12.28 show snmp engineID

show snmp engineID	
目的	SNMP エンジン ID を表示します。
Command	show snmp engineID
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：SNMP エンジン ID を表示する方法を示します。

```
# show snmp engineID

Local SNMP engineID: 8000011603fc6dd1f2821f00 ...(1)
```

項番	説明
(1)	SNMP エンジン ID を表示します。

4.13 ミラーリングコマンド

ミラーリング関連の設定コマンドは以下のとおりです。

- monitor session destination interface
- monitor session destination remote vlan
- monitor session source interface
- monitor session source acl
- monitor session source remote vlan
- remote-span
- no monitor session

ミラーリング関連の show コマンドは以下のとおりです。

- show monitor session

4.13.1 monitor session destination interface

monitor session destination interface	
目的	ローカルモニターセッション、もしくはリモートモニターセッション（モニター先装置）において、ミラーリングトラフィックを送信する宛先インターフェースを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	monitor session ID destination interface IF-ID no monitor session ID destination interface IF-ID
Parameter	ID：セッション番号を、1～4 の範囲で指定します。 IF-ID：宛先インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	宛先インターフェースは、1 つのモニターセッションに 1 個のみ設定できます。 本コマンドで、任意のインターフェースを複数のモニターセッションの宛先インターフェースとして設定できます。
制限・注意	• すでに送信元インターフェースとして設定されているインターフェースは、宛先インターフェースとして設定できません。 • すでに monitor session destination remote vlan コマンドで宛先インターフェースとして設定されているインターフェースは、本コマンドで宛先インターフェースとして設定できません。 • ApresiaNP2500 シリーズでは、送信元インターフェース設定が rx 指定（送信元アクセスリスト含む）のみのモニターセッションは、装置全体で最大 4 個まで設定できますが、送信元インターフェース設定に tx 指定を含むモニターセッションは、設定できるのは装置全体で最大 1 個です。 • リモートモニターセッション（モニター先装置）では、リモートモニターVLAN を monitor session destination interface コマンドで設定した宛先インターフェースにも設定してください。宛先インターフェースに VLAN を設定するには switchport access vlan コマンドを使用してください。なお、宛先インターフェースでトラ

monitor session destination interface	
	フィックを受信した場合には、リモートモニターVLAN の他のポートに中継してしまうことに注意してください。
バージョン	1.08.02

使用例：セッション番号 1、宛先インターフェースをポート 1/0/1、送信元インターフェースをポート 1/0/2〜1/0/4 として、ローカルモニターセッションを設定する方法を示します。

```
# configure terminal
(config)# monitor session 1 destination interface port 1/0/1
(config)# monitor session 1 source interface port 1/0/2-4
(config)#
```

4.13.2 monitor session destination remote vlan

monitor session destination remote vlan	
目的	リモートモニターセッション（モニター元装置）において、ミラーリングトラフィックを送信するリモートモニターVLAN と宛先インターフェースを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	monitor session ID destination remote vlan VLAN-ID interface IF-ID no monitor session ID destination remote vlan
Parameter	ID：セッション番号を、1〜4 の範囲で指定します。 VLAN-ID：リモートモニターVLAN を、2〜4094 の範囲で指定します。 IF-ID：宛先インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	リモートモニターVLAN と宛先インターフェースは、1 つのモニターセッションに 1 個のみ設定できます。 本コマンドでリモートモニターセッション（モニター元装置）を設定する場合、宛先インターフェースに指定したリモートモニターVLAN が割り当てられていなくても、ミラーリングトラフィックはリモートモニターVLAN のタグ付きフレームとして送信されます。
制限・注意	• 対象となるミラーリング元のトラフィックが「自装置の CPU から送信する自発パケット」の場合には、ミラーリングトラフィックに本コマンドで指定したリモートモニターVLAN の VLAN タグを付与できない制限があります。そのため、リモートモニターセッションを使用する場合は、「自装置の CPU から送信する自発パケット」が対象にならないよう注意して使用してください。 • すでに送信元インターフェースとして設定されているインターフェースは、宛先インターフェースとして設定できません。 • すでに宛先インターフェースとして設定されているインターフェースは、本コマンドで宛先インターフェースとして設定できません。 • すでに任意のモニターセッションでリモートモニターVLAN として設定されている VLAN は、別のモニターセッションのリモートモニターVLAN として設定できませ

monitor session destination remote vlan	
	ん。 • ApresiaNP2500 シリーズでは、送信元インターフェース設定が rx 指定（送信元アクセスリスト含む）のみのモニターセッションは、装置全体で最大 4 個まで設定できますが、送信元インターフェース設定に tx 指定を含むモニターセッションは、設定できるのは装置全体で最大 1 個です。
バージョン	1.08.02

使用例：セッション番号 2、リモートモニターVLAN を 100、宛先インターフェースをポート 1/0/6、送信元インターフェースを rx 指定のポート 1/0/2～1/0/4 として、リモートモニターセッション（モニター元装置）を設定する方法を示します。

```
# configure terminal
(config)# monitor session 2 destination remote vlan 100 interface port 1/0/6
(config)# monitor session 2 source interface port 1/0/2-4 rx
(config)#
```

4.13.3 monitor session source interface

monitor session source interface	
目的	ローカルモニターセッション、もしくはリモートモニターセッション（モニター元装置）において、ミラーリングする送信元インターフェースを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	monitor session ID source interface {IF-ID [,|-] [both | rx | tx] | cpu rx} no monitor session ID source interface {IF-ID [,|-] | cpu rx}
Parameter	ID：セッション番号を、1～4 の範囲で指定します。 IF-ID：送信元インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定 both（省略可能）：送受信トラフィックを対象にする場合に指定します。 rx（省略可能）：受信トラフィックを対象にする場合に指定します。 tx（省略可能）：送信トラフィックを対象にする場合に指定します。 cpu rx：CPU で受信したトラフィックを対象にする場合に指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	送信元インターフェースは、1 つのモニターセッションに複数設定できます。 both, rx, tx パラメーターを省略すると、both パラメーターを指定した場合と同様の動作になります。また、both パラメーターを指定して設定した場合は、構成情報では rx パラメーターと tx パラメーターの設定として表示されます。
制限・注意	• 送信トラフィックをミラーリング対象にする場合、実際に装置から送信される際の VLAN タグの有無にかかわらず、ミラーリングトラフィックは VLAN タグ付きフレームとしてミラーリングされます。 • cpu rx パラメーターを指定して CPU で受信したトラフィックを対象にする場合、以下の制限があります。

monitor session source interface	
	• 装置で受信した際の VLAN タグの有無にかかわらず、ミラーリングトラフィックは VLAN タグ付きフレームとしてミラーリングされます。 • スタック構成の場合、スタックポート間でやり取りする制御フレームが VID=4095 のタグ付きフレームとしてミラーリングされますが、このミラーリングトラフィックは無視してください。 • リモートモニターセッション（モニター元装置）の送信元インターフェースとして使用する場合は、以下の仕様制限があります。そのため、リモートモニターセッション（モニター元装置）の場合は基本的には rx 指定で設定し、受信トラフィックのみを対象にして使用することを推奨します。 • 自装置の CPU から送信する自発パケットに対しては、monitor session destination remote vlan コマンドで指定したリモートモニターVLAN の VLAN タグを付与できない制限 • すでに宛先インターフェースとして設定されているインターフェースは、送信元インターフェースとして設定できません。 • すでに任意のモニターセッションで送信元インターフェースとして設定されているインターフェースは、別のモニターセッションの送信元インターフェースとして設定できません。 • すでにリモートモニターセッション（モニター先装置）として設定されているセッションでは、送信元インターフェースは設定できません。 • ApresiaNP2500 シリーズでは、送信元インターフェース設定が rx 指定（送信元アクセスリスト含む）のみのモニターセッションは、装置全体で最大 4 個まで設定できますが、送信元インターフェース設定に tx 指定を含むモニターセッションは、設定できるのは装置全体で最大 1 個です。 • ポートリダンダントの ready ポート、スパニングツリーのブロッキング状態のポート、MMRP-Plus の Blocking ポートを、それぞれ rx、tx の送信元インターフェースに設定した場合、該当するポートで受信、送信したパケットはミラーリングされます。
バージョン	1.08.02

使用例：セッション番号 1、宛先インターフェースをポート 1/0/1、送信元インターフェースをポート 1/0/2～1/0/4 として、ローカルモニターセッションを設定する方法を示します。

```
# configure terminal
(config)# monitor session 1 destination interface port 1/0/1
(config)# monitor session 1 source interface port 1/0/2-4
(config)#
```

4.13.4 monitor session source acl

monitor session source acl	
目的	ローカルモニターセッション、もしくはリモートモニターセッション（モニター元装置）において、フローベースのモニターを行うための送信元アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	monitor session ID source acl ACL-NAME no monitor session ID source acl ACL-NAME
Parameter	ID：セッション番号を、1～4 の範囲で指定します。 ACL-NAME：フローベースのモニターを行うための送信元アクセスリストを指定し

monitor session source acl	
	ます。本コマンドでは受信方向のトラフィックのミラーリングのみサポートしているため、受信方向に適用されたアクセスリストを指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	送信元アクセスリストは、1 つのモニターセッションに 1 個のみ設定できます。 指定したアクセスリストの permit ルールにマッチしたトラフィックだけでなく、deny ルールにマッチしたトラフィックもミラーリングされます。 指定するアクセスリストは、expert access-group コマンド、mac access-group コマンド、ip access-group コマンド、arp access-group コマンド、または ipv6 access-group コマンドで受信方向を指定してモニター対象のポートに適用するか、もしくは VLAN アクセスマップコマンドを介してモニター対象の VLAN に適用する必要があります。
制限・注意	• 本コマンドで送信方向に適用されたアクセスリスト（例：ip access-group TEST out）を指定しても、送信トラフィックはミラーリングできません。 • すでに任意のモニターセッションで送信元アクセスリストとして設定されているアクセスリストは、別のモニターセッションの送信元アクセスリストとして設定できません。 • すでにリモートモニターセッションのモニター先装置として設定されているセッションでは、送信元アクセスリストは設定できません。 • ApresiaNP2500 シリーズでは、送信元インターフェース設定が rx 指定（送信元アクセスリスト含む）のみのモニターセッションは、装置全体で最大 4 個まで設定できますが、送信元インターフェース設定に tx 指定を含むモニターセッションは、設定できるのは装置全体で最大 1 個です。 • 存在しないアクセスリストを指定しても設定できますが、警告メッセージが表示されます。
バージョン	1.08.02

使用例：セッション番号 2、宛先インターフェースをポート 1/0/1、送信元アクセスリストを受信方向に適用された拡張 MAC アクセスリスト「MAC-Monitored-Flow」として、ローカルモニターセッションを設定する方法を示します。

```
# configure terminal
(config)# monitor session 2 destination interface port 1/0/1
(config)# monitor session 2 source acl MAC-Monitored-Flow
(config)#
```

4.13.5 monitor session source remote vlan

monitor session source remote vlan	
目的	リモートモニターセッション（モニター先装置）において、ミラーリング元のリモートモニターVLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	monitor session ID source remote vlan VLAN-ID no monitor session ID source remote vlan
Parameter	ID：セッション番号を、1～4 の範囲で指定します。

monitor session source remote vlan	
	VLAN-ID：リモートモニターVLAN を、2～4094 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	リモートモニターVLAN は、1 つのモニターセッションに 1 個のみ設定できます。 リモートモニターセッション（モニター先装置）では、本コマンドでミラーリング元のリモートモニターVLAN を設定し、monitor session destination interface コマンドで宛先インターフェースを設定します。
制限・注意	• 任意のモニターセッションでリモートモニターVLAN として設定済みの VLAN は、別のモニターセッションのリモートモニターVLAN として設定できません。 • すでにローカルモニターセッションとして設定されているセッションでは、ミラーリング元のリモートモニターVLAN は設定できません。 • リモートモニターセッション（モニター先装置）では、ミラーリングトラフィック（リモートモニターVLAN のタグ付きフレーム）を受信するインターフェースに、リモートモニターVLAN を設定してください。受信インターフェースに VLAN を設定するには switchport trunk allowed vlan コマンドを使用してください。
バージョン	1.08.02

使用例：セッション番号 2、宛先インターフェースをポート 1/0/4、ミラーリング元のリモートモニターVLAN を VLAN 100 として、リモートモニターセッション（モニター先装置）を設定する方法を示します。なお、本設定例ではモニター元のミラーリングトラフィックはポート 1/0/1 で受信して、ポート 1/0/4 から送信されます。

```
# configure terminal
(config)# vlan 100
(config-vlan)# remote-span
(config-vlan)# exit
(config)# interface port 1/0/1
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk allowed vlan 100
(config-if-port)# exit
(config)# interface port 1/0/4
(config-if-port)# switchport mode access
(config-if-port)# switchport access vlan 100
(config-if-port)# exit
(config)# monitor session 2 source remote vlan 100
(config)# monitor session 2 destination interface port 1/0/4
(config)#
```

4.13.6 remote-span

remote-span	
目的	VLAN をリモートモニターVLAN として設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	remote-span no remote-span
Parameter	なし
デフォルト	なし

remote-span	
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	VLAN をリモートモニターVLAN として設定した場合、その VLAN では MAC アドレス学習が無効になります。 リモートモニターVLAN は、リモートモニターセッションの中継装置と、モニター先装置で設定します。
制限・注意	• リモートモニターセッションに関係する中継装置のミラーリングトラフィックを中継するポートは、リモートモニターVLAN をタグ付きメンバーポートとして設定してください。
バージョン	1.08.02

使用例：リモートモニターセッションの中継装置で、VLAN 100 をリモートモニターVLAN として設定し、ポート 1/0/1 とポート 1/0/5 を中継ポートとして設定する方法を示します。

```
# configure terminal
(config)# vlan 100
(config-vlan)# remote-span
(config-vlan)# exit
(config)#
(config)# interface port 1/0/1
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk allowed vlan 100
(config-if-port)# exit
(config)# interface port 1/0/5
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk allowed vlan 100
(config-if-port)# exit
(config)#
```

4.13.7 no monitor session

no monitor session	
目的	モニターセッションを削除します。
Command	no monitor session ID
Parameter	ID：セッション番号を 1～4 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを実行すると、指定したセッション番号のモニターセッション設定がすべて削除されます。
制限・注意	-
バージョン	1.08.02

使用例：セッション番号 1 のモニターセッションを削除する方法を示します。

```
# configure terminal
(config)# no monitor session 1
(config)#
```

4.13.8 show monitor session

show monitor session	
目的	モニターセッションの設定を表示します。
Command	show monitor session [ID	remote	local]
Parameter	ID（省略可能）：セッション番号を 1～4 の範囲で指定します。 remote（省略可能）：リモートモニターセッションを表示します。 local（省略可能）：ローカルモニターセッションを表示します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のセッション番号を指定しない場合は、すべてのモニターセッションの設定が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：セッション番号 1 のモニターセッションの設定を表示する方法を示します。

```
# show monitor session 1

 Session 1 ...(1)
     Session Type: local session ...(2)
     Destination Port: Port1/0/1 ...(3)
     Flow Based Source: IPv4-Monitor-List ...(4)
     Source Ports: ...(5)
         Both:
             Port1/0/4
         RX:
             Port1/0/3
         TX:
             Port1/0/2

 Total Entries: 1
```

項番	説明
(1)	セッション番号を表示します。
(2)	セッションタイプを表示します。 local session：ローカルモニターセッション remote source session：リモートモニターセッション（モニター元装置） remote destination session：リモートモニターセッション（モニター先装置）
(3)	モニターセッションの宛先インターフェース（ポート番号またはポートチャネル番号）を表示します。
(4)	モニターセッションの送信元アクセスリストを表示します。
(5)	モニターセッションの送信元インターフェース（ポート番号またはポートチャネル番号）を表示します。 Both：ミラーリング対象が受信フレームおよび送信フレームの送信元インターフェース RX：ミラーリング対象が受信フレームのみの送信元インターフェース TX：ミラーリング対象が送信フレームのみの送信元インターフェース

使用例：リモートモニターセッションの設定を表示する方法を示します。

```
# show monitor session remote

 Session 1 ...(1)
     Session Type: remote source session ...(2)
     Destination Remote VLAN: VLAN 2001 ...(3)
     Destination Port: Port1/0/12 ...(4)
     Source Ports: ...(5)
         RX:
             Port1/0/1

 Session 4 ...(1)
     Session Type: remote destination session ...(2)
     Source Remote VLAN: VLAN 4090 ...(6)
     Destination Port: Port1/0/8 ...(4)

 Total Entries: 2
```

項番	説明
(1)	セッション番号を表示します。
(2)	セッションタイプを表示します。 local session：ローカルモニターセッション remote source session：リモートモニターセッション（モニター元装置） remote destination session：リモートモニターセッション（モニター先装置）
(3)	リモートモニターセッション（モニター元装置）で設定した、リモートモニターVLAN を表示します。
(4)	モニターセッションの宛先インターフェース（ポート番号またはポートチャネル番号）を表示します。
(5)	モニターセッションの送信元インターフェース（ポート番号またはポートチャネル番号）を表示します。 Both：ミラーリング対象が受信フレームおよび送信フレームの送信元インターフェース RX：ミラーリング対象が受信フレームのみの送信元インターフェース TX：ミラーリング対象が送信フレームのみの送信元インターフェース
(6)	リモートモニターセッション（モニター先装置）で設定した、ミラーリング元のリモートモニターVLAN を表示します。

4.14 LLDP コマンド

LLDP（Link Layer Discovery Protocol）関連の設定コマンドは以下のとおりです。

- lldp run
- lldp transmit
- lldp receive
- lldp forward
- lldp tx-delay
- lldp tx-interval
- lldp hold-multiplier
- lldp reinit
- lldp fast-count
- lldp subtype port-id
- lldp tlv-select
- lldp management-address
- lldp dot1-tlv-select
- lldp dot3-tlv-select
- lldp med-tlv-select
- lldp err-disable
- lldp notification enable
- lldp med notification enable
- snmp-server enable traps lldp
- snmp-server enable traps lldp med

LLDP（Link Layer Discovery Protocol）関連の show／操作コマンドは以下のとおりです。

- show lldp
- show lldp interface
- show lldp local interface
- show lldp management-address
- show lldp neighbors interface
- show lldp traffic
- show lldp traffic interface
- clear lldp table
- clear lldp counters

4.14.1 lldp run

lldp run	
目的	LLDP 機能のグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	lldp run no lldp run
Parameter	なし
デフォルト	無効
モード	グローバル設定モード

lldp run	
特権レベル	レベル：12
ガイドライン	本コマンドはグローバルな LLDP 機能の有効／無効を設定します。 物理ポートごとの LLDPDU 送信の有効／無効は lldp transmit コマンドを、物理ポートごとの LLDPDU 受信の有効／無効は lldp receive コマンドを使用します。
制限・注意	• ApresiaNP シリーズでは、「Chassis ID と Port ID の組み合わせが同じ LLDPDU」を複数ポートで受信するような使い方はできません。各ポートで受信する LLDPDU は「Chassis ID と Port ID の組み合わせがユニークな LLDPDU」になるようにして使用してください。 • 例えば、対向が AEOS8 製品でポートチャネルで接続する場合に、AEOS8 製品の LAG のメンバーポートすべてで同じ description 設定にしてしまうと、この条件にあてはまります。この場合は、AEOS8 製品において各メンバーポートごとにユニークな LLDPDU を送信するように変更してください。詳細に関しては AEOS8 製品のコマンドリファレンスを参照してください。
バージョン	1.08.02

使用例：LLDP 機能をグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# lldp run
(config)#
```

4.14.2 lldp transmit

lldp transmit	
目的	LLDPDU の送信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	lldp transmit no lldp transmit
Parameter	なし
デフォルト	有効（lldp transmit）
モード	インターフェース設定モード（port, range）
特権レベル	レベル：12
ガイドライン	-
制限・注意	• LLDP 疑似リンクダウン機能を有効に設定した物理ポートでは、LLDPDU の送信を無効にできません。 • LLDP 機能を使用する場合は、lldp run コマンドも有効にする必要があります。
バージョン	1.08.02

使用例：ポート 1/0/1 で、LLDPDU の送信を無効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# no lldp transmit
(config-if-port)#
```

4.14.3 lldp receive

lldp receive	
目的	LLDPDU の受信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	lldp receive no lldp receive
Parameter	なし
デフォルト	有効 (lldp receive)
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	-
制限・注意	• LLDP 疑似リンクダウン機能を有効に設定した物理ポートでは、LLDPDU の受信を無効にできません。 • LLDP 機能を使用する場合は、lldp run コマンドも有効にする必要があります。
バージョン	1.08.02

使用例：ポート 1/0/1 で、LLDPDU の受信を無効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# no lldp receive
(config-if-port)#
```

4.14.4 lldp forward

lldp forward	
目的	LLDP 転送機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	lldp forward no lldp forward
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	LLDP 転送機能を有効にすると、受信した LLDPDU を、受信した VLAN の他ポートに転送するようになります。なお、LLDP 転送機能を有効にする場合は、no lldp run コマンドで LLDP 機能のグローバル設定を無効にする必要があります。
制限・注意	• 転送される LLDPDU は、送信ポートの種別にかかわらず常にタグなしフレームの形式で転送されます。
バージョン	1.08.02

使用例：LLDP 転送機能を有効にする方法を示します。

```
# configure terminal
(config)# lldp forward
(config)#
```

4.14.5 lldp tx-delay

lldp tx-delay	
目的	LLDPDU の送信遅延間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lldp tx-delay SECONDS no lldp tx-delay
Parameter	SECONDS：LLDPDU の送信遅延間隔を、1～8192 秒の範囲で指定します。
デフォルト	2 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• LLDPDU の送信遅延間隔は、lldp tx-interval コマンドで設定する送信間隔の 4 分の 1 以下に設定してください。
バージョン	1.08.02

使用例：LLDPDU の送信遅延間隔を 8 秒に設定する方法を示します。

```
# configure terminal
(config)# lldp tx-delay 8
(config)#
```

4.14.6 lldp tx-interval

lldp tx-interval	
目的	LLDPDU の送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lldp tx-interval SECONDS no lldp tx-interval
Parameter	SECONDS：LLDPDU を連続送信する場合の送信間隔を、5～32,768 秒の範囲で指定します。
デフォルト	30 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• LLDPDU の送信間隔は、lldp tx-delay コマンドで設定する送信遅延間隔の 4 倍以上に設定してください。
バージョン	1.08.02

使用例：LLDPDU の送信間隔を 50 秒に設定する方法を示します。

```
# configure terminal
(config)# lldp tx-interval 50
(config)#
```

4.14.7 lldp hold-multiplier

lldp hold-multiplier	
目的	送信する LLDPDU の TTL 値を決定するための、LLDPDU 送信間隔の乗数（Message TX Hold Multiplier）を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lldp hold-multiplier VALUE no hold-multiplier
Parameter	VALUE：LLDPDU 送信間隔の乗数（Message TX Hold Multiplier）を、2～10 の範囲で指定します。
デフォルト	4
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	送信する LLDPDU の TTL 値（隣接装置での情報保持時間）は、LLDPDU 送信間隔（lldp tx-interval）×乗数（lldp hold-multiplier）で決定されます。
制限・注意	-
バージョン	1.08.02

使用例：LLDPDU 送信間隔の乗数（Message TX Hold Multiplier）を 3 に設定する方法を示します。

```
# configure terminal
(config)# lldp hold-multiplier 3
(config)#
```

4.14.8 lldp reinit

lldp reinit	
目的	LLDP 再初期化の遅延時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lldp reinit SECONDS no lldp reinit
Parameter	SECONDS：LLDP 再初期化の遅延時間を、1～10 秒の範囲で指定します。
デフォルト	2 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：LLDP 再初期化の遅延時間を 5 秒に設定する方法を示します。

```
# configure terminal
(config)# lldp reinit 5
(config)#
```

4.14.9 lldp fast-count

lldp fast-count	
目的	LLDP-MED fast start 処理の実行回数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lldp fast-count VALUE no lldp fast-count
Parameter	VALUE：LLDP-MED fast start 処理の実行回数を 1～10 回の範囲で指定します。
デフォルト	4
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	LLDP-MED Capabilities TLV が検出されると、アプリケーション層では fast start メカニズムを開始します。
制限・注意	-
バージョン	1.08.02

使用例：LLDP-MED fast start 処理の実行回数を 10 回に設定する方法を示します。

```
# configure terminal
(config)# lldp fast-count 10
(config)#
```

4.14.10 lldp subtype port-id

lldp subtype port-id	
目的	Port ID TLV のサブタイプを設定します。デフォルト設定に戻すには、lldp subtype port-id local コマンドを使用します。
Command	lldp subtype port-id {mac-address | local}
Parameter	mac-address：Port ID TLV のサブタイプを MAC Address(3)に指定します。Port ID フィールドには、対象ポートの MAC アドレスがセットされます。 local：Port ID TLV のサブタイプを Locally assigned(7)に指定します。Port ID フィールドには、対象ポートのポート番号（例：Port1/0/21）がセットされます。
デフォルト	local
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で、Port ID TLV のサブタイプを mac-address に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp subtype port-id mac-address
(config-if-port)#
```

4.14.11 lldp tlv-select

lldp tlv-select	
目的	IEEE 802.1AB basic management set のオプション TLV のうち、LLDPDU に付加して隣接装置に通知する TLV を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	lldp tlv-select [port-description | system-capabilities | system-description | system-name] no lldp tlv-select [port-description | system-capabilities | system-description | system-name]
Parameter	LLDPDU に付加して通知する TLV を、以下のパラメーターで指定します。 • port-description（省略可能）：Port Description TLV • system-capabilities（省略可能）：System Capabilities TLV • system-description（省略可能）：System Description TLV • system-name（省略可能）：System Name TLV
デフォルト	IEEE 802.1AB basic management set のオプション TLV は未選択
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	System Name TLV で通知する System Name は、snmp-server name コマンドで設定できます。 パラメーターを指定しないで実行した場合は、すべてのパラメーターが有効になります。また、パラメーターを指定しないで no lldp tlv-select を実行した場合は、すべてのパラメーターが無効になります。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で、すべての lldp tlv-select 設定を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp tlv-select
(config-if-port)#
```

使用例：ポート 1/0/1 で、System Name TLV の通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp tlv-select system-name
(config-if-port)#
```

4.14.12 lldp management-address

lldp management-address	
目的	Management Address TLV で通知する管理用 IP アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	lldp management-address [IP-ADDRESS | IPV6-ADDRESS] no lldp management-address [IP-ADDRESS | IPV6-ADDRESS]
Parameter	IP-ADDRESS（省略可能）：管理用 IPv4 アドレスを指定します。 IPV6-ADDRESS（省略可能）：管理用 IPv6 アドレスを指定します。

lldp management-address	
デフォルト	設定なし（Management Address TLV は通知されない）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	lldp management-address コマンドで指定する管理用 IP アドレスは、装置の VLAN インターフェース、もしくはループバックインターフェースに設定済みの IP アドレスを指定できます。未設定の IP アドレスや、マネージメントポートに設定した IP アドレスは指定できません。 管理用 IP アドレスを指定しないで lldp management-address を設定した場合は、デフォルトの IP アドレス（IP アドレスが設定された VLAN インターフェースのうち、最小 VLAN ID の VLAN インターフェースに設定された IP アドレス）が管理用 IP アドレスとして通知されます。なお、VLAN インターフェースに 1 つも IP アドレスが設定されていない場合は通知されません。 装置の IP アドレス設定を削除した場合は、その IP アドレスを管理用 IP アドレスとして指定した lldp management-address 設定も削除されます。 管理用 IP アドレスを指定しないで no lldp management-address を実行した場合は、すべての lldp management-address 設定が削除されます。
制限・注意	• 同一ポートで「管理用 IP アドレス指定の設定」と「管理用 IP アドレス未指定の設定」を同時に設定した場合は、「管理用 IP アドレス指定の設定」が優先されます。
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/2 で、Management Address TLV で通知する管理用 IPv4 アドレスを 10.1.1.1 に設定する方法を示します。

```
# configure terminal
(config)# interface range port 1/0/1-1/0/2
(config-if-port-range)# lldp management-address 10.1.1.1
(config-if-port-range)#
```

使用例：ポート 1/0/3～1/0/4 で、Management Address TLV で通知する管理用 IPv6 アドレスを 2001:db8:10:10::100 に設定する方法を示します。

```
# configure terminal
(config)# interface range port 1/0/3-1/0/4
(config-if-port-range)# lldp management-address 2001:db8:10:10::100
(config-if-port-range)#
```

使用例：ポート 1/0/5 で、すべての lldp management-address 設定を削除して、Management Address TLV が通知されないようにする方法を示します。

```
# configure terminal
(config)# interface port 1/0/5
(config-if-port)# no lldp management-address
(config-if-port)#
```

4.14.13 lldp dot1-tlv-select

lldp dot1-tlv-select	
目的	IEEE 802.1 Organizationally Specific TLVs のうち、LLDPDU（LLDP data unit）に付加して隣接装置に通知する TLV を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	lldp dot1-tlv-select {port-vlan | protocol-vlan VLAN-ID [,|-] | vlan-name

lldp dot1-tlv-select	
	[VLAN-ID [,|-]] | protocol-identity [NAME]} no lldp dot1-tlv-select {port-vlan | protocol-vlan [VLAN-ID [,|-]] | vlan-name [VLAN-ID [,|-]] | protocol-identity [NAME]}
Parameter	port-vlan：Port VLAN ID TLV を通知する場合に指定します。 protocol-vlan VLAN-ID：Port and Protocol VLAN ID（PPVID）TLV で通知する VLAN ID を 1～4094 の範囲で指定します。最大 16 個まで、複数指定できます。 vlan-name [VLAN-ID]：VLAN Name TLV で通知する VLAN ID を 1～4094 の範囲で指定します。VLAN ID を指定しないで設定した場合は、すべての VLAN（1～4094）を指定した形式で設定されます。 protocol-identity [NAME]：Protocol Identity TLV で通知するプロトコルを、以下のパラメーターで指定します。特定のプロトコルを指定しないで設定した場合は、すべてのプロトコルに対して設定されます。 • eapol：Extensible Authentication Protocol（EAP）over LAN • lacp：Link Aggregation Control Protocol • stp：スパニングツリープロトコル
デフォルト	IEEE 802.1 Organizationally Specific TLV は未選択
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	PPVID TLV は、protocol-vlan パラメーターで指定した VLAN が、対象ポートでプロトコル VLAN として設定されている場合に通知されます。 VLAN Name TLV は、vlan-name パラメーターで指定した VLAN が、対象ポートに設定されている場合に通知されます。 Protocol Identity TLV は、protocol-identity パラメーターで指定したプロトコルが、対象ポートで有効に設定されている場合に通知されます。
制限・注意	• lldp dot1-tlv-select protocol-vlan が設定済みの状態で、別の VLAN ID を指定して再度設定した場合は、元の設定を上書き設定します。 • lldp dot1-tlv-select vlan-name が設定済みの状態で、別の VLAN ID を指定して再度設定した場合は、元の設定に新たに指定した VLAN ID が追加されます。
バージョン	1.08.02

使用例：ポート 1/0/1 で、Port VLAN ID TLV の通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp dot1-tlv-select port-vlan
(config-if-port)#
```

使用例：ポート 1/0/1 で、VLAN 1～3 を指定して、PPVID TLV の通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp dot1-tlv-select protocol-vlan 1-3
(config-if-port)#
```

使用例：ポート 1/0/1 で、VLAN 1～3 を指定して、VLAN Name TLV の通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp dot1-tlv-select vlan-name 1-3
(config-if-port)#
```

使用例：ポート 1/0/1 で、LACP を指定して、Protocol Identity TLV の通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp dot1-tlv-select protocol-identity lacp
(config-if-port)#
```

4.14.14 lldp dot3-tlv-select

lldp dot3-tlv-select	
目的	IEEE 802.3 Organizationally Specific TLVs のうち、LLDPDU に付加して隣接装置に通知する TLV を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size] no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]
Parameter	LLDPDU に付加して通知する TLV を、以下のパラメーターで指定します。 • mac-phy-cfg（省略可能）：MAC/PHY Configuration/Status TLV • link-aggregation（省略可能）：Link Aggregation TLV • power（省略可能）：Power Via MDI TLV、PoE 対応ポートでのみ設定可能 • max-frame-size（省略可能）：Maximum Frame Size TLV
デフォルト	IEEE 802.3 Organizationally Specific TLV は未選択
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	パラメーターを指定しないで実行した場合は、すべてのパラメーターが有効になります。また、パラメーターを指定しないで no lldp dot3-tlv-select を実行した場合は、すべてのパラメーターが無効になります。
制限・注意	• PoE 非対応ポートではパラメーターを指定しないで lldp dot3-tlv-select、または no lldp dot3-tlv-select を実行することはできません。
バージョン	1.08.02

使用例：ポート 1/0/1 で、MAC/PHY Configuration/Status TLV の通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp dot3-tlv-select mac-phy-cfg
(config-if-port)#
```

4.14.15 lldp med-tlv-select

lldp med-tlv-select	
目的	LLDP-MED TLV のうち、LLDPDU に付加して隣接装置に通知する TLV を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management] no lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]
Parameter	LLDPDU に付加して通知する TLV を、以下のパラメーターで指定します。 • capabilities（省略可能）：LLDP-MED Capabilities TLV（LLDP-MED に対応していることを示す情報） • inventory-management（省略可能）：LLDP-MED Inventory Management TLV（LLDP-MED 対応機器の管理情報） • network-policy（省略可能）：LLDP-MED Network Policy TLV • power-management（省略可能）：LLDP-MED Extended Power-via-MDI TLV、PoE 対応ポートでのみ設定可能
デフォルト	LLDP-MED TLV は未選択
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	LLDP-MED Capabilities TLV の通知を無効にすると、他の LLDP-MED の通知が有効に設定されている場合でも、そのポートの LLDP-MED は無効になります。 LLDP-MED Capabilities TLV の通知を有効に設定しても、対向の終端装置から LLDP-MED TLV が付加された LLDPDU を受信して LLDP 情報が登録されるまでは、LLDP-MED TLV が付加されていない LLDPDU を送信します。対向の終端装置から LLDP-MED TLV が付加された LLDPDU を受信して LLDP 情報が登録されている間は、LLDP-MED TLV が付加された LLDPDU を送信します。 LLDP-MED Network Policy TLV の通知を有効にした場合、Network Policy TLV の各フィールドの値は以下のように決定されます。 • Tagged フラグ：voice vlan mode auto tag 設定、もしくは voice vlan mode manual 設定で Voice VLAN がタグ付きメンバーとして割り当てられている場合は、Tagged フラグ：Yes として設定されます。voice vlan mode auto untag 設定、もしくは voice vlan mode manual 設定で Voice VLAN がタグなしメンバーとして割り当てられている場合は、Tagged フラグ：No として設定されます。 • VLAN ID：Voice VLAN が有効の場合は、voice vlan コマンドで指定した VLAN ID が設定されます。Voice VLAN が無効の場合は、0 が設定されます。 • L2 Priority：voice vlan qos コマンドで指定した優先度が設定されます。 • DSCP Priority：voice vlan dscp で指定した DSCP が設定されます。DSCP が未設定の場合は、0 が設定されます。 パラメーターを指定しないで実行した場合は、すべてのパラメーターが有効になります。また、パラメーターを指定しないで no lldp med-tlv-select を実行した場合は、すべてのパラメーターが無効になります。
制限・注意	• PoE 非対応ポートではパラメーターを指定しないで lldp med-tlv-select、または no lldp med-tlv-select を実行することはできません。

lldp med-tlv-select	
バージョン	1.08.02

使用例：ポート 1/0/1 で、LLDP-MED Capabilities TLV の通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp med-tlv-select capabilities
(config-if-port)#
```

4.14.16 lldp err-disable

lldp err-disable	
目的	物理ポートで LLDP 疑似リンクダウン機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	lldp err-disable no lldp err-disable
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	LLDP 疑似リンクダウン機能を使用する場合は、自装置と対向装置の両方のポートで有効にして使用してください。LLDP 疑似リンクダウン機能を有効にすると、LLDPDU の受信状態や受信内容に基づいて、ポートを LLDP 疑似リンクダウン状態に遷移／復旧します。 LLDP 疑似リンクダウン機能を有効にしたポートでリンク障害などにより対向装置からの LLDPDU を受信しなくなったり、対向装置からリンク異常を検知した内容の LLDPDU を受信すると、ポートは LLDP 疑似リンクダウン状態に遷移します。 LLDP 疑似リンクダウン機能を有効にしたポートがリンクアップすると、まだ対向装置の情報を取得していない状態では LLDP 疑似リンクダウン状態になります。対向装置の情報を取得すると LLDP 疑似リンクダウン状態は復旧します。LLDPDU の送信タイミングは対向装置と同期しているわけではないため、自装置側のポートと対向装置側のポートの LLDP 疑似リンクダウン状態の復旧タイミングには時間差が発生することに注意してください。 LLDP 疑似リンクダウン状態の物理ポートは、show interfaces status コマンドの Status 項目では "connected" と表示されますが、show interfaces コマンドでは "link status is errDis" と表示されます。また、show interfaces description コマンドの Status 項目では "errDis" と表示されます。 ポートチャネルのメンバーポートが LLDP 疑似リンクダウン状態になった場合は、show channel-group channel コマンドのメンバーポートのステータスは hot-sby になります。 物理ポートで指定した MMRP-Plus のリングポートが LLDP 疑似リンクダウン状態になった場合は、show mmrp-plus status ring コマンドや show mmrp-plus status port コマンドのポートのリンク状態(Link Status 項目)は "errDis" と表示され、その MMRP-Plus リングポートはダウンします。
制限・注意	• LLDP 疑似リンクダウン機能と LACP は、同一ポートで併用できません。 • 物理ポートで LLDP 疑似リンクダウン機能と STP/RSTP/MSTP/RPVST+/ERPS 機

lldp err-disable	
	能は併用できません。 • LLDP 疑似リンクダウン状態の物理ポートは、VLAN インターフェースではリンクアップしているポートとして扱われます。 • ポートチャネル（スタティックモード）のメンバーポートで LLDP 疑似リンクダウン機能を使用している場合、LLDP 疑似リンクダウン状態の復旧タイミングは自装置と対向装置で同期しているわけではないため、リンクアップ後にポートチャネルのメンバーポートとして復旧するタイミングも同期しないことに注意してください。例えば、自装置側ポートが先にメンバーポートとして復旧し対向装置側ポートがまだ復旧していない状態では、自装置側のそのポートから送信したトラフィックは対向装置側で破棄されます。 • ApresiaNP シリーズでは、「Chassis ID と Port ID の組み合わせが同じ LLDPDU」を複数ポートで受信するような使い方はできません。各ポートで受信する LLDPDU は「Chassis ID と Port ID の組み合わせがユニークな LLDPDU」になるようにして使用してください。
バージョン	1.08.02

使用例：ポート 1/0/1 で、LLDP 疑似リンクダウン機能を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp err-disable
(config-if-port)#
```

4.14.17 lldp notification enable

lldp notification enable	
目的	LLDP 関連の SNMP トラップ送信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	lldp notification enable no lldp notification enable
Parameter	-
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	-
制限・注意	• LLDP 関連の SNMP トラップ送信を有効にする場合は、snmp-server enable traps lldp コマンドも有効にする必要があります。
バージョン	1.08.02

使用例：ポート 1/0/1 で、LLDP 関連の SNMP トラップ送信を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp notification enable
(config-if-port)#
```

4.14.18 lldp med notification enable

lldp med notification enable	
目的	LLDP-MED 関連の SNMP トラップ送信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	lldp med notification enable no lldp med notification enable
Parameter	-
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	-
制限・注意	• LLDP-MED 関連の SNMP トラップ送信を有効にする場合は、snmp-server enable traps lldp med コマンドも有効にする必要があります。
バージョン	1.08.02

使用例：ポート 1/0/1 で、LLDP-MED 関連の SNMP トラップ送信を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp med notification enable
(config-if-port)#
```

4.14.19 snmp-server enable traps lldp

snmp-server enable traps lldp	
目的	LLDP 関連の SNMP トラップのグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps lldp no snmp-server enable traps lldp
Parameter	-
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。 物理ポートごとの LLDP 関連の SNMP トラップ送信の有効／無効は lldp notification enable コマンドを使用します。
制限・注意	-
バージョン	1.08.02

使用例：LLDP 関連の SNMP トラップのグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps lldp
(config)#
```

4.14.20 snmp-server enable traps lldp med

snmp-server enable traps lldp med	
目的	LLDP-MED 関連の SNMP トラップのグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps lldp med no snmp-server enable traps lldp med
Parameter	-
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。 物理ポートごとの LLDP-MED 関連の SNMP トラップ送信の有効／無効は lldp med notification enable コマンドを使用します。
制限・注意	-
バージョン	1.08.02

使用例：LLDP-MED 関連の SNMP トラップのグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps lldp med
(config)#
```

4.14.21 show lldp

show lldp	
目的	装置の一般的な LLDP 設定を表示します。
Command	show lldp
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：装置の一般的な LLDP 設定の表示方法を示します。

```
# show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address ... (1)
    Chassis ID                : FC-6D-D1-F2-82-1F ... (2)
    System Name               : Switch ... (3)
    System Description        : ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
                                Ver.1.08.02 ... (4)
    System Capabilities Supported: Repeater, Bridge ... (5)
    System Capabilities Enabled  : Repeater, Bridge ... (6)
LLDP-MED System Information:
    Device Class              : Network Connectivity Device ... (7)
```

```
    Hardware Revision          : A ...(8)
    Firmware Revision          : 1.00.00 ...(9)
    Software Revision          : 1.08.02 ...(10)
    Serial Number              : 304210000053 ...(11)
    Manufacturer Name          : APRESIA Systems, Ltd ...(12)
    Model Name                 : ApresiaNP2500-8MT4X-PoE Gigabit ...(13)
    Asset ID                   : ...(14)
    PoE Device Type            : PSE Device ...(15)
    PoE PSE Power Source       : Primary ...(16)

LLDP Configurations
    LLDP State                 : Disabled ...(17)
    LLDP Forward State         : Disabled ...(18)
    Message TX Interval        : 30 ...(19)
    Message TX Hold Multiplier: 4 ...(20)
    ReInit Delay               : 2 ...(21)
    TX Delay                   : 2 ...(22)

LLDP-MED Configuration:
    Fast Start Repeat Count    : 4 ...(23)
```

項番	説明
(1)	Chassis ID TLV のサブタイプを表示します。ApresiaNP シリーズでは、Chassis ID TLV のサブタイプは MAC address(4)で送信します。
(2)	Chassis ID TLV で通知する情報を表示します。サブタイプが MAC Address のため、自装置の MAC アドレスを表示します。
(3)	System Name TLV で通知される、システム名を表示します。
(4)	System Description TLV を通知される、自装置の説明を表示します。
(5)	System Capabilities TLV で通知される、自装置で利用可能な機能の情報を表示します。
(6)	自装置で有効化されている機能の情報を表示します。
(7)	LLDP-MED 対応機器として動作する際に通知するデバイスクラスを表示します。
(8)	LLDP-MED 対応機器として動作する際に通知するハードウェアリビジョンを表示します。
(9)	LLDP-MED 対応機器として動作する際に通知するファームウェアリビジョンを表示します。
(10)	LLDP-MED 対応機器として動作する際に通知するソフトウェアリビジョンを表示します。
(11)	LLDP-MED 対応機器として動作する際に通知するシリアル番号を表示します。
(12)	LLDP-MED 対応機器として動作する際に通知するメーカー名を表示します。
(13)	LLDP-MED 対応機器として動作する際に通知するモデル名を表示します。
(14)	LLDP-MED 対応機器として動作する際に通知するアセット ID を表示します。
(15)	LLDP-MED 対応機器として動作する際に通知するデバイスタイプを表示します。
(16)	LLDP-MED 対応機器として動作する際に通知するパワーソースを表示します。
(17)	装置全体の LLDP 設定の有効(Enabled)／無効(Disabled)を表示します。
(18)	LLDP 転送の有効(Enabled)／無効(Disabled)を表示します。
(19)	LLDPDU の送信間隔(秒)を表示します。
(20)	送信する LLDPDU の TTL 値を決定するための、LLDPDU 送信間隔の乗数を表示します。
(21)	LLDP 再初期化の遅延時間(秒)を表示します。
(22)	LLDPDU の送信遅延間隔(秒)を設定します。

項番	説明
(23)	LLDP-MED fast start 処理の実行回数を表示します。

4.14.22 show lldp interface

show lldp interface	
目的	物理ポートの LLDP 設定を表示します。
Command	show lldp interface port PORTS
Parameter	port PORTS：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の LLDP 設定を表示する方法を示します。

```
# show lldp interface port 1/0/1

Port ID: Port1/0/1 ...(1)
------------------------------------------------------------------------------
Port ID                                                  :Port1/0/1 ...(2)
Admin Status                                             :TX and RX ...(3)
Error disable                                            :Disabled ...(4)
Notification                                             :Disabled ...(5)
Basic Management TLVs:
    Port Description                                     :Disabled ...(6)
    System Name                                          :Disabled ...(7)
    System Description                                   :Disabled ...(8)
    System Capabilities                                  :Disabled ...(9)
    Enabled Management Address: ...(10)
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                         :Disabled ...(11)
    Enabled Port_and_Protocol_VLAN_ID ...(12)
        (None)
    Enabled VLAN Name ...(13)
        (None)
    Enabled Protocol_Identity ...(14)
        (None)
IEEE 802.3 Organizationally Specific TLVs:

    MAC/PHY Configuration/Status                         :Disabled ...(15)
    Power Via MDI                                        :Disabled ...(16)
    Link Aggregation                                     :Disabled ...(17)
    Maximum Frame Size                                   :Disabled ...(18)

Organizationally Specific TLVs:

    Link Fault TLV                                       :Disabled ...(19)

LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                            :Disabled ...(20)
    LLDP-MED Network Policy TLV                          :Disabled ...(21)
    LLDP-MED Extended Power Via MDI PSE TLV              :Disabled ...(22)
```

```
    LLDP-MED Inventory TLV                                  :Disabled ...(23)
```

項番	説明
(1)	ポート番号を表示します。
(2)	ポート番号を表示します。
(3)	LLDPDU の送受信それぞれについて有効／無効を表示します。 TX and RX：送受信ともに有効 TX Only：送信のみ有効 RX Only：受信のみ有効 Disabled：送受信ともに無効
(4)	LLDP 疑似リンクダウン機能の有効(Enabled)／無効(Disabled)を表示します。
(5)	LLDP 関連と LLDP-MED 関連の SNMP トラップの有効／無効を表示します。 Disabled：無効 LLDP：LLDP 関連の SNMP トラップのみ有効 LLDP-MED：LLDP-MED 関連の SNMP トラップのみ有効 LLDP and LLDP-MED：LLDP 関連と LLDP-MED 関連の SNMP トラップが有効
(6)	Port Description TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(7)	System Name TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(8)	System Description TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(9)	System Capabilities TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(10)	Management Address TLV で通知する管理用 IP アドレスを表示します。Management Address TLV を通知しない場合は(None)と表示されます。
(11)	Port VLAN ID TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(12)	Port and Protocol VLAN ID (PPVID) TLV で通知する VLAN ID を表示します。PPVID TLV を通知しない場合は(None)と表示されます。
(13)	VLAN Name TLV で通知する VLAN ID を表示します。VLAN Name TLV を通知しない場合は(None)と表示されます。
(14)	Protocol Identity TLV で通知するプロトコルを表示します。Protocol Identity TLV を通知しない場合は(None)と表示されます。
(15)	MAC/PHY Configuration/Status TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(16)	Power Via MDI TLV 付加の有効(Enabled)／無効(Disabled)を表示します。PoE 対応ポートでのみ表示されます。
(17)	Link Aggregation TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(18)	Maximum Frame Size TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(19)	ベンダー独自の Link Fault TLV (LLDP 疑似リンクダウンに関する情報) 付加の有効(Enabled)／無効(Disabled)を表示します。
(20)	LLDP-MED Capabilities TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(21)	LLDP-MED Network Policy TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(22)	LLDP-MED Extended Power-via-MDI TLV 付加の有効(Enabled)／無効(Disabled)を表示します。
(23)	LLDP-MED Inventory Management TLV 付加の有効(Enabled)／無効(Disabled)を表示します。

4.14.23 show lldp local interface

show lldp local interface	
目的	各 TLV の通知が有効になっている場合に、LLDP TLV に含めて隣接装置に通知される物理ポート情報を表示します。
Command	show lldp local interface port PORTS [brief | detail]
Parameter	port PORTS：物理ポートを指定します。複数指定できます。 brief（省略可能）：情報を要約モードで表示します。 detail（省略可能）：情報を詳細モードで表示します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：隣接装置に通知する場合のポート 1/0/8 の物理ポート情報を、標準モードで表示する方法を示します。

```
# show lldp local interface port 1/0/8

Port ID: Port1/0/8 ...(1)
------------------------------------------------------------------------------
Port ID Subtype                          : Local ...(2)
Port ID                                  : Port1/0/8 ...(3)
Port Description                         : APRESIA Systems, Ltd
                                           ApresiaNP2500-8MT4X-PoE HW A
                                           firmware 1.08.02 Port 8 on Unit 1 ...(4)
Port PVID                                : 1 ...(5)
Management Address Count                 : 1 ...(6)
PPVID Entries Count                      : 0 ...(7)
VLAN Name Entries Count                  : 2 ...(8)
Protocol Identity Entries Count          : 0 ...(8)
MAC/PHY Configuration/Status             : (See Detail) ...(10)
Power Via MDI                            : (See Detail) ...(11)
Link Aggregation                         : (See Detail) ...(12)
Maximum Frame Size                       : 1536 ...(13)
Link Fault                               : - ...(14)
LLDP-MED capabilities                    : (See Detail) ...(15)
Network Policy                           : (See Detail) ...(16)
Extended power via MDI                   : (See Detail) ...(17)
```

項番	説明
(1)	ポート番号を表示します。
(2)	Port ID TLV のサブタイプを表示します。 Local：Locally assigned(7) MAC Address：MAC address(3)
(3)	Port ID TLV のサブタイプが local 設定の場合は、ポート番号を表示します。Port ID TLV のサブタイプが mac-address 設定の場合は、対象ポートの MAC アドレスを表示します。
(4)	Port Description TLV で通知される、ポートの説明を表示します。

項番	説明
(5)	Port VLAN ID TLV で通知される、ポートの VLAN ID を表示します。
(6)	Management Address TLV で通知される、管理用 IP アドレスの数を表示します。
(7)	Port and Protocol VLAN ID（PPVID）TLV で通知される、プロトコル VLAN の数を表示します。
(8)	VLAN Name TLV で通知される、VLAN の数を表示します。
(9)	Protocol Identity TLV で通知される、プロトコルの数を表示します。
(10)	MAC/PHY Configuration/Status TLV で通知される情報は、詳細モードで確認します。
(11)	Power Via MDI TLV で通知される情報は、詳細モードで確認します。PoE 対応ポートでのみ表示されます。
(12)	Link Aggregation TLV で通知される情報は、詳細モードで確認します。
(13)	Maximum Frame Size TLV で通知される、最大フレームサイズを表示します。
(14)	LLDP 疑似リンクダウンに関する情報を表示します。 -：自装置側ポートは無効設定 Normal：自装置側ポートは正常状態 Fault：自装置側ポートは LLDP 疑似リンクダウン状態
(15)	LLDP-MED Capabilities TLV で通知される情報は、詳細モードで確認します。
(16)	LLDP-MED Network Policy TLV で通知される情報は、詳細モードで確認します。
(17)	LLDP-MED Extended Power-via-MDI TLV で通知される情報は、詳細モードで確認します。

使用例：隣接装置に通知する場合のポート 1/0/8 の物理ポート情報を、要約モードで表示する方法を示します。

```
# show lldp local interface port 1/0/8 brief

Port ID: Port1/0/8 ...(1)
------------------------------------------------------------------------------
Port ID Subtype                          : Local ...(2)
Port ID                                  : Port1/0/8 ...(3)
Port Description                         : APRESIA Systems, Ltd
                                           ApresiaNP2500-8MT4X-PoE HW A
                                           firmware 1.08.02 Port 8 on Unit 1 ...(4)
```

項番	説明
(1)	ポート番号を表示します。
(2)	Port ID TLV のサブタイプを表示します。 Local：Locally assigned(7) MAC Address：MAC address(3)
(3)	Port ID TLV のサブタイプが local 設定の場合は、ポート番号を表示します。Port ID TLV のサブタイプが mac-address 設定の場合は、対象ポートの MAC アドレスを表示します。
(4)	Port Description TLV で通知される、ポートの説明を表示します。

使用例：隣接装置に通知する場合のポート 1/0/8 の物理ポート情報を、詳細モードで表示する方法を示します。

```
# show lldp local interface port 1/0/8 detail
```

```
Port ID: Port1/0/8 ...(1)
------------------------------------------------------------------------------
Port ID Subtype                              : Local ...(2)
Port ID                                      : Port1/0/8 ...(3)
Port Description                             : APRESIA Systems, Ltd
                                               ApresiaNP2500-8MT4X-PoE HW A
                                               firmware 1.08.02 Port 8 on Unit 1 ...(4)
Port PVID                                    : 1 ...(5)
Management Address Count                     : 1 ...(6)

        Address 1 :
        Subtype                              : IPv4
        Address                              : 192.0.2.100
        IF Type                              : IfIndex
        OID                                  : 1.3.6.1.4.1.278.1.42.10

PPVID Entries Count                          : 0 ...(7)
    (None)
VLAN Name Entries Count                      : 2 ...(8)
    Entry 1 :
        VLAN ID                              : 1
        VLAN Name                            : default

    Entry 2 :
        VLAN ID                              : 10
        VLAN Name                            : VLAN0010

Protocol Identity Entries Count              : 0 ...(9)
    (None)
MAC/PHY Configuration/Status                 : ...(10)
    Auto-Negotiation Support                 : Supported
    Auto-Negotiation Enabled                 : Enabled
    Auto-Negotiation Advertised Capability   : 8c01(hex)
    Auto-Negotiation Operational MAU Type    : 001e(hex)

Power Via MDI                                : ...(11)
    Port Class                               : PSE
    PSE MDI Power Support                    : Supported
    PSE MDI Power State                      : Enabled
    PSE Pairs Control Ability                : Uncontrollable
    PSE Power Pair                           : 1
    Power Class                              : 0

Link Aggregation                             : ...(12)
    Aggregation Capability                   : Aggregated
    Aggregation Status                       : Not Currently in Aggregation
    Aggregation Port ID                      : 0

Maximum Frame Size                           : 1536 ...(13)

Link Fault                                   : - ...(14)

LLDP-MED Capabilities Support: ...(15)
    Capabilities              :Support
    Network Policy            :Support
    Location Identification   :Not Support
    Extended Power Via MDI PSE :Support
    Extended Power Via MDI PD  :Not Support
    Inventory                 :Support

Network Policy: ...(16)
  Application Type :Voice
    VLAN ID                       :0
```

```
    Priority                        :5
    DSCP                            :0
    Unknown                         :False
    Tagged                          :False

Extended Power Via MDI: ...(17)
    Power Priority                  :Low
    Power Value                     :15.40 Watts
```

項番	説明
(1)	ポート番号を表示します。
(2)	Port ID TLV のサブタイプを表示します。 Local：Locally assigned(7) MAC Address：MAC address(3)
(3)	Port ID TLV のサブタイプが local 設定の場合は、ポート番号を表示します。Port ID TLV のサブタイプが mac-address 設定の場合は、対象ポートの MAC アドレスを表示します。
(4)	Port Description TLV で通知される、ポートの説明を表示します。
(5)	Port VLAN ID TLV で通知される、ポートの VLAN ID を表示します。
(6)	Management Address TLV で通知される、管理用 IP アドレスの数と IP アドレス情報を表示します。0 個の場合は、IP アドレス情報は(None)と表示されます。
(7)	Port and Protocol VLAN ID (PPVID) TLV で通知される、プロトコル VLAN の数と VLAN 情報を表示します。0 個の場合は、VLAN 情報は(None)と表示されます。
(8)	VLAN Name TLV で通知される、VLAN の数と VLAN 情報を表示します。
(9)	Protocol Identity TLV で通知される、プロトコルの数とプロトコル情報を表示します。0 個の場合は、プロトコル情報は(None)と表示されます。
(10)	MAC/PHY Configuration/Status TLV で通知される情報を表示します。
(11)	Power Via MDI TLV で通知される情報を表示します。PoE 対応ポートでのみ表示されます。
(12)	Link Aggregation TLV で通知される情報を表示します。
(13)	Maximum Frame Size TLV で通知される、最大フレームサイズを表示します。
(14)	LLDP 疑似リンクダウンに関する情報を表示します。 -：自装置側ポートは無効設定 Normal：自装置側ポートは正常状態 Fault：自装置側ポートは LLDP 疑似リンクダウン状態
(15)	LLDP-MED Capabilities TLV で通知される情報を表示します。
(16)	LLDP-MED Network Policy TLV で通知される情報を表示します。
(17)	LLDP-MED Extended Power-via-MDI TLV で通知される情報を表示します。

4.14.24 show lldp management-address

show lldp management-address	
目的	Management Address TLV で通知する管理用アドレス情報を表示します。
Command	show lldp management-address [IP-ADDRESS | IPV6-ADDRESS]
Parameter	IP-ADDRESS (省略可能)：表示する管理用 IPv4 アドレスを指定します。 IPV6-ADDRESS (省略可能)：表示する管理用 IPv6 アドレスを指定します。

show lldp management-address	
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべての管理用アドレス情報を表示する方法を示します。

```
# show lldp management-address

Address 1 : (default)
-----------------------------------------------
    Subtype                                 : IPv4 ...(1)
    Address                                 : 192.0.2.100 ...(2)
    IF Type                                 : IfIndex ...(3)
    OID                                     : 1.3.6.1.4.1.278.1.42.10 ...(4)
    Advertising Ports                       : - ...(5)

Address 2 :
-----------------------------------------------
    Subtype                                 : IPv4
    Address                                 : 192.0.2.100
    IF Type                                 : IfIndex
    OID                                     : 1.3.6.1.4.1.278.1.42.10
    Advertising Ports                       :
      Port1/0/1,Port1/0/5

Total Entries: 2
```

項番	説明
(1)	管理用アドレスのサブタイプ（IPv4／IPv6）を表示します。
(2)	管理用アドレスを表示します。
(3)	管理用アドレスのインターフェースタイプを表示します。
(4)	管理用アドレスの装置を判別する OID を表示します。
(5)	対象の管理用アドレスを Management Address TLV で通知するポート番号を表示します。

4.14.25 show lldp neighbors interface

show lldp neighbors interface	
目的	隣接装置の LLDP 情報を表示します。
Command	show lldp neighbors interface port PORTS [brief | detail]
Parameter	port PORTS：物理ポートを指定します。複数指定できます。 brief（省略可能）：情報を要約モードで表示します。 detail（省略可能）：情報を詳細モードで表示します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-

show lldp neighbors interface	
バージョン	1.08.02

使用例：ポート 1/0/5 で学習した隣接装置の LLDP 情報を、標準モードで表示する方法を示します。

```
# show lldp neighbors interface port 1/0/5

Port ID: Port1/0/5 ...(1)
------------------------------------------------------------------------------
Remote Entities Count : 1 ...(2)
Entity 1 ...(3)
    Chassis ID Subtype                      : MAC Address ...(4)
    Chassis ID                              : 00-40-66-AC-2C-90 ...(5)
    Port ID Subtype                         : Local ...(6)
    Port ID                                 : Port1/0/20 ...(7)
    Port Description                        : APRESIA Systems, Ltd ApresiaNP5
                                              000-48T4X HW A firmware 1.05.01
                                               Port 20 on Unit 1 ...(8)
    System Name                             : Test-NP5000 ...(9)
    System Description                      : ApresiaNP5000-48T4X Gigabit Eth
                                              ernet Switch Ver.1.05.01 ...(10)
    System Capabilities                     : Bridge, Router ...(11)
    Management Address Count                : 1 ...(12)
    Port PVID                               : 0 ...(13)
    PPVID Entries Count                     : 0 ...(14)
    VLAN Name Entries Count                 : 2 ...(15)
    Protocol ID Entries Count               : 0 ...(16)
    MAC/PHY Configuration/Status            : (None) ...(17)
    Power Via MDI                           : (None) ...(18)
    Link Aggregation                        : (None) ...(19)
    Maximum Frame Size                      : 1536 ...(20)
    Link Fault                              : - ...(21)
    LLDP-MED capabilities                   : (See Detail) ...(22)
    Extended power via MDI                  : (See Detail) ...(23)
    Network policy                          : (See Detail) ...(24)
    Inventory Management                    : (See Detail) ...(25)
    Unknown TLVs Count                      : 0 ...(26)
```

項番	説明
(1)	自装置のポート番号を表示します。
(2)	登録された隣接装置の数を表示します。
(3)	登録番号を表示します。
(4)	隣接装置から通知された、Chassis ID TLV のサブタイプを表示します。
(5)	隣接装置から Chassis ID TLV で通知された、Chassis ID 情報を表示します。
(6)	隣接装置から通知された、Port ID TLV のサブタイプを表示します。
(7)	隣接装置から Port ID TLV で通知された、Port ID 情報を表示します。
(8)	隣接装置から Port Description TLV で通知された、ポートの説明を表示します。
(9)	隣接装置から System Name TLV で通知された、システム名を表示します。
(10)	隣接装置から System Description TLV で通知された、システムの説明を表示します。
(11)	隣接装置から System Capabilities TLV で通知された、システムの利用可能な能力を表示します。
(12)	隣接装置から Management Address TLV で通知された、管理用 IP アドレスの数を表示します。

項番	説明
(13)	隣接装置から Port VLAN ID TLV で通知された、ポートの VLAN ID を表示します。
(14)	隣接装置から Port and Protocol VLAN ID（PPVID）TLV で通知された、プロトコル VLAN の数を表示します。
(15)	隣接装置から VLAN Name TLV で通知された、VLAN の数を表示します。
(16)	隣接装置から Protocol Identity TLV で通知された、プロトコルの数を表示します。
(17)	隣接装置から MAC/PHY Configuration/Status TLV で通知された情報は、詳細モードで確認します。
(18)	隣接装置から Power Via MDI TLV で通知された情報は、詳細モードで確認します。
(19)	隣接装置から Link Aggregation TLV で通知された情報は、詳細モードで確認します。
(20)	隣接装置から Maximum Frame Size TLV で通知された、最大フレームサイズを表示します。
(21)	隣接装置からベンダー独自の Link Fault TLV で通知された、LLDP 疑似リンクダウンに関する情報を表示します。 -：隣接装置側ポートは無効設定 Normal：隣接装置側ポートは正常状態 Fault：隣接装置側ポートは LLDP 疑似リンクダウン状態
(22)	隣接装置から LLDP-MED Capabilities TLV で通知された情報は、詳細モードで確認します。
(23)	隣接装置から LLDP-MED Extended Power-via-MDI TLV で通知された情報は、詳細モードで確認します。
(24)	隣接装置から LLDP-MED Network Policy TLV で通知された情報は、詳細モードで確認します。
(25)	隣接装置から LLDP-MED Inventory Management TLV で通知された情報は、詳細モードで確認します。
(26)	隣接装置から通知された、未知の TLV の数を表示します。

使用例：ポート 1/0/5 で学習した隣接装置の LLDP 情報を、要約モードで表示する方法を示します。

```
# show lldp neighbors interface port 1/0/5 brief

Port ID: Port1/0/5 ...(1)
------------------------------------------------------------------------------
Remote Entities Count : 1 ...(2)
Entity 1 ...(3)
    Chassis ID Subtype                          : MAC Address ...(4)
    Chassis ID                                  : 00-40-66-AC-2C-90 ...(5)
    Port ID Subtype                             : Local ...(6)
    Port ID                                     : Port1/0/20 ...(7)
    Port Description                            : APRESIA Systems, Ltd ApresiaNP5
                                                  000-48T4X HW A firmware 1.05.01
                                                   Port 20 on Unit 1 ...(8)
```

項番	説明
(1)	自装置のポート番号を表示します。
(2)	登録された隣接装置の数を表示します。
(3)	登録番号を表示します。

項番	説明
(4)	隣接装置から通知された、Chassis ID TLV のサブタイプを表示します。
(5)	隣接装置から Chassis ID TLV で通知された、Chassis ID 情報を表示します。
(6)	隣接装置から通知された、Port ID TLV のサブタイプを表示します。
(7)	隣接装置から Port ID TLV で通知された、Port ID 情報を表示します。
(8)	隣接装置から Port Description TLV で通知された、ポートの説明を表示します。

使用例：ポート 1/0/5 で学習した隣接装置の LLDP 情報を、詳細モードで表示する方法を示します。

```
# show lldp neighbors interface port 1/0/5 detail

Port ID: Port1/0/5 ...(1)
------------------------------------------------------------------------------
Remote Entities Count : 1 ...(2)
Entity 1 ...(3)
    Chassis ID Subtype                          : MAC Address ...(4)
    Chassis ID                                  : 00-40-66-AC-2C-90 ...(5)
    Port ID Subtype                             : Local ...(6)
    Port ID                                     : Port1/0/20 ...(7)
    Port Description                            : APRESIA Systems, Ltd ApresiaNP5
                                                  000-48T4X HW A firmware 1.05.01
                                                   Port 20 on Unit 1 ...(8)
    System Name                                 : Test-NP5000 ...(9)
    System Description                          : ApresiaNP5000-48T4X Gigabit Eth
                                                  ernet Switch Ver.1.05.01 ...(10)
    System Capabilities                         : Bridge, Router ...(11)
    Management Address Count                    : 1 ...(12)
        Entry 1 :
            Subtype                             : IPv4
            Address                             : 192.168.10.100
            IF Type                             : IfIndex
            OID                                 : 1.3.6.1.4.1.278.1.42.2.0


    Port PVID                                   : 0 ...(13)
    PPVID Entries Count                         : 0 ...(14)
        (None)

    VLAN Name Entries Count                     : 2 ...(15)
        Entry 1 :
            VLAN ID                             : 1
            VLAN Name                           : default
        Entry 2 :
            VLAN ID                             : 10
            VLAN Name                           : Test-VLAN10

    Protocol ID Entries Count                   : 0 ...(16)
        (None)

    MAC/PHY Configuration/Status                : (None) ...(17)
    Power Via MDI                               : (None) ...(18)
    Link Aggregation                            : (None) ...(19)
    Maximum Frame Size                          : 1536 ...(20)
    Link Fault                                  : - ...(21)
    Unknown TLVs Count                          : 0 ...(22)
        (None)

        LLDP-MED Capabilities Enabled: ...(23)
            Capabilities                  : Not Support
            Network Policy                : Not Support
```

```
            Location Identification         : Not Support
            Extended Power Via MDI          : Not Support
            Inventory                       : Not Support


    Inventory Management: ...(24)
        None
```

項番	説明
(1)	自装置のポート番号を表示します。
(2)	登録された隣接装置の数を表示します。
(3)	登録番号を表示します。
(4)	隣接装置から通知された、Chassis ID TLV のサブタイプを表示します。
(5)	隣接装置から Chassis ID TLV で通知された、Chassis ID 情報を表示します。
(6)	隣接装置から通知された、Port ID TLV のサブタイプを表示します。
(7)	隣接装置から Port ID TLV で通知された、Port ID 情報を表示します。
(8)	隣接装置から Port Description TLV で通知された、ポートの説明を表示します。
(9)	隣接装置から System Name TLV で通知された、システム名を表示します。
(10)	隣接装置から System Description TLV で通知された、システムの説明を表示します。
(11)	隣接装置から System Capabilities TLV で通知された、システムの利用可能な能力を表示します。
(12)	隣接装置から Management Address TLV で通知された、管理用 IP アドレスの数と IP アドレス情報を表示します。0 個の場合は、IP アドレス情報は(None)と表示されます。
(13)	隣接装置から Port VLAN ID TLV で通知された、ポートの VLAN ID を表示します。
(14)	隣接装置から Port and Protocol VLAN ID（PPVID）TLV で通知された、プロトコル VLAN の数と VLAN 情報を表示します。0 個の場合は、VLAN 情報は(None)と表示されます。
(15)	隣接装置から VLAN Name TLV で通知された、VLAN の数と VLAN 情報を表示します。0 個の場合は、VLAN 情報は(None)と表示されます。
(16)	隣接装置から Protocol Identity TLV で通知された、プロトコルの数とプロトコル情報を表示します。0 個の場合は、プロトコル情報は(None)と表示されます。
(17)	隣接装置から MAC/PHY Configuration/Status TLV で通知された情報を表示します。
(18)	隣接装置から Power Via MDI TLV で通知された情報を表示します。
(19)	隣接装置から Link Aggregation TLV で通知された情報を表示します。
(20)	隣接装置から Maximum Frame Size TLV で通知された、最大フレームサイズを表示します。
(21)	隣接装置からベンダー独自の Link Fault TLV で通知された、LLDP 疑似リンクダウンに関する情報を表示します。 -：隣接装置側ポートは無効設定 Normal：隣接装置側ポートは正常状態 Fault：隣接装置側ポートは LLDP 疑似リンクダウン状態
(22)	隣接装置から通知された、未知の TLV の数と TLV 情報を表示します。
(23)	隣接装置から LLDP-MED Capabilities TLV で通知された情報を表示します。
(24)	隣接装置から LLDP-MED Inventory Management TLV で通知された情報を表示します。

4.14.26 show lldp traffic

show lldp traffic	
目的	グローバルな LLDP 統計情報を表示します。
Command	show lldp traffic
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：グローバルな LLDP 統計情報を表示する方法を示します。

```
# show lldp traffic

Last Change Time  : 293034 ...(1)
Total Inserts     : 3 ...(2)
Total Deletes     : 0 ...(3)
Total Drops       : 0 ...(4)
Total Ageouts     : 2 ...(5)
```

項番	説明
(1)	lldpStatsRemTablesLastChangeTime の MIB の値（sysUpTime）を表示します。
(2)	LLDP テーブルに登録した回数を表示します。
(3)	クリアコマンドや、TTL 値が 0 秒の LLDPDU を受信して LLDP テーブルから削除した回数を表示します。
(4)	リソース不足のため、LLDP テーブルに登録されなかった回数を表示します。
(5)	TTL expired により LLDP テーブルから削除された回数を表示します。

4.14.27 show lldp traffic interface

show lldp traffic interface	
目的	ポートの LLDP 統計情報を表示します。
Command	show lldp traffic interface port PORTS
Parameter	port PORTS：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の LLDP 統計情報を表示する方法を示します。

```
# show lldp traffic interface port 1/0/1

Port ID : Port1/0/1 ...(1)
```

```
-------------------------------------------
    Total Transmits      : 0 ...(2)
    Total Discards       : 0 ...(3)
    Total Errors         : 0 ...(4)
    Total Receives       : 0 ...(5)
    Total TLV Discards   : 0 ...(6)
    Total TLV Unknowns   : 0 ...(7)
    Total Ageouts        : 0 ...(8)
```

項番	説明
(1)	ポート番号を表示します。
(2)	送信した LLDPDU の数を表示します。
(3)	廃棄した LLDPDU の数を表示します。
(4)	受信した無効な LLDPDU の数を表示します。
(5)	受信した LLDPDU の数を表示します。
(6)	廃棄した情報 (TLV) の数を表示します。
(7)	受信した未知の情報 (TLV) の数を表示します。
(8)	TTL expired により LLDP テーブルから削除された回数を表示します。

4.14.28 clear lldp table

clear lldp table	
目的	LLDP テーブルに登録された隣接装置の LLDP 情報を削除します。
Command	clear lldp table {all | interface port PORTS}
Parameter	all：すべてのポートの LLDP 情報を削除する場合に指定します。 interface port PORTS：LLDP 情報を削除する物理ポートを指定します。複数指定できます。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべてのポートの LLDP 情報を削除する方法を示します。

```
# clear lldp table all
#
```

4.14.29 clear lldp counters

clear lldp counters	
目的	LLDP 統計情報を消去します。
Command	clear lldp counters [all | interface port PORTS]
Parameter	all（省略可能）：すべてのポートの LLDP 統計情報、およびグローバルな LLDP 統計情報を消去する場合に指定します。 interface port PORTS（省略可能）：LLDP 統計情報を消去する物理ポートを指定します。複数指定できます。

clear lldp counters	
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	パラメーター省略時は、グローバルな LLDP 統計情報のみが消去されます。
制限・注意	-
バージョン	1.08.02

使用例：すべてのポートの LLDP 統計情報、およびグローバルな LLDP 統計情報を消去する方法を示します。

```
# clear lldp counters all
#
```

4.15 Ethernet OAM コマンド

Ethernet OAM 関連の設定コマンドは以下のとおりです。

- ethernet oam
- ethernet oam mode
- ethernet oam link-monitor error-symbol
- ethernet oam link-monitor error-frame
- ethernet oam link-monitor error-frame-period
- ethernet oam link-monitor error-frame-seconds
- ethernet oam remote-failure critical-event

Ethernet OAM 関連の show／操作コマンドは以下のとおりです。

- show ethernet oam configuration
- show ethernet oam status
- show ethernet oam statistics
- show ethernet oam event-log
- clear ethernet oam statistics
- clear ethernet oam event-log
- ethernet oam remote-loopback start / stop
- ethernet oam received-remote-loopback

4.15.1 ethernet oam

ethernet oam	
目的	Ethernet OAM を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ethernet oam no ethernet oam
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	アクティブモードの場合は、Ethernet OAM を有効にすると自ら Information OAMPDU を送信して OAM ディスカバリー処理を開始します。対向ポートはアクティブモード、またはパッシブモードで設定します。 パッシブモードの場合は、Ethernet OAM を有効にしても自らは Information OAMPDU を送信せずに、対向ポートからの Information OAMPDU を受信するまで待機します。対向ポートから Information OAMPDU を受信すると、OAM ディスカバリー処理を開始します。対向ポートはアクティブモードで設定します。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で Ethernet OAM を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
```

```
(config-if-port)# ethernet oam
(config-if-port)#
```

4.15.2 ethernet oam mode

ethernet oam mode	
目的	Ethernet OAM の動作モードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ethernet oam mode {active | passive} no ethernet oam mode
Parameter	active：アクティブモードに設定する場合に指定します。 passive：パッシブモードに設定する場合に指定します。
デフォルト	アクティブモード（ethernet oam mode active）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	アクティブモードのインターフェースでは以下の 2 つのアクションが許可されます。パッシブモードのインターフェースでは許可されません。 • Ethernet OAM ディスカバリー処理の開始 • リモートループバックの開始要求／停止要求の送信（ethernet oam remote-loopback start / stop）
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の Ethernet OAM の動作モードをアクティブモードに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ethernet oam mode active
(config-if-port)#
```

4.15.3 ethernet oam link-monitor error-symbol

ethernet oam link-monitor error-symbol	
目的	Errored Symbol Period イベントの有効／無効、しきい値と監視ウィンドウを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ethernet oam link-monitor error-symbol [threshold VALUE] [window VALUE] no ethernet oam link-monitor error-symbol [threshold | window]
Parameter	threshold VALUE（省略可能）：しきい値として設定するシンボルエラー数を 0～4,294,967,295 の範囲で指定します。 window VALUE（省略可能）：しきい値を定義する対象の期間を 10～600（100 ミリ秒単位：1～60 秒）の範囲で指定します。
デフォルト	Errored Symbol Period イベントは有効 （ethernet oam link-monitor error-symbol） しきい値：1、監視ウィンドウ：10（1 秒） （ethernet oam link-monitor error-symbol threshold 1 window 10）
モード	インターフェース設定モード(port, range)

ethernet oam link-monitor error-symbol	
特権レベル	レベル：12
ガイドライン	Errored Symbol Period イベントの有効／無効を設定するには、パラメーターを指定しないコマンド形式で実施します。Errored Symbol Period イベントが有効な場合、しきい値としてシンボルエラー数を監視します。 監視ウィンドウで指定した期間中に発生したシンボルエラー数がしきい値を超えた場合に、Errored Symbol Period イベントが記録され、Errored Symbol Period Event TLV を含む Event Notification OAMPDU が送信されます。
制限・注意	• Errored Symbol Period イベントの有効／無効設定と、しきい値と監視ウィンドウのパラメーター設定は、構成情報では別に表示されます。デフォルト設定に戻す場合は、それぞれの no 形式のコマンドを実行してください。
バージョン	1.08.02

使用例：ポート 1/0/1 で Errored Symbol Period イベントを無効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# no ethernet oam link-monitor error-symbol
(config-if-port)#
```

使用例：ポート 1/0/1 の Errored Symbol Period イベントのしきい値を 100 に、監視ウィンドウを 300（30 秒）に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ethernet oam link-monitor error-symbol threshold 100 window 300
(config-if-port)#
```

4.15.4 ethernet oam link-monitor error-frame

ethernet oam link-monitor error-frame	
目的	Errored Frame イベントの有効／無効、しきい値と監視ウィンドウを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ethernet oam link-monitor error-frame [threshold VALUE] [window VALUE] no ethernet oam link-monitor error-frame [threshold | window]
Parameter	threshold VALUE（省略可能）：しきい値として設定するエラーフレーム数を 0～4,294,967,295 の範囲で指定します。 window VALUE（省略可能）：しきい値を定義する対象の期間を 10～600（100 ミリ秒単位：1～60 秒）の範囲で指定します。
デフォルト	Errored Frame イベントは有効 （ethernet oam link-monitor error-frame） しきい値：1、監視ウィンドウ：10（1 秒） （ethernet oam link-monitor error-frame threshold 1 window 10）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	Errored Frame イベントの有効／無効を設定するには、パラメーターを指定しないコマンド形式で実施します。Errored Frame イベントが有効な場合、しきい値としてエラーフレーム数を監視します。

ethernet oam link-monitor error-frame	
	監視ウィンドウで指定した期間中に発生したエラーフレーム数がしきい値を超えた場合に、Errored Frame イベントが記録され、Errored Frame Event TLV を含む Event Notification OAMPDU が送信されます。
制限・注意	• Errored Frame イベントの有効／無効設定と、しきい値と監視ウィンドウのパラメーター設定は、構成情報では別に表示されます。デフォルト設定に戻す場合は、それぞれの no 形式のコマンドを実行してください。
バージョン	1.08.02

使用例：ポート 1/0/1 で Errored Frame イベントを無効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# no ethernet oam link-monitor error-frame
(config-if-port)#
```

使用例：ポート 1/0/1 の Errored Frame イベントのしきい値を 100 に、監視ウィンドウを 300（30 秒）に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ethernet oam link-monitor error-frame threshold 100 window 300
(config-if-port)#
```

4.15.5 ethernet oam link-monitor error-frame-period

ethernet oam link-monitor error-frame-period	
目的	Errored Frame Period イベントの有効／無効、しきい値と監視ウィンドウを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ethernet oam link-monitor error-frame-period [threshold VALUE] [window VALUE] no ethernet oam link-monitor error-frame-period [threshold | window]
Parameter	threshold VALUE（省略可能）：しきい値として設定するエラーフレーム数を 0～4,294,967,295 の範囲で指定します。 window VALUE（省略可能）：しきい値を定義する対象のフレーム数を指定します。設定範囲は、「下位の物理レイヤーで 100 ミリ秒の間に受信できる最小フレームサイズのフレーム数」～「下位の物理レイヤーで 1 分間に受信できる最小フレームサイズのフレーム数」です。
デフォルト	Errored Frame Period イベントは有効 （ethernet oam link-monitor error-frame-period） しきい値：1，監視ウィンドウ：下位の物理レイヤーで 1 秒間に受信できる最小フレームサイズのフレーム数
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	Errored Frame Period イベントの有効／無効を設定するには、パラメーターを指定しないコマンド形式で実施します。Errored Frame Period イベントが有効な場合、しきい値としてエラーフレーム数を監視します。 監視ウィンドウで指定したフレーム数を受信する間に発生したエラーフレーム数がしきい値を超えた場合に、Errored Frame Period イベントが記録され、Errored

ethernet oam link-monitor error-frame-period	
	Frame Period Event TLV を含む Event Notification OAMPDU が送信されます。
制限・注意	• Errored Frame Period イベントの有効／無効設定と、しきい値と監視ウィンドウのパラメーター設定は、構成情報では別に表示されます。デフォルト設定に戻す場合は、それぞれの no 形式のコマンドを実行してください。
バージョン	1.08.02

使用例：ポート 1/0/1 で Errored Frame Period イベントを無効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# no ethernet oam link-monitor error-frame-period
(config-if-port)#
```

使用例：ポート 1/0/1 の Errored Frame Period イベントのしきい値を 100 に、監視ウィンドウを 1488100 フレームに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ethernet oam link-monitor error-frame-period threshold 100 window
1488100
(config-if-port)#
```

4.15.6 ethernet oam link-monitor error-frame-seconds

ethernet oam link-monitor error-frame-seconds	
目的	Errored Frame Seconds Summary イベントの有効／無効、しきい値と監視ウィンドウを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ethernet oam link-monitor error-frame-seconds [threshold VALUE] [window VALUE] no ethernet oam link-monitor error-frame-seconds [threshold | window]
Parameter	threshold VALUE（省略可能）：しきい値として設定する、エラーフレームを検出した秒数を、1～900 秒の範囲で指定します。 window VALUE（省略可能）：しきい値を定義する対象の期間を 100～9000（100 ミリ秒単位：10～900 秒）の範囲で指定します。
デフォルト	Errored Frame Seconds Summary イベントは有効 （ethernet oam link-monitor error-frame-seconds） しきい値：1、監視ウィンドウ：600（60 秒） （ethernet oam link-monitor error-frame-seconds threshold 1 window 600）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	Errored Frame Seconds Summary イベントの有効／無効を設定するには、パラメーターを指定しないコマンド形式で実施します。Errored Frame Seconds Summary イベントが有効な場合、1 秒以内に少なくとも 1 個のエラーフレームを検出したことがある秒数を監視します。 監視ウィンドウで指定した期間中に「エラーフレームを検出した秒数」がしきい値を超えた場合に、Errored Frame Seconds Summary イベントが記録され、Errored Frame Seconds Summary Event TLV を含む Event Notification OAMPDU が送信されます。

ethernet oam link-monitor error-frame-seconds	
制限・注意	• Errored Frame Seconds Summary イベントの有効／無効設定と、しきい値と監視ウィンドウのパラメーター設定は、構成情報では別に表示されます。デフォルト設定に戻す場合は、それぞれの no 形式のコマンドを実行してください。
バージョン	1.08.02

使用例：ポート 1/0/1 で Errored Frame Seconds Summary イベントを無効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# no ethernet oam link-monitor error-frame-seconds
(config-if-port)#
```

使用例：ポート 1/0/1 の Errored Frame Seconds Summary イベントのしきい値を 60 に、監視ウィンドウを 6000（600 秒）に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ethernet oam link-monitor error-frame-seconds threshold 60 window 6000
(config-if-port)#
```

4.15.7 ethernet oam remote-failure critical-event

ethernet oam remote-failure critical-event	
目的	指定したインターフェースでクリティカルイベントの通知を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ethernet oam remote-failure critical-event no ethernet oam remote-failure critical-event
Parameter	なし
デフォルト	有効（ethernet oam remote-failure critical-event）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	クリティカルイベントの通知を有効にすると以下コマンド操作時にクリティカルイベントが記録されて、Critical Event ビットがセットされた OAMPDU を送信します。 • 対象ポートで shutdown コマンドを設定した場合 • 対象ポートで Ethernet OAM を無効（no ethernet oam）に変更した場合
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 でクリティカルイベントの通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ethernet oam remote-failure critical-event
(config-if-port)#
```

4.15.8 show ethernet oam configuration

show ethernet oam configuration	
目的	Ethernet OAM の設定を表示します。
Command	show ethernet oam configuration [interface port PORTS]

show ethernet oam configuration	
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の Ethernet OAM の設定を表示する方法を示します。

```
# show ethernet oam configuration interface port 1/0/1

Port1/0/1 ...(1)
------------------------------------------------------------
OAM                       : Disabled ...(2)
Mode                      : Active ...(3)
Dying Gasp                : Enabled ...(4)
Critical Event            : Enabled ...(5)
Remote Loopback OAMPDU    : Not Processed ...(6)

Symbol Error ...(7)
  Notify State            : Enabled ...(8)
  Window                  : 10 deciseconds ...(9)
  Threshold               : 1 Error Symbol ...(10)

Frame Error ...(11)
  Notify State            : Enabled
  Window                  : 10 deciseconds
  Threshold               : 1 Error Frame

Frame Period Error ...(12)
  Notify State            : Enabled
  Window                  : 1488100 Frames
  Threshold               : 1 Error Frame

Frame Seconds Error ...(13)
  Notify State            : Enabled
  Window                  : 600 deciseconds
  Threshold               : 1 Error Seconds
```

項番	説明
(1)	ポート番号を表示します。
(2)	Ethernet OAM の有効(Enabled)／無効(Disabled)を表示します。
(3)	Ethernet OAM の動作モード（Active：アクティブモード／Passive：パッシブモード）を表示します。
(4)	Dying Gasp イベント通知の有効(Enabled)／無効(Disabled)を表示します。
(5)	クリティカルイベント通知の有効(Enabled)／無効(Disabled)を表示します。
(6)	ピアから受信したリモートループバック設定要求の処理方法を表示します。 Processed：リモートループバックモード設定要求を処理する Not Processed：リモートループバックモード設定要求を無視する
(7)	Errored Symbol Period イベントに関する情報を表示します。
(8)	イベントの有効(Enabled)／無効(Disabled)を表示します。

項番	説明
(9)	対象イベントの監視ウィンドウの設定値を表示します。
(10)	対象イベントのしきい値を表示します。
(11)	Errored Frame イベントに関する情報を表示します。
(12)	Errored Frame Period イベントに関する情報を表示します。
(13)	Errored Frame Seconds Summary イベントに関する情報を表示します。

4.15.9 show ethernet oam status

show ethernet oam status	
目的	Ethernet OAM の状態を表示します。
Command	show ethernet oam status [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の Ethernet OAM の状態を表示する方法を示します。

```
# show ethernet oam status interface port 1/0/1

Port1/0/1 ...(1)
  Local client ...(2)
    Admin state                   : Enabled ...(3)
    Mode                          : Active ...(4)
    Max OAMPDU size               : 1518 bytes ...(5)
    Remote loopback               : Supported ...(6)
    Unidirectional                : Not supported ...(7)
    Link monitoring               : Supported ...(8)
    Variable request              : Not supported ...(9)
    PDU revision                  : 0 ...(10)
    Operation status              : Operational ...(11)
    Loopback status               : No loopback ...(12)

  Remote client ...(13)
    Mode                          : Active
    MAC address                   : 0040.66AA.56AC ...(14)
    Vendor (OUI)                  : 004066 ...(15)
    Max OAMPDU size               : 1518 bytes
    Unidirection                  : Not supported
    Link monitoring               : Supported
    Variable request              : Not supported
    PDU revision                  : 0
```

項番	説明
(1)	ポート番号を表示します。
(2)	自装置側の情報を表示します。
(3)	Ethernet OAM の有効(Enabled)／無効(Disabled)を表示します。
(4)	Ethernet OAM の動作モード（Active：アクティブモード／Passive：パッシブモード）を表

項番	説明
	示します。
(5)	OAMPDU の最大サイズを表示します。
(6)	ループバックモードの対応状況(Supported／Not supported)を表示します。
(7)	単方向リンクでの OAMPDU 送信の対応状況(Supported／Not supported)を表示します。
(8)	Event Notification 送受信の対応状況(Supported／Not supported)を表示します。
(9)	Variable Request 送受信の対応状況(Supported／Not supported)を表示します。
(10)	OAMPDU のリビジョンを表示します。
(11)	Ethernet OAM の状態を表示します。 Disable：Ethernet OAM が無効 LinkFault：リンク障害を検出 PassiveWait：パッシブモードのポートでピアが Ethernet OAM に対応しているか確認中 ActiveSendLocal：アクティブモードのポートでローカル情報を送信中 SendLocalAndRemote：ピアを検出済み（設定待ち） SendLocalAndRemoteOk：ピアを検出済み（設定済み） PeeringLocallyRejected：ローカル OAM エンティティーはピアを拒否 PeeringRemotelyRejected：リモート OAM エンティティーはローカル装置を拒否 Operational：Ethernet OAM を利用可能（ローカル装置とピアの両方が接続を受け入れ） NonOperHalfDuplex：ポートが半二重ポートのため不完全動作
(12)	ポートのループバック状態を表示します。 No loopback：非ループバック状態 Local loopback：自装置側のポートがループバック状態 Remote loopback：隣接装置側のポートがループバック状態
(13)	隣接装置側の情報を表示します。
(14)	MAC アドレスを表示します。
(15)	MAC アドレスのベンダー識別子を表示します。

4.15.10 show ethernet oam statistics

show ethernet oam statistics	
目的	Ethernet OAM の統計情報を表示します。
Command	show ethernet oam statistics [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の Ethernet OAM の統計情報を表示する方法を示します。

```
# show ethernet oam statistics interface port 1/0/1

Port1/0/1 ...(1)
-------------------------------------------------------------
```

```
  Information OAMPDU TX                  : 0 ...(2)
  Information OAMPDU RX                  : 0 ...(3)
  Unique Event Notification OAMPDU TX    : 0 ...(4)
  Unique Event Notification OAMPDU RX    : 0 ...(5)
  Duplicate Event Notification OAMPDU TX: 0 ...(6)
  Duplicate Event Notification OAMPDU RX: 0 ...(7)
  Loopback Control OAMPDU TX             : 0 ...(8)
  Loopback Control OAMPDU RX             : 0 ...(9)
  Variable Request OAMPDU TX             : 0 ...(10)
  Variable Request OAMPDU RX             : 0 ...(11)
  Variable Response OAMPDU TX            : 0 ...(12)
  Variable Response OAMPDU RX            : 0 ...(13)
  Organization Specific OAMPDUs TX       : 0 ...(14)
  Organization Specific OAMPDUs RX       : 0 ...(15)
  Unsupported OAMPDU TX                  : 0 ...(16)
  Unsupported OAMPDU RX                  : 0 ...(17)
  Frames Lost Due To OAM                 : 0 ...(18)
```

項番	説明
(1)	ポート番号を表示します。
(2)	Information OAMPDU の送信数を表示します。
(3)	Information OAMPDU の受信数を表示します。
(4)	Unique Event Notification OAMPDU の送信数を表示します。
(5)	Unique Event Notification OAMPDU の受信数を表示します。
(6)	Duplicate Event Notification OAMPDU の送信数を表示します。
(7)	Duplicate Event Notification OAMPDU の受信数を表示します。
(8)	Loopback Control OAMPDU の送信数を表示します。
(9)	Loopback Control OAMPDU の受信数を表示します。
(10)	Variable Request OAMPDU の送信数を表示します。
(11)	Variable Request OAMPDU の受信数を表示します。
(12)	Variable Response OAMPDU の送信数を表示します。
(13)	Variable Response OAMPDU の受信数を表示します。
(14)	Organization Specific OAMPDU の送信数を表示します。
(15)	Organization Specific OAMPDU の受信数を表示します。
(16)	非対応な OAMPDU の送信数を表示します。
(17)	非対応な OAMPDU の受信数を表示します。
(18)	Ethernet OAM によって廃棄されたフレーム数を表示します。

4.15.11 show ethernet oam event-log

show ethernet oam event-log	
目的	Ethernet OAM のイベントログを表示します。
Command	show ethernet oam event-log [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。

show ethernet oam event-log	
制限・注意	• イベントログは装置全体で 1000 個まで記録されます。1000 個を超えた場合は、一番古いイベントログから上書きされます。
バージョン	1.08.02

使用例：ポート 1/0/1 の Ethernet OAM のイベントログを表示する方法を示します。

```
# show ethernet oam event-log interface port 1/0/1

Port1/0/1 ...(1)
    Local Faults: ...(2)
    -------------
      0 Link Fault records ...(3)
      0 Dying Gasp records ...(4)
      0 Critical Event records ...(5)

    Remote Faults: ...(6)
    -------------
      0 Link Fault records
      0 Dying Gasp records
      1 Critical Event records
         Event index : 1 ...(7)
         Time stamp  : 2022-07-07 11:14 ...(8)


    Local event logs: ...(9)
    -------------
      0 Errored Symbol records ...(10)
      1 Errored Frame records ...(11)
         Event index         : 2
         Time stamp          : 2022-07-07 11:20
         Error frame/symbol  : 542 ...(12)
         Window              : 1000 (millisecond) ...(13)
         Threshold           : 1 ...(14)
         Accumulated errors  : 542 ...(15)

      0 Errored Frame Period records ...(16)
      1 Errored Frame Second records ...(17)
         Event index         : 3
         Time stamp          : 2022-07-07 11:20
         Error frame/symbol  : 1
         Window              : 60000 (millisecond)
         Threshold           : 1
         Accumulated errors  : 1


    Remote event logs: ...(18)
    -------------
      0 Errored Symbol records
      0 Errored Frame records
      0 Errored Frame Period records
      0 Errored Frame Second records
```

項番	説明
(1)	ポート番号を表示します。
(2)	自装置側で生成した Fault イベントの情報を表示します。
(3)	リンク障害のイベントログ数を表示します。
(4)	Dying Gasp のイベントログ数を表示します。

項番	説明
(5)	クリティカルイベントのログ数を表示します。
(6)	隣接装置側で生成した Fault イベントの情報を表示します。
(7)	イベントログ番号を表示します。
(8)	イベント発生時のタイムスタンプを表示します。
(9)	自装置側で生成したイベントログの情報を表示します。
(10)	Errored Symbol Period イベントログの数を表示します。
(11)	Errored Frame イベントログの数を表示します。
(12)	しきい値を比較する値（シンボルエラー数、エラーフレーム数、エラーフレームを検出した秒数）を表示します。
(13)	設定した監視ウィンドウの値を表示します。
(14)	設定したしきい値を表示します。
(15)	しきい値を比較する値の累積数を表示します。
(16)	Errored Frame Period イベントログの数を表示します。
(17)	Errored Frame Seconds Summary イベントログの数を表示します。
(18)	隣接装置側で生成したイベントログの情報を表示します。

4.15.12 clear ethernet oam statistics

clear ethernet oam statistics	
目的	Ethernet OAM の統計情報を消去します。
Command	clear ethernet oam statistics [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が消去されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の Ethernet OAM の統計情報を消去する方法を示します。

```
# clear ethernet oam statistics interface port 1/0/1
#
```

4.15.13 clear ethernet oam event-log

clear ethernet oam event-log	
目的	Ethernet OAM のイベントログを削除します。
Command	clear ethernet oam event-log [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が削除されます。

clear ethernet oam event-log	
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の Ethernet OAM のイベントログを削除する方法を示します。

```
# clear ethernet oam event-log interface port 1/0/1
#
```

4.15.14 ethernet oam remote-loopback start / stop

ethernet oam remote-loopback start / stop	
目的	隣接装置の対向ポートに対して、ループバックモードの開始要求、または停止要求を送信します。
Command	ethernet oam remote-loopback start interface port PORTS ethernet oam remote-loopback stop interface port PORTS
Parameter	interface port PORTS：物理ポートを指定します。複数指定できます。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドは、隣接装置の対向ポートをループバックモードに変更(start)、または解除(stop)するためのコマンドです。ループバックモードに変更された対向ポートでは、受信したパケットを折り返して送信するようになるため、本コマンドを使用する場合は十分に検討して使用してください。 本コマンドを使用して隣接装置の対向ポートをループバックモードに変更するには、対向装置の対向ポートを「リモートループバックモード設定要求を処理するモード(ethernet oam received-remote-loopback process)」に設定してから、本装置で ethernet oam remote-loopback start コマンドを実施します。 隣接装置の対向ポートのループバックモード状態を解除するには、本装置で ethernet oam remote-loopback stop コマンドを実施します。
制限・注意	• 以下のポートでは、本コマンドは使用できません。 • Ethernet OAM が未確立（対向を未認識）のポート • Ethernet OAM の動作モードがパッシブモードのポート • すでにループバックモード（Local loopback）に変更されているポート • 対向装置の対向ポートが「リモートループバックモード設定要求を無視するモード（デフォルト設定、ethernet oam received-remote-loopback ignore)」の場合でも、ethernet oam remote-loopback start コマンドを実施すると短時間の通信ロスが発生します。
バージョン	1.08.02

使用例：ポート 1/0/1 から、隣接装置の対向ポートに対してループバックモードの開始を要求する方法を示します。

```
# ethernet oam remote-loopback start interface port 1/0/1
#
```

4.15.15 ethernet oam received-remote-loopback

ethernet oam received-remote-loopback	
目的	隣接装置から受信したリモートループバック設定要求の処理方法を設定します。デフォルト設定に戻すには、ethernet oam received-remote-loopback ignore コマンドを使用します。
Command	ethernet oam received-remote-loopback {process | ignore}
Parameter	process：隣接装置からのリモートループバックモード設定要求を処理する場合に指定します。 ignore：隣接装置からのリモートループバックモード設定要求を無視する場合に指定します。
デフォルト	ignore（リモートループバックモード設定要求を無視）
モード	インターフェース設定モード（port, range）
特権レベル	レベル：12
ガイドライン	本コマンドがデフォルト設定の場合は、隣接装置の対向ポートからリモートループバック設定要求を受信しても処理せずに無視されます。 本コマンドを ethernet oam received-remote-loopback process に設定した場合は、隣接装置の対向ポートからのリモートループバック設定要求を処理します。隣接装置の対向ポートで ethernet oam remote-loopback start コマンドが実施されると、本装置のポートはループバック状態に変更されます。ethernet oam remote-loopback stop コマンドが実施されると、本装置のポートのループバック状態は解除されます。 ループバック状態に変更されたポートでは、受信したパケットを折り返して送信するようになるため、本コマンドを使用する場合は十分に検討して使用してください。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で、隣接装置から受信したリモートループバック設定要求を処理するように設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ethernet oam received-remote-loopback process
(config-if-port)#
```

4.16 単方向リンク検出(ULD)コマンド

単方向リンク検出(ULD)関連の設定コマンドは以下のとおりです。

- uld enable
- uld action
- uld discovery-time
- errdisable recovery cause uld

単方向リンク検出(ULD)関連の show コマンドは以下のとおりです。

- show uld

4.16.1 uld enable

uld enable	
目的	単方向リンク検出機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	uld enable no uld enable
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	単方向リンク検出機能を使用する場合は、本コマンドを設定する前に ethernet oam コマンドで対象ポートの Ethernet OAM を有効にしてください。また、対向装置のポートでも Ethernet OAM と単方向リンク検出機能を有効にする必要があります。 単方向リンク検出機能を有効にしたポートが、一度も対向から対応した OAMPDU を受信していない状態の間は、Discovery プロセスは開始されません。 単方向リンク検出プロセスは、Discovery プロセスが完了してお互いを正常に認識した後、または Discovery プロセスが開始してから指定した時間経過した後に開始されます。
制限・注意	• 単方向リンク検出機能は独自仕様のため、他社製品の同等機能との相互接続はサポートしていません。
バージョン	1.08.02

使用例：ポート 1/0/1 で、Ethernet OAM と単方向リンク検出機能を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ethernet oam
(config-if-port)# uld enable
(config-if-port)#
```

4.16.2 uld action

uld action	
目的	単方向リンク検出機能のアクションを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。

uld action	
Command	uld action shutdown no uld action
Parameter	shutdown：単方向リンク（双方向通信不可の場合も含む）を検出した際に、対象ポートをシャットダウン（err-disabled 状態に変更）する場合に指定します。
デフォルト	対象ポートのシャットダウンは無効（no uld action）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	本コマンドがデフォルト設定の場合でも、単方向リンクを検出するとログ（例：ULD Port1/0/1 is detected as unidirectional link）は出力されます。 シャットダウン（err-disabled 状態に変更）されたポートを復旧するには、以下の 2 つの方法があります。 • errdisable recovery cause uld コマンドを使用して、単方向リンク検出機能によって err-disabled 状態に変更されたポートの自動復旧を有効にできます。 • ポートに対して shutdown コマンドを実行した後、no shutdown コマンドを実行することで、手動でポートを復旧できます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で、単方向リンク検出機能のアクションをシャットダウン（err-disabled 状態に変更）に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# uld action shutdown
(config-if-port)#
```

4.16.3 uld discovery-time

uld discovery-time	
目的	単方向リンク検出機能の Discovery プロセスの完了待機時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	uld discovery-time SECONDS no uld discovery-time
Parameter	SECONDS：完了待機時間を 5～65,535 秒の範囲で指定します。
デフォルト	5 秒
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	単方向リンク検出機能を有効にしたポートがリンクアップして、対向から対応した OAMPDU を受信すると、Discovery プロセスが開始されます。お互いを正常に認識すると、単方向リンク検出プロセスは開始されます。 Discovery プロセスが本コマンドで指定した時間内に完了しない場合も、単方向リンク検出プロセスは開始されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で、Discovery プロセスの完了待機時間を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# uld discovery-time 300
(config-if-port)#
```

4.16.4 errdisable recovery cause uld

errdisable recovery cause uld	
目的	単方向リンク検出機能によって err-disabled 状態に変更されたポートの自動復旧を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	errdisable recovery cause uld [interval SECONDS] no errdisable recovery cause uld [interval]
Parameter	interval SECONDS（省略可能）：自動復旧するまでの待機時間を、5～86,400 秒の範囲で指定します。指定しない場合は 300 秒になります。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドの詳細や関連する show コマンドは「4.18 エラー復旧コマンド」を参照してください。 本コマンドを設定すると、単方向リンク検出機能によって err-disabled 状態に変更されたポートを、指定した時間で自動復旧することができます。 err-disabled 状態に変更されたポートのリンク状態は、show interfaces コマンドでは "link status is down (error disabled: OAM Unidirectional Link)" と表示されます。show interfaces status コマンドの Status 項目では "err-disabled" と表示されます。 本コマンドの設定有無にかかわらず、err-disabled 状態のポートに対して shutdown コマンドを実行した後、no shutdown コマンドを実行することで、手動でポートを復旧することもできます。
制限・注意	• 本設定は構成情報ではエラー復旧コマンド関連（ラベル# ERRDISABLE）で表示されます。 • interval パラメーターをデフォルト（300 秒）以外に指定して設定している場合には、削除する際にも interval パラメーターまで指定して削除してください。 • 単方向リンク検出機能を有効にしたポートが、一度も対向から対応した OAMPDU を受信していない状態の間は、Discovery プロセスは開始されません。そのため、例えばリンクダウンを伴わない双方向通信障害などによりシャットダウン（err-disabled 状態に変更）されたポートが、本コマンドで自動復旧、または shutdown コマンドの設定／削除で手動復旧してリンクアップした際に、まだ通信障害が残っている状態では、その障害を再度検出してシャットダウンされないことに注意してください。そのような状況を回避したい場合は、本コマンドの自動復旧は使用せず、通信障害が解消された後に shutdown コマンドの設定／削除で手動復旧してください。
バージョン	1.08.02

使用例：単方向リンク検出機能によって err-disabled 状態に変更されたポートの自動復旧を、復旧までの待機時間 200 秒で有効にする方法を示します。

```
# configure terminal
(config)# errdisable recovery cause uld interval 200
(config)#
```

4.16.5 show uld

show uld	
目的	単方向リンク検出機能の情報を表示します。
Command	show uld [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の単方向リンク検出機能の情報を表示する方法を示します。

```
# show uld interface port 1/0/1

Port1/0/1 ...(1)
    Admin State             : Enabled ...(2)
    Oper Status             : Enabled ...(3)
    Action                  : Shutdown ...(4)
    Link Status             : Unknown ...(5)
    Discovery Time(Sec)     : 5 ...(6)
```

項番	説明
(1)	ポート番号を表示します。
(2)	単方向リンク検出機能の有効(Enabled)／無効(Disabled)を表示します。
(3)	動作状態を表示します。 Enabled：対応した OAMPDU を受信している状態 Disabled：対応した OAMPDU を未受信の状態
(4)	単方向リンク検出機能のアクション設定を表示します。 Shutdown：単方向リンク検出時にポートをシャットダウン（err-disabled 状態に変更） Normal：単方向リンク検出時にログのみ出力
(5)	対向とのネゴシエーション状態を表示します。 Bidirectional：お互いを正常に認識している状態 RX Fault：受信方向の通信障害（双方向通信不可の場合も含む）を検出した状態 TX Fault：送信方向の通信障害を検出した状態 Link Down：対象ポートがリンクダウンしている状態（err-disabled 状態は除く） Unknown：ネゴシエーションが完了していない状態
(6)	Discovery プロセスの完了待機時間を表示します。

4.17 CFM コマンド

CFM（Connectivity Fault Management）関連の設定コマンドは以下のとおりです。

- cfm global enable
- cfm enable
- cfm domain
- mip creation（MD）
- sender-id（MD）
- cfm ma
- mepid-list
- ccm interval
- mip creation（MA）
- sender-id（MA）
- cfm mep
- mep enable
- ccm enable
- pdu-priority
- fault-alarm
- alarm-time
- ais
- lck
- cfm mp-ltr-all

CFM（Connectivity Fault Management）関連の show／操作コマンドは以下のとおりです。

- show cfm
- show cfm interface
- show cfm domain
- show cfm ma
- show cfm mepid
- show cfm mep fault
- show cfm counter ccm
- show cfm remote-mep
- show cfm mip ccm
- show cfm pkt-cnt interface
- show cfm mp-ltr-all
- cfm lck start / cfm lck stop
- clear cfm counter ccm
- clear cfm pkt-cnt interface

CFM ループバックテスト、CFM リンクトレース関連の show／操作コマンドは以下のとおりです。

- cfm loopback test
- cfm linktrace
- show cfm linktrace
- clear cfm linktrace

4.17.1 cfm global enable

cfm global enable	
目的	CFM 機能のグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	cfm global enable no cfm global enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 本機能はアクセスリスト機能と同じハードウェアリソース（Ingress グループ）を使用します。本機能で使用中の Ingress グループは、他の機能では使用できません。グループの利用状況は show access-list resource reserved-group コマンドで確認できます。
バージョン	1.08.02

使用例：CFM 機能のグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# cfm global enable
(config)#
```

4.17.2 cfm enable

cfm enable	
目的	CFM 機能のインターフェースごとの設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	cfm enable no cfm enable
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	CFM 機能で使用する各 CFM PDU は VLAN タグが付与された形式で送信されます。そのため、CFM 機能を使用する場合、CFM PDU を送受信するポートはトランクポート（switchport mode trunk コマンド）に設定してください。
制限・注意	-
バージョン	1.08.02

使用例：指定したポートで CFM 機能を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm enable
(config-if-port)#
```

4.17.3 cfm domain

cfm domain	
目的	メンテナンスドメイン(MD)を設定します。また、CFM MD 設定モードに遷移します。遷移後のプロンプトは (config-cfm-md)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	cfm domain NAME level VALUE no cfm domain NAME
Parameter	domain NAME：MD 名を最大 22 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 level VALUE：ドメインレベルを 0～7 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	各 MD には、サービスプロバイダーやオペレーターで使用中の名前と使用可能な他の名前と重複しない、独自の名前が付いています。これにより、MD ごとの管理責任が容易に識別できます。ドメイン間の階層関係を定義するために、独自のドメインレベル（0～7）が割り当てられます。ドメインの範囲が大きいほど、ドメインレベルの値が高くなります。 入力がエラーである場合、または MD 名がすでに存在する場合、MD は作成されません。MD が削除されると、MD に基づく設定も削除されます。 MD は装置全体で最大 8 個まで設定できます。
制限・注意	• ERPS 機能と併用する場合は、ドメインレベルを ERPS のリング MEL 値（管理レベル）より低く設定してください。
バージョン	1.08.02

使用例：MD 名が op-domain でドメインレベル 2 の MD を定義する方法を示します。

```
# configure terminal
(config)# cfm domain op-domain level 2
(config-cfm-md)#
```

4.17.4 mip creation（MD）

mip creation（MD）	
目的	CFM MD 設定モードにおける、メンテナンス中間ポイント(MIP)作成ルールを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mip creation {none | auto | explicit} no mip creation
Parameter	none：対象 MA において MIP を作成しない場合に指定します。 auto：対象 MA と監視対象 VLAN が同じでより低いドメインレベルの MA が存在しない環境において、対象 MA のポート（対象 MA の MEP 配置ポート、監視対象 VLAN が同じでより高いドメインレベルの MA の MEP 配置ポートは除く）に MIP を配置する場合に指定します。 explicit：対象 MA と監視対象 VLAN が同じでより低いドメインレベルの MA（以後 LOW-MA、複数存在する場合は自身より次に低いドメインレベルの MA）が存在し、かつその LOW-MA に MEP が設定されている場合に、その LOW-MA の MEP 配置

mip creation (MD)	
	ポートに対象 MA の MIP を配置する場合に指定します。
デフォルト	none
モード	CFM MD 設定モード
特権レベル	レベル：12
ガイドライン	MIP は CFM ループバックテストのターゲットとして応答できるため、通信経路の MIP ごとの到達確認に役立ちます。 本設定は、MD に含まれている MA で MIP を自動作成するデフォルト設定として機能します。このデフォルト設定に従うかどうかは、CFM MA 設定モードの mip creation コマンドで設定します。
制限・注意	• 同じ MA では、同一ポートに MEP と MIP を同時に配置することはできません。両方の設定がある場合には MEP が配置されます。 • 監視対象 VLAN が同じ MA が複数存在する場合は、ドメインレベルが異なっていても 1 つのポートに配置できる MIP は監視対象 VLAN に対して 1 つです。基本的には一番低いドメインレベルの MA の設定が優先されます。 • 対象 MA と監視対象 VLAN が同じでより低いドメインレベルの MA（以後 LOW-MA）が存在しない環境で explicit 指定で設定した場合は、MIP は配置されません。また、LOW-MA が存在する環境で auto 指定で設定した場合は、explicit 指定と同様の動作になります。
バージョン	1.08.02

使用例：MD 名が op-domain の MD において、MIP 生成ルールを auto に設定する方法を示します。

```
# configure terminal
(config)# cfm domain op-domain level 2
(config-cfm-md)# mip creation auto
(config-cfm-md)#
```

4.17.5 sender-id（MD）

sender-id (MD)	
目的	CFM MD 設定モードにおける、CFM PDU への Sender ID TLV の付加ルールを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	sender-id {none | chassis | manage | chassis-manage} no sender-id
Parameter	none：Sender ID TLV を付加しない場合に指定します。 chassis：Chassis ID 情報を含む Sender ID TLV を付加する場合に指定します。 manage：Management Address 情報を含む Sender ID TLV を付加する場合に指定します。 chassis-manage：Chassis ID 情報と Management Address 情報を含む Sender ID TLV を付加する場合に指定します。
デフォルト	none
モード	CFM MD 設定モード
特権レベル	レベル：12
ガイドライン	本設定は、MD に含まれている MA のメンテナンスポイントによる Sender ID TLV の付加ルールのデフォルト設定として機能します。このデフォルト設定に従うかどう

sender-id (MD)	
	かは、CFM MA 設定モードの sender-id コマンドで設定します。
制限・注意	-
バージョン	1.08.02

使用例：MD 名が op-domain の MD において、CFM PDU に Chassis ID 情報を含む Sender ID TLV を付加するように設定する方法を示します。

```
# configure terminal
(config)# cfm domain op-domain level 2
(config-cfm-md)# sender-id chassis
(config-cfm-md)#
```

4.17.6 cfm ma

cfm ma	
目的	メンテナンスアソシエーション(MA)を設定します。また、CFM MA 設定モードに遷移します。遷移後のプロンプトは (config-cfm-ma)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	cfm ma name NAME [vlan VLAN-ID] no cfm ma name NAME
Parameter	name NAME：MA 名を最大 22 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 vlan VLAN-ID (省略可能)：監視対象 VLAN を 1～4094 の範囲で指定します。
デフォルト	なし
モード	CFM MD 設定モード
特権レベル	レベル：12
ガイドライン	新規に MA を設定する際は、必ず監視対象 VLAN を指定してコマンドを実行する必要があります。設定済みの MA に対しては vlan パラメーターを省略してコマンドを実行する必要があります。いずれの場合も、コマンドを実行後は CFM MA 設定モードに遷移します。 同一 MD に複数の MA を設定する場合は、各 MA 名はユニークな名称になるように設定する必要があります。 MA が削除されると、MA に基づく設定も削除されます。 MA は装置全体で最大 32 個まで設定できます。
制限・注意	-
バージョン	1.08.02

使用例：MD 名が op-domain の MD において、MA 名が op1 で監視する VLAN ID が 2 の MA を定義する方法を示します。

```
# configure terminal
(config)# cfm domain op-domain level 2
(config-cfm-md)# cfm ma name op1 vlan 2
(config-cfm-ma)#
```

4.17.7 mepid-list

mepid-list	
目的	MA の MEP ID リストを設定します。MEP ID をリストに追加する場合は、mepid-list add コマンドを使用します。MEP ID をリストから削除する場合は、mepid-list delete コマンドを使用します。
Command	mepid-list {add | delete} ID
Parameter	add：MEP ID を MA の MEP ID リストに追加する場合に指定します。 delete：MEP ID を MA の MEP ID リストから削除する場合に指定します。 ID：MEP ID を 1～8191 の範囲で指定します。
デフォルト	MEP ID の登録なし
モード	CFM MA 設定モード
特権レベル	レベル：12
ガイドライン	cfm mep コマンドで MEP を作成する前に、本コマンドで MEP ID を MA の MEP ID リストに追加してください。
制限・注意	-
バージョン	1.08.02

使用例：MD 名が op-domain で MA 名が op1 の MA において、MEP ID リストに MEP ID 1 と 2 を追加する方法を示します。

```
# configure terminal
(config)# cfm domain op-domain level 2
(config-cfm-md)# cfm ma name op1 vlan 2
(config-cfm-ma)# mepid-list add 1,2
(config-cfm-ma)#
```

4.17.8 ccm interval

ccm interval	
目的	メンテナンスアソシエーション(MA)の CCM 送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ccm interval INTERVAL no ccm interval
Parameter	INTERVAL：CCM の送信間隔を指定します。以下のいずれかを選択します。 • 100ms：100 ミリ秒。CPU の処理能力をすべて使用する可能性があるため、CFM ソフトウェアモードでは推奨されません。 • 1sec：1 秒 • 10sec：10 秒 • 1min：1 分 • 10min：10 分
デフォルト	CCM の送信間隔：10sec
モード	CFM MA 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-

ccm interval	
バージョン	1.08.02

使用例：CCM の送信間隔の設定方法を示します。

```
# configure terminal
(config)# cfm domain op-domain level 2
(config-cfm-md)# cfm ma name op1 vlan 2
(config-cfm-ma)# ccm interval 10sec
(config-cfm-ma)#
```

4.17.9 mip creation（MA）

mip creation（MA）	
目的	CFM MA 設定モードにおける、メンテナンス中間ポイント(MIP)作成ルールを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mip creation {none | auto | explicit | defer} no mip creation
Parameter	none：対象 MA において MIP を作成しない場合に指定します。 auto：対象 MA と監視対象 VLAN が同じでより低いドメインレベルの MA が存在しない環境において、対象 MA のポート（対象 MA の MEP 配置ポート、監視対象 VLAN が同じでより高いドメインレベルの MA の MEP 配置ポートは除く）に MIP を配置する場合に指定します。 explicit：対象 MA と監視対象 VLAN が同じでより低いドメインレベルの MA（以後 LOW-MA、複数存在する場合は自身より次に低いドメインレベルの MA）が存在し、かつその LOW-MA に MEP が設定されている場合に、その LOW-MA の MEP 配置ポートに対象 MA の MIP を配置する場合に指定します。 defer：CFM MD 設定モードの mip creation コマンドで設定した MIP 作成ルールを引き継ぐ場合に指定します。
デフォルト	defer
モード	CFM MA 設定モード
特権レベル	レベル：12
ガイドライン	MIP は CFM ループバックテストのターゲットとして応答できるため、通信経路の MIP ごとの到達確認に役立ちます。
制限・注意	• 同じ MA では、同一ポートに MEP と MIP を同時に配置することはできません。両方の設定がある場合には MEP が配置されます。 • 監視対象 VLAN が同じ MA が複数存在する場合は、ドメインレベルが異なっていても 1 つのポートに配置できる MIP は監視対象 VLAN に対して 1 つです。基本的には一番低いドメインレベルの MA の設定が優先されます。 • 対象 MA と監視対象 VLAN が同じでより低いドメインレベルの MA（以後 LOW-MA）が存在しない環境で explicit 指定で設定した場合は、MIP は配置されません。また、LOW-MA が存在する環境で auto 指定で設定した場合は、explicit 指定と同様の動作になります。
バージョン	1.08.02

使用例：MD 名が op-domain で MA 名が op-ma1 の MA において、MIP 生成ルールを auto に設定する方法を示します。

```
# configure terminal
(config)# cfm domain op-domain level 2
(config-cfm-md)# cfm ma name op-ma1 vlan 2
(config-cfm-ma)# mip creation auto
(config-cfm-ma)#
```

4.17.10 sender-id（MA）

sender-id（MA）	
目的	CFM MA 設定モードにおける、CFM PDU への Sender ID TLV の付加ルールを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	sender-id {none | chassis | manage | chassis-manage | defer} no sender-id
Parameter	none：Sender ID TLV を付加しない場合に指定します。 chassis：Chassis ID 情報を含む Sender ID TLV を付加する場合に指定します。 manage：Management Address 情報を含む Sender ID TLV を付加する場合に指定します。 chassis-manage：Chassis ID 情報と Management Address 情報を含む Sender ID TLV を付加する場合に指定します。 defer：CFM MD 設定モードの sender-id コマンドで設定した Sender ID TLV の付加ルールを引き継ぐ場合に指定します。
デフォルト	defer
モード	CFM MA 設定モード
特権レベル	レベル：12
ガイドライン	デフォルトでは、CFM MD 設定モードの sender-id コマンドで設定した Sender ID TLV の付加ルールに従います。
制限・注意	-
バージョン	1.08.02

使用例：MD 名が op-domain で MA 名が op-ma1 の MA において、CFM PDU に Chassis ID 情報を含む Sender ID TLV を付加するように設定する方法を示します。

```
# configure terminal
(config)# cfm domain op-domain level 2
(config-cfm-md)# cfm ma name op-ma1 vlan 2
(config-cfm-ma)# sender-id chassis
(config-cfm-ma)#
```

4.17.11 cfm mep

cfm mep	
目的	メンテナンスエンドポイント(MEP)を設定します。また、CFM MEP 設定モードに遷移します。遷移後のプロンプトは（config-cfm-mep)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	cfm mep mepid ID ma name NAME domain NAME [direction {up | down}] no cfm mep mepid ID ma name NAME domain NAME

cfm mep	
Parameter	mepid ID：MEP ID を 1～8191 の範囲で指定します。 ma name NAME：MA 名を指定します。 domain NAME：MD 名を指定します。 direction（省略可能）：MEP の配置方向を、以下のいずれかで指定します。 • up：対象ポートの装置内部方向で CFM PDU を送受信する、Up MEP を作成する場合に指定します。 • down：対象ポートの装置外部方向で CFM PDU を送受信する、Down MEP を作成する場合に指定します。
デフォルト	なし
モード	インターフェース設定モード(port)
特権レベル	レベル：12
ガイドライン	新規に MEP を設定する際は、必ず MEP の配置方向を指定してコマンドを実行する必要があります。設定済みの MEP に対しては direction パラメーターを省略してコマンドを実行する必要があります。いずれの場合も、コマンドを実行後は CFM MEP 設定モードに遷移します。 本コマンドで MEP を作成する前に、mepid-list コマンドで MEP ID を MA の MEP ID リストに追加してください。 MEP は装置全体で最大 32 個まで設定できます。
制限・注意	• 同一 MA では Up MEP と Down MEP を同時に設定することはできません。 • 同一 MA のポートに MEP と MIP を同時に作成することはできません。両方の設定がある場合には MEP が作成されます。 • 本コマンドは、範囲指定のインターフェース設定モード(range)では実施しないでください。
バージョン	1.08.02

使用例：MD 名が op-domain で MA 名が op1 の MA のポート 1/0/1 に、MEP ID 1 の Up MEP を定義する方法を示します。

```
# configure terminal
(config)# cfm domain op-domain level 2
(config-cfm-md)# cfm ma name op1 vlan 2
(config-cfm-ma)# mepid-list add 1-2
(config-cfm-ma)# exit
(config-cfm-md)# exit
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name op1 domain op-domain direction up
(config-cfm-mep)#
```

4.17.12 mep enable

mep enable	
目的	MEP を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	mep enable no mep enable
Parameter	なし

mep enable	
デフォルト	無効
モード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の設定済みの MEP（MEPID=1, MA 名=ma3, MD 名=md3）で、MEP を有効に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3
(config-cfm-mep)# mep enable
(config-cfm-mep)#
```

4.17.13 ccm enable

ccm enable	
目的	MEP の Continuity Check Message（CCM）機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ccm enable no ccm enable
Parameter	なし
デフォルト	無効
モード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の設定済みの MEP（MEPID=1, MA 名=ma3, MD 名=md3）で、CCM 機能を有効に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3
(config-cfm-mep)# ccm enable
(config-cfm-mep)#
```

4.17.14 pdu-priority

pdu-priority	
目的	MEP から送信する CFM PDU の IEEE 802.1p 優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	pdu-priority COS-VALUE no pdu-priority
Parameter	COS-VALUE：IEEE 802.1p 優先度を 0～7 の範囲で指定します。

pdu-priority	
デフォルト	7
モード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の設定済みの MEP（MEPID=1, MA 名=ma3, MD 名=md3）で、MEP から送信する CFM PDU の IEEE 802.1p 優先度を 4 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3
(config-cfm-mep)# pdu-priority 4
(config-cfm-mep)#
```

4.17.15 fault-alarm

fault-alarm	
目的	通知可能な障害アラームの種別を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	fault-alarm {none | all | mac-status | remote-ccm | error-ccm | xcon-ccm} no fault-alarm
Parameter	none：障害アラームを送信しない場合に指定します。 all：すべてのタイプの障害アラームを送信する場合に指定します。 mac-status：優先度が「DefMACstatus」以上の障害に対して障害アラームを送信する場合に指定します。 remote-ccm：優先度が「DefRemoteCCM」以上の障害に対して障害アラームを送信する場合に指定します。 error-ccm：優先度が「DefErrorCCM」以上の障害に対して障害アラームを送信する場合に指定します。 xcon-ccm：「DefXconCCM」の障害アラームだけを送信する場合に指定します。
デフォルト	none
モード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	本コマンドで指定した種別の障害を検出した場合に、SNMP トラップとして障害アラームを出力することができます。 MEP で検出できる障害を優先度の低いものから並べると、以下のとおりです。 • DefRDICCM：RDI ビットがセットされた CCM を受信 • DefMACstatus：Port Status TLV または Interface Status TLV を介してエラー状態を示す CCM を受信 • DefRemoteCCM：MEP ID リストに登録された MEP からの CCM を未受信 • DefErrorCCM：無効な CCM を受信（MEP ID が重複した CCM、MEP ID リストに無い MEP ID の CCM、CCM 送信間隔設定が異なる CCM など）

fault-alarm	
	• DefXconCCM：他の MA からの可能性がある CCM を受信
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の設定済みの MEP（MEPID=1, MA 名=ma3, MD 名=md3）で、すべてのタイプの障害アラームを送信可能に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3
(config-cfm-mep)# fault-alarm all
(config-cfm-mep)#
```

4.17.16 alarm-time

alarm-time	
目的	障害アラームの送信待機時間、およびリセット待機時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	alarm-time {delay VALUE | reset VALUE} no alarm-time {delay | reset}
Parameter	delay VALUE：障害を検出してから障害アラームを送信するまでの待機時間を、250～1000 の範囲で指定します。単位は 100 分の 1 秒です。 reset VALUE：検出したすべての障害がなくなってから障害アラームをリセットするまでの待機時間を、250～1000 の範囲で指定します。単位は 100 分の 1 秒です。
デフォルト	障害アラームの送信待機時間：250、障害アラームのリセット待機時間：1000
モード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	MEP で障害を検出すると、障害アラームの送信遅延タイマーが開始されます。送信待機時間が経過しても障害が存在している場合に、障害アラームが送信されます。なお、送信待機時間の間に複数の障害が検出された場合は、最も優先度の高い障害の障害アラームのみが送信されます。 障害アラームが送信された後に新たな障害を検出すると、前の障害よりも優先度が高い場合は、新しい障害アラームがすぐに送信されます。前の障害よりも優先度が低い場合は、新しい障害アラームは送信されません。 MEP で検出したすべての障害がなくなると、障害アラームのリセットタイマーが開始されます。リセット待機時間が経過しても障害が存在していない場合に、障害アラームはリセットされます。
制限・注意	• 障害アラームの送信待機時間設定と、リセット待機時間設定は、構成情報では別に表示されます。デフォルト設定に戻す場合は、それぞれの no 形式のコマンドを実行してください。
バージョン	1.08.02

使用例：ポート 1/0/1 の設定済みの MEP（MEPID=1, MA 名=ma3, MD 名=md3）で、障害アラームの送信待機時間を 500 に、障害アラームのリセット待機時間を 500 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3
```

```
(config-cfm-mep)# alarm-time delay 500
(config-cfm-mep)# alarm-time reset 500
(config-cfm-mep)#
```

4.17.17 ais

ais	
目的	AIS（Alarm Indication Signal）機能の有効／無効、その他のパラメーターを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ais [period {1sec | 1min}] [level VALUE] no ais [period | level]
Parameter	period {1sec | 1min}（省略可能）：AIS フレームの送信間隔を、1sec（1 秒）、または 1min（1 分）で指定します。 level VALUE（省略可能）：AIS フレームを送信するドメインレベルを、0～7 の範囲で指定します。
デフォルト	AIS は無効（no ais） 送信間隔は 1 秒（ais period 1sec） ドメインレベルは未指定（no ais level）
モード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	AIS 機能の有効／無効を設定するには、パラメーターを指定しないコマンド形式で実施します。 ドメインレベルが決定されていない状態では、障害を検出しても AIS フレームは送信されません。ドメインレベルを手動で設定していない場合、同じ監視対象 VLAN で、かつドメインレベルが上位の MA が存在すると、そのドメインレベルで AIS フレームを送信します。
制限・注意	• AIS 機能の有効／無効設定と、送信間隔設定、およびドメインレベル設定は、構成情報では別に表示されます。デフォルト設定に戻す場合は、それぞれの no 形式のコマンドを実行してください。
バージョン	1.08.02

使用例：ポート 1/0/1 の設定済みの MEP（MEPID=1, MA 名=ma3, MD 名=md3）で、AIS 機能を有効に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3
(config-cfm-mep)# ais
(config-cfm-mep)#
```

使用例：ポート 1/0/1 の設定済みの MEP（MEPID=1, MA 名=ma3, MD 名=md3）で、AIS フレームの送信間隔を 1 分に、ドメインレベルを 6 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3
(config-cfm-mep)# ais period 1min
(config-cfm-mep)# ais level 6
(config-cfm-mep)#
```

4.17.18 lck

lck	
目的	LCK（Lock Signal）機能の有効／無効、その他のパラメーターを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lck [period {1sec | 1min}] [level VALUE] no lck [period | level]
Parameter	period {1sec | 1min}（省略可能）：LCK フレームの送信間隔を、1sec（1 秒）、または 1min（1 分）で指定します。 level VALUE（省略可能）：LCK フレームを送信するドメインレベルを、0～7 の範囲で指定します。
デフォルト	LCK は無効（no lck） 送信間隔は 1 秒（lck period 1sec） ドメインレベルは未指定（no lck level）
モード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	LCK 機能の有効／無効を設定するには、パラメーターを指定しないコマンド形式で実施します。 ドメインレベルが決定されていない状態では、LCK フレームの送信開始を実施しても LCK フレームは送信されません。ドメインレベルを手動で設定していない場合、同じ監視対象 VLAN で、かつドメインレベルが上位の MA が存在すると、そのドメインレベルで LCK フレームを送信します。
制限・注意	• LCK 機能の有効／無効設定と、送信間隔設定、およびドメインレベル設定は、構成情報では別に表示されます。デフォルト設定に戻す場合は、それぞれの no 形式のコマンドを実行してください。
バージョン	1.08.02

使用例：ポート 1/0/1 の設定済みの MEP（MEPID=1，MA 名=ma3，MD 名=md3）で、LCK 機能を有効に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3
(config-cfm-mep)# lck
(config-cfm-mep)#
```

使用例：ポート 1/0/1 の設定済みの MEP（MEPID=1，MA 名=ma3，MD 名=md3）で、LCK フレームの送信間隔を 1 分に、ドメインレベルを 6 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3
(config-cfm-mep)# lck period 1min
(config-cfm-mep)# lck level 6
(config-cfm-mep)#
```

4.17.19 cfm mp-ltr-all

cfm mp-ltr-all	
目的	すべてのメンテナンスポイントが LTR（Link Trace Reply）を応答する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。

cfm mp-ltr-all	
Command	cfm mp-ltr-all no cfm mp-ltr-all
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	IEEE 802.1ag 仕様では、ブリッジは LTM（Link Trace Message）に対して 1 つの LTR で応答します。本コマンドを有効にすると、LTM の中継パス上のすべてのメンテナンスポイントが、同一ブリッジにあるかどうかにかかわらず、LTR を応答するようになります。
制限・注意	• 必要がない場合は、本コマンドは有効にしないでください。
バージョン	1.08.02

使用例：すべてのメンテナンスポイントが LTR を応答する機能を有効にする方法を示します。

```
# configure terminal
(config)# cfm mp-ltr-all
(config)#
```

4.17.20 show cfm

show cfm	
目的	CFM のグローバル設定を表示します。
Command	show cfm
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：CFM のグローバル設定を表示する方法を示します。

```
# show cfm

CFM State: Enabled ...(1)
Domain Name: md5 ...(2)              Level: 5 ...(3)
Domain Name: md6                     Level: 6
```

項番	説明
(1)	CFM のグローバル設定の有効(Enabled)／無効(Disabled)を表示します。
(2)	MD 名を表示します。
(3)	ドメインレベルを表示します。

4.17.21 show cfm interface

show cfm interface	
目的	指定したポートの CFM 情報を表示します。
Command	show cfm interface [port PORTS]
Parameter	port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の CFM 情報を表示する方法を示します。

```
# show cfm interface port 1/0/1

Port1/0/1 ...(1)
CFM is enabled ...(2)
MAC Address: FC-6D-D1-F2-82-20 ...(3)

  Domain Name: md5 ...(4)
  Level: 5 ...(5)
  MA Name: ma5 ...(6)
  VID: 10 ...(7)
  MEPID: 2 ...(8)
  Direction: Down ...(9)

  Domain Name: md6
  Level: 6
  MA Name: ma6
  VID: 10
  MEPID: MIP
```

項番	説明
(1)	ポート番号を表示します。
(2)	CFM のポートごとの有効(CFM is enabled)／無効(CFM is disabled)を表示します。
(3)	MAC アドレスを表示します。
(4)	MD 名を表示します。
(5)	ドメインレベルを表示します。
(6)	MA 名を表示します。
(7)	監視対象 VLAN を表示します。
(8)	MEP ID を表示します。対象が MIP の場合は MIP と表示されます。
(9)	MEP の配置方向（Up／Down）を表示します。

4.17.22 show cfm domain

show cfm domain	
目的	MD 情報を表示します。
Command	show cfm domain NAME

show cfm domain	
Parameter	NAME：MD 名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MD 名が op-domain の MD 情報を表示する方法を示します。

```
# show cfm domain op-domain

Domain Name: op-domain ...(1)
Domain Level: 2 ...(2)
MIP Creation: Auto ...(3)
SenderID TLV: Chassis ...(4)
MA Name: op1 ...(5)
MA Name: op-mal
```

項番	説明
(1)	MD 名を表示します。
(2)	ドメインレベルを表示します。
(3)	MIP の作成方法を表示します。 Auto：自動作成 Explicit：既存の下位の MEP が設定されているポートで MIP を作成 None：MIP を作成しない
(4)	Sender ID TLV の付加ルールを表示します。 Chassis：Chassis ID 情報を含む Sender ID TLV を付加 Chassis_manage：Chassis ID 情報と Management Address 情報を含む Sender ID TLV を付加 Manage：Management Address 情報を含む Sender ID TLV を付加 None：Sender ID TLV を付加しない
(5)	MD 内に存在する MA を表示します。

4.17.23 show cfm ma

show cfm ma	
目的	MA 情報を表示します。
Command	show cfm ma name NAME domain NAME
Parameter	ma name NAME domain NAME：MA 名と MD 名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MD 名が md5 で MA 名が ma5 の MA 情報を表示する方法を示します。

```
# show cfm ma name ma5 domain md5

MA Name: ma5 ...(1)
MA VID: 10 ...(2)
MIP Creation: Auto ...(3)
CCM Interval: 10 seconds ...(4)
SenderID TLV: Chassis ...(5)
MEPID List  : 1-2 ...(6)
    (7)        (8)           (9)
   MEPID: 1  Port: 1/0/2  Direction: Up
```

項番	説明
(1)	MA 名を表示します。
(2)	監視対象 VLAN を表示します。
(3)	MIP の作成方法を表示します。 Auto：自動作成 Explicit：既存の下位の MEP が設定されているポートで MIP を作成 None：MIP を作成しない Defer：MD の設定に従う
(4)	CCM の送信間隔を表示します。
(5)	Sender ID TLV の付加ルールを表示します。 Chassis：Chassis ID 情報を含む Sender ID TLV を付加 Chassis_manage：Chassis ID 情報と Management Address 情報を含む Sender ID TLV を付加 Manage：Management Address 情報を含む Sender ID TLV を付加 None：Sender ID TLV を付加しない Defer：MD の設定に従う
(6)	MEP ID リストを表示します。
(7)	MEP ID を表示します。
(8)	ポート番号を表示します。
(9)	MEP の配置方向（Up／Down）を表示します。

4.17.24 show cfm mepid

show cfm mepid	
目的	MEP 情報を表示します。
Command	show cfm mepid ID ma name NAME domain NAME
Parameter	mepid ID ma name NAME domain NAME：MEP ID を 1～8191 の範囲で指定し、所属する MA 名と MD 名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MD 名が op-domain で MA 名が op-ma の MA に所属する MEP ID 2 の MEP 情報を表示する方法を示します。

```
# show cfm mepid 2 ma name op-ma domain op-domain

MEPID: 2 ... (1)
Port: 1/0/9 ... (2)
Direction: Up ... (3)
CFM Port Status: Enabled ... (4)
MAC Address: FC-6D-D1-F2-82-28 ... (5)
MEP State: Enabled ... (6)
CCM State: Enabled ... (7)
PDU Priority: 7 ... (8)
Fault Alarm: Disabled ... (9)
Alarm Time: 250 centisecond((1/100)s) ... (10)
Alarm Reset Time: 1000 centisecond((1/100)s) ... (11)
Highest Fault: Some Remote MEP MAC Status Error ... (12)
AIS State: Disabled ... (13)
AIS Period: 1 Second ... (14)
AIS Client Level: Invalid ... (15)
AIS Status: Not Detected ... (16)
LCK State: Disabled ... (17)
LCK Period: 1 Second ... (18)
LCK Client Level: Invalid ... (19)
LCK Status: Not Detected ... (20)
LCK Action: Stop ... (21)
Out-of-Sequence CCMs Received: 0 ... (22)
Cross-connect CCMs Received: 0 ... (23)
Error CCMs Received: 0 ... (24)              Normal CCMs Received: 0 ... (25)
Port Status CCMs Received: 0 ... (26)        If Status CCMs Received: 0 ... (27)
CCMs transmitted: 14813 ... (28)             In-order LBRs Received: 0 ... (29)
Out-of-order LBRs Received: 0 ... (30)       Next LTM Trans ID: 1 ... (31)
Unexpected LTRs Received: 0 ... (32)         LBMs Transmitted: 0 ... (33)
AIS PDUs Received: 0 ... (34)                AIS PDUs Transmitted: 0 ... (35)
LCK PDUs Received: 0 ... (36)                LCK PDUs Transmitted: 0 ... (37)
```

項番	説明
(1)	MEP ID を表示します。
(2)	ポート番号を表示します。
(3)	MEP の配置方向 (Up／Down) を表示します。
(4)	CFM のポートごとの有効(Enabled)／無効(Disabled)を表示します。
(5)	MAC アドレスを表示します。
(6)	MEP の有効(Enabled)／無効(Disabled)を表示します。
(7)	CCM の有効(Enabled)／無効(Disabled)を表示します。
(8)	CCM の IEEE 802.1p 優先度を表示します。
(9)	障害アラームの送信設定を表示します。 Disabled：障害アラームを送信しない All：すべての障害に対して送信 Some Remote MEP MAC Status Error：「DefMACstatus」以上の障害に対して送信 Some Remote MEP Down：「DefRemoteCCM」以上の障害に対して送信 Error CCM Received：「DefErrorCCM」以上の障害に対して送信 Cross-connect CCM Received：「DefXconCCM」の障害に対してのみ送信
(10)	障害アラームの送信待機時間を表示します。

項番	説明
(11)	障害アラームのリセット待機時間を表示します。
(12)	MEP で検出された最高優先度の障害を表示します。 None：障害を検出していない状態 Some Remote MEP Defect Indication：「DefRDICCM」を検出 Some Remote MEP MAC Status Error：「DefMACstatus」を検出 Some Remote MEP Down：「DefRemoteCCM」を検出 Error CCM Received：「DefErrorCCM」を検出 Cross-connect CCM Received：「DefXconCCM」を検出
(13)	AIS 機能の有効(Enabled)／無効(Disabled)を表示します。
(14)	AIS フレームの送信間隔を表示します。
(15)	AIS フレームを送信するドメインレベルを表示します。ドメインレベルが未決定の場合は Invalid と表示されます。
(16)	AIS フレームの受信状況 (Not Detected：未検出／Detected：検出) を表示します。
(17)	LCK 機能の有効(Enabled)／無効(Disabled)を表示します。
(18)	LCK フレームの送信間隔を表示します。
(19)	LCK フレームを送信するドメインレベルを表示します。ドメインレベルが未決定の場合は Invalid と表示されます。
(20)	LCK フレームの受信状況 (Not Detected：未検出／Detected：検出) を表示します。
(21)	LCK フレームの送信状況 (Stop：停止／Start：開始) を表示します。
(22)	不正な順序で受信した CCM の数を表示します。
(23)	他の MA から受信した CCM の数を表示します。
(24)	無効な CCM の数を表示します。
(25)	通常の CCM の数を表示します。
(26)	ポート状態を含めて送信された CCM の数を表示します。
(27)	ステータスを含めて送信された CCM の数を表示します。
(28)	送信済み CCM の数を表示します。
(29)	有効なメッセージおよび有効な順序で受信した LBR の数を表示します。
(30)	不正な順序で受信した LBR の数を表示します。
(31)	LTM の次の送信先を表示します。
(32)	装置で受信した予期しない LTR の数を表示します。
(33)	送信した LBM の数を表示します。
(34)	受信した AIS フレームの数を表示します。
(35)	送信した AIS フレームの数を表示します。
(36)	受信した LCK フレームの数を表示します。
(37)	送信した LCK フレームの数を表示します。

4.17.25 show cfm mep fault

show cfm mep fault	
目的	MEP で検出した障害情報を表示します。

show cfm mep fault	
Command	show cfm mep fault
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MEP で検出した障害情報を表示する方法を示します。

```
# show cfm mep fault

Domain Name: md5 ...(1)
MA Name: ma5 ...(2)
MEPID: 2 ...(3)
Status: Some Remote MEP Down ...(4)
AIS Status: Normal ...(5)
LCK Status: Normal ...(6)
```

項番	説明
(1)	MD 名を表示します。
(2)	MA 名を表示します。
(3)	障害を検出した MEP ID を表示します。
(4)	MEP で検出された最高優先度の障害を表示します。 None：障害を検出していない状態 Some Remote MEP Defect Indication：「DefRDICCM」を検出 Some Remote MEP MAC Status Error：「DefMACstatus」を検出 Some Remote MEP Down：「DefRemoteCCM」を検出 Error CCM Received：「DefErrorCCM」を検出 Cross-connect CCM Received：「DefXconCCM」を検出
(5)	AIS フレームの受信状況（AIS Received：受信中／Normal：未受信）を表示します。
(6)	LCK フレームの受信状況（LCK Received：受信中／Normal：未受信）を表示します。

4.17.26 show cfm counter ccm

show cfm counter ccm	
目的	すべての MEP の CCM 受信カウンターを表示します。
Command	show cfm counter ccm
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべての MEP の CCM 受信カウンターを表示する方法を示します。

```
# show cfm counter ccm

CCM counters:
 (1)           (2)          (3)           (4)                (5)
MEPID: 1      VID: 10     Level: 5      Direction: Up     Port: 1/0/1
 XCON: 0 ...(6)     Error: 10 ...(7)    Normal: 1862 ...(8)
MEPID: 1002   VID: 210    Level: 3      Direction: Down   Port: 1/0/2
 XCON: 7            Error: 0            Normal: 431

Total:
 XCON: 7            Error: 10           Normal: 2293
```

項番	説明
(1)	MEP ID を表示します。
(2)	監視対象 VLAN を表示します。
(3)	ドメインレベルを表示します。
(4)	MEP の配置方向（Up／Down）を表示します。
(5)	ポート番号を表示します。
(6)	他の MA からの可能性がある CCM の受信数を表示します。
(7)	無効な CCM の受信数を表示します。
(8)	有効な CCM の受信数を表示します。

4.17.27 show cfm remote-mep

show cfm remote-mep	
目的	リモート MEP 情報を表示します。
Command	show cfm remote-mep mepid ID ma name NAME domain NAME [remote-mepid ID]
Parameter	mepid ID ma name NAME domain NAME：リモート MEP 情報を表示するローカル装置の MEP ID を 1～8191 の範囲で指定し、所属する MA 名と MD 名を指定します。 remote-mepid ID（省略可能）：リモート MEP ID を 1～8191 の範囲で指定します。指定しない場合、すべてのリモート MEP 情報が表示されます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• 本コマンドで表示される「最後に有効な CCM を受信した時間」は、コマンド実行ごとに 1 秒程度バラついて表示されます。
バージョン	1.08.02

使用例：MD 名が op-domain で MA 名が op-ma の MA に所属する MEP ID 1 のリモート MEP 情報を表示する方法を示します。

```
# show cfm remote-mep mepid 1 ma name op-ma domain op-domain

Remote MEPID: 2 ...(1)
```

```
MAC Address: 00-40-66-20-48-0F ...(2)
(3)          (4)
Status: OK,  RDI: Yes
(5)                    (6)
Port State: Blocked, Interface Status: Up
Last CCM Serial Number: 180 ...(7)
Sender Chassis ID: None ...(8)
Sender Management Address: None ...(9)
Detect Time: 2016-07-06 10:29:02 ...(10)

Remote MEPID: 3
MAC Address: FF-FF-FF-FF-FF-FF
Status: FAILED,  RDI: No
Port State: No, Interface Status: No
Last CCM Serial Number: 0
Sender Chassis ID: None
Sender Management Address: None
Detect Time: 2016-07-06 10:27:46
```

項番	説明
(1)	MEP ID リストに登録されているリモート MEP の MEP ID を表示します。
(2)	リモート MEP の MAC アドレスを表示します。一度も有効な CCM を受信したことがない状態では FF-FF-FF-FF-FF-FF と表示されます。
(3)	リモート MEP からの CCM 受信状態を表示します。 IDLE：アイドル状態（自装置の MEP がまだ使用できない状態） START：自装置の MEP が使用可能になってからタイムアウトタイマーがまだ満了しておらず、かつ有効な CCM を受信していない状態 FAILED：有効な CCM を受信していない状態 OK：有効な CCM を受信している状態
(4)	最後に受信した有効な CCM の RDI ビットを表示します。 Yes：RDI ビットがセットされている（リモート MEP が障害を検出している状態） No：RDI ビットがセットされていない（リモート MEP が障害を検出していない状態）
(5)	最後に受信した有効な CCM に含まれる、Port Status TLV の値を表示します。 No：CCM 未受信、または受信した CCM に Port Status TLV が含まれていない Blocked：psBlocked(1) Up：psUp(2)
(6)	最後に受信した有効な CCM に含まれる、Interface Status TLV の値を表示します。 No：CCM 未受信、または受信した CCM に Interface Status TLV が含まれていない Up：isUp(1) Down：isDown(2) Testing：isTesting(3) Unknown：isUnknown(4) Dormant：isDormant(5) Notpresent：isNotPresent(6) Lowerlayerdown：isLowerLayerDown(7)
(7)	最後に受信した有効な CCM の Sequence Number を表示します。
(8)	最後に受信した有効な CCM に含まれる、Sender ID TLV の Chassis ID の値を表示します。含まれない場合は None 表示です。
(9)	最後に受信した有効な CCM に含まれる、Sender ID TLV の Management Address の値を

項番	説明
	表示します。含まれない場合は None 表示です。
(10)	最後に有効な CCM を受信した時間を表示します。自装置の MEP が使用可能になってから一度も有効な CCM を受信したことがない場合は、リモート MEP からの CCM 受信状態が FAILED になった時間を表示します。

4.17.28 show cfm mip ccm

show cfm mip ccm	
目的	MIP CCM データベースエントリーを表示します。
Command	show cfm mip ccm
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MIP CCM データベースエントリーの表示方法を示します。

```
# show cfm mip ccm

VID: 10 ...(1)
MAC Address: 00-40-66-20-48-01 ...(2)
Port: 1/0/12 ...(3)

VID: 10
MAC Address: 00-40-66-20-48-0F
Port: 1/0/14

Total: 2 ...(4)
```

項番	説明
(1)	監視対象 VLAN を表示します。
(2)	受信した CCM の送信元 MEP の MAC アドレスを表示します。
(3)	CCM を受信したポート番号を表示します。
(4)	MIP の CCM データベースエントリー数を表示します。

4.17.29 show cfm pkt-cnt interface

show cfm pkt-cnt interface	
目的	ポートの CFM カウンターを表示します。
Command	show cfm pkt-cnt interface [port PORTS] [rx] [tx]
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。 rx (省略可能)：RX カウンターのみ表示する場合に指定します。 tx (省略可能)：TX カウンターのみ表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード

show cfm pkt-cnt interface	
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の CFM カウンターを表示する方法を示します。

```
# show cfm pkt-cnt interface port 1/0/1

Port1/0/1 ...(1)
  CFM RX Statistics
    AllPkt:498 ...(2)  CCM:484 ...(3)
    LBR:8 ...(4)       LBM:4 ...(5)
    LTR:2 ...(6)       LTM:0 ...(7)
    VidDrop:0 ...(8)   OpcoDrop:0 ...(9)
  CFM TX Statistics
    AllPkt:257 ...(10) CCM:243 ...(11)
    LBR:4 ...(12)      LBM:8 ...(13)
    LTR:0 ...(14)      LTM:2 ...(15)
```

項番	説明
(1)	ポート番号を表示します。
(2)	受信したすべての CFM PDU 数を表示します。
(3)	受信 CCM 数を表示します。
(4)	受信 LBR 数を表示します。
(5)	受信 LBM 数を表示します。
(6)	受信 LTR 数を表示します。
(7)	受信 LTM 数を表示します。
(8)	監視対象 VLAN で受信できなくて廃棄された CFM PDU 数を表示します。
(9)	予期しない OP コードのために廃棄された CFM PDU 数を表示します。
(10)	送信したすべての CFM PDU 数を表示します。
(11)	送信 CCM 数を表示します。
(12)	送信 LBR 数を表示します。
(13)	送信 LBM 数を表示します。
(14)	送信 LTR 数を表示します。
(15)	送信 LTM 数を表示します。

4.17.30 show cfm mp-ltr-all

show cfm mp-ltr-all	
目的	すべてのメンテナンスポイントが LTR（Link Trace Reply）を応答する機能の有効／無効を表示します。
Command	show cfm mp-ltr-all
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード

show cfm mp-ltr-all	
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべてのメンテナンスポイントが LTR（Link Trace Reply）を応答する機能の有効／無効を表示する方法を示します。

```
# show cfm mp-ltr-all

All MPs reply LTRs: Disabled ...(1)
```

項番	説明
(1)	すべてのメンテナンスポイントが LTR を応答する機能の有効(Enabled)／無効(Disabled)を表示します。

4.17.31 cfm lck start / cfm lck stop

cfm lck start / cfm lck stop	
目的	LCK フレームの送信の開始／停止を実施します。
Command	■ LCK フレーム送信の開始 cfm lck start mepid ID ma name NAME domain NAME ■ LCK フレーム送信の停止 cfm lck stop mepid ID ma name NAME domain NAME
Parameter	mepid ID ma name NAME domain NAME：MEP ID を 1～8191 の範囲で指定し、所属する MA 名と MD 名を指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MEP（MEPID=1, MA 名=ma3, MD 名=md3）で、LCK フレームの送信を開始する方法を示します。

```
# cfm lck start mepid 1 ma name ma3 domain md3
#
```

4.17.32 clear cfm counter ccm

clear cfm counter ccm	
目的	すべての MEP の CCM 受信カウンターをクリアします。
Command	clear cfm counter ccm
Parameter	なし
モード	特権実行モード
特権レベル	レベル：12

clear cfm counter ccm	
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべての MEP の CCM 受信カウンターをクリアする方法を示します。

```
# clear cfm counter ccm
#
```

4.17.33 clear cfm pkt-cnt interface

clear cfm pkt-cnt interface	
目的	ポートの CFM カウンターをクリアします。
Command	clear cfm pkt-cnt interface {port PORTS | all} [rx] [tx]
Parameter	port PORTS：CFM カウンターをクリアする物理ポートを指定します。複数指定できます。 all：すべてのポートの CFM カウンターをクリアする場合に指定します。 rx（省略可能）：RX カウンターのみクリアする場合に指定します。 tx（省略可能）：TX カウンターのみクリアする場合に指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の CFM カウンターの TX カウンターのみをクリアする方法を示します。

```
# clear cfm pkt-cnt interface port 1/0/1 tx
#
```

4.17.34 cfm loopback test

cfm loopback test	
目的	CFM ループバックテストを実施します。
Command	cfm loopback test {MAC-ADDRESS | remote-mepid ID} mepid ID ma name NAME domain NAME [num VALUE] [length LENGTH | pattern STRING] [pdu-priority COS-VALUE]
Parameter	MAC-ADDRESS：宛先 MAC アドレスを、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） remote-mepid ID：宛先 MEP ID を指定します。 mepid ID ma name NAME domain NAME：LBM（Loop Back Message）を送信する MEP ID を 1～8191 の範囲で指定し、所属する MA 名と MD 名を指定します。

cfm loopback test	
	num VALUE（省略可能）：送信回数を 1～65,535 回の範囲で指定します。指定しない場合は 4 回です。 length LENGTH（省略可能）：送信する LBM のペイロード長を 0～1500 の範囲で指定します。デフォルトは 0 です。 pattern STRING（省略可能）：Data TLV を含めるかどうかを指定すると共に、Data TLV に含める任意のデータ容量を指定します。最大 1500 文字で指定します。スペースは使用できません。 pdu-priority COS-VALUE（省略可能）：送信される LBM で設定する IEEE 802.1p 優先度を指定します。指定しない場合、MEP によって送信される CCM と同じ優先度が使用されます。
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	ループバックテストは Ctrl+C キーを押すと終了できます。宛先 MAC アドレスは、この MAC アドレスによって到達できる宛先 MEP または MIP を表すユニキャストアドレス、または、マルチキャストループバック機能で使用されるマルチキャストアドレスを指定します。 マルチキャストループバック機能が使用されている場合、宛先 MAC アドレスは、MEP のレベルに一致するマルチキャストアドレスを指定する必要があります。 MEP ID は、LBM を開始するために使用する送信元 MEP を表します。
制限・注意	-
バージョン	1.08.02

使用例：MD 名が op-domain で MA 名が op-ma の MA に所属する MEP ID 2 から、00-40-66-B4-96-E5 宛てに CFM ループバックテストを実施する方法を示します。

```
# cfm loopback test 00-40-66-B4-96-E5 mepid 2 ma name op-ma domain op-domain

Reply from 00-40-66-B4-96-E5: bytes=0 time<10ms
Reply from 00-40-66-B4-96-E5: bytes=0 time<10ms
Reply from 00-40-66-B4-96-E5: bytes=0 time<10ms
Reply from 00-40-66-B4-96-E5: bytes=0 time<10ms

CFM loopback statistics for 00-40-66-B4-96-E5:
        Packets: Sent=4, Received=4, Lost=0(0% loss).
```

4.17.35 cfm linktrace

cfm linktrace	
目的	CFM リンクトレースを実施します。
Command	cfm linktrace MAC-ADDRESS mepid ID ma name NAME domain NAME [ttl VALUE] [pdu-priority COS-VALUE]
Parameter	MAC-ADDRESS：宛先 MAC アドレスを、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX）

cfm linktrace	
	mepid ID ma name NAME domain NAME：LTM（Link Trace Message）を送信する MEP ID を 1～8191 の範囲で指定し、所属する MA 名と MD 名を指定します。 ttl VALUE（省略可能）：LTM の TTL 値を 2～255 の範囲で指定します。デフォルトは 64 です。 pdu-priority COS-VALUE（省略可能）：送信される LTM で設定する IEEE 802.1p 優先度を指定します。指定しない場合、MEP によって送信される CCM と同じ優先度が使用されます。
モード	ユーザー実行モード、特権実行モード
特権レベル	レベル：1
ガイドライン	CFM リンクトレース結果は show cfm linktrace コマンドで確認できます。
制限・注意	-
バージョン	1.08.02

使用例：MD 名が op-domain で MA 名が op-ma の MA に所属する MEP ID 2 から、00-40-66-B4-96-E5 宛てに CFM リンクトレースを実施する方法を示します。

```
# cfm linktrace 00-40-66-b4-96-e5 mepid 2 ma name op-ma domain op-domain

Transaction ID: 0

#
# show cfm linktrace

Transaction ID: 0
From MEPID 2 to 00-40-66-B4-96-E5
Start Time: 2021-01-20 14:36:08
Hop: 1
   Ingress MAC Address: 00-40-66-59-6A-0E
   Egress MAC Address : 00-40-66-59-6A-12
   Forwarded: Yes  Relay Action: FDB
Hop: 2
   MEPID: 5
   Ingress MAC Address: 00-40-66-B4-96-E5
   Egress MAC Address : 00-00-00-00-00-00
   Forwarded: No  Relay Action: Hit
```

4.17.36 show cfm linktrace

show cfm linktrace	
目的	CFM リンクトレース結果を表示します。
Command	show cfm linktrace [mepid ID ma name NAME domain NAME [trans-id ID]]
Parameter	mepid ID ma name NAME domain NAME（省略可能）：CFM リンクトレース結果を表示する MEP ID を 1～8191 の範囲で指定し、所属する MA 名と MD 名を指定します。 trans-id ID（省略可能）：表示するトランザクション ID を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定の MEP ID を指定しない場合は、すべての結果が表示されます。
制限・注意	• 受信した LTR（Link Trace Reply）の情報は、最大 128 個まで保持できます。例え

show cfm linktrace	
	ば、宛先まで 5 ホップの CFM リンクトレース結果には、5 個の LTR 情報が含まれます。LTR 情報の合計が上限に到達した後は、古い情報から上書きされます。
バージョン	1.08.02

使用例：すべての CFM リンクトレース結果を表示する方法を示します。

```
# show cfm linktrace

Transaction ID: 0 ...(1)
From MEPID 2 to 00-40-66-B4-96-E5 ...(2)
Start Time: 2021-01-20 14:36:08 ...(3)
Hop: 1 ...(4)
   Ingress MAC Address: 00-40-66-59-6A-0E ...(5)
   Egress MAC Address : 00-40-66-59-6A-12 ...(6)
   (7)              (8)
   Forwarded: Yes  Relay Action: FDB
Hop: 2
   MEPID: 5 ...(9)
   Ingress MAC Address: 00-40-66-B4-96-E5
   Egress MAC Address : 00-00-00-00-00-00
   Forwarded: No  Relay Action: Hit
```

項番	説明
(1)	トランザクション ID を表示します。
(2)	LTM の送信元 MEP ID、および宛先 MAC アドレスを表示します。
(3)	CFM リンクトレースの開始日時を表示します。
(4)	CFM リンクトレースの経路の順番を表示します。
(5)	LTM を受信したメンテナンスポイントの MAC アドレスを表示します。
(6)	LTM を送信したメンテナンスポイントの MAC アドレスを表示します。
(7)	メンテナンスポイントにおける CFM リンクトレースの転送状態（Yes：転送状態／No：非転送状態）を表示します。
(8)	CFM リンクトレースの状態を表示します。 FDB：MAC アドレステーブルによって、送信ポートを決定 MPDB：MIP の CCM データベースによって、送信ポートを決定 Hit：LTM の宛先と一致するメンテナンスポイントに到達
(9)	宛先の MEP ID を表示します。

4.17.37 clear cfm linktrace

clear cfm linktrace	
目的	CFM リンクトレースの実施結果を削除します。
Command	clear cfm linktrace {mepid ID ma name NAME domain NAME | all}
Parameter	mepid ID ma name NAME domain NAME：CFM リンクトレース結果を削除する MEP ID を 1～8191 の範囲で指定し、所属する MA 名と MD 名を指定します。 all：すべての CFM リンクトレースの結果を削除する場合に指定します。
モード	特権実行モード
特権レベル	レベル：12

clear cfm linktrace	
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MD 名が op-domain で MA 名が op-ma の MA に所属する MEP ID 2 の CFM リンクトレース結果を削除する方法を示します。

```
# clear cfm linktrace mepid 2 ma name op-ma domain op-domain
#
```

4.18 エラー復旧コマンド

エラー復旧関連の設定コマンドは以下のとおりです。

- errdisable recovery

エラー復旧関連の show コマンドは以下のとおりです。

- show errdisable recovery

4.18.1 errdisable recovery

errdisable recovery	
目的	err-disabled 状態のポートの自動復旧を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	errdisable recovery cause {all | loop-detection | storm-control | uld | psecure-violation} [interval SECONDS] no errdisable recovery cause {all | loop-detection | storm-control | uld | psecure-violation} [interval]
Parameter	all：ループ検知機能、ストームコントロール機能、単方向リンク検出機能、ポートセキュリティー機能によって err-disabled 状態に変更されたポートに対して、自動復旧を有効にする場合に指定します。 loop-detection：ループ検知機能によって err-disabled 状態に変更されたポートに対して、自動復旧を有効にする場合に指定します。 storm-control：ストームコントロール機能によって err-disabled 状態に変更されたポートに対して、自動復旧を有効にする場合に指定します。 uld：単方向リンク検出機能によって err-disabled 状態に変更されたポートに対して、自動復旧を有効にする場合に指定します。 psecure-violation：ポートセキュリティー機能によって err-disabled 状態に変更されたポートに対して、自動復旧を有効にする場合に指定します。 interval SECONDS（省略可能）：自動復旧するまでの待機時間を、5～86,400 秒の範囲で指定します。指定しない場合は 300 秒になります。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを設定すると、ループ検知機能、ストームコントロール機能、単方向リンク検出機能、ポートセキュリティー機能によって err-disabled 状態に変更されたポートを、指定した時間待機した後に自動復旧することができます。 各機能で err-disabled 状態に変更されたポートのリンク状態は、show interfaces コマンドでは以下のように表示されます。 • ループ検知機能（動作モードがポートベースモードの場合）：link status is down（error disabled: Loop Detection） • ストームコントロール機能：link status is down（error disabled: Storm Control） • 単方向リンク検出機能：link status is down（error disabled: OAM Unidirectional Link） • ポートセキュリティー機能：link status is down（error disabled: Port

errdisable recovery	
	Security） また、err-disabled 状態に変更されたポートのリンク状態は、show interfaces status コマンドの Status 項目では "err-disabled" と表示されます。 本コマンドの設定有無にかかわらず、err-disabled 状態のポートに対して shutdown コマンドを実行した後、no shutdown コマンドを実行することで、手動でポートを復旧することもできます。 本コマンドの対象がループ検知機能の場合は、以下の自動復旧設定として動作します。詳細に関しては「5.6.9 errdisable recovery cause loop-detection」を参照してください。 • ループを検知した場合の動作が shutdown（デフォルト設定）の場合は、ループ検知機能によって err-disabled 状態に変更されたポート／VLAN を、指定した時間で自動復旧する設定。 • ループを検知した場合の動作が notify-only（ループを検知しても閉塞は行わず、ログ／トラップの通知のみ行うモード）の場合は、各 show コマンドのループ検知表示を、指定した時間で正常状態の表示に自動復旧する設定。
制限・注意	• interval パラメーターをデフォルト（300 秒）以外に指定して設定している場合には、削除する際にも interval パラメーターまで指定して削除してください。
バージョン	1.08.02 1.12.01：psecure-violation パラメーター追加

使用例：ループ検知機能、ストームコントロール機能、単方向リンク検出機能、ポートセキュリティー機能によって err-disabled 状態に変更されたポートの自動復旧を、復旧までの待機時間 200 秒で有効にする方法を示します。

```
# configure terminal
(config)# errdisable recovery cause all interval 200
(config)#
```

4.18.2 show errdisable recovery

show errdisable recovery	
目的	err-disabled 状態のポートの自動復旧設定の情報を表示します。
Command	show errdisable recovery
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	本コマンドの対象がループ検知機能の場合は、err-disabled 状態に変更されたポートの情報、またはループ検知状態のポート（動作設定が notify-only の場合）の情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：err-disabled 状態のポートの自動復旧設定の情報を表示する方法を示します。

```
# show errdisable recovery
(1)                                  (2)          (3)
ErrDisable Cause                     State        Interval
-----------------------------------  -----------  -------------
```

```
Port Security                              disabled      300 seconds
Storm Control                              enabled       300 seconds
Loop Detection                             enabled       300 seconds
ULD                                        disabled      300 seconds

Interfaces that will be recovered at the next timeout:
(4)          (1)                                       (5)
Interface    Errdisable Cause                          Time left(sec)
---------    ----------------------------------------  --------------
Port1/0/1    Loop Detection                            229
```

項番	説明
(1)	検知の要因となった機能を表示します。 Loop Detection：ループ検知機能 Storm Control：ストームコントロール機能 ULD：単方向リンク検出機能 Port Security：ポートセキュリティー機能
(2)	自動復旧設定の有効(enabled)／無効(disabled)を表示します。
(3)	ポートが自動復旧されるまでの時間設定を表示します。
(4)	err-disabled 状態に変更されたポートを表示します。 対象がループ検知機能で VLAN ベースモードの場合は、ポートおよびフレームの送受信が停止された VLAN を表示します。 対象がループ検知機能でループを検知した場合の動作が notify-only の場合は、ループ検知状態のポートを表示します。
(5)	err-disabled 状態に変更されたポートが自動復旧されるまでの残り時間を表示します。 対象がループ検知機能でループを検知した場合の動作が notify-only の場合は、ループ検知状態のポートが自動復旧されるまでの残り時間を表示します。

4.19 Zero Touch Provisioning(ZTP)コマンド

Zero Touch Provisioning(ZTP)関連の設定コマンドは以下のとおりです。

- ztp enable

Zero Touch Provisioning(ZTP)関連の show コマンドは以下のとおりです。

- show ztp

4.19.1 ztp enable

ztp enable	
目的	ZTP 機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。なお、ApresiaNP2500 シリーズには ZTP スイッチが搭載されているため、ZTP 機能の有効／無効は ZTP スイッチの状態(ON/OFF)と本コマンドの設定により決定されます。
Command	ztp enable [force] no ztp enable
Parameter	force（省略可能）：ZTP スイッチが OFF 状態の場合でも、装置起動時に ZTP を強制的に動作させる場合に指定します。
デフォルト	有効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ApresiaNP2500 シリーズの ZTP 機能は、以下の条件を満たす場合に、装置起動時に動作します。 • ZTP スイッチが ON 状態（no ztp enable 設定以外） • ZTP スイッチが OFF 状態でも、ztp enable force 設定の場合 ApresiaNP2500 シリーズの ZTP 機能は、以下の条件を満たす場合は、装置起動時に動作しません。 • SD カードブート用の SD カードが挿入されている場合は、SD カードブートによる起動が優先 • ZTP スイッチが OFF 状態 • ZTP スイッチが ON 状態でも、no ztp enable 設定の場合 • ZTP によって、新しくダウンロードしたファームウェアファイルに更新するため自動的に再起動された場合 ZTP を途中で中断したい場合は、コンソールポートに接続した端末で Ctrl+C キーを入力することにより中断できます。 ApresiaNP2500 シリーズでは、ZTP 動作中は ZTP LED が緑点灯します。 ZTP が動作を開始すると、VLAN 1 インターフェースは自動的に DHCP クライアントになり、DHCP サーバーから各種情報を取得します。DHCP サーバーからの情報取得に失敗した場合は、ZTP は処理を終了し、ZTP LED を 3 分間赤点灯させます。 DHCP サーバーでは、以下の方法で各種情報を指定します。 • TFTP サーバーの IP アドレスは、DHCP オプション 150 (TFTP Server Address)、もしくは siaddr フィールドで指定。DHCP オプション 150 で指定された IP アドレス、siaddr フィールドの IP アドレスの順番で、TFTP サーバーからダウンロードが成功するまで順次適用される。

ztp enable	
	• ファームウェアファイル名は最大 32 文字で、DHCP オプション 125（Vendor-Identifying Vendor-Specific Information）で指定。enterprise-number は 278 固定、subopt-code は 1 固定。 • 構成情報ファイル名は最大 32 文字で、DHCP オプション 67（Bootfile name）で指定。DHCP オプション 67（Bootfile name）を指定しない場合は、file フィールドで指定。 ファームウェアファイル名を取得している場合は、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。TFTP サーバーからのファームウェアファイルのダウンロードに失敗した場合は、ZTP 処理は終了し、ZTP LED を 3 分間赤点灯させます。なお、ファームウェアファイル名を取得していない場合は、本処理はスキップされます。 構成情報ファイル名を取得している場合は、TFTP サーバーから構成情報ファイルをダウンロードします。TFTP サーバーからの構成情報ファイルのダウンロードに失敗した場合は、ZTP 処理は終了し、ZTP LED を 3 分間赤点灯させます。なお、構成情報ファイル名を取得していない場合は、本処理はスキップされます。 ファームウェアファイル（現在のバージョンと異なるバージョン）と構成情報ファイルをダウンロードした後は、それらのファイルを以下のように装置に反映します。なお、現在のバージョンと同じバージョンのファームウェアファイルを取得した場合は、そのファームウェアファイルは反映されません。 • ファームウェアファイル（現在のバージョンと異なるバージョン）と構成情報ファイルを取得した場合、「プライマリーブートイメージファイルを、ダウンロードしたファームウェアファイルに変更」「プライマリー構成情報ファイルを、ダウンロードした構成情報ファイルに変更」して、自動的に再起動。 • ファームウェアファイル（現在のバージョンと異なるバージョン）だけを取得した場合、「プライマリーブートイメージファイルを、ダウンロードしたファームウェアファイルに変更」して、自動的に再起動。 • 構成情報ファイルだけを取得した場合、「プライマリー構成情報ファイルを、ダウンロードした構成情報ファイルに変更」して、さらに running-config に反映される。このケースでは再起動は発生しない。
制限・注意	• スタック構成の装置では、ZTP 機能は使用できません。 • マネージメントポート経由での ZTP はサポートしていません。 • startup-config が工場出荷状態の装置で ZTP が失敗した場合は、装置は工場出荷状態の設定で起動するため、ZTP が失敗した場合にループが発生するようなケーブル接続状態では、ZTP を使用しないでください。 • ファームウェアファイルと構成情報ファイルは、同じ TFTP サーバーに保存しておく必要があります。
バージョン	1.08.02

使用例：ZTP 機能を有効にする方法を示します。

```
# configure terminal
(config)# ztp enable
WARNING: ZTP is enabled now, but it won't take effect until reboot.
(config)#
```

4.19.2 show ztp

show ztp	
目的	ZTP の状態を表示します。
Command	show ztp
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ZTP 機能の状態を表示する方法を示します。

```
# show ztp

ZTP Bootup State      : Enabled ...(1)
ZTP Current State     : Enabled Force ...(2)
Current Firmware      : /c:/test-firmware.had ...(3)
Current Configure     : /c:/test-config.cfg ...(4)

Result of last time: ...(5)
  ZTP Process Result    : - ...(6)
  DHCP Server           : - ...(7)
  DHCP Discover Retry   : - ...(8)
  TFTP Server           : - ...(9)
  Gateway IP address    : - ...(10)
  Download Firmware     : - ...(11)
  Download Configure    : - ...(12)

Result of this time: ...(13)
  ZTP Process Result    : Success (Same image) ...(6)
  DHCP Server           : 10.1.1.101 ...(7)
  DHCP Discover Retry   : 0 ...(8)
  TFTP Server           : 192.168.20.200 ...(9)
  Gateway IP address    : 10.1.1.254 ...(10)
  Download Firmware     : //192.168.20.200/test-firmware.had ...(11)
  Download Configure    : //192.168.20.200/test-config.cfg ...(12)
```

項番	説明
(1)	起動時の ZTP 設定を表示します。 Enabled Force Slide Switch：ZTP スイッチが ON 状態で ztp enable 設定 Enabled Force：ztp enabe force 設定 Disabled：以下のいずれかの状態 • ZTP スイッチが OFF 状態で ztp enable 設定 • ZTP スイッチが OFF 状態で no ztp enable 設定 • ZTP スイッチが ON 状態で no ztp enable 設定
(2)	現在の ZTP 設定を表示します。 Enabled Force Slide Switch：ZTP スイッチが ON 状態で ztp enable 設定 Enabled Force：ztp enabe force 設定 Disabled：以下のいずれかの状態 • ZTP スイッチが OFF 状態で ztp enable 設定

項番	説明
	• ZTP スイッチが OFF 状態で no ztp enable 設定 • ZTP スイッチが ON 状態で no ztp enable 設定
(3)	現在のプライマリーブートイメージファイル設定を表示します。
(4)	現在のプライマリー構成情報ファイル設定を表示します。
(5)	前回の ZTP の動作結果を表示します。
(6)	ZTP の動作結果を表示します。 • Success：ZTP が動作成功 • Success (Same image)：ZTP が動作成功 (ファームウェアファイルが同じバージョン) • Not default config：ztp enable 設定で、startup-config が工場出荷状態以外のため ZTP 未動作 • interrupted ZTP processing from console：コンソールから Ctrl+C で ZTP 中断 • SD-card boot：SD カードブートで起動したため ZTP 未動作 • Fail (DHCP connection timeout)：DHCP サーバーから応答なし • Fail (DHCP <ip-address> : TFTP Server information was not found)：TFTP サーバーの IP アドレスを未取得 • Fail (DHCP no gateway IP address)：TFTP サーバーが別セグメントの場合に、デフォルトゲートウェイの IP アドレスを未取得 • Fail (TFTP server ARP no reply)：TFTP サーバー、もしくはデフォルトゲートウェイの ARP 解決に失敗 【各種ファイルの取得失敗時の表示】 XX はファイル種別ごとに表示が異なります。ファイル種別は、IMAGE（ファームウェアファイル)、CONFIG (構成情報ファイル) です。 • Fail (XX <file> file name size over)：ファイル名が 33 文字以上 • Fail (XX <file> TFTP connection failed)：TFTP サーバーへの接続に失敗 • Fail (XX <file> file not found)：指定ファイルが TFTP サーバーに存在しない (TFTP Error Codes 1 を受信) • Fail (XX <file> file access error)：指定ファイルにアクセス失敗 (TFTP Error Codes 1 以外を受信) • Fail (XX <file> TFTP timeout)：転送途中にタイムアウト発生 • Fail (XX <file> invalid file)：ダウンロードしたファイルが不適切 • Fail (XX <file> disk full or allocation exceeded)：フラッシュメモリーの空き容量不足で保存に失敗 • Fail (XX <file> flash access error)：フラッシュメモリーへの書き込みアクセスに失敗
(7)	DHCP サーバーの IP アドレスを表示します。
(8)	DHCP Discover メッセージを再送した回数を表示します。
(9)	TFTP サーバーの IP アドレスを表示します。
(10)	デフォルトゲートウェイの IP アドレスを表示します。
(11)	ファームウェアファイル名を表示します。
(12)	構成情報ファイル名を表示します。
(13)	今回の ZTP の動作結果を表示します。

4.20 タイムレンジコマンド

タイムレンジ機能関連の設定コマンドは以下のとおりです。

- time-range
- periodic

タイムレンジ機能関連の show コマンドは以下のとおりです。

- show time-range

4.20.1 time-range

time-range	
目的	タイムレンジプロファイルを設定します。また、タイムレンジ設定モードに遷移します。遷移後のプロンプトは（config-time-range)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	time-range NAME no time-range NAME
Parameter	NAME：タイムレンジプロファイル名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本機能は、タイムベース PoE を実現するために使用されます。poe power-inline コマンドで、設定されたタイムレンジプロファイルを指定することにより、PoE 給電の開始、および終了時刻を設定することができます。
制限・注意	• periodic コマンドが未設定のタイムレンジプロファイルは、構成情報には反映されず、show time-range コマンドでも表示されません。
バージョン	1.10.01

使用例：タイムレンジプロファイル「weekdays」を設定する方法を示します。

```
# configure terminal
(config)# time-range weekdays
(config-time-range)#
```

4.20.2 periodic

periodic	
目的	タイムレンジを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	periodic {daily HH:MM to HH:MM | weekly DAY HH:MM to [DAY] HH:MM} no periodic {daily HH:MM to HH:MM | weekly DAY HH:MM to [DAY] HH:MM}
Parameter	daily：毎日有効なタイムレンジの開始時刻、終了時刻を指定します。 • HH:MM：開始時刻を 24 時間表記で指定します。 • to HH:MM：終了時刻を 24 時間表記で指定します。 weekly：毎週有効なタイムレンジの開始曜日・時刻、終了曜日・時刻を指定します。

periodic	
	• DAY：開始曜日を以下のキーワードを指定します。 • sunday、または sun（日曜日） • monday、または mon（月曜日） • tuesday、または tue（火曜日） • wednesday、または wed（水曜日） • thursday、または thu（木曜日） • friday、または fri（金曜日） • saturday、または sat（土曜日） • HH:MM：開始時刻を 24 時間表記で指定します。 • to [DAY] HH:MM：終了曜日・時刻を指定します。開始曜日と終了曜日が同じ場合は、曜日は省略できます。
デフォルト	なし
モード	タイムレンジ設定モード
特権レベル	レベル：12
ガイドライン	daily を指定した場合、毎日指定の開始時刻で機能が有効になり、終了時刻で機能が無効になります。 weekly を指定した場合は、以下の動作になります。 • 終了曜日を指定した場合、毎週開始曜日の開始時刻で機能が有効になり、終了曜日の終了時刻で機能が無効になります。 • 終了曜日を指定しない場合、毎週開始曜日の開始時刻で機能が有効になり、同じ曜日の終了時刻で機能が無効になります。 1 つのタイムレンジプロファイルに、複数のタイムレンジを設定することができます。複数設定したタイムレンジの指定範囲が重複している場合は、実際の動作はマージされます。（例：同じタイムレンジプロファイルに "periodic daily 00:00 to 12:00" と "periodic daily 08:00 to 18:00" を設定した場合は、実際の動作は「開始時刻 0:00 ～ 終了時刻 18:00」になります）
制限・注意	• タイムレンジは、装置全体で最大 64 個まで設定できます。 • 開始曜日／終了曜日で指定するキーワードに対しては[TAB]キーによるコマンド補完は動作しません。 • 実際に機能が有効、および無効になる時刻は、設定された開始時刻、終了時刻から最大 60 秒遅れる場合があります。
バージョン	1.10.01

使用例：タイムレンジプロファイル「weekdays」を作成し、タイムレンジを開始曜日・時刻「月曜日 0:00」、終了曜日・時刻「金曜日 23:59」に設定する方法を示します。

```
# configure terminal
(config)# time-range weekdays
(config-time-range)# periodic weekly monday 00:00 to friday 23:59
(config-time-range)#
```

4.20.3 show time-range

show time-range	
目的	タイムレンジ設定を表示します。
Command	show time-range [NAME]

show time-range	
Parameter	NAME（省略可能）：タイムレンジプロファイル名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.10.01

使用例：すべてのタイムレンジプロファイルのタイムレンジ設定を表示する方法を示します。

```
# show time-range

Time Range Profile: ip-phone ...(1)
Daily 09:00 to 19:00 ...(2)

Time Range Profile: other_device ...(1)
Weekly Monday     07:00 to Friday     23:00 ...(2)

Total Entries: 2
```

項番	説明
(1)	タイムレンジプロファイル名を表示します。
(2)	タイムレンジを表示します。

5 レイヤー2

5.1 FDB コマンド

FDB 関連の設定コマンドは以下のとおりです。

- mac-address-table aging-time
- mac-address-table aging destination-hit
- mac-address-table learning
- mac-address-table static

FDB 関連の show／操作コマンドは以下のとおりです。

- show mac-address-table
- show mac-address-table aging-time
- show mac-address-table learning
- clear mac-address-table

5.1.1 mac-address-table aging-time

mac-address-table aging-time	
目的	MAC アドレステーブルのエージングタイムを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mac-address-table aging-time SECONDS no mac-address-table aging-time
Parameter	SECONDS：エージングタイムを 0 秒または 10～1,000,000 秒の範囲で指定します。0 秒に設定するとエージングタイムアウトは無効化されます。
デフォルト	300 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 実際に MAC アドレステーブルからエントリーが削除されるのは設定値～設定値×2 の時間になります。
バージョン	1.08.02

使用例：MAC アドレステーブルのエージングタイムを 200 秒に設定する方法を示します。

```
# configure terminal
(config)# mac-address-table aging-time 200
(config)#
```

5.1.2 mac-address-table aging destination-hit

mac-address-table aging destination-hit	
目的	宛先 MAC アドレスによる更新機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	mac-address-table aging destination-hit no mac-address-table aging destination-hit

mac-address-table aging destination-hit	
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	MAC アドレスエントリーのエージングタイムアウトまでの残り時間は、送信元 MAC アドレスと VLAN が一致するパケットを受信した場合に延長されます。 本コマンドで宛先 MAC アドレスによる更新機能を有効にすると、宛先 MAC アドレスと VLAN が一致するパケットを送信する場合にも、エージングタイムアウトまでの残り時間が延長されるようになります。
制限・注意	-
バージョン	1.08.02

使用例：宛先 MAC アドレスによる更新機能を有効にする方法を示します。

```
# configure terminal
(config)# mac-address-table aging destination-hit
(config)#
```

5.1.3 mac-address-table learning

mac-address-table learning	
目的	物理ポートでの MAC アドレス学習を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	mac-address-table learning interface port PORTS no mac-address-table learning interface port PORTS
Parameter	interface port PORTS：物理ポートを指定します。複数指定できます。
デフォルト	全ポートで有効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ポートチャネルで MAC アドレス学習を無効にする場合は、ポートチャネルのすべてのメンバーポートで無効にしてください。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1,1/0/5 で MAC アドレス学習を無効にする方法を示します。

```
# configure terminal
(config)# no mac-address-table learning interface port 1/0/1,1/0/5
(config)#
```

5.1.4 mac-address-table static

mac-address-table static	
目的	MAC アドレステーブルにスタティック MAC アドレスエントリーを追加します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mac-address-table static MAC-ADDRESS vlan VLAN-ID {interface IF-ID [,|-] | drop}

mac-address-table static	
	no mac-address-table static {all | MAC-ADDRESS vlan VLAN-ID [interface IF-ID] [,|-]}
Parameter	MAC-ADDRESS：スタティックエントリーの MAC アドレスを、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） vlan VLAN-ID：追加するエントリーの VLAN ID を 1～4094 の範囲で指定します。 interface IF-ID：転送先のインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定 drop：指定 VLAN で受信した送信元 MAC アドレスまたは宛先 MAC アドレスが一致するフレームを廃棄する場合に指定します。本パラメーターはユニキャスト MAC アドレスエントリーでのみ指定できます。 all：すべてのスタティック MAC アドレスエントリーを削除する場合に指定します。
デフォルト	スタティック MAC アドレスエントリーの設定なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ユニキャスト MAC アドレスエントリーの場合、インターフェースは 1 つだけ指定できます。マルチキャスト MAC アドレスエントリーの場合、複数のインターフェースを指定できます。 ユニキャスト MAC アドレスエントリーを削除する場合、インターフェースを指定する必要はありません。 マルチキャスト MAC アドレスエントリーを削除する場合、インターフェースを指定すると、指定したインターフェースだけが削除されます。インターフェースを指定しない場合は、マルチキャスト MAC アドレスエントリー全体が削除されます。
制限・注意	• スタティック MAC アドレスの最大登録数は 640 エントリーです。最大登録数の内訳は以下のとおりです。 • ユニキャスト MAC アドレス：256 エントリー • drop パラメーターを指定した MAC アドレス：256 エントリー • マルチキャスト MAC アドレス：128 エントリー • 装置の MAC アドレスを指定したエントリーは設定できません。 • 設定したすべてのインターフェースを含むコマンド形式でマルチキャスト MAC アドレスエントリーを削除すると、構成情報からは削除されますが MAC アドレステーブルには転送先インターフェースのないマルチキャスト MAC アドレスエントリーが残ります。そのため、マルチキャスト MAC アドレスエントリーを削除する場合は、必ずインターフェースを指定しないコマンド形式で実施してください。
バージョン	1.08.02

使用例：VLAN 4 で MAC アドレスが 00:00:5E:00:53:11、転送先インターフェースがポート 1/0/1 のスタティック MAC アドレスエントリーを設定する方法を示します。

```
# configure terminal
(config)# mac-address-table static 0000.5e00.5311 vlan 4 interface port 1/0/1
(config)#
```

使用例：VLAN 4 で MAC アドレスが 00:00:5E:00:53:22、転送先インターフェースがポートチャネル 2 のスタティック MAC アドレスエントリーを設定する方法を示します。

```
# configure terminal
(config)# interface range port 1/0/5-6
(config-if-port-range)# channel-group 2 mode on
(config-if-port-range)# exit
(config)# mac-address-table static 0000.5e00.5322 vlan 4 interface port-channel 2
(config)#
```

5.1.5 show mac-address-table

show mac-address-table	
目的	特定の MAC アドレスエントリー、または特定のインターフェースや特定の VLAN の MAC アドレスエントリーを表示します。
Command	**show mac-address-table** [**dynamic** | **static**] [**address** MAC-ADDRESS | **interface** IF-ID | **vlan** VLAN-ID]
Parameter	dynamic（省略可能）：ダイナミック MAC アドレスエントリーだけを表示する場合に指定します。 static（省略可能）：スタティック MAC アドレスエントリーだけを表示する場合に指定します。 address MAC-ADDRESS（省略可能）：特定の MAC アドレスエントリーを表示する場合に、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） interface IF-ID（省略可能）：MAC アドレスエントリーを表示するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 vlan VLAN-ID（省略可能）：MAC アドレスエントリーを表示する VLAN ID を 1～4094 の範囲で指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	パラメーター省略時は、すべてのエントリーが表示されます。
制限・注意	• スタック構成では、各スタックメンバー装置が個々に MAC アドレスを学習します。そして、その学習した MAC アドレスは CPU を介してスタックメンバー装置間で同期を行います。そのため、スタック構成全体で FDB 同期が完了するまでには、非スタック装置の場合よりも多くの時間を要します。 • スタック構成において、スタックメンバー装置をまたぐポート間でステーションムーブが発生（学習済みの MAC アドレスが登録状態のまま、別のスタックメンバー

show mac-address-table	
	装置のポートでフレームを受信して再学習）した場合、初回フレーム受信時には再学習されないことがあります。また、FDB 同期の仕組みの制限により、再学習されずに該当 MAC アドレスが MAC アドレステーブルから削除されることがあります。このような場合でも、移動先のポートで再度フレームを受信することで正常に再学習されます。 • ポートセキュリティー機能によって登録された MAC アドレスは「タイプ：Static」のエントリーとして表示されますが、スタティック MAC アドレスエントリーとは別扱いのため、show mac-address-table static コマンドでは表示されません。
バージョン	1.08.02

使用例：MAC アドレスエントリー「00-00-5E-00-53-F2」を表示する方法を示します。

```
# show mac-address-table address 00-00-5E-00-53-F2
(1)    (2)                 (3)          (4)
VLAN   MAC Address         Type         Ports
----   -----------------   ----------   -------------------------
  10   00-00-5E-00-53-F2   Dynamic      Port1/0/11

Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	MAC アドレスを表示します。
(3)	エントリーのタイプ（Static：スタティック／Dynamic：ダイナミック）を表示します。
(4)	ポート番号を表示します。

使用例：すべてのスタティック MAC アドレスエントリーを表示する方法を示します。

```
# show mac-address-table static
(1)    (2)                 (3)          (4)
VLAN   MAC Address         Type         Ports
----   -----------------   ----------   -------------------------
   1   FC-6D-D1-F2-82-1F   Static       CPU
   4   00-00-5E-00-53-11   Static       Port1/0/1
   4   00-00-5E-00-53-22   Static       port-channel2

Total Entries: 3
```

項番	説明
(1)	VLAN ID を表示します。
(2)	MAC アドレスを表示します。
(3)	エントリーのタイプ（Static：スタティック／Dynamic：ダイナミック）を表示します。
(4)	ポート番号を表示します。

使用例：VLAN 10 のすべての MAC アドレスエントリーを表示する方法を示します。

```
# show mac-address-table vlan 10
(1)    (2)                 (3)          (4)
VLAN   MAC Address         Type         Ports
----   -----------------   ----------   -------------------------
  10   00-00-5E-00-53-F1   Dynamic      Port1/0/4
```

```
  10   00-00-5E-00-53-F2  Dynamic      Port1/0/11
  10   00-40-66-A8-CC-41  Dynamic      Port1/0/12

Total Entries: 3
```

項番	説明
(1)	VLAN ID を表示します。
(2)	MAC アドレスを表示します。
(3)	エントリーのタイプ (Static：スタティック／Dynamic：ダイナミック) を表示します。
(4)	ポート番号を表示します。

5.1.6 show mac-address-table aging-time

show mac-address-table aging-time	
目的	MAC アドレステーブルのエージングタイムの設定値を表示します。
Command	show mac-address-table aging-time
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MAC アドレステーブルのエージングタイムの設定値を表示する方法を示します。

```
# show mac-address-table aging-time

 Aging Time is 300 seconds. ...(1)
```

項番	説明
(1)	MAC アドレステーブルのエージングタイムの設定値を表示します。

5.1.7 show mac-address-table learning

show mac-address-table learning	
目的	MAC アドレス学習の有効／無効を表示します。
Command	show mac-address-table learning [interface port PORTS]
Parameter	interface port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/6 の、MAC アドレス学習の有効／無効を表示する方法を示します。

```
# show mac-address-table learning interface port 1/0/1-6
```

```
(1)                          (2)
Port                         State
-------------------------    --------
Port1/0/1                    Enabled
Port1/0/2                    Enabled
Port1/0/3                    Enabled
Port1/0/4                    Enabled
Port1/0/5                    Enabled
Port1/0/6                    Enabled
```

項番	説明
(1)	ポート番号を表示します。
(2)	MAC アドレス学習の有効(Enabled)／無効(Disabled)を表示します。

5.1.8 clear mac-address-table

clear mac-address-table	
目的	MAC アドレステーブルからダイナミック MAC アドレスエントリーを削除します。
Command	clear mac-address-table dynamic {all | address MAC-ADDRESS | interface IF-ID | vlan VLAN-ID}
Parameter	all：すべてのダイナミック MAC アドレスエントリーを削除する場合に指定します。 address MAC-ADDRESS：削除するダイナミック MAC アドレスエントリーを、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） interface IF-ID：ダイナミック MAC アドレスエントリーをすべて削除するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 vlan VLAN-ID：ダイナミック MAC アドレスエントリーをすべて削除する VLAN ID を 1～4094 の範囲で指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ダイナミック MAC アドレスエントリー「00-00-5E-00-53-F2」を削除する方法を示します。

```
# clear mac-address-table dynamic address 00-00-5E-00-53-F2
#
```

5.2 ジャンボフレームコマンド

ジャンボフレーム関連のコマンドは以下のとおりです。

- max-rcv-frame-size

5.2.1 max-rcv-frame-size

max-rcv-frame-size	
目的	許容する最大イーサネットフレームサイズを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	max-rcv-frame-size BYTES no max-rcv-frame-size
Parameter	BYTES：許容する最大イーサネットフレームサイズを 64～12,288 バイトの範囲で指定します。
デフォルト	1536 バイト
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	設定したサイズを超えるオーバーサイズのフレームは破棄されます。
制限・注意	• ApresiaNP2500 シリーズでは最大 9216 バイトまでサポートしています。 • RJ-45 ポート（10BASE-T/100BASE-TX/1000BASE-T）でフレーム中継中に本コマンドを実行すると、一瞬フレームロスが発生します。 • UTP ポートでは、タグなしフレームの場合は、宛先 MAC アドレス～FCS が「設定値」のサイズまで送受信できます。タグ付きフレームの場合は、宛先 MAC アドレス～FCS が「設定値＋4 バイト」のサイズまで送受信できます。 • SFP/SFP+ポートでは、フレームの形式（タグなし／タグ付き）にかかわらず、宛先 MAC アドレス～FCS が「設定値」のサイズまで送受信できます。
バージョン	1.08.02

使用例：ポート 1/0/1 で許容する最大イーサネットフレームサイズを 6000 バイトに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# max-rcv-frame-size 6000
(config-if-port)#
```

5.3 ポートチャネルコマンド

ポートチャネル関連の設定コマンドは以下のとおりです。

- channel-group
- lacp port-priority
- lacp timeout
- lacp system-priority
- port-channel load-balance

ポートチャネル関連の show コマンドは以下のとおりです。

- show channel-group
- show channel-group channel
- show channel-group load-balance
- show channel-group sys-id

5.3.1 channel-group

channel-group	
目的	ポートチャネルのメンバーポートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	channel-group ID mode {on | active | passive} no channel-group
Parameter	ID：チャネルグループ ID を 1～48 の範囲で指定します。なお、LACP モードで使用できるチャネルグループ数は最大 32 個（チャネルグループ ID は任意の ID を指定可能）です。 on：スタティックモードのポートチャネルを構成する場合に指定します。 active：LACP モードのポートチャネルを構成する場合に指定します。本パラメーターで指定したメンバーポートは、アクティブモードになります。 passive：LACP モードのポートチャネルを構成する場合に指定します。本パラメーターで指定したメンバーポートは、パッシブモードになります。
デフォルト	なし
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	設定可能なチャネルグループ数は、最大 48 個です。 LACP を使用できるチャネルグループ数は最大 32 個（チャネルグループ ID は任意の ID を指定可能）です。例えば、LACP を使用して 32 個のポートチャネルを設定した場合、残りの 16 個はスタティックモードのポートチャネルとして使用できます。 ApresiaNP シリーズでは、1 つのポートチャネルに設定可能なメンバーポートは最大 8 ポートです。 スタティックモードのポートチャネルを構成する場合は、対向装置側もスタティックモードのポートチャネルで構成します。 LACP モードのポートチャネルを構成する場合は、対向装置側も LACP モードのポートチャネルで構成します。 • アクティブモードに設定したメンバーポートでは、対向ポートの設定に関係な

channel-group	
	く LACPDU を送信してネゴシエーションを開始します。対向ポートはアクティブモード、またはパッシブモードで設定します。 • パッシブモードに設定したメンバーポートでは、自らはネゴシエーションを開始せず、対向ポートから LACPDU を受信するとネゴシエーションを開始します。対向ポートはアクティブモードで設定します。 メンバーポートの削除後、対象のポートチャネルに 1 つもメンバーポートが存在しなくなると、対象のポートチャネルは自動的に削除されます。また、no interface port-channel コマンドでも、指定したチャネルグループ ID のポートチャネルを削除できます。
制限・注意	• ポートセキュリティー機能が有効なポートは、ポートチャネルのメンバーポートとして設定できません。 • 物理ポートは 1 つのポートチャネルのメンバーポートとして設定できます。すでにポートチャネルのメンバーポートとして設定されている物理ポートを、別のチャネルグループ ID のメンバーポートとして設定できません。 • 設定済みのスタティックモードのポートチャネルに、LACP モードを指定してメンバーポートを追加することはできません。同様に、設定済みの LACP モードのポートチャネルに、スタティックモードを指定してメンバーポートを追加することはできません。 • 1 つのポートチャネルにおいて、異なる帯域のメンバーポートが混在する構成は未サポートです。同じポートチャネルに属するメンバーポートは、同一の帯域設定で構成してください。 • ERPS または MMRP-Plus のリングポートに指定したポートチャネルでメンバーポートを追加・削除したり、対象のポートチャネル自体を削除するには、ERPS または MMRP-Plus を無効状態にする必要があります。ループなどが発生しないよう注意して実施してください。 • 本コマンドでポートチャネルのメンバーポートを設定・削除をする場合、負荷軽減のために、複数インターフェースの範囲設定モード（interface range port コマンド）は使用せず、単一インターフェースの設定モード（interface port コマンド）を使用してください。 • LACP と LLDP 疑似リンクダウン機能は、同一ポートで併用できません。
バージョン	1.08.02

使用例：ポート 1/0/4 を、LACP モード（アクティブモード）でチャネルグループ ID 3 のメンバーポートとして設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/4
(config-if-port)# channel-group 3 mode active
(config-if-port)#
```

5.3.2 lacp port-priority

lacp port-priority	
目的	LACP のポート優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lacp port-priority PRIORITY no lacp port-priority

lacp port-priority	
Parameter	PRIORITY：LACP のポート優先度を 1～65,535 の範囲で指定します。
デフォルト	32,768
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	LACP のポート優先度は、値が小さいほど優先度が高くなります。
制限・注意	• ApresiaNP シリーズでは、1 つのポートチャネルに設定可能なメンバーポートは最大 8 ポートです。
バージョン	1.08.02

使用例：ポート 1/0/4 の LACP のポート優先度を、20000 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/4
(config-if-port)# lacp port-priority 20000
(config-if-port)#
```

5.3.3 lacp timeout

lacp timeout	
目的	LACPDU の受信タイムアウトを検知するための LACP タイマーを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lacp timeout {short | long} no lacp timeout
Parameter	short：LACPDU の受信タイムアウト時間を 3 秒にする場合に指定します。自装置および対向装置が short 設定の場合は、LACPDU の送信間隔は 1 秒になります。 long：LACPDU の受信タイムアウト時間を 90 秒にする場合に指定します。自装置および対向装置が long 設定の場合は、LACPDU の送信間隔は 30 秒になります。
デフォルト	long (受信タイムアウト時間：90 秒)
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	LACPDU の送信間隔は対向装置の受信タイムアウト時間に依存するため、LACP タイマーの設定は自装置側と対向装置側で同じにする必要があります。
制限・注意	• 本設定を short に設定すると、リンクダウンを伴わない障害の検知時間は短縮されますが、LACPDU トラフィックが増えるため CPU 負荷が増加します。受信タイムアウト検知などが頻発する場合は、本設定を long に変更するか、スタティックモードのポートチャネルに変更して使用してください。
バージョン	1.08.02

使用例：ポート 1/0/1 の LACP タイマーを long に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lacp timeout long
(config-if-port)#
```

5.3.4 lacp system-priority

lacp system-priority	
目的	LACP のシステム優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	lacp system-priority PRIORITY no lacp system-priority
Parameter	PRIORITY：LACP のシステム優先度を 1～65,535 の範囲で指定します。
デフォルト	32,768
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	LACP のシステム優先度は、値が小さいほど優先度が高くなります。自装置と対向装置のシステム優先度が同じ場合は、装置の MAC アドレスによって優先度が決定されます。
制限・注意	-
バージョン	1.08.02

使用例：LACP のシステム優先度を 4096 に設定する方法を示します。

```
# configure terminal
(config)# lacp system-priority 4096
(config)#
```

5.3.5 port-channel load-balance

port-channel load-balance	
目的	ポートチャネルの負荷分散アルゴリズムを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	port-channel load-balance {src-dst-mac | dst-mac | src-mac | src-dst-ip | dst-ip | src-ip} no port-channel load-balance
Parameter	使用する負荷分散アルゴリズムを、以下のパラメーターで指定します。 • src-dst-mac：宛先 MAC アドレスと送信元 MAC アドレスで負荷分散 • dst-mac：宛先 MAC アドレスで負荷分散 • src-mac：送信元 MAC アドレスで負荷分散 • src-dst-ip：送信元 IP アドレスと宛先 IP アドレスで負荷分散 • dst-ip：宛先 IP アドレスで負荷分散 • src-ip：送信元 IP アドレスで負荷分散
デフォルト	src-dst-mac（宛先 MAC アドレスと送信元 MAC アドレスで負荷分散）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	設定できる負荷分散アルゴリズムは 1 つです。装置のすべてのポートチャネルに適用されます。 宛先 MAC アドレスが学習済みのユニキャストの場合に、指定したパラメーターの条件でバランシングされます。詳細に関しては「ポートチャネルの負荷分散」を参照してください。

port-channel load-balance	
制限・注意	-
バージョン	1.08.02

■ ポートチャネルの負荷分散

設定	対象	MAC 学習状況	負荷分散の基になる情報
デフォルト設定（src-dst-mac）	すべて	学習済み	宛先 MAC アドレス、送信元 MAC アドレス、VLAN ID、イーサタイプ
		未学習	宛先 MAC アドレス、送信元 MAC アドレス
dst-mac	すべて	学習済み	宛先 MAC アドレス、VLAN ID、イーサタイプ
		未学習	宛先 MAC アドレス
src-mac	すべて	学習済み	送信元 MAC アドレス、VLAN ID、イーサタイプ
		未学習	送信元 MAC アドレス
src-dst-ip	IP パケット	学習済み	送信元 IPv4/IPv6 アドレス、宛先 IPv4/IPv6 アドレス
	非 IP パケット	学習済み	宛先 MAC アドレス、送信元 MAC アドレス、VLAN ID、イーサタイプ
	すべて	未学習	宛先 MAC アドレス、送信元 MAC アドレス
dst-ip	IP パケット	学習済み	宛先 IPv4/IPv6 アドレス
	非 IP パケット	学習済み	宛先 MAC アドレス、VLAN ID、イーサタイプ
	すべて	未学習	宛先 MAC アドレス
src-ip	IP パケット	学習済み	送信元 IPv4/IPv6 アドレス
	非 IP パケット	学習済み	送信元 MAC アドレス、VLAN ID、イーサタイプ
	すべて	未学習	送信元 MAC アドレス

※ MAC 学習状況が未学習パターンには、ブロードキャスト、マルチキャストの場合を含む

使用例：ポートチャネルの負荷分散アルゴリズムを src-ip に設定する方法を示します。

```
# configure terminal
(config)# port-channel load-balance src-ip
(config)#
```

5.3.6 show channel-group

show channel-group	
目的	ポートチャネルの概要情報を表示します。
Command	show channel-group
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-

show channel-group	
バージョン	1.08.02

使用例：ポートチャネルの概要情報を表示する方法を示します。

```
# show channel-group

load-balance algorithm: src-dst-mac ...(1)
System-ID: 32768,FC-6D-D1-F2-82-1F ...(2)
(3)              (4)
Group            Protocol
-----------------------
3                LACP
```

項番	説明
(1)	ポートチャネルの負荷分散アルゴリズムを表示します。 src-dst-mac：送信元 MAC アドレスと宛先 MAC アドレスで負荷分散 dst-mac：宛先 MAC アドレスで負荷分散 src-mac：送信元 MAC アドレスで負荷分散 src-dst-ip：送信元 IP アドレスと宛先 IP アドレスで負荷分散 dst-ip：宛先 IP アドレスで負荷分散 src-ip：送信元 IP アドレスで負荷分散
(2)	LACP のシステム識別子（LACP のシステム優先度、MAC アドレス）を表示します。
(3)	チャネルグループ ID を表示します。
(4)	動作モード（Static：スタティックモード／LACP：LACP モード）を表示します。

5.3.7 show channel-group channel

show channel-group channel	
目的	ポートチャネルの詳細情報を表示します。
Command	show channel-group channel [ID] {detail | neighbor}
Parameter	ID（省略可能）：チャネルグループ ID を 1～48 の範囲で指定します。 detail：自装置側の情報を表示する場合に指定します。 neighbor：対向装置側の情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のチャネルグループ ID を指定しない場合は、すべてのポートチャネルの情報が表示されます。
制限・注意	• Description 項目は AEOS-NP2500 Ver. 1.10.01 以降で表示されます。それより前のバージョンでは表示されません。
バージョン	1.08.02 1.10.01：Description 項目を追加 1.11.01：LACP 状態の凡例を修正

使用例：すべてのポートチャネルの詳細情報を表示する方法を示します。

```
# show channel-group channel detail
```

```
Flag: ...(1)
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode
LACP state: ...(2)
  bndl:     Port is attached to an aggregator and bundled with other ports.
  hot-sby:  Port is in a hot-standby state.
  down:     Port is down.

Channel Group 3 ...(3)
  Member Ports: 2, Maxports = 8, Protocol: LACP ...(4)
  Description: TEST[to 2F-L2-1 ch31] ...(5)
   (6)              (7)     (8)           (9)          (10)
                            LACP          Port         Port
  Port              Flags   State         Priority     Number
  ------------------------------------------------------------
  Port1/0/4         SA      bndl          32768        4
  Port1/0/5         SA      bndl          32768        5
```

項番	説明
(1)	フラグの説明を表示します。
(2)	LACP の状態の説明を表示します。
(3)	チャネルグループ ID を表示します。
(4)	メンバーポート数、設定可能な最大ポート数（本装置では最大 8 ポート）、および動作モード（Static：スタティックモード／LACP：LACP モード）を表示します。
(5)	設定したポートチャネルの説明を表示します。
(6)	メンバーポートのポート番号を表示します。
(7)	フラグを表示します。スタティックモードでは N/A 表示。
(8)	LACP の状態を表示します。
(9)	LACP のポート優先度を表示します。スタティックモードでは N/A 表示。
(10)	ポート番号(ifindex)を表示します。スタティックモードでは N/A 表示。

使用例：ポートチャネル 3 の対向装置側の情報を表示する方法を示します。

```
# show channel-group channel 3 neighbor

Flag: ...(1)
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode

Channel Group 3 ...(2)
   (3)              (4)                          (5)         (6)         (7)
                    Partner                      Partner     Partner     Partner
  Port              System ID                    PortNo      Flags       Port_Pri
  ------------------------------------------------------------------------------
  Port1/0/4         32768,00-40-66-70-04-00      4           SA          32768
  Port1/0/5         32768,00-40-66-70-04-00      5           SA          32768
```

項番	説明
(1)	フラグの説明を表示します。
(2)	チャネルグループ ID を表示します。
(3)	自装置のメンバーポートのポート番号を表示します。
(4)	対向装置側の LACP のシステム識別子（LACP のシステム優先度、MAC アドレス）を表示し

項番	説明
	ます。スタティックモードでは N/A 表示。
(5)	対向装置側のポート番号(ifindex)を表示します。スタティックモードでは N/A 表示。
(6)	対向装置側のフラグを表示します。スタティックモードでは N/A 表示。
(7)	対向装置側の LACP のポート優先度を表示します。スタティックモードでは N/A 表示。

5.3.8 show channel-group load-balance

show channel-group load-balance	
目的	ポートチャネルの負荷分散アルゴリズムを表示します。
Command	show channel-group load-balance
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポートチャネルの負荷分散アルゴリズムを表示する方法を示します。

```
# show channel-group load-balance

load-balance algorithm: src-ip ...(1)
```

項番	説明
(1)	ポートチャネルの負荷分散アルゴリズムを表示します。 src-dst-mac：送信元 MAC アドレスと宛先 MAC アドレスで負荷分散 dst-mac：宛先 MAC アドレスで負荷分散 src-mac：送信元 MAC アドレスで負荷分散 src-dst-ip：送信元 IP アドレスと宛先 IP アドレスで負荷分散 dst-ip：宛先 IP アドレスで負荷分散 src-ip：送信元 IP アドレスで負荷分散

5.3.9 show channel-group sys-id

show channel-group sys-id	
目的	LACP のシステム識別子情報を表示します。
Command	show channel-group sys-id
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：LACP のシステム識別子情報を表示する方法を示します。

```
# show channel-group sys-id

System-ID: 32768,FC-6D-D1-F2-82-1F ...(1)
```

項番	説明
(1)	LACP のシステム識別子（LACP のシステム優先度、MAC アドレス）を表示します。

5.4 ポートリダンダントコマンド

ポートリダンダント関連の設定コマンドは以下のとおりです。

- redundant group-number
- redundant group-number preempt
- redundant mac-address-table-update
- redundant fdb-flush send enable
- redundant fdb-flush receive enable
- redundant fdb-flush vid
- redundant fdb-flush dst-mac

ポートリダンダント関連の show コマンドは以下のとおりです。

- show redundant

5.4.1 redundant group-number

redundant group-number	
目的	インターフェースをリダンダントグループに割り当てます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	redundant group-number ID {primary | secondary} no redundant group-number
Parameter	ID：リダンダントグループ ID を 1～32 の範囲で指定します。 primary：Primary ポートに指定します。 secondary：Secondary ポートに指定します。
デフォルト	なし
モード	インターフェース設定モード(port, port-channel)
特権レベル	レベル：12
ガイドライン	ポートリダンダントは、Primary ポートと Secondary ポートのペアで構成される、レイヤー2 の冗長機能です。通常時は、Primary ポートが Active 状態でトラフィックを中継し、Secondary ポートが Ready 状態でトラフィックの中継を抑止します。 ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 インターフェースが参加できるリダンダントグループは 1 つだけです。
制限・注意	• 本コマンドは複数インターフェースの範囲設定モード(range)では設定できません。 • ポートリダンダント機能は、同一インターフェースで STP/RSTP/MSTP/RPVST+ 機能、ERPS 機能、MMRP-Plus 機能、ループ検知機能（loop-detection action notify-only 設定時を除く）と併用できません。 • Ready 状態のポートはトラフィックの中継を抑止している状態ですが、物理ポートはリンクアップしているため、レイヤー3 機能の VLAN インターフェースとしてはリンクアップしているポートとして扱われます。
バージョン	1.08.02

使用例：ポート 1/0/4 をリダンダントグループ ID=3 の Primary ポートに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/4
(config-if-port)# redundant group-number 3 primary
(config-if-port)#
```

5.4.2 redundant group-number preempt

redundant group-number preempt	
目的	指定したポートリダンダントグループに対して、プリエンプトモードを無効に設定、またはプリエンプトモードのディレイ時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	redundant group-number ID preempt {disable | delay SECONDS} no redundant group-number ID preempt
Parameter	ID：リダンダントグループ ID を 1～32 の範囲で指定します。 disable：プリエンプトモードを無効にする場合に指定します。 delay SECONDS：ディレイ時間を 0～300 秒の範囲で指定します。
デフォルト	プリエンプトモード有効、ディレイ時間：0 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	以下の操作を行うと、Primary ポートと Secondary ポートの状態が初期状態（Primary ポートが Active 状態で、Secondary ポートが Ready 状態）に戻ります。これはポートの状態を強制的に変更する方法となります。 • プリエンプトモード無効に設定したリダンダントグループが「Secondary ポートが Active 状態、Primary ポートが Ready 状態」になっている場合に、本設定でプリエンプトモードを有効に変更すると、すぐさまポートの状態が初期状態に戻ります。 • プリエンプトモード有効でディレイ時間を 0 秒以外に設定したリダンダントグループが「Secondary ポートが Active 状態、Primary ポートが Ready 状態でディレイ時間の経過待ち」になっている場合に、本設定でディレイ時間を変更すると、すぐさまポートの状態が初期状態に戻ります。
制限・注意	-
バージョン	1.08.02

使用例：リダンダントグループ ID=3 でプリエンプトモードを無効にする方法を示します。

```
# configure terminal
(config)# redundant group-number 3 preempt disable
(config)#
```

5.4.3 redundant mac-address-table-update

redundant mac-address-table-update	
目的	Active 状態のポートが切り替わる際に、MAC アドレス再学習フレームを送信する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	redundant mac-address-table-update count VALUE no redundant mac-address-table-update
Parameter	VALUE：送信回数を 1～3 回の範囲で指定します。

redundant mac-address-table-update	
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• Active 状態のポートが切り戻る場合に、対向装置のリンクアップのタイミングによってはすべての再学習フレームを受信できないことが考えられます。そのような場合には、再学習フレームの送信回数を 2～3 回に増やしてください。
バージョン	1.08.02

使用例：送信回数=3 回指定で MAC アドレス再学習フレームの送信を有効にする方法を示します。

```
# configure terminal
(config)# redundant mac-address-table count 3
(config)#
```

5.4.4 redundant fdb-flush send enable

redundant fdb-flush send enable	
目的	Active 状態のポートが切り替わる際に、FDB フラッシュフレームを送信する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	redundant fdb-flush send enable count VALUE no redundant fdb-flush send enable
Parameter	VALUE：送信回数を 1～3 回の範囲で指定します。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	FDB フラッシュフレームによる MAC アドレステーブルのクリアを行う場合、クリアが必要なすべてのスイッチで、redundant fdb-flush receive enable コマンドの設定が有効である必要があります。 FDB フラッシュフレームの送信元 MAC アドレスは自装置の MAC アドレスで、EtherType は 0x8820 です。また、FDB フラッシュフレームには常に VLAN タグが付与されており、優先度は 7 です。
制限・注意	• 本コマンドはアクセスリスト機能と同じハードウェアリソース（Ingress グループ）を使用します。本コマンドで使用中の Ingress グループは、AccessDefender 制御用の 1 グループ、ループ検知、およびポートリダンダントの一部コマンドで同じ 1 グループを共有しますが、その他の機能では使用できません。グループの利用状況は show access-list resource reserved-group コマンドで確認できます。
バージョン	1.08.02

使用例：送信回数=3 回指定で FDB フラッシュフレームの送信を有効にする方法を示します。

```
# configure terminal
(config)# redundant fdb-flush send enable count 3
(config)#
```

5.4.5 redundant fdb-flush receive enable

redundant fdb-flush receive enable	
目的	FDB フラッシュフレームを受信して MAC アドレステーブルをクリアする機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	redundant fdb-flush receive enable no redundant fdb-flush receive enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本設定を有効にすると、FDB フラッシュフレーム（宛先 MAC アドレスが redundant fdb-flush dst-mac コマンドで設定した MAC アドレスと一致するフレーム）を受信した場合に、MAC アドレステーブルをクリアします。
制限・注意	• 本コマンドはアクセスリスト機能と同じハードウェアリソース（Ingress グループ）を使用します。本コマンドで使用中の Ingress グループは、AccessDefender 制御用の 1 グループ、ループ検知、およびポートリダンダントの一部コマンドで同じ 1 グループを共有しますが、その他の機能では使用できません。グループの利用状況は show access-list resource reserved-group コマンドで確認できます。
バージョン	1.08.02

使用例：FDB フラッシュフレームを受信して MAC アドレステーブルをクリアする機能を有効にする方法を示します。

```
# configure terminal
(config)# redundant fdb-flush receive enable
(config)#
```

5.4.6 redundant fdb-flush vid

redundant fdb-flush vid	
目的	FDB フラッシュフレームの VLAN タグの VLAN ID を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	redundant fdb-flush vid VLAN-ID no redundant fdb-flush vid
Parameter	VLAN-ID：FDB フラッシュフレームの VLAN ID を 1～4094 の範囲で指定します。
デフォルト	0
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：FDB フラッシュフレームの VLAN ID を 1 に設定する方法を示します。

```
# configure terminal
(config)# redundant fdb-flush vid 1
(config)#
```

5.4.7 redundant fdb-flush dst-mac

redundant fdb-flush dst-mac	
目的	FDB フラッシュフレームの宛先 MAC アドレスを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	redundant fdb-flush dst-mac MAC-ADDRESS no redundant fdb-flush dst-mac
Parameter	MAC-ADDRESS：FDB フラッシュフレームの宛先 MAC アドレスを、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX）
デフォルト	01:40:66:C0:4F:44
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：FDB フラッシュフレームの宛先 MAC アドレスを 01-00-5E-90-10-00 に設定する方法を示します。

```
# configure terminal
(config)# redundant fdb-flush dst-mac 01-00-5E-90-10-00
(config)#
```

5.4.8 show redundant

show redundant	
目的	リダンダントグループ情報を表示します。
Command	show redundant [portbase]
Parameter	portbase（省略可能）：ポートリダンダントを設定したインターフェースの情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• Primary ポートまたは Secondary ポートをポートチャネル指定で使用する場合、本コマンドではポートチャネル自体の状態を表示するため、ポートチャネルのメンバーポートのリンクアップ／リンクダウン状態は確認できません。ポートチャネルのメンバーポートの状態は show channel-group channel コマンドで確認してください。 • 例えば、Primary ポートに設定したポートチャネルの一部メンバーポートがリンクダウンしていても、ポートチャネル自体がアップしていてポートリダンダントが Active 状態の場合は、本コマンドでは対象ポートチャネルのすべてのメンバーポー

show redundant	
	トが "a" 表示になります。
バージョン	1.08.02

使用例：すべてのポートリダンダントの情報を表示する方法を示します。

```
# show redundant

 Mac-address-table-update    :Disable ...(1)
 FDB-flush send              :Enable (count 3) ...(2)
 FDB-flush receive           :Disable ...(3)
 VLAN ID                     :300 ...(4)
 Dst MAC address             :01-40-66-C0-4F-44 ...(5)
 A: Active      a: Active (port-channel)
 R: Ready       r: Ready (port-channel)
 D: Link Down   d: Link Down (port-channel)
          (7)
(6)    C Pre Port
              1      8 9
GrpNo         +------+ +---
  1    1  -   AR..... ....
  8    1  -   ........ aarr
```

項番	説明
(1)	MAC アドレス再学習フレーム送信の有効(Enable)／無効(Disable)を表示します。有効時には送信回数も表示します。
(2)	FDB フラッシュフレーム送信の有効(Enable)／無効(Disable)を表示します。有効時には送信回数も表示します。
(3)	FDB フラッシュフレーム受信の有効(Enabled)／無効(Disable)を表示します。
(4)	FDB フラッシュフレームの VLAN タグの VLAN ID を表示します。
(5)	FDB フラッシュフレームの宛先 MAC アドレスを表示します。
(6)	リダンダントグループ ID ごとに、プリエンプトモードと切り戻り遅延時間の設定、ポートリダンダントの設定、およびポートのリンク状態を表示します。 "C"列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。
(7)	プリエンプトモードと切り戻り遅延時間を表示します。 -：プリエンプトモード有効で切り戻り遅延時間 0 秒設定 Dis：プリエンプトモード無効 1-300：プリエンプトモード有効で、切り戻り遅延時間(秒)を表示

使用例：ポートリダンダントを設定したインターフェースの情報を表示する方法を示します。

```
# show redundant portbase
(1)              (2)       (3)      (4)
Port             Status    GrpNo    Pri/Sec
Port1/0/1        Active    1        Primary
Port1/0/2        Ready     1        Secondary
Port-channel20   Active    8        Primary
Port-channel21   Ready     8        Secondary
```

項番	説明
(1)	ポートリダンダントを設定したポート番号またはポートチャネル番号を表示します。

項番	説明
(2)	ポートリダンダントの動作状態を表示します。 Active：トラフィックの中継が可能な状態 Ready：トラフィックの中継を抑止している状態 Down：対象ポート、またはポートチャネルがダウンしている状態
(3)	リダンダントグループ ID を表示します。
(4)	ポート種別を表示します。 Primary：ポートリダンダントの Primary ポート Secondary：ポートリダンダントの Secondary ポート

5.5 リンクダウン連携コマンド

リンクダウン連携関連の設定コマンドは以下のとおりです。

- link-relay

リンクダウン連携関連の show コマンドは以下のとおりです。

- show link-relay
- show link-relay status

5.5.1 link-relay

link-relay	
目的	リンクダウン連携機能を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	**link-relay id** ID **track-port interface port** PORTS **relay-port interface port** PORTS **no link-relay id** ID
Parameter	id ID：リンクダウン連携インスタンスを 1～32 の範囲で指定します。 track-port interface port PORTS：リンク状態を監視する物理ポート（監視ポート）を指定します。複数指定できます。 relay-port interface port PORTS：監視ポートのリンク状態に追従してリンクダウン／リンクアップする物理ポート（リレーポート）を指定します。複数指定できます。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	監視ポートとして設定したすべてのポートがリンクダウンすると、リレーポートとして設定したすべてのポートが強制的にリンクダウンされます。 監視ポートとして設定したすべてのポートがリンクダウンしている状態から 1 つ以上のポートがリンクアップすると、リレーポートとして設定したすべてのポートの強制的なリンクダウン状態が解除されてリンクアップに戻ります。 あるポートを複数のリンクダウン連携インスタンスのリレーポートとして設定することもできますが、その場合は以下のように動作します。 • そのリレーポートが所属する複数のリンクダウン連携インスタンスのいずれか 1 つで切り替わり条件（監視ポートがすべてリンクダウン）を満たすと、リレーポートが強制的にリンクダウンされます。 • そのリレーポートが所属するすべてのリンクダウン連携インスタンスで復旧条件（監視ポートが 1 つ以上リンクアップ）を満たすと、リレーポートの強制的なリンクダウン状態が解除されてリンクアップに戻ります。
制限・注意	• 任意のリンクダウン連携インスタンスで監視ポートとして設定済みのポートは、別のリンクダウン連携インスタンスの監視ポートまたはリレーポートとして設定できません。 • 任意のリンクダウン連携インスタンスでリレーポートとして設定済みのポートは、別のリンクダウン連携インスタンスの監視ポートとして設定できません。
バージョン	1.08.02

使用例：リンクダウン連携インスタンス=1 を指定して、「ポート 1/0/1～1/0/3 のすべてがリンクダウンした場合に、ポート 1/0/8 とポート 1/0/12 を強制的にリンクダウンさせる」設定を行う方法を示します。

```
# configure terminal
(config)# link-relay id 1 track-port interface port 1/0/1-3 relay-port interface port
1/0/8,1/0/12
(config)#
```

5.5.2 show link-relay

show link-relay	
目的	リンクダウン連携設定およびポートのリンク状態を表示します。
Command	show link-relay
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：リンクダウン連携設定およびポートのリンク状態を表示する方法を示します。

```
# show link-relay

Track Port T: LinkUp t: LinkDown
Relay Port R: LinkUp r: LinkDown
(1)
   C Port
      1       8 9
ID    +-------+ +---
1  1  TTt....R ...R
32 1  ....t... .r..
```

項番	説明
(1)	リンクダウン連携インスタンスごとに、リンクダウン連携設定、およびポートのリンク状態を表示します。 "C"列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。

5.5.3 show link-relay status

show link-relay status	
目的	リンクダウン連携インスタンスごとの監視ポートの状態を表示します。
Command	show link-relay status
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-

show link-relay status	
バージョン	1.08.02

使用例：リンクダウン連携インスタンスごとの監視ポートの状態を表示する方法を示します。

```
# show link-relay status
(1) (2)      (3)
ID  Status  Remain Ports
--  ------  ------------
1   Up      2
32  Down    0
```

項番	説明
(1)	リンクダウン連携インスタンスを表示します。
(2)	リンクダウン連携インスタンスの状態を表示します。 Down：すべての監視ポートがリンクダウン状態 Up：少なくとも 1 ポート以上の監視ポートがリンクアップ状態
(3)	リンクアップ状態の監視ポートの数を表示します。

5.6 ループ検知コマンド

ループ検知関連の設定コマンドは以下のとおりです。

- loop-detection global enable
- loop-detection enable（Interface）
- loop-detection interval
- loop-detection frame-type untagged
- loop-detection mode
- loop-detection vlan
- loop-detection action notify-only
- loop-detection no-check-src
- errdisable recovery cause loop-detection
- snmp-server enable traps loop-detection

ループ検知関連の show／操作コマンドは以下のとおりです。

- show loop-detection
- show loop-detection status
- clear loop-detection information

5.6.1 loop-detection global enable

loop-detection global enable	
目的	ループ検知機能のグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	loop-detection global enable no loop-detection global enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• ループ検知機能（loop-detection action notify-only 設定時を除く）は、同一インターフェースで STP/RSTP/MSTP/RPVST+機能、ERPS 機能、MMRP-Plus 機能、ポートリダンダント機能と併用できません。 • 同一インターフェース（ポート、ポートチャネル）で STP/RSTP 機能と併用する場合は、事前に対象インターフェースへ loop-detection action notify-only コマンドを設定してください。 • 同一インターフェース（ポート、ポートチャネル）で MSTP/RPVST+機能、ERPS 機能、MMRP-Plus 機能と併用する場合は、事前に対象インターフェースへ loop-detection action notify-only コマンドを設定してください。また、VLAN ごとに検知したい場合は VLAN ベースモードに変更してください。 • 本機能はアクセスリスト機能と同じハードウェアリソース（Ingress グループ）を使用します。本機能で使用中の Ingress グループは、AccessDefender 制御用の 1 グループ、ループ検知、およびポートリダンダントの一部コマンドで同じ 1 グループを共有しますが、その他の機能では使用できません。グループの利用状況は show

loop-detection global enable	
	access-list resource reserved-group コマンドで確認できます。
バージョン	1.08.02

使用例：ループ検知機能のグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# loop-detection global enable
(config)#
```

5.6.2 loop-detection enable（Interface）

loop-detection enable（Interface）	
目的	ループ検知機能のインターフェースごとの設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	loop-detection enable no loop-detection enable
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。
制限・注意	• ループ検知機能（loop-detection action notify-only 設定時を除く）は、同一インターフェースで STP/RSTP/MSTP/RPVST+機能、ERPS 機能、MMRP-Plus 機能、ポートリダンダント機能と併用できません。 • 同一インターフェース（ポート、ポートチャネル）で STP/RSTP 機能と併用する場合は、事前に対象インターフェースへ loop-detection action notify-only コマンドを設定してください。 • 同一インターフェース（ポート、ポートチャネル）で MSTP/RPVST+機能、ERPS 機能、MMRP-Plus 機能と併用する場合は、事前に対象インターフェースへ loop-detection action notify-only コマンドを設定してください。また、VLAN ごとに検知したい場合は VLAN ベースモードに変更してください。 • 本機能はアクセスリスト機能と同じハードウェアリソース（Ingress グループ）を使用します。本機能で使用中の Ingress グループは、AccessDefender 制御用の 1 グループ、ループ検知、およびポートリダンダントの一部コマンドで同じ 1 グループを共有しますが、その他の機能では使用できません。グループの利用状況は show access-list resource reserved-group コマンドで確認できます。
バージョン	1.08.02

使用例：ポート 1/0/1 で、ループ検知機能を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# loop-detection enable
(config-if-port)#
```

5.6.3 loop-detection interval

loop-detection interval	
目的	ループ検知フレームの送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	loop-detection interval SECONDS no loop-detection interval
Parameter	SECONDS：ループ検知フレームの送信間隔を 1～32,767 秒の範囲で指定します。
デフォルト	10 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ループ検知フレームの送信間隔を 20 秒に設定する方法を示します。

```
# configure terminal
(config)# loop-detection interval 20
(config)#
```

5.6.4 loop-detection frame-type untagged

loop-detection frame-type untagged	
目的	アクセスポートなどから送信するループ検知フレームの形式を、タグなしフレーム形式に変更する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	loop-detection frame-type untagged no loop-detection frame-type untagged
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	以下のループ検知フレームは、デフォルトでは VID=0 のタグ付きフレーム形式で送信しますが、本コマンドを有効にすると、タグなしフレーム形式に変更することができます。 • ポートベースモードの場合に送信するループ検知フレーム • VLAN ベースモードで、タグなし形式のフレームを送信する設定のポート（アクセスポート、トランクポートのネイティブ VLAN など）から送信するループ検知フレーム
制限・注意	• トンネルポートから送信するループ検知フレームは、本コマンドの有効／無効にかかわらず、常にタグなしフレーム形式のループ検知フレームを送信します。 • VLAN ベースモードで、タグ付き形式のフレームを送信する設定のポート（トランクポートなど）から送信するループ検知フレームは、本コマンドの有効／無効にかかわらず、常にタグ付き形式のループ検知フレーム（VID=ループ検知を有効にした VLAN）を送信します。

loop-detection frame-type untagged	
バージョン	1.12.01

使用例：アクセスポートなどから送信するループ検知フレームの形式を、タグなしフレーム形式に変更する方法を示します。

```
# configure terminal
(config)# loop-detection frame-type untagged
(config)#
```

5.6.5 loop-detection mode

loop-detection mode	
目的	ループ検知の動作モードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	loop-detection mode {port-based | vlan-based} no loop-detection mode
Parameter	port-based：ポートベースモードにする場合に指定します。 vlan-based：VLAN ベースモードにする場合に指定します。
デフォルト	ポートベースモード
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	通常、ポートベースのループ検知は、ユーザーに接続されるポートで使用されます。また、VLAN ベースのループ検知は、隣接装置がループ検知機能をサポートしていない場合に、トランクポートで使用されます。 ポートベースのループ検知を使用する場合は、VID=0 のタグが付いたループ検知フレームをループ検知が有効なポートから送信します。ループを検知した場合は、以下のように動作します。 • ループ検知フレームを送信したポートと同じポートで受信した場合は、その受信ポートがシャットダウン（err-disabled 状態に変更）されます。 • ループ検知フレームを送信したポートとは異なるポートで受信した場合、その受信ポートのループ検知が有効なら、その受信ポートがシャットダウン（err-disabled 状態に変更）されます。 • ループ検知フレームを送信したポートとは異なるポートで受信した場合、その受信ポートのループ検知が無効なら、そのループ検知フレームを送信したポートがシャットダウン（err-disabled 状態に変更）されます。 ポートチャネルでポートベースのループ検知を有効にしていてループを検知した場合は、そのポートチャネルのすべてのメンバーポートがシャットダウン（err-disabled 状態に変更）されます。 VLAN ベースのループ検知を使用する場合は、ループ検知が有効な VLAN ごとに、タグ付き形式のループ検知フレームを送信します。ポートにタグなし VLAN が所属する場合は、VID=0 のタグが付いたループ検知フレームが送信されます。ループを検知した場合は、以下のように動作します。 • ループ検知フレームを送信したポートと同じポートで受信した場合は、その受信ポートの対象 VLAN が err-disabled 状態になります。 • ループ検知フレームを送信したポートとは異なるポートで受信した場合、その受信ポートのループ検知が有効なら、その受信ポートの対象 VLAN が err-

loop-detection mode	
	disabled 状態になります。 • ループ検知フレームを送信したポートとは異なるポートで受信した場合、その受信ポートのループ検知が無効なら、そのループ検知フレームを送信したポートの対象 VLAN が err-disabled 状態になります。 ポートチャネルで VLAN ベースのループ検知を有効にしていてループを検知した場合は、そのポートチャネルのすべてのメンバーポートの対象 VLAN が err-disabled 状態になります。 ハイブリッドポートのように複数のタグなし VLAN が割り当てられたポートで VLAN ベースのループ検知を使用する場合は、ループ検知が有効な VLAN ごとに、VID=0 のタグが付いたループ検知フレームが送信されます。ループ検知フレーム内部の情報フィールドに VLAN 情報が含まれているため、動作自体は VLAN ベースのループ検知モードと同じです。 err-disabled 状態に変更されたポート／VLAN を復旧するには、以下の 2 つの方法があります。 • errdisable recovery cause loop-detection コマンドを使用して、ループ検知機能によって err-disabled 状態に変更されたポート／VLAN の自動復旧を有効にできます。 • ポートに対して shutdown コマンドを実行した後、no shutdown コマンドを実行することで、手動でポート／VLAN を復旧できます。VLAN ベースのループ検知を使用していてこの復旧方法を実施する際は、対象ポートがリンクダウン／リンクアップするため、対象ポートに所属するすべての VLAN に影響があることに注意してください。
制限・注意	• ループ検知可能な VLAN 数は、装置全体で最大 100 個です。 • VLAN ベースモードに設定している場合、ループ検知機能を有効にしている VLAN すべてに対してループ検知フレームを送信します。ループ検知フレームは 1 秒間に最大 80 個ずつ送信されます。
バージョン	1.08.02

使用例：ループ検知モードをポートベースに設定する方法を示します。

```
# configure terminal
(config)# loop-detection mode port-based
(config)#
```

5.6.6 loop-detection vlan

loop-detection vlan	
目的	ループ検知の動作モードが VLAN ベースモードの場合に、ループ検知を有効にする VLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	loop-detection vlan VLAN-LIST [,|-] no loop-detection vlan VLAN-LIST [,|-]
Parameter	VLAN-LIST：ループ検知の動作モードが VLAN ベースモードの場合に、ループ検知を有効にする VLAN ID を 1～4094 の範囲で設定します。複数指定できます。
デフォルト	すべての VLAN に対して有効
モード	グローバル設定モード
特権レベル	レベル：12

loop-detection vlan	
ガイドライン	デフォルト設定以外の状態で、設定済みの内容と異なる VLAN ID を指定して実行した場合は、設定済みの内容に差分の VLAN ID が追加されます。 設定済みの内容から特定の VLAN ID を削除したい場合は、no loop-detection vlan コマンドで削除したい VLAN ID だけを指定して実行します。 設定済みの VLAN ID をすべて指定して no loop-detection vlan コマンドを実施、または loop-detection vlan 1-4094 を実施するとデフォルト設定に戻ります。
制限・注意	• ループ検知フレームは 1 秒間に最大 80 個ずつ、有効にした VLAN の数だけ送信されます。 • 装置全体でループ検知できる VLAN の最大数は 100 個です。最大数まで検知した状態では、新たに別の VLAN でループが発生しても検知できません。検知状態の VLAN 数が最大数より少なくなれば、新たに別の VLAN でも検知可能です。
バージョン	1.08.02

使用例：ループ検知の動作モードが VLAN ベースモードの場合に、VLAN 100～200 でループ検知を有効にする方法を示します。

```
# configure terminal
(config)# loop-detection vlan 100-200
(config)#
```

5.6.7 loop-detection action notify-only

loop-detection action notify-only	
目的	ループ検知機能が有効なインターフェースにおいて、ループ検知時に当該インターフェースの閉塞、またはインターフェースの当該 VLAN でフレームの送受信停止を行わず、ログ、トラップによる通知のみ行うモードに設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	loop-detection action notify-only no loop-detection action notify-only
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード (interface port-channel コマンド) で設定してください。 本設定が有効の場合でも、ループを検知すると show loop-detection コマンド／show loop-detection status コマンドの Result 項目／Time Left 項目はループ検知表示になります。また、閉塞は行われませんが、show errdisable recovery コマンドでもループ検知ポート／VLAN として表示されます。 自動復旧設定(errdisable recovery cause loop-detection)が有効な場合は、最初にループを検知してから指定した時間が経過すると、各 show コマンドの表示は正常状態の表示に戻ります。その時点でまだループが解消していない場合は再度検知してループ検知表示になりますが、ループが解消していれば正常状態の表示のままです。 自動復旧設定が無効な場合は、ループが解消しても以下のいずれかの方法で手動復旧するまでは、各 show コマンドはループ検知表示のままになります。

loop-detection action notify-only	
	• 暫定的に自動復旧設定(errdisable recovery cause loop-detection)を適用することで、指定時間が経過すると各 show コマンドの表示が正常状態に戻ります。その後、自動復旧設定を削除して元に戻します。 • 対象ポートに対して shutdown コマンドを実行した後、no shutdown コマンドを実行することで、各 show コマンドの表示が正常状態に戻ります。なお、この方法の場合は対象ポートのリンクダウン／リンクアップを伴うことに注意してください。
制限・注意	• 本設定が有効の場合、ループが継続されている間は loop-detection interval コマンドで設定された間隔でログが出力され続けます。ループが解消された場合、約 30 秒後にループ検知ログの出力が停止します。 • 本コマンドをポートチャネルで設定する場合は、先にポートチャネルのメンバーポートを設定してから本コマンドを設定してください。メンバーポート未設定のポートチャネルで本コマンドを設定すると、コマンドは実行できますが、構成情報に表示されない制限があります。メンバーポートを設定すると表示されます。
バージョン	1.08.02

使用例：ポート 1/0/1 で、ループ検知時に当該インターフェースの閉塞、またはインターフェースの当該 VLAN でフレームの送受信停止を行わず、ログ、トラップによる通知のみ行うモードに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# loop-detection action notify-only
(config-if-port)#
```

5.6.8 loop-detection no-check-src

loop-detection no-check-src	
目的	ループ検知機能が有効なインターフェースにおいて、他の装置が送信したループ検知フレームを受信した場合にもループ検知するモードに設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	loop-detection no-check-src no loop-detection no-check-src
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード (interface port-channel コマンド) で設定してください。
制限・注意	• 本設定が有効なポートでは、ApresiaLight シリーズ(GM/FM/GS)が送信するループ検知フレームを受信した場合にもループを検知するようになります。なお、ApresiaLightGC シリーズが送信するループ検知フレームの場合は、受信してもループ検知はしません。 • 本コマンドをポートチャネルで設定する場合は、先にポートチャネルのメンバーポートを設定してから本コマンドを設定してください。メンバーポート未設定のポートチャネルで本コマンドを設定すると、コマンドは実行できますが、構成情報に表示されない制限があります。メンバーポートを設定すると表示されます。

loop-detection no-check-src	
バージョン	1.08.02

使用例：ポート 1/0/1 で、他の装置が送信したループ検知フレームを受信した場合にもループ検知するモードに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# loop-detection no-check-src
(config-if-port)#
```

5.6.9 errdisable recovery cause loop-detection

errdisable recovery cause loop-detection	
目的	ループ検知機能によって err-disabled 状態に変更されたポート／VLAN、またはループ検知表示のポート／VLAN（動作設定が notify-only の場合）の自動復旧を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	errdisable recovery cause loop-detection [interval SECONDS] no errdisable recovery cause loop-detection [interval]
Parameter	interval SECONDS（省略可能）：自動復旧するまでの待機時間を、5～86,400 秒の範囲で指定します。指定しない場合は 300 秒になります。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドの詳細や関連する show コマンドは「4.18 エラー復旧コマンド」を参照してください。 ループを検知した場合の動作が shutdown（デフォルト設定）の場合は、本コマンドを設定すると、ループ検知機能によって err-disabled 状態に変更されたポート／VLAN を、指定した時間で自動復旧することができます。 ループを検知した場合の動作が notify-only（ループを検知しても閉塞は行わず、ログ／トラップの通知のみ行うモード）の場合は、本コマンドを設定すると、各 show コマンドのループ検知表示を、指定した時間で正常状態の表示に自動復旧することができます。 ループ検知の動作モードがポートベースモードの場合、err-disabled 状態に変更されたポートのリンク状態は、show interfaces コマンドでは "link status is down (error disabled: Loop Detection)" と表示されます。show interfaces status コマンドの Status 項目では "err-disabled" と表示されます。 ポートベースのループ検知を使用している場合は、本コマンドの設定有無にかかわらず、err-disabled 状態のポートに対して shutdown コマンドを実行した後、no shutdown コマンドを実行することで、手動でポートを復旧することもできます。 VLAN ベースのループ検知を使用している場合も、ループを検知した VLAN が所属するポートに対して shutdown コマンド／no shutdown コマンドを実施することで手動で VLAN の err-disabled 状態を復旧することもできますが、この方法では対象ポートがリンクダウン／リンクアップするため、対象ポートに所属するすべての VLAN に影響があることに注意してください。
制限・注意	• 本設定は構成情報ではエラー復旧コマンド関連（ラベル# ERRDISABLE）で表示されます。

errdisable recovery cause loop-detection	
	• interval パラメーターをデフォルト（300 秒）以外に指定して設定している場合には、削除する際にも interval パラメーターまで指定して削除してください。
バージョン	1.08.02

使用例：ループ検知機能によって err-disabled 状態に変更されたポート／VLAN の自動復旧を、復旧までの待機時間 200 秒で有効にする方法を示します。

```
# configure terminal
(config)# errdisable recovery cause loop-detection interval 200
(config)#
```

5.6.10 snmp-server enable traps loop-detection

snmp-server enable traps loop-detection	
目的	ループ検知機能の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps loop-detection no snmp-server enable traps loop-detection
Parameter	なし
デフォルト	有効（snmp-server enable traps loop-detection）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。
制限・注意	-
バージョン	1.13.01

使用例：ループ検知機能の SNMP トラップを無効にする方法を示します。

```
# configure terminal
(config)# no snmp-server enable traps loop-detection
(config)#
```

5.6.11 show loop-detection

show loop-detection	
目的	ループ検知機能の設定とループ検知状態を表示します。
Command	show loop-detection [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定 • range port：物理ポートの範囲指定 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。

show loop-detection	
	ループを検知した場合の動作が notify-only（ループを検知しても閉塞は行わず、ログ／トラップの通知のみ行うモード）の場合でも、ループを検知すると Result 項目／Time Left 項目はループ検知表示になります。
制限・注意	• Frame Type 項目は AEOS-NP2500 Ver. 1.12.01 以降で表示されます。それぞれ、それより前のバージョンでは表示されません。
バージョン	1.08.02 1.12.01：Frame Type 項目を追加

使用例：ループ検知機能の設定とループ検知状態を表示する方法を示します。

```
# show loop-detection

 Loop Detection       : Disabled ...(1)
 Detection Mode       : port-based ...(2)
 Enabled VLAN         : all VLANs ...(3)
 Interval             : 10 seconds ...(4)
 Frame Type           : Priority Tag ...(5)
 (6)              (7)        (8)          (9)       (10)               (11)
 Interface        noChkSrc   Action       State     Result             Time Left
 ---------------  --------   -----------  --------  -----------------  ----------
 Port1/0/1        Enabled    shutdown     Enabled   Normal             -
 Port1/0/2        Disabled   shutdown     Disabled  Normal             -
 Port1/0/3        Disabled   shutdown     Disabled  Normal             -
 Port1/0/4        Disabled   shutdown     Disabled  Normal             -
 Port1/0/5        Disabled   shutdown     Disabled  Normal             -
 Port1/0/6        Disabled   shutdown     Disabled  Normal             -
 Port1/0/7        Disabled   shutdown     Disabled  Normal             -
 Port1/0/8        Disabled   shutdown     Disabled  Normal             -
 Port1/0/9        Disabled   shutdown     Disabled  Normal             -
 Port1/0/10       Disabled   shutdown     Disabled  Normal             -
 Port1/0/11       Disabled   shutdown     Disabled  Normal             -
 Port1/0/12       Disabled   shutdown     Disabled  Normal             -
 Port-channel2    Disabled   notify-only  Enabled   Normal             -
```

項番	説明
(1)	ループ検知機能のグローバル設定の有効(Enabled)／無効(Disabled)を表示します。
(2)	ループ検知の動作モードを表示します。 port-based：ポートベースモード vlan-based：VLAN ベースモード
(3)	VLAN ベースモードでループ検知が有効な VLAN を表示します。loop-detection vlan コマンドがデフォルト設定で、すべての VLAN でループ検知が有効な場合は「all VLANs」と表示されます。
(4)	ループ検知フレームの送信間隔を表示します。
(5)	ループ検知フレームの形式を表示します。 Priority Tag：デフォルト設定時(no loop-detection frame-type untagged) Untagged：loop-detection frame-type untagged コマンド設定時
(6)	ポート番号またはポートチャネル番号を表示します。
(7)	no-check-src オプションの有効(Enabled)／無効(Disabled)を表示します。
(8)	ループを検知した場合の動作を表示します。 shutdown：ループを検知したインターフェース、または VLAN を閉塞する

項番	説明
	notify-only：ループを検知しても閉塞は行わず、ログ／トラップの通知のみ行う
(9)	インターフェースごとのループ検知機能の有効(Enabled)／無効(Disabled)を表示します。
(10)	ループ検知状態を表示します。 Normal：ループを検知していない状態 Loop：ループを検知した状態（ポートベースモード） Loop on VLAN XX：VLAN XX でループを検知した状態（VLAN ベースモード）
(11)	ループを検知した場合の動作が shutdown（デフォルト設定）の場合は、err-disabled 状態に変更されたポート／VLAN が自動復旧されるまでの残り時間(秒)を表示します。 ループを検知した場合の動作が notify-only の場合は、ループ検知表示が自動復旧されるまでの残り時間(秒)を表示します。 XX：自動復旧されるまでの残り時間(秒) infinite：自動復旧設定が無効で、ループを検知した状態 -：ループを検知していない状態

使用例：ポートチャネル 2 のループ検知機能の設定とループ検知状態を表示する方法を示します。

```
# show loop-detection interface port-channel 2
 (1)              (2)       (3)           (4)       (5)                (6)
 Interface        noChkSrc  Action        State     Result             Time Left
 ---------------  --------  ------------  --------  -----------------  ----------
 Port-channel2    Disabled  notify-only   Enabled   Normal             -
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	no-check-src オプションの有効(Enabled)／無効(Disabled)を表示します。
(3)	ループを検知した場合の動作を表示します。 shutdown：ループを検知したインターフェース、または VLAN を閉塞する notify-only：ループを検知しても閉塞は行わず、ログ／トラップの通知のみ行う
(4)	インターフェースごとのループ検知機能の有効(Enabled)／無効(Disabled)を表示します。
(5)	ループ検知状態を表示します。 Normal：ループを検知していない状態 Loop：ループを検知した状態（ポートベースモード） Loop on VLAN XX：VLAN XX でループを検知した状態（VLAN ベースモード）
(6)	ループを検知した場合の動作が shutdown（デフォルト設定）の場合は、err-disabled 状態に変更されたポート／VLAN が自動復旧されるまでの残り時間(秒)を表示します。 ループを検知した場合の動作が notify-only の場合は、ループ検知表示が自動復旧されるまでの残り時間(秒)を表示します。 XX：自動復旧されるまでの残り時間(秒) infinite：自動復旧設定が無効で、ループを検知した状態 -：ループを検知していない状態

5.6.12 show loop-detection status

show loop-detection status	
目的	ループ検知機能の状態を表示します。
Command	show loop-detection status [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定 • range port：物理ポートの範囲指定 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、ループ検知機能が有効なすべてのインターフェースの情報が表示されます。 ループを検知した場合の動作が notify-only（ループを検知しても閉塞は行わず、ログ／トラップの通知のみ行うモード）の場合でも、ループを検知すると Result 項目／Time Left 項目はループ検知表示になります。
制限・注意	• ループ検知フレームは最大 64kbps で受信制限しているため、Receive 項目で表示される受信ループ検知フレーム数は、実際にポートで受信しているループ検知フレーム数より少なく表示されることがあります。
バージョン	1.12.01

使用例：ループ検知機能の状態を表示する方法を示します。

```
# show loop-detection status
 (1)              (2)    (3)       (4)          (5)          (6)
Interface         VLAN   Result    Time Left    Receive      Last Detection Time
---------------   ----   -------   ----------   ----------   -------------------
Port1/0/1         10     Loop      infinite              -   2022-09-02 09:47:12
Port1/0/2         20     Loop      infinite            232   2022-09-02 09:52:24
                  30     Loop      infinite            242   2022-09-02 09:53:24
Port-channel1     All    Normal    -                     0   -
```

項番	説明
(1)	ループ検知機能が有効なポート番号またはポートチャネル番号を表示します。
(2)	VLAN ベースモードで、ループを検知した VLAN を表示します。 XX：ループを検知した VLAN ID All：ループを検知した VLAN が存在しない状態
(3)	ループ検知状態を表示します。 Normal：ループを検知していない状態 Loop：ループを検知した状態
(4)	ループを検知した場合の動作が shutdown（デフォルト設定）の場合は、err-disabled 状態に変更されたポート／VLAN が自動復旧されるまでの残り時間(秒)を表示します。 ループを検知した場合の動作が notify-only の場合は、ループ検知表示が自動復旧されるまでの残り時間(秒)を表示します。 XX：自動復旧されるまでの残り時間(秒) infinite：自動復旧設定が無効で、ループを検知した状態 -：ループを検知していない状態

項番	説明
(5)	ログ／トラップの通知のみを行う設定(loop-detection action notify-only)の場合に、CPUで受信したループ検知フレームの累積受信数を表示します。「ループを検知した日時」が更新された場合、累積受信数のカウントも一度クリアされます。
(6)	最も直近にループを検知した日時を表示します。ログ／トラップの通知のみを行う設定(loop-detection action notify-only)では、定期的(loop-detection interval)にループ検知状態が継続しているかが確認されます。そして、継続している場合は「ループを検知した日時」が更新されます。

5.6.13 clear loop-detection information

clear loop-detection information	
目的	ループ検知状態に関連する情報を消去します。
Command	clear loop-detection information [interface IF-ID [,|-]]
Parameter	interface IF-ID (省略可能)：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定 • range port：物理ポートの範囲指定 • port-channel <1-48>：ポートチャネル指定
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドを実行すると、show loop-detection status コマンドで表示される「CPU で受信したループ検知フレームの累積受信数」と「最も直近にループを検知した日時」の情報が消去されます。 特定のインターフェースを指定しない場合は、ループ検知機能が有効なすべてのインターフェースの情報が消去されます。
制限・注意	-
バージョン	1.12.01

使用例：ループ検知状態に関連する情報を消去する方法を示します。

```
# clear loop-detection information
#
```

5.7 ストームコントロールコマンド

ストームコントロール関連の設定コマンドは以下のとおりです。

- storm-control
- storm-control action
- storm-control polling interval
- storm-control polling retries
- errdisable recovery cause storm-control
- snmp-server enable traps storm-control

ストームコントロール関連の show コマンドは以下のとおりです。

- show storm-control

5.7.1 storm-control

storm-control	
目的	ストームコントロール機能のしきい値を指定して有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {**pps** PPS-RISE [PPS-LOW] | **kbps** KBPS-RISE [KBPS-LOW] | LEVEL-RISE [LEVEL-LOW]} **no storm-control** {**broadcast** | **multicast** | **unicast**}
Parameter	broadcast：ブロードキャストを対象にする場合に指定します。 multicast：マルチキャストを対象にする場合に指定します。 unicast：Unknown ユニキャストを対象にする場合に指定します。アクションが shutdown 設定の場合は、Unknown ユニキャストだけでなく宛先学習済みユニキャストも対象になる仕様制限があります。 level pps PPS-RISE [PPS-LOW]：しきい値を 1 秒あたりの受信パケット数で指定します。 • PPS-RISE：上限値を 0～2,147,483,647 の範囲で指定します。 • PPS-LOW（省略可能）：下限値を 0～2,147,483,647 の範囲で指定します。指定しない場合は PPS-RISE の 80%の値となります。 level kbps KBPS-RISE [KBPS-LOW]：しきい値を 1 秒あたりの受信 Kbps で指定します。本パラメーターで設定した場合は、アクションとして shutdown は設定できません。また、ストームの検知／解消を示すログおよびトラップは出力されません。 • IFG（Inter Frame Gap）と Preamble を含めないで計測する仕様です。 • KBPS-RISE：上限値を 0～2,147,483,647 の範囲で 64Kbps 単位で指定します。 • KBPS-LOW（省略可能）：下限値を 0～2,147,483,647 の範囲で 64Kbps 単位で指定します。指定しない場合は KBPS-RISE の 80%の値となります。 level LEVEL-RISE [LEVEL-LOW]：しきい値をポートの総帯域幅に対するパーセンテージで指定します。本パラメーターで設定した場合は、アクションとして shutdown は設定できません。また、ストームの検知／解消を示すログおよびトラップは出力されません。 • IFG（Inter Frame Gap）と Preamble を含めないで計測する仕様です。 • LEVEL-RISE：上限値を 0～100 の範囲で指定します。

storm-control	
	• LEVEL-LOW（省略可能）：下限値を 0～100 の範囲で指定します。指定しない場合は LEVEL-RISE の 80%の値となります。
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ストームコントロールを使用する場合、しきい値は pps（1 秒あたりの受信パケット数）で指定することを推奨します。しきい値を kbps またはパーセンテージで指定した場合は、様々な制限事項があることに注意してください。 ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 ポートチャネルでストームコントロール機能を設定すると、ポートチャネルのすべてのメンバーポートに同じ内容でストームコントロール機能が設定されます。あるメンバーポートがストームを検知すると、アクションはそのメンバーポートにのみ適用されます。 アクションが drop 設定の場合、上限値を超えると対象トラフィックは上限値に帯域制限されます。 アクションが shutdown 設定の場合、上限値を超えると対象ポートはシャットダウン(err-disabled 状態に変更) されます。 しきい値が上限値を超えた場合にストーム検知ログを、下限値を下回った場合にストーム解消ログを出力します。
制限・注意	• しきい値の単位パラメーター（pps, kbps, パーセンテージ）は、同一ポートではすべて同じにする必要があります。すでに設定されている状態で、別の単位パラメーターを指定して設定した場合は、そのポートの既存の設定は削除されます。 • しきい値を kbps またはパーセンテージで設定した場合は、アクションとして shutdown は設定できません。 • しきい値を kbps またはパーセンテージで設定した場合は、ストームの検知／解消を示すログおよびトラップは出力されません。 • アクションに drop もしくは none を指定した場合は、Unicast に関するストームの検知／解消を示すログおよびトラップは出力されません。 • ポートチャネルでのストームコントロールは、AEOS-NP2500 Ver. 1.10.01 以降でサポートしています。それより前のバージョンでは対応していません。また、それより前のバージョンでは、本コマンドをポートチャネルのメンバーポートで設定することもできません。
バージョン	1.08.02 1.10.01：ポートチャネルでのストームコントロールをサポート

使用例：ポート 1/0/1 で、ブロードキャストのストームコントロールを上限値 500pps で有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# storm-control broadcast level pps 500
(config-if-port)#
```

使用例：ポートチャネル 1 で、マルチキャストのストームコントロールを上限値 300pps で有効にする方法を示します。

```
# configure terminal
(config)# interface port-channel 1
(config-if-port-channel)# storm-control multicast level pps 300
(config-if-port-channel)#
```

5.7.2 storm-control action

storm-control action	
目的	ストームコントロール機能のアクションを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	storm-control action {shutdown | drop | none} no storm-control action
Parameter	shutdown：上限値を超えると、ポートをシャットダウン（err-disabled 状態に変更）し、ログおよびトラップ(有効時)を出力する場合に指定します。 drop：上限値を超えると、対象トラフィックを上限値に帯域制限し、ログおよびトラップ(有効時)を出力する場合に指定します。 none：上限値を超えても帯域制限せずに、ログおよびトラップ(有効時)のみ出力する場合に指定します。
デフォルト	帯域制限動作（drop）
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 ポートチャネルでストームコントロール機能を設定すると、ポートチャネルのすべてのメンバーポートに同じ内容でストームコントロール機能が設定されます。あるメンバーポートがストームを検知すると、アクションはそのメンバーポートにのみ適用されます。 シャットダウン（err-disabled 状態に変更）されたポートを復旧するには、以下の 2 つの方法があります。 • errdisable recovery cause storm-control コマンドを使用して、ストームコントロール機能によって err-disabled 状態に変更されたポートの自動復旧を有効にできます。 • ポートに対して shutdown コマンドを実行した後、no shutdown コマンドを実行することで、手動でポートを復旧できます。
制限・注意	• しきい値を kbps またはパーセンテージで設定した場合は、アクションとして shutdown は設定できません。 • しきい値を kbps またはパーセンテージで設定した場合は、ストームの検知／解消を示すログおよびトラップは出力されません。 • マルチキャストのストーム検知には以下の制限動作があります。 • アクションが drop 設定の場合、宛先 IPv4 アドレスが予約 IPv4 マルチキャストアドレス（224.0.0.0～224.0.0.255）のパケットを、show storm-control コマンドやログ出力では multicast パラメーターの対象として扱いますが、帯域制限動作だけは broadcast パラメーターの対象として扱われる仕様制限があります。

storm-control action	

	• ユニキャストのストーム検知には以下の制限動作があります。
	  • アクションが drop または none 設定の場合、ストームの検知／解消を示すログおよびトラップは出力されません。
	  • アクションが shutdown 設定の場合は、Unknown ユニキャストだけでなく宛先学習済みユニキャストも対象になる仕様制限があります。ユニキャスト（Unknown ユニキャストと宛先学習済みユニキャストの両方）が上限値を超えると、シャットダウン（err-disabled 状態に変更）されます。
	• ポートチャネルでのストームコントロールは、AEOS-NP2500 Ver. 1.10.01 以降でサポートしています。それより前のバージョンでは対応していません。

バージョン	1.08.02 1.10.01：ポートチャネルでのストームコントロールをサポート

使用例：ポート 1/0/1 で、ストームコントロール機能のアクションを shutdown に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# storm-control action shutdown
(config-if-port)#
```

使用例：ポートチャネル 1 で、ストームコントロール機能のアクションを drop に設定する方法を示します。

```
# configure terminal
(config)# interface port-channel 1
(config-if-port-channel)# storm-control action drop
(config-if-port-channel)#
```

5.7.3 storm-control polling interval

storm-control polling interval	
目的	ストームコントロール機能の検知ポーリング間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	storm-control polling interval SECONDS no storm-control polling interval
Parameter	SECONDS：検知ポーリング間隔を 5～600 秒の範囲で指定します。
デフォルト	5 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポーリング間隔を 15 秒に設定する方法を示します。

```
# configure terminal
(config)# storm-control polling interval 15
(config)#
```

5.7.4 storm-control polling retries

storm-control polling retries	
目的	ストームコントロール機能の、シャットダウン（err-disabled 状態に変更）するまでのリトライ回数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	storm-control polling retries {VALUE | infinite} no storm-control polling retries
Parameter	VALUE：アクションが shutdown 設定の場合に、ストームを検知してからシャットダウン（err-disabled 状態に変更）するまでのリトライ回数を、0～360 回の範囲で指定します。 infinite：ストームを検知してもシャットダウン（err-disabled 状態に変更）しない場合に指定します。
デフォルト	3 回
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：リトライ回数を 5 回に設定する方法を示します。

```
# configure terminal
(config)# storm-control polling retries 5
(config)#
```

5.7.5 errdisable recovery cause storm-control

errdisable recovery cause storm-control	
目的	ストームコントロール機能によって err-disabled 状態に変更されたポートの自動復旧を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	errdisable recovery cause storm-control [interval SECONDS] no errdisable recovery cause storm-control [interval]
Parameter	interval SECONDS（省略可能）：自動復旧するまでの待機時間を、5～86,400 秒の範囲で指定します。指定しない場合は 300 秒になります。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドの詳細や関連する show コマンドは「4.18 エラー復旧コマンド」を参照してください。 本コマンドを設定すると、ストームコントロール機能によって err-disabled 状態に変更されたポートを、指定した時間で自動復旧することができます。 err-disabled 状態に変更されたポートのリンク状態は、show interfaces コマンドでは "link status is down（error disabled: Storm Control)" と表示されます。show interfaces status コマンドの Status 項目では "err-disabled" と表示されます。 本コマンドの設定有無にかかわらず、err-disabled 状態のポートに対して shutdown

errdisable recovery cause storm-control	
	コマンドを実行した後、no shutdown コマンドを実行することで、手動でポートを復旧することもできます。
制限・注意	• 本設定は構成情報ではエラー復旧コマンド関連（ラベル# ERRDISABLE）で表示されます。 • interval パラメーターをデフォルト（300 秒）以外に指定して設定している場合には、削除する際にも interval パラメーターまで指定して削除してください。
バージョン	1.08.02

使用例：ストームコントロール機能によって err-disabled 状態に変更されたポートの自動復旧を、復旧までの待機時間 200 秒で有効にする方法を示します。

```
# configure terminal
(config)# errdisable recovery cause storm-control interval 200
(config)#
```

5.7.6 snmp-server enable traps storm-control

snmp-server enable traps storm-control	
目的	ストームコントロール機能の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps storm-control no snmp-server enable traps storm-control
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。
制限・注意	-
バージョン	1.13.01

使用例：ストームコントロール機能の SNMP トラップを有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps storm-control
(config)#
```

5.7.7 show storm-control

show storm-control	
目的	ストームコントロールの状態を表示します。
Command	show storm-control interface IF-ID [,|-] [broadcast | multicast | unicast]
Parameter	interface IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定 • range port：物理ポートの範囲指定 • port-channel <1-48>：ポートチャネル指定 broadcast（省略可能）：ブロードキャストのストームコントロールの状態を表示する

show storm-control	
	場合に指定します。 multicast（省略可能）：マルチキャストのストームコントロールの状態を表示する場合に指定します。 unicast（省略可能）：Unknown ユニキャストのストームコントロールの状態を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• しきい値を kbps またはパーセンテージで設定していて、かつ受信パケットのサイズが 64 バイト以外の場合は、Current 項目と State 項目を正常に表示できない制限があります。 • ユニキャストのストームコントロールでは、Unknown ユニキャストと宛先学習済みユニキャストの両方が Current 項目でカウントされます。アクションが drop 設定の場合、State 項目は Current 項目が上限値を超えると Dropped と表示されるため、実際には Unknown ユニキャストが上限値に達しておらず破棄されていなくても、State 項目が Dropped と表示されることがあります。
バージョン	1.08.02 1.10.01：ポートチャネルでのストームコントロールをサポート

使用例：ポート 1/0/1～1/0/6 の、ブロードキャストのストームコントロールの状態を表示する方法を示します。

```
# show storm-control interface range port 1/0/1-1/0/6 broadcast
 (1)          (2)       (3)                    (4)          (5)
 Interface    Action    Threshold              Current      State
 ------------------------------------------------------------------------
 Port1/0/1    Drop      500/300 pps            200 pps      Forwarding
 Port1/0/2    Drop      80/64 %                20 %         Forwarding
 Port1/0/3    Drop      80/64 %                70 %         Dropped
 Port1/0/4    Shutdown  60/50 %                20 %         Forwarding
 Port1/0/5    None      60000/50000 kbps       2000 kbps    Forwarding
 Port1/0/6    None      -                      -            Inactive

 Total Entries: 6
```

項番	説明
(1)	ポート番号を表示します。
(2)	アクションを表示します。 Shutdown：ポートをシャットダウン（err-disabled 状態に変更）する Drop：上限値を超えるパケットを破棄する None：処理しない
(3)	しきい値の上限値／下限値、および単位を表示します。単位は以下を意味します。 pps：packets per second、1 秒あたりの受信パケット数 kbps：kilobit per second、1 秒あたりの受信キロビット数 %：ポートの総帯域幅に対する、受信トラフィックのパーセンテージ
(4)	対象トラフィックの現在の受信量を表示します。
(5)	アクションの状況を表示します。

項番	説明
	Forwarding：転送（受信量に問題がないためストームコントロールが実行されていない） Dropped：上限値を超えるパケットを破棄 Link Down：物理的なリンクダウン Error Disabled：ストームコントロールによるシャットダウン（err-disabled 状態） Inactive：ストームコントロール無効

使用例：ポート 1/0/1～1/0/2 のストームコントロールの状態を表示する方法を示します。

```
# show storm-control interface range port 1/0/1-2
 (1)                                  (2)
Polling Interval  : 5 sec             Shutdown Retries    : 3 times
 (3)         (4)         (5)       (6)                    (7)           (8)
Interface   Storm       Action    Threshold              Current       State
-------------------------------------------------------------------------------
Port1/0/1   Broadcast   Drop      80/64 %                50%           Forwarding
Port1/0/1   Multicast   Drop      80/64 %                50%           Forwarding
Port1/0/1   Unicast     Drop      80/64 %                50%           Forwarding
Port1/0/2   Broadcast   Shutdown  500/300 pps            -             Error Disabled
Port1/0/2   Multicast   Shutdown  500/300 pps            -             Error Disabled
Port1/0/2   Unicast     Shutdown  500/300 pps            -             Error Disabled

Total Entries: 6
```

項番	説明
(1)	ポーリング間隔を表示します。
(2)	シャットダウン（err-disabled 状態に変更）するまでのリトライ回数を表示します。
(3)	ポート番号を表示します。
(4)	監視するトラフィックの種類を表示します。
(5)	アクションを表示します。 Shutdown：ポートをシャットダウン（err-disabled 状態に変更）する Drop：上限値を超えるパケットを破棄する None：処理しない
(6)	しきい値の上限値／下限値、および単位を表示します。単位は以下を意味します。 pps：packets per second、1 秒あたりの受信パケット数 kbps：kilobit per second、1 秒あたりの受信キロビット数 %：ポートの総帯域幅に対する、受信トラフィックのパーセンテージ
(7)	対象トラフィックの現在の受信量を表示します。
(8)	アクションの状況を表示します。 Forwarding：転送（受信量に問題がないためストームコントロールが実行されていない） Dropped：上限値を超えるパケットを破棄 Link Down：物理的なリンクダウン Error Disabled：ストームコントロールによるシャットダウン（err-disabled 状態） Inactive：ストームコントロール無効

使用例：ポートチャネル 25（メンバーポートはポート 1/0/1 とポート 1/0/2）のストームコントロールの状態を表示する方法を示します。

```
# show storm-control interface port-channel 25
 (1)                                  (2)
Polling Interval  : 5 sec             Shutdown Retries    : 3 times
 (3)         (4)         (5)       (6)                    (7)           (8)
Interface   Storm       Action    Threshold              Current       State
-------------------------------------------------------------------------------
Group-25    Broadcast   Drop      1000/800 pps           -             -
Group-25    Multicast   Drop      2000/1600 pps          -             -
Group-25    Unicast     Drop      -                      -             -
-------------------------------------------------------------------------------
Port1/0/1   Broadcast   Drop      1000/800 pps           0 pps         Forwarding
Port1/0/1   Multicast   Drop      2000/1600 pps          0 pps         Forwarding
Port1/0/1   Unicast     Drop      -                      -             Inactive
Port1/0/2   Broadcast   Drop      1000/800 pps           0 pps         Forwarding
Port1/0/2   Multicast   Drop      2000/1600 pps          0 pps         Forwarding
Port1/0/2   Unicast     Drop      -                      -             Inactive

Total Entries: 6
```

項番	説明
(1)	ポーリング間隔を表示します。
(2)	シャットダウン（err-disabled 状態に変更）するまでのリトライ回数を表示します。
(3)	上段には指定したポートチャネル番号を、下段にはそのポートチャネルのメンバーポートを表示します。
(4)	監視するトラフィックの種類を表示します。
(5)	アクションを表示します。 Shutdown：ポートをシャットダウン（err-disabled 状態に変更）する Drop：上限値を超えるパケットを破棄する None：処理しない
(6)	しきい値の上限値／下限値、および単位を表示します。単位は以下を意味します。 pps：packets per second、1 秒あたりの受信パケット数 kbps：kilobit per second、1 秒あたりの受信キロビット数 %：ポートの総帯域幅に対する、受信トラフィックのパーセンテージ
(7)	対象トラフィックの現在の受信量を表示します。
(8)	アクションの状況を表示します。 Forwarding：転送（受信量に問題がないためストームコントロールが実行されていない） Dropped：上限値を超えるパケットを破棄 Link Down：物理的なリンクダウン Error Disabled：ストームコントロールによるシャットダウン（err-disabled 状態） Inactive：ストームコントロール無効

5.8 Egress フィルタリングコマンド

Egress フィルタリング関連の設定コマンドは以下のとおりです。

- egress-filtering

Egress フィルタリング関連の show コマンドは以下のとおりです。

- show egress-filtering

5.8.1 egress-filtering

egress-filtering	
目的	Egress フィルタリングを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	egress-filtering {umc | uuc | bc} no egress-filtering {umc | uuc | bc}
Parameter	umc：宛先不明マルチキャストフレームを対象にする場合に指定します。 uuc：宛先不明ユニキャストフレームを対象にする場合に指定します。 bc：ブロードキャストフレームを対象にする場合に指定します。
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	Egress フィルタリングを有効にしたインターフェースでは、指定したフレームのハードウェア中継による送信が制限(破棄)されます。 ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード (interface port-channel コマンド) で設定してください。 宛先不明マルチキャストフレームを指定して有効にした場合は、以下の機能で学習／設定したマルチキャストフレームは、Egress フィルタリングによる制限(破棄)の対象外になります。 • IGMP スヌーピングで学習した IPv4 マルチキャスト • MLD スヌーピングで学習した IPv6 マルチキャスト • mac-address-table static コマンドで設定したマルチキャスト MAC アドレスエントリー
制限・注意	• CPU から送信されるフレーム、および CPU によりソフトウェア中継されるフレームは Egress フィルタリングによる制限(破棄)の対象外です。 • 同一ポート／同一ポートチャネルで、egress-filtering umc と「IGMP スヌーピングの ip igmp snooping unregistered-filter、または MLD スヌーピングの ipv6 mld snooping unregistered-filter」の併用は未サポートです。 • Egress フィルタリングは MAC アドレスベースで処理されます。 • 宛先不明マルチキャストフレームを指定した場合は予約 IPv4 マルチキャスト(224.0.0.0/24)、および予約 IPv6 マルチキャスト(ff02::/111, ff02::1:ff00:0/104, ff05::/111)も制限(破棄)されます。
バージョン	1.10.02

使用例：ポート 1/0/1 で、宛先不明マルチキャストを指定して Egress フィルタリングを有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# egress-filtering umc
(config-if-port)#
```

5.8.2 show egress-filtering

show egress-filtering	
目的	Egress フィルタリングの設定を表示します。
Command	show egress-filtering {umc | uuc | bc}
Parameter	umc：宛先不明マルチキャストフレームの設定を表示する場合に指定します。 uuc：宛先不明ユニキャストフレームの設定を表示する場合に指定します。 bc：ブロードキャストフレームの設定を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	ポートチャネルのメンバーポートで egress-filtering を設定しても、本コマンドでは表示されません。ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。
制限・注意	-
バージョン	1.10.02

使用例：Egress フィルタリングの設定を表示する方法を示します。

```
# show egress-filtering umc

Unknown Multicast Egress Filtering: 1/0/3-1/0/4,1/0/6, port-channel5 ...(1)

# show egress-filtering uuc

Unknown Unicast Egress Filtering: 1/0/1,1/0/5 ...(2)

# show egress-filtering bc

Broadcast Egress Filtering: 1/0/1,1/0/3 ...(3)
```

項番	説明
(1)	宛先不明マルチキャストフレームの Egress フィルタリングを有効にしたポート番号およびポートチャネル番号を表示します。
(2)	宛先不明ユニキャストフレームの Egress フィルタリングを有効にしたポート番号およびポートチャネル番号を表示します。
(3)	ブロードキャストフレームの Egress フィルタリングを有効にしたポート番号およびポートチャネル番号を表示します。

5.9 マルチキャストフィルタリングモードコマンド

マルチキャストフィルタリングモード関連の設定コマンドは以下のとおりです。

- multicast filtering-mode

マルチキャストフィルタリングモード関連の show コマンドは以下のとおりです。

- show multicast filtering-mode

5.9.1 multicast filtering-mode

multicast filtering-mode	
目的	VLAN ごとのマルチキャストフレームの中継処理方法（マルチキャストフィルタリングモード）を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered} no multicast filtering-mode
Parameter	forward-all：登録済み／未登録にかかわらず、すべてのマルチキャストフレームを同一 VLAN のすべてのポートにフラッディングする場合に指定します。 forward-unregistered：登録済みのマルチキャストフレームは登録されたポートのみに転送し、未登録のマルチキャストフレームはフラッディングする場合に指定します。 filter-unregistered：登録済みのマルチキャストフレームは登録されたポートのみに転送し、未登録のマルチキャストフレームはフィルタリングする場合に指定します。
デフォルト	forward-unregistered
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	登録済み／未登録のマルチキャストフレームとは、以下を意味します。 • マルチキャスト MAC アドレス宛てのスタティック MAC アドレスエントリー設定あり（登録済み）／設定なし（未登録） • IGMP スヌーピング使用時に、IPv4 マルチキャスト転送キャッシュに登録済み／未登録 • MLD スヌーピング使用時に、IPv6 マルチキャスト転送キャッシュに登録済み／未登録 本コマンドを filter-unregistered モードで設定した場合でも、以下の予約されたアドレス宛てのマルチキャストフレームは、フィルタリングされずにフラッディング中継されます。なおこのケースでは、予約 IPv6 マルチキャスト宛て（ff0X::除く）はソフトウェア中継に変更されます。 • 予約 IPv4 マルチキャスト（224.0.0.0～224.0.0.255） • AEOS-NP2500 Ver. 1.12.01 以降：予約 IPv6 マルチキャスト（ff0X::, ff02::/111, ff02::1:ff00:0/104, ff05::/111） • AEOS-NP2500 Ver. 1.12.01 より前のバージョン：予約 IPv6 マルチキャスト（ff0X::, ff02::1, ff02::2, ff05::2, ff02::1:ff00:0/104, ff02::4, ff02::5, ff02::6, ff02::9, ff02::c, ff02::d, ff02::12, ff02::16, ff02::1:2, ff02::1:3, ff05::1:3）
制限・注意	• IGMP スヌーピングの ip igmp snooping unregistered-filter、または MLD スヌーピングの ipv6 mld snooping unregistered-filter を使用する場合は、対象

multicast filtering-mode	
	VLAN のマルチキャストフィルタリングモードはデフォルト設定(multicast filtering-mode forward-unregistered)のまま使用してください。
バージョン	1.08.02 1.12.01：filter-unregistered モード設定時のフィルター対象外の予約 IPv6 マルチキャストの仕様変更

使用例：VLAN 100 でマルチキャストフィルタリングモードを filter-unregistered に設定する方法を示します。

```
# configure terminal
(config)# vlan 100
(config-vlan)# multicast filtering-mode filter-unregistered
(config-vlan)#
```

5.9.2 show multicast filtering-mode

show multicast 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。
Command	show multicast filtering-mode [vlan VLAN-ID]
Parameter	vlan VLAN-ID（省略可能）：マルチキャストフィルタリングモードを表示する VLAN ID を 1～4094 の範囲で指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべての VLAN のマルチキャストフィルタリングモードを表示する方法を示します。

```
# show multicast filtering-mode
(1)                               (2)
Interface                         Layer 2 Multicast Filtering Mode
--------------------------------  --------------------------------
default                           forward-unregistered
VLAN0002                          forward-unregistered

Total Entries: 2
```

項番	説明
(1)	VLAN 名を表示します。
(2)	マルチキャストフィルタリングモードを表示します。 forward-all：すべてのマルチキャストフレームをフラッディング forward-unregistered：登録済みのマルチキャストフレームは登録されたポートのみに転送し、未登録のマルチキャストフレームはフラッディング filter-unregistered：登録済みのマルチキャストフレームは登録されたポートのみに転送し、未登録のマルチキャストフレームはフィルタリング

5.10 IGMP スヌーピングコマンド

IGMP スヌーピング関連の設定コマンドは以下のとおりです。

- ip igmp snooping
- ip igmp snooping（VLAN）
- ip igmp snooping unregistered-filter
- ip igmp snooping dyn-mr-aging-time
- ip igmp snooping mrouter
- ip igmp snooping minimum-version
- ip igmp snooping fast-leave
- ip igmp snooping querier
- ip igmp snooping query-version
- ip igmp snooping query-interval
- ip igmp snooping query-max-response-time
- ip igmp snooping robustness-variable
- ip igmp snooping last-member-query-interval
- ip igmp snooping static-group
- ip igmp snooping report-suppression
- ip igmp snooping suppression-time
- ip igmp snooping proxy-reporting
- ip igmp snooping unknown-data learn
- ip igmp snooping unknown-data expiry-time
- ip igmp snooping unknown-data limit
- ip igmp snooping ignore-topology-change-notification

IGMP スヌーピング関連の show／操作コマンドは以下のとおりです。

- show ip igmp snooping
- show ip igmp snooping mrouter
- show ip igmp snooping groups
- show ip igmp snooping static-group
- show ip igmp snooping statistics
- clear ip igmp snooping groups
- clear ip igmp snooping unknown-data
- clear ip igmp snooping statistics

5.10.1 ip igmp snooping

ip igmp snooping	
目的	グローバル設定モードで、装置全体の IGMP スヌーピング機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping no ip igmp snooping
Parameter	なし
デフォルト	装置全体の IGMP スヌーピング機能は無効
モード	グローバル設定モード

ip igmp snooping	
特権レベル	レベル：12
ガイドライン	IGMP スヌーピング機能を使用する場合は、グローバル設定モードの ip igmp snooping コマンドで装置全体の IGMP スヌーピング機能を有効にして、VLAN 設定モードの ip igmp snooping コマンドで対象 VLAN を有効にしてください。
制限・注意	• ApresiaNP2500 シリーズの IGMP スヌーピングは、MAC アドレスベースで処理されます。そのため、同一 MAC アドレスのマルチキャストグループの中継動作は同じになることに注意してください。 • 例えば、同一 MAC アドレス(01:00:5E:01:01:01)の 232.1.1.1 と 239.1.1.1 のマルチキャストグループをマルチキャストルーターポートで受信しているとします。その状況で、あるポートで 239.1.1.1 への参加メッセージを受信して参加すると、show ip igmp snooping groups や show ip mroute forwarding-cache では 239.1.1.1 だけをそのポートに中継しているように見えますが、実際には 232.1.1.1 もそのポートに中継されます。 • 同様に、あるポートが 232.1.1.1 と 239.1.1.1 の両方に参加している状況で、そのポートで 239.1.1.1 からの離脱メッセージを受信すると、show ip igmp snooping groups や show ip mroute forwarding-cache では 239.1.1.1 は離脱したように見えますが、実際には同一 MAC アドレスの 232.1.1.1 が参加状態のため、232.1.1.1 だけでなく 239.1.1.1 もまだそのポートに中継されます。 • また、MAC アドレスベースで処理されるため、IGMPv3 の送信元指定の参加要求を受信して登録されても、送信元フィルタリングは動作しないことに注意してください。show ip igmp snooping groups や show ip mroute forwarding-cache では指定した送信元の情報を含んで表示されますが、送信元が一致しないマルチキャストグループも中継されます。
バージョン	1.08.02

使用例：グローバル設定モードで IGMP スヌーピング機能を有効にする方法を示します。

```
# configure terminal
(config)# ip igmp snooping
(config)#
```

5.10.2 ip igmp snooping (VLAN)

ip igmp snooping (VLAN)	
目的	VLAN 設定モードで、対象 VLAN の IGMP スヌーピング機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping no ip igmp snooping
Parameter	なし
デフォルト	すべての VLAN の IGMP スヌーピング機能は無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	IGMP スヌーピング機能を使用する場合は、グローバル設定モードの ip igmp snooping コマンドで装置全体の IGMP スヌーピング機能を有効にして、VLAN 設定モードの ip igmp snooping コマンドで対象 VLAN を有効にしてください。
制限・注意	-

ip igmp snooping（VLAN）	
バージョン	1.08.02

使用例：VLAN 1 の IGMP スヌーピング機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping
(config-vlan)#
```

5.10.3 ip igmp snooping unregistered-filter

ip igmp snooping unregistered-filter	
目的	IGMP スヌーピングとして未登録のマルチキャストパケットを、送信せずに破棄（unregistered-filter）するインターフェースを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping unregistered-filter interface IF-ID [,|-] no ip igmp snooping unregistered-filter interface IF-ID [,|-]
Parameter	interface IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	設定なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドのフィルター対象になる「IGMP スヌーピングとして未登録のマルチキャストパケット」とは、以下のいずれにも登録されていないエントリーが対象になります。 • IGMP スヌーピングテーブルに登録されていないエントリー宛てのマルチキャストパケット（IGMP スヌーピングエントリーは show ip igmp snooping groups コマンドで確認可能） • IPv4 マルチキャスト転送キャッシュに登録されていないエントリー宛てのマルチキャストパケット（IPv4 マルチキャスト転送キャッシュは show ip mroute forwarding-cache コマンドで確認可能） 以下のマルチキャストパケットは、本コマンドのフィルター対象外です。 • IGMP スヌーピングテーブルに登録されているマルチキャスト • IGMP スヌーピングテーブルには登録されていないが、IPv4 マルチキャスト転送キャッシュには登録されているマルチキャスト • 予約 IPv4 マルチキャスト（224.0.0.0/24） • mac-address-table static コマンドでスタティックに設定したマルチキャスト MAC アドレスエントリー宛てのマルチキャスト 本コマンドの unregistered-filter はマルチキャストルーターポートに設定した場合にも動作するため、マルチキャストルーターポートでは設定しないことを推奨します。
制限・注意	• 本コマンドを使用する場合、対象 VLAN のマルチキャストフィルタリングモードはデフォルト設定（multicast filtering-mode forward-unregistered）のまま使用してください。 • 同一ポート／同一ポートチャネルで「宛先不明マルチキャストフレームを対象にした Egress フィルタリング（egress-filtering umc）」の併用は未サポートです。

ip igmp snooping unregistered-filter	
	• 本コマンドで設定する unregistered-filter は、ポート／ポートチャネルごとの設定なことに注意してください。VLAN ごとにマルチキャストルーターポートが異なるような場合は、すべての VLAN でマルチキャストルーターポートが同一になるような設計に見直してから使用してください。 • 本機能はアクセスリスト機能と同じハードウェアリソース（Ingress グループ）を使用します。本機能で使用中の Ingress グループは、他の機能では使用できません。グループの利用状況は show access-list resource reserved-group コマンドで確認できます。
バージョン	1.12.01

使用例：ポート 1/0/1～1/0/8 を指定して、IGMP スヌーピングの unregistered-filter を設定する方法を示します。

```
# configure terminal
(config)# ip igmp snooping unregistered-filter interface port 1/0/1-8
(config)#
```

5.10.4 ip igmp snooping dyn-mr-aging-time

ip igmp snooping dyn-mr-aging-time	
目的	動的に学習したマルチキャストルーターポートのエージングタイムを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip igmp snooping dyn-mr-aging-time SECONDS no ip igmp snooping dyn-mr-aging-time
Parameter	SECONDS：エージングタイムを 10～65,535 秒の範囲で指定します。
デフォルト	300 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	IGMP スヌーピングを有効にすると、クエリアが送信する Membership Query の受信ポートや、PIM または DVMRP 制御パケットの受信ポートを、マルチキャストルーターポートとして動的に学習します。本コマンドでは、動的に学習したマルチキャストルーターポートのエージングタイムを設定できます。
制限・注意	• マルチキャストルーターポートのエージングタイムは、学習／更新のトリガーとなるパケットの送信間隔よりも大きな値を設定してください。
バージョン	1.08.02

使用例：動的に学習したマルチキャストルーターポートのエージングタイムを、100 秒に設定する方法を示します。

```
# configure terminal
(config)# ip igmp snooping dyn-mr-aging-time 100
(config)#
```

5.10.5 ip igmp snooping mrouter

ip igmp snooping mrouter	
目的	マルチキャストルーターポートをスタティックに設定します。また、マルチキャストルーターポートになることを禁止するインターフェースを設定します。設定を削除す

ip igmp snooping mrouter	
	る場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping mrouter [forbidden] interface IF-ID [,|-] no ip igmp snooping mrouter [forbidden] interface IF-ID [,|-]
Parameter	forbidden（省略可能）：マルチキャストルーターポートになることを禁止するインターフェースを設定する場合に指定します。 interface IF-ID：マルチキャストルーターポートとして設定するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	マルチキャストルーターポートの設定なし
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	IGMP スヌーピングを有効にすると、クエリアが送信する Membership Query の受信ポートや、PIM または DVMRP 制御パケットの受信ポートを、マルチキャストルーターポートとして動的に学習します。本コマンドでは、マルチキャストルーターポートをスタティックに設定できます。 マルチキャストルーターポートとしてポートチャネルを指定する場合は、interface port-channel パラメーターで指定してください。ポートチャネルのメンバーポートを指定して設定しないでください。 forbidden パラメーターを指定して設定すると、対象のインターフェースが動的に学習してマルチキャストルーターポートになることを禁止できます。
制限・注意	• 設定する VLAN に所属していないポートまたはポートチャネルを指定して設定した場合は、警告メッセージが表示されます。
バージョン	1.08.02

使用例：VLAN 1 のポート 1/0/1 をマルチキャストルーターポートとしてスタティックに設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping mrouter interface port 1/0/1
(config-vlan)#
```

5.10.6 ip igmp snooping minimum-version

ip igmp snooping minimum-version	
目的	レシーバーからの参加要求（Membership Report）を許可する IGMP の最小バージョンを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping minimum-version {2 | 3} no ip igmp snooping minimum-version
Parameter	2：IGMPv1 Membership Report による参加要求を拒否する場合に指定します。 3：IGMPv1 Membership Report、または IGMPv2 Membership Report による参加要求を拒否する場合に指定します。
デフォルト	最小バージョンの設定なし
モード	VLAN 設定モード

ip igmp snooping minimum-version	
特権レベル	レベル：12
ガイドライン	本コマンドは Membership Report にのみ適用されます。拒否された Membership Report はマルチキャストルーターポートに中継されません。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、参加要求を許可する IGMP の最小バージョンを 2 に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping minimum-version 2
(config-vlan)#
```

5.10.7 ip igmp snooping fast-leave

ip igmp snooping fast-leave	
目的	IGMP スヌーピングの高速離脱機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping fast-leave [group-list ACL-NAME] no ip igmp snooping fast-leave
Parameter	group-list ACL-NAME（省略可能）：IGMP スヌーピングの高速離脱の対象にするマルチキャストグループを定義した、IP アクセスリストを指定します。指定しない場合、すべてのマルチキャストグループが高速離脱の対象になります。
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	IGMP スヌーピングの高速離脱の対象にするマルチキャストグループを指定する場合は、IP アクセスリストで対象となるマルチキャストグループを permit ルールの「宛先 IP アドレス」条件で指定します。「送信元 IP アドレス」条件はサポートしていないため any で設定してください。また、deny ルールはサポートしていません。 IGMP スヌーピングの高速離脱機能が有効な場合は、自装置が代表クエリア／非代表クエリアのいずれの場合でも、レシーバーからの離脱要求を受信すると、即座に対象の IGMP スヌーピングエントリーを削除します。 IGMP スヌーピングの高速離脱機能が無効な場合は、レシーバーが離脱要求を送信すると、IGMP スヌーピングエントリーのタイマー（削除されるまでの時間）は以下のように更新されます。そして、いずれのレシーバーからも応答がない場合はタイマーが満了して削除されます。 • 自装置が代表クエリアでレシーバーからの離脱要求を受信すると、「ロバストネス変数×ip igmp snooping last-member-query-interval コマンドで設定した送信間隔」が現状のタイマー値よりも小さい場合は、その値に更新されます。 • 自装置が非代表クエリアで代表クエリアからの Group-Specific Query または Group-and-Source-Specific Query を受信すると、「ロバストネス変数×Group-Specific Query または Group-and-Source-Specific Query の最大応答時間」が現状のタイマー値よりも小さい場合は、その値に更新されます。
制限・注意	• 説明に記載されている種別以外のアクセスリストを指定して使用できません。

ip igmp snooping fast-leave	
	• 本設定の group-list パラメーターで指定する IP アクセスリストでは、装置のハードウェアリソースを使用しません。
バージョン	1.08.02

使用例：VLAN 1 で、IGMP スヌーピングの高速離脱機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping fast-leave
(config-vlan)#
```

5.10.8 ip igmp snooping querier

ip igmp snooping querier	
目的	IGMP スヌーピングのクエリアを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping querier no ip igmp snooping querier
Parameter	なし
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	同一サブネットに所属するクエリアが複数存在する場合は、IPv4 アドレスの小さいクエリアが代表クエリアになります。 本装置が代表クエリア／非代表クエリアのいずれの場合でも、IGMP スヌーピングエントリーが登録／更新された際のタイマー（削除されるまでの時間）は、自装置のパラメーター（ip igmp snooping query-interval コマンド、ip igmp snooping robustness-variable コマンド）で決定されます。
制限・注意	• IGMP スヌーピングのクエリアを有効にするには、対象 VLAN の VLAN インターフェースを作成し、IPv4 アドレスが設定されている必要があります。 • セカンダリーIP アドレスでは IGMP クエリア機能は動作しません。
バージョン	1.08.02

使用例：VLAN 1 で、IGMP スヌーピングのクエリアを有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping querier
(config-vlan)#
```

5.10.9 ip igmp snooping query-version

ip igmp snooping query-version	
目的	IGMP スヌーピングのクエリアのバージョンを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip igmp snooping query-version {1 | 2 | 3} no ip igmp snooping query-version

ip igmp snooping query-version	
Parameter	{1 | 2 | 3}：IGMP スヌーピングのクエリアのバージョンを指定します。
デフォルト	IGMP バージョン 3
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	本コマンドで設定する IGMP バージョン設定は、IGMP のクエリアが送信する Membership Query に反映されます。 本コマンドでクエリアのバージョンを 2 または 3 に設定していて、かつ同一サブネットに所属するクエリアが複数存在する場合は、IPv4 アドレスの小さいクエリアが代表クエリアになります。 本コマンドでクエリアのバージョンを 1 に設定すると、本装置のクエリアは常に代表クエリアとして動作します。そのため、バージョン 1 設定で使用する場合は、同一サブネットに他のクエリアが存在しない環境で使用してください。
制限・注意	• IGMP バージョン 2 または IGMP バージョン 3 のクエリアを使用しているサブネットには、IGMP バージョン 1 のクエリアを接続しないようにしてください。
バージョン	1.08.02

使用例：VLAN 1 で、IGMP スヌーピングのクエリアのバージョンを 2 に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping query-version 2
(config-vlan)#
```

5.10.10 ip igmp snooping query-interval

ip igmp snooping query-interval	
目的	IGMP スヌーピングのクエリアが定期的に送信する Membership Query の送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip igmp snooping query-interval SECONDS no ip igmp snooping query-interval
Parameter	SECONDS：定期的に送信する Membership Query の送信間隔を、1～31,744 秒の範囲で指定します。
デフォルト	125 秒
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• Membership Query の送信間隔は、Membership Query の最大応答時間よりも大きい値になるように設定する必要があります。
バージョン	1.08.02

使用例：VLAN 1 で、IGMP スヌーピングのクエリアが定期的に送信する Membership Query の送信間隔を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping query-interval 300
(config-vlan)#
```

5.10.11 ip igmp snooping query-max-response-time

ip igmp snooping query-max-response-time	
目的	IGMP スヌーピングのクエリアが送信する Membership Query で通知される最大応答時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip igmp snooping query-max-response-time SECONDS no ip igmp snooping query-max-response-time
Parameter	SECONDS：Membership Query の最大応答時間を 1～25 秒の範囲で指定します。
デフォルト	10 秒
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• Membership Query の最大応答時間は、Membership Query の送信間隔よりも小さい値になるように設定する必要があります。
バージョン	1.08.02

使用例：VLAN 1 で、Membership Query の最大応答時間を 20 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping query-max-response-time 20
(config-vlan)#
```

5.10.12 ip igmp snooping robustness-variable

ip igmp snooping robustness-variable	
目的	IGMP スヌーピングのロバストネス変数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip igmp snooping robustness-variable VALUE no ip igmp snooping robustness-variable
Parameter	VALUE：ロバストネス変数を 1～7 の範囲で指定します。
デフォルト	2
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	ロバストネス変数を大きく設定することで、IGMP スヌーピングエントリーが削除されるまでの残り時間などを増やすことができます。これにより、輻輳などで IGMP メッセージがパケットロスすることへの影響を緩和できます。 Group Membership Interval（IGMP スヌーピングエントリーのレシーバーが存在しないと判断するまでの時間）は、以下の計算式で算出されます。 • (ロバストネス変数×クエリー送信間隔) + (1×最大応答時間) Other Querier Present Interval（自装置が非代表クエリアの場合に、代表クエリアが存在しないと判断するまでの時間）は、以下の計算式で算出されます。 • (ロバストネス変数×クエリー送信間隔) + (0.5×最大応答時間) IGMP スヌーピングのクエリアが有効設定の場合に、装置を起動した直後などは、通常よりも短い間隔で Membership Query を送信します。その送信間隔は通常のクエ

ip igmp snooping robustness-variable	
	リー送信間隔の 1/4 で、ロバストネス変数の回数送信されます。 IGMP スヌーピングのクエリアが有効で自装置が代表クエリアの場合に、登録済みのエントリーに対して離脱要求を受信すると、Group-Specific Query または Group-and-Source-Specific Query を送信します。その送信間隔は ip igmp snooping last-member-query-interval コマンドで設定した送信間隔で、ロバストネス変数の回数送信されます。
制限・注意	• ロバストネス変数を 1 で使用することは規格で推奨されていないため、ロバストネス変数は 2 以上で使用してください。
バージョン	1.08.02

使用例：VLAN 1 で、IGMP スヌーピングのロバストネス変数を 3 に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping robustness-variable 3
(config-vlan)#
```

5.10.13 ip igmp snooping last-member-query-interval

ip igmp snooping last-member-query-interval	
目的	IGMP スヌーピングのクエリアの、Group-Specific Query または Group-and-Source-Specific Query の送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip igmp snooping last-member-query-interval SECONDS no ip igmp snooping last-member-query-interval
Parameter	SECONDS：Group-Specific Query または Group-and-Source-Specific Query の送信間隔を、1～25 秒の範囲で指定します。
デフォルト	1 秒
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	IGMP スヌーピングのクエリアが有効で自装置が代表クエリアの場合に、登録済みの IGMP スヌーピングエントリーに対して離脱要求を受信すると、Group-Specific Query または Group-and-Source-Specific Query を送信します。その送信間隔は本コマンドで設定した送信間隔で、ロバストネス変数の回数送信されます。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、Group-Specific Query または Group-and-Source-Specific Query の送信間隔を、3 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping last-member-query-interval 3
(config-vlan)#
```

5.10.14 ip igmp snooping static-group

ip igmp snooping static-group	
目的	スタティック IGMP スヌーピングエントリーを設定します。設定を削除する場合は、

ip igmp snooping static-group	
	no 形式のコマンドを使用します。
Command	ip igmp snooping static-group GROUP-ADDRESS interface IF-ID [,|-] no ip igmp snooping static-group GROUP-ADDRESS [interface IF-ID [,|-]]
Parameter	GROUP-ADDRESS：IPv4 マルチキャストグループアドレスを指定します。 interface IF-ID：スタティック IGMP スヌーピングエントリーに登録するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	スタティック IGMP スヌーピングエントリーの設定なし
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1、IPv4 マルチキャストグループアドレス 233.252.0.1、登録ポート 1/0/5 で、スタティック IGMP スヌーピングエントリーを設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping static-group 233.252.0.1 interface port 1/0/5
(config-vlan)#
```

5.10.15 ip igmp snooping report-suppression

ip igmp snooping report-suppression	
目的	IGMP スヌーピングのレポート抑制機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping report-suppression no ip igmp snooping report-suppression
Parameter	なし
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	レポート抑制機能は、IGMPv1 と IGMPv2 トラフィックにだけ機能します。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、IGMP スヌーピングのレポート抑制機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping report-suppression
(config-vlan)#
```

5.10.16 ip igmp snooping suppression-time

ip igmp snooping suppression-time	
目的	重複した IGMP レポート、または脱退メッセージを抑制する期間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip igmp snooping suppression-time SECONDS no ip igmp snooping suppression-time
Parameter	SECONDS：重複した IGMP レポートを抑制する期間を 1～300 秒の範囲で指定します。
デフォルト	10 秒
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	抑制期間を短くすると、重複する IGMP パケットの送信間隔が短くなります。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1000 で、抑制期間を 125 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ip igmp snooping suppression-time 125
(config-vlan)#
```

5.10.17 ip igmp snooping proxy-reporting

ip igmp snooping proxy-reporting	
目的	IGMP スヌーピングのプロキシレポーティング機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping proxy-reporting [source IP-ADDRESS] no ip igmp snooping proxy-reporting
Parameter	source IP-ADDRESS（省略可能）：プロキシレポーティングの送信元 IPv4 アドレスを指定します。
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	source IP-ADDRESS で IPv4 アドレスを指定しない場合は 0.0.0.0 が使用されます。
制限・注意	• 本コマンドを使用する場合は、対象 VLAN の VLAN インターフェースに IPv4 アドレスを設定して使用してください。
バージョン	1.08.02

使用例：VLAN 1 で送信元 IP=192.0.2.100 を指定して IGMP スヌーピングのプロキシレポーティング機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping proxy-reporting source 192.0.2.100
(config-vlan)#
```

5.10.18 ip igmp snooping unknown-data learn

ip igmp snooping unknown-data learn	
目的	レシーバーが存在しない IPv4 マルチキャストを受信した場合に、宛先が未知の IPv4 マルチキャストとして学習する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping unknown-data learn no ip igmp snooping unknown-data learn
Parameter	なし
デフォルト	有効（ip igmp snooping unknown-data learn）
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	本設定が有効（デフォルト設定）の場合は、レシーバーからの参加要求を受信していない状態で IPv4 マルチキャストを受信すると、宛先が未知の IPv4 マルチキャストとして IPv4 マルチキャスト転送キャッシュと IGMP スヌーピングテーブルに登録されます。 登録された宛先が未知の IPv4 マルチキャストは、マルチキャストルーターポートにのみ転送され、それ以外のポートには転送されません。 本設定を無効にすると、宛先が未知の IPv4 マルチキャストを登録しないように変更できます。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、レシーバーが存在しない IPv4 マルチキャストを受信した場合に、宛先が未知の IPv4 マルチキャストとして学習する機能を無効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# no ip igmp snooping unknown-data learn
(config-vlan)#
```

5.10.19 ip igmp snooping unknown-data expiry-time

ip igmp snooping unknown-data expiry-time	
目的	IGMP スヌーピングで学習した宛先が未知の IPv4 マルチキャストの有効期限を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip igmp snooping unknown-data expiry-time SECONDS no ip igmp snooping unknown-data expiry-time
Parameter	SECONDS：有効期限を 1～65,535 秒の範囲で指定します。
デフォルト	有効期限なし（no ip igmp snooping unknown-data expiry-time）
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、IGMP スヌーピングで学習した宛先が未知の IPv4 マルチキャストの有効期限を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping unknown-data expiry-time 300
(config-vlan)#
```

5.10.20 ip igmp snooping unknown-data limit

ip igmp snooping unknown-data limit	
目的	IGMP スヌーピングで学習する宛先が未知の IPv4 マルチキャストの上限数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip igmp snooping unknown-data limit VALUE no ip igmp snooping unknown-data limit
Parameter	VALUE：上限数を 1～128 の範囲で指定します。
デフォルト	128
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：IGMP スヌーピングで学習する宛先が未知の IPv4 マルチキャストの上限数を、100 に設定する方法を示します。

```
# configure terminal
(config)# ip igmp snooping unknown-data limit 100
(config)#
```

5.10.21 ip igmp snooping ignore-topology-change-notification

ip igmp snooping ignore-topology-change-notification	
目的	スパニングツリープロトコルのトポロジーの変化を無視し、誘発されるクエリーを送信しない機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ip igmp snooping ignore-topology-change-notification no ip igmp snooping ignore-topology-change-notification
Parameter	なし
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	IGMP スヌーピングを有効にした装置では、スパニングツリー動作によって生じたリンクレイヤートポロジーの変化を認識します。スパニングツリーでポートの有効と無効が切り替わると、ネットワークの収束期間を短縮するために、すべてのアクティブな非ルーターポートに一般クエリーが送信されます。 トポロジーの変化を無視するように IGMP スヌーピングを設定する場合に、本コマンドを実行してください。
制限・注意	-

ip igmp snooping ignore-topology-change-notification	
バージョン	1.08.02

使用例：VLAN 1 で、スパニングツリープロトコルのトポロジーの変化を無視する機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping ignore-topology-change-notification
(config-vlan)#
```

5.10.22 show ip igmp snooping

show ip igmp snooping	
目的	IGMP スヌーピングの設定を表示します。
Command	show ip igmp snooping [vlan VLAN-ID [,|-]]
Parameter	vlan VLAN-ID（省略可能）：IGMP スヌーピングの設定を表示する VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	VLAN を指定しない場合、IGMP スヌーピングが有効なすべての VLAN の IGMP スヌーピングの設定を表示します。
制限・注意	• Unregistered-filter interfaces 項目は AEOS-NP2500 Ver. 1.12.01 以降で表示されます。それより前のバージョンでは表示されません。
バージョン	1.08.02 1.12.01：Unregistered-filter interfaces 項目を追加

使用例：IGMP スヌーピングの設定を表示する方法を示します。

```
# show ip igmp snooping

IGMP snooping global state        : Disabled ...(1)
Dynamic mrouter aging time        : 300 seconds ...(2)
Unknown data limit                : 128 ...(3)
Unregistered-filter interfaces    : 1/0/1-1/0/5 ...(4)
                                    1/0/7-1/0/8
                                    port-channel5

VLAN #10 configuration ...(5)
    IGMP snooping state               : Enabled ...(6)
    Minimum version                   : v1 ...(7)
    Fast leave                        : Enabled (host-based) ...(8)
    Report suppression                : Disabled ...(9)
    Suppression time                  : 10 seconds ...(10)
    Querier state                     : Enabled (Non-active) ...(11)
    Query version                     : v3 ...(12)
    Query interval                    : 125 seconds ...(13)
    Max response time                 : 10 seconds ...(14)
    Robustness value                  : 2 ...(15)
    Last member query interval        : 1 seconds ...(16)
    Proxy reporting                   : Disabled (Source 0.0.0.0) ...(17)
    Unknown data learning             : Enabled ...(18)
    Unknown data expiry time          : Infinity ...(19)
    Ignore topology change            : Disabled ...(20)

Total Entries: 1
```

項番	説明
(1)	IGMP スヌーピング機能のグローバル設定の有効(Enabled)／無効(Disabled)を表示します。
(2)	学習したマルチキャストルーターポートのエージングタイムの設定値を表示します。
(3)	IGMP スヌーピングで学習する宛先が未知の IPv4 マルチキャストの上限数を表示します。
(4)	IGMP スヌーピングの unregistered-filter を設定したポート番号またはポートチャネル番号を表示します。
(5)	VLAN ID を表示します。
(6)	VLAN ごとの IGMP スヌーピング機能の有効(Enabled)／無効(Disabled)を表示します。
(7)	レシーバーからの参加要求(Membership Report)を許可する IGMP の最小バージョンを表示します。 v1：最小バージョンの制限なし (デフォルト設定) v2：IGMPv1 ホストの参加を制限し、IGMPv2/v3 ホストのみ許可 v3：IGMPv1/v2 ホストの参加を制限し、IGMPv3 ホストのみ許可
(8)	IGMP スヌーピングの高速離脱機能の有効(Enabled)／無効(Disabled)を表示します。group-list オプションを指定して有効にした場合は、対象の IP アクセスリスト名も表示されます。
(9)	IGMP スヌーピングのレポート抑制機能の有効(Enabled)／無効(Disabled)を表示します。
(10)	重複した IGMP レポート、または脱退メッセージを抑制する期間を表示します。
(11)	IGMP スヌーピングのクエリアの有効／無効を表示します。 Enabled (Active)：IGMP スヌーピングのクエリアが有効で、アクティブ状態 Enabled (Non-active)：IGMP スヌーピングのクエリアが有効で、非アクティブ状態 Disabled：IGMP スヌーピングのクエリアが無効
(12)	IGMP スヌーピングのクエリアで使用する IGMP のバージョンを表示します。
(13)	IGMP スヌーピングのクエリアが定期的に送信する Membership Query の送信間隔を表示します。
(14)	IGMP スヌーピングのクエリアが送信する Membership Query で通知される最大応答時間を表示します。
(15)	IGMP スヌーピングのロバストネス変数を表示します。
(16)	IGMP スヌーピングのクエリアの、Group-Specific Query または Group-and-Source-Specific Query の送信間隔を表示します。
(17)	IGMP スヌーピングのプロキシレポーティング機能の有効(Enabled)／無効(Disabled)を表示します。source オプションを指定して有効にした場合は、指定した送信元 IPv4 アドレスも表示されます。
(18)	レシーバーが存在しない IPv4 マルチキャストを受信した場合に、宛先が未知の IPv4 マルチキャストとして学習する機能の有効(Enabled)／無効(Disabled)を表示します。
(19)	IGMP スヌーピングで学習した宛先が未知の IPv4 マルチキャストの有効期限を表示します。デフォルト設定 (有効期限なし) の場合は Infinity と表示されます。
(20)	スパニングツリープロトコルに起因するクエリー送信禁止の有効(Enabled)／無効(Disabled)を表示します。

5.10.23 show ip igmp snooping mrouter

show ip igmp snooping mrouter	
目的	IGMP スヌーピングのマルチキャストルーターポート情報を表示します。
Command	show ip igmp snooping mrouter [vlan VLAN-ID [,|-]]
Parameter	vlan VLAN-ID（省略可能）：IGMP スヌーピングのマルチキャストルーターポート情報を表示する VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	VLAN を指定しない場合、IGMP スヌーピングが有効なすべての VLAN のマルチキャストルーターポート情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：IGMP スヌーピングのマルチキャストルーターポート情報を表示する方法を示します。

```
# show ip igmp snooping mrouter
(1)     (2)
VLAN    Ports
-----   ----------------------------
10      1/0/8,port-channel5 (static)
        1/0/1-1/0/2 (forbidden)
        1/0/12 (dynamic)

Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	ポート番号またはポートチャネル番号を表示します。 (dynamic)：学習したマルチキャストルーターポート (static)：スタティックに設定したマルチキャストルーターポート (forbidden)：マルチキャストルーターポートになることを禁止したポート

5.10.24 show ip igmp snooping groups

show ip igmp snooping groups	
目的	IGMP スヌーピングエントリーを表示します。
Command	show ip igmp snooping groups [GROUP-ADDRESS | vlan VLAN-ID [,|-]]
Parameter	GROUP-ADDRESS（省略可能）：表示する IGMP スヌーピングエントリーの、IPv4 マルチキャストグループアドレスを指定します。 vlan VLAN-ID（省略可能）：表示する IGMP スヌーピングエントリーの VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	IPv4 マルチキャストグループアドレスまたは VLAN を指定しない場合、すべての IGMP スヌーピングエントリーが表示されます。
制限・注意	-

show ip igmp snooping groups	
バージョン	1.08.02

使用例：IGMP スヌーピングエントリーを表示する方法を示します。

```
# show ip igmp snooping groups

IGMP Snooping Connected Group Membership:
(1)       (2)              (3)              (4)  (5)        (6)
VLAN ID  Group address    Source address   FM  Exp(sec)  Interface
-------  ---------------  ---------------  --  --------  ---------
10       233.252.0.1             *         EX  226       1/0/4

Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	IPv4 マルチキャストグループアドレスを表示します。
(3)	送信元 IPv4 アドレスを表示します。 ApresiaNP2500 シリーズの IGMP スヌーピングは MAC アドレスベースで処理されるため、送信元フィルタリングは動作しません。
(4)	フィルターモード（IN：INCLUDE モード／EX：EXCLUDE モード）を表示します。
(5)	IGMP スヌーピングエントリーが削除されるまでの残り時間(秒)を表示します。
(6)	ポート番号またはポートチャネル番号を表示します。

5.10.25 show ip igmp snooping static-group

show ip igmp snooping static-group	
目的	スタティック IGMP スヌーピングエントリーを表示します。
Command	show ip igmp snooping static-group [GROUP-ADDRESS | vlan VLAN-ID [,|-]]
Parameter	GROUP-ADDRESS（省略可能）：表示するスタティック IGMP スヌーピングエントリーの、IPv4 マルチキャストグループアドレスを指定します。 vlan VLAN-ID（省略可能）：表示するスタティック IGMP スヌーピングエントリーの VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	IPv4 マルチキャストグループアドレスまたは VLAN を指定しない場合、すべてのスタティック IGMP スヌーピングエントリーが表示されます。
制限・注意	-
バージョン	1.08.02

使用例：スタティック IGMP スヌーピングエントリーを表示する方法を示します。

```
# show ip igmp snooping static-group
(1)       (2)              (3)
VLAN ID  Group address    Interface
-------  ---------------  ------------------------
10       233.252.0.100    1/0/4,port-channel2
```

```
Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	IPv4 マルチキャストグループアドレスを表示します。
(3)	ポート番号またはポートチャネル番号を表示します。

5.10.26 show ip igmp snooping statistics

show ip igmp snooping statistics	
目的	IGMP スヌーピングの統計情報を表示します。
Command	**show ip igmp snooping statistics** {**interface** [IF-ID [,|-]] | **vlan** [VLAN-ID [,|-]]}
Parameter	interface：インターフェースの IGMP スヌーピングの統計情報を表示する場合に指定します。 IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定 vlan：VLAN の IGMP スヌーピングの統計情報を表示する場合に指定します。 VLAN-ID（省略可能）：IGMP スヌーピングの統計情報を表示する VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	interface パラメーターを指定して特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。 vlan パラメーターを指定して特定の VLAN を指定しない場合は、IGMP スヌーピングが有効なすべての VLAN の情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/2 の IGMP スヌーピングの統計情報を表示する方法を示します。

```
# show ip igmp snooping statistics interface port 1/0/2

Interface Port1/0/2 ...(1)
  IGMPv1 Rx: Report 0, Query 0 ...(2)
  IGMPv2 Rx: Report 0, Query 0, Leave 0 ...(3)
  IGMPv3 Rx: Report 0, Query 0 ...(4)
  IGMPv1 Tx: Report 0, Query 0 ...(5)
  IGMPv2 Tx: Report 0, Query 0, Leave 0 ...(6)
  IGMPv3 Tx: Report 0, Query 5 ...(7)

Total Entries: 1
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。

項番	説明
(2)	対象インターフェースで受信した IGMPv1 の Report, Query の数を表示します。
(3)	対象インターフェースで受信した IGMPv2 の Report, Query, Leave の数を表示します。
(4)	対象インターフェースで受信した IGMPv3 の Report, Query の数を表示します。
(5)	対象インターフェースから送信した IGMPv1 の Report, Query の数を表示します。
(6)	対象インターフェースから送信した IGMPv2 の Report, Query, Leave の数を表示します。
(7)	対象インターフェースから送信した IGMPv3 の Report, Query の数を表示します。

5.10.27 clear ip igmp snooping groups

clear ip igmp snooping groups	
目的	動的に学習した IGMP スヌーピングエントリーを削除します。
Command	clear ip igmp snooping groups {all | GROUP-ADDRESS [vlan VLAN-ID]}
Parameter	all：すべての動的に学習した IGMP スヌーピングエントリーを削除する場合に指定します。 GROUP-ADDRESS［vlan VLAN-ID］：削除する IGMP スヌーピングエントリーの IPv4 マルチキャストグループアドレスと VLAN（省略可能）を指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドの削除対象には、宛先が未知の IPv4 マルチキャストとして学習した IGMP スヌーピングエントリーも含まれます。
制限・注意	-
バージョン	1.08.02

使用例：すべての動的に学習した IGMP スヌーピングエントリーを削除する方法を示します。

```
# clear ip igmp snooping groups all
#
```

5.10.28 clear ip igmp snooping unknown-data

clear ip igmp snooping unknown-data	
目的	宛先が未知の IPv4 マルチキャストとして学習した IGMP スヌーピングエントリーを削除します。
Command	clear ip igmp snooping unknown-data {all | vlan VLAN-ID | group GROUP-ADDRESS}
Parameter	all：すべての宛先が未知の IGMP スヌーピングエントリーを削除する場合に指定します。 vlan VLAN-ID：指定した VLAN の、宛先が未知の IGMP スヌーピングエントリーを削除する場合に指定します。 group GROUP-ADDRESS：指定した IPv4 マルチキャストグループアドレスの、宛先が未知の IGMP スヌーピングエントリーを削除する場合に指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-

clear ip igmp snooping unknown-data	
制限・注意	-
バージョン	1.08.02

使用例：宛先が未知の IPv4 マルチキャストとして学習した IGMP スヌーピングエントリーを、すべて削除する方法を示します。

```
# clear ip igmp snooping unknown-data all
#
```

5.10.29 clear ip igmp snooping statistics

clear ip igmp snooping statistics	
目的	IGMP スヌーピングの統計情報を消去します。
Command	clear ip igmp snooping statistics {all | vlan VLAN-ID | interface IF-ID}
Parameter	all：すべての IGMP スヌーピングの統計情報を消去する場合に指定します。 vlan VLAN-ID：IGMP スヌーピングの統計情報を消去する VLAN を指定します。 interface IF-ID：IGMP スヌーピングの統計情報を消去するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべての IGMP スヌーピングの統計情報を消去する方法を示します。

```
# clear ip igmp snooping statistics all
#
```

5.11 MLD スヌーピングコマンド

MLD スヌーピング関連の設定コマンドは以下のとおりです。

- ipv6 mld snooping
- ipv6 mld snooping（VLAN）
- ipv6 mld snooping unregistered-filter
- ipv6 mld snooping mrouter
- ipv6 mld snooping minimum-version
- ipv6 mld snooping fast-leave
- ipv6 mld snooping querier
- ipv6 mld snooping query-version
- ipv6 mld snooping query-interval
- ipv6 mld snooping query-max-response-time
- ipv6 mld snooping robustness-variable
- ipv6 mld snooping last-listener-query-interval
- ipv6 mld snooping static-group
- ipv6 mld snooping report-suppression
- ipv6 mld snooping suppression-time
- ipv6 mld snooping proxy-reporting
- ipv6 mld snooping unknown-data learn
- ipv6 mld snooping unknown-data expiry-time
- ipv6 mld snooping unknown-data limit
- ipv6 mld snooping ignore-topology-change-notification

MLD スヌーピング関連の show／操作コマンドは以下のとおりです。

- show ipv6 mld snooping
- show ipv6 mld snooping mrouter
- show ipv6 mld snooping groups
- show ipv6 mld snooping static-group
- show ipv6 mld snooping statistics
- clear ipv6 mld snooping groups
- clear ipv6 mld snooping unknown-data
- clear ipv6 mld snooping statistics

5.11.1 ipv6 mld snooping

ipv6 mld snooping	
目的	グローバル設定モードで、装置全体の MLD スヌーピング機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping no ipv6 mld snooping
Parameter	なし
デフォルト	装置全体の MLD スヌーピング機能は無効
モード	グローバル設定モード
特権レベル	レベル：12

ipv6 mld snooping	
ガイドライン	MLD スヌーピング機能を使用する場合は、グローバル設定モードの ipv6 mld snooping コマンドで装置全体の MLD スヌーピング機能を有効にして、VLAN 設定モードの ipv6 mld snooping コマンドで対象 VLAN を有効にしてください。
制限・注意	• ApresiaNP2500 シリーズの MLD スヌーピングは、MAC アドレスベースで処理されます。そのため、同一 MAC アドレスのマルチキャストグループの中継動作は同じになることに注意してください。 • 例えば、同一 MAC アドレス(33:33:00:01:00:01)の ff05::db8:1:1 と ff08::db8:1:1 のマルチキャストグループをマルチキャストルーターポートで受信しているとします。その状況で、あるポートで ff08::db8:1:1 への参加メッセージを受信して参加すると、show ipv6 mld snooping groups や show ipv6 mroute forwarding-cache では ff08::db8:1:1 だけをそのポートに中継しているように見えますが、実際には ff05::db8:1:1 もそのポートに中継されます。 • 同様に、あるポートが ff05::db8:1:1 と ff08::db8:1:1 の両方に参加している状況で、そのポートで ff08::db8:1:1 からの離脱メッセージを受信すると、show ipv6 mld snooping groups や show ipv6 mroute forwarding-cache では ff08::db8:1:1 は離脱したように見えますが、実際には同一 MAC アドレスの ff05::db8:1:1 が参加状態のため、ff05::db8:1:1 だけでなく ff08::db8:1:1 もまだそのポートに中継されます。 • また、MAC アドレスベースで処理されるため、MLDv2 の送信元指定の参加要求を受信して登録されても、送信元フィルタリングは動作しないことに注意してください。show ipv6 mld snooping groups や show ipv6 mroute forwarding-cache では指定した送信元の情報を含んで表示されますが、送信元が一致しないマルチキャストグループも中継されます。
バージョン	1.08.02

使用例：グローバル設定モードで MLD スヌーピング機能を有効にする方法を示します。

```
# configure terminal
(config)# ipv6 mld snooping
(config)#
```

5.11.2 ipv6 mld snooping (VLAN)

ipv6 mld snooping (VLAN)	
目的	VLAN 設定モードで、対象 VLAN の MLD スヌーピング機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping no ipv6 mld snooping
Parameter	なし
デフォルト	すべての VLAN の MLD スヌーピング機能は無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	MLD スヌーピング機能を使用する場合は、グローバル設定モードの ipv6 mld snooping コマンドで装置全体の MLD スヌーピング機能を有効にして、VLAN 設定モードの ipv6 mld snooping コマンドで対象 VLAN を有効にしてください。
制限・注意	-

ipv6 mld snooping（VLAN）	
バージョン	1.08.02

使用例：VLAN 1 の MLD スヌーピング機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping
(config-vlan)#
```

5.11.3 ipv6 mld snooping unregistered-filter

ipv6 mld snooping unregistered-filter	
目的	MLD スヌーピングとして未登録のマルチキャストパケットを、送信せずに破棄（unregistered-filter）するインターフェースを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping unregistered-filter interface IF-ID [,|-] no ipv6 mld snooping unregistered-filter interface IF-ID [,|-]
Parameter	interface IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	設定なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドのフィルター対象になる「MLD スヌーピングとして未登録のマルチキャストパケット」とは、以下のいずれにも登録されていないエントリーが対象になります。 • MLD スヌーピングテーブルに登録されていないエントリー宛てのマルチキャストパケット（MLD スヌーピングエントリーは show ipv6 mld snooping groups コマンドで確認可能） • IPv6 マルチキャスト転送キャッシュに登録されていないエントリー宛てのマルチキャストパケット（IPv6 マルチキャスト転送キャッシュは show ipv6 mroute forwarding-cache コマンドで確認可能） 以下のマルチキャストパケットは、本コマンドのフィルター対象外です。 • MLD スヌーピングテーブルに登録されているマルチキャスト • MLD スヌーピングテーブルには登録されていないが、IPv6 マルチキャスト転送キャッシュには登録されているマルチキャスト • 予約 IPv6 マルチキャスト（ff02::/111, ff02::1:ff00:0/104, ff05::/111） • mac-address-table static コマンドでスタティックに設定したマルチキャスト MAC アドレスエントリー宛てのマルチキャスト 本コマンドの unregistered-filter はマルチキャストルーターポートに設定した場合にも動作するため、マルチキャストルーターポートでは設定しないことを推奨します。
制限・注意	• 本コマンドを使用する場合、対象 VLAN のマルチキャストフィルタリングモードはデフォルト設定（multicast filtering-mode forward-unregistered）のまま使用してください。 • 同一ポート／同一ポートチャネルで「宛先不明マルチキャストフレームを対象にした Egress フィルタリング（egress-filtering umc）」の併用は未サポートです。

ipv6 mld snooping unregistered-filter	
	• 本コマンドで設定する unregistered-filter は、ポート／ポートチャネルごとの設定なことに注意してください。VLAN ごとにマルチキャストルーターポートが異なるような場合は、すべての VLAN でマルチキャストルーターポートが同一になるような設計に見直してから使用してください。 • 本機能はアクセスリスト機能と同じハードウェアリソース（Ingress グループ）を使用します。本機能で使用中の Ingress グループは、他の機能では使用できません。グループの利用状況は show access-list resource reserved-group コマンドで確認できます。
バージョン	1.12.01

使用例：ポート 1/0/1～1/0/8 を指定して、MLD スヌーピングの unregistered-filter を設定する方法を示します。

```
# configure terminal
(config)# ipv6 mld snooping unregistered-filter interface port 1/0/1-8
(config)#
```

5.11.4 ipv6 mld snooping mrouter

ipv6 mld snooping mrouter	
目的	マルチキャストルーターポートをスタティックに設定します。また、マルチキャストルーターポートになることを禁止するインターフェースを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping mrouter {[forbidden] interface IF-ID [,|-] | learn pimv6} no ipv6 mld snooping mrouter {[forbidden] interface IF-ID [,|-] | learn pimv6}
Parameter	forbidden（省略可能）：マルチキャストルーターポートになることを禁止するインターフェースを設定する場合に指定します。 interface IF-ID：マルチキャストルーターポートとして設定するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定 learn pimv6：マルチキャストルーターポートの動的な学習を有効にする場合に指定します。
デフォルト	マルチキャストルーターポート：設定なし 動的な学習：有効（ipv6 mld snooping mrouter learn pimv6）
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	MLD スヌーピングを有効にすると、クエリアが送信する Multicast Listener Query の受信ポートや、IPv6 PIM 制御パケットの受信ポートを、マルチキャストルーターポートとして動的に学習します。本コマンドでは、マルチキャストルーターポートをスタティックに設定できます。 マルチキャストルーターポートとしてポートチャネルを指定する場合は、interface port-channel パラメーターで指定してください。ポートチャネルのメンバーポートを指定して設定しないでください。 forbidden パラメーターを指定して設定すると、対象のインターフェースが動的に学

ipv6 mld snooping mrouter	
	習してマルチキャストルーターポートになることを禁止できます。
制限・注意	• 設定する VLAN に所属していないポートまたはポートチャネルを指定して設定した場合は、警告メッセージが表示されます。
バージョン	1.08.02

使用例：VLAN 1 のポート 1/0/1 をマルチキャストルーターポートとしてスタティックに設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping mrouter interface port 1/0/1
(config-vlan)#
```

使用例：VLAN 4 で、マルチキャストルーターポートの動的な学習を無効にする方法を示します。

```
# configure terminal
(config)# vlan 4
(config-vlan)# no ipv6 mld snooping mrouter learn pimv6
(config-vlan)#
```

5.11.5 ipv6 mld snooping minimum-version

ipv6 mld snooping minimum-version	
目的	リスナーからの参加要求(Multicast Listener Report)を許可する MLD の最小バージョンを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping minimum-version 2 no ipv6 mld snooping minimum-version
Parameter	なし
デフォルト	最小バージョンの設定なし
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	本コマンドは Multicast Listener Report にのみ適用されます。拒否された Multicast Listener Report はマルチキャストルーターポートに中継されません。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、参加要求を許可する MLD の最小バージョンを 2 に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping minimum-version 2
(config-vlan)#
```

5.11.6 ipv6 mld snooping fast-leave

ipv6 mld snooping fast-leave	
目的	MLD スヌーピングの高速離脱機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping fast-leave [group-list ACL-NAME] no ipv6 mld snooping fast-leave

ipv6 mld snooping fast-leave	
Parameter	group-list ACL-NAME（省略可能）：MLD スヌーピングの高速離脱の対象にするマルチキャストグループを定義した、IPv6 アクセスリストを指定します。指定しない場合、すべてのマルチキャストグループが高速離脱の対象になります。
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	MLD スヌーピングの高速離脱の対象にするマルチキャストグループを指定する場合は、IPv6 アクセスリストで対象となるマルチキャストグループを permit ルールの「宛先 IPv6 アドレス」条件で指定します。「送信元 IPv6 アドレス」条件はサポートしていないため any で設定してください。また、deny ルールはサポートしていません。 MLD スヌーピングの高速離脱機能が有効な場合は、自装置が代表クエリア／非代表クエリアのいずれの場合でも、リスナーからの離脱要求を受信すると、即座に対象の MLD スヌーピングエントリーを削除します。 MLD スヌーピングの高速離脱機能が無効な場合は、リスナーが離脱要求を送信すると、MLD スヌーピングエントリーのタイマー（削除されるまでの時間）は以下のように更新されます。そして、いずれのリスナーからも応答がない場合はタイマーが満了して削除されます。 • 「ロバストネス変数×ipv6 mld snooping last-listener-query-interval コマンドで設定した送信間隔」が現状のタイマー値よりも小さい場合は、その値に更新されます。
制限・注意	• 説明に記載されている種別以外のアクセスリストを指定して使用できません。 • 本設定の group-list パラメーターで指定する IPv6 アクセスリストでは、装置のハードウェアリソースを使用しません。
バージョン	1.08.02

使用例：VLAN 1 で、MLD スヌーピングの高速離脱機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping fast-leave
(config-vlan)#
```

5.11.7 ipv6 mld snooping querier

ipv6 mld snooping querier	
目的	MLD スヌーピングのクエリアを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping querier no ipv6 mld snooping querier
Parameter	なし
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	同一サブネットに所属するクエリアが複数存在する場合は、IPv6 アドレスの小さいクエリアが代表クエリアになります。

ipv6 mld snooping querier	
	本装置が代表クエリア／非代表クエリアのいずれの場合でも、MLD スヌーピングエントリーが登録／更新された際のタイマー（削除されるまでの時間）は、自装置のパラメーター（ipv6 mld snooping query-interval コマンド、ipv6 mld snooping robustness-variable コマンド）で決定されます。
制限・注意	• MLD スヌーピングのクエリアを有効にするには、対象 VLAN の VLAN インターフェースを作成し、IPv6 アドレスが設定されている必要があります。
バージョン	1.08.02

使用例：VLAN 1 で、MLD スヌーピングのクエリアを有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping querier
(config-vlan)#
```

5.11.8 ipv6 mld snooping query-version

ipv6 mld snooping query-version	
目的	MLD スヌーピングのクエリアのバージョンを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 mld snooping query-version {1 | 2} no ipv6 mld snooping query-version
Parameter	{1 | 2}：MLD スヌーピングのクエリアのバージョンを指定します。
デフォルト	MLD バージョン 2
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	本コマンドで設定する MLD バージョン設定は、MLD のクエリアが送信する Multicast Listener Query に反映されます。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、MLD スヌーピングのクエリアのバージョンを 1 に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping query-version 1
(config-vlan)#
```

5.11.9 ipv6 mld snooping query-interval

ipv6 mld snooping query-interval	
目的	MLD スヌーピングのクエリアが定期的に送信する Multicast Listener Query の送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 mld snooping query-interval SECONDS no ipv6 mld snooping query-interval
Parameter	SECONDS：定期的に送信する Multicast Listener Query の送信間隔を、1～31,744 秒の範囲で指定します。
デフォルト	125 秒

ipv6 mld snooping query-interval	
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• Multicast Listener Query の送信間隔は、Multicast Listener Query の最大応答時間よりも大きい値になるように設定する必要があります。
バージョン	1.08.02

使用例：VLAN 1 で、MLD スヌーピングのクエリアが定期的に送信する Multicast Listener Query の送信間隔を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping query-interval 300
(config-vlan)#
```

5.11.10 ipv6 mld snooping query-max-response-time

ipv6 mld snooping query-max-response-time	
目的	MLD スヌーピングのクエリアが送信する Multicast Listener Query で通知される最大応答時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 mld snooping query-max-response-time SECONDS no ipv6 mld snooping query-max-response-time
Parameter	SECONDS：Multicast Listener Query の最大応答時間を 1～25 秒の範囲で指定します。
デフォルト	10 秒
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• Multicast Listener Query の最大応答時間は、Multicast Listener Query の送信間隔よりも小さい値になるように設定する必要があります。
バージョン	1.08.02

使用例：VLAN 1 で、Multicast Listener Query の最大応答時間を 20 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping query-max-response-time 20
(config-vlan)#
```

5.11.11 ipv6 mld snooping robustness-variable

ipv6 mld snooping robustness-variable	
目的	MLD スヌーピングのロバストネス変数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 mld snooping robustness-variable VALUE no ipv6 mld snooping robustness-variable

ipv6 mld snooping robustness-variable	
Parameter	VALUE：ロバストネス変数を 1～7 の範囲で指定します。
デフォルト	2
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	ロバストネス変数を大きく設定することで、MLD スヌーピングエントリーが削除されるまでの残り時間などを増やすことができます。これにより、輻輳などで MLD メッセージがパケットロスすることへの影響を緩和できます。 Multicast Address Listening Interval（MLD スヌーピングエントリーのリスナーが存在しないと判断するまでの時間）は、以下の計算式で算出されます。 • (ロバストネス変数×クエリー送信間隔) + (最大応答時間) Other Querier Present Timeout（自装置が非代表クエリアの場合に、代表クエリアが存在しないと判断するまでの時間）は、以下の計算式で算出されます。 • (ロバストネス変数×クエリー送信間隔) + (0.5×最大応答時間) MLD スヌーピングのクエリアが有効設定の場合に、装置を起動した直後などは、通常よりも短い間隔で Multicast Listener Query を送信します。その送信間隔は通常のクエリー送信間隔の 1/4 で、ロバストネス変数の回数送信されます。 MLD スヌーピングのクエリアが有効で自装置が代表クエリアの場合に、登録済みのエントリーに対して離脱要求を受信すると、Multicast Address Specific Query または Multicast Address and Source Specific Query を送信します。その送信間隔は ipv6 mld snooping last-listener-query-interval コマンドで設定した送信間隔で、ロバストネス変数の回数送信されます。
制限・注意	• ロバストネス変数を 1 で使用することは規格で推奨されていないため、ロバストネス変数は 2 以上で使用してください。
バージョン	1.08.02

使用例：VLAN 1 で、MLD スヌーピングのロバストネス変数を 3 に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping robustness-variable 3
(config-vlan)#
```

5.11.12 ipv6 mld snooping last-listener-query-interval

ipv6 mld snooping last-listener-query-interval	
目的	MLD スヌーピングのクエリアの、Multicast Address Specific Query または Multicast Address and Source Specific Query の送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 mld snooping last-listener-query-interval SECONDS no ipv6 mld snooping last-listener-query-interval
Parameter	SECONDS：Multicast Address Specific Query または Multicast Address and Source Specific Query の送信間隔を、1～25 秒の範囲で指定します。
デフォルト	1 秒
モード	VLAN 設定モード
特権レベル	レベル：12

ipv6 mld snooping last-listener-query-interval	
ガイドライン	MLD スヌーピングのクエリアが有効で自装置が代表クエリアの場合に、登録済みの MLD スヌーピングエントリーに対して離脱要求を受信すると、Multicast Address Specific Query または Multicast Address and Source Specific Query を送信します。その送信間隔は本コマンドで設定した送信間隔で、ロバストネス変数の回数送信されます。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、Multicast Address Specific Query または Multicast Address and Source Specific Query の送信間隔を、3 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping last-listener-query-interval 3
(config-vlan)#
```

5.11.13 ipv6 mld snooping static-group

ipv6 mld snooping static-group	
目的	スタティック MLD スヌーピングエントリーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping static-group GROUP-ADDRESS interface IF-ID [,|-] no ipv6 mld snooping static-group GROUP-ADDRESS [interface IF-ID [,|-]]
Parameter	GROUP-ADDRESS：IPv6 マルチキャストグループアドレスを指定します。 interface IF-ID：スタティック MLD スヌーピングエントリーに登録するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	スタティック MLD スヌーピングエントリーの設定なし
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1、IPv6 マルチキャストグループアドレス ff05::db8:1:1、登録ポート 1/0/5 で、スタティック MLD スヌーピングエントリーを設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping static-group ff05::db8:1:1 interface port 1/0/5
(config-vlan)#
```

5.11.14 ipv6 mld snooping report-suppression

ipv6 mld snooping report-suppression	
目的	MLD スヌーピングのレポート抑制機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。

ipv6 mld snooping report-suppression	
Command	ipv6 mld snooping report-suppression no ipv6 mld snooping report-suppression
Parameter	なし
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	レポート抑制機能は、MLDv1 トラフィックだけに動作します。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 100 で、MLD スヌーピングのレポート抑制機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 100
(config-vlan)# ipv6 mld snooping report-suppression
(config-vlan)#
```

5.11.15 ipv6 mld snooping suppression-time

ipv6 mld snooping suppression-time	
目的	重複した MLD レポート、または脱退メッセージを抑制する期間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 mld snooping suppression-time SECONDS no ipv6 mld snooping suppression-time
Parameter	SECONDS：重複した MLD レポートを抑制する期間を 1～300 秒の範囲で指定します。
デフォルト	10 秒
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	抑制期間を短くすると、重複する MLD パケットの送信間隔が短くなります。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1000 で、抑制期間を 125 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ipv6 mld snooping suppression-time 125
(config-vlan)#
```

5.11.16 ipv6 mld snooping proxy-reporting

ipv6 mld snooping proxy-reporting	
目的	MLD スヌーピングのプロキシレポーティング機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping proxy-reporting [source IPV6-ADDRESS]

ipv6 mld snooping proxy-reporting	
	no ipv6 mld snooping proxy-reporting
Parameter	source IPV6-ADDRESS（省略可能）：プロキシレポーティングの送信元 IPv6 アドレスを指定します。
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	source IPV6-ADDRESS で IPv6 アドレスを指定しない場合はゼロアドレスが使用されます。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、MLD スヌーピングのプロキシレポーティング機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping proxy-reporting
(config-vlan)#
```

5.11.17 ipv6 mld snooping unknown-data learn

ipv6 mld snooping unknown-data learn	
目的	リスナーが存在しない IPv6 マルチキャストを受信した場合に、宛先が未知の IPv6 マルチキャストとして学習する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping unknown-data learn no ipv6 mld snooping unknown-data learn
Parameter	なし
デフォルト	有効（ipv6 mld snooping unknown-data learn）
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	本設定が有効（デフォルト設定）の場合は、リスナーからの参加要求を受信していない状態で IPv6 マルチキャストを受信すると、宛先が未知の IPv6 マルチキャストとして IPv6 マルチキャスト転送キャッシュと MLD スヌーピングテーブルに登録されます。 登録された宛先が未知の IPv6 マルチキャストは、マルチキャストルーターポートにのみ転送され、それ以外のポートには転送されません。 本設定を無効にすると、宛先が未知の IPv6 マルチキャストを登録しないように変更できます。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、リスナーが存在しない IPv6 マルチキャストを受信した場合に、宛先が未知の IPv6 マルチキャストとして学習する機能を無効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# no ipv6 mld snooping unknown-data learn
```

```
(config-vlan)#
```

5.11.18 ipv6 mld snooping unknown-data expiry-time

ipv6 mld snooping unknown-data expiry-time	
目的	MLD スヌーピングで学習した宛先が未知の IPv6 マルチキャストの有効期限を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 mld snooping unknown-data expiry-time SECONDS no ipv6 mld snooping unknown-data expiry-time
Parameter	SECONDS：有効期限を 1～65,535 秒の範囲で指定します。
デフォルト	有効期限なし（no ipv6 mld snooping unknown-data expiry-time）
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、MLD スヌーピングで学習した宛先が未知の IPv6 マルチキャストの有効期限を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping unknown-data expiry-time 300
(config-vlan)#
```

5.11.19 ipv6 mld snooping unknown-data limit

ipv6 mld snooping unknown-data limit	
目的	MLD スヌーピングで学習する宛先が未知の IPv6 マルチキャストの上限数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 mld snooping unknown-data limit VALUE no ipv6 mld snooping unknown-data limit
Parameter	VALUE：上限数を 1～128 の範囲で指定します。
デフォルト	128
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MLD スヌーピングで学習する宛先が未知の IPv6 マルチキャストの上限数を、100 に設定する方法を示します。

```
# configure terminal
(config)# ipv6 mld snooping unknown-data limit 100
(config)#
```

5.11.20 ipv6 mld snooping ignore-topology-change-notification

ipv6 mld snooping ignore-topology-change-notification	
目的	スパニングツリープロトコルのトポロジーの変化を無視し、誘発されるクエリーを送信しない機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ipv6 mld snooping ignore-topology-change-notification no ipv6 mld snooping ignore-topology-change-notification
Parameter	なし
デフォルト	無効
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	MLD スヌーピングを有効にした装置では、スパニングツリー動作によって生じたリンクレイヤートポロジーの変化を認識します。スパニングツリーでポートの有効と無効が切り替わると、ネットワークの収束期間を短縮するために、すべてのアクティブな非ルーターポートに一般クエリーが送信されます。 トポロジーの変化を無視するように MLD スヌーピングを設定する場合に、本コマンドを実行してください。
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1 で、スパニングツリープロトコルのトポロジーの変化を無視する機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping ignore-topology-change-notification
(config-vlan)#
```

5.11.21 show ipv6 mld snooping

show ipv6 mld snooping	
目的	MLD スヌーピングの設定を表示します。
Command	show ipv6 mld snooping [vlan VLAN-ID [,|-]]
Parameter	vlan VLAN-ID（省略可能）：MLD スヌーピングの設定を表示する VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	VLAN を指定しない場合、MLD スヌーピングが有効なすべての VLAN の MLD スヌーピングの設定を表示します。
制限・注意	• Unregistered-filter interfaces 項目は AEOS-NP2500 Ver. 1.12.01 以降で表示されます。それより前のバージョンでは表示されません。
バージョン	1.08.02 1.12.01：Unregistered-filter interfaces 項目を追加

使用例：MLD スヌーピングの設定を表示する方法を示します。

```
# show ipv6 mld snooping
```

```
MLD snooping global state          : Disabled ...(1)
Unknown data limit                 : 128 ...(2)
Unregistered-filter interfaces     : 1/0/1-1/0/5 ...(3)
                                     1/0/7-1/0/8
                                     port-channel5

VLAN #10 configuration ...(4)
    MLD snooping state                 : Enabled ...(5)
    Minimum version                    : v1 ...(6)
    Fast leave                         : Enabled (host-based) ...(7)
    Report suppression                 : Disabled ...(8)
    Suppression time                   : 10 seconds ...(9)
    Proxy reporting                    : Disabled (Source ::) ...(10)
    Mrouter port learning              : Enabled ...(11)
    Querier state                      : Enabled (Non-active) ...(12)
    Query version                      : v2 ...(13)
    Query interval                     : 125 seconds ...(14)
    Max response time                  : 10 seconds ...(15)
    Robustness value                   : 2 ...(16)
    Last listener query interval       : 1 seconds ...(17)
    Unknown data learning              : Enabled ...(18)
    Unknown data expiry time           : Infinity ...(19)
    Ignore topology change             : Disabled ...(20)

Total Entries: 1
```

項番	説明
(1)	MLD スヌーピング機能のグローバル設定の有効(Enabled)／無効(Disabled)を表示します。
(2)	MLD スヌーピングで学習する宛先が未知の IPv6 マルチキャストの上限数を表示します。
(3)	MLD スヌーピングの unregistered-filter を設定したポート番号またはポートチャネル番号を表示します。
(4)	VLAN ID を表示します。
(5)	VLAN ごとの MLD スヌーピング機能の有効(Enabled)／無効(Disabled)を表示します。
(6)	リスナーからの参加要求(Multicast Listener Report)を許可する MLD の最小バージョンを表示します。 v1：最小バージョンの制限なし (デフォルト設定) v2：MLDv1 ホストの参加を制限し、MLDv2 ホストのみ許可
(7)	MLD スヌーピングの高速離脱機能の有効(Enabled)／無効(Disabled)を表示します。group-list オプションを指定して有効にした場合は、対象の IPv6 アクセスリスト名も表示されます。
(8)	MLD スヌーピングのレポート抑制機能の有効(Enabled)／無効(Disabled)を表示します。
(9)	重複した MLD レポート、または脱退メッセージを抑制する期間を表示します。
(10)	MLD スヌーピングのプロキシレポーティング機能の有効(Enabled)／無効(Disabled)を表示します。source オプションを指定して有効にした場合は、指定した送信元 IPv6 アドレスも表示されます。
(11)	マルチキャストルーターポートの自動学習の有効(Enabled)／無効(Disabled)を表示します。
(12)	MLD スヌーピングのクエリアの有効／無効を表示します。 Enabled (Active)：MLD スヌーピングのクエリアが有効で、アクティブ状態 Enabled (Non-active)：MLD スヌーピングのクエリアが有効で、非アクティブ状態

項番	説明
	Disabled：MLD スヌーピングのクエリアが無効
(13)	MLD スヌーピングのクエリアで使用する MLD のバージョンを表示します。
(14)	MLD スヌーピングのクエリアが定期的に送信する Multicast Listener Query の送信間隔を表示します。
(15)	MLD スヌーピングのクエリアが送信する Multicast Listener Query で通知される最大応答時間を表示します。
(16)	MLD スヌーピングのロバストネス変数を表示します。
(17)	MLD スヌーピングのクエリアの、Multicast Address Specific Query または Multicast Address and Source Specific Query の送信間隔を表示します。
(18)	リスナーが存在しない IPv6 マルチキャストを受信した場合に、宛先が未知の IPv6 マルチキャストとして学習する機能の有効(Enabled)／無効(Disabled)を表示します。
(19)	MLD スヌーピングで学習した宛先が未知の IPv6 マルチキャストの有効期限を表示します。デフォルト設定（有効期限なし）の場合は Infinity と表示されます。
(20)	スパニングツリープロトコルに起因するクエリー送信禁止の有効(Enabled)／無効(Disabled)を表示します。

5.11.22 show ipv6 mld snooping mrouter

show ipv6 mld snooping mrouter	
目的	MLD スヌーピングのマルチキャストルーターポート情報を表示します。
Command	show ipv6 mld snooping mrouter [vlan VLAN-ID [,|-]]
Parameter	vlan VLAN-ID（省略可能）：MLD スヌーピングのマルチキャストルーターポート情報を表示する VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	VLAN を指定しない場合、MLD スヌーピングが有効なすべての VLAN のマルチキャストルーターポート情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：MLD スヌーピングのマルチキャストルーターポート情報を表示する方法を示します。

```
# show ipv6 mld snooping mrouter
(1)     (2)
VLAN    Ports
-----   -----------------------------
10      1/0/8,port-channel5 (static)
        1/0/1-1/0/2 (forbidden)
        1/0/12 (dynamic)

Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	ポート番号またはポートチャネル番号を表示します。 （dynamic）：学習したマルチキャストルーターポート

項番	説明
	(static)：スタティックに設定したマルチキャストルーターポート (forbidden)：マルチキャストルーターポートになることを禁止したポート

5.11.23 show ipv6 mld snooping groups

show ipv6 mld snooping groups	
目的	MLD スヌーピングエントリーを表示します。
Command	show ipv6 mld snooping groups [GROUP-ADDRESS | vlan VLAN-ID [,|-]]
Parameter	GROUP-ADDRESS（省略可能）：表示する MLD スヌーピングエントリーの、IPv6 マルチキャストグループアドレスを指定します。 vlan VLAN-ID（省略可能）：表示する MLD スヌーピングエントリーの VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	IPv6 マルチキャストグループアドレスまたは VLAN を指定しない場合、すべての MLD スヌーピングエントリーが表示されます。
制限・注意	-
バージョン	1.08.02

使用例：MLD スヌーピングエントリーを表示する方法を示します。

```
# show ipv6 mld snooping groups

MLD Snooping Connected Group Membership:
(1)      (2)                    (3)                    (4) (5)       (6)
VLAN ID Group address          Source address         FM Exp(sec)  Interface
------- ---------------------- ---------------------- -- -------- ---------
10      ff05::db8:0:1                    *            EX 213      1/0/4

Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	IPv6 マルチキャストグループアドレスを表示します。
(3)	送信元 IPv6 アドレスを表示します。 ApresiaNP2500 シリーズの MLD スヌーピングは MAC アドレスベースで処理されるため、送信元フィルタリングは動作しません。
(4)	フィルターモード (IN：INCLUDE モード／EX：EXCLUDE モード) を表示します。
(5)	MLD スヌーピングエントリーが削除されるまでの残り時間(秒)を表示します。
(6)	ポート番号またはポートチャネル番号を表示します。

5.11.24 show ipv6 mld snooping static-group

show ipv6 mld snooping static-group	
目的	スタティック MLD スヌーピングエントリーを表示します。
Command	show ipv6 mld snooping static-group [GROUP-ADDRESS | vlan VLAN-ID

show ipv6 mld snooping static-group	
	[,|-]]
Parameter	GROUP-ADDRESS（省略可能）：表示するスタティック MLD スヌーピングエントリーの、IPv6 マルチキャストグループアドレスを指定します。 vlan VLAN-ID（省略可能）：表示するスタティック MLD スヌーピングエントリーの VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	IPv6 マルチキャストグループアドレスまたは VLAN を指定しない場合、すべてのスタティック MLD スヌーピングエントリーが表示されます。
制限・注意	-
バージョン	1.08.02

使用例：スタティック MLD スヌーピングエントリーを表示する方法を示します。

```
# show ipv6 mld snooping static-group
 (1)       (2)                                        (3)
VLAN ID  Group address                                Interface
-------  ---------------                              ------------------------
10       ff05::db8:0:5555                             1/0/4,port-channel2

Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	IPv6 マルチキャストグループアドレスを表示します。
(3)	ポート番号またはポートチャネル番号を表示します。

5.11.25 show ipv6 mld snooping statistics

show ipv6 mld snooping statistics	
目的	MLD スヌーピングの統計情報を表示します。
Command	show ipv6 mld snooping statistics {interface [IF-ID [,|-]] | vlan [VLAN-ID [,|-]]}
Parameter	interface：インターフェースの MLD スヌーピングの統計情報を表示する場合に指定します。 IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定 vlan：VLAN の MLD スヌーピングの統計情報を表示する場合に指定します。 VLAN-ID（省略可能）：MLD スヌーピングの統計情報を表示する VLAN を指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	interface パラメーターを指定して特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。

show ipv6 mld snooping statistics	
	vlan パラメーターを指定して特定の VLAN を指定しない場合は、MLD スヌーピングが有効なすべての VLAN の情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/2 の MLD スヌーピングの統計情報を表示する方法を示します。

```
# show ipv6 mld snooping statistics interface port 1/0/2

Interface Port1/0/2 ...(1)
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0 ...(2)
  Tx: v1Report 0, v2Report 0, Query 138, v1Done 0 ...(3)

Total Entries: 1
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	対象インターフェースで受信した MLDv1 Report, MLDv2 Report, Query, MLDv1 Done の数を表示します。
(3)	対象インターフェースから送信した MLDv1 Report, MLDv2 Report, Query, MLDv1 Done の数を表示します。

5.11.26 clear ipv6 mld snooping groups

clear ipv6 mld snooping groups	
目的	動的に学習した MLD スヌーピングエントリーを削除します。
Command	clear ipv6 mld snooping groups {all | GROUP-ADDRESS [vlan VLAN-ID]}
Parameter	all：すべての動的に学習した MLD スヌーピングエントリーを削除する場合に指定します。 GROUP-ADDRESS [vlan VLAN-ID]：削除する MLD スヌーピングエントリーの IPv6 マルチキャストグループアドレスと VLAN（省略可能）を指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドの削除対象には、宛先が未知の IPv6 マルチキャストとして学習した MLD スヌーピングエントリーも含まれます。
制限・注意	-
バージョン	1.08.02

使用例：すべての動的に学習した MLD スヌーピングエントリーを削除する方法を示します。

```
# clear ipv6 mld snooping groups all
#
```

5.11.27 clear ipv6 mld snooping unknown-data

clear ipv6 mld snooping unknown-data	
目的	宛先が未知の IPv6 マルチキャストとして学習した MLD スヌーピングエントリーを削除します。

clear ipv6 mld snooping unknown-data	
Command	clear ipv6 mld snooping unknown-data {all | vlan VLAN-ID | group GROUP-ADDRESS}
Parameter	all：すべての宛先が未知の MLD スヌーピングエントリーを削除する場合に指定します。 vlan VLAN-ID：指定した VLAN の、宛先が未知の MLD スヌーピングエントリーを削除する場合に指定します。 group GROUP-ADDRESS：指定した IPv6 マルチキャストグループアドレスの、宛先が未知の MLD スヌーピングエントリーを削除する場合に指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：宛先が未知の IPv6 マルチキャストとして学習した MLD スヌーピングエントリーを、すべて削除する方法を示します。

```
# clear ipv6 mld snooping unknown-data all
#
```

5.11.28 clear ipv6 mld snooping statistics

clear ipv6 mld snooping statistics	
目的	MLD スヌーピングの統計情報を消去します。
Command	clear ipv6 mld snooping statistics {all | vlan VLAN-ID | interface IF-ID}
Parameter	all：すべての MLD スヌーピングの統計情報を消去する場合に指定します。 vlan VLAN-ID：MLD スヌーピングの統計情報を消去する VLAN を指定します。 interface IF-ID：MLD スヌーピングの統計情報を消去するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべての MLD スヌーピングの統計情報を消去する方法を示します。

```
# clear ipv6 mld snooping statistics all
#
```

5.12 リングプロテクション(ERPS)コマンド

リングプロテクション(ERPS)関連の設定コマンドは以下のとおりです。

- ethernet ring g8032 profile
- revertive (ERPS)
- tcn-propagation
- timer (ERPS)
- ethernet ring g8032
- port0
- port1
- instance (ERPS)
- sub-ring
- description (ERPS)
- level
- profile (ERPS)
- rpl
- r-aps channel-vlan
- inclusion-list vlan-ids
- activate

リングプロテクション(ERPS)関連の show コマンドは以下のとおりです。

- show ethernet ring g8032

5.12.1 ethernet ring g8032 profile

ethernet ring g8032 profile	
目的	G.8032 プロファイルを設定します。また、G.8032 プロファイル設定モードに遷移します。遷移後のプロンプトは (config-erps-ring-profile)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ethernet ring g8032 profile NAME no ethernet ring g8032 profile NAME
Parameter	NAME：G.8032 プロファイル名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 最大登録可能数は 8 個です。
バージョン	1.08.02

使用例：G.8032 プロファイル「campus」を設定する方法を示します。

```
# configure terminal
(config)# ethernet ring g8032 profile campus
(config-erps-ring-profile)#
```

5.12.2 revertive (ERPS)

revertive (ERPS)	
目的	障害をクリアする場合に、運用系トランスポートエンティティーに戻します。装置リンクの障害状態をクリアした後、RPL が失敗していなければ、no revertive コマンドを実行して使用を継続します。
Command	revertive no revertive
Parameter	なし
デフォルト	有効
モード	G.8032 プロファイル設定モード
特権レベル	レベル：12
ガイドライン	障害をクリアする場合、トラフィックチャネルは WTR タイマーが切れると元の状態に戻ります。WTR タイマーは、障害が断続的に生じる場合に保護状態が頻繁に切り替わらないようにするためのものです。非切り戻し動作モードでは、装置リンクの障害状態がクリアされた後に RPL が失敗していなければ、トラフィックチャネルは RPL の使用を継続します。 リングプロテクション(ERPS)では、運用系トランスポートエンティティーのリソースがさらに最適化されることがあります。そのため、すべてのリングリンクが利用可能になった後、運用系トランスポートエンティティーに戻すことが推奨されます。 この動作ではトラフィックが中断されるため、運用系トランスポートエンティティーに直ちに戻すことにメリットがない場合もあります。その場合は、リングプロテクション(ERPS)を元に戻さないようにすることで、トラフィックの 2 回目の中断を回避できます。
制限・注意	• 運用中は設定を変更しないでください。
バージョン	1.08.02

使用例：G.8032 プロファイル「campus」において、切り戻し機能を無効にする方法を示します。

```
# configure terminal
(config)# ethernet ring g8032 profile campus
(config-erps-ring-profile)# no revertive
(config-erps-ring-profile)#
```

5.12.3 tcn-propagation

tcn-propagation	
目的	サブリング ERP インスタンスからメジャーリング ERP インスタンスへの、トポロジー変更通知の伝達を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	tcn-propagation no tcn-propagation
Parameter	なし
デフォルト	無効
モード	G.8032 プロファイル設定モード
特権レベル	レベル：12
ガイドライン	-

tcn-propagation	
制限・注意	-
バージョン	1.08.02

使用例：G.8032 プロファイル「campus」において、トポロジー変更通知の伝達を有効にする方法を示します。

```
# configure terminal
(config)# ethernet ring g8032 profile campus
(config-erps-ring-profile)# tcn-propagation
(config-erps-ring-profile)#
```

5.12.4 timer (ERPS)

timer (ERPS)	
目的	ERP ドメイン用のタイマーを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	timer {guard MILLISECONDS | hold-off SECONDS | wtr MINUTES} no timer [guard | hold-off | wtr]
Parameter	guard MILLISECONDS：ガードタイマー値を 10～2000 ミリ秒の範囲 (10 の倍数で指定) で指定します。 hold-off SECONDS：ホールドオフタイマー値を 0～10 秒の範囲で指定します。 wtr MINUTES：WTR タイマー値を 1～12 分の範囲で指定します。
デフォルト	ガードタイマー：500 ミリ秒 ホールドオフタイマー：0 秒 WTR タイマー：5 分
モード	G.8032 プロファイル設定モード
特権レベル	レベル：12
ガイドライン	デフォルト設定に戻すときに、パラメーターを何も指定しない場合、すべてのタイマーがリセットされます。
制限・注意	-
バージョン	1.08.02

使用例：G.8032 プロファイル「campus」において、ガードタイマーを 700 ミリ秒、ホールドオフタイマーを 1 秒、WTR タイマーを 1 分に設定する方法を示します。

```
# configure terminal
(config)# ethernet ring g8032 profile campus
(config-erps-ring-profile)# timer guard 700
(config-erps-ring-profile)# timer hold-off 1
(config-erps-ring-profile)# timer wtr 1
(config-erps-ring-profile)#
```

5.12.5 ethernet ring g8032

ethernet ring g8032	
目的	リングを設定します。また、ERPS 設定モードに遷移します。遷移後のプロンプトは (config-erps-ring)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。

ethernet ring g8032	
Command	ethernet ring g8032 RING-NAME no ethernet ring g8032 RING-NAME
Parameter	RING-NAME：リング名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 最大登録可能数は 14 個です。
バージョン	1.08.02

使用例：リング「major-ring」を設定する方法を示します。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)#
```

5.12.6 port0

port0	
目的	リングの第 1 リングポートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	port0 interface IF-ID no port0
Parameter	interface IF-ID：第 1 リングポートに設定するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
デフォルト	なし
モード	ERPS 設定モード
特権レベル	レベル：12
ガイドライン	以下の条件をすべて満たす場合、リングトポロジーは正常に動作せず、ループを生成します。 • 指定したインターフェースがポートチャネルである • ERPS インスタンスが有効化されている • ポートチャネルメンバーが変更または削除されている
制限・注意	• ERPS 機能は、同一装置で STP/RSTP/MSTP/RPVST+機能、MMRP-Plus 機能と併用できません。また、同一インターフェースでループ検知機能 (loop-detection action notify-only 設定時を除く)、ポートリダンダント機能と併用できません。
バージョン	1.08.02

使用例：リング「major-ring」の第 1 リングポートを、ポート 1/0/1 に設定する方法を示します。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# port0 interface port 1/0/1
```

```
(config-erps-ring)#
```

5.12.7 port1

port1	
目的	リングの第 2 リングポートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	port1 {interface IF-ID | none} no port1
Parameter	interface IF-ID：第 2 リングポートに設定するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 none：第 2 リングポートが存在しない場合に指定します。
デフォルト	なし
モード	ERPS 設定モード
特権レベル	レベル：12
ガイドライン	相互接続ノードがオープンリングのローカルノードのエンドポイントである場合は、port1 none コマンドを実行してください。 以下の条件をすべて満たす場合、リングトポロジーは正常に動作せず、ループを生成します。 • 指定したインターフェースがポートチャネルである • ERPS インスタンスが有効化されている • ポートチャネルメンバーが変更または削除されている
制限・注意	• ERPS 機能は、同一装置で STP/RSTP/MSTP/RPVST+機能、MMRP-Plus 機能と併用できません。また、同一インターフェースでループ検知機能（loop-detection action notify-only 設定時を除く）、ポートリダンダント機能と併用できません。
バージョン	1.08.02

使用例：リング「major-ring」の第 2 リングポートを、ポート 1/0/2 に設定する方法を示します。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# port1 interface port 1/0/2
(config-erps-ring)#
```

5.12.8 instance（ERPS）

instance（ERPS）	
目的	ERP インスタンスを設定します。また、ERPS インスタンス設定モードに遷移します。遷移後のプロンプトは（config-erps-ring-instance)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	instance ID no instance ID
Parameter	ID：ERP インスタンスの識別子を 1～32 の範囲で指定します。
デフォルト	なし
モード	ERPS 設定モード

instance (ERPS)	
特権レベル	レベル：12
ガイドライン	ERP インスタンスを設定する前に、対象リングのリングポートを port0 コマンドと port1 コマンドで設定する必要があります。
制限・注意	• ERP インスタンスは 1 リングに 1 個までのサポートとなります。
バージョン	1.08.02

使用例：リング「major-ring」において、ERP インスタンス 1 を設定する方法を示します。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# port0 interface port 1/0/1
(config-erps-ring)# port1 interface port 1/0/2
(config-erps-ring)# instance 1
(config-erps-ring-instance)#
```

5.12.9 sub-ring

sub-ring	
目的	サブリングを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	sub-ring RING-NAME no sub-ring RING-NAME
Parameter	RING-NAME：サブリングのリング名を指定します。
デフォルト	なし
モード	ERPS 設定モード
特権レベル	レベル：12
ガイドライン	メジャーリングとサブリングが共用するリンクを接続するポートは、メジャーリングのリングポートとして設定します。 メジャーリングとサブリングに設定する ERP インスタンスは別のインスタンスにする必要があります。
制限・注意	-
バージョン	1.08.02

使用例：メジャーリング「ring1」において、サブリング「ring2」を設定する方法を示します。

```
# configure terminal
(config)# ethernet ring g8032 ring1
(config-erps-ring)# port0 interface port 1/0/1
(config-erps-ring)# port1 interface port 1/0/2
(config-erps-ring)# instance 1
(config-erps-ring-instance)# exit
(config-erps-ring)# exit
(config)#
(config)# ethernet ring g8032 ring2
(config-erps-ring)# port0 interface port 1/0/21
(config-erps-ring)# port1 none
(config-erps-ring)# instance 2
(config-erps-ring-instance)# exit
(config-erps-ring)# exit
(config)#
(config)# ethernet ring g8032 ring1
(config-erps-ring)# sub-ring ring2
```

```
(config-erps-ring)#
```

5.12.10 description（ERPS）

description（ERPS）	
目的	ERP インスタンスの説明を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	description STRING no description
Parameter	STRING：ERP インスタンスの説明を最大 64 文字で指定します。ASCII コードの印字可能な文字のうち、？を除いた文字を使用可能です。スペースも使用できます。
デフォルト	なし
モード	ERPS インスタンス設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：リング「major-ring」の ERP インスタンス 1 において、ERP インスタンスの説明「ERPS Major-Ring Instance 1」を設定する方法を示します。本使用例では、先に設定が必要な他コマンドは設定済みとします。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# instance 1
(config-erps-ring-instance)# description ERPS Major-Ring Instance 1
(config-erps-ring-instance)#
```

5.12.11 level

level	
目的	ERP インスタンスのリング MEL 値（管理レベル）を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	level VALUE no level
Parameter	VALUE：ERP インスタンスのリング MEL 値（管理レベル）を 0～7 の範囲で指定します。
デフォルト	1
モード	ERPS インスタンス設定モード
特権レベル	レベル：12
ガイドライン	同じ ERP インスタンスに加わるリングノードのリング MEL 値（管理レベル）は、すべて同一に設定してください。
制限・注意	• CFM 機能と併用する場合は、リング MEL 値（管理レベル）を CFM のドメインレベルより高く設定してください。
バージョン	1.08.02

使用例：リング「major-ring」の ERP インスタンス 1 において、リング MEL 値を 6 に設定する方法を示します。本使用例では、先に設定が必要な他コマンドは設定済みとします。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# instance 1
(config-erps-ring-instance)# level 6
(config-erps-ring-instance)#
```

5.12.12 profile（ERPS）

profile (ERPS)	
目的	ERP インスタンスに関連付ける G.8032 プロファイルを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	profile NAME no profile NAME
Parameter	NAME：ERP インスタンスに関連付ける G.8032 プロファイル名を指定します。
デフォルト	なし
モード	ERPS インスタンス設定モード
特権レベル	レベル：12
ガイドライン	複数の ERP インスタンスに同じ G.8032 プロファイルを関連付けることができます。一般的に、同じ G.8032 プロファイルを関連付けた ERP インスタンスでは同じ VLAN を保護するか、または、ある ERP インスタンスが保護する VLAN が別の ERP インスタンスが保護する VLAN のサブセットになります。
制限・注意	• 対象の ERP インスタンスが有効な状態では、関連付ける G.8032 プロファイルを変更できません。
バージョン	1.08.02

使用例：リング「major-ring」の ERP インスタンス 1 において、G.8032 プロファイル「campus」を関連付ける方法を示します。本使用例では、先に設定が必要な他コマンドは設定済みとします。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# instance 1
(config-erps-ring-instance)# profile campus
(config-erps-ring-instance)#
```

5.12.13 rpl

rpl	
目的	RPL オーナーおよびネイバーとしてノードを設定して、RPL ポートを割り当てます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	rpl {port0 | port1} [owner] no rpl
Parameter	port0：物理リングの第 1 リングポート（port0）を RPL ポートとして設定する場合に指定します。 port1：物理リングの第 2 リングポート（port1）を RPL ポートとして設定する場合に指定します。 owner（省略可能）：装置を RPL オーナーとして設定する場合に指定します。
デフォルト	なし

rpl	
モード	ERPS インスタンス設定モード
特権レベル	レベル：12
ガイドライン	設定されている ERP インスタンスの RPL オーナーノード、ネイバーノードまたは次のネイバーノードとしてのリングノード、RPL ポートとして動作するリングポートを指定するコマンドです。
制限・注意	-
バージョン	1.08.02

使用例：リング「major-ring」の ERP インスタンス 1 において、RPL オーナーとして第 1 リングポート（port0）を RPL ポートに設定する方法を示します。本使用例では、先に設定が必要な他コマンドは設定済みとします。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# instance 1
(config-erps-ring-instance)# rpl port0 owner
(config-erps-ring-instance)#
```

5.12.14 r-aps channel-vlan

r-aps channel-vlan	
目的	ERP インスタンス用の APS チャネル VLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	r-aps channel-vlan VLAN-ID no r-aps channel-vlan
Parameter	VLAN-ID：ERP インスタンスに使用する APS チャネル VLAN を 1～4094 の範囲で指定します。
デフォルト	なし
モード	ERPS インスタンス設定モード
特権レベル	レベル：12
ガイドライン	ERP インスタンスの動作中に APS チャネル VLAN が削除されると、ERP インスタンスは無効の状態になり、操作できなくなります。 各 ERP インスタンスには、一意の APS チャネル VLAN が必要です。 サブリング ERP インスタンスの APS チャネル VLAN は、サブリングの仮想チャネルでもあります。
制限・注意	• ERP インスタンスを動作状態にする場合は、APS チャネル VLAN をあらかじめ割り当ててください。 • コマンドの設定には APS チャネル VLAN は必要ありませんが、ERP インスタンスが動作状態になる前には設定してください。
バージョン	1.08.02

使用例：リング「major-ring」の ERP インスタンス 1 において、APS チャネル VLAN を VLAN 4000 に設定する方法を示します。本使用例では、先に設定が必要な他コマンドは設定済みとします。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# instance 1
```

```
(config-erps-ring-instance)# r-aps channel-vlan 4000
(config-erps-ring-instance)#
```

5.12.15 inclusion-list vlan-ids

inclusion-list vlan-ids	
目的	リングプロテクションのメカニズムによって保護される VLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	inclusion-list vlan-ids VLAN-ID [,|-] no inclusion-list vlan-ids VLAN-ID [,|-]
Parameter	VLAN-ID：対象の ERP インスタンスで保護される VLAN ID を 1～4094 の範囲で指定します。複数指定できます。
デフォルト	なし
モード	ERPS インスタンス設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 保護する VLAN の数が多くなるに従って、FDB フラッシュ処理時間も長くなります。(例：100 個の VLAN を設定した場合、1 秒程度)
バージョン	1.08.02

使用例：リング「major-ring」の ERP インスタンス 1 において、保護する VLAN を VLAN 100～200 に設定する方法を示します。本使用例では、先に設定が必要な他コマンドは設定済みとします。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# instance 1
(config-erps-ring-instance)# inclusion-list vlan-ids 100-200
(config-erps-ring-instance)#
```

5.12.16 activate

activate	
目的	ERP インスタンスを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	activate no activate
Parameter	なし
デフォルト	無効
モード	ERPS インスタンス設定モード
特権レベル	レベル：12
ガイドライン	以下の条件では、アクティブ化される ERP インスタンスは非動作状態になります。 • 設定した APS チャネル VLAN が存在しない。 • 設定したリングポートが、APS チャネル VLAN のタグ付きメンバーポートでない。 上にあげた 3 項目の設定以外に、サービスを保護する VLAN の設定と RPL 関連の設定も、ERP インスタンスの動作には不可欠です。
制限・注意	• アクティブ化の前に、リングポート、APS チャネル VLAN、および G.8032 プロ

activate	
	ファイルを設定してください。
バージョン	1.08.02

使用例：リング「major-ring」の ERP インスタンス 1 を有効にする方法を示します。本使用例では、先に設定が必要な他コマンドは設定済みとします。

```
# configure terminal
(config)# ethernet ring g8032 major-ring
(config-erps-ring)# instance 1
(config-erps-ring-instance)# activate
(config-erps-ring-instance)#
```

5.12.17 show ethernet ring g8032

show ethernet ring g8032	
目的	ERP インスタンスの情報を表示します。
Command	show ethernet ring g8032 {status | brief} [RING-NAME]
Parameter	status：ERP インスタンスの詳細情報を表示する場合に指定します。 brief：ERP インスタンスの概要を表示する場合に指定します。 RING-NAME（省略可能）：リング名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ERP インスタンスの詳細情報を表示する方法を示します。

```
# show ethernet ring g8032 status

 ERPS Version: G.8032v1 ...(1)
 ----------------------------
 Ethernet Ring ring1 ...(2)
 Admin Port0: Port1/0/1 ...(3)
 Admin Port1: Port1/0/2 ...(3)
 ----------------------------
 Instance  : 1 ...(4)
 Instance Status: Protection ...(5)
 (6)                 (7)
 R-APS Channel : 2,Protected VLANs:1,3-4094
 Port0: Port1/0/1, SF blocked ...(8)
 Port1: Port1/0/2, Forwarding ...(8)
 Profile: ...(9)
 Description : ...(10)
 Guard Timer: 500 milliseconds ...(11)
 Hold-off Timer: 0 milliseconds ...(12)
 WTR Timer: 5 minutes ...(13)
 Revertive ...(14)
 MEL: 1 ...(15)
 RPL Role: Owner ...(16)
 RPL Port: Port0 ...(17)
 Sub Ring Instance : 2, TC Propagation State: Disabled ...(18)

 ----------------------------
```

```
Ethernet Ring ring2
Admin Port0: Port1/0/3
Admin Port1: virtual_channel
----------------------------
Instance  : 2
Instance Status: Protection
R-APS Channel : 3,Protected VLANs:1-2,4-4094
Port0: Port1/0/3, Blocking
Port1: virtual_channel, Forwarding
Profile: p1
Description :
Guard Timer: 500 milliseconds
Hold-off Timer: 0 milliseconds
WTR Timer: 5 minutes
Revertive
MEL: 1
RPL Role: Owner
RPL Port: Port0
Sub Ring Instance: none
```

項番	説明
(1)	リングプロテクション(ERPS)の対応バージョンを表示します。
(2)	リング名を表示します。
(3)	リングポート（port0、port1）として使用するポート番号またはポートチャネル番号を表示します。
(4)	インスタンス ID を表示します。
(5)	ERP インスタンスの現在のリングノードの状態を表示します。 Deactivated：非アクティブ Idle：アイドル Protection：保護
(6)	ERP インスタンスの APS チャネル VLAN を表示します。
(7)	ERP インスタンスで保護している VLAN を表示します。
(8)	リングポート（port0、port1）の状態を表示します。 Forwarding：転送 Blocked：閉塞（リンクアップ時） SF Blocked：閉塞（リンクダウン時）
(9)	ERP インスタンスに関連付けられたプロファイル名を表示します。
(10)	ERP インスタンスの説明を表示します。
(11)	ガードタイマーのタイマー値を表示します。
(12)	ホールドオフタイマーのタイマー値を表示します。
(13)	WTR タイマーのタイマー値を表示します。
(14)	切り戻し機能の有効(Revertive)／無効(Non-revertive)を表示します。
(15)	ERP インスタンスのリング MEL 値（管理レベル）を表示します。
(16)	ノードの役割（Owner：RPL オーナー／None：役割なし）を表示します。
(17)	RPL ポートとして設定されているリングポートを表示します。
(18)	サブリングとして使用するリングに関する情報を表示します。 none：サブリングなし TC Propagation State:Enabled：トポロジー変更通知を伝達する

項番	説明
	TC Propagation State:Disabled：トポロジー変更通知を伝達しない

使用例：ERP インスタンスの概要情報を表示する方法を示します。

```
# show ethernet ring g8032 brief

ERPS Version : G.8032v1 ...(1)
(2)                              (3)      (4)          (5)
Ring                             InstID   Status       Port-State
-----                            ----     -----        -------
ring1                            1        Idle         p0:Port1/0/1,Blocking(RPL)
                                                       p1:Port1/0/2,Forwarding
ring2                            2        Idle         p0:Port1/0/3,Forwarding
                                                       p1:-,Forwarding
Total Entries: 2
```

項番	説明
(1)	リングプロテクション(ERPS)の対応バージョンを表示します。
(2)	リング名を表示します。
(3)	ERP インスタンスのインスタンス ID を表示します。
(4)	ERP インスタンスの現在の状態を表示します。 Deactivated：ERP インスタンスが非アクティブ Idle：ERP インスタンスは標準状態（RPL ポートが閉塞状態） Protection：いずれかのリングポートで障害を検出（RPL ポートが開放状態）
(5)	現在の RPL ポート（port0、port1）のポート番号またはポートチャネル番号、および状態を表示します。 Blocked：閉塞（リンクアップ時） Blocked（RPL）：閉塞（リンクアップ時） SF Blocked：閉塞（リンクダウン時） SF Blocked（RPL）：閉塞（リンクダウン時） Forwarding：開放

5.13 MMRP-Plus コマンド

MMRP-Plus 関連の設定コマンドは以下のとおりです。

- mmrp-plus enable
- mmrp-plus switch hello-interval
- mmrp-plus switch polling-rate
- mmrp-plus vlangroup slave-vid
- no mmrp-plus ring
- mmrp-plus ring name
- mmrp-plus ring vid
- mmrp-plus ring vlangroup
- mmrp-plus ring ring-master
- mmrp-plus ring divided-master
- mmrp-plus ring divided-slave
- mmrp-plus ring aware
- mmrp-plus ring revertive
- mmrp-plus ring transmit-fdb-flush port
- mmrp-plus ring transmit-fdb-flush retransmit enable
- mmrp-plus ring fdb-flush port
- mmrp-plus ring fdb-flush timer
- mmrp-plus ring listening-timer
- mmrp-plus ring hello-timeout
- mmrp-plus ring port-restart enable
- mmrp-plus ring port-restart forcedown-time
- mmrp-plus ring port-restart linkup-wait
- mmrp-plus ring uplink port

MMRP-Plus 関連の show／操作コマンドは以下のとおりです。

- show mmrp-plus configuration
- show mmrp-plus configuration ring
- show mmrp-plus vlangroup
- show mmrp-plus status
- show mmrp-plus status port
- show mmrp-plus status ring
- clear mmrp-plus failure ring
- debug mmrp

5.13.1 mmrp-plus enable

mmrp-plus enable	
目的	MMRP-Plus を有効にし、リングの動作を開始します。無効にする場合は、no 形式のコマンドを使用します。
Command	mmrp-plus enable no mmrp-plus enable
Parameter	なし

mmrp-plus enable	
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	コマンド実行後、MMRP-Plus が有効になるまで、時間がかかる場合があります。
制限・注意	• AEOS-NP2500 Ver. 1.13.01 以降では、MMRP-Plus 機能と STP/RSTP/MSTP/RPVST+機能との装置併用をサポートしました。なお、同一インターフェース（物理ポートまたはポートチャネル）では引き続き併用不可です。装置併用をする場合は、MMRP-Plus 機能のリングポート（物理ポートまたはポートチャネル）において、必ずスパニングツリープロトコルのインターフェースごとの設定を無効（spanning-tree state disable）にしてください。 • AEOS-NP2500 Ver. 1.13.01 より前のバージョンでは、MMRP-Plus 機能と STP/RSTP/MSTP/RPVST+機能は、同一装置で併用できません。 • MMRP-Plus 機能と ERPS 機能は、同一装置で併用できません。 • MMRP-Plus 機能は、同一インターフェースでループ検知機能（loop-detection action notify-only 設定時を除く）、ポートリダンダント機能と併用できません。 • 本機能はアクセスリスト機能と同じハードウェアリソース（Ingress グループ）を使用します。本機能で使用中の Ingress グループは、他の機能では使用できません。グループの利用状況は show access-list resource reserved-group コマンドで確認できます。
バージョン	1.08.02 1.13.01：装置併用に関する仕様変更

使用例：MMRP-Plus を有効にする方法を示します。

```
# configure terminal
(config)# mmrp-plus enable
(config)#
```

5.13.2 mmrp-plus switch hello-interval

mmrp-plus switch hello-interval	
目的	MMRP-Plus のハローフレームの送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus switch hello-interval MILLISECONDS no mmrp-plus switch hello-interval
Parameter	MILLISECONDS：ハローフレームの送信間隔を 100～10000 ミリ秒の範囲で指定します。
デフォルト	100 ミリ秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	MMRP-Plus のハローフレームの送信間隔を長く設定すると、ネットワーク構成によっては MMRP-Plus の動作が不安定になることがあります。
制限・注意	• 本コマンドの設定値は、同一リング内のすべての装置で揃えてください。 • MMRP-Plus 動作中に本設定を変更しても反映されません。本設定を反映するには、no mmrp-plus enable コマンドにて MMRP-Plus をいったん無効状態にした

mmrp-plus switch hello-interval	
	後、再度 MMRP-Plus を有効にしてください。
バージョン	1.08.02

使用例：ハローフレームの送信間隔を 1000 ミリ秒に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus switch hello-interval 1000
(config)#
```

5.13.3 mmrp-plus switch polling-rate

mmrp-plus switch polling-rate	
目的	MMRP-Plus のハローフレームのポーリングレートを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus switch polling-rate VALUE no mmrp-plus switch polling-rate
Parameter	VALUE：ハローフレームのポーリングレートを 2～100 の範囲で指定します。
デフォルト	10 倍
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ポーリングレート（polling-rate）を 10 に設定していて、ハローフレームの送信間隔（hello-interval）を 100 ミリ秒（デフォルト）に設定している場合は、ハローフレーム受信タイムアウト時間は、100 ミリ秒×10＝1000 ミリ秒（1 秒）になります。 ポーリングレート（polling-rate）が大きいほど、障害を検知するまでに時間がかかります。
制限・注意	• 本コマンドの設定値は、同一リング内のすべての装置で揃えてください。 • MMRP-Plus 動作中に本設定を変更しても反映されません。本設定を反映するには、no mmrp-plus enable コマンドにて MMRP-Plus をいったん無効状態にした後、再度 MMRP-Plus を有効にしてください。
バージョン	1.08.02

使用例：ハローフレームのポーリングレートを 5 倍に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus switch polling-rate 5
(config)#
```

5.13.4 mmrp-plus vlangroup slave-vid

mmrp-plus vlangroup slave-vid	
目的	MMRP-Plus の VLAN グループのスレーブ VLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mmrp-plus vlangroup GROUP slave-vid VLAN-ID [,|-] no mmrp-plus vlangroup GROUP [slave-vid VLAN-ID [,|-]]
Parameter	GROUP：VLAN グループの番号を 1～8 の範囲で指定します。 VLAN-ID：スレーブ VLAN として使用する VLAN ID を 1～4094 の範囲で指定します。複数指定できます。

mmrp-plus vlangroup slave-vid	
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドで指定した VLAN がスレーブ VLAN に設定され、その他の VLAN が、マスターVLAN に設定されます。 MMRP-Plus のリングに VLAN グループを割り当てるには、mmrp-plus ring vlangroup コマンドを使用します。MMRP-Plus のリングに VLAN グループを割り当てると、マスターVLAN では、マスターポートは Forwarding 状態になり、スレーブポートは Blocking 状態になります。一方、スレーブ VLAN では、マスターポートは Blocking 状態になり、スレーブポートは Forwarding 状態になります。 スレーブ VLAN をマスターVLAN に戻すには、no mmrp-plus vlangroup slave-vid コマンドを使用します。本コマンドで VLAN ID を省略した場合は、すべての VLAN がマスターVLAN に戻ります。
制限・注意	• 分散マスター構成で使用する場合は、分散マスター装置と分散スレーブ装置で同一の設定にしてください。設定が異なると、MMRP-Plus が正常に動作しないことがあります。 • 本設定は、リング内の任意の経路がリンクダウン（マスター装置およびスレーブ装置の MMRP-Plus リングポートの状態が Forwarding、または Down）時に変更してください。リング内の経路がすべてリンクアップ時に変更を行うとループが発生する可能性があります。
バージョン	1.08.02

使用例：VLAN グループ 8 のスレーブ VLAN を VLAN 1001～1100 に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus vlangroup 8 slave-vid 1001-1100
(config)#
```

5.13.5 no mmrp-plus ring

no mmrp-plus ring	
目的	指定したリング ID に関する MMRP-Plus の設定をすべて削除します。
Command	no mmrp-plus ring ID [,|-]
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：リング ID 1 に関する MMRP-Plus の設定をすべて削除する方法を示します。

```
# configure terminal
(config)# no mmrp-plus ring 1
(config)#
```

5.13.6 mmrp-plus ring name

mmrp-plus ring name	
目的	MMRP-Plus のリングに名前を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] name NAME no mmrp-plus ring ID [,|-] name
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 NAME：MMRP-Plus のリング名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：リング ID 1 のリング名を「Ring1」に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1 name Ring1
(config)#
```

5.13.7 mmrp-plus ring vid

mmrp-plus ring vid	
目的	MMRP-Plus で使用する MMRP-Plus 制御フレームの VLAN ID を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] vid VLAN-ID no mmrp-plus ring ID [,|-] vid
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 VLAN-ID：MMRP-Plus 制御フレームの VLAN ID を 1～4094 の範囲で指定します。
デフォルト	VLAN 1
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	MMRP-Plus が有効、かつ、以下のいずれかを設定している場合は、リングが動作しているため本設定は変更できません。 • mmrp-plus ring ring-master コマンド • mmrp-plus ring divided-master コマンド • mmrp-plus ring divided-slave コマンド • mmrp-plus ring aware コマンド 本コマンドで設定を変更する場合は、上記のコマンドで設定を変更する前（MMRP-Plus 動作前）に、本コマンドを実行してください。MMRP-Plus 動作中に本コマンドを実行する場合は、MMRP-Plus のリングに設定されている上記のコマンドの設定を

mmrp-plus ring vid	
	削除してください。
制限・注意	• MMRP-Plus 制御フレームの VLAN ID は、同一の MMRP-Plus のリング内のすべての MMRP-Plus 装置に対して、同一の設定にしてください。 • MMRP-Plus 制御フレームを送受信する VLAN は、「MMRP-Plus 制御フレームを送受信する専用 VLAN」としてリングごとに用意し、ユーザーVLAN と分けることを推奨します。 • 複数のリングで MMRP-Plus 制御フレームを送受信する VLAN を同一 VLAN ID に設定した場合、ハローフレームを複数のポートで受信するため、FDB 書き換えが常時発生します。そのため、リングを複数設定する場合、MMRP-Plus 制御フレームを送受信する VLAN はリングごとに異なる VLAN ID を設定することを推奨します。 • MMRP-Plus 制御フレームの VLAN として設定された VLAN は、no vlan コマンドを実行しても削除できません。
バージョン	1.08.02

使用例：リング ID 1 の MMRP-Plus 制御フレームの VLAN を VLAN 100 に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1 vid 100
(config)#
```

5.13.8 mmrp-plus ring vlangroup

mmrp-plus ring vlangroup	
目的	MMRP-Plus のリングに VLAN グループを割り当てます。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] vlangroup GROUP no mmrp-plus ring ID [,|-] vlangroup
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 GROUP：VLAN グループ番号を 1～8 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	MMRP-Plus が有効、かつ、以下のいずれかを設定している場合は、リングが動作しているため本設定は変更できません。 • mmrp-plus ring ring-master コマンド • mmrp-plus ring divided-master コマンド • mmrp-plus ring divided-slave コマンド • mmrp-plus ring aware コマンド 本コマンドで設定を変更する場合は、上記のコマンドで設定を変更する前（MMRP-Plus 動作前）に、本コマンドを実行してください。MMRP-Plus 動作中に本コマンドを実行する場合は、MMRP-Plus のリングに設定されている上記のコマンドの設定を削除してください。
制限・注意	• リングの動作中は、VLAN グループの割り当てができません。VLAN グループの割り当て、および VLAN グループの変更は、リング構成を解除し、no mmrp-plus

mmrp-plus ring vlangroup	
	enable コマンドでリングの動作を停止してから行ってください。
バージョン	1.08.02

使用例：リング ID 1 に VLAN グループ 8 を割り当てる方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1 vlangroup 8
(config)#
```

5.13.9 mmrp-plus ring ring-master

mmrp-plus ring ring-master	
目的	シングルマスター構成の MMRP-Plus リングを構成する、マスター装置のマスターポートとスレーブポートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	**mmrp-plus ring** ID **ring-master master** IF-ID **slave** IF-ID **no mmrp-plus ring** ID **ring-master**
Parameter	ID：リング ID を 1～1000 の範囲で指定します。 master IF-ID：マスターポートに設定するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 slave IF-ID：スレーブポートに設定するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	スタック跨ぎのポートチャネルを、マスターポートまたはスレーブポートとして使用することはできません。 ポートチャネルを指定する場合は、あらかじめメンバーポートを設定してください。メンバーポートが 1 ポートも存在しないポートチャネルを指定して本コマンドを設定できません。
制限・注意	• リングポートは、装置ごとに最大 50 個まで設定できます。スタック構成を組んでいても、リングポート数は装置 1 台分の値となります。 • MMRP-Plus のリングポートでは、ループ検知機能（loop-detection action notify-only 設定時を除く）、CFM 機能を有効にすることは未サポートです。 • MMRP-Plus のリングポートに指定したポートチャネルでメンバーポートを追加・削除したり、ポートチャネル自体を削除するには、MMRP-Plus を無効状態にする必要があります。ループなどが発生しないよう注意して実施してください。 • MMRP-Plus 制御フレームの送出・中継を他のユーザートラフィックよりも優先させるために、MMRP-Plus のリングポートでは以下のいずれかの設定により、制御フレームを中継する送信キュー（デフォルト設定では送信キュー7）が Strict Priority Queuing でスケジューリングされるように設定してください。

mmrp-plus ring ring-master	
	• リングポートのスケジューリング設定を Strict Priority Queuing に設定（mls qos scheduler sp） • リングポートのスケジューリング設定が WRR（Weighted Round Robin）の場合は、wrr-queue bandwidth コマンドで送信キュー7 の重みを 0 に設定（例：wrr-queue bandwidth 1 2 3 4 5 6 7 0） • リングポートのスケジューリング設定が WDRR（Weighted Deficit Round Robin）の場合は、wdrr-queue bandwidth コマンドで送信キュー7 の重みを 0 に設定（例：wdrr-queue bandwidth 1 2 3 4 5 6 7 0） • なお、一部の機種（ApresiaNP5000 シリーズ、ApresiaNP4000 シリーズ）では、対象ポートが輻輳状態の場合に mls qos scheduler 設定を正常に変更できない制限があるため、mls qos scheduler 設定を変更する場合は対象ポートを shutdown 設定で閉塞した状態で設定を変更してください。 • 1 つのポートチャネルにおいて、異なる帯域のメンバーポートが混在する構成は未サポートです。そのような構成のポートチャネルを MMRP-Plus のリングポートに指定しないでください。
バージョン	1.08.02

使用例：リング ID 1 のマスターポートをポート 1/0/1 に、スレーブポートをポートチャネル 1 に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1 ring-master master port 1/0/1 slave port-channel 1
(config)#
```

5.13.10 mmrp-plus ring divided-master

mmrp-plus ring divided-master	
目的	分散マスター構成の MMRP-Plus リングを構成する、分散マスター装置の分散マスターポートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID divided-master IF-ID no mmrp-plus ring ID divided-master
Parameter	ID：リング ID を 1～1000 の範囲で指定します。 IF-ID：分散マスターポートに設定するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	スタック跨ぎのポートチャネルを、分散マスターポートとして使用することはできません。 ポートチャネルを指定する場合は、あらかじめメンバーポートを設定してください。メンバーポートが 1 ポートも存在しないポートチャネルを指定して本コマンドを設定できません。
制限・注意	• リングポートは、装置ごとに最大 50 個まで設定できます。スタック構成を組んでいても、リングポート数は装置 1 台分の値となります。

mmrp-plus ring divided-master	
	• MMRP-Plus のリングポートでは、ループ検知機能（loop-detection action notify-only 設定時を除く）、CFM 機能を有効にすることは未サポートです。 • MMRP-Plus のリングポートに指定したポートチャネルでメンバーポートを追加・削除したり、ポートチャネル自体を削除するには、MMRP-Plus を無効状態にする必要があります。ループなどが発生しないよう注意して実施してください。 • MMRP-Plus 制御フレームの送出・中継を他のユーザートラフィックよりも優先させるために、MMRP-Plus のリングポートでは以下のいずれかの設定により、制御フレームを中継する送信キュー（デフォルト設定では送信キュー7）が Strict Priority Queuing でスケジューリングされるように設定してください。 　• リングポートのスケジューリング設定を Strict Priority Queuing に設定（mls qos scheduler sp） 　• リングポートのスケジューリング設定が WRR（Weighted Round Robin）の場合は、wrr-queue bandwidth コマンドで送信キュー7 の重みを 0 に設定（例：wrr-queue bandwidth 1 2 3 4 5 6 7 0） 　• リングポートのスケジューリング設定が WDRR（Weighted Deficit Round Robin）の場合は、wdrr-queue bandwidth コマンドで送信キュー7 の重みを 0 に設定（例：wdrr-queue bandwidth 1 2 3 4 5 6 7 0） • なお、一部の機種（ApresiaNP5000 シリーズ、ApresiaNP4000 シリーズ）では、対象ポートが輻輳状態の場合に mls qos scheduler 設定を正常に変更できない制限があるため、mls qos scheduler 設定を変更する場合は対象ポートを shutdown 設定で閉塞した状態で設定を変更してください。 • 1 つのポートチャネルにおいて、異なる帯域のメンバーポートが混在する構成は未サポートです。そのような構成のポートチャネルを MMRP-Plus のリングポートに指定しないでください。
バージョン	1.08.02

使用例：リング ID 3 の分散マスターポートをポート 1/0/7 に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 3 divided-master port 1/0/7
(config)#
```

5.13.11 mmrp-plus ring divided-slave

mmrp-plus ring divided-slave	
目的	分散マスター構成の MMRP-Plus リングを構成する、分散スレーブ装置の分散スレーブポートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID divided-slave IF-ID no mmrp-plus ring ID divided-slave
Parameter	ID：リング ID を 1～1000 の範囲で指定します。 IF-ID：分散スレーブポートに設定するインターフェースを、以下のパラメーターで指定します。 　• port：物理ポート指定 　• port-channel <1-48>：ポートチャネル指定
デフォルト	なし
モード	グローバル設定モード

mmrp-plus ring divided-slave	
特権レベル	レベル：12
ガイドライン	スタック跨ぎのポートチャネルを、分散スレーブポートとして使用することはできません。 ポートチャネルを指定する場合は、あらかじめメンバーポートを設定してください。メンバーポートが 1 ポートも存在しないポートチャネルを指定して本コマンドを設定できません。

制限・注意	• リングポートは、装置ごとに最大 50 個まで設定できます。スタック構成を組んでいても、リングポート数は装置 1 台分の値となります。
	
	• MMRP-Plus のリングポートでは、ループ検知機能（loop-detection action notify-only 設定時を除く）、CFM 機能を有効にすることは未サポートです。
	
	• MMRP-Plus のリングポートに指定したポートチャネルでメンバーポートを追加・削除したり、ポートチャネル自体を削除するには、MMRP-Plus を無効状態にする必要があります。ループなどが発生しないよう注意して実施してください。
	
	• MMRP-Plus 制御フレームの送出・中継を他のユーザートラフィックよりも優先させるために、MMRP-Plus のリングポートでは以下のいずれかの設定により、制御フレームを中継する送信キュー（デフォルト設定では送信キュー7）が Strict Priority Queuing でスケジューリングされるように設定してください。
	  • リングポートのスケジューリング設定を Strict Priority Queuing に設定（mls qos scheduler sp）
	  • リングポートのスケジューリング設定が WRR（Weighted Round Robin）の場合は、wrr-queue bandwidth コマンドで送信キュー7 の重みを 0 に設定（例：wrr-queue bandwidth 1 2 3 4 5 6 7 0）
	  • リングポートのスケジューリング設定が WDRR（Weighted Deficit Round Robin）の場合は、wdrr-queue bandwidth コマンドで送信キュー7 の重みを 0 に設定（例：wdrr-queue bandwidth 1 2 3 4 5 6 7 0）
	
	• なお、一部の機種（ApresiaNP5000 シリーズ、ApresiaNP4000 シリーズ）では、対象ポートが輻輳状態の場合に mls qos scheduler 設定を正常に変更できない制限があるため、mls qos scheduler 設定を変更する場合は対象ポートを shutdown 設定で閉塞した状態で設定を変更してください。
	
	• 1 つのポートチャネルにおいて、異なる帯域のメンバーポートが混在する構成は未サポートです。そのような構成のポートチャネルを MMRP-Plus のリングポートに指定しないでください。

バージョン	1.08.02

使用例：リング ID 3 の分散スレーブポートをポートチャネル 1 に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 3 divided-slave port-channel 1
(config)#
```

5.13.12 mmrp-plus ring aware

mmrp-plus ring aware	
目的	アウェア装置のアウェアポートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID aware IF-ID IF-ID

mmrp-plus ring aware	
	no mmrp-plus ring ID aware
Parameter	ID：リング ID を 1～1000 の範囲で指定します。 IF-ID：アウェアポートに設定するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ポートチャネルを指定する場合は、あらかじめメンバーポートを設定してください。メンバーポートが 1 ポートも存在しないポートチャネルを指定して本コマンドを設定できません。
制限・注意	• リングポートは、装置ごとに最大 50 個まで設定できます。スタック構成を組んでいても、リングポート数は装置 1 台分の値となります。 • MMRP-Plus のリングポートでは、ループ検知機能（loop-detection action notify-only 設定時を除く）、CFM 機能を有効にすることは未サポートです。 • MMRP-Plus のリングポートに指定したポートチャネルでメンバーポートを追加・削除したり、ポートチャネル自体を削除するには、MMRP-Plus を無効状態にする必要があります。ループなどが発生しないよう注意して実施してください。 • MMRP-Plus 制御フレームの送出・中継を他のユーザートラフィックよりも優先させるために、MMRP-Plus のリングポートでは以下のいずれかの設定により、制御フレームを中継する送信キュー（デフォルト設定では送信キュー7）が Strict Priority Queuing でスケジューリングされるように設定してください。 • リングポートのスケジューリング設定を Strict Priority Queuing に設定（mls qos scheduler sp） • リングポートのスケジューリング設定が WRR（Weighted Round Robin）の場合は、wrr-queue bandwidth コマンドで送信キュー7 の重みを 0 に設定（例：wrr-queue bandwidth 1 2 3 4 5 6 7 0） • リングポートのスケジューリング設定が WDRR（Weighted Deficit Round Robin）の場合は、wdrr-queue bandwidth コマンドで送信キュー7 の重みを 0 に設定（例：wdrr-queue bandwidth 1 2 3 4 5 6 7 0） • なお、一部の機種（ApresiaNP5000 シリーズ、ApresiaNP4000 シリーズ）では、対象ポートが輻輳状態の場合に mls qos scheduler 設定を正常に変更できない制限があるため、mls qos scheduler 設定を変更する場合は対象ポートを shutdown 設定で閉塞した状態で設定を変更してください。 • 1 つのポートチャネルにおいて、異なる帯域のメンバーポートが混在する構成は未サポートです。そのような構成のポートチャネルを MMRP-Plus のリングポートに指定しないでください。
バージョン	1.08.02

使用例：リング ID 5 のアウェアポートを、ポート 1/0/1 とポート 1/0/2 に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 5 aware port 1/0/1 port 1/0/2
(config)#
```

5.13.13 mmrp-plus ring revertive

mmrp-plus ring revertive	
目的	リンクダウン障害が復旧した後の切り戻り方法を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] revertive {SECONDS | disable} no mmrp-plus ring ID [,|-] revertive
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 SECONDS：自動切り戻りタイマー値を 0～86,400 秒の範囲で指定します。 disable：手動切り戻りに設定する場合に指定します。
デフォルト	自動切り戻り（切り戻りタイマー値：0 秒）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	切り戻りタイマー値が 0（デフォルト設定）の場合は、リンクダウン障害が復旧するとすぐに Listening 状態へ遷移し、リング復旧処理が開始されます。この場合は、リング復旧待機状態（FailureUp）には遷移しません。 切り戻りタイマー値が 0 以外に設定されている場合は、リンクダウン障害が復旧するとリング復旧待機状態（FailureUp）に遷移します。そして、切り戻りタイマー値の経過後に Listening 状態へ遷移し、リング復旧処理が開始されます。 disable パラメーターを指定した場合は、clear mmrp-plus failure ring コマンドを実行するまではリング復旧処理が開始されません。
制限・注意	-
バージョン	1.08.02

使用例：リング ID 5 のリンクダウン障害が復旧した後の切り戻り方法を、手動切り戻りに設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 5 revertive disable
(config)#
```

5.13.14 mmrp-plus ring transmit-fdb-flush port

mmrp-plus ring transmit-fdb-flush port	
目的	指定リングで障害が発生もしくは復旧したときに、異なるリングに対して MAC アドレステーブルを消去するための FDB フラッシュフレームを送信するポートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] transmit-fdb-flush port PORTS no mmrp-plus ring ID [,|-] transmit-fdb-flush port
Parameter	ID：障害発生元となる MMRP-Plus リングのリング ID を 1～1000 の範囲で指定します。複数指定できます。 PORTS：FDB フラッシュフレームの送信ポートを指定します。複数指定できます。
デフォルト	なし
モード	グローバル設定モード

mmrp-plus ring transmit-fdb-flush port	
特権レベル	レベル：12
ガイドライン	本機能は分散マスター構成のリングでのみ有効な機能で、分散マスター装置、分散スレーブ装置で使用できます。 隣接する複数のリングの経路変更が連動して動作する必要があるネットワーク構成の場合に、本コマンドで FDB フラッシュフレームを送信するポートを設定します。
制限・注意	• 本機能は、シングルマスター構成のマスター装置、またはアウェア装置では使用できません。
バージョン	1.08.02

使用例：リング ID 3 での障害発生／復旧時に、別リングの MMRP-Plus リングポート 1/0/5 から FDB フラッシュフレームを送信する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 3 transmit-fdb-flush port 1/0/5
(config)#
```

5.13.15 mmrp-plus ring transmit-fdb-flush retransmit enable

mmrp-plus ring transmit-fdb-flush retransmit enable	
目的	分散マスターポートもしくは分散スレーブポートで受信した別リングから送信されてきた FDB フラッシュフレームを、異なるリングへ中継する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] transmit-fdb-flush retransmit enable no mmrp-plus ring ID [,|-] transmit-fdb-flush retransmit enable
Parameter	ID：FDB フラッシュフレームの中継元となる MMRP-Plus リングのリング ID を 1～1000 の範囲で指定します。複数指定できます。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本機能を使用する場合は、mmrp-plus ring transmit-fdb-flush port コマンドも設定する必要があります。 本機能を有効にしたリングでは、分散マスターポートもしくは分散スレーブポートで FDB フラッシュフレームを受信した場合、mmrp-plus ring transmit-fdb-flush port コマンドで指定されているポートに中継します。
制限・注意	• 複数のリングで本機能を有効にした際に FDB フラッシュフレームの中継がループしないよう、終端に該当するリングでは本機能を有効にしないでください。本機能を使用する際はネットワーク設計を十分に検討して使用してください。
バージョン	1.08.02

使用例：リング ID 3 の分散マスター装置または分散スレーブ装置において、別リングから送信されてきた FDB フラッシュフレームを、異なるリングへ中継する機能を有効にする方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 3 transmit-fdb-flush retransmit enable
(config)#
```

5.13.16 mmrp-plus ring fdb-flush port

<table>
<tr><th colspan="2">mmrp-plus ring fdb-flush port</th></tr>
<tr><td>目的</td><td>MMRP-Plus リングで障害発生／復旧時に FDB エントリーを消去するポートを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。</td></tr>
<tr><td>Command</td><td>mmrp-plus ring ID [,|-] fdb-flush port PORTS
no mmrp-plus ring ID [,|-] fdb-flush port</td></tr>
<tr><td>Parameter</td><td>ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。
PORTS：障害発生／復旧時に FDB エントリーを消去するポートをすべて指定します。複数指定できます。</td></tr>
<tr><td>デフォルト</td><td>すべてのポートで FDB エントリーを消去する</td></tr>
<tr><td>モード</td><td>グローバル設定モード</td></tr>
<tr><td>特権レベル</td><td>レベル：12</td></tr>
<tr><td>ガイドライン</td><td>本コマンドを設定する場合は、対象 MMRP-Plus リングのリングポートを含めて設定してください。
ポートチャネルで FDB エントリーを消去する場合は、該当するポートチャネルのすべてのメンバーポートを指定してください。
本コマンドの設定によって、MMRP-Plus リングの障害発生および復旧時の FDB エントリーと ARP キャッシュエントリーの消去動作が変わります。デフォルト設定時と、本コマンドを MMRP-Plus ポートを含めて設定した場合の、それぞれのエントリーの消去対象になるポートを以下に示します。
<table>
<tr><th>設定</th><th>FDB エントリーの
消去対象ポート</th><th>ARP キャッシュエントリーの
消去対象ポート</th></tr>
<tr><td>デフォルト設定時</td><td>MMRP-Plus ポートを含むすべてのポート</td><td>MMRP-Plus ポートのみ</td></tr>
<tr><td>MMRP-Plus ポートを含めてポート指定時</td><td>MMRP-Plus ポートを含む指定ポート</td><td>MMRP-Plus ポートと指定ポート</td></tr>
</table>
設定済みの状態で本コマンドを新たに設定すると、上書き設定されます。そのため本コマンドを設定する際は、すべての対象ポート（MMRP-Plus ポートを含む）を指定して設定してください。</td></tr>
<tr><td>制限・注意</td><td>• 分散マスター構成の場合、分散マスター装置と分散スレーブ装置の間の「渡りポート」は当該 MMRP-Plus の MMRP-Plus ポートではないため、デフォルト設定では障害発生／復旧時に「渡りポート」に登録された ARP キャッシュエントリーは連動して消去されません。そのため、「渡りポート」に登録された ARP キャッシュエントリーも消去させたい場合は、本コマンドで明示的に指定して設定してください。</td></tr>
<tr><td>バージョン</td><td>1.08.02</td></tr>
</table>

使用例：リング ID 1 で障害発生／復旧時に FDB エントリーを消去するポートを、ポート 1/0/1～1/0/2、ポート 1/0/5、ポート 1/0/11 を指定して設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1 fdb-flush port 1/0/1-2,1/0/5,1/0/11
(config)#
```

5.13.17 mmrp-plus ring fdb-flush timer

mmrp-plus ring fdb-flush timer	
目的	FDB フラッシュタイマーを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] fdb-flush timer SECONDS no mmrp-plus ring ID [,|-] fdb-flush timer
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 SECONDS：FDB フラッシュタイマーを 0～10 秒の範囲で指定します。
デフォルト	1 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	FDB フラッシュタイマーは、MMRP-Plus によって MAC アドレステーブルがクリアされた後に、MAC アドレスの学習を停止する時間です。
制限・注意	• 本コマンドの設定値は、同一リング内のすべての装置で揃えてください。
バージョン	1.08.02

使用例：リング ID 2 の FDB フラッシュタイマーを 2 秒に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 2 fdb-flush timer 2
(config)#
```

5.13.18 mmrp-plus ring listening-timer

mmrp-plus ring listening-timer	
目的	リスニングタイマーを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] listening-timer SECONDS no mmrp-plus ring ID [,|-] listening-timer
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 SECONDS：リスニングタイマーを 1～86,400 秒の範囲で指定します。
デフォルト	10 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	リスニングタイマーは、MMRP-Plus リングポートの Listening 状態のタイムアウト時間です。
制限・注意	• 本コマンドの設定値は、同一リング内のすべての装置で揃えてください。
バージョン	1.08.02

使用例：リング ID 1 のリスニングタイマーを 30 秒に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1 listening-timer 30
(config)#
```

5.13.19 mmrp-plus ring hello-timeout

mmrp-plus ring hello-timeout	
目的	MMRP-Plus のハローフレームの受信タイムアウト時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] hello-timeout SECONDS no mmrp-plus ring ID [,|-] hello-timeout
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 SECONDS：MMRP-Plus ハローフレームの受信タイムアウト時間を 1～86,400 秒の範囲で指定します。
デフォルト	1 秒（実際の動作では、ハローフレームの受信停止を検出するとすぐに経路の切り替え動作が開始されます）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドで設定する時間は、MMRP-Plus のハローフレームの受信停止を検出してから、経路の切り替え動作を開始するまでの時間です。受信タイムアウト時間経過後、経路の切り替え動作が開始されます。 受信タイムアウト時間を変更する場合は、以下の設定をデフォルト値以下に設定してください。 • mmrp-plus switch polling-rate コマンド • mmrp-plus switch hello-interval コマンド
制限・注意	• 本コマンドの設定値は、同一リング内のすべての装置で揃えてください。 • MMRP-Plus のリングポートで LLDP 疑似リンクダウン機能（lldp err-disable コマンド）を併用する場合、リンクダウンを伴わない片方向通信障害が発生した際に MMRP-Plus がハロータイムアウトを検知して切り替わるよりも先に LLDP 疑似リンクダウン機能で障害を検知するように、本設定を「LLDPDU の情報保持時間」よりも大きく設定することを推奨します。 • 同様に、MMRP-Plus のリングポートが LACP モードのポートチャネルの場合は、リンクダウンを伴わない片方向通信障害が発生した際に MMRP-Plus がハロータイムアウトを検知して切り替わるよりも先に LACP モードのポートチャネルで障害を検知するように、本設定を「LACPDU の受信タイムアウト時間」よりも大きく設定することを推奨します。 • 受信タイムアウト時間は、実際の動作では、受信タイムアウト時間から 1 秒を引いた時間になります。受信タイムアウト時間を 1 秒に設定した場合は、MMRP-Plus のハローフレームの受信停止を検出するとすぐに経路の切り替え動作が開始されます。
バージョン	1.08.02

使用例：リング ID 1 の MMRP-Plus のハローフレームの受信タイムアウト時間を 10 秒に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1 hello-timeout 10
(config)#
```

5.13.20 mmrp-plus ring port-restart enable

mmrp-plus ring port-restart enable	
目的	ポートリスタート機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] port-restart enable no mmrp-plus ring ID [,|-] port-restart enable
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ポートリスタート機能は、分散マスター装置、分散スレーブ装置、シングルマスター構成のマスター装置で使用できます。 ポートリスタート機能は、非 MMRP-Plus スイッチを接続する場合に有効な機能です。基本的には「分散マスターポートと分散スレーブポートの間に、1 台の非 MMRP-Plus スイッチを接続して収容する構成」で使用します。 ポートリスタート機能を有効にすると、リング復旧時にマスター（スレーブ）ポートのリンクを強制的にリンクダウン（瞬断）し、対向スイッチの FDB エントリーを消去します。 ポートリスタート機能をマルチリングで有効にする場合は、MMRP-Plus 制御フレームの VLAN は、リングごとに異なる VLAN を指定することを推奨します。
制限・注意	• ポートリスタート機能はアウェア装置では使用できません。 • MMRP-Plus アウェア機能に対応したスイッチと接続する場合は、ポートリスタート機能は使用しないでください。 • ポートリスタート機能とアップリンクポート連携機能（mmrp-plus ring uplink port コマンド）は、同一リングでは併用できません。 • ポートリスタート機能を有効にしたリングポートでは、LLDP 疑似リンクダウン機能（lldp err-disable コマンド）は併用できません。 • 同一リングに属する装置のマスター/スレーブポートは、ポートリスタート機能（mmrp-plus ring port-restart enable コマンド）の設定値を同一にしてください。
バージョン	1.08.02

使用例：リング ID 2 でポートリスタート機能を有効にする方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 2 port-restart enable
(config)#
```

5.13.21 mmrp-plus ring port-restart forcedown-time

mmrp-plus ring port-restart forcedown-time	
目的	ポートリスタート機能によるリンク瞬断時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] port-restart forcedown-time VALUE no mmrp-plus ring ID [,|-] port-restart forcedown-time

mmrp-plus ring port-restart forcedown-time	
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 VALUE：リンク瞬断時間を 1～30（100 ミリ秒単位）の範囲で指定します。
デフォルト	5（500 ミリ秒）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• リンク瞬断時間が短いと対向スイッチの FDB がクリアされない場合が想定されます。その場合は、本設定のリンク瞬断時間を長く設定するようにしてください。
バージョン	1.08.02

使用例：リング ID 2 のポートリスタート機能のリンク瞬断時間を 1000 ミリ秒に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 2 port-restart forcedown-time 10
(config)#
```

5.13.22 mmrp-plus ring port-restart linkup-wait

mmrp-plus ring port-restart linkup-wait	
目的	ポートリスタート機能のリンク保護時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] port-restart linkup-wait VALUE no mmrp-plus ring ID [,|-] port-restart linkup-wait
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 VALUE：リンク保護時間を 50～600（100 ミリ秒単位）の範囲で指定します。
デフォルト	100（10 秒）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	リンク保護時間は、対向装置でリンクが復旧する前に意図しない MMRP-Plus の不要な切り替え/切り戻りを防止するためのものです。 リンク復旧時（ポートリスタート動作開始）からリンク保護時間が経過するまでの間、マスターポートおよびスレーブポートのリンク検知、MMRP-Plus ハローフレームの受信タイムアウト検知は停止します。
制限・注意	• 本コマンドの設定値は、同一リング内のすべての装置で揃えてください。 • リンク保護時間が短い場合、対向スイッチのリンクが確立せず、MMRP-Plus の不要な切り替え/切り戻りが生じることがあります。
バージョン	1.08.02

使用例：リング ID 2 のポートリスタート機能のリンク保護時間を 10 秒に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 2 port-restart linkup-wait 100
(config)#
```

5.13.23 mmrp-plus ring uplink port

mmrp-plus ring uplink port	
目的	分散マスター装置および分散スレーブ装置のアップリンクポート連携機能を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mmrp-plus ring ID [,|-] uplink port PORTS no mmrp-plus ring ID [,|-] uplink port
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。 PORTS：アップリンクポートに設定するポートを指定します。複数指定できます。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	アップリンクポート連携機能は分散マスター構成のリングでのみ有効な機能で、分散マスター装置、分散スレーブ装置で使用できます。 アップリンクポート連携機能は、アップリンクが全断となった場合でも装置がネットワークから孤立するのを防ぐために使用します。指定したアップリンクポートがすべてダウンした場合、指定したリング ID の分散マスター（分散スレーブ）ポートは Forwarding に遷移し、同時に Hello フレームの送信を停止し、対向の分散スレーブ（分散マスター）ポートも Forwarding に遷移させます。この状態でいずれかのアップリンクポートがリンクアップすると、分散マスター（分散スレーブ）ポートも復旧して Listening に遷移し、Hello フレームの送信を再開します。 アップリンクポートには、別リングのポートを指定することも可能です。 アップリンクポートに別リングのポートが設定されていて、かつその別リングで mmrp-plus ring revertive が設定されている場合、以下のように動作します。 • AEOS-NP2500 Ver. 1.10.01 より前のバージョンでは、アップリンクポートに指定した別リングのポートがリンクアップして Failure 状態に遷移すると、分散マスター（分散スレーブ）ポートは Listening 状態に遷移し復旧を開始します。 • AEOS-NP2500 Ver. 1.10.01 以降では、アップリンクポートに指定した別リングのポートがリンクアップして Failure 状態に遷移しても復旧を開始せず、別リングのポートが Listening 状態になると、分散マスター（分散スレーブ）ポートは Listening 状態に遷移し復旧を開始します。 ポートチャネルを直接指定することはできません。ポートチャネルへ設定する場合は、ポートチャネルのメンバーポートをすべて指定してください。
制限・注意	• アップリンクポート連携機能は、シングルマスター構成のマスター装置、またはアウェア装置では使用できません。 • アップリンクポート連携機能とポートリスタート機能（mmrp-plus ring port-restart enable コマンド）は、同一リングで併用できません。 • アップリンクポート連携機能とポートリダンダント機能は、同一インターフェースで併用できません。 • AEOS-NP2500 Ver. 1.10.01 以降では、以下の設定制限があります。 • 複数のリングで別の同一リングのポートをアップリンクポートに設定することはできません。 • ある 1 つのリングにおいて、複数の別リングのポートをアップリンクポートとして同時に設定することはできません。

mmrp-plus ring uplink port	
バージョン	1.08.02 1.10.01：復旧動作の仕様変更

使用例：リング ID 101 のアップリンクポートをポート 1/0/1～1/0/5 に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 101 uplink port 1/0/1-5
(config)#
```

5.13.24 show mmrp-plus configuration

show mmrp-plus configuration	
目的	MMRP-Plus の設定を表示します。
Command	show mmrp-plus configuration
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MMRP-Plus の設定を表示する方法を示します。

```
# show mmrp-plus configuration

MMRP-Plus Switch Configuration
        Status         : Enable ...(1)
        Hello interval : 100ms ...(2)
        Polling rate   : 1000ms ...(3)

MMRP-Plus Ring Configuration:
 RM: Ring Master, RA: Ring Aware, DM: Divided Master, DS: Divided Slave
 Vid : Hello VID
 Fdb : FDB Flush Timer
 Pr  : Port Restart (O: enable -: disable)
 Vg  : VLAN Group
 Re  : Revertive setting
 Ht  : Hello Timeout Timer
 Lis : Listening Timer
 P   : Port-Channel                                        (11)
(4)  (5)       (6)  (7)         (7)          (8)   (9)   (10)  (12)     (13)  (14)
ID   Name      Type Pt1         Pt2        | Vid   Fdb   Pr Vg Re       Ht    Lis
-------------------------------------------+-----------------------------------
1    R01-A     RA   1/0/1       1/0/2      | 4011  1     -  -  0        1     10
2    R01-1-M   RM   1/0/5(M)    1/0/6(S)   | 4012  1     -  1  60       1     10
3    TEST03    DM   P5                     | 4013  1     O  -  disable  1     10
4    Ring004   DS               1/0/12     | 4014  1     -  2  0        1     10
```

項番	説明
(1)	MMRP-Plus の有効(Enable)／無効(Disable)を表示します。
(2)	MMRP-Plus のハローフレームの送信間隔を表示します。
(3)	MMRP-Plus のハローフレームのポーリングレートを表示します。

項番	説明
(4)	MMRP-Plus のリング ID を表示します。
(5)	MMRP-Plus のリング名を表示します。リング名が 8 文字以上の場合は、先頭の 7 文字までが表示されます。
(6)	MMRP-Plus のリングの動作モードを表示します。 RM：シングルマスター RA：アウェア DM：分散マスター DS：分散スレーブ
(7)	ポート番号またはポートチャネル番号を表示します。番号の前に P が表示されている場合はポートチャネル番号です。 シングルマスター構成では、マスターポートに(M)、スレーブポートに(S)が付与されて表示されます。
(8)	MMRP-Plus 制御フレームの VLAN ID を表示します。
(9)	FDB フラッシュタイマーを表示します。
(10)	ポートリスタート機能の有効(O)／無効(-)を表示します。
(11)	関連付けられた VLAN グループ番号を表示します。
(12)	切り戻りタイマーを表示します。disable パラメーター指定時は disable と表示されます。
(13)	ハローフレームの受信タイムアウト時間を表示します。
(14)	リスニングタイマーを表示します。

5.13.25 show mmrp-plus configuration ring

show mmrp-plus configuration ring	
目的	MMRP-Plus のリングごとの設定を表示します。
Command	show mmrp-plus configuration ring ID [,|-]
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	VLAN グループ関連の項目(VLAN Group)は、マスター装置、分散マスター装置、分散スレーブ装置の場合に表示されます。 ポートリスタート機能の項目(Port-Restart)は、マスター装置、分散マスター装置、分散スレーブ装置の場合に表示されます。 FDB フラッシュフレーム送信／中継機能の項目(FDBFlush Transmit)は、分散マスター装置、分散スレーブ装置の場合に表示されます。 アップリンクポート連携機能の項目(Uplink)は、分散マスター装置、分散スレーブ装置の場合に表示されます。
制限・注意	-
バージョン	1.08.02

使用例：リング ID 1 のマスター装置の設定を表示する方法を示します。

```
# show mmrp-plus configuration ring 1
```

```
================================================================================
Ring ID             : 1 ...(1)
Ring name           : TEST-RING1 ...(2)
Type                : Ring Master ...(3)
Master Port         : 1/0/1 ...(4)
Slave Port          : 1/0/2 ...(4)
VLAN ID             : 4001 ...(5)
VLAN Group          : 2 ...(6)
  Master VID        : 1-19,21-29,31-39,41-4094 ...(7)
  Slave VID         : 20,30,40 ...(8)
Listening Time      : 10 s ...(9)
FDB Flush
  Timer             : 1 s ...(10)
  Port              : - ...(11)
Hello-timeout       : 1 s ...(12)
Revertive           : 0 s ...(13)
Port-Restart        : Disable ...(14)
  Forcedown Time    : 500 ms ...(15)
  Link Up Wait      : 10000 ms ...(16)
```

項番	説明
(1)	MMRP-Plus のリング ID を表示します。
(2)	MMRP-Plus のリング名を表示します。
(3)	MMRP-Plus のリングの動作モードを表示します。 Ring Master：シングルマスター Ring Aware：アウェア Divided Master：分散マスター Divided Slave：分散スレーブ
(4)	リングポートを表示します。リングポート種別により項目名称が以下のように変更されます。ポートチャネルの場合はポートチャネル番号とメンバーポートのポート番号が表示されます。 マスターポート(物理ポート)：Master Port スレーブポート(物理ポート)：Slave Port アウェアポート(物理ポート)：Aware Port マスターポート(ポートチャネル)：Master Port-Channel スレーブポート(ポートチャネル)：Slave Port-Channel アウェアポート(ポートチャネル)：Aware Port-Channel
(5)	MMRP-Plus 制御フレームの VLAN ID を表示します。
(6)	関連付けられた VLAN グループ番号を表示します。未指定時は Default と表示されます。
(7)	マスターVLAN を表示します。
(8)	スレーブ VLAN を表示します。
(9)	リスニングタイマーを表示します。
(10)	FDB フラッシュタイマーを表示します。
(11)	リングが切り替わる際に FDB エントリーを消去するポート番号を表示します。
(12)	ハローフレームの受信タイムアウト時間を表示します。
(13)	切り戻りタイマーを表示します。disable パラメーター指定時は Disable と表示されます。
(14)	ポートリスタート機能の有効(Enable)／無効(Disable)を表示します。
(15)	ポートリスタート機能のリンク瞬断時間を表示します。

項番	説明
(16)	ポートリスタート機能のリンク保護時間を表示します。

使用例：リング ID 2 のアウェア装置の設定を表示する方法を示します。

```
# show mmrp-plus configuration ring 2

================================================================================
Ring ID             : 2 ...(1)
Ring name           : TEST-RING2 ...(2)
Type                : Ring Aware ...(3)
Aware Port          : 1/0/3 ...(4)
Aware Port          : 1/0/4 ...(4)
VLAN ID             : 4002 ...(5)
Listening Time      : 10 s ...(6)
FDB Flush
  Timer             : 1 s ...(7)
  Port              : - ...(8)
Hello-timeout       : 1 s ...(9)
Revertive           : 0 s ...(10)
```

項番	説明
(1)	MMRP-Plus のリング ID を表示します。
(2)	MMRP-Plus のリング名を表示します。
(3)	MMRP-Plus のリングの動作モードを表示します。 Ring Master：シングルマスター Ring Aware：アウェア Divided Master：分散マスター Divided Slave：分散スレーブ
(4)	リングポートを表示します。リングポート種別により項目名称が以下のように変更されます。ポートチャネルの場合はポートチャネル番号とメンバーポートのポート番号が表示されます。 マスターポート(物理ポート)：Master Port スレーブポート(物理ポート)：Slave Port アウェアポート(物理ポート)：Aware Port マスターポート(ポートチャネル)：Master Port-Channel スレーブポート(ポートチャネル)：Slave Port-Channel アウェアポート(ポートチャネル)：Aware Port-Channel
(5)	MMRP-Plus 制御フレームの VLAN ID を表示します。
(6)	リスニングタイマーを表示します。
(7)	FDB フラッシュタイマーを表示します。
(8)	リングが切り替わる際に FDB エントリーを消去するポート番号を表示します。
(9)	ハローフレームの受信タイムアウト時間を表示します。
(10)	切り戻りタイマーを表示します。disable パラメーター指定時は Disable と表示されます。

使用例：リング ID 3 の分散マスター装置の設定を表示する方法を示します。

```
# show mmrp-plus configuration ring 3

================================================================================
```

```
Ring ID             : 3 ...(1)
Ring name           : TEST-RING3 ...(2)
Type                : Divided Master ...(3)
Master Port         : 1/0/5 ...(4)
VLAN ID             : 4003 ...(5)
VLAN Group          : 2 ...(6)
  Master VID        : 1-19,21-29,31-39,41-4094 ...(7)
  Slave VID         : 20,30,40 ...(8)
Listening Time      : 10 s ...(9)
FDB Flush
  Timer             : 1 s ...(10)
  Port              : - ...(11)
Hello-timeout       : 1 s ...(12)
Revertive           : 0 s ...(13)
Port-Restart        : Disable ...(14)
  Forcedown Time    : 500 ms ...(15)
  Link Up Wait      : 10000 ms ...(16)
FDBFlush Transmit
  Port              : - ...(17)
  Retransmit        : Disable ...(18)
Uplink
  Port              : 1/0/9-1/0/10 ...(19)
```

項番	説明
(1)	MMRP-Plus のリング ID を表示します。
(2)	MMRP-Plus のリング名を表示します。
(3)	MMRP-Plus のリングの動作モードを表示します。 Ring Master：シングルマスター Ring Aware：アウェア Divided Master：分散マスター Divided Slave：分散スレーブ
(4)	リングポートを表示します。リングポート種別により項目名称が以下のように変更されます。ポートチャネルの場合はポートチャネル番号とメンバーポートのポート番号が表示されます。 マスターポート(物理ポート)：Master Port スレーブポート(物理ポート)：Slave Port アウェアポート(物理ポート)：Aware Port マスターポート(ポートチャネル)：Master Port-Channel スレーブポート(ポートチャネル)：Slave Port-Channel アウェアポート(ポートチャネル)：Aware Port-Channel
(5)	MMRP-Plus 制御フレームの VLAN ID を表示します。
(6)	関連付けられた VLAN グループ番号を表示します。未指定時は Default と表示されます。
(7)	マスターVLAN を表示します。
(8)	スレーブ VLAN を表示します。
(9)	リスニングタイマーを表示します。
(10)	FDB フラッシュタイマーを表示します。
(11)	リングが切り替わる際に FDB エントリーを消去するポート番号を表示します。
(12)	ハローフレームの受信タイムアウト時間を表示します。
(13)	切り戻りタイマーを表示します。disable パラメーター指定時は Disable と表示されます。

項番	説明
(14)	ポートリスタート機能の有効(Enable)／無効(Disable)を表示します。
(15)	ポートリスタート機能のリンク瞬断時間を表示します。
(16)	ポートリスタート機能のリンク保護時間を表示します。
(17)	FDB フラッシュフレーム送信機能で指定した送信ポートを表示します。
(18)	FDB フラッシュフレーム中継機能の有効(Enable)／無効(Disable)を表示します。
(19)	アップリンクポート連携機能で指定したアップリンクポートを表示します。

5.13.26 show mmrp-plus vlangroup

show mmrp-plus vlangroup	
目的	VLAN グループのマスターVLAN、およびスレーブ VLAN を表示します。
Command	show mmrp-plus vlangroup [GROUP]
Parameter	GROUP (省略可能)：VLAN グループ番号を 1～8 の範囲で指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN グループ 8 のマスターVLAN、およびスレーブ VLAN を表示する方法を示します。

```
# show mmrp-plus vlangroup 8

VLAN Group Configuration: Group 8 ...(1)
  Master VID    : 1-4094 ...(2)
  Slave VID     : - ...(3)
```

項番	説明
(1)	VLAN グループ番号を表示します。
(2)	マスターVLAN を表示します。
(3)	スレーブ VLAN を表示します。

5.13.27 show mmrp-plus status

show mmrp-plus status	
目的	MMRP-Plus の動作状態を表示します。
Command	show mmrp-plus status
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MMRP-Plus の動作状態を表示する方法を示します。

```
# show mmrp-plus status

VLAN group  : Default ...(1)
  Master VLAN : 1-4094 ...(2)
  Slave VLAN  : - ...(3)
-------------------------------------------------------------------------------
 (4)         (5)    (6)           (7)              (8)              (9)
 Pt.         Ring   MMRP          Master VLAN      Slave VLAN       Ring name
 /Pt-C.      ID     Port Mode     Port Status      Port Status
-------------------------------------------------------------------------------
 1/0/1       1      Ring Aware    Forwarding       Forwarding       0123456789
 1/0/2       1      Ring Aware    Forwarding       Forwarding       0123456789
 1/0/5       3      Ring Master   Down             Down             r3
 1/0/6       3      Ring Slave    Down             Down             r3
 1/0/4       4      Div Master    Down             Down

VLAN group  : 2
  Master VLAN : 2-8,11-4094
  Slave VLAN  : 1,9-10
-------------------------------------------------------------------------------
 Pt.         Ring   MMRP          Master VLAN      Slave VLAN       Ring name
 /Pt-C.      ID     Port Mode     Port Status      Port Status
-------------------------------------------------------------------------------
 1/0/3       2      Div Slave     Down             Down
 P1          5      Div Slave     Down             Down
```

項番	説明
(1)	VLAN グループ番号を表示します。未指定時は Default と表示されます。
(2)	マスターVLAN を表示します。
(3)	スレーブ VLAN を表示します。
(4)	ポート番号またはポートチャネル番号を表示します。番号の前に P が表示されている場合はポートチャネル番号です。
(5)	MMRP-Plus のリング ID を表示します。
(6)	リングポートの動作モードを表示します。 Ring Master：マスターポート Ring Slave：スレーブポート Ring Aware：アウェアポート Div Master：分散マスターポート Div Slave：分散スレーブポート
(7)	対象リングポートのマスターVLAN に対する状態を表示します。 Blocking：ユーザーフレームの中継を抑止している状態 Forwarding：ユーザーフレームを中継している状態 Down：障害発生中ですべての通信不可 FailureUp：リング復旧待機状態（すべての通信不可） Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(8)	対象リングポートのスレーブ VLAN に対する状態を表示します。 Blocking：ユーザーフレームの中継を抑止している状態 Forwarding：ユーザーフレームを中継している状態 Down：障害発生中ですべての通信不可

項番	説明
	FailureUp：リング復旧待機状態（すべての通信不可） Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(9)	MMRP-Plus のリング名を表示します。リング名が 11 文字以上の場合は、先頭の 10 文字までが表示されます。

5.13.28 show mmrp-plus status port

show mmrp-plus status port	
目的	MMRP-Plus のポートごとの動作状態を表示します。
Command	show mmrp-plus status IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	アウェア装置では、本コマンドの Port Mode 項目は以下のように表示されます。 • Ring Aware Default：MMRP-Plus 有効後で MMRP-Plus ハローフレーム未受信状態の場合、または正常時に反対方向の MMRP-Plus ハローフレームを受信した場合。 • Ring Aware Master：スレーブポートからの MMRP-Plus ハローフレーム（HelloB1/HelloF1）を受信した場合。 • Ring Aware Slave：マスターポートからの MMRP-Plus ハローフレーム（HelloB2/HelloF2）を受信した場合。
制限・注意	-
バージョン	1.08.02

使用例：MMRP-Plus のポートチャネル 1 の動作状態を表示する方法を示します。

```
# show mmrp-plus status port-channel 1

================================================================================
Port-Channel 1 (Port 1/0/9-1/0/10) ...(1)
  Ring ID           : 5 ...(2)
  Ring Name         : ...(3)
  Port Mode         : Divided Slave ...(4)
  VLAN Group        : 2 ...(5)
    Master VLAN     : 2-8,11-4094 ...(6)
    Slave VLAN      : 1,9-10 ...(7)
  Link Status       : Down ...(8)
  MMRP-Plus Status  : Down ...(9)
    Master VLAN     : Down ...(10)
    Slave VLAN      : Down ...(11)
  Connection        : Broken ...(12)
--------------------------------------------------------------------
   (13)              (14)                      (15)
  Frame Type       Receive Frame Count     Transmit Frame Count
--------------------------------------------------------------------
  HelloB1                              0                        0
  HelloB2                              0                        -
  HelloF1                              0                        0
  HelloF2                              0                        -
  FDB Flush                            0                        1
```

```
  Link Down                0                0
  Link Up                  0                0
  Blocking                 0                0
  Forwarding               0                0
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。ポートチャネルの場合はポートチャネル番号とメンバーポートのポート番号が表示されます。
(2)	MMRP-Plus のリング ID を表示します。
(3)	MMRP-Plus のリング名を表示します。
(4)	リングポートの動作モードを表示します。 Ring Master：マスターポート Ring Slave：スレーブポート Ring Aware Default：デフォルト状態のアウェアポート Ring Aware Master：スレーブポート方向に接続されたアウェアポート Ring Aware Slave：マスターポート方向に接続されたアウェアポート Divided Master：分散マスターポート Divided Slave：分散スレーブポート
(5)	VLAN グループ番号を表示します。未指定時は Default と表示されます。
(6)	マスターVLAN を表示します。
(7)	スレーブ VLAN を表示します。
(8)	ポートのリンク状態を表示します。
(9)	リングポートの MMRP-Plus 状態を表示します。 ■ マスターポート、スレーブポート、分散マスターポート、分散スレーブポートの場合 Blocking：リング正常時 Forwarding：リング障害時 ■ アウェアポートの場合 Forwarding：リング正常時、リング障害時 ■ 共通 Down：対象リングポートがダウン状態 FailureUp：対象リングポートがダウン状態から復旧して、リング復旧待機状態 Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(10)	対象リングポートのマスターVLAN に対する状態を表示します。 Blocking：ユーザーフレームの中継を抑止している状態 Forwarding：ユーザーフレームを中継している状態 Down：障害発生中ですべての通信不可 FailureUp：リング復旧待機状態（すべての通信不可） Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(11)	対象リングポートのスレーブ VLAN に対する状態を表示します。 Blocking：ユーザーフレームの中継を抑止している状態 Forwarding：ユーザーフレームを中継している状態 Down：障害発生中ですべての通信不可 FailureUp：リング復旧待機状態（すべての通信不可）

項番	説明
	Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(12)	リングの接続状態を表示します。 Normal：正常状態（MMRP-Plus ハローフレーム受信中） Broken：障害発生中（MMRP-Plus ハローフレーム未受信） Abnormal：異常状態（正常時とは反対方向の MMRP-Plus ハローフレーム受信）
(13)	MMRP-Plus 制御フレームの種別を表示します。 HelloB1：Blocking 状態のスレーブが送信する MMRP-Plus ハローフレーム HelloB2：Blocking 状態のマスターが送信する MMRP-Plus ハローフレーム HelloF1：Forwarding 状態のスレーブが送信する MMRP-Plus ハローフレーム HelloF2：Forwarding 状態のマスターが送信する MMRP-Plus ハローフレーム FDB Flush：FDB エントリーのクリア要求を示す制御フレーム Link Down：リンクダウン検知を示す制御フレーム Link Up：リンクアップ検知を示す制御フレーム Blocking：Blocking 状態へ遷移時のマスター/スレーブが送信する制御フレーム
(14)	受信した MMRP-Plus 制御フレーム数を表示します。
(15)	送信した MMRP-Plus 制御フレーム数を表示します。

5.13.29 show mmrp-plus status ring

show mmrp-plus status ring	
目的	MMRP-Plus のリングごとの動作状態を表示します。
Command	show mmrp-plus status ring ID [,|-]
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	アウェア装置では、本コマンドの Port Mode 項目は以下のように表示されます。 • Ring Aware Default：MMRP-Plus 有効後で MMRP-Plus ハローフレーム未受信状態の場合、または正常時に反対方向の MMRP-Plus ハローフレームを受信した場合。 • Ring Aware Master：スレーブポートからの MMRP-Plus ハローフレーム（HelloB1/HelloF1）を受信した場合。 • Ring Aware Slave：マスターポートからの MMRP-Plus ハローフレーム（HelloB2/HelloF2）を受信した場合。
制限・注意	-
バージョン	1.08.02

使用例：MMRP-Plus のリング ID 1 の動作状態を表示する方法を示します。

```
# show mmrp-plus status ring 1

================================================================================
Port 1/0/1 ...(1)
  Ring ID           : 1 ...(2)
  Ring Name         : 01234567890123456789012345678912 ...(3)
  Port Mode         : Ring Aware Slave ...(4)
  VLAN Group        : Default ...(5)
    Master VLAN     : 1-4094 ...(6)
```

```
    Slave VLAN      : - ...(7)
  Link Status       : 1G/F ...(8)
  MMRP-Plus Status  : Forwarding ...(9)
    Master VLAN     : Forwarding ...(10)
    Slave VLAN      : Forwarding ...(11)
  Connection        : Normal ...(12)
-------------------------------------------------------------------
   (13)               (14)                      (15)
  Frame Type        Receive Frame Count     Transmit Frame Count
-------------------------------------------------------------------
  HelloB1                             0                        -
  HelloB2                           338                        -
  HelloF1                             0                        -
  HelloF2                            10                        -
  FDB Flush                           0                        0
  Link Down                           0                        0
  Link Up                             0                        0
  Blocking                            3                        0
  Forwarding                          0                        0
===================================================================================
Port 1/0/2
  Ring ID           : 1
  Ring Name         : 01234567890123456789012345678912
  Port Mode         : Ring Aware Master
  VLAN Group        : Default
    Master VLAN     : 1-4094
    Slave VLAN      : -
  Link Status       : 1G/F
  MMRP-Plus Status  : Forwarding
    Master VLAN     : Forwarding
    Slave VLAN      : Forwarding
  Connection        : Normal
-------------------------------------------------------------------
  Frame Type        Receive Frame Count     Transmit Frame Count
-------------------------------------------------------------------
  HelloB1                           339                        -
  HelloB2                             0                        -
  HelloF1                            10                        -
  HelloF2                             0                        -
  FDB Flush                           0                        0
  Link Down                           0                        0
  Link Up                             0                        0
  Blocking                            3                        0
  Forwarding                          0                        0
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。ポートチャネルの場合はポートチャネル番号とメンバーポートのポート番号が表示されます。
(2)	MMRP-Plus のリング ID を表示します。
(3)	MMRP-Plus のリング名を表示します。
(4)	リングポートの動作モードを表示します。 Ring Master：マスターポート Ring Slave：スレーブポート Ring Aware Default：デフォルト状態のアウェアポート Ring Aware Master：スレーブポート方向に接続されたアウェアポート Ring Aware Slave：マスターポート方向に接続されたアウェアポート Divided Master：分散マスターポート

項番	説明
	Divided Slave：分散スレーブポート
(5)	VLAN グループ番号を表示します。未指定時は Default と表示されます。
(6)	マスターVLAN を表示します。
(7)	スレーブ VLAN を表示します。
(8)	ポートのリンク状態を表示します。
(9)	リングポートの MMRP-Plus 状態を表示します。 ■ マスターポート、スレーブポート、分散マスターポート、分散スレーブポートの場合 Blocking：リング正常時 Forwarding：リング障害時 ■ アウェアポートの場合 Forwarding：リング正常時、リング障害時 ■ 共通 Down：対象リングポートがダウン状態 FailureUp：対象リングポートがダウン状態から復旧して、リング復旧待機状態 Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(10)	対象リングポートのマスターVLAN に対する状態を表示します。 Blocking：ユーザーフレームの中継を抑止している状態 Forwarding：ユーザーフレームを中継している状態 Down：障害発生中ですべての通信不可 FailureUp：リング復旧待機状態（すべての通信不可） Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(11)	対象リングポートのスレーブ VLAN に対する状態を表示します。 Blocking：ユーザーフレームの中継を抑止している状態 Forwarding：ユーザーフレームを中継している状態 Down：障害発生中ですべての通信不可 FailureUp：リング復旧待機状態（すべての通信不可） Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(12)	リングの接続状態を表示します。 Normal：正常状態（MMRP-Plus ハローフレーム受信中） Broken：障害発生中（MMRP-Plus ハローフレーム未受信） Abnormal：異常状態（正常時とは反対方向の MMRP-Plus ハローフレーム受信）
(13)	MMRP-Plus 制御フレームの種別を表示します。 HelloB1：Blocking 状態のスレーブが送信する MMRP-Plus ハローフレーム HelloB2：Blocking 状態のマスターが送信する MMRP-Plus ハローフレーム HelloF1：Forwarding 状態のスレーブが送信する MMRP-Plus ハローフレーム HelloF2：Forwarding 状態のマスターが送信する MMRP-Plus ハローフレーム FDB Flush：FDB エントリーのクリア要求を示す制御フレーム Link Down：リンクダウン検知を示す制御フレーム Link Up：リンクアップ検知を示す制御フレーム Blocking：Blocking 状態へ遷移時のマスター/スレーブが送信する制御フレーム
(14)	受信した MMRP-Plus 制御フレーム数を表示します。

項番	説明
(15)	送信した MMRP-Plus 制御フレーム数を表示します。

5.13.30 clear mmrp-plus failure ring

clear mmrp-plus failure ring	
目的	MMRP-Plus の手動切り戻りを実行します。
Command	clear mmrp-plus failure ring ID [,|-]
Parameter	ID：リング ID を 1～1000 の範囲で指定します。複数指定できます。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドを実行するとリング復旧処理が開始され、リング復旧待機状態(FailureUp)のリングポートは Listening 状態へ遷移します。 mmrp-plus ring revertive コマンドを使用して自動切り戻り機能を有効にしている場合に本コマンドを実行すると、切り戻りタイマーが期限切れになる前にリング復旧処理を開始できます。
制限・注意	-
バージョン	1.08.02

使用例：リング ID 1 の手動切り戻りを実行する方法を示します。

```
# clear mmrp-plus failure ring 1
#
```

5.13.31 debug mmrp

debug mmrp	
目的	MMRP-Plus のデバッグ機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	debug mmrp [event | hello | cpu | fdbflush] no debug mmrp [event | hello | cpu | fdbflush]
Parameter	有効にするデバッグ情報のカテゴリーを指定します。 • event（省略可能）：イベント関連 • hello（省略可能）：ハローフレーム関連 • cpu（省略可能）：CPU パケット関連 • fdbflush（省略可能）：FDB フラッシュ関連
デフォルト	無効
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	MMRP-Plus のデバッグ機能の有効／無効は、パラメーターをすべて省略したコマンド形式で実行します。
制限・注意	• 本コマンドはデバッグ目的の機能のため、運用環境では有効にしないでください。
バージョン	1.08.02

使用例：MMRP-Plus のイベント関連のデバッグ機能を有効にする方法を示します。

```
# debug mmrp
# debug mmrp event
#
```

5.14 スパニングツリープロトコルコマンド

スパニングツリープロトコル関連の設定コマンドは以下のとおりです。

- forward-bpdu global enable
- spanning-tree global state
- spanning-tree mode
- spanning-tree priority
- spanning-tree（timers）
- spanning-tree tx-hold-count
- spanning-tree nni-bpdu-address
- spanning-tree state
- spanning-tree cost
- spanning-tree guard root
- spanning-tree link-type
- spanning-tree portfast
- spanning-tree port-priority
- spanning-tree tcnfilter
- spanning-tree forward-bpdu
- spanning-tree mst configuration
- instance（MSTP）
- name（MSTP）
- revision（MSTP）
- spanning-tree mst priority
- spanning-tree mst hello-time
- spanning-tree mst max-hops
- spanning-tree mst cost
- spanning-tree mst port-priority
- snmp-server enable traps stp

スパニングツリープロトコル関連の show／操作コマンドは以下のとおりです。

- show spanning-tree
- show spanning-tree configuration interface
- show spanning-tree mst
- clear spanning-tree detected-protocols

5.14.1 forward-bpdu global enable

forward-bpdu global enable	
目的	装置全体で BPDU のハードウェア転送を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	forward-bpdu global enable no forward-bpdu global enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード

forward-bpdu global enable	
特権レベル	レベル：12
ガイドライン	本機能が有効の場合、受信した BPDU は各ポートの VLAN 設定に従ってハードウェア転送されます。 本機能を使用する場合は、spanning-tree mode コマンドはデフォルト設定のままで使用してください。また、BPDU のソフトウェア転送機能（spanning-tree forward-bpdu）も無効（デフォルト設定）のままで使用してください。
制限・注意	• スパニングツリープロトコルが有効の場合（spanning-tree global state enable）は、本機能を有効にできません。
バージョン	1.10.01

使用例：BPDU のハードウェア転送機能を有効にする方法を示します。

```
# configure terminal
(config)# forward-bpdu global enable
(config)#
```

5.14.2 spanning-tree global state

spanning-tree global state	
目的	スパニングツリープロトコルのグローバル設定を有効または無効にします。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree global state {enable | disable} no spanning-tree global state
Parameter	enable：グローバル設定を有効にする場合に指定します。 disable：グローバル設定を無効にする場合に指定します。
デフォルト	無効（spanning-tree global state disable）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• AEOS-NP2500 Ver. 1.13.01 以降では、STP/RSTP/MSTP/RPVST+機能と MMRP-Plus 機能との装置併用をサポートしました。なお、同一インターフェース（物理ポートまたはポートチャネル）では引き続き併用不可です。装置併用をする場合は、MMRP-Plus 機能のリングポート（物理ポートまたはポートチャネル）において、必ずスパニングツリープロトコルのインターフェースごとの設定を無効（spanning-tree state disable）にしてください。 • AEOS-NP2500 Ver. 1.13.01 より前のバージョンでは、STP/RSTP/MSTP/RPVST+機能と MMRP-Plus 機能は、同一装置で併用できません。 • STP/RSTP/MSTP/RPVST+機能と ERPS 機能は、同一装置で併用できません。 • STP/RSTP/MSTP/RPVST+機能は、同一インターフェースでループ検知機能（loop-detection action notify-only 設定時を除く）、ポートリダンダント機能、VLAN 変換機能と併用できません。 • BPDU ハードウェア転送機能が有効な場合（forward-bpdu global enable）は、本コマンドを有効にできません。
バージョン	1.08.02

spanning-tree global state	
	1.13.01：装置併用に関する仕様変更

使用例：スパニングツリープロトコルを有効にする方法を示します。

```
# configure terminal
(config)# spanning-tree global state enable
(config)#
```

5.14.3 spanning-tree mode

spanning-tree mode	
目的	スパニングツリープロトコルを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree mode {mstp | rstp | stp | rpvst+} no spanning-tree mode
Parameter	使用するスパニングツリープロトコルを以下のパラメーターで指定します。 • mstp：マルチプルスパニングツリープロトコル（MSTP） • rstp：ラピッドスパニングツリープロトコル（RSTP） • stp：スパニングツリープロトコル（IEEE 802.1D 準拠） • rpvst+：ラピッド Per-VLAN スパニングツリープロトコル（RPVST+）
デフォルト	RSTP
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	動作中と異なるスパニングツリープロトコルを指定して上書き設定した場合には、スパニングツリー機能がリスタートします。その結果、すべてのスパニングツリーポートの状態は一度ブロッキング状態に遷移します。 本コマンドで動作モードを rpvst+に設定している場合、通常の BPDU に加えて RPVST+で使用する BPDU も転送しなくなります。
制限・注意	• 本コマンドで動作モードを「stp, rstp, mstp」から「rpvst+」に変更する場合、または「rpvst+」から「stp, rstp, mstp」に変更する場合は、設定が反映されるのに時間がかかります。
バージョン	1.08.02

使用例：スパニングツリープロトコルの動作モードとして、RSTP を設定する方法を示します。

```
# configure terminal
(config)# spanning-tree mode rstp
(config)#
```

5.14.4 spanning-tree priority

spanning-tree priority	
目的	ブリッジ優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree priority PRIORITY no spanning-tree priority
Parameter	PRIORITY：ブリッジ優先度を 0～61,440 の範囲から 4096 の倍数で指定します。

spanning-tree priority	
デフォルト	32,768
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ブリッジ優先度は値が小さいほど、優先度は高くなります。 本コマンドは、以下のブリッジ優先度を設定する場合に使用できます。 • STP のブリッジ優先度 • RSTP のブリッジ優先度 • MSTP インスタンス 0 のブリッジ優先度 • VLAN 1 の RPVST+ブリッジ優先度
制限・注意	-
バージョン	1.08.02

使用例：ブリッジ優先度を 4096 に設定する方法を示します。

```
# configure terminal
(config)# spanning-tree priority 4096
(config)#
```

5.14.5 spanning-tree (timers)

spanning-tree (timers)	
目的	スパニングツリープロトコルの各種タイマーを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree {hello-time SECONDS | forward-time SECONDS | max-age SECONDS} no spanning-tree {hello-time | forward-time | max-age}
Parameter	hello-time SECONDS：ハロータイムを、1～2 秒の範囲で指定します。 forward-time SECONDS：フォワードディレイタイムを、4～30 秒の範囲で指定します。フォワードディレイタイムは、「最大エージタイム÷2＋1 秒」以上の値になるように設定してください。 max-age SECONDS：最大エージタイムを、6～40 秒の範囲で指定します。最大エージタイムは、「(フォワードディレイタイム－1 秒)×2」以下の値になるように設定してください。
デフォルト	ハロータイム：2 秒 フォワードディレイタイム：15 秒 最大エージタイム：20 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• MSTP のハロータイマーを設定する場合は、spanning-tree mst hello-time コマンドを使用します。
バージョン	1.08.02

使用例：スパニングツリープロトコルの各種タイマーを設定する方法を示します。

```
# configure terminal
(config)# spanning-tree hello-time 1
(config)# spanning-tree forward-time 16
(config)# spanning-tree max-age 21
(config)#
```

5.14.6 spanning-tree tx-hold-count

spanning-tree tx-hold-count	
目的	1 秒間の中断前に送信を許可する BPDU の上限の数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree tx-hold-count VALUE no spanning-tree tx-hold-count
Parameter	VALUE：一時停止までに送信できる BPDU の最大数を、1～10 の範囲で指定します。
デフォルト	6
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	送信する hold BPDU の数を指定するコマンドです。ポート上の BPDU の送信は、カウンターによって制御されます。カウンターは、BPDU の送信ごとにインクリメントされ、1 秒に 1 回デクリメントされます。カウンターが transmit hold のカウント値に達すると、送信は 1 秒間中断します。
制限・注意	-
バージョン	1.08.02

使用例：transmit hold のカウント値を、5 に設定する方法を示します。

```
# configure terminal
(config)# spanning-tree tx-hold-count 5
(config)#
```

5.14.7 spanning-tree nni-bpdu-address

spanning-tree nni-bpdu-address	
目的	サービスプロバイダーサイトで、BPDU の宛先アドレスを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree nni-bpdu-address {dot1d | dot1ad} no spanning-tree nni-bpdu-address
Parameter	dot1d：BPDU の宛先アドレスとして、Customer Bridge Group Address（01-80-C2-00-00-00）を使用する場合に指定します。 dot1ad：BPDU の宛先アドレスとして、Provider Bridge Group Address（01-80-C2-00-00-08）を使用する場合に指定します。
デフォルト	Customer Bridge Group Address
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	通常、BPDU の宛先アドレスとして Customer Bridge Group Address が使用されます。

spanning-tree nni-bpdu-address	
	すべてのスパニングツリープロトコルに有効です。
制限・注意	• サービスプロバイダーサイトで NNI ポートとして動作する、VLAN トランクポート上だけで機能します。
バージョン	1.08.02

使用例：VLAN トランクポート上で、dot1ad アドレスを BPDU の宛先アドレスとして設定する方法を示します。

```
# configure terminal
(config)# spanning-tree nni-bpdu-address dot1ad
(config)#
```

5.14.8 spanning-tree state

spanning-tree state	
目的	スパニングツリープロトコルのインターフェースごとの設定を有効または無効にします。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree state {enable | disable} no spanning-tree state
Parameter	enable：インターフェースごとの設定を有効にする場合に指定します。 disable：インターフェースごとの設定を無効にする場合に指定します。
デフォルト	有効（spanning-tree state enable）
モード	インターフェース設定モード（port, range, port-channel）
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 インターフェースのスパニングツリープロトコルが無効な場合、スパニングツリープロトコルエンジンは、インターフェースによって受信された BPDU を送信しません。また、処理も行いません。
制限・注意	• AEOS-NP2500 Ver. 1.13.01 以降では、STP/RSTP/MSTP/RPVST+機能と MMRP-Plus 機能との装置併用をサポートしました。なお、同一インターフェース（物理ポートまたはポートチャネル）では引き続き併用不可です。装置併用をする場合は、MMRP-Plus 機能のリングポート（物理ポートまたはポートチャネル）において、必ずスパニングツリープロトコルのインターフェースごとの設定を無効（spanning-tree state disable）にしてください。 • AEOS-NP2500 Ver. 1.13.01 より前のバージョンでは、STP/RSTP/MSTP/RPVST+機能と MMRP-Plus 機能は、同一装置で併用できません。 • STP/RSTP/MSTP/RPVST+機能と ERPS 機能は、同一装置で併用できません。 • STP/RSTP/MSTP/RPVST+機能は、同一インターフェースでループ検知機能（loop-detection action notify-only 設定時を除く）、ポートリダンダント機能、VLAN 変換機能と併用できません。
バージョン	1.08.02 1.13.01：装置併用に関する仕様変更

使用例：ポート 1/0/1 で、スパニングツリープロトコルを有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# spanning-tree state enable
(config-if-port)#
```

5.14.9 spanning-tree cost

spanning-tree cost	
目的	パスコストを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree cost COST no spanning-tree cost
Parameter	COST：パスコストを、1～200000000 の範囲で指定します。
デフォルト	インターフェースの帯域幅設定から算出
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本コマンドは、以下のパスコストを設定する場合に使用できます。 • STP 使用時のパスコスト • RSTP 使用時のパスコスト • VLAN 1 の RPVST+使用時のパスコスト
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/7 のパスコストを、20000 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/7
(config-if-port)# spanning-tree cost 20000
(config-if-port)#
```

5.14.10 spanning-tree guard root

spanning-tree guard root	
目的	ルートガードを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	spanning-tree guard root no spanning-tree guard root
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 ルートガードは、意図しないスイッチが接続されてルートブリッジが変更されることを防止するために、ルートガード有効ポートで現在のルートブリッジよりも優先度の

spanning-tree guard root	
	高い BPDU を受信しても、それがルートブリッジになることを防ぎます。この状態の間は、対象ポートは alternate ポート（blocking 状態）になります。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 でルートガードを有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# spanning-tree guard root
(config-if-port)#
```

5.14.11 spanning-tree link-type

spanning-tree link-type	
目的	インターフェースのリンクタイプを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree link-type {point-to-point | shared} no spanning-tree link-type
Parameter	point-to-point：インターフェースのリンクタイプを、ポイントツーポイントリンクに設定する場合に指定します。 shared：インターフェースのリンクタイプを、シェアードリンクに設定する場合に指定します。
デフォルト	デュプレックス設定を基に自動設定
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 デフォルト設定の場合、全二重ポートはポイントツーポイントリンクになります。半二重ポートはシェアードリンクになります。 本設定は、すべてのスパニングツリープロトコルに有効です。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/7 のリンクタイプを、ポイントツーポイントリンクに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/7
(config-if-port)# spanning-tree link-type point-to-point
(config-if-port)#
```

5.14.12 spanning-tree portfast

spanning-tree portfast	
目的	Port Fast モードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree portfast {disable | edge | network}

spanning-tree portfast	
	no spanning-tree portfast
Parameter	disable：Port Fast モードを無効にする場合に指定します。 edge：Port Fast モードをエッジポートにする場合に指定します。 network：Port Fast モードをネットワークポートにする場合に指定します。
デフォルト	network
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 Port Fast モードを無効に設定した場合は、対象ポートは常に Non-port-fast 状態になります。Non-port-fast 状態でリンクアップ後に BPDU を受信しない場合は、転送遅延時間（最大エージタイム、フォワードディレイタイム）が経過するとフォワーディング状態に遷移します。リンクアップ後に BPDU を受信した場合は、それぞれのスパニングツリープロトコルに従って動作します。 Port Fast モードをエッジポートに設定した場合は、リンクアップ後すぐに port-fast 状態になり、転送遅延時間を待つことなくフォワーディング状態に遷移します。なお、port-fast 状態のポートでも、その後 BPDU を受信すると Non-port-fast 状態に変更されます。 Port Fast モードをネットワークポートに設定した場合は、リンクアップ後 3 秒間は Non-port-fast 状態にとどまります。その間に BPDU を受信しない場合は port-fast 状態になり、転送遅延時間を待つことなくフォワーディング状態に遷移します。3 秒の待機中に BPDU を受信した場合は、それぞれのスパニングツリープロトコルに従って動作します。
制限・注意	• スパニングツリープロトコルが STP の場合、デフォルト設定（spanning-tree portfast network）でも Port Fast モードを無効に設定した場合と同等の動作になります。 • 予期しないトポロジーループや、データパケットループが発生する恐れがあるため、spanning-tree portfast の実行には注意が必要です。
バージョン	1.08.02

使用例：ポート 1/0/7 で、Port Fast モードをエッジポートに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/7
(config-if-port)# spanning-tree portfast edge
(config-if-port)#
```

5.14.13 spanning-tree port-priority

spanning-tree port-priority	
目的	ポート優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree port-priority PRIORITY no spanning-tree port-priority
Parameter	PRIORITY：ポート優先度を、0～240 の範囲から 16 の倍数で指定します。

spanning-tree port-priority	
デフォルト	128
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本コマンドは、以下のポート優先度を設定する場合に使用できます。 • STP のポート優先度 • RSTP のポート優先度 • MSTP インスタンス 0 のポート優先度 • VLAN 1 の RPVST+のポート優先度
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/7 のポート優先度を、32 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/7
(config-if-port)# spanning-tree port-priority 32
(config-if-port)#
```

5.14.14 spanning-tree tcnfilter

spanning-tree tcnfilter	
目的	特定のインターフェースで、トポロジー変更通知（TCN）のフィルタリングを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	spanning-tree tcnfilter no spanning-tree tcnfilter
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 インターフェースに TCN フィルターモードを設定する場合、受信する TC イベントは無視されます。 TCN フィルターモードの設定は、すべてのスパニングツリープロトコルに有効です。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/7 で、TCN フィルタリングを設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/7
(config-if-port)# spanning-tree tcnfilter
(config-if-port)#
```

5.14.15 spanning-tree forward-bpdu

spanning-tree forward-bpdu	
目的	BPDU のソフトウェア転送を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	spanning-tree forward-bpdu no spanning-tree forward-bpdu
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード (interface port-channel コマンド) で設定してください。 装置はデフォルトでは受信した BPDU を転送しませんが、本機能を有効にすると BPDU をソフトウェア転送します。 spanning-tree mode rpvst+に設定されている場合、通常の BPDU に加えて RPVST+で使用する BPDU も転送しなくなりますが、本機能を有効にすると RPVST+で使用する BPDU もソフトウェア転送します。
制限・注意	• 本機能によるソフトウェア転送では、転送先ポートがタグなしフレームとして送信する VLAN 設定 (トンネルポートを除く) の場合でも、タグ付きフレームの BPDU として送信します。そのため、送信ポートの VLAN 設定どおりに転送したい場合は、BPDU のハードウェア転送機能 (forward-bpdu global enable) を使用してください。 • 装置として転送可能な最大レートは 64Kbps です。
バージョン	1.08.02

使用例：BPDU の転送を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# spanning-tree forward-bpdu
(config-if-port)#
```

5.14.16 spanning-tree mst configuration

spanning-tree mst configuration	
目的	MSTP コンフィグレーションモードに遷移します。遷移後のプロンプトは (config-mst)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	spanning-tree mst configuration no spanning-tree mst configuration
Parameter	なし
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを no 形式で実行すると、以下の設定が削除されます。 • instance (MSTP)

spanning-tree mst configuration	
	• name（MSTP） • revision（MSTP） • spanning-tree mst priority（MSTP インスタンス 0 の設定は除く） • spanning-tree mst cost（MSTP インスタンス 0 の設定は除く） • spanning-tree mst port-priority（MSTP インスタンス 0 の設定は除く）
制限・注意	-
バージョン	1.08.02

使用例：MSTP コンフィグレーションモードに遷移する方法を示します。

```
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)#
```

5.14.17 instance（MSTP）

instance（MSTP）	
目的	1 つの VLAN、または複数の VLAN を MSTP インスタンスにマッピングします。インスタンスを削除する場合は、VLAN を指定しないで no instance コマンドを使用します。VLAN をデフォルトのインスタンス（CIST）へ戻す場合は、VLAN を指定して no instance コマンドを使用します。
Command	instance INSTANCE-ID vlans VLAN-ID [,|-] no instance INSTANCE-ID [vlans VLAN-ID [,|-]]
Parameter	INSTANCE-ID：指定した VLAN をマッピングする MSTP インスタンス番号を、1～16 の範囲で指定します。 vlans VLAN-ID：指定したインスタンスへ VLAN をマッピングする場合、またはインスタンスから VLAN を削除する場合に、VLAN ID を 1～4094 の範囲で指定します。複数指定できます。
デフォルト	なし
モード	MSTP コンフィグレーションモード
特権レベル	レベル：12
ガイドライン	マッピングされてない VLAN は、CIST インスタンスへマッピングされます。VLAN をインスタンスへマッピングするときに、インスタンスが存在しない場合は、インスタンスが自動的に出力されます。インスタンスのすべての VLAN が削除されると、インスタンスも自動的に削除されます。
制限・注意	-
バージョン	1.08.02

使用例：範囲指定した VLAN を、インスタンス 2 へマッピングする方法を示します。

```
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)# instance 2 vlans 1-100
(config-mst)#
```

5.14.18 name（MSTP）

name (MSTP)	
目的	MSTP 領域の名前を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	name NAME no name NAME
Parameter	NAME：リージョン名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	装置の MAC アドレス
モード	MSTP コンフィグレーションモード
特権レベル	レベル：12
ガイドライン	同じ VLAN マッピングとコンフィグレーションバージョンの複数の装置は、MSTP 領域名が異なる場合、異なる MSTP 領域に属するとみなされます。
制限・注意	-
バージョン	1.08.02

使用例：MSTP コンフィグレーション名を「MName」に設定する方法を示します。

```
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)# name MName
(config-mst)#
```

5.14.19 revision（MSTP）

revision (MSTP)	
目的	MSTP コンフィグレーションのリビジョン番号を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	revision VALUE no revision
Parameter	VALUE：MSTP コンフィグレーションのリビジョン番号を、0～65535 の範囲で指定します。
デフォルト	0
モード	MSTP コンフィグレーションモード
特権レベル	レベル：12
ガイドライン	同じコンフィグレーションで異なるバージョンが設定された 2 つのイーサネット装置は、2 つの異なる領域に属するとみなされます。
制限・注意	-
バージョン	1.08.02

使用例：MSTP コンフィグレーションのリビジョン番号を、2 に設定する方法を示します。

```
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)# revision 2
(config-mst)#
```

5.14.20 spanning-tree mst priority

spanning-tree mst priority	
目的	指定した MSTP インスタンスのブリッジ優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree mst INSTANCE-ID priority PRIORITY no spanning-tree mst INSTANCE-ID priority
Parameter	INSTANCE-ID：MSTP インスタンス番号を、0～16 の範囲で指定します。 PRIORITY：ブリッジ優先度を 0～61,440 の範囲から 4096 の倍数で指定します。
デフォルト	32,768
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ブリッジ優先度は値が小さいほど、優先度は高くなります。 本コマンドを MSTP インスタンス 0 を指定して実施した場合は、構成情報では MSTP インスタンス指定の無いコマンド形式(spanning-tree priority PRIORITY)で表示されます。
制限・注意	• 本コマンドを設定する前に、instance (MSTP)コマンドで対象の MSTP インスタンスを設定してください。
バージョン	1.08.02

使用例：MSTP インスタンス 2 のブリッジ優先度を 4096 に設定する方法を示します。

```
# configure terminal
(config)# spanning-tree mst 2 priority 4096
(config)#
```

5.14.21 spanning-tree mst hello-time

spanning-tree mst hello-time	
目的	MSTP で使用される 1 ポートあたりのハロータイムを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree mst hello-time SECONDS no spanning-tree mst hello-time
Parameter	SECONDS：指定されたポートが各設定メッセージを定期的に送信する間隔（ハロータイム）を、1～2 秒の範囲で指定します。
デフォルト	2
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。
制限・注意	• MSTP ハロータイムは、MSTP だけで有効です。
バージョン	1.08.02

使用例：ポート 1/0/1 のポートハロータイムを、1 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
```

```
(config-if-port)# spanning-tree mst hello-time 1
(config-if-port)#
```

5.14.22 spanning-tree mst max-hops

spanning-tree mst max-hops	
目的	MSTP の最大ホップ数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree mst max-hops VALUE no spanning-tree mst max-hops
Parameter	VALUE：MSTP の最大ホップ数を、6～40 ホップの範囲で指定します。
デフォルト	20 ホップ
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：MSTP の最大ホップ数を設定する方法を示します。

```
# configure terminal
(config)# spanning-tree mst max-hops 19
(config)#
```

5.14.23 spanning-tree mst cost

spanning-tree mst cost	
目的	指定した MSTP インスタンスのパスコストを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree mst INSTANCE-ID cost COST no spanning-tree mst INSTANCE-ID cost
Parameter	INSTANCE-ID：MSTP インスタンス番号を、0～16 の範囲で指定します。 COST：パスコストを、1～200000000 の範囲で指定します。
デフォルト	インターフェースの帯域幅設定から算出
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。
制限・注意	• 本コマンドを設定する前に、instance (MSTP)コマンドで対象の MSTP インスタンスを設定してください。
バージョン	1.08.02

使用例：ポート 1/0/1 の MSTP インスタンス 2 のパスコストを、50 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# spanning-tree mst 2 cost 50
(config-if-port)#
```

5.14.24 spanning-tree mst port-priority

spanning-tree mst port-priority	
目的	指定した MSTP インスタンスのポート優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree mst INSTANCE-ID port-priority PRIORITY no spanning-tree mst INSTANCE-ID port-priority
Parameter	INSTANCE-ID：MSTP インスタンス番号を、0～16 の範囲で指定します。 PRIORITY：ポート優先度を、0～240 の範囲から 16 の倍数で指定します。
デフォルト	128
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本コマンドを MSTP インスタンス 0 を指定して実施した場合は、構成情報では MSTP インスタンス指定の無いコマンド形式(spanning-tree port-priority PRIORITY)で表示されます。
制限・注意	• 本コマンドを設定する前に、instance (MSTP)コマンドで対象の MSTP インスタンスを設定してください。
バージョン	1.08.02

使用例：ポート 1/0/1 の MSTP インスタンス 2 のポート優先度を、32 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# spanning-tree mst 2 port-priority 32
(config-if-port)#
```

5.14.25 snmp-server enable traps stp

snmp-server enable traps stp	
目的	スパニングツリープロトコル機能の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps stp [new-root] [topology-chg] no snmp-server enable traps stp [new-root] [topology-chg]
Parameter	new-root（省略可能）：新ルートブリッジ通知を有効にする場合に指定します。 topology-chg（省略可能）：トポロジー変更通知を有効にする場合に指定します。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	パラメーターを指定しない場合は、すべてのパラメーターが対象になります。 本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。
制限・注意	-

snmp-server enable traps stp	
バージョン	1.08.02

使用例：スパニングツリープロトコル機能の SNMP トラップを有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps stp
(config)#
```

5.14.26 show spanning-tree

show spanning-tree	
目的	STP または RSTP の動作状況を表示します。
Command	show spanning-tree [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• STP または RSTP 以外のモードで動作中の場合は、本コマンドを実行してもエラーメッセージが表示されます。 • interface パラメーターを使用してリンクダウン状態のインターフェースを指定しても、何も表示されません。
バージョン	1.08.02

使用例：STP または RSTP の動作状況を表示する方法を示します。

```
# show spanning-tree

 Spanning Tree: Enabled ...(1)
 Protocol Mode: RSTP ...(2)
 Tx-hold-count: 6 ...(3)
 NNI BPDU Address: dot1d(01-80-C2-00-00-00) ...(4)
 Root ID Priority: 8192 ...(5)
         Address: 00-40-66-B4-96-B5 ...(6)
         (7)                (8)              (9)
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Bridge ID Priority: 32768 (priority 32768  sys-id-ext 0) ...(10)
         Address: FC-6D-D1-00-4C-9C ...(11)
         (12)               (13)             (14)
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Topology Changes Count: 1 ...(15)
 (16)             (17)       (18)       (19)       (20)      (21)    (22)
                                                    Priority Link
 Interface        Role       State      Cost       .Port#    Type    Edge
 ---------------- ---------- ---------- ---------- --------- ------ ---------
 Port1/0/1        designated forwarding 20000      128.1     p2p     non-edge
 Port1/0/2        designated forwarding 20000      128.2     p2p     non-edge
 Port1/0/11       root       forwarding 20000      128.11    p2p     non-edge
```

項番	説明
(1)	STP または RSTP の有効(Enabled)／無効(Disabled)を表示します。

項番	説明
(2)	スパニングツリープロトコルを表示します。 RSTP：ラピッドスパニングツリープロトコル STP compatible：スパニングツリープロトコル
(3)	転送保留カウント値を表示します。
(4)	BPDU の宛先 MAC アドレスを表示します。
(5)	ルートブリッジの優先度を表示します。
(6)	ルートブリッジの MAC アドレスを表示します。
(7)	ルートブリッジのハロータイムを表示します。
(8)	ルートブリッジの最大エージタイムを表示します。
(9)	ルートブリッジのフォワードディレイタイムを表示します。
(10)	自装置の優先度を表示します。
(11)	自装置の MAC アドレスを表示します。
(12)	自装置のハロータイムを表示します。
(13)	自装置の最大エージタイムを表示します。
(14)	自装置のフォワードディレイタイムを表示します。
(15)	スパニングツリープロトコルのトポロジーが変更された回数を表示します。
(16)	ポート番号またはポートチャネル番号を表示します。
(17)	ポートの役割を表示します。 root：ルートポート designated：指定ポート alternate：代替ポート backup：バックアップポート disabled：無効ポート
(18)	ポートのステータスを表示します。 forwarding：フォワーディング状態 blocking：ブロッキング状態（ディスカーディング状態） learning：ラーニング状態 disabled：無効状態
(19)	ポートのパスコストを表示します。
(20)	ポート ID（ポート優先度＋ポート番号(ifindex)）を表示します。
(21)	ポートのリンクタイプの動作状況を表示します。 p2p：ポイントツーポイントリンク shared：シェアードリンク
(22)	Port Fast モードの動作状況を表示します。 edge：エッジポート non-edge：無効ポート

5.14.27 show spanning-tree configuration interface

show spanning-tree configuration interface	
目的	スパニングツリープロトコルのインターフェース関連の設定を表示します。

show spanning-tree configuration interface	
Command	show spanning-tree configuration interface [IF-ID [,|-]]
Parameter	IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 のスパニングツリープロトコル設定を表示する方法を示します。

```
# show spanning-tree configuration interface port 1/0/1

Port1/0/1 ...(1)
 Spanning tree state: Enabled ...(2)
 Port path cost: 0 ...(3)
 Port priority: 128 ...(4)
 Port Identifier: 128.1 ...(5)
 Link type: auto ...(6)
 Port fast: auto ...(7)
 Hello time: 2 seconds ...(8)
 Guard root: Disabled ...(9)
 TCN filter: Disabled ...(10)
 Bpdu forward: Disabled ...(11)
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	ポートのスパニングツリープロトコルの有効(Enabled)／無効(Disabled)を表示します。
(3)	ポートのパスコストを表示します。
(4)	ポート優先度を表示します。
(5)	ポート ID（ポート優先度＋ポート番号(ifindex)）を表示します。
(6)	ポートのリンクタイプの設定を表示します。デフォルトの自動判別設定の場合、全二重ポートはポイントツーポイントリンク、半二重ポートはシェアードリンクと判別されます。 auto：自動判別設定 p2p：手動設定（ポイントツーポイントリンク） shared：手動設定（シェアードリンク）
(7)	Port Fast モードの設定を表示します。 auto：ネットワークポート edge：エッジポート none-edge：無効ポート
(8)	MSTP で使用するポートごとのハロータイムを表示します。動作モードが MSTP の場合のみ表示されます。
(9)	ルートガードの有効(Enabled)／無効(Disabled)を表示します。
(10)	トポロジー変更通知(TCN)のフィルタリング機能の有効(Enabled)／無効(Disabled)を表示

項番	説明
	します。
(11)	BPDU のソフトウェア転送の有効(Enabled)／無効(Disabled)を表示します。

5.14.28 show spanning-tree mst

show spanning-tree mst	
目的	MSTP の情報を表示します。
Command	**show spanning-tree mst** [**configuration** [**digest**]] **show spanning-tree mst** [**instance** INSTANCE-ID [,|-]] [**interface** IF-ID [,|-]] [**detail**]
Parameter	configuration（省略可能）：MSTP インスタンスに割り当てられた VLAN を表示する場合に指定します。 digest（省略可能）：MSTP リージョンの MD5 ダイジェストを表示する場合に指定します。 instance INSTANCE-ID（省略可能）：MSTP 情報を表示する MSTP インスタンス番号を、0～16 の範囲で指定します。複数指定できます。 interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定 detail（省略可能）：詳細情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定の MSTP インスタンスを指定しない場合は、MSTP が有効なすべての MSTP インスタンスの情報が表示されます。 MSTP とプライベート VLAN を併用していて、プライマリーVLAN とセカンダリーVLAN が異なる MSTP インスタンスにマッピングされている場合には、show spanning-tree mst configuration コマンドで警告メッセージが表示されます。
制限・注意	• MSTP 以外のモードで動作中の場合は、本コマンドを実行してもエラーメッセージが表示されます。 • interface パラメーターを使用してリンクダウン状態のインターフェースを指定しても、何も表示されません。
バージョン	1.08.02

使用例：MSTP 情報を表示する方法を示します。

```
# show spanning-tree mst
 (1)                    (2)
 Spanning tree: Enabled,protocol: MSTP
 NNI BPDU Address: dot1d(01-80-C2-00-00-00) ...(3)
 Number of MST instances: 2 ...(4)
     (5)     (6)
 >>>>MST00  vlans mapped : 1-9,20-4094
 (7)                                  (8)
 Bridge Address: FC-6D-D1-00-4C-9C, Priority: 32768 (32768 sysid 0)
 (9)                                              (10)
 Designated Root Address: 00-40-66-B4-96-B5, Priority: 4096 (4096 sysid 0)
 CIST  External Root Cost : 0 ...(11)
```

```
 (12)                                                (13)
Regional Root Bridge Address: 00-40-66-B4-96-B5, Priority: 4096 (4096 sysid 0)
CIST  Internal Root Cost : 20000 ... (14)
 (15)                                          (16)
Designated Bridge Address: 00-40-66-B4-96-B5, Priority: 4096 (4096 sysid 0)
Topology Changes Count: 4 ... (17)
 (18)            (19)        (20)        (21)       (22)      (23)    (24)
                                                    Priority Link
Interface       Role        State       Cost       .Port#    Type    Edge
--------------- ----------- ----------- ---------- -------- ------ --------
Port1/0/1       designated forwarding 20000      128.1     p2p     edge
Port1/0/2       designated forwarding 20000      128.2     p2p     edge
Port1/0/12      root       forwarding 20000      128.12    p2p     non-edge

>>>>MST01  vlans mapped : 10-19
Bridge Address: FC-6D-D1-00-4C-9C, Priority: 32769 (32768 sysid 1)
 (25)                                          (26)
Regional Root Address: 00-40-66-B4-96-B5, Priority: 8193 (8192 sysid 1)
MSTI  Internal Root Cost : 20000 ... (27)
Designated Bridge Address: 00-40-66-B4-96-B5, Priority: 8193 (8192 sysid 1)
Topology Changes Count: 4

                                                    Priority Link
Interface       Role        State       Cost       .Port#    Type    Edge
--------------- ----------- ----------- ---------- -------- ------ --------
Port1/0/1       designated forwarding 20000      128.1     p2p     edge
Port1/0/2       disabled   disabled   20000      128.2     p2p     edge
Port1/0/12      root       forwarding 20000      128.12    p2p     non-edge
```

項番	説明
(1)	MSTP の有効(Enabled)／無効(Disabled)を表示します。
(2)	スパニングツリープロトコルを表示します。
(3)	BPDU の宛先 MAC アドレスを表示します。
(4)	MSTP インスタンス数を表示します。
(5)	MSTP インスタンス番号を表示します。
(6)	MSTP インスタンスに割り当てられている VLAN を表示します。
(7)	自装置の MAC アドレスを表示します。
(8)	自装置の優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。
(9)	CIST ルートの MAC アドレスを表示します。
(10)	CIST ルートの優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。
(11)	CIST 外部ルートパスコストを表示します。
(12)	CIST リージョナルルートの MAC アドレスを表示します。
(13)	CIST リージョナルルートの優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。
(14)	CIST 内部ルートパスコストを表示します。
(15)	ルートポートで受信した BPDU の送信元装置の MAC アドレスを表示します。自装置がルートブリッジの場合は自装置の MAC アドレスを表示します。
(16)	ルートポートで受信した BPDU の送信元装置の優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。自装置がルートブリッジの場合は自装置の優先度を表示します。
(17)	スパニングツリープロトコルのトポロジーが変更された回数を表示します。

項番	説明
(18)	ポート番号またはポートチャネル番号を表示します。
(19)	ポートの役割を表示します。 root：ルートポート designated：指定ポート alternate：代替ポート backup：バックアップポート disabled：無効ポート master：MSTI マスターポート
(20)	ポートのステータスを表示します。 forwarding：フォワーディング状態 blocking：ブロッキング状態（ディスカーディング状態） learning：ラーニング状態 disabled：無効状態
(21)	ポートのパスコストを表示します。
(22)	ポート ID（ポート優先度＋ポート番号(ifindex)）を表示します。
(23)	ポートのリンクタイプの動作状況を表示します。 p2p：ポイントツーポイントリンク shared：シェアードリンク
(24)	Port Fast モードの動作状況を表示します。 edge：エッジポート non-edge：無効ポート
(25)	MSTI リージョナルルートの MAC アドレスを表示します。
(26)	MSTI リージョナルルートの優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。
(27)	MSTI リージョナルルートまでのパスコストを表示します。

使用例：ポート 1/0/12 の MSTP 情報を表示する方法を示します。

```
# show spanning-tree mst interface port 1/0/12

Port1/0/12 ...(1)
 (2)                          (3)
 Configured link type: auto, operation status: point-to-point
 (4)                                  (5)
 Configured fast-forwarding: auto, operation status: non-edge
 Bpdu statistic counter: sent: 29, received: 404 ...(6)
 (7)       (8)         (9)         (10)       (11)
                                               Priority
 Instance Role        State       Cost       .Port#
 -------- ----        -----       ------     ---------
 MST00    root        forwarding 20000      128.12

 MST01    root        forwarding 20000      128.12
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	ポートのリンクタイプの設定を表示します。デフォルトの自動判別設定の場合、全二重ポー

項番	説明
	トはポイントツーポイントリンク、半二重ポートはシェアードリンクと判別されます。 auto：自動判別設定 p2p：手動設定（ポイントツーポイントリンク） shared：手動設定（シェアードリンク）
(3)	ポートのリンクタイプの動作状況を表示します。 point-to-point：ポイントツーポイントリンク shared：シェアードリンク
(4)	Port Fast モードの設定を表示します。 auto：ネットワークポート edge：エッジポート non-edge：無効ポート
(5)	Port Fast モードの動作状況を表示します。 edge：エッジポート non-edge：無効ポート
(6)	BPDU の送受信数を表示します。
(7)	MSTP インスタンス番号を表示します。
(8)	ポートの役割を表示します。 root：ルートポート designated：指定ポート alternate：代替ポート backup：バックアップポート disabled：無効ポート master：MSTI マスターポート
(9)	ポートのステータスを表示します。 forwarding：フォワーディング状態 blocking：ブロッキング状態（ディスカーディング状態） learning：ラーニング状態 disabled：無効状態
(10)	ポートのパスコストを表示します。
(11)	ポート ID（ポート優先度＋ポート番号(ifindex)）を表示します。

使用例：ポート 1/0/12 の MSTP 情報を、詳細モードで表示する方法を示します。

```
# show spanning-tree mst interface port 1/0/12 detail

Port1/0/12 ...(1)
 (2)                          (3)
 Configured link type: auto, operation status: point-to-point
 (4)                                  (5)
 Configured fast-forwarding: auto, operation status: non-edge
 Bpdu statistic counter: sent: 29, received: 408 ...(6)
      (7)                  (8)
 >>>>MST instance: 00,  vlans mapped : 1-9,20-4094
 Port state: forwarding ...(9)
 Port role: root ...(10)
              (11)             (12)            (13)
 Port info : port ID 128.12, priority: 128, cost: 20000
 (14)                                          (15)
```

```
Designated root address: 00-40-66-B4-96-B5, priority: 4096
 (16)                                    (17)
Regional Root address: 00-40-66-B4-96-B5, priority: 4096
 (18)                                              (19)          (20)
Designated bridge address: 00-40-66-B4-96-B5, priority: 4096, port id: 128.49

>>>>MST instance: 01,  vlans mapped : 10-19
Port state: forwarding
Port role: root
Port info : port ID 128.12, priority: 128, cost: 20000
 (21)                                          (22)
Designated root address: 00-40-66-B4-96-B5, priority: 8193
 (23)                                              (24)          (25)
Designated bridge address: 00-40-66-B4-96-B5, priority: 8193, port id: 128.49
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	ポートのリンクタイプの設定を表示します。デフォルトの自動判別設定の場合、全二重ポートはポイントツーポイントリンク、半二重ポートはシェアードリンクと判別されます。 auto：自動判別設定 p2p：手動設定（ポイントツーポイントリンク） shared：手動設定（シェアードリンク）
(3)	ポートのリンクタイプの動作状況を表示します。 point-to-point：ポイントツーポイントリンク shared：シェアードリンク
(4)	Port Fast モードの設定を表示します。 auto：ネットワークポート edge：エッジポート non-edge：無効ポート
(5)	Port Fast モードの動作状況を表示します。 edge：エッジポート non-edge：無効ポート
(6)	BPDU の送受信数を表示します。
(7)	MSTP インスタンス番号を表示します。
(8)	MSTP インスタンスに割り当てられている VLAN を表示します。
(9)	ポートのステータスを表示します。 forwarding：フォワーディング状態 blocking：ブロッキング状態（ディスカーディング状態） learning：ラーニング状態 disabled：無効状態
(10)	ポートの役割を表示します。 root：ルートポート designated：指定ポート alternate：代替ポート backup：バックアップポート disabled：無効ポート master：MSTI マスターポート

項番	説明
(11)	ポート ID (ポート優先度 + ポート番号(ifindex)) を表示します。
(12)	ポート優先度を表示します。
(13)	ポートのパスコストを表示します。
(14)	CIST ルートの MAC アドレスを表示します。
(15)	CIST ルートの優先度を表示します。
(16)	CIST リージョナルルートの MAC アドレスを表示します。
(17)	CIST リージョナルルートの優先度を表示します。
(18)	対象リンクで CIST リージョナルルートに一番近い装置の MAC アドレスを表示します。
(19)	対象リンクで CIST リージョナルルートに一番近い装置の優先度を表示します。
(20)	対象リンクで CIST リージョナルルートに一番近い装置のポート ID（ポート優先度 + ポート番号(ifindex)) を表示します。
(21)	MSTI リージョナルルートの MAC アドレスを表示します。
(22)	MSTI リージョナルルートの優先度を表示します。
(23)	対象リンクで MSTI リージョナルルートに一番近い装置の MAC アドレスを表示します。
(24)	対象リンクで MSTI リージョナルルートに一番近い装置の優先度を表示します。
(25)	対象リンクで MSTI リージョナルルートに一番近い装置のポート ID（ポート優先度 + ポート番号(ifindex)) を表示します。

使用例：MSTP インスタンスマッピングコンフィグレーションを表示する方法を示します。

```
# show spanning-tree mst configuration

 Name      : TEST ...(1)
 (2)           (3)
 Revision : 1,Instances configured: 2
 (4)           (5)
 Instance    Vlans
 --------    ------------------------------------------------------------------
      0      1-9,20-4094
      1      10-19
```

項番	説明
(1)	リージョン名を表示します。
(2)	リビジョン番号を表示します。
(3)	MSTP インスタンス数を表示します。
(4)	MSTP インスタンス番号を表示します。
(5)	MSTP インスタンスに割り当てられている VLAN を表示します。

使用例：スパニングツリーMSTP コンフィグレーションダイジェストを表示する方法を示します。

```
# show spanning-tree mst configuration digest

 Name      : TEST ...(1)
 (2)           (3)
 Revision : 1,Instances configured: 2
 Digest    : 8D0D3583ABF2D8F6F4CD1141B77F53D7 ...(4)
```

項番	説明
(1)	リージョン名を表示します。
(2)	リビジョン番号を表示します。
(3)	MSTP インスタンス数を表示します。
(4)	MSTP リージョンの MD5 ダイジェストを表示します。

5.14.29 clear spanning-tree detected-protocols

clear spanning-tree detected-protocols	
目的	指定したインターフェースのプロトコルマイグレーションを再試行します。
Command	clear spanning-tree detected-protocols {all | interface IF-ID}
Parameter	all：すべてのポートに検知動作を行わせます。 interface IF-ID：検知動作を行わせるインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドを使用すると、ポートのプロトコルマイグレーション状態を強制的に SEND_RSTP 状態に遷移させます。この動作は、特定の LAN 上のすべてのレガシーブリッジが削除されたかどうかをテストするために使用できます。LAN 上に STP ブリッジが存在しない場合、指定したモード（RSTP または MSTP）でポートが動作します。STP ブリッジが存在する場合は、ポートは STP で動作します。
制限・注意	-
バージョン	1.08.02

使用例：すべてのポートでプロトコルマイグレーションを再試行させる方法を示します。

```
# clear spanning-tree detected-protocols all
Clear spanning-tree detected-protocols? (y/n) [n]  y
```

5.15 RPVST+コマンド

RPVST+（ラピッド Per-VLAN スパニングツリープラス）関連の設定コマンドは以下のとおりです。

- spanning-tree vlan
- spanning-tree vlan priority
- spanning-tree vlan (timers)
- spanning-tree vlan cost
- spanning-tree vlan port-priority

RPVST+（ラピッド Per-VLAN スパニングツリープラス）関連の show コマンドは以下のとおりです。

- show spanning-tree vlan
- show spanning-tree vlan interface

5.15.1 spanning-tree vlan

spanning-tree vlan	
目的	指定した VLAN の RPVST+を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	spanning-tree vlan VLAN-ID no spanning-tree vlan VLAN-ID
Parameter	VLAN-ID：RPVST+を有効にする VLAN ID を、1～4094 の範囲で指定します。
デフォルト	VLAN 1 のみ有効（無効に変更不可）、その他の VLAN は無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを no 形式で実行すると、対象 VLAN の以下の設定も削除されます。 • spanning-tree vlan priority • spanning-tree vlan (timers) • spanning-tree vlan cost • spanning-tree vlan port-priority
制限・注意	• サポートする VLAN 数は、装置全体で最大 200 個です。 • AEOS-NP2500 Ver. 1.13.01 以降では、STP/RSTP/MSTP/RPVST+機能と MMRP-Plus 機能との装置併用をサポートしました。なお、同一インターフェース（物理ポートまたはポートチャネル）では引き続き併用不可です。装置併用をする場合は、MMRP-Plus 機能のリングポート（物理ポートまたはポートチャネル）において、必ずスパニングツリープロトコルのインターフェースごとの設定を無効（spanning-tree state disable）にしてください。 • AEOS-NP2500 Ver. 1.13.01 より前のバージョンでは、STP/RSTP/MSTP/RPVST+機能と MMRP-Plus 機能は、同一装置で併用できません。 • STP/RSTP/MSTP/RPVST+機能と ERPS 機能は、同一装置で併用できません。 • STP/RSTP/MSTP/RPVST+機能は、同一インターフェースでループ検知機能（loop-detection action notify-only 設定時を除く）、ポートリダンダント機能、VLAN 変換機能と併用できません。 • PVST+との相互接続は未サポートです。 • 他のレイヤー2 機能、およびレイヤー3 機能（スタック機能を含む）によって CPU

<table>
<tr><th colspan="2">spanning-tree vlan</th></tr>
<tr><td></td><td>が過負荷となった場合、RPVST+パケットの処理が遅れることがあります。
• CPU が過負荷とならない RPVST+の送受信 VLAN×ポート数の目安は、最大で 600 個です。この数を超えると、トラフィックの損失やネットワークトポロジーの変更が発生する場合があります。以下の表を参考に、上限値を超えないようにポート数や VLAN 数を設定してください。なお、ポートの RPVST+機能は、デフォルトで有効設定になっていますので、使用しないポートは spanning-tree state disable コマンドにて無効に変更してください。
<table>
<tr><th>VLAN 数</th><th>各ポートの役割(Role)</th><th>ポート数</th></tr>
<tr><td rowspan="2">200</td><td>Root Port, Alternate Port, Backup Port</td><td>3</td></tr>
<tr><td>Designated Port</td><td>3</td></tr>
<tr><td rowspan="2">100</td><td>Root Port, Alternate Port, Backup Port</td><td>6</td></tr>
<tr><td>Designated Port</td><td>6</td></tr>
<tr><td rowspan="2">50</td><td>Root Port, Alternate Port, Backup Port</td><td>12</td></tr>
<tr><td>Designated Port</td><td>12</td></tr>
</table>
• 併用する機能や本コマンドで設定する VLAN 数が増加すると CPU 負荷により収束時間が 3 秒以上かかることがあります。</td></tr>
<tr><td>バージョン</td><td>1.08.02
1.13.01：装置併用に関する仕様変更</td></tr>
</table>

使用例：VLAN 10 の RPVST+を有効にする方法を示します。

```
# configure terminal
(config)# spanning-tree vlan 10
(config)#
```

5.15.2 spanning-tree vlan priority

spanning-tree vlan priority	
目的	指定した VLAN の RPVST+のブリッジ優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree vlan VLAN-ID priority PRIORITY no spanning-tree vlan VLAN-ID priority
Parameter	VLAN-ID：VLAN ID を、1～4094 の範囲で指定します。 PRIORITY：ブリッジ優先度を 0～61,440 の範囲から 4096 の倍数で指定します。
デフォルト	32,768
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ブリッジ優先度は値が小さいほど、優先度は高くなります。 本コマンドを VLAN 1 を指定して実施した場合は、構成情報では VLAN ID 指定の無いコマンド形式(spanning-tree priority PRIORITY)で表示されます。
制限・注意	• 本コマンドを設定する前に、spanning-tree vlan コマンドで対象 VLAN の RPVST+を有効にしてください。
バージョン	1.08.02

使用例：VLAN 10 の RPVST+のブリッジ優先度を 4096 に設定する方法を示します。

```
# configure terminal
(config)# spanning-tree vlan 10 priority 4096
(config)#
```

5.15.3 spanning-tree vlan (timers)

spanning-tree vlan (timers)	
目的	指定した VLAN の RPVST+の各種タイマーを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree vlan VLAN-ID {hello-time SECONDS | forward-time SECONDS | max-age SECONDS} no spanning-tree vlan VLAN-ID {hello-time | forward-time | max-age}
Parameter	VLAN-ID：VLAN ID を、1～4094 の範囲で指定します。 hello-time SECONDS：ハロータイムを、1～2 秒の範囲で指定します。 forward-time SECONDS：フォワードディレイタイムを、4～30 秒の範囲で指定します。フォワードディレイタイムは、「最大エージタイム÷2＋1 秒」以上の値になるように設定してください。 max-age SECONDS：最大エージタイムを、6～40 秒の範囲で指定します。最大エージタイムは、「(フォワードディレイタイム－1 秒)×2」以下の値になるように設定してください。
デフォルト	ハロータイム：2 秒 フォワードディレイタイム：15 秒 最大エージタイム：20 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを VLAN 1 を指定して実施した場合は、構成情報ではそれぞれ VLAN ID 指定の無い以下のコマンド形式で表示されます。 • ハロータイム設定：spanning-tree hello-time SECONDS • フォワードディレイタイム設定：spanning-tree forward-time SECONDS • 最大エージタイム設定：spanning-tree max-age SECONDS
制限・注意	• 本コマンドを設定する前に、spanning-tree vlan コマンドで対象 VLAN の RPVST+を有効にしてください。
バージョン	1.08.02

使用例：VLAN 10 の RPVST+の各種タイマーを設定する方法を示します。

```
# configure terminal
(config)# spanning-tree vlan 10 hello-time 1
(config)# spanning-tree vlan 10 forward-time 16
(config)# spanning-tree vlan 10 max-age 21
(config)#
```

5.15.4 spanning-tree vlan cost

spanning-tree vlan cost	
目的	指定した VLAN の RPVST+のパスコストを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。

spanning-tree vlan cost	
Command	spanning-tree vlan VLAN-ID cost COST no spanning-tree vlan VLAN-ID cost
Parameter	VLAN-ID：VLAN ID を、1～4094 の範囲で指定します。 COST：RPVST+のパスコストを、1～200000000 の範囲で指定します。
デフォルト	インターフェースの帯域幅設定から算出
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本コマンドを VLAN 1 を指定して実施した場合は、構成情報では VLAN ID 指定の無いコマンド形式(spanning-tree cost COST)で表示されます。
制限・注意	• 本コマンドを設定する前に、spanning-tree vlan コマンドで対象 VLAN の RPVST+を有効にしてください。 • 本コマンドをポートチャネルで設定する場合は、先にポートチャネルのメンバーポートを設定してから本コマンドを設定してください。メンバーポート未設定のポートチャネルで本コマンドを設定すると、コマンドは実行できますが、構成情報に表示されない制限があります。メンバーポートを設定すると表示されます。
バージョン	1.08.02

使用例：ポート 1/0/2 の VLAN 10 の RPVST+パスコストを、2000 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/2
(config-if-port)# spanning-tree vlan 10 cost 2000
(config-if-port)#
```

5.15.5 spanning-tree vlan port-priority

spanning-tree vlan port-priority	
目的	指定した VLAN の RPVST+のポート優先度を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	spanning-tree vlan VLAN-ID port-priority PRIORITY no spanning-tree vlan VLAN-ID port-priority
Parameter	VLAN-ID：VLAN ID を、1～4094 の範囲で指定します。 PRIORITY：RPVST+のポート優先度を、0～240 の範囲で指定します。
デフォルト	128
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本コマンドを VLAN 1 を指定して実施した場合は、構成情報では VLAN ID 指定の無いコマンド形式(spanning-tree port-priority PRIORITY)で表示されます。
制限・注意	• 本コマンドを設定する前に、spanning-tree vlan コマンドで対象 VLAN の RPVST+を有効にしてください。

spanning-tree vlan port-priority	
	• 本コマンドをポートチャネルで設定する場合は、先にポートチャネルのメンバーポートを設定してから本コマンドを設定してください。メンバーポート未設定のポートチャネルで本コマンドを設定すると、コマンドは実行できますが、構成情報に表示されない制限があります。メンバーポートを設定すると表示されます。
バージョン	1.08.02

使用例：ポート 1/0/2 の VLAN 10 の RPVST+ポート優先度を、32 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/2
(config-if-port)# spanning-tree vlan 10 port-priority 32
(config-if-port)#
```

5.15.6 show spanning-tree vlan

show spanning-tree vlan	
目的	指定した VLAN の RPVST+の動作状況を表示します。
Command	show spanning-tree vlan [VLAN-ID]
Parameter	VLAN-ID（省略可能）：RPVST+の動作状況を表示する VLAN ID を、1～4094 の範囲で指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定の VLAN を指定しない場合は、RPVST+が有効なすべての VLAN の情報が表示されます。
制限・注意	• RPVST+以外のモードで動作中の場合は、本コマンドを実行してもエラーメッセージが表示されます。
バージョン	1.08.02

使用例：VLAN 10 の RPVST+の動作状況を表示する方法を示します。

```
# show spanning-tree vlan 10

VLAN10 ...(1)
 Spanning tree enabled protocol RPVST+ ...(2)
 Root ID Priority: 32778 ...(3)
         Address: FC-6D-D1-F2-82-1F ...(4)
         This bridge is the root. ...(5)
         (6)                (7)              (8)
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Bridge ID Priority: 32778 (priority 32768  sys-id-ext 10) ...(9)
         Address: FC-6D-D1-F2-82-1F ...(10)
         (11)               (12)             (13)
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Topology Changes Count: 1 ...(14)
 (15)             (16)       (17)       (18)       (19)      (20)    (21)
                                                   Priority Link
 Interface        Role       State      Cost       .Port#   Type    Edge
 ---------------- ---------- ---------- ---------- -------- ------ --------
 Port1/0/1        designated forwarding 20000      128.1    p2p     non-edge
 Port1/0/2        designated forwarding 20000      128.2    p2p     non-edge
```

項番	説明
(1)	VLAN ID を表示します。
(2)	有効になっているスパニングツリープロトコルを表示します。
(3)	ルートブリッジの優先度を表示します。
(4)	ルートブリッジの MAC アドレスを表示します。
(5)	自装置がルートブリッジの場合に表示されます。
(6)	ルートブリッジのハロータイムを表示します。
(7)	ルートブリッジの最大エージタイムを表示します。
(8)	ルートブリッジのフォワードディレイタイムを表示します。
(9)	自装置の優先度（対象 VLAN のブリッジ優先度と VLAN ID）を表示します。
(10)	自装置の MAC アドレスを表示します。
(11)	自装置のハロータイムを表示します。
(12)	自装置の最大エージタイムを表示します。
(13)	自装置のフォワードディレイタイムを表示します。
(14)	RPVST+のトポロジーが変更された回数を表示します。
(15)	ポート番号またはポートチャネル番号を表示します。
(16)	ポートの役割を表示します。 root：ルートポート designated：指定ポート alternate：代替ポート backup：バックアップポート disabled：無効ポート
(17)	ポートのステータスを表示します。 forwarding：フォワーディング状態 blocking：ブロッキング状態（ディスカーディング状態） learning：ラーニング状態 disabled：無効状態
(18)	ポートのパスコストを表示します。
(19)	ポート ID（ポート優先度＋ポート番号(ifindex)）を表示します。
(20)	ポートのリンクタイプの動作状況を表示します。 p2p：ポイントツーポイントリンク shared：シェアードリンク
(21)	Port Fast モードの動作状況を表示します。 edge：エッジポート non-edge：無効ポート

5.15.7 show spanning-tree vlan interface

show spanning-tree vlan interface	
目的	指定した VLAN のインターフェース関連の RPVST+詳細情報を表示します。
Command	show spanning-tree vlan VLAN-ID interface IF-ID [,|-]
Parameter	VLAN-ID：インターフェース関連の RPVST+詳細情報を表示する VLAN ID を、1～

show spanning-tree vlan interface	
	4094 の範囲で指定します。 IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• RPVST+以外のモードで動作中の場合は、本コマンドを実行してもエラーメッセージが表示されます。 • リンクダウン状態のインターフェースを指定しても、何も表示されません。
バージョン	1.08.02

使用例：VLAN 10 のポート 1/0/1 の RPVST+詳細情報を表示する方法を示します。

```
# show spanning-tree vlan 10 interface port 1/0/1
(1)           (2)
Port1/0/1  of VLAN10
 (3)                    (4)
 Port role: designated, Port state: learning
 (5)                    (6)                  (7)
 Port path cost: 20000, Port priority: 128, Port Identifier: 128.1
 (8)                                  (9)
 Designated root bridge priority: 32768, address: FC-6D-D1-F2-82-1F
 (10)                                (11)
 Designated bridge priority: 32768, address: FC-6D-D1-F2-82-1F
 (12)                        (13)
 Designated port id: 128.1, designated path cost: 0
 (14)                         (15)
 Configured link type: auto, operation status: p2p
 (16)                                (17)
 Configured fast-forwarding: auto, operation status: non-edge
 BPDU: sent: 33, received: 0 ...(18)
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	VLAN ID を表示します。
(3)	ポートの役割を表示します。 root：ルートポート designated：指定ポート alternate：代替ポート backup：バックアップポート disabled：無効ポート
(4)	ポートのステータスを表示します。 forwarding：フォワーディング状態 blocking：ブロッキング状態（ディスカーディング状態） learning：ラーニング状態 disabled：無効状態
(5)	ポートのパスコストを表示します。

項番	説明
(6)	ポート優先度を表示します。
(7)	ポート ID (ポート優先度 + ポート番号(ifindex)) を表示します。
(8)	ルートブリッジの優先度を表示します。
(9)	ルートブリッジの MAC アドレスを表示します。
(10)	対象リンクでルートブリッジに一番近い装置の優先度を表示します。
(11)	対象リンクでルートブリッジに一番近い装置の MAC アドレスを表示します。
(12)	対象リンクでルートブリッジに一番近い装置のポート ID (ポート優先度 + ポート番号(ifindex)) を表示します。
(13)	対象リンクでルートブリッジに一番近い装置からルートブリッジまでのパスコストを表示します。
(14)	ポートのリンクタイプの設定を表示します。デフォルトの自動判別設定の場合、全二重ポートはポイントツーポイントリンク、半二重ポートはシェアードリンクと判別されます。 auto：自動判別設定 point-to-point：手動設定 (ポイントツーポイントリンク) shared：手動設定 (シェアードリンク)
(15)	ポートのリンクタイプの動作状況を表示します。 p2p：ポイントツーポイントリンク shared：シェアードリンク
(16)	Port Fast モードの設定を表示します。 auto：ネットワークポート edge：エッジポート non-edge：無効ポート
(17)	Port Fast モードの動作状況を表示します。 edge：エッジポート non-edge：無効ポート
(18)	BPDU の送受信数を表示します。

5.16 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（中継パス制限）関連の設定コマンドは以下のとおりです。

- traffic-segmentation forward

トラフィックセグメンテーション（中継パス制限）関連の show コマンドは以下のとおりです。

- show traffic-segmentation forward

5.16.1 traffic-segmentation forward

traffic-segmentation forward	
目的	受信したフレームの転送を許可するインターフェース（転送ドメイン）を設定します。 設定を削除する場合は、no 形式のコマンドを使用します。
Command	traffic-segmentation forward interface IF-ID [,|-] no traffic-segmentation forward interface IF-ID [,|-]
Parameter	interface IF-ID：転送を許可する宛先インターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • range port：物理ポートの範囲指定
デフォルト	なし（転送ドメインは未設定）
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 転送ドメインを設定した場合、設定したインターフェースで受信したフレームの転送先は、転送ドメインで指定した宛先インターフェースに制限されます。 転送ドメインが未設定の場合は、中継パス制限による転送先インターフェースの制限は行われません。 本コマンドが設定済みの状態で再度設定を実施した場合は、差分の宛先インターフェースが追加されます。 転送を許可する宛先インターフェースとしてポートチャネルを指定する場合は、そのポートチャネルのすべてのメンバーポートを指定してください。なお、宛先インターフェースとしてポートチャネルのメンバーポートを 1 つでも指定して設定した場合は、残りのメンバーポートも自動的に設定されます。同様に、宛先インターフェースとしてポートチャネルのメンバーポートを 1 つでも指定して削除した場合は、残りのメンバーポートも自動的に削除されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で受信したフレームの転送を許可するインターフェース（転送ドメイン）を、ポート 1/0/1～1/0/6 に制限する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# traffic-segmentation forward interface range port 1/0/1-6
(config-if-port)#
```

5.16.2 show traffic-segmentation forward

show traffic-segmentation forward	
目的	受信したフレームの転送を許可するインターフェース（転送ドメイン）を表示します。
Command	show traffic-segmentation forward [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定 • range port：物理ポートの範囲指定 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：転送ドメインを設定したすべてのインターフェースの設定を表示する方法を示します。

```
# show traffic-segmentation forward
(1)                (2)
Interface          Forwarding Domain
---------------    ------------------------------------------------------------
Port1/0/1          Port1/0/2-1/0/5,1/0/11-1/0/12
Port-channel40     Port1/0/6-1/0/12

Total Entries: 2
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	受信したフレームの転送を許可するインターフェース（転送ドメイン）を表示します。

5.17 VLAN コマンド

VLAN 関連の設定コマンドは以下のとおりです。

- vlan
- name（VLAN）
- switchport mode
- switchport access vlan
- switchport trunk allowed vlan
- switchport trunk native vlan
- switchport hybrid allowed vlan
- switchport hybrid native vlan
- protocol-vlan profile
- protocol-vlan profile（Interface）
- acceptable-frame
- ingress-checking

VLAN 関連の show コマンドは以下のとおりです。

- show vlan
- show vlan interface
- show protocol-vlan

5.17.1 vlan

vlan	
目的	VLAN を設定します。また、VLAN 設定モードに遷移します。遷移後のプロンプトは (config-vlan)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	vlan VLAN-ID [,|-] no vlan VLAN-ID [,|-]
Parameter	VLAN-ID：VLAN ID を 1～4094 の範囲で指定します。複数指定できます。
デフォルト	VLAN 1 がデフォルト VLAN として作成済み
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	デフォルトで作成済みの VLAN 1 は削除できません。 VLAN を削除すると、削除した VLAN を指定した switchport access vlan 設定も削除されます。
制限・注意	• VLAN 設定モードのプライベート VLAN 関連の設定、または remote-span 設定が残っている VLAN は削除できません。
バージョン	1.08.02

使用例：VLAN 1000～1005 を作成する方法を示します。

```
# configure terminal
(config)# vlan 1000-1005
(config-vlan)#
```

5.17.2 name（VLAN）

name（VLAN）	
目的	VLAN 名を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	name NAME no name
Parameter	NAME：VLAN 名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	VLAN 1 は default（name default 設定） VLAN 1 以外は VLANXXXX（XXXX は VLAN ID と等しい 4 桁の数値）（例：VLAN 2 の場合は VLAN0002、VLAN 123 の場合は VLAN0123）
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN 1000 の VLAN 名を「admin-vlan」に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# name admin-vlan
(config-vlan)#
```

5.17.3 switchport mode

switchport mode	
目的	インターフェースの VLAN モードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport mode {access | hybrid | trunk | dot1q-tunnel} no switchport mode
Parameter	access：アクセスポートとして設定する場合に指定します。 hybrid：ハイブリッドポートとして設定する場合に指定します。 trunk：トランクポートとして設定する場合に指定します。 dot1q-tunnel：トンネルポートとして設定する場合に指定します。
デフォルト	access
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 アクセスポートは、設定した 1 つのアクセス VLAN のタグなしメンバーとして動作します。 ハイブリッドポートは、設定した複数の VLAN のタグ付きメンバー、またはタグなしメンバーとして動作します。ハイブリッドポートはプロトコル VLAN で使用します。

switchport mode	
	トランクポートは、設定した複数の VLAN のタグ付きメンバーと、1 つのネイティブ VLAN のタグなしメンバーとして動作します。switchport trunk native vlan tag コマンドを設定した場合は、ネイティブ VLAN もタグ付きメンバーとして動作します。トランクポートの目的は、装置対装置接続をサポートすることです。 トンネルポートは、VLAN トンネル（Q-in-Q）使用時のサービス VLAN の UNI ポートとして動作します。 本コマンドで VLAN モードが変更された場合、以前の VLAN モードに関係する VLAN 関連の設定も削除されます。
制限・注意	• インターフェースをトランクポートとして設定した場合、デフォルトでは switchport trunk allowed vlan all 設定のため、装置内に設定されているすべての VLAN がトランクポートで許可する VLAN になります。 • 本コマンドでトランクポートに設定、またはトランクポートから他の VLAN モードに変更する場合、負荷軽減のために、複数インターフェースの範囲設定モード（interface range port コマンド）は使用せず、単一インターフェースの設定モード（interface port コマンド）を使用してください。
バージョン	1.08.02

使用例：ポート 1/0/1 をトランクポートとして設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode trunk
(config-if-port)#
```

使用例：ポート 1/0/2 をトンネルポートとして設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/2
(config-if-port)# switchport mode dot1q-tunnel
(config-if-port)#
```

5.17.4 switchport access vlan

switchport access vlan	
目的	インターフェースのアクセス VLAN を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport access vlan VLAN-ID no switchport access vlan
Parameter	VLAN-ID：アクセス VLAN を 1～4094 の範囲で指定します。
デフォルト	VLAN 1（switchport access vlan 1）
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	本コマンド設定時に指定した VLAN が未作成の場合は、自動的に作成されます。 ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はアクセスポートまたはトンネルポートで設定できます。 指定できるアクセス VLAN は 1 つだけです。後から実行されたコマンドによって、前

switchport access vlan	
	のコマンドが上書きされます。
制限・注意	• 対象インターフェースの VLAN モードをアクセスモードまたはトンネルモード以外に変更すると、本設定も削除されます。
バージョン	1.08.02

使用例：ポート 1/0/1 を VLAN 1000 のアクセスポートに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode access
(config-if-port)# switchport access vlan 1000
(config-if-port)#
```

5.17.5 switchport trunk allowed vlan

switchport trunk allowed vlan	
目的	トランクポートで許可する VLAN を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport trunk allowed vlan {all | [add | remove | except] VLAN-ID [,|-]} no switchport trunk allowed vlan
Parameter	all：すべての VLAN を許可する場合に指定します。 add（省略可能）：許可する VLAN のリストに追加する場合に指定します。 remove（省略可能）：許可する VLAN のリストから削除する場合に指定します。 except（省略可能）：指定した VLAN を削除して、それ以外のすべての VLAN を許可する場合に指定します。 VLAN-ID：VLAN ID を 1～4094 の範囲で指定します。複数指定できます。add または remove パラメーターを指定しない場合、既存の設定がすべて上書きされます。
デフォルト	all（すべての VLAN を許可）
モード	インターフェース設定モード（port, range, port-channel）
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はトランクポートで設定できます。 許可する VLAN として割り当てられた VLAN は、ネイティブ VLAN 以外はタグ付きメンバーとして、ネイティブ VLAN はタグなしメンバーとして動作します。 switchport trunk native vlan tag コマンドを設定した場合は、ネイティブ VLAN もタグ付きメンバーとして動作します。
制限・注意	• 本コマンド設定時に指定した VLAN が未作成の場合でも、VLAN は自動的に作成されません。別途 vlan コマンドで作成してください。 • 対象インターフェースの VLAN モードをトランクモード以外に変更すると、本設定も削除されます。 • add または remove パラメーターを指定しないで設定した場合は、既存の設定がすべて上書きされることに注意してください。既存の設定に新たに VLAN を追加したい場合は、add パラメーターを指定して設定してください。既存の設定から VLAN

switchport trunk allowed vlan	
	を削除したい場合は、remove パラメーターを指定して設定してください。 • 本コマンドでトランクポートで許可する VLAN を設定・削除する場合、負荷軽減のために、複数インターフェースの範囲設定モード（interface range port コマンド）は使用せず、単一インターフェースの設定モード（interface port コマンド）を使用してください。
バージョン	1.08.02

使用例：トランクポートとして設定済みのポート 1/0/1 で、既存の設定に VLAN 1000 を許可する VLAN として追加する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport trunk allowed vlan add 1000
(config-if-port)#
```

5.17.6 switchport trunk native vlan

switchport trunk native vlan	
目的	トランクポートのネイティブ VLAN を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport trunk native vlan {VLAN-ID | tag} no switchport trunk native vlan [tag]
Parameter	VLAN-ID：トランクポートのネイティブ VLAN を 1～4094 の範囲で指定します。 tag：ネイティブ VLAN のタグ付きモードを有効にする場合に指定します。
デフォルト	VLAN 1（switchport trunk native vlan 1） タグなしモード（no switchport trunk native vlan tag）
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はトランクポートで設定できます。 ネイティブ VLAN を使用する場合は、ネイティブ VLAN も switchport trunk allowed vlan コマンドで許可 VLAN として追加する必要があります。 通常はネイティブ VLAN からタグなしフレームとして送信しますが、tag オプションでネイティブ VLAN のタグ付きモードを有効にした場合は、ネイティブ VLAN からタグ付きフレームとして送信します。なお、受信時の受け入れ可能なフレームタイプは、acceptable-frame コマンドで設定します。
制限・注意	• 本コマンド設定時に指定した VLAN が未作成の場合でも、VLAN は自動的に作成されません。別途 vlan コマンドで作成してください。 • 対象インターフェースの VLAN モードをトランクモード以外に変更すると、本設定も削除されます。
バージョン	1.08.02

使用例：ポート 1/0/1 をトランクポートに設定し、トランクポートのネイティブ VLAN を 20 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk native vlan 20
(config-if-port)#
```

5.17.7 switchport hybrid allowed vlan

switchport hybrid allowed vlan	
目的	ハイブリッドポートで許可する VLAN を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} VLAN-ID [,|-] no switchport hybrid allowed vlan
Parameter	add（省略可能）：許可する VLAN のリストに追加する場合に指定します。 tagged：VLAN のタグ付きメンバーとして設定する場合に指定します。 untagged：VLAN のタグなしメンバーとして設定する場合に指定します。 remove：許可する VLAN のリストから削除する場合に指定します。 VLAN-ID：VLAN ID を 1～4094 の範囲で指定します。複数指定できます。add または remove パラメーターを指定しない場合、既存の設定がすべて上書きされます。
デフォルト	untagged 1（VLAN 1 のタグなしメンバーポート）
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はハイブリッドポートで設定できます。untagged パラメーターを指定して設定する場合はトンネルポートでも設定できます。 すでに VLAN のタグなしメンバーとして設定されている VLAN ID を add tagged パラメーターを指定して設定した場合は、VLAN のタグなしメンバーから削除され、VLAN のタグ付きメンバーとして追加されます。 すでに VLAN のタグ付きメンバーとして設定されている VLAN ID を add untagged パラメーターを指定して設定した場合は、VLAN のタグ付きメンバーから削除され、VLAN のタグなしメンバーとして追加されます。
制限・注意	• 本コマンド設定時に指定した VLAN が未作成の場合でも、VLAN は自動的に作成されません。別途 vlan コマンドで作成してください。 • 対象インターフェースの VLAN モードをハイブリッドモード以外に変更すると、本設定も削除されます。 • トンネルポートで untagged パラメーターを指定して設定している場合は、対象インターフェースの VLAN モードをトンネルモード以外に変更すると、本設定も削除されます。 • add または remove パラメーターを指定しないで設定した場合は、既存の設定がすべて上書きされることに注意してください。既存の設定に新たに VLAN を追加したい場合は、add パラメーターを指定して設定してください。既存の設定から VLAN

switchport hybrid allowed vlan	
	を削除したい場合は、remove パラメーターを指定して設定してください。 • 本コマンドでハイブリッドポートで許可する VLAN を設定・削除する場合、負荷軽減のために、複数インターフェースの範囲設定モード（interface range port コマンド）は使用せず、単一インターフェースの設定モード（interface port コマンド）を使用してください。
バージョン	1.08.02

使用例：ハイブリッドポートとして設定済みのポート 1/0/1 で、既存の設定に VLAN 1000 をタグ付きメンバーとして、VLAN 2000 と VLAN 3000 をタグなしメンバーとして追加する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport hybrid allowed vlan add tagged 1000
(config-if-port)# switchport hybrid allowed vlan add untagged 2000,3000
(config-if-port)#
```

5.17.8 switchport hybrid native vlan

switchport hybrid native vlan	
目的	ハイブリッドポートのネイティブ VLAN を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport hybrid native vlan VLAN-ID no switchport hybrid native vlan
Parameter	VLAN-ID：ハイブリッドポートのネイティブ VLAN を 1～4094 の範囲で指定します。
デフォルト	VLAN 1（switchport hybrid native vlan 1）
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はハイブリッドポートで設定できます。 ネイティブ VLAN を使用する場合は、ネイティブ VLAN も switchport hybrid allowed vlan コマンドで許可 VLAN として追加する必要があります。 switchport hybrid allowed vlan untagged で追加した場合は、ネイティブ VLAN からタグなしフレームとして送信します。switchport hybrid allowed vlan tagged で追加した場合は、ネイティブ VLAN からタグ付きフレームとして送信します。なお、受信時の受け入れ可能なフレームタイプは、acceptable-frame コマンドで設定します。
制限・注意	• 本コマンド設定時に指定した VLAN が未作成の場合でも、VLAN は自動的に作成されません。別途 vlan コマンドで作成してください。 • 対象インターフェースの VLAN モードをハイブリッドモード以外に変更すると、本設定も削除されます。
バージョン	1.08.02

使用例：ポート 1/0/1 をハイブリッドポートに設定し、ハイブリッドポートのネイティブ VLAN を 20 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode hybrid
(config-if-port)# switchport hybrid allowed vlan add untagged 20
(config-if-port)# switchport hybrid native vlan 20
(config-if-port)#
```

5.17.9 protocol-vlan profile

protocol-vlan profile	
目的	プロトコルグループを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	protocol-vlan profile ID frame-type {ethernet2 | snap | llc} ether-type VALUE no protocol-vlan profile ID
Parameter	ID：プロトコルグループ ID を 1～16 の範囲で指定します。 frame-type：フレームタイプを以下の中から指定します。 • ethernet2：イーサネット II フレーム • snap：IEEE 802.2 SNAP フレーム • llc：IEEE 802.2 LLC フレーム VALUE：比較する値を 0x0～0xFFFF（16 進数）の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	各フレームタイプの比較対象は以下です。 • ethernet2 を指定した場合は、イーサタイプと比較します。 • snap を指定した場合は、SNAP ヘッダーのタイプと比較します。 • llc を指定した場合は、LLC ヘッダーの DSAP/SSAP と比較します。 プロトコルグループ設定を削除すると、削除したプロトコルグループ ID の protocol-vlan profile（Interface）設定も削除されます。
制限・注意	• 設定済みのプロトコルグループ ID は上書き設定できません。
バージョン	1.08.02

使用例：プロトコルグループ ID 10 で、IPv6 プロトコル（フレームタイプは ethernet2、値は 0x86dd）のプロトコルグループを設定する方法を示します。

```
# configure terminal
(config)# protocol-vlan profile 10 frame-type ethernet2 ether-type 0x86dd
(config)#
```

5.17.10 protocol-vlan profile（Interface）

protocol-vlan profile（Interface）	
目的	指定したプロトコルグループにマッチしたフレームの受信 VLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	protocol-vlan profile ID vlan VLAN-ID [priority COS-VALUE]

protocol-vlan profile（Interface）	
	no protocol-vlan profile [ID]
Parameter	ID：プロトコルグループ ID を 1～16 の範囲で指定します。 VLAN-ID：受信 VLAN を 1～4094 の範囲で指定します。 priority COS-VALUE（省略可能）：受信フレームの CoS 値を、0～7 の範囲で指定します。指定しない場合、優先度は 0 に設定されます。
デフォルト	なし
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はハイブリッドポートまたはトンネルポートで設定できます。 1 つのプロトコルグループにつき 1 つの受信 VLAN を設定できます。また、複数のプロトコルグループの受信 VLAN を、同じ VLAN に設定することもできます。
制限・注意	• グローバル設定モードの protocol-vlan profile 設定を削除すると、削除したプロトコルグループ ID に関連する本設定も削除されます。 • 対象インターフェースの VLAN モードをハイブリッドモードまたはトンネルモード以外に変更すると、本設定も削除されます。
バージョン	1.08.02

使用例：ポート 1/0/1 で、プロトコルグループ ID 10 とプロトコルグループ ID 11 の受信 VLAN を、VLAN 3000 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# protocol-vlan profile 10 vlan 3000
(config-if-port)# protocol-vlan profile 11 vlan 3000
(config-if-port)#
```

5.17.11 acceptable-frame

acceptable-frame	
目的	受信可能なフレームタイプ（タグ付きフレーム or タグなしフレーム）を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	acceptable-frame {tagged-only | untagged-only | admit-all} no acceptable-frame
Parameter	tagged-only：タグ付きフレームのみ受信を許可する場合に指定します。 untagged-only：タグなしフレームのみ受信を許可する場合に指定します。 admit-all：すべてのタイプ（タグ付き、タグなし）のフレームの受信を許可する場合に指定します。
デフォルト	アクセスポート：untagged-only 他の VLAN モードのポート：admit-all
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モー

acceptable-frame	
	ド（interface port-channel コマンド）で設定してください。
制限・注意	• 対象インターフェースの VLAN モードを現在設定されている VLAN モードから他の VLAN モードに変更すると、本設定も削除されて各 VLAN モードのデフォルト設定に戻ります。
バージョン	1.08.02

使用例：ポート 1/0/1 で受信可能なフレームタイプを tagged-only に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# acceptable-frame tagged-only
(config-if-port)#
```

5.17.12 ingress-checking

ingress-checking	
目的	タグ付きフレームを受信した際の VLAN ID チェックを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	ingress-checking no ingress-checking
Parameter	なし
デフォルト	有効（ingress-checking）
モード	インターフェース設定モード（port, range, port-channel）
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 VLAN ID チェックが有効（デフォルト設定）の場合は、受信したタグ付きフレームの VLAN ID に一致する VLAN が対象ポートに割り当てられている場合にのみ受信できます。割り当てられていない場合は受信できません。 VLAN ID チェックが無効の場合は、受信したタグ付きフレームの VLAN ID に一致する VLAN が対象ポートに割り当てられていない場合でも、一致する VLAN が装置で設定済みの場合はその VLAN で受信します。
制限・注意	• 対象インターフェースの VLAN モードを現在設定されている VLAN モードから他の VLAN モードに変更すると、本設定もデフォルト設定に戻ります。
バージョン	1.08.02

使用例：ポート 1/0/1 で、タグ付きフレームを受信した際の VLAN ID チェックを有効（デフォルト設定）にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ingress-checking
(config-if-port)#
```

5.17.13 show vlan

show vlan	
目的	VLAN の設定を表示します。

show vlan	
Command	show vlan [VLAN-ID [,|-] | detail]
Parameter	VLAN-ID（省略可能）：メンバーポート情報を表示する VLAN ID を 1～4094 の範囲で指定します。複数指定できます。 detail（省略可能）：VLAN の詳細情報を表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定の VLAN を指定しない場合は、すべての VLAN の情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：現在のすべての VLAN の設定を表示する方法を示します。

```
# show vlan

 VLAN 1 ...(1)
   Name : default ...(2)
   Description : ...(3)
   Tagged Member Ports   : ...(4)
   Untagged Member Ports : 1/0/1-1/0/2,1/0/9-1/0/12 ...(5)
 VLAN 100
   Name : VLAN0100
   Description :
   Tagged Member Ports   : 1/0/11-1/0/12
   Untagged Member Ports : 1/0/3-1/0/5
 VLAN 200
   Name : VLAN0200
   Description :
   Tagged Member Ports   : 1/0/11-1/0/12
   Untagged Member Ports : 1/0/6-1/0/8
 Total Entries: 3
```

項番	説明
(1)	VLAN ID を表示します。
(2)	VLAN 名を表示します。
(3)	対応するレイヤー2 VLAN インターフェースの description 設定を表示します。
(4)	VLAN のタグ付きメンバーポートを表示します。
(5)	VLAN のタグなしメンバーポートを表示します。

使用例：VLAN の詳細情報を表示する方法を示します。

```
# show vlan detail

--- vlan port information --- ...(1)
                a = access  t = trunk  h = hybrid
                p = private-vlan  d = dot1q-tunnel
                C Port
                  1      8 9
                  +------+ +---
 Port Mode      1 aaaaaaaa aatt

--- vlan mapping information --- ...(2)
                u = untag  t = tag
```

```
                C Port
                  1       8 9
 Name       VID   +-------+ +---
default       1 1 uu...... uuuu
VLAN0100    100 1 ..uuu... ..tt
VLAN0200    200 1 .....uuu ..tt
```

項番	説明
(1)	ポートの VLAN モードを表示します。 "C"列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。
(2)	VLAN ID ごとに、ポートのタグなし、またはタグ付きを表示します。 "C"列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。

5.17.14 show vlan interface

show vlan interface	
目的	VLAN 関連のインターフェース設定を表示します。
Command	show vlan interface [IF-ID [,|-]]
Parameter	IF-ID (省略可能)：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	• AccessDefender 機能のダイナミック VLAN によって VLAN がダイナミックに割り当てられても、show vlan interface コマンドで表示される VLAN 情報には反映されません。本コマンドでは、switchport access vlan などの各コマンドで設定した VLAN 情報を表示します。
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/6 の VLAN 情報、受け入れチェックの有効／無効、および受け入れ可能なフレームタイプの情報を表示する方法を示します。

```
# show vlan interface port 1/0/1-6

 Port1/0/1 ...(1)
   VLAN mode              : Access ...(2)
   Access VLAN            : 10 ...(3)
   Ingress checking       : Enabled ...(4)
   Acceptable frame type  : Untagged-Only ...(5)

 Port1/0/2
   VLAN mode              : Trunk
   Native VLAN            : 1 (Untagged) ...(6)
   Trunk allowed VLAN     : 1-4094 ...(7)
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All

 Port1/0/3
   VLAN mode              : Hybrid
   Native VLAN            : 1 ...(8)
```

```
  Hybrid untagged VLAN  : 1,50,60 ...(9)
  Hybrid tagged VLAN    : 10,20 ...(10)
  Ingress checking      : Enabled
  Acceptable frame type : Admit-All

Port1/0/4
  VLAN mode             : Dot1q-Tunnel
  Access VLAN           : 10 ...(11)
  Hybrid untagged VLAN  : 50,60 ...(12)
  Ingress checking      : Enabled
  Acceptable frame type : Admit-All

Port1/0/5
  VLAN mode             : Promiscuous
  Native VLAN           : 100 ...(13)
  Ingress checking      : Enabled
  Acceptable frame type : Admit-All

Port1/0/6
  VLAN mode             : Host
  Native VLAN           : 101 ...(14)
  Ingress checking      : Enabled
  Acceptable frame type : Admit-All
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	インターフェースの VLAN 動作モードを表示します。 Access：アクセスモード Trunk：トランクモード Hybrid：ハイブリッドモード Dot1q-Tunnel：トンネルモード Promiscuous：プライベート VLAN のプロミスキャスポート Host：プライベート VLAN のホストポート
(3)	アクセスモードのポートにおいて、switchport access vlan コマンドで設定したアクセス VLAN を表示します。
(4)	受信したフレームの受け入れチェックの有効(Enabled)／無効(Disabled)を表示します。
(5)	受け入れ可能なフレームタイプを表示します。 Tagged-Only：タグ付きフレームのみ Untagged-Only：タグなしフレームのみ Admit-All：すべてのフレーム
(6)	トランクモードのポートにおいて、switchport trunk native vlan コマンドで設定したネイティブ VLAN を表示します。 (Untagged)：ネイティブ VLAN はタグなしモード (tagged)：ネイティブ VLAN はタグ付きモード
(7)	トランクモードのポートにおいて、switchport trunk allowed vlan コマンドで許可した VLAN を表示します。
(8)	ハイブリッドモードのポートにおいて、switchport hybrid native vlan コマンドで設定したネイティブ VLAN を表示します。
(9)	ハイブリッドモードのポートにおいて、switchport hybrid allowed vlan コマンドで untagged 指定で許可した VLAN を表示します。
(10)	ハイブリッドモードのポートにおいて、switchport hybrid allowed vlan コマンドで

項番	説明
	tagged 指定で許可した VLAN を表示します。
(11)	トンネルモードのポートにおいて、switchport access vlan コマンドで設定したアクセス VLAN を表示します。
(12)	トンネルモードのポートにおいて、switchport hybrid allowed vlan コマンドで untagged 指定で許可した VLAN を表示します。
(13)	プライベート VLAN のプロミスキャスポートにおいて、switchport private-vlan mapping コマンドで設定したプライマリーVLAN を表示します。
(14)	プライベート VLAN のホストポートにおいて、switchport private-vlan host-association コマンドで設定したセカンダリーVLAN を表示します。

5.17.15 show protocol-vlan

show protocol-vlan	
目的	プロトコル VLAN の設定を表示します。
Command	show protocol-vlan {profile [ID [,|-]] | interface [IF-ID [,|-]]}
Parameter	profile：プロトコルグループの設定を表示する場合に指定します。 ID（省略可能）：設定を表示するプロトコルグループ ID を、1～16 の範囲で指定します。複数指定できます。 interface：インターフェースのプロトコル VLAN 識別設定を表示する場合に指定します。 IF-ID（省略可能）：プロトコル VLAN 識別設定を表示するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	profile パラメーターを指定して特定のプロトコルグループ ID を指定しない場合は、すべてのプロトコルグループ ID の情報が表示されます。 interface パラメーターを指定して特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：すべてのプロトコルグループの設定を表示する方法を示します。

```
# show protocol-vlan profile
 (1)          (2)           (3)
Profile ID  Frame-type   Ether-type
----------  -----------  ----------------
1           Ethernet2    0x86DD(IPv6)
2           Ethernet2    0x0800(IP)
3           Ethernet2    0x0806(ARP)
```

項番	説明
(1)	プロトコルグループ ID を表示します。

項番	説明
(2)	フレームタイプの種類を表示します。
(3)	フレームタイプの値を表示します。

使用例：ポート 1/0/1～1/0/3 のプロトコル VLAN 識別設定を表示する方法を示します。

```
# show protocol-vlan interface port 1/0/1-3
 (1)               (2)                  (3)    (4)
 Interface         Protocol Group ID    VLAN   Priority
 ---------------   ------------------   ----   --------
 Port1/0/1         1                    1      5
                   10                   3      0
 Port1/0/2         11                   2001   4
                   12                   3002   1
 Port1/0/3         2                    100    6
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	インターフェースに割り当てられているプロトコルグループ ID を表示します。
(3)	プロトコルグループにマッチした場合に受信する VLAN の VLAN ID を表示します。
(4)	受信フレームの CoS 値を表示します。

5.18 プライベート VLAN コマンド

プライベート VLAN 関連の設定コマンドは以下のとおりです。

- private-vlan
- private-vlan association
- switchport mode private-vlan
- switchport private-vlan host-association
- switchport private-vlan mapping

プライベート VLAN 関連の show／操作コマンドは以下のとおりです。

- show vlan private-vlan
- private-vlan synchronize

5.18.1 private-vlan

private-vlan	
目的	プライベート VLAN として使用する VLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	private-vlan {community | isolated | primary} no private-vlan {community | isolated | primary}
Parameter	community：対象 VLAN を、セカンダリーVLAN の「コミュニティーVLAN」として設定する場合に指定します。 isolated：対象 VLAN を、セカンダリーVLAN の「独立 VLAN」として設定する場合に指定します。 primary：対象 VLAN を、プライマリーVLAN として設定する場合に指定します。
デフォルト	なし
モード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	プライベート VLAN は、1 つのプライマリーVLAN に 1 つ以上のセカンダリーVLAN（1 つの独立 VLAN、複数のコミュニティーVLAN）を関連付けて設定します。 • プロミスキャスポートで受信したトラフィックは、すべてのプロミスキャスポートとホストポートに中継可能です。 • 独立 VLAN のホストポートで受信したトラフィックは、プロミスキャスポートにのみ中継可能です。独立 VLAN の別のホストポートや、コミュニティーVLAN のホストポートには中継しません。 • コミュニティーVLAN のホストポートで受信したトラフィックは、プロミスキャスポート、および同じコミュニティーVLAN の別のホストポートに中継可能です。異なるコミュニティーVLAN のホストポートや、独立 VLAN のホストポートには中継しません。 プライベート VLAN のポート（プロミスキャスポート、ホストポート）では、Untag フレームを送受信します。 プライベート VLAN では、通常の VLAN より多くの MAC アドレステーブルを使用します。以下に例を示します。 • プロミスキャスポート（switchport private-vlan mapping 10 add 101-103）で MAC アドレス(A)からフレームを受信すると、「プライマリーVLAN 10 の

private-vlan	
	MAC アドレス(A)のエントリー」と、「セカンダリーVLAN (VLAN 101, VLAN 102, VLAN 103) の MAC アドレス(A)のエントリー」の、合計 4 個の MAC アドレスエントリーが登録されます。 • ホストポート (switchport private-vlan host-association 10 101) で MAC アドレス(B)からフレームを受信すると、「プライマリーVLAN 10 の MAC アドレス(B)のエントリー」と、「セカンダリーVLAN 101 の MAC アドレス(B)のエントリー」の、合計 2 個の MAC アドレスエントリーが登録されます。 プライベート VLAN でスタティック MAC アドレスエントリーを設定する場合は、プライマリーVLAN のエントリーとして設定します。スタティック MAC アドレスエントリーを 1 個設定すると、プライベート VLAN に必要なセカンダリーVLAN 用のダイナミック MAC アドレスエントリーが自動的に生成されます。
制限・注意	• VLAN 1 はプライベート VLAN として使用できません。 • セカンダリーVLAN では、VLAN インターフェース (interface vlan コマンド) を作成して IP アドレスを設定することはできません。プライマリーVLAN では設定できますが、ホストポート経由ではその IP アドレスとの通信 (Telnet や ping など、すべての IP 通信) はできません。 • プライベート VLAN では、以下機能との併用は不可、または未サポートです。 • プライベート VLAN と他 VLAN との間の Layer3 中継 • OSPF や VRRP など、すべての Layer3 関連機能 (ただし、プロミスキャスポート経由の管理用のスタティックルートは除く) • DHCP 関連機能、CFM 機能、IGMP スヌーピング機能、MLD スヌーピング機能、RPVST+機能、VLAN ベースモードのループ検知機能 • AccessDefender 機能のダイナミック VLAN、Gateway 認証、DHCP スヌーピング • その他、ホストポート経由で装置の IP アドレスとの通信が関連する機能 • すでに、switchport access vlan コマンドや switchport hybrid allowed vlan コマンドでポートを割り当て済みの VLAN は、プライベート VLAN として設定できません。 • すでに、interface vlan コマンドで Layer3 インターフェースを設定済みの VLAN は、セカンダリーVLAN として設定できません。 • プライベート VLAN では、基本的にプロミスキャスポートとホストポートを使用しますが、同じポリシーのプライベート VLAN をスイッチを跨いで構築する場合のみ、スイッチ間を接続するポートはトランクポート設定で接続します。ただし、この構成の場合、以下のようなフラッディングトラフィックが増える仕様制限があることに注意してください。以下では、2 台のスイッチ (SW1 と SW2) をトランクポート設定で接続している構成を例に説明します。 • SW1 のプロミスキャスポートで受信し、宛先 MAC アドレスの端末が SW2 のホストポートの先に存在する場合、そのトラフィックは SW1 では常にフラッディング中継動作になります。 • SW1 のホストポートで受信し、宛先 MAC アドレスの端末が SW2 のプロミスキャスポートの先に存在する場合、そのトラフィックは SW1 では常にフラッディング中継動作になります。
バージョン	1.08.02

使用例：VLAN 1000 をプライマリーVLAN、VLAN 1001 を独立 VLAN、VLAN 1002 をコミュニティーVLAN として設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# private-vlan primary
(config-vlan)# exit
(config)# vlan 1001
(config-vlan)# private-vlan isolated
(config-vlan)# exit
(config)# vlan 1002
(config-vlan)# private-vlan community
(config-vlan)#
```

5.18.2 private-vlan association

private-vlan association	
目的	プライマリーVLAN とセカンダリーVLAN の関連付けを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	private-vlan association {add SECONDARY-VLAN-ID [,|-] | remove SECONDARY-VLAN-ID [,|-]} no private-vlan association
Parameter	add SECONDARY-VLAN-ID：対象のプライマリーVLAN に関連付けるセカンダリーVLAN を、2～4094 の範囲で指定します。複数指定できます。 remove SECONDARY-VLAN-ID：対象のプライマリーVLAN から関連付けを削除するセカンダリーVLAN を、2～4094 の範囲で指定します。複数指定できます。
デフォルト	なし
モード	プライマリーVLAN の VLAN 設定モード
特権レベル	レベル：12
ガイドライン	セカンダリーVLAN は、1 つのプライマリーVLAN だけに関連付けられます。
制限・注意	-
バージョン	1.08.02

使用例：プライマリーVLAN 1000 に、セカンダリーVLAN 1001 とセカンダリーVLAN 1002 を関連付ける方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# private-vlan association add 1001-1002
(config-vlan)#
```

5.18.3 switchport mode private-vlan

switchport mode private-vlan	
目的	プライベート VLAN のインターフェースの VLAN モードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport mode private-vlan {host | promiscuous} no switchport mode
Parameter	host：セカンダリーVLAN 用のホストポート（独立 VLAN のホストポート、コミュニティーVLAN のホストポート）として設定する場合に指定します。 promiscuous：プライマリーVLAN 用のプロミスキャスポートとして設定する場合に

switchport mode private-vlan	
	指定します。
デフォルト	access
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 セカンダリーVLAN のホストポートは、本コマンドでホストポートに設定し、switchport private-vlan host-association コマンドで VLAN を割り当てます。 プライマリーVLAN のプロミスキャスポートは、本コマンドでプロミスキャスポートに設定し、switchport private-vlan mapping コマンドで VLAN を割り当てます。 プライベート VLAN は基本的にプロミスキャスポートとホストポートを使用しますが、同じポリシーのプライベート VLAN をスイッチを跨いで構築する場合のみ、スイッチ間を接続するポートはトランクポート設定で接続します。スイッチ間を接続するトランクポートは、switchport mode trunk コマンドでトランクポートに設定し、switchport trunk allowed vlan コマンドで VLAN を割り当てます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 をホストポートに、ポート 1/0/2 をプロミスキャスポートに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode private-vlan host
(config-if-port)# exit
(config)# interface port 1/0/2
(config-if-port)# switchport mode private-vlan promiscuous
(config-if-port)#
```

5.18.4 switchport private-vlan host-association

switchport private-vlan host-association	
目的	ホストポートに割り当てる VLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	switchport private-vlan host-association PRIMARY-VLAN-ID SECONDARY-VLAN-ID no switchport private-vlan host-association
Parameter	PRIMARY-VLAN-ID：プライマリーVLAN を 2～4094 の範囲で指定します。 SECONDARY-VLAN-ID：セカンダリーVLAN を 2～4094 の範囲で指定します。
デフォルト	なし
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 指定したセカンダリーVLAN が独立 VLAN の場合、対象ポートは独立 VLAN のホストポートになります。独立 VLAN のホストポートで受信したトラフィックは、プロミ

switchport private-vlan host-association	
	スキャスポートにのみ中継可能です。独立 VLAN の別のホストポートや、コミュニティーVLAN のホストポートには中継しません。 指定したセカンダリーVLAN がコミュニティーVLAN の場合、対象ポートはコミュニティーVLAN のホストポートになります。コミュニティーVLAN のホストポートで受信したトラフィックは、プロミスキャスポート、および同じコミュニティーVLAN の別のホストポートに中継可能です。異なるコミュニティーVLAN のホストポートや、独立 VLAN のホストポートには中継しません。 ホストポートで MAC アドレスを学習する場合は、「プライマリーVLAN の MAC アドレスエントリー」と「セカンダリーVLAN の MAC アドレスエントリー」の、合計 2 個の MAC アドレスエントリーが登録されます。
制限・注意	• 本コマンドを設定する前に、private-vlan association コマンドでプライマリー VLAN とセカンダリーVLAN の関連付けを設定しておく必要があります。関連付けされていない組み合わせを指定しても設定できません。
バージョン	1.08.02

使用例：ポート 1/0/1 をホストポートに設定し、「プライマリーVLAN 1000、セカンダリーVLAN 1001」を割り当てる方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode private-vlan host
(config-if-port)# switchport private-vlan host-association 1000 1001
(config-if-port)#
```

5.18.5 switchport private-vlan mapping

switchport private-vlan mapping	
目的	プロミスキャスポートに割り当てる VLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	switchport private-vlan mapping PRIMARY-VLAN-ID {add SECONDARY-VLAN-ID [,|-] | remove SECONDARY-VLAN-ID [,|-]} no switchport private-vlan mapping
Parameter	PRIMARY-VLAN-ID：プライマリーVLAN を 2～4094 の範囲で指定します。 add SECONDARY-VLAN-ID：追加するセカンダリーVLAN を、2～4094 の範囲で指定します。複数指定できます。 remove SECONDARY-VLAN-ID：削除するセカンダリーVLAN を、2～4094 の範囲で指定します。複数指定できます。
デフォルト	なし
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 プロミスキャスポートで受信したトラフィックは、すべてのプロミスキャスポートとホストポートに中継可能です。 プロミスキャスポートで MAC アドレスを学習する場合は、「プライマリーVLAN の MAC アドレスエントリー」と「本コマンドで割り当てたセカンダリーVLAN の MAC

switchport private-vlan mapping	
	アドレスエントリー」が登録されます。
制限・注意	• 本コマンドを設定する前に、private-vlan association コマンドでプライマリー VLAN とセカンダリーVLAN の関連付けを設定しておく必要があります。関連付けされていない組み合わせを指定しても設定できません。
バージョン	1.08.02

使用例：ポート 1/0/2 をプロミスキャスポートに設定し、「プライマリーVLAN 1000、セカンダリーVLAN 1001 とセカンダリーVLAN 1002」を割り当てる方法を示します。

```
# configure terminal
(config)# interface port 1/0/2
(config-if-port)# switchport mode private-vlan promiscuous
(config-if-port)# switchport private-vlan mapping 1000 add 1001,1002
(config-if-port)#
```

5.18.6 show vlan private-vlan

show vlan private-vlan	
目的	プライベート VLAN の設定を表示します。
Command	show vlan private-vlan
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：プライベート VLAN の設定を表示する方法を示します。

```
# show vlan private-vlan
(1)             (2)               (3)         (4)
Primary VLAN    Secondary VLAN    Type        Interface
------------------------------------------------------
1000            1001              Isolated    1/0/1-1/0/2
1000            1002              Community   1/0/2

Total Entries: 2
```

項番	説明
(1)	プライマリーVLAN の VLAN ID を表示します。
(2)	セカンダリーVLAN の VLAN ID を表示します。
(3)	セカンダリーVLAN のタイプを表示します。 Isolated：独立 VLAN Community：コミュニティーVLAN
(4)	ポート番号を表示します。ポートチャネルでプライベート VLAN を設定した場合は、メンバーポートのポート番号が表示されます。

5.18.7 private-vlan synchronize

private-vlan synchronize	
目的	プライベート VLAN で MSTP を使用する場合に、セカンダリーVLAN をプライマリーVLAN と同じ MSTP インスタンスにマッピングします。
Command	private-vlan synchronize
Parameter	なし
モード	MSTP コンフィグレーションモード
特権レベル	レベル：12
ガイドライン	プライベート VLAN で MSTP を使用する場合は、instance（MSTP)コマンドで、プライマリーVLAN とセカンダリーVLAN を同じ MSTP インスタンスにマッピングする必要があります。 プライマリーVLAN とセカンダリーVLAN が異なる MSTP インスタンスにマッピングされている場合は、show spanning-tree mst configuration コマンドに注意喚起を促すメッセージが表示されます。（例：The following secondary VLANs are not mapped to the same instance as its primary VLAN: 101-103） そのような状況で本コマンドを実行すると、セカンダリーVLAN がプライマリーVLAN と同じ MSTP インスタンスにマッピングされるように設定が変更されます。
制限・注意	• 本コマンドは MSTP コンフィグレーションモード実施する実行コマンドで、実施しても構成情報には残りません。
バージョン	1.08.02

使用例：private-vlan synchronize コマンドの実行例を示します。

```
# show spanning-tree mst configuration

 Name      : TEST-MSTP
 Revision : 0,Instances configured: 3
 Instance    Vlans
 --------    ----------------------------------------------------------------
      0      1-9,11-19,21-29,31-39,41-4094
      1      10
      2      20,30,40
 The following secondary VLANs are not mapped to the same instance as its primary VLAN:    101-103

#
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)# private-vlan synchronize
(config-mst)# end
#
# show spanning-tree mst configuration

 Name      : TEST-MSTP
 Revision : 0,Instances configured: 3
 Instance    Vlans
 --------    ----------------------------------------------------------------
      0      1-9,11-19,21-29,31-39,41-100,104-4094
      1      10,101-103
      2      20,30,40
```

5.19 VLAN トンネルコマンド

VLAN トンネル関連の設定コマンドは以下のとおりです。

- dot1q inner ethertype
- dot1q tunneling ethertype
- switchport vlan mapping
- vlan mapping profile
- vlan mapping rule
- switchport vlan mapping profile
- vlan mapping miss drop
- dot1q-tunnel trust inner-priority
- dot1q-tunnel insert dot1q-tag

VLAN トンネル関連の show コマンドは以下のとおりです。

- show dot1q ethertype
- show vlan mapping
- show dot1q-tunnel
- show vlan mapping profile

5.19.1 dot1q inner ethertype

dot1q inner ethertype	
目的	装置のカスタマーVLAN タグの TPID を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	dot1q inner ethertype VALUE no dot1q inner ethertype
Parameter	VALUE：カスタマーVLAN タグの TPID を 0x1～0xFFFF（16 進数）の範囲で指定します。
デフォルト	0x8100
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	カスタマーVLAN タグの TPID は、装置全体の設定です。 指定した値は、受信フレームがカスタマーVLAN タグ付きかどうかの判断に使用されます。
制限・注意	-
バージョン	1.08.02

使用例：カスタマーVLAN タグの TPID を 0x9100 に設定する方法を示します。

```
# configure terminal
(config)# dot1q inner ethertype 0x9100
(config)#
```

5.19.2 dot1q tunneling ethertype

dot1q tunneling ethertype	
目的	トランクポートのサービスプロバイダーVLAN タグの TPID を設定します。デフォル

dot1q tunneling ethertype	
	ト設定に戻すには、no 形式のコマンドを使用します。
Command	dot1q tunneling ethertype VALUE no dot1q tunneling ethertype
Parameter	VALUE：サービスプロバイダーVLAN タグの TPID を 0x1～0xFFFF（16 進数）の範囲で指定します。
デフォルト	0x8100
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はトランクポートで設定できます。 指定した値は、トランクポートから送信されるフレームのサービスプロバイダーVLAN タグの TPID になります。また、トランクポートで受信したフレームのサービスプロバイダーVLAN タグを識別するためにも使用されます。
制限・注意	• 対象インターフェースの VLAN モードをトランクモード以外に変更すると、本設定も削除されます。
バージョン	1.08.02

使用例：トランクモードに設定したポート 1/0/1 で、サービスプロバイダーVLAN タグの TPID を 0x88a8 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode trunk
(config-if-port)# dot1q tunneling ethertype 0x88a8
(config-if-port)#
```

5.19.3 switchport vlan mapping

switchport vlan mapping	
目的	トランクポートで使用する VLAN 変換エントリーや、トンネルポートで使用するサービス VLAN マッピングエントリーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	■ VLAN 変換エントリー switchport vlan mapping original-vlan ORIGINAL-VLAN [ORIGINAL-INNER-VLAN] resultant-vlan RESULTANT-VLAN [RESULTANT-INNER-VLAN] [priority COS-VALUE] ■ サービス VLAN マッピングエントリー switchport vlan mapping original-vlan ORIGINAL-VLAN [,|-] dot1q-tunnel DOT1Q-TUNNEL-VLAN [priority COS-VALUE] ■ 削除コマンド no switchport vlan mapping original-vlan ORIGINAL-VLAN [,|-] [ORIGINAL-INNER-VLAN]
Parameter	■ VLAN 変換エントリー ORIGINAL-VLAN：受信フレームの VLAN ID を 1～4094 の範囲で指定します。

switchport vlan mapping	
	ORIGINAL-INNER-VLAN（省略可能）：トランクポートの場合に、受信フレームのカスタマーVLAN タグの VLAN ID を 1～4094 の範囲で指定します。 resultant-vlan RESULTANT-VLAN：受信フレームの VLAN 変換後の VLAN ID（装置で中継する VLAN）を、1～4094 の範囲で指定します。 RESULTANT-INNER-VLAN（省略可能）：トランクポートの場合に、受信フレームの VLAN 変換後のカスタマーVLAN タグの VLAN ID を 1～4094 の範囲で指定します。 priority COS-VALUE（省略可能）：エントリーに一致したフレームに反映する優先度を指定します。省略した場合は優先度は 0 に設定されます。 ■ サービス VLAN マッピングエントリー ORIGINAL-VLAN：受信フレームの VLAN ID を 1～4094 の範囲で指定します。複数指定できます。 dot1q-tunnel DOT1Q-TUNNEL-VLAN：トンネルポートにおいて、サービス VLAN マッピングエントリーにマッチしたフレームを受信する VLAN ID を、1～4094 の範囲で指定します。 priority COS-VALUE（省略可能）：エントリーに一致したフレームに反映する優先度を指定します。省略した場合は優先度は 0 に設定されます。
デフォルト	なし
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 <VLAN 変換エントリー> resultant-vlan RESULTANT-VLAN 設定は、主にトランクポートで VLAN 変換エントリーを設定するために使用します。受信したフレームの VLAN ID が ORIGINAL-VLAN と一致した場合に、RESULTANT-VLAN で指定した VLAN ID に変換されます。また、送信するフレームの VLAN ID が RESULTANT-VLAN と一致した場合に、ORIGINAL-VLAN で指定した VLAN ID に変換されます。 トランクポートで 2 段タグフレームの VLAN 変換エントリー（switchport vlan mapping original-vlan ORIGINAL-VLAN ORIGINAL-INNER-VLAN resultant-vlan RESULTANT-VLAN RESULTANT-INNER-VLAN コマンド）を設定した場合は、カスタマーVLAN タグの VLAN ID も VLAN 変換されます。なお、ORIGINAL-INNER-VLAN を指定して RESULTANT-INNER-VLAN を指定しない形式で設定した場合は、カスタマーVLAN タグの VLAN ID は変換されません。 トンネルポートで VLAN 変換エントリーを使用する場合は、1 段タグフレームの VLAN 変換エントリー（switchport vlan mapping original-vlan ORIGINAL-VLAN resultant-vlan RESULTANT-VLAN コマンド）を使用します。2 段タグフレームの VLAN 変換エントリーは使用できません。受信したカスタマーVLAN タグ付きフレームの VLAN ID が ORIGINAL-VLAN と一致した場合に、カスタマーVLAN タグを削除して受信します。また、トンネルポートから送信するフレームにカスタマーVLAN タグがない場合に、VLAN ID が ORIGINAL-VLAN のカスタマーVLAN タグを付加して送信します。

switchport vlan mapping	
	<サービス VLAN マッピングエントリー> dot1q-tunnel DOT1Q-TUNNEL-VLAN 設定は、トンネルポートでサービス VLAN マッピングエントリーを設定するために使用します。トンネルポートで受信したカスタマーVLAN タグ付きフレームの VLAN ID が ORIGINAL-VLAN と一致した場合に、DOT1Q-TUNNEL-VLAN で指定した VLAN で受信します。 一致するサービス VLAN マッピングエントリーが存在しておらず、受信したトンネルポートで vlan mapping miss drop コマンドが有効な場合は、その受信フレームは破棄されます。vlan mapping miss drop コマンドが無効の場合は、switchport access vlan コマンドで設定したアクセス VLAN が割り当てられていれば、その VLAN で受信します。

制限・注意	• すでに「ORIGINAL-VLAN (A), RESULTANT-VLAN (B)」の VLAN 変換エントリーが設定されている場合には、別の ORIGINAL-VLAN (A 以外)を設定済みの RESULTANT-VLAN (B)に変換するような VLAN 変換エントリーは設定できません。同様に、ORIGINAL-VLAN (A)を別の RESULTANT-VLAN (B 以外)に変換するような VLAN 変換エントリーも設定できません。
	• 設定可能な VLAN マッピングルールの最大数は、装置全体で 1,024 個です。
	• 本コマンドはポートチャネル 33 以降では設定できません。
	• VLAN 変換機能と STP/RSTP/MSTP/RPVST+機能は、同一インターフェースで併用できません。
	• ApresiaNP2500 シリーズでは、以下の仕様制限があります。
	  • 2 段タグフレームの VLAN 変換エントリーを適用したポートでエントリーに一致する 2 段タグ付きフレームを受信する際には、受信した 2 段タグ付きフレームの「サービス VLAN タグの優先度」と「カスタマーVLAN タグの優先度」の両方が、priority オプションの値に変更されます。
	  • 2 段タグフレームの VLAN 変換エントリーを適用したポートからエントリーに一致する 2 段タグ付きフレームを送信する際には、送信する 2 段タグ付きフレームの「カスタマーVLAN タグの優先度」も、装置内部の優先度の値に変更されます。

バージョン	1.08.02

使用例：トランクポートに設定したポート 1/0/1 で、以下の VLAN 変換エントリーを設定する方法を示します。

- 送受信するフレームの VLAN ID が 100 の場合、装置内部では VLAN 1100 に変換
- 送受信するフレームの VLAN ID が 200 の場合、装置内部では VLAN 1200 に変換

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode trunk
(config-if-port)# switchport vlan mapping original-vlan 100 resultant-vlan 1100
(config-if-port)# switchport vlan mapping original-vlan 200 resultant-vlan 1200
(config-if-port)#
```

使用例：トンネルモードに設定したポート 1/0/2 で、受信したカスタマーVLAN タグ付きフレームの VLAN ID が 700 の場合に、VLAN 1700 で受信できるように設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/2
(config-if-port)# switchport mode dot1q-tunnel
(config-if-port)# switchport vlan mapping original-vlan 700 dot1q-tunnel 1700
```

```
(config-if-port)# switchport hybrid allow vlan add untagged 1700
(config-if-port)#
```

5.19.4 vlan mapping profile

vlan mapping profile	
目的	VLAN マッピングプロファイルを設定します。また、VLAN マッピングプロファイル設定モードに遷移します。遷移後のプロンプトは（config-vlan-map)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	vlan mapping profile ID [type PROFILE-TYPE] no vlan mapping profile ID
Parameter	ID：VLAN マッピングプロファイル ID を 1～1000 の範囲で指定します。ID の値が小さいほど、優先度は高くなります。 type PROFILE-TYPE（省略可能）：VLAN マッピングプロファイルのタイプを以下のパラメーターで指定します。 • ethernet：レイヤー2 フィールドの情報を対象とする場合に指定します。 • ip：IP パケットの情報を対象とする場合に指定します。 • ipv6：IPv6 パケットの情報を対象とする場合に指定します。 • ethernet ip：レイヤー2 フィールドの情報と、IP パケットの情報を対象とする場合に指定します。 それぞれのタイプで使用できる抽出条件は、vlan mapping rule コマンドの「VLAN マッピングルールのタイプごとの抽出条件一覧」を参照。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	新規に VLAN マッピングプロファイルを設定する際は、必ずプロファイルタイプを指定してコマンドを実行する必要があります。設定済みの VLAN マッピングプロファイルに対しては type パラメーターの指定は不要です。 VLAN マッピングプロファイル設定を削除すると、削除した VLAN マッピングプロファイル ID の switchport vlan mapping profile 設定も削除されます。
制限・注意	-
バージョン	1.08.02

使用例：VLAN マッピングプロファイル ID 1 をタイプ「ethernet」で設定する方法を示します。

```
# configure terminal
(config)# vlan mapping profile 1 type ethernet
(config-vlan-map)#
```

5.19.5 vlan mapping rule

vlan mapping rule	
目的	VLAN マッピングプロファイルの VLAN マッピングルールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	rule [SEQ] match CONDITION dot1q-tunnel outer-vid VLAN-ID [priority COS-VALUE] [inner-vid VLAN-ID] rule [SEQ] match CONDITION translate outer-vid VLAN-ID [priority COS-

vlan mapping rule	
	VALUE] no rule SEQ [,|-]
Parameter	SEQ（省略可能）：VLAN マッピングルールのシーケンス番号を 1～10000 の範囲で指定します。小さい番号ほど、ルールの優先度が高くなります。 CONDITION：使用する抽出条件を指定します。詳細は「VLAN マッピングルールのタイプごとの抽出条件一覧」と「VLAN マッピングルールの抽出条件」を参照。 dot1q-tunnel outer-vid VLAN-ID：抽出条件に一致したフレームを受信する VLAN を指定します。 priority COS-VALUE（省略可能）：受信フレームの CoS 値を指定します。指定しない場合は、自動的に 0 として設定されます。 inner-vid VLAN-ID（省略可能）：タグなしフレームを受信した場合に、指定した VLAN ID のカスタマーVLAN タグを付加して受信します。 translate outer-vid VLAN-ID：抽出条件に一致したフレームがカスタマーVLAN のタグ付きフレームの場合に、そのカスタマーVLAN タグを削除して受信する VLAN を指定します。
デフォルト	なし
モード	VLAN マッピングプロファイル設定モード
特権レベル	レベル：12
ガイドライン	シーケンス番号を指定しない場合は、開始値 10 から増分値 10 でインクリメントした番号のうち、まだ使用されていない一番小さい番号が自動的に割り当てられます。 抽出条件「送信元 MAC アドレス」と「宛先 MAC アドレス」で指定する MAC アドレスは、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） inner-vid オプションは、受信フレームがタグなしフレームの場合にのみ動作します。 複数の異なるタイプの VLAN マッピングプロファイルを、1 つのインターフェースに設定することもできます。
制限・注意	-
バージョン	1.08.02

■ VLAN マッピングルールのタイプごとの抽出条件一覧

タイプ	使用できる抽出条件
ethernet	送信元 MAC アドレス、宛先 MAC アドレス、カスタマーVLAN タグの CoS 値、カスタマーVLAN タグの VLAN ID、イーサタイプ
ip	送信元 IP アドレス、宛先 IP アドレス、DSCP、送信元 L4 ポート番号、宛先 L4 ポート番号、IP プロトコル番号
ipv6	送信元 IPv6 アドレス、宛先 IPv6 アドレス

タイプ	使用できる抽出条件
ethernet ip	送信元 MAC アドレス、宛先 MAC アドレス、カスタマーVLAN タグの CoS 値、カスタマーVLAN タグの VLAN ID、イーサタイプ、送信元 IP アドレス、宛先 IP アドレス、送信元 L4 ポート番号、宛先 L4 ポート番号、IP プロトコル番号

※ 複数の抽出条件を指定する場合は、この表に記載した先頭の抽出条件から順番に指定する。

■ VLAN マッピングルールの抽出条件

抽出条件	概要
送信元 MAC アドレス	src-mac SRC-MAC-ADDR：送信元 MAC アドレスを指定
宛先 MAC アドレス	dst-mac DST-MAC-ADDR：宛先 MAC アドレスを指定
CoS	priority COS-VALUE：カスタマーVLAN タグの優先度を 0～7 の範囲で指定
VLAN ID	inner-vid VLAN-ID：カスタマーVLAN タグの VLAN ID を 1～4094 の範囲で指定
イーサタイプ	ether-type TYPE：イーサタイプを 0x0～0xFFFF の範囲で指定
送信元 IP アドレス	src-ip SRC-IP-ADDR/MASK：送信元 IPv4 アドレスを指定
宛先 IP アドレス	dst-ip DST-IP-ADDR/MASK：宛先 IPv4 アドレスを指定
DSCP	dscp DSCP：DSCP を 0～63 の範囲で指定します。
送信元 L4 ポート番号	src-port SRC-L4-PORT：送信元 TCP/UDP ポート番号を 1～65535 の範囲で指定
宛先 L4 ポート番号	dst-port DST-L4-PORT：宛先 TCP/UDP ポート番号を 1～65535 の範囲で指定
IP プロトコル番号	ip-protocol ID：IP プロトコル番号を 0～255 の範囲で指定
送信元 IPv6 アドレス	src-ipv6 SRC-IPV6-ADDR/LENGTH：送信元 IPv6 アドレスを指定
宛先 IPv6 アドレス	dst-ipv6 DST-IPV6-ADDR/LENGTH：宛先 IPv6 アドレスを指定

使用例：VLAN マッピングプロファイル ID 1 をタイプ「ip」で設定し、以下の VLAN マッピングルールを設定する方法を示します。

- ルール 10、抽出条件「送信元 IPv4 アドレス 100.1.1.0/24」の場合、VLAN 100 で受信
- ルール 20、抽出条件「宛先 IPv4 アドレス 200.1.1.0/24」の場合、VLAN 200 で受信

```
# configure terminal
(config)# vlan mapping profile 1 type ip
(config-vlan-map)# rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel outer-vid 100
(config-vlan-map)# rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel outer-vid 200
(config-vlan-map)#
```

5.19.6 switchport vlan mapping profile

switchport vlan mapping profile	
目的	トンネルモードに設定したインターフェースに、VLAN マッピングプロファイルを適用します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	switchport vlan mapping profile ID no switchport vlan mapping profile ID
Parameter	ID：VLAN マッピングプロファイル ID を 1～1000 の範囲で指定します。
デフォルト	なし

switchport vlan mapping profile	
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード (interface port-channel コマンド) で設定してください。 本設定はトンネルポートで設定できます。 VLAN マッピングプロファイルが適用されている場合、VLAN マッピングルールに一致した受信フレームは、そのマッピングルールで指定された VLAN で受信します。 複数の VLAN マッピングプロファイルを、1 つのインターフェースに設定することもできます。

制限・注意	• vlan mapping profile 設定を削除すると、削除した VLAN マッピングプロファイル ID に関連する本設定も削除されます。
	• 対象インターフェースの VLAN モードをトンネルモード以外に変更すると、本設定も削除されます。
	• ApresiaNP2500 シリーズでは、装置で同時に適用できる VLAN マッピングプロファイルの組み合わせに以下の仕様制限があります。
	  • 以下の状況では、新たに ethernet ip タイプの VLAN マッピングプロファイルを適用できません。
	  • ethernet/ipv6 タイプの 2 種類が適用済み
	  • ip/ipv6 タイプの 2 種類が適用済み
	  • 以下の状況では、新たに ipv6 タイプの VLAN マッピングプロファイルを適用できません。
	  • ethernet/ethernet ip タイプの 2 種類が適用済み
	  • ip/ethernet ip タイプの 2 種類が適用済み
	  • 以下の状況では、新たに ethernet タイプ、または ip タイプの VLAN マッピングプロファイルを適用できません。
	  • ipv6/ethernet ip タイプの 2 種類が適用済み

バージョン	1.08.02

使用例：トンネルモードに設定したポート 1/0/1 で、VLAN マッピングプロファイル ID 1 を適用する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode dot1q-tunnel
(config-if-port)# switchport vlan mapping profile 1
(config-if-port)#
```

5.19.7 vlan mapping miss drop

vlan mapping miss drop	
目的	トンネルポートで受信したカスタマーVLAN タグ付きフレームが、VLAN マッピングに一致しない場合に破棄する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	vlan mapping miss drop no vlan mapping miss drop
Parameter	なし

vlan mapping miss drop	
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はトンネルポートで設定できます。 本機能を有効にすると、トンネルポートで受信したカスタマーVLAN タグ付きフレームが、サービス VLAN マッピングエントリー（switchport vlan mapping original-vlan dot1q-tunnel コマンド）、もしくは VLAN マッピングルール（vlan mapping rule コマンド）に一致しない場合に破棄されます。 本機能は受信フレームがタグなしフレームの場合は対象外で、VLAN マッピングに一致しない場合でも破棄されません。
制限・注意	• 対象インターフェースの VLAN モードをトンネルモード以外に変更すると、本設定も削除されます。
バージョン	1.08.02

使用例：トンネルモードに設定したポート 1/0/1 で、受信したカスタマーVLAN タグ付きフレームが VLAN マッピングに一致しない場合に破棄する機能を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode dot1q-tunnel
(config-if-port)# vlan mapping miss drop
(config-if-port)#
```

5.19.8 dot1q-tunnel trust inner-priority

dot1q-tunnel trust inner-priority	
目的	トンネルポートで受信したカスタマーVLAN タグ付きフレームの優先度を反映して受信する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	dot1q-tunnel trust inner-priority no dot1q-tunnel trust inner-priority
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はトンネルポートで設定できます。 本機能を有効にしたトンネルポートで受信したカスタマーVLAN タグ付きフレームの、カスタマーVLAN タグの優先度をそのフレームの CoS 値として反映して受信します。 本機能とサービス VLAN マッピングエントリー（switchport vlan mapping original-vlan dot1q-tunnel コマンド）の priority オプションでは、本機能の方が優先されます。

dot1q-tunnel trust inner-priority	
	本機能と VLAN マッピングルール（vlan mapping rule コマンド）の priority オプションでは、VLAN マッピングルールの priority オプションの方が優先されます。
制限・注意	• 対象インターフェースの VLAN モードをトンネルモード以外に変更すると、本設定も削除されます。
バージョン	1.08.02

使用例：トンネルモードに設定したポート 1/0/1 で、受信したカスタマーVLAN タグ付きフレームの優先度を反映して受信する機能を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode dot1q-tunnel
(config-if-port)# dot1q-tunnel trust inner-priority
(config-if-port)#
```

5.19.9 dot1q-tunnel insert dot1q-tag

dot1q-tunnel insert dot1q-tag	
目的	トンネルポートで受信したタグなしフレームに、カスタマーVLAN タグを挿入して受信する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	dot1q-tunnel insert dot1q-tag DOT1Q-VLAN no dot1q-tunnel insert dot1q-tag
Parameter	DOT1Q-VLAN：挿入するカスタマーVLAN タグの VLAN ID を指定します。
デフォルト	なし
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 本設定はトンネルポートで設定できます。 本機能を有効にしたトンネルポートでは、送信する際にカスタマーVLAN タグが削除されてタグなしフレームとして送信されます。 本機能は VLAN マッピングルール（vlan mapping rule コマンド）に一致して受信したタグなしフレームに対しては動作しません。
制限・注意	• 対象インターフェースの VLAN モードをトンネルモード以外に変更すると、本設定も削除されます。
バージョン	1.08.02

使用例：トンネルモードに設定したポート 1/0/1 で、受信したタグなしフレームに VLAN 10 のカスタマーVLAN タグを挿入して受信する機能を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport mode dot1q-tunnel
(config-if-port)# dot1q-tunnel insert dot1q-tag 10
(config-if-port)#
```

5.19.10 show dot1q ethertype

show dot1q ethertype	
目的	装置のカスタマーVLAN タグの TPID 設定と、トランクポートのサービスプロバイダーVLAN タグの TPID 設定を表示します。
Command	show dot1q ethertype [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、装置のカスタマーVLAN タグの TPID 設定と、すべてのトランクポートのサービスプロバイダーVLAN タグの TPID 設定が表示されます。 トランクポート以外のインターフェースを指定して実行しても表示されません。
制限・注意	-
バージョン	1.08.02

使用例：装置のカスタマーVLAN タグの TPID 設定と、すべてのトランクポートのサービスプロバイダーVLAN タグの TPID 設定を表示する方法を示します。

```
# show dot1q ethertype

 802.1q inner Ethernet Type is 0x8100 ...(1)
Port1/0/2 ...(2)
  802.1q tunneling Ethernet Type is 0x8100 ...(3)
Port1/0/11
  802.1q tunneling Ethernet Type is 0x8100
Port-channel2
  802.1q tunneling Ethernet Type is 0x8100
```

項番	説明
(1)	装置全体のカスタマーVLAN タグの TPID 設定を表示します。
(2)	VLAN 動作モードがトランクモードのポート番号またはポートチャネル番号を表示します。
(3)	サービスプロバイダーVLAN タグの TPID 設定を表示します。

5.19.11 show vlan mapping

show vlan mapping	
目的	サービス VLAN マッピングエントリーと VLAN 変換エントリーの設定を表示します。
Command	show vlan mapping [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのサービス VLAN マッピングエ

show vlan mapping	
	ントリーと VLAN 変換エントリーの設定が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：すべてのサービス VLAN マッピングエントリーと VLAN 変換エントリーの設定を表示する方法を示します。

```
# show vlan mapping
(1)              (2)             (3)                  (4)       (5)
Interface        Original VLAN   Translated VLAN      Priority  Status
---------------  --------------  -------------------  --------  --------
Port1/0/1        2               dot1q-tunnel 10      5         Active
Port1/0/1        3               dot1q-tunnel 20      0         Active
Port1/0/5        1001            translate 10         0         Active
Port1/0/5        1002            translate 20         3         Active
Port1/0/7        101/1234        translate 10/111     2         Active
Port1/0/7        102/2345        translate 20/222     0         Active
Port-channel1    500             dot1q-tunnel 600     5         Active
Port-channel2    2001            translate 30         0         Active
Port-channel2    2002/50         translate 40/555     3         Active

Total Entries: 9
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	サービス VLAN マッピングエントリーの場合は「受信フレームのカスタマーVLAN」を表示します。 トランクポートに適用した VLAN 変換エントリーの場合は「装置外でのサービス VLAN」、もしくは「装置外でのサービス VLAN/装置外でのカスタマーVLAN」を表示します。 トンネルポートに適用した VLAN 変換エントリーの場合は「装置外でのカスタマーVLAN」を表示します。
(3)	dot1q-tunnel はサービス VLAN マッピングエントリーを、translate は VLAN 変換エントリーを意味します。 サービス VLAN マッピングエントリーの場合は「受信するサービス VLAN」を表示します。 VLAN 変換エントリーの場合は「装置内でのサービス VLAN」、もしくは「装置内でのサービス VLAN/装置内でのカスタマーVLAN」を表示します。
(4)	受信時にエントリーに一致したフレームに反映する優先度を表示します。
(5)	エントリーのステータスを表示します。

5.19.12 show dot1q-tunnel

show dot1q-tunnel	
目的	トンネルポート関連の設定を表示します。
Command	show dot1q-tunnel [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード

show dot1q-tunnel	
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのトンネルポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：すべてのトンネルポートの設定を表示する方法を示します。

```
# show dot1q-tunnel

dot1q Tunnel Interface: Port1/0/1 ...(1)
  Trust inner priority       : Disabled ...(2)
  VLAN mapping miss drop     : Disabled ...(3)
  Insert dot1q tag           : VLAN 111 ...(4)
  VLAN mapping profiles      : 1 ...(5)

dot1q Tunnel Interface: Port1/0/12
  Trust inner priority       : Disabled
  VLAN mapping miss drop     : Enabled

dot1q Tunnel Interface: Port-channel1
  Trust inner priority       : Enabled
  VLAN mapping miss drop     : Disabled
```

項番	説明
(1)	VLAN 動作モードがトンネルモードのポート番号またはポートチャネル番号を表示します。
(2)	受信カスタマーVLAN タグの、優先度反映オプションの有効(Enabled)／無効(Disabled)を表示します。
(3)	VLAN マッピングに一致しないカスタマーVLAN タグ付きフレームの、受信破棄オプションの有効(Enabled)／無効(Disabled)を表示します。
(4)	受信タグなしフレームへのカスタマーVLAN タグの付加オプション有効時に、付加するカスタマーVLAN タグの VLAN ID を表示します。無効（デフォルト設定）の場合は表示されません。
(5)	インターフェースに適用されている VLAN マッピングプロファイルを表示します。未設定の場合は表示されません。

5.19.13 show vlan mapping profile

show vlan mapping profile	
目的	VLAN マッピングプロファイルの設定を表示します。
Command	show vlan mapping profile [ID]
Parameter	ID（省略可能）：VLAN マッピングプロファイル ID を 1～1000 の範囲で指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定の VLAN マッピングプロファイル ID を指定しない場合は、すべての VLAN マッピングプロファイルの情報が表示されます。
制限・注意	-

バージョン	1.08.02

使用例：すべての VLAN マッピングプロファイルの設定を表示する方法を示します。

```
# show vlan mapping profile
(1)                     (2)
VLAN mapping profile:1  type:ip
     (3)
    rule 10 match src-ip 10.1.1.100/32, action dot1q-tunnel outer-vid 10, priority 4
    rule 20 match src-ip 10.1.1.200/32, action dot1q-tunnel outer-vid 20, priority 0
Total Entries: 2
VLAN mapping profile:2  type:ethernet
    rule 10 match src-mac 00-00-11-11-22-22, action translate outer-vid 30, priority 3
    rule 20 match src-mac 00-AA-BB-CC-DD-EE, action translate outer-vid 40, priority 1
Total Entries: 2
```

項番	説明
(1)	VLAN マッピングプロファイル ID を表示します。
(2)	VLAN マッピングプロファイルタイプを表示します。
(3)	VLAN マッピングルールを表示します。

5.20 Voice VLAN コマンド

Voice VLAN 関連の設定コマンドは以下のとおりです。

- voice vlan
- voice vlan qos
- voice vlan dscp
- voice vlan aging
- voice vlan mac-address
- voice vlan mode
- voice vlan enable

Voice VLAN 関連の show コマンドは以下のとおりです。

- show voice vlan
- show voice vlan device
- show voice vlan lldp-med device

5.20.1 voice vlan

voice vlan	
目的	Voice VLAN として使用する VLAN ID を指定して、Voice VLAN を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	voice vlan VLAN-ID no voice vlan
Parameter	VLAN-ID：Voice VLAN の VLAN ID を 2～4094 の範囲で指定します。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	Voice VLAN として設定できる VLAN は装置で 1 つです。 Voice VLAN を動作させるためには、対象インターフェースで voice vlan enable コマンドの設定も必要です。 Voice VLAN を動作させると、アクセスリストの Ingress グループを 1 グループ使用します。 Voice VLAN が有効なインターフェースでは、受信したトラフィックの送信元 MAC アドレスが voice vlan mac-address コマンドで指定した MAC アドレスと一致した場合、その MAC アドレスの端末は Voice VLAN 端末として登録されます。そして、その Voice VLAN 端末からのトラフィックは音声パケットとみなされ、Voice VLAN で受信して転送されます。 LLDP-MED が有効な場合、Voice VLAN が有効なインターフェースで対応する LLDP-MED を受信すると、LLDP-MED 端末として登録されます。そして、受信した Network Policy TLV の優先度が反映されて転送されます。なお、送信元 MAC アドレスが voice vlan mac-address コマンドで指定した MAC アドレスと一致した場合は、Voice VLAN で設定した優先度が反映されます。
制限・注意	• 登録可能な Voice VLAN 端末は、装置全体で最大 1024 端末です。端末数が最大に到達していない場合でも、ハードウェアの制限で Voice VLAN 端末として登録されないことがあります。

voice vlan	
	• 登録可能な LLDP-MED 端末は、装置全体で最大 128 端末です。 • Voice VLAN には VLAN 1 は指定できません。また、未設定の VLAN ID を指定しても設定できません。 • Voice VLAN として設定された VLAN は、Voice VLAN が有効な状態では削除／変更できません。 • Voice VLAN 機能を使用する場合は、AccessDefender の動的 VLAN 割り当てを使用しないでください。
バージョン	1.08.02

使用例：Voice VLAN として VLAN 1000 を指定して有効にする方法を示します。

```
# configure terminal
(config)# voice vlan 1000
(config)#
```

5.20.2 voice vlan qos

voice vlan qos	
目的	受信した Voice VLAN トラフィックの CoS 値を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	voice vlan qos COS-VALUE no voice vlan qos
Parameter	COS-VALUE：受信フレームの CoS 値を、0～7 の範囲で指定します。
デフォルト	CoS 値：5
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドにより、Voice VLAN が有効なインターフェースで受信した Voice VLAN 端末からの音声パケットが、指定された CoS 値にマーキングされます。 Voice VLAN 端末からの音声パケットがタグ付きの場合、パケットの 802.1p 優先度は無視され、本コマンドで設定された CoS 値で動作します。
制限・注意	-
バージョン	1.08.02

使用例：受信した Voice VLAN トラフィックの CoS 値を 6 に設定する方法を示します。

```
# configure terminal
(config)# voice vlan qos 6
(config)#
```

5.20.3 voice vlan dscp

voice vlan dscp	
目的	受信した Voice VLAN トラフィックの DSCP を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	voice vlan dscp VALUE no voice vlan dscp

voice vlan dscp	
Parameter	VALUE：DSCP を 0～63 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドにより、Voice VLAN が有効なインターフェースで受信した Voice VLAN 端末からの音声パケットが、指定された DSCP にマーキングされます。 本設定がデフォルト設定の場合、Voice VLAN 端末の音声パケットの DSCP は変更されません。
制限・注意	-
バージョン	1.08.02

使用例：受信した Voice VLAN トラフィックの DSCP を 46 に設定する方法を示します。

```
# configure terminal
(config)# voice vlan dscp 46
(config)#
```

5.20.4 voice vlan aging

voice vlan aging	
目的	Voice VLAN 端末のエージングタイムを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	voice vlan aging MINUTES no voice vlan aging
Parameter	MINUTES：エージングタイムを 1～65,535 分の範囲で指定します。
デフォルト	720 分
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	Voice VLAN 端末からの音声パケットが停止し、その端末の MAC アドレスが MAC アドレステーブルからエージングタイムアウトして削除されると、Voice VLAN 端末のエージングタイマーが開始されます。その後、エージングタイマーが満了すると対象の Voice VLAN 端末が削除されます。 Voice VLAN の動作モードが自動モードの場合、対象のインターフェースからすべての Voice VLAN 端末が削除されると、自動的に割り当てた VLAN も削除されます。
制限・注意	-
バージョン	1.08.02

使用例：Voice VLAN 端末のエージングタイムを 30 分に設定する方法を示します。

```
# configure terminal
(config)# voice vlan aging 30
(config)#
```

5.20.5 voice vlan mac-address

voice vlan mac-address	
目的	Voice VLAN 端末として認識する MAC アドレスを設定します。設定を削除する場合

voice vlan mac-address	
	は、no 形式のコマンドを使用します。
Command	voice vlan mac-address MAC-ADDRESS MASK [description STRING] no voice vlan mac-address MAC-ADDRESS MASK
Parameter	MAC-ADDRESS MASK：MAC アドレスとマスクを、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） description STRING（省略可能）：OUI などの関連付ける名称を、最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、？ を除いた文字を使用可能です。スペースも使用できます。
デフォルト	以下のベンダーの OUI（MAC アドレスの上位 24 ビット）が登録済み • 00:01:E3 Siemens • 00:03:6B Cisco • 00:09:6E Avaya • 00:0F:E2 Huawei&3COM • 00:60:B9 NEC&Philips • 00:D0:1E Pingtel • 00:E0:75 Veritel • 00:E0:BB 3COM
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	受信したトラフィックの送信元 MAC アドレスが本設定で指定した MAC アドレスと一致した場合に、Voice VLAN 端末として登録されます。
制限・注意	• デフォルト設定以外で設定可能な MAC アドレスは最大 8 個です。 • デフォルト設定の MAC アドレスは削除できません。 • Voice VLAN が有効な状態で本設定を変更した場合は、Voice VLAN をいったん無効にしてから再度有効にしてください。
バージョン	1.08.02

使用例：MAC アドレスが 00:40:66:00:00:00、マスクが FF:FF:FF:00:00:00、名称が Apresia で、Voice VLAN 端末として認識する MAC アドレスを設定する方法を示します。

```
# configure terminal
(config)# voice vlan mac-address 0040.6600.0000 ffff.ff00.0000 description Apresia
(config)#
```

5.20.6 voice vlan mode

voice vlan mode	
目的	Voice VLAN の動作モードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	voice vlan mode {auto untag | auto tag | manual} no voice vlan mode

voice vlan mode	
Parameter	auto untag：自動モード(untag) auto tag：自動モード(tag) manual：マニュアルモード
デフォルト	自動モード(untag)
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード (interface port-channel コマンド) で設定してください。 Voice VLAN は、アクセスモード、またはハイブリッドモードのインターフェースで設定できます。 自動モード(untag)の場合、Voice VLAN 端末が登録されると、対象インターフェースに Voice VLAN がタグなしメンバーとして割り当てられます。 自動モード(tag)の場合、Voice VLAN 端末が登録されると、対象インターフェースに Voice VLAN がタグ付きメンバーとして割り当てられます。なお、自動モード(tag)の場合は、対象インターフェースの ingress-checking を無効に設定してください。 マニュアルモードの場合、switchport hybrid allowed vlan コマンドで Voice VLAN をタグ付き、またはタグなしメンバーとして、あらかじめ割り当てておく必要があります。 受信する音声パケットが VLAN タグなし形式、または VID=0 のタグ付き形式の場合は、LLDP-MED との併用はしないでください。
制限・注意	• Voice VLAN の動作モードが自動モード(untag, tag)で、対象インターフェースに最初に登録された端末が LLDP-MED 端末の場合、割り当てられる Voice VLAN のタグなし／タグ付きは、受信した Network Policy TLV の tagged フラグに従います。
バージョン	1.08.02

使用例：ポート 1/0/1 で Voice VLAN の動作モードをマニュアルモードに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# voice vlan mode manual
(config-if-port)#
```

5.20.7 voice vlan enable

voice vlan enable	
目的	インターフェースの Voice VLAN を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	voice vlan enable no voice vlan enable
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)

voice vlan enable	
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。 Voice VLAN は、アクセスモード、またはハイブリッドモードのインターフェースで設定できます。 Voice VLAN を動作させるためには、グローバル設定モードで voice vlan コマンドの設定も必要です。 Voice VLAN を動作させると、アクセスリストの Ingress グループを 1 グループ使用します。
制限・注意	• Voice VLAN 機能を使用する場合は、AccessDefender の動的 VLAN 割り当てを使用しないでください。
バージョン	1.08.02

使用例：ポート 1/0/1 で Voice VLAN を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# voice vlan enable
(config-if-port)#
```

5.20.8 show voice vlan

show voice vlan	
目的	Voice VLAN の設定を表示します。
Command	show voice vlan [interface [IF-ID [,|-]]]
Parameter	interface（省略可能）：インターフェースの Voice VLAN 関連の設定を表示する場合に指定します。 IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、グローバル設定モードの設定を表示します。 interface パラメーターを指定して特定のインターフェースを指定しない場合は、すべてのインターフェースの Voice VLAN 関連の設定が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：Voice VLAN の設定を表示する方法を示します。

```
# show voice vlan

 Voice VLAN ID          : 2 ...(1)
 Voice VLAN CoS         : 5 ...(2)
 Dscp                   : Disable ...(3)
 Aging Time             : 720 minutes ...(4)
```

```
Member Ports          : 1/0/1-1/0/2,1/0/5-1/0/6 ...(5)
Dynamic Member Ports : 1/0/1-1/0/2 ...(6)

Voice VLAN OUI        : ...(7)

OUI Address         Mask                Description
------------------  ------------------  --------------
00-01-E3-00-00-00   FF-FF-FF-00-00-00   Siemens
00-03-6B-00-00-00   FF-FF-FF-00-00-00   Cisco
00-09-6E-00-00-00   FF-FF-FF-00-00-00   Avaya
00-0F-E2-00-00-00   FF-FF-FF-00-00-00   Huawei&3COM
00-60-B9-00-00-00   FF-FF-FF-00-00-00   NEC&Philips
00-D0-1E-00-00-00   FF-FF-FF-00-00-00   Pingtel
00-E0-75-00-00-00   FF-FF-FF-00-00-00   Veritel
00-E0-BB-00-00-00   FF-FF-FF-00-00-00   3COM

Total OUI: 8
```

項番	説明
(1)	Voice VLAN の VLAN ID を表示します。
(2)	Voice VLAN の CoS 値を表示します。
(3)	Voice VLAN の DSCP を表示します。未設定時は Disable と表示されます。
(4)	Voice VLAN 端末のエージングタイムの設定値を表示します。
(5)	Voice VLAN を有効にしたポート番号を表示します。ポートチャネルの場合はメンバーポートのポート番号が表示されます。
(6)	動作モードが自動モード(untag, tag)の場合に、自動的に Voice VLAN に割り当てられたポート番号を標示します。ポートチャネルが自動的に割り当てられた場合は、すべてのメンバーポートのポート番号が表示されます。
(7)	Voice VLAN 端末として登録する MAC アドレスを表示します。

使用例：ポート 1/0/5～1/0/7 の Voice VLAN の設定を表示する方法を示します。

```
# show voice vlan interface port 1/0/5-7
 (1)              (2)        (3)
 Interface        State      Mode
 ---------------  ---------  -----------
 Port1/0/5        Enabled    Auto/Untag
 Port1/0/6        Enabled    Manual
 Port1/0/7        Disabled   Auto/Untag
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	Voice VLAN の有効(Enabled)／無効(Disabled)を表示します。
(3)	Voice VLAN の動作モードを表示します。 Auto/Untag：自動モード(untag) Auto/Tag：自動モード(tag) Manual：マニュアルモード

5.20.9 show voice vlan device

show voice vlan device	
目的	Voice VLAN 端末を表示します。

show voice vlan device	
Command	show voice vlan device [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：Voice VLAN 端末を表示する方法を示します。

```
# show voice vlan device
 (1)              (2)                (3)                (4)
 Interface        Voice Device       Start Time         Status
 ---------------  -----------------  -----------------  ------
 Port1/0/2        00-01-E3-33-33-33  2020-03-05 16:11   Active
 Port-channel5    00-01-E3-11-11-11  2020-03-05 16:10   Aging
 Port-channel5    00-01-E3-22-22-22  2020-03-05 16:10   Active

 Total Entries: 3
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	Voice VLAN 端末の MAC アドレスを表示します。
(3)	Voice VLAN 端末が登録された日時を表示します。
(4)	Voice VLAN 端末の状態を表示します。 Active：Voice VLAN 端末の MAC アドレスが MAC アドレステーブルに登録されている状態 Aging：Voice VLAN 端末の MAC アドレスが MAC アドレステーブルから削除され、Voice VLAN 端末のエージングタイマーが開始している状態

5.20.10 show voice vlan lldp-med device

show voice vlan lldp-med device	
目的	LLDP-MED 端末を表示します。
Command	show voice vlan lldp-med device [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	-

show voice vlan lldp-med device	
バージョン	1.08.02

使用例：LLDP-MED 端末を表示する方法を示します。

```
# show voice vlan lldp-med device

 Index               : 1 ...(1)
 Interface           : Port1/0/2 ...(2)
 Chassis ID Subtype  : Network Address ...(3)
 Chassis ID          : 10.1.2.3 ...(4)
 Port ID Subtype     : MAC Address ...(5)
 Port ID             : 00-40-66-11-11-11 ...(6)
 Create Time         : 3/5/2020  16:25:55 ...(7)
 Remain Time         : 120 Seconds ...(8)

 Index               : 2
 Interface           : Port-channel5
 Chassis ID Subtype  : Network Address
 Chassis ID          : 20.1.1.1
 Port ID Subtype     : MAC Address
 Port ID             : 00-40-66-22-22-22
 Create Time         : 3/5/2020  16:25:56
 Remain Time         : 120 Seconds
```

項番	説明
(1)	登録番号を表示します。
(2)	ポート番号またはポートチャネル番号を表示します。
(3)	LLDP-MED 端末から通知された、Chassis ID TLV のサブタイプを表示します。
(4)	LLDP-MED 端末から Chassis ID TLV で通知された、Chassis ID 情報を表示します。
(5)	LLDP-MED 端末から通知された、Port ID TLV のサブタイプを表示します。
(6)	LLDP-MED 端末から Port ID TLV で通知された、Port ID 情報を表示します。
(7)	登録された日時を表示します。
(8)	エージングタイムアウトまでの残り時間を表示します。

5.21 ポートセキュリティーコマンド

ポートセキュリティー関連の設定コマンドは以下のとおりです。

- port-security limit global
- switchport port-security
- switchport port-security maximum
- switchport port-security mode
- switchport port-security mac-address
- switchport port-security violation
- switchport port-security aging time
- switchport port-security aging type
- errdisable recovery cause psecure-violation

ポートセキュリティー関連の show／操作コマンドは以下のとおりです。

- show port-security
- show port-security address
- clear port-security

5.21.1 port-security limit global

port-security limit global	
目的	ポートセキュリティー機能で許可する MAC アドレスの、装置全体の最大数を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	port-security limit global VALUE no port-security limit global
Parameter	VALUE：許可する MAC アドレスの装置全体の最大数を、1～12,288 の範囲で指定します。
デフォルト	設定なし（未設定時は装置全体の最大数は 12,288 で動作）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	switchport port-security violation コマンドが restrict または shutdown で設定されている場合は、装置全体の最大数を超過したことを検知すると、それを知らせるログ（Limit on system entry number has been exceeded）が出力されます。
制限・注意	• すでにポートセキュリティー機能で登録したエントリーが存在する場合、その数よりも少ない値を指定して装置全体の最大数を設定することはできません。
バージョン	1.12.01

使用例：ポートセキュリティー機能で許可する MAC アドレスの装置全体の最大数を 24 に設定する方法を示します。

```
# configure terminal
(config)# port-security limit global 24
(config)#
```

5.21.2 switchport port-security

switchport port-security	
目的	ポートセキュリティー機能を有効にします。無効にする場合は、no 形式のコマンドを

switchport port-security	
	使用します。
Command	switchport port-security no switchport port-security
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	ポートセキュリティー機能を有効にしたポートでは、登録された MAC アドレスからの通信のみ許可し、許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を破棄します。許可する MAC アドレスは switchport port-security mac-address コマンドで手動で設定します。また、ポートごとの最大数まで空きがある状態では、受信した順に最大数まで動的に登録されます。 ポートセキュリティー機能で手動または動的に登録されたエントリーは、show port-security address コマンドで確認します。show mac-address-table コマンドでも「タイプ：Static」のエントリーとして表示されますが、スタティック MAC アドレスエントリーとは別扱いのため、show mac-address-table static コマンドでは表示されません。
制限・注意	• ポートセキュリティー機能は、AccessDefender による認証が有効なポートや、ポートチャネルのメンバーポートでは併用できません。 • ポートセキュリティー機能を有効にすると、対象ポートで学習済みの MAC アドレスエントリーは削除されます。 • ポートセキュリティー機能を無効にすると、対象ポートで動的に登録されたエントリーは削除されます。 • 一般的に、ポートセキュリティー機能は不正な端末からのアクセスを防止するために、エッジスイッチの端末を収容するアクセス側のポートで使用します。冗長プロトコルの制御パケットなどを中継する幹線ポートで使用すると、制御パケットが中継されずに冗長プロトコルが正常に動作しなくなるため、幹線ポートではポートセキュリティー機能を使用しないでください。
バージョン	1.12.01

使用例：ポート 1/0/1 でポートセキュリティー機能を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport port-security
(config-if-port)#
```

5.21.3 switchport port-security maximum

switchport port-security maximum	
目的	ポートセキュリティー機能で許可する MAC アドレスの、ポートごとの最大数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport port-security maximum VALUE no switchport port-security maximum
Parameter	VALUE：許可する MAC アドレスのポートごとの最大数を、1～12,288 の範囲で指定します。

switchport port-security maximum	
デフォルト	32
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	ポートごとの最大数を、switchport port-security mac-address コマンドで手動で設定するエントリー数と同じにすることで、動的なエントリーの登録を防止できます。 switchport port-security violation コマンドが restrict または shutdown で設定されている場合は、ポートごとの最大数を超過したことを検知すると、それを知らせるログ（MAC address <mac-address> causes port security violation on Port<port>）が出力されます。なお、このログを出力してから約 1 分間は、新たに超過したことを検知してもログは出力されません。
制限・注意	• すでにポートセキュリティー機能で登録したエントリーが存在する場合、その数よりも少ない値を指定してポートごとの最大数を設定することはできません。
バージョン	1.12.01

使用例：ポート 1/0/1 で、ポートセキュリティー機能で許可する MAC アドレスのポートごとの最大数を 2 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport port-security maximum 2
(config-if-port)#
```

5.21.4 switchport port-security mode

switchport port-security mode	
目的	動的に登録されるエントリーの動作モードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport port-security mode {delete-on-timeout | permanent} no switchport port-security mode
Parameter	delete-on-timeout：動的に登録されたエントリーをエージングタイムアウト対象にする場合に指定します。 permanent：動的に登録されたエントリーをエージングタイムアウト対象にしないで、自動的にエントリー設定を追加する場合に指定します。
デフォルト	delete-on-timeout
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	delete-on-timeout モードの場合、動的に登録されたエントリーは、エージングタイムアウトすると削除されます。 permanent モードの場合、動的に登録されると、構成情報(running-config)にもエントリー設定（permanent パラメーター指定の switchport port-security mac-address コマンド設定）が自動的に追加されます。この状態で設定を保存すると、次回起動時にもエントリー設定を引き継ぐことができます。
制限・注意	• permanent モードから delete-on-timeout モードに変更すると、対象ポートに設定済みの permanent パラメーター指定のエントリー設定は削除されます。
バージョン	1.12.01

使用例：ポート 1/0/1 で、動的に登録されるエントリーの動作モードを permanent モードに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport port-security mode permanent
(config-if-port)#
```

5.21.5 switchport port-security mac-address

switchport port-security mac-address	
目的	ポートセキュリティー機能のエントリーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	switchport port-security mac-address [permanent] MAC-ADDRESS [vlan VLAN-ID] no switchport port-security mac-address [permanent] MAC-ADDRESS [vlan VLAN-ID]
Parameter	permanent（省略可能）：動的に登録されて自動的に設定が追加されたエントリーとする場合に指定します。 MAC-ADDRESS：許可する MAC アドレスを、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） vlan VLAN-ID（省略可能）：エントリーの VLAN ID を 1～4094 の範囲で指定します。設定時に省略した場合は、対象ポートのアクセス VLAN、またはネイティブ VLAN の VLAN ID が自動的に付与されます。
デフォルト	なし
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	本コマンドで、ポートセキュリティー機能で通信を許可する MAC アドレスを設定します。permanent パラメーターを指定して手動で設定することもできますが、通常は permanent パラメーター未指定のコマンド形式で設定します。 動的に登録されるエントリーの動作モードが permanent モードの場合は、動的に登録されると、構成情報(running-config)にも permanent パラメーター指定のエントリー設定が自動的に追加されます。 permanent パラメーター指定のエントリーは clear port-security コマンドでの削除対象になります。削除されると、構成情報(running-config)の設定も削除されます。
制限・注意	• 同一エントリー（同じ MAC アドレス／同じ VLAN ID）を、複数ポートに登録することはできません。 • すでに装置全体の最大数まで登録されている状態、またはすでにポートごとの最大数まで登録されている状態では、新たにエントリーを設定できません。 • 以下ポートでは、permanent パラメーター指定のエントリーは設定できません。 • ポートセキュリティー機能が無効なポート

switchport port-security mac-address	
	• delete-on-timeout モードのポート • 動的に登録されるエントリーの動作モードを permanent モードから delete-on-timeout モードに変更すると、対象ポートに設定済みの permanent パラメーター指定のエントリー設定は削除されます。 • ポートセキュリティー機能は、MAC アドレステーブルのリソースも使用します。MAC アドレステーブルのリソースが足りない状況では、本コマンドによるエントリー設定や、動的なエントリー登録はできません。
バージョン	1.12.01

使用例：ポート 1/0/1 で、MAC アドレスが 00:00:5E:00:53:11、VLAN ID が 20 のエントリーを設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport port-security mac-address 0000.5e00.5311 vlan 20
(config-if-port)#
```

5.21.6 switchport port-security violation

switchport port-security violation	
目的	許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport port-security violation {protect | restrict | shutdown} no switchport port-security violation
Parameter	protect：許可しない MAC アドレスからの通信を破棄する場合に指定します。 restrict：許可しない MAC アドレスからの通信を破棄し、CPU カウンターでカウント、ログ出力を行う場合に指定します。 shutdown：許可しない MAC アドレスからの通信を受信した場合に、対象ポートをシャットダウン（err-disabled 状態に変更）する場合に指定します。ログ出力も行われます。
デフォルト	許可しない MAC アドレスからの通信を破棄（protect）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	本設定を restrict に指定した場合、ポートごとの最大数を超過した場合に CPU カウンターでカウントします。CPU カウンターは show port-security コマンドで確認できます。 本設定を shutdown に指定した場合、ポートごとの最大数を超過した場合にシャットダウン（err-disabled 状態に変更）されます。シャットダウンされたポートを復旧するには、以下の 2 つの方法があります。 • errdisable recovery cause psecure-violation コマンドを使用して、ポートセキュリティー機能によって err-disabled 状態に変更されたポートの自動復旧を有効にできます。 • ポートに対して shutdown コマンドを実行した後、no shutdown コマンドを実行することで、手動でポートを復旧できます。
制限・注意	• 装置全体の最大数を超過した場合は、restrict 指定時の「CPU カウンターのカウン

switchport port-security violation	
	ト」と、shutdown 指定時の「シャットダウン（err-disabled 状態に変更）」は動作しません。いずれも、ポートごとの最大数を超過した場合に動作します。
バージョン	1.12.01

使用例：ポート 1/0/1 で、許可しない端末からの通信を受信した場合の動作を shutdown に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport port-security violation shutdown
(config-if-port)#
```

5.21.7 switchport port-security aging time

switchport port-security aging time	
目的	delete-on-timeout モードのポートにおいて、動的に登録されたエントリーのエージングタイムを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport port-security aging time MINUTES no switchport port-security aging time
Parameter	MINUTES：エージングタイムを 0～1440（分）の範囲で指定します。
デフォルト	0 分
モード	インターフェース設定モード（port, range）
特権レベル	レベル：12
ガイドライン	エージングタイムがデフォルトの 0 分設定の場合は、エージングタイムアウトは行われません。
制限・注意	-
バージョン	1.12.01

使用例：ポート 1/0/1 で、動的に登録されたエントリーのエージングタイムを 30 分に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport port-security aging time 30
(config-if-port)#
```

5.21.8 switchport port-security aging type

switchport port-security aging type	
目的	delete-on-timeout モードのポートにおいて、動的に登録されたエントリーのエージングタイムのタイプを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	switchport port-security aging type {absolute | inactivity} no switchport port-security aging type
Parameter	absolute：登録されてからの経過時間で判断する場合に指定します。 inactivity：無通信になってからの経過時間で判断する場合に指定します。
デフォルト	エントリーが登録されてからの経過時間（absolute）

switchport port-security aging type	
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	absolute タイプの場合、エントリーが登録されてから指定したエージングタイムが経過すると、対象のエントリーは削除されます。 inactivity タイプの場合、エントリーが無通信になったと判断されてから指定したエージングタイムが経過すると、対象のエントリーは削除されます。エントリーからの通信が実際に無くなってから、そのエントリーが無通信になったと判断するまでには、最大で「MAC アドレステーブルのエージングタイム（mac-address-table aging-time)」の時間がかかります。
制限・注意	-
バージョン	1.12.01

使用例：ポート 1/0/1 で、動的に登録されたエントリーのエージングタイムのタイプを inactivity に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# switchport port-security aging type inactivity
(config-if-port)#
```

5.21.9 errdisable recovery cause psecure-violation

errdisable recovery cause psecure-violation	
目的	ポートセキュリティー機能によって err-disabled 状態に変更されたポートの自動復旧を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	errdisable recovery cause psecure-violation [interval SECONDS] no errdisable recovery cause psecure-violation [interval]
Parameter	interval SECONDS（省略可能）：自動復旧するまでの待機時間を、5～86,400 秒の範囲で指定します。指定しない場合は 300 秒になります。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドの詳細や関連する show コマンドは「4.18 エラー復旧コマンド」を参照してください。 本コマンドを設定すると、ポートセキュリティー機能によって err-disabled 状態に変更されたポートを、指定した時間で自動復旧することができます。 err-disabled 状態に変更されたポートのリンク状態は、show interfaces コマンドでは "link status is down（error disabled: Port Security)" と表示されます。show interfaces status コマンドの Status 項目では "err-disabled" と表示されます。 本コマンドの設定有無にかかわらず、err-disabled 状態のポートに対して shutdown コマンドを実行した後、no shutdown コマンドを実行することで、手動でポートを復旧することもできます。
制限・注意	• 本設定は構成情報ではエラー復旧コマンド関連（ラベル# ERRDISABLE）で表示されます。 • interval パラメーターをデフォルト（300 秒）以外に指定して設定している場合に

errdisable recovery cause psecure-violation	
	は、削除する際にも interval パラメーターまで指定して削除してください。
バージョン	1.12.01

使用例：ポートセキュリティー機能によって err-disabled 状態に変更されたポートの自動復旧を、復旧までの待機時間 200 秒で有効にする方法を示します。

```
# configure terminal
(config)# errdisable recovery cause psecure-violation interval 200
(config)#
```

5.21.10 show port-security

show port-security	
目的	ポートセキュリティー機能の情報を表示します。
Command	show port-security [interface IF-ID [,|-]]
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定 • range port：物理ポートの範囲指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	-
バージョン	-
目的	1.12.01

使用例：ポートセキュリティー機能の情報を表示する方法を示します。

```
# show port-security

 D:Delete-on-Timeout    P:Permanent
 (1)          (2)   (3)     (4)          (5)          (6)        (7)      (8)
 Interface    Max   Curr    Violation    Violation    Security   Admin    Current
 No.          No.    No.      Act.       Count            Mode   State    State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 Port1/0/1    2     2     Shutdown -                     P  Enabled  Forwarding
 Port1/0/2    1     1     Restrict 2485                  D  Enabled  Forwarding
 Port1/0/3    32    1     Protect  -                     D  Enabled  Forwarding
 Port1/0/4    32    0     Protect  -                     D  Disabled -
 Port1/0/5    32    0     Protect  -                     D  Disabled -
～～省略～～
```

項番	説明
(1)	ポート番号を表示します。
(2)	ポートセキュリティー機能で許可する MAC アドレスのポートごとの最大数を表示します。
(3)	現時点で登録されているエントリー数を表示します。
(4)	許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作を表示します。 Protect：許可しない MAC アドレスからの通信を破棄

項番	説明
	Restrict：許可しない MAC アドレスからの通信を破棄、CPU カウンターでカウント、ログ出力 Shutdown：対象ポートをシャットダウン（err-disabled 状態に変更）、ログ出力
(5)	許可しない MAC アドレスからの通信を受信した場合の動作が Restrict の場合に、CPU カウンターでカウントした許可しない MAC アドレスからのパケット数を表示します。CPU 宛てに中継されなかったパケットはカウントされません。
(6)	動的に登録されるエントリーの動作モードを表示します。 D：動的に登録されたエントリーがエージングタイムアウトするモード P：動的に登録されたエントリーがエージングタイムアウトしないモード
(7)	ポートセキュリティー機能の有効(Enabled)／無効(Disabled)を表示します。
(8)	ポートの状態を表示します。 Forwarding：ポートセキュリティー機能が有効な状態 Err-disabled：シャットダウン（err-disabled 状態に変更）された状態 -：ポートセキュリティー機能が無効な状態

5.21.11 show port-security address

show port-security address	
目的	ポートセキュリティー機能のエントリーを表示します。
Command	show port-security [interface IF-ID [,|-]] address
Parameter	interface IF-ID（省略可能）：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定 • range port：物理ポートの範囲指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースのエントリーが表示されます。
制限・注意	-
バージョン	1.12.01

使用例：ポートセキュリティー機能のエントリーを表示する方法を示します。

```
# show port-security address
 (1)           (2)      (3)                (4)                (5)
 Interface     VLAN ID MAC Address        Address Type       Remaining Time
                                                                (mins)
 ------------ ------- ----------------- ----------------- --------------
 Port1/0/1     20      00-00-5E-00-53-11 Permanent          -     (I)
 Port1/0/1     20      00-00-5E-00-53-22 Permanent          -     (I)
 Port1/0/2     30      00-00-5E-00-53-AA Delete-on-Timeout 476
 Port1/0/3     50      00-00-5E-00-53-BB Delete-on-Timeout 18    (I)

 Total Entries: 4
```

項番	説明
(1)	ポート番号を表示します。
(2)	VLAN ID を表示します。

項番	説明
(3)	MAC アドレスを表示します。
(4)	エントリーのタイプを表示します。 Permanent：switchport port-security mac-address コマンドで設定したエントリー、または permanent モードのポートで動的に登録されて自動的に設定されたエントリー Delete-on-Timeout：delete-on-timeout モードのポートで動的に登録された、エージングタイムアウト対象になるエントリー
(5)	エージングタイムアウトまでの残り時間を表示します。 エントリーのタイプが Permanent の場合は、残り時間は表示されません。 エージングタイムのタイプが inactivity タイプの場合、残り時間の後ろに(I)が表示されます。また、対象エントリーが無通信になったと判断する前の状態では、残り時間は表示されません。

5.21.12 clear port-security

clear port-security	
目的	ポートセキュリティー機能で動的に登録されたエントリーを削除します。
Command	clear port-security all clear port-security address MAC-ADDRESS [vlan VLAN-ID] clear port-security interface IF-ID [,|-] [vlan VLAN-ID]
Parameter	all：動的に登録されたすべてのエントリーを削除する場合に指定します。 address MAC-ADDRESS：削除するエントリーの MAC アドレスを、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） interface IF-ID：エントリーをすべて削除するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • range port：物理ポートの範囲指定 vlan VLAN-ID（省略可能）：削除するエントリーの VLAN ID を 1～4094 の範囲で指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	switchport port-security mac-address コマンドで permanent パラメーター指定で設定したエントリーも、本コマンドでの削除対象になります。削除されると構成情報(running-config)から設定も削除されます。 本コマンドでポートセキュリティー機能で動的に登録されたエントリーを削除すると、MAC アドレステーブルからも削除されます。
制限・注意	• ポートセキュリティー機能で動的に登録されたエントリーは、show mac-address-table コマンドでは「タイプ：Static」のエントリーとして表示されるため、clear mac-address-table コマンドや冗長機能の FDB Flush では MAC アドレステーブルから削除されません。

clear port-security	
バージョン	1.12.01

使用例：ポートセキュリティー機能で動的に登録された、MAC アドレスが 00-00-5E-00-53-AA のエントリーを削除する方法を示します。

```
# clear port-security address 00-00-5E-00-53-AA
#
```

6 レイヤー3

6.1 プロトコル非依存コマンド

プロトコル非依存コマンド関連の設定コマンドは以下のとおりです。

- ip route
- ipv6 route

プロトコル非依存コマンド関連の show コマンドは以下のとおりです。

- show ip route
- show ip route summary
- show ipv6 route
- show ipv6 route summary

6.1.1 ip route

ip route	
目的	IPv4 スタティックルートを設定します。ApresiaNP2500 シリーズではデフォルトルートのみ設定できます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip route 0.0.0.0/0 IP-ADDRESS [primary | backup] no ip route 0.0.0.0/0 IP-ADDRESS
Parameter	0.0.0.0/0：デフォルトルートを設定する場合に指定します。 IP-ADDRESS：ネクストホップの IP アドレスを指定します。 primary（省略可能）：プライマリールートを設定する場合に指定します。 backup（省略可能）：バックアップルートを設定する場合に指定します。
デフォルト	スタティックルートの設定なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	宛先ネットワークアドレスが同じで、ネクストホップが異なる 2 つのスタティックルート（プライマリールート、バックアップルート）を設定することができます。 オプションパラメーターを省略して設定した場合は、primary パラメーターが自動的に付与されてプライマリールートとして設定されます。すでに同一ネットワーク宛てのプライマリールートが設定されている場合は、backup パラメーターが自動的に付与されてバックアップルートとして設定されます。 プライマリールートはバックアップルートよりも優先されます。プライマリールートが非アクティブな場合は、バックアップルートが使用されます。
制限・注意	• ApresiaNP2500 シリーズではデフォルトルートのみ設定できます。 • ip address dhcp 設定と「ユーザーによるデフォルトスタティックルート設定」は、同一装置で併用できません。例えば、「ユーザーによるデフォルトスタティックルート設定」がある状態で ip address dhcp を設定すると、そのデフォルトスタティックルート設定は削除されます。 • 構成情報では、宛先ネットワークは「ネットワークアドレスとプレフィックス長」形式で表示されます。

ip route	
バージョン	1.08.02

使用例：ネクストホップ 10.1.1.254 宛ての IPv4 デフォルトスタティックルートを設定する方法を示します。

```
# configure terminal
(config)# ip route 0.0.0.0/0 10.1.1.254
(config)#
```

6.1.2 ipv6 route

ipv6 route	
目的	IPv6 スタティックルートを設定します。ApresiaNP2500 シリーズではデフォルトルートのみ設定できます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	**ipv6 route default** [IF-NAME] IPV6-ADDRESS [**primary** | **backup**] **no ipv6 route default** [IF-NAME] IPV6-ADDRESS
Parameter	default：デフォルトルートを設定する場合に指定します。 IF-NAME（省略可能）：転送先インターフェース（vlan と VLAN ID の間を空けない形式）を指定します。 IPV6-ADDRESS：ネクストホップの IPv6 アドレスを指定します。IPv6 アドレスがリンクローカルアドレスの場合は、転送先インターフェースも指定してください。 primary（省略可能）：プライマリールートを設定する場合に指定します。 backup（省略可能）：バックアップルートを設定する場合に指定します。
デフォルト	スタティックルートの設定なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	宛先ネットワークアドレスが同じで、ネクストホップが異なる 2 つのスタティックルート（プライマリールート、バックアップルート）を設定することができます。 オプションパラメーターを省略して設定した場合は、primary パラメーターが自動的に付与されてプライマリールートとして設定されます。すでに同一ネットワーク宛てのプライマリールートが設定されている場合は、backup パラメーターが自動的に付与されてバックアップルートとして設定されます。 プライマリールートはバックアップルートよりも優先されます。プライマリールートが非アクティブな場合は、バックアップルートが使用されます。
制限・注意	• ApresiaNP2500 シリーズではデフォルトルートのみ設定できます。 • 転送先インターフェース（vlan と VLAN ID の間を空けない形式）を省略して設定しても、構成情報では表示されます。
バージョン	1.08.02

使用例：ネクストホップ vlan1 fe80::1111 宛ての IPv6 デフォルトスタティックルートを設定する方法を示します。

```
# configure terminal
(config)# ipv6 route default vlan1 fe80::1111
(config)#
```

6.1.3 show ip route

show ip route	
目的	IPv4 ルーティングテーブルを表示します。
Command	show ip route [IP-ADDRESS [MASK] | PROTOCOL]
Parameter	IP-ADDRESS（省略可能）：ルート情報を表示する IP アドレスを指定します。指定した IP アドレスに到達するために Longest prefix match（最長一致）規則に従って選択されたルート情報が表示されます。 IP-ADDRESS MASK（省略可能）：ルート情報を表示するネットワークアドレスとサブネットマスクを指定します。 PROTOCOL（省略可能）：プロトコルを指定してルート情報を表示する場合に、以下のパラメーターで指定します。 • connected：自装置に直接接続されているネットワーク • static：スタティックルートで設定されたルート情報
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• ApresiaNP2500 シリーズでは、hardware パラメーターを指定した表示は未サポートです。
バージョン	1.08.02

使用例：IPv4 ルーティングテーブルを表示する方法を示します。

```
# show ip route
Code: C - connected, S - static

      * - candidate default

Gateway of last resort is 192.0.2.254 to network 0.0.0.0 ...(1)
(2)   (3)        (4)    (5)               (6)
S*    0.0.0.0/0 [1/1] via 192.0.2.254, vlan1
C     10.0.0.0/24 is directly connected, mgmt_ipif
C     192.0.2.0/24 is directly connected, vlan1

Total Entries: 3
```

項番	説明
(1)	デフォルトゲートウェイの IP アドレス（デフォルトルートのネクストホップアドレス）を表示します。
(2)	対象ルートを学習したプロトコルを表示します。 C：自装置に直接接続されているネットワーク S：スタティックルート *：デフォルトルートの場合に表示されます
(3)	宛先ネットワークアドレスを表示します。
(4)	前の数値は、対象ルートを学習したプロトコルの AD 値を表示します。 後ろの数値は、対象ルートのメトリックを表示します。
(5)	対象ルートのネクストホップアドレスを表示します。
(6)	対象ルートの送信インターフェースを表示します。

6.1.4 show ip route summary

show ip route summary	
目的	IPv4 ルーティングテーブルの概要情報を表示します。
Command	show ip route summary
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：IPv4 ルーティングテーブルの概要情報を表示する方法を示します。

```
# show ip route summary
(1)               (2)
Route Source      Networks
Connected         2
Static            1
Total             3
```

項番	説明
(1)	ルート情報を学習したプロトコルを表示します。
(2)	ルート情報の数を表示します。

6.1.5 show ipv6 route

show ipv6 route	
目的	IPv6 ルーティングテーブルを表示します。
Command	show ipv6 route
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：IPv6 ルーティングテーブルを表示する方法を示します。

```
# show ipv6 route

IPv6 Routing Table
Code: C - connected, S - static
      SLAAC - Stateless address auto-configuration
(1)   (2)  (3)   (4)                    (5)
S     ::/0 [1/1] via 2001:db8::aaaa:1, vlan1
C     2001:db8::/64 [0/1] is directly connected, vlan1

Total Entries: 2 entries, 2 routes
```

項番	説明
(1)	対象ルートを学習したプロトコルを表示します。 C：自装置に直接接続されているネットワーク S：スタティックルート SLAAC：ステートレスアドレス自動設定によって学習したデフォルトルート
(2)	宛先ネットワークアドレスを表示します。
(3)	前の数値は、対象ルートを学習したプロトコルの AD 値を表示します。 後ろの数値は、対象ルートのメトリックを表示します。
(4)	対象ルートのネクストホップアドレスを表示します。
(5)	対象ルートの送信インターフェースを表示します。

6.1.6 show ipv6 route summary

show ipv6 route summary	
目的	IPv6 ルーティングテーブルの概要情報を表示します。
Command	show ipv6 route summary
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：IPv6 ルーティングテーブルの概要情報を表示する方法を示します。

```
# show ipv6 route summary
(1)              (2)
Route Source     Networks
Connected        1
Static           1
SLAAC            0
Total            2
```

項番	説明
(1)	ルート情報を学習したプロトコルを表示します。
(2)	ルート情報の数を表示します。

6.2 IPv4 マルチキャストコマンド

IPv4 マルチキャスト関連の show コマンドは以下のとおりです。

- show ip mroute forwarding-cache

6.2.1 show ip mroute forwarding-cache

show ip mroute forwarding-cache	
目的	IPv4 マルチキャスト転送キャッシュを表示します。
Command	show ip mroute forwarding-cache [group-addr GROUP-ADDRESS [source-addr SOURCE-ADDRESS]]
Parameter	group-addr GROUP-ADDRESS（省略可能）：フォワーディングキャッシュを表示するマルチキャストグループアドレスを指定します。 source-addr SOURCE-ADDRESS（省略可能）：マルチキャスト送信元の IPv4 アドレスを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	IPv4 マルチキャスト転送キャッシュには、IGMP スヌーピングのためのフォワーディングキャッシュが登録されます。
制限・注意	• IPv4 マルチキャスト転送キャッシュは最大 1024 個まで登録できます。なお、フォワーディングキャッシュのリソースは IPv6 マルチキャストと共有します。 • ApresiaNP2500 シリーズでは、IPv4 マルチキャストと IPv6 マルチキャストをハードウェア転送するためのスイッチ LSI リソースは、あわせて最大 1024 リソースまで使用できます。1 個のマルチキャストエントリーあたり 1 個のリソースを使用します。 • 例えば、すでに IPv6 マルチキャストエントリーが 200 個存在する場合は、IPv4 マルチキャストエントリーは 824 個まで登録可能です。
バージョン	1.08.02

使用例：IPv4 マルチキャスト転送キャッシュを表示する方法を示します。

```
# show ip mroute forwarding-cache

(*, 232.1.1.1) VLAN0010 ...(1)
  Outgoing interface list: 1/0/1 ...(2)

(*, 232.1.1.3) VLAN0010
  Outgoing interface list: 1/0/2, port-channel5

Total Entries: 2
```

項番	説明
(1)	IPv4 マルチキャストエントリーを表示します。
(2)	出力インターフェース ID (物理ポート、ポートチャネル) のリストを表示します。

6.3 IPv6 マルチキャストコマンド

IPv6 マルチキャスト関連の show コマンドは以下のとおりです。

- show ipv6 mroute forwarding-cache

6.3.1 show ipv6 mroute forwarding-cache

show ipv6 mroute forwarding-cache	
目的	IPv6 マルチキャスト転送キャッシュを表示します。
Command	show ipv6 mroute forwarding-cache [group-addr GROUP-ADDRESS [source-addr SOURCE-ADDRESS]]
Parameter	group-addr GROUP-ADDRESS（省略可能）：フォワーディングキャッシュを表示するマルチキャストグループアドレスを指定します。 source-addr SOURCE-ADDRESS（省略可能）：マルチキャスト送信元の IPv6 アドレスを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	IPv6 マルチキャスト転送キャッシュには、MLD スヌーピングのためのフォワーディングキャッシュが登録されます。
制限・注意	• IPv6 マルチキャスト転送キャッシュは最大 1024 個まで登録できます。なお、フォワーディングキャッシュのリソースは IPv4 マルチキャストと共有します。 • ApresiaNP2500 シリーズでは、IPv4 マルチキャストと IPv6 マルチキャストをハードウェア転送するためのスイッチ LSI リソースは、あわせて最大 1024 リソースまで使用できます。1 個のマルチキャストエントリーあたり 1 個のリソースを使用します。 • 例えば、すでに IPv4 マルチキャストエントリーが 500 個存在する場合は、IPv6 マルチキャストエントリーは 524 個まで登録可能です。
バージョン	1.08.02

使用例：IPv6 マルチキャスト転送キャッシュを表示する方法を示します。

```
# show ipv6 mroute forwarding-cache

(*, ff0e::1:1:1:1) VLAN0010 ...(1)
  Outgoing interface list: 1/0/1 ...(2)

(*, ff0e::1:1:1:3) VLAN0010
  Outgoing interface list: 1/0/2, port-channel5

Total Entries: 2
```

項番	説明
(1)	IPv6 マルチキャストエントリーを表示します。
(2)	出力インターフェース ID (物理ポート、ポートチャネル) のリストを表示します。

7 QoS

7.1 QoS コマンド

QoS 関連の設定コマンドは以下のとおりです。

- priority-queue cos-map
- mls qos scheduler
- wrr-queue bandwidth
- wdrr-queue bandwidth
- mls qos trust
- mls qos cos
- mls qos map dscp-cos
- mls qos map cos-color
- mls qos map dscp-color
- mls qos dscp-mutation
- mls qos map dscp-mutation
- queue rate-limit
- rate-limit input
- rate-limit output

QoS 関連の show コマンドは以下のとおりです。

- show mls qos queueing
- show mls qos interface scheduler
- show mls qos interface trust
- show mls qos interface cos
- show mls qos interface map dscp-cos
- show mls qos interface map cos-color
- show mls qos interface map dscp-color
- show mls qos map dscp-mutation
- show mls qos interface dscp-mutation
- show mls qos interface queue-rate-limit
- show mls qos interface rate-limit

7.1.1 priority-queue cos-map

priority-queue cos-map	
目的	CoS 値から送信キューへのマッピングを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	priority-queue cos-map QUEUE-ID COS-LIST no priority-queue cos-map
Parameter	QUEUE-ID：送信キューを 0～7 の範囲で指定します。 COS-LIST：CoS 値を 0～7 の範囲で指定します。複数の CoS 値を指定する場合は、半角空白で区切って指定します。
デフォルト	CoS 0 = 送信キュー 2 CoS 1 = 送信キュー 0

priority-queue cos-map	
	CoS 2 = 送信キュー 1 CoS 3 = 送信キュー 3 CoS 4 = 送信キュー 4 CoS 5 = 送信キュー 5 CoS 6 = 送信キュー 6 CoS 7 = 送信キュー 7
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：CoS 値が 3,5,6 の場合は、送信キュー 2 にマッピングする方法を示します。

```
# configure terminal
(config)# priority-queue cos-map 2 3 5 6
(config)#
```

7.1.2 mls qos scheduler

mls qos scheduler	
目的	送信キューのスケジューリングアルゴリズムを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mls qos scheduler {sp | rr | wrr | wdrr} no mls qos scheduler
Parameter	sp：Strict Priority Queuing に設定する場合に指定します。 rr：Round Robin スケジューリングに設定する場合に指定します。 wrr：WRR（Weighted Round Robin）スケジューリングに設定する場合に指定します。重みが 0 の送信キューは Strict Priority Queuing で動作します。 wdrr：WDRR（Weighted Deficit Round Robin）スケジューリングに設定する場合に指定します。重みが 0 の送信キューは Strict Priority Queuing で動作します。
デフォルト	WRR（Weighted Round Robin）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で送信キューのスケジューリングアルゴリズムを Strict Priority Queuing に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# mls qos scheduler sp
(config-if-port)#
```

7.1.3 wrr-queue bandwidth

wrr-queue bandwidth	
目的	WRR（Weighted Round Robin）スケジューリングの重みを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	wrr-queue bandwidth WEIGHT0...WEIGHT7 no wrr-queue bandwidth
Parameter	WEIGHT0...WEIGHT7：WRR スケジューリングの各送信キューの重みを 0～127 の範囲で指定します。
デフォルト	すべての送信キューの重み：1
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	本設定は、mls qos scheduler コマンドでスケジューリングアルゴリズムが WRR（Weighted Round Robin）に設定されている場合に有効です。 重みが 0 の送信キューは Strict Priority Queuing で動作します。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で、スケジューリングアルゴリズムを WRR に設定し、WRR スケジューリングの重みを、「送信キュー 0 = 重み 1」「送信キュー 1 = 重み 2」・・・「送信キュー 7 = 重み 8」に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# mls qos scheduler wrr
(config-if-port)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
(config-if-port)#
```

7.1.4 wdrr-queue bandwidth

wdrr-queue bandwidth	
目的	WDRR（Weighted Deficit Round Robin）スケジューリングの重みを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	wdrr-queue bandwidth QUANTUM0...QUANTUM7 no wdrr-queue bandwidth
Parameter	QUANTUM0...QUANTUM7：WDRR スケジューリングの各送信キューの重みを 0～127 の範囲で指定します。
デフォルト	すべての送信キューの重み：1
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	本設定は、mls qos scheduler コマンドでスケジューリングアルゴリズムが WDRR（Weighted Deficit Round Robin）に設定されている場合に有効です。 重みが 0 の送信キューは Strict Priority Queuing で動作します。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で、スケジューリングアルゴリズムを WDRR に設定し、WDRR スケジューリングの重みを、「送信キュー 0 = 重み 1」「送信キュー 1 = 重み 2」・・・「送信キュー 7 = 重み 8」に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# mls qos scheduler wdrr
(config-if-port)# wdrr-queue bandwidth 1 2 3 4 5 6 7 8
(config-if-port)#
```

7.1.5 mls qos trust

mls qos trust	
目的	受信トラフィックを分類する情報元フィールドを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	**mls qos trust** {**cos** | **dscp**} **no mls qos trust**
Parameter	cos：受信トラフィックの CoS を信頼するモードに設定する場合に指定します。 dscp：受信トラフィックの DSCP を信頼するモードに設定する場合に指定します。
デフォルト	cos（受信トラフィックの CoS を信頼するモード）
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	「受信トラフィックの CoS を信頼するモード」の場合、受信したタグ付きフレームの CoS がそのまま装置内部の優先度として適用されます。タグなしフレームの場合は、mls qos cos コマンドで設定したデフォルトの CoS 値が適用されます。 「受信トラフィックの DSCP を信頼するモード」の場合、受信した IP パケットの DSCP を基に、mls qos map dscp-cos コマンドの「DSCP から CoS 値へのマッピング」で反映された CoS 値が装置内部の優先度として適用されます。なお、非 IP パケットの場合は「受信トラフィックの CoS を信頼するモード」の場合と同じ動作になります。 トンネルポートでは、受信 VLAN を決定する方法によって、装置内部の優先度の決定方法も異なります。 • 受信 VLAN を決定する方法が switchport vlan mapping コマンド、または switchport access vlan コマンドの場合は、以下のように装置内部の優先度が決定されます。 　• 「受信トラフィックの CoS を信頼するモード」の場合は、switchport vlan mapping コマンドなら switchport vlan mapping コマンドの priority オプション、switchport access vlan コマンドなら mls qos cos コマンドで設定したデフォルトの CoS 値が適用されます。 　• 「受信トラフィックの DSCP を信頼するモード」の場合は、IP パケットの DSCP を基に決定されます。非 IP パケットの場合は「受信トラフィックの CoS を信頼するモード」の場合と同じ動作になります。 　• mls qos cos コマンドの override パラメーターを有効に設定すると、デフォルトの CoS 値が適用されます。 • 受信 VLAN を決定する方法が vlan mapping rule コマンドの場合は、mls qos trust コマンドや mls qos cos コマンドの設定にかかわらず、vlan mapping rule コマンドの priority オプションにより装置内部の優先度が決定されます。 トラフィック初期カラーは、「受信トラフィックの CoS を信頼するモード」の場合は

mls qos trust	
	mls qos map cos-color コマンドの「CoS からトラフィック初期カラーへのマッピング」が反映され、「受信トラフィックの DSCP を信頼するモード」の場合は mls qos map dscp-color コマンドの「DSCP からトラフィック初期カラーへのマッピング」が反映されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 を「受信トラフィックの DSCP を信頼するモード」に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# mls qos trust dscp
(config-if-port)#
```

7.1.6 mls qos cos

mls qos cos	
目的	ポートのデフォルトの CoS 値を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mls qos cos {COS-VALUE | override} no mls qos cos
Parameter	COS-VALUE：受信したタグなしフレームに適用されるデフォルトの CoS 値を、0～7 の範囲で指定します。 override：タグ付きフレーム、タグなしフレームにかかわらず、すべての受信フレームにデフォルトの CoS 値を適用する場合に指定します。
デフォルト	デフォルトの CoS 値：0 override 設定：無効
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	mls qos trust コマンドで受信トラフィックの分類設定が「trust CoS：受信トラフィックの CoS を信頼するモード」の場合、受信したタグなしフレームにデフォルトの CoS 値が適用されます。受信トラフィックの分類設定が「trust DSCP：受信トラフィックの DSCP を信頼するモード」の場合でも、受信したタグなしフレームが非 IP パケットの場合は、デフォルトの CoS 値が適用されます。 受信トラフィックの分類設定が「trust DSCP：受信トラフィックの DSCP を信頼するモード」の場合でも、override パラメーターを有効に設定すると、IP パケットを含むすべての受信フレームに対してデフォルトの CoS 値が適用されます。 トンネルポートで、vlan mapping rule コマンドによって受信 VLAN が決定される場合は、mls qos trust コマンドや mls qos cos コマンドの設定にかかわらず、vlan mapping rule コマンドの priority オプションにより装置内部の優先度が決定されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 のデフォルトの CoS 値を 3 に設定する方法を示します。

```
# configure terminal
```

```
(config)# interface port 1/0/1
(config-if-port)# mls qos cos 3
(config-if-port)#
```

7.1.7 mls qos map dscp-cos

mls qos map dscp-cos	
目的	Differentiated Services Code Point（DSCP）から CoS 値へのマッピングを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mls qos map dscp-cos DSCP-LIST to COS-VALUE no mls qos map dscp-cos DSCP-LIST
Parameter	DSCP-LIST：DSCP を 0～63 の範囲で指定します。複数の DSCP を指定する場合はコンマで区切るか、ハイフンで範囲を指定します。コンマとハイフンの前後には、スペースを入力しないでください。 COS-VALUE：CoS 値を 0～7 の範囲で指定します。
デフォルト	DSCP 0～7 = CoS 0 DSCP 8～15 = CoS 1 DSCP 16～23 = CoS 2 DSCP 24～31 = CoS 3 DSCP 32～39 = CoS 4 DSCP 40～47 = CoS 5 DSCP 48～55 = CoS 6 DSCP 56～63 = CoS 7
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	DSCP から CoS 値へのマッピングを使用する場合は、mls qos trust コマンドで「受信トラフィックの DSCP を信頼するモード」に設定します。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/6 で、DSCP が 12,16,18 の場合は CoS 1 にマッピングする方法を示します。

```
# configure terminal
(config)# interface port 1/0/6
(config-if-port)# mls qos map dscp-cos 12,16,18 to 1
(config-if-port)#
```

7.1.8 mls qos map cos-color

mls qos map cos-color	
目的	受信トラフィックの CoS からトラフィック初期カラーへのマッピングを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mls qos map cos-color COS-LIST to {green | yellow | red} no mls qos map cos-color
Parameter	COS-LIST：CoS を 0～7 の範囲で指定します。複数の CoS を指定する場合はコンマで区切るか、ハイフンで範囲を指定します。コンマとハイフンの前後には、スペースを入力しないでください。

mls qos map cos-color	
	green：トラフィック初期カラーをグリーンにする場合に指定します。 yellow：トラフィック初期カラーをイエローにする場合に指定します。 red：トラフィック初期カラーをレッドにする場合に指定します。
デフォルト	CoS 0～7 = green
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	CoS からトラフィック初期カラーへのマッピングを使用する場合は、mls qos trust コマンドで「受信トラフィックの CoS を信頼するモード」に設定します。
制限・注意	• 「受信トラフィックの CoS を信頼するモード」では、対象がタグなしフレームの場合は本設定にかかわらずトラフィック初期カラーはグリーンになります。
バージョン	1.08.02

使用例：ポート 1/0/1 で、CoS 1～7 のトラフィック初期カラーをレッドに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# mls qos map cos-color 1-7 to red
(config-if-port)#
```

7.1.9 mls qos map dscp-color

mls qos map dscp-color	
目的	受信トラフィックの DSCP からトラフィック初期カラーへのマッピングを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mls qos map dscp-color DSCP-LIST to {green | yellow | red} no mls qos map dscp-color DSCP-LIST
Parameter	DSCP-LIST：DSCP を 0～63 の範囲で指定します。複数の DSCP を指定する場合はコンマで区切るか、ハイフンで範囲を指定します。コンマとハイフンの前後には、スペースを入力しないでください。 green：トラフィック初期カラーをグリーンにする場合に指定します。 yellow：トラフィック初期カラーをイエローにする場合に指定します。 red：トラフィック初期カラーをレッドにする場合に指定します。
デフォルト	DSCP 0～63 = green
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	DSCP からトラフィック初期カラーへのマッピングを使用する場合は、mls qos trust コマンドで「受信トラフィックの DSCP を信頼するモード」に設定します。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で、DSCP 61～63 のトラフィック初期カラーをイエローに設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
```

```
(config-if-port)# mls qos map dscp-color 61-63 to yellow
(config-if-port)#
```

7.1.10 mls qos dscp-mutation

mls qos dscp-mutation	
目的	受信時の Differentiated Services Code Point（DSCP）変換マップを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mls qos dscp-mutation DSCP-MAP-NAME no mls qos dscp-mutation
Parameter	DSCP-MAP-NAME：DSCP 変換マップ名を指定します。
デフォルト	なし
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	受信時の DSCP 変換マップを使用する場合は、mls qos trust コマンドで「受信トラフィックの DSCP を信頼するモード」に設定します。 受信した IP パケットの DSCP が設定した DSCP 変換マップに従って変換されます。 受信時の DSCP 変換マップを設定した場合でも、以下の機能は変換前の DSCP を基に動作します。 • mls qos map dscp-cos コマンドで設定した「DSCP から CoS へのマッピング」 • mls qos map dscp-color コマンドで設定した「DSCP からトラフィック初期カラーへのマッピング」 • service-policy input コマンドで同一ポートに設定した受信側ポリシーマップ
制限・注意	• 未定義の DSCP 変換マップを指定して設定した場合は、WARNING メッセージが表示されます。
バージョン	1.08.02

使用例：DSCP 変換マップ「mutemap2」を「DSCP 30 なら DSCP 8 に変換する」設定で定義し、ポート 1/0/1 の受信時の DSCP 変換マップとして適用する方法を示します。

```
# configure terminal
(config)# mls qos map dscp-mutation mutemap2 30 to 8
(config)# interface port 1/0/1
(config-if-port)# mls qos dscp-mutation mutemap2
(config-if-port)#
```

7.1.11 mls qos map dscp-mutation

mls qos map dscp-mutation	
目的	Differentiated Services Code Point（DSCP）変換マップを定義します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mls qos map dscp-mutation DSCP-MAP-NAME DSCP-LIST to OUTPUT-DSCP no mls qos map dscp-mutation DSCP-MAP-NAME
Parameter	DSCP-MAP-NAME：DSCP 変換マップ名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 DSCP-LIST：DSCP を 0～63 の範囲で指定します。複数の DSCP を指定する場合はコンマで区切るか、ハイフンで範囲を指定します。コンマとハイフンの前後には、ス

mls qos map dscp-mutation	
	ペースを入力しないでください。 OUTPUT-DSCP：変換後の DSCP を 0～63 の範囲で指定します。
デフォルト	DSCP 変換マップは未定義 定義済み DSCP 変換マップの場合は、変換前 DSCP = 変換後 DSCP
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	DSCP 変換マップを使用する場合は、mls qos dscp-mutation コマンドで適用する DSCP 変換マップを受信ポートに設定します。
制限・注意	• 定義できる DSCP 変換マップは最大 255 個です。
バージョン	1.08.02

使用例：DSCP 変換マップ「mutemap2」を「DSCP 30 なら DSCP 8 に変換する」「DSCP 20 なら DSCP 10 に変換する」設定で定義する方法を示します。

```
# configure terminal
(config)# mls qos map dscp-mutation mutemap2 30 to 8
(config)# mls qos map dscp-mutation mutemap2 20 to 10
(config)#
```

7.1.12 queue rate-limit

queue rate-limit	
目的	送信キューの最小保証帯域、最大帯域を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	queue QUEUE-ID rate-limit {MIN-KBPS | percent MIN-PERCENTAGE} {MAX-KBPS | percent MAX-PERCENTAGE} no queue QUEUE-ID rate-limit
Parameter	QUEUE-ID：最小保証帯域と最大帯域を設定するキューID を指定します。 MIN-KBPS：指定したキューに割り当てる最小保証帯域を、64～10,000,000（Kbps）の範囲で指定します。 percent MIN-PERCENTAGE：インターフェースの帯域に対する最小保証帯域の割合を 1～100（%）の範囲で指定します。 MAX-KBPS：指定したキューの最大帯域を、64～10,000,000（Kbps）の範囲で指定します。 percent MAX-PERCENTAGE：インターフェースの帯域に対する最大帯域の割合を 1～100（%）の範囲で指定します。
デフォルト	なし
モード	インターフェース設定モード（port, range）
特権レベル	レベル：12
ガイドライン	本機能の帯域計測仕様は、IFG（Inter Frame Gap）と Preamble を含めないで計測する仕様です。 最小保証帯域を設定すると、対象ポートが輻輳状態でも、そのキューから送信するトラフィックが指定した最小帯域分は破棄されずに送信されます。 最大帯域を設定すると、そのキューから送信するトラフィックが指定した最大帯域に

queue rate-limit	
	制限されます。 MIN-KBPS パラメーターと MAX-KBPS パラメーターの設定値は、1Kbps 単位で任意の値を指定できますが、動作時は 64Kbps 単位に切り捨てた値で動作します。 最小帯域の設定時には、設定した最小帯域が保証されるよう、最小帯域の総計がインターフェース帯域の 75%未満になるように設定してください。絶対優先度が最高値のキューには、最小保証帯域を設定する必要はありません。すべてのキューで最小帯域の条件を満たしていれば、最高値のキュー内のトラフィックが最優先で処理されるためです。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 のキュー2 において、最小保証帯域を 1000Kbps に、最大帯域を 200,000Kbps に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# queue 2 rate-limit 1000 200000
(config-if-port)#
```

7.1.13 rate-limit input

rate-limit input	
目的	受信ポートごとの帯域制限を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	rate-limit input {KBPS | percent PERCENTAGE} [BURST] no rate-limit input
Parameter	KBPS：受信帯域制限値を 64～10,000,000（Kbps）の範囲で指定します。 percent PERCENTAGE：受信帯域制限値を 1～100（%）の範囲で指定します。 BURST（省略可能）：バーストサイズを 0～16,380（KByte）の範囲で指定します。
デフォルト	なし
モード	インターフェース設定モード（port, range）
特権レベル	レベル：12
ガイドライン	本機能の帯域計測仕様は、IFG（Inter Frame Gap）と Preamble を含めないで計測する仕様です。 対象ポートのフロー制御機能が有効な場合は、受信したトラフィックが帯域制限値を超えると、PAUSE フレームを送信します。 KBPS パラメーターの設定値は、1Kbps 単位で任意の値を指定できますが、動作時は 64Kbps 単位に切り捨てた値で動作します。 BURST パラメーターは 4 の倍数値で設定できます。それ以外の数値を指定した場合には指定した値より小さい有効値に自動的に変更されます。
制限・注意	• BURST パラメーターを 0 に設定した場合は帯域制限は動作しません。BURST パラメーターには 0 を設定しないでください。 • 運用中にバーストサイズの設定を大きい値から小さい値に変更すると、トラフィック状況によっては一時的にパケットの中継が停止します。そのため、バーストサイ

rate-limit input	
	ズの設定を大きい値から小さい値に変更する場合は、no rate-limit input コマンドで削除してから、再度設定してください。 • バーストサイズは明示的に指定して設定してください。なお、BURST パラメーターを省略して設定した場合は、以下のように設定されます。 • 帯域制限値を Kbps 指定で設定した場合：帯域制限値で指定した数値と同じ数値を、BURST パラメーターの数値として指定した形式で設定される。 • 帯域制限値を percent 指定で設定した場合：リンクアップした際に、通信速度と percent 指定から算出された帯域制限値と同じ数値を、BURST パラメーターの数値として指定した形式で設定される。
バージョン	1.08.02

使用例：ポート 1/0/5 で受信帯域制限値を 8000Kbps に、バーストサイズを 16KByte に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/5
(config-if-port)# rate-limit input 8000 16
(config-if-port)#
```

7.1.14 rate-limit output

rate-limit output	
目的	送信ポートごとの帯域制限を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	rate-limit output {KBPS | percent PERCENTAGE} [BURST] no rate-limit output
Parameter	KBPS：送信帯域制限値を 64～10,000,000（Kbps）の範囲で指定します。 percent PERCENTAGE：送信帯域制限値を 1～100（%）の範囲で指定します。 BURST（省略可能）：バーストサイズを 0～16,380（KByte）の範囲で指定します。
デフォルト	なし
モード	インターフェース設定モード（port, range）
特権レベル	レベル：12
ガイドライン	本機能の帯域計測仕様は、IFG（Inter Frame Gap）と Preamble を含めないで計測する仕様です。 KBPS パラメーターの設定値は、1Kbps 単位で任意の値を指定できますが、動作時は 64Kbps 単位に切り捨てた値で動作します。 BURST パラメーターは 4 の倍数値で設定できます。それ以外の数値を指定した場合には指定した値より小さい有効値に自動的に変更されます。
制限・注意	• BURST パラメーターを 0 に設定した場合は帯域制限は動作しません。BURST パラメーターには 0 を設定しないでください。 • 運用中にバーストサイズの設定を大きい値から小さい値に変更すると、トラフィック状況によっては一時的にパケットの中継が停止します。そのため、バーストサイズの設定を大きい値から小さい値に変更する場合は、no rate-limit output コマンドで削除してから、再度設定してください。 • バーストサイズは明示的に指定して設定してください。なお、BURST パラメーター

rate-limit output	
	を省略して設定した場合は、以下のように設定されます。 • 帯域制限値を Kbps 指定で設定した場合：帯域制限値で指定した数値と同じ数値を、BURST パラメーターの数値として指定した形式で設定される。 • 帯域制限値を percent 指定で設定した場合：リンクアップした際に、通信速度と percent 指定から算出された帯域制限値と同じ数値を、BURST パラメーターの数値として指定した形式で設定される。
バージョン	1.08.02

使用例：ポート 1/0/5 で送信帯域制限値を 40Mbps に、バーストサイズを 512KByte に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/5
(config-if-port)# rate-limit output 40000 512
(config-if-port)#
```

7.1.15 show mls qos queueing

show mls qos queueing	
目的	CoS 値から送信キューへのマッピング設定を表示します。また、指定したポートの WRR スケジューリングの重みと、WDRR スケジューリングの重みを表示します。
Command	show mls qos queueing [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、CoS 値から送信キューへのマッピング設定が表示されます。 特定のポートを指定した場合は、WRR スケジューリングの重みと WDRR スケジューリングの重みが表示されます。
制限・注意	-
バージョン	1.08.02

使用例：CoS 値から送信キューへのマッピング設定を表示する方法を示します。

```
# show mls qos queueing

 CoS-queue map:
   (1)    (2)
   CoS    QID
   ---    ---
    0      2
    1      0
    2      1
    3      3
    4      4
    5      5
    6      6
    7      7
```

項番	説明
(1)	CoS 値を表示します。
(2)	送信キュー番号を表示します。

使用例：ポート 1/0/3 の、WRR スケジューリングの重みと WDRR スケジューリングの重みを表示します。

```
# show mls qos queueing interface port 1/0/3

Interface: Port1/0/3 ...(1)
 wrr bandwidth weights: ...(2)
   QID  Weights
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      1
 wdrr bandwidth weights: ...(3)
   QID  Quantum
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      1
```

項番	説明
(1)	ポート番号を表示します。
(2)	WRR スケジューリングの重みを表示します。
(3)	WDRR スケジューリングの重みを表示します。

7.1.16 show mls qos interface scheduler

show mls qos interface scheduler	
目的	スケジューリングアルゴリズム設定を表示します。
Command	show mls qos interface [port PORTS] scheduler
Parameter	port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/2 の、スケジューリングアルゴリズム設定を表示する方法を示します。

```
# show mls qos interface port 1/0/1-1/0/2 scheduler
```

```
 (1)            (2)
Interface      Scheduler Method
------------   -----------------
Port1/0/1      sp
Port1/0/2      wrr
```

項番	説明
(1)	ポート番号を表示します。
(2)	スケジューリングアルゴリズムを表示します。 sp：Strict Priority Queuing rr：Round Robin スケジューリング wrr：WRR (Weighted Round Robin) スケジューリング wdrr：WDRR (Weighted Deficit Round Robin) スケジューリング

7.1.17 show mls qos interface trust

show mls qos interface trust	
目的	受信トラフィックの分類設定を表示します。
Command	show mls qos interface [port PORTS] trust
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/2～1/0/5 の、受信トラフィックの分類設定を表示する方法を示します。

```
# show mls qos interface port 1/0/2-1/0/5 trust
 (1)            (2)
Interface      Trust State
------------   ------------
Port1/0/2      trust CoS
Port1/0/3      trust CoS
Port1/0/4      trust CoS
Port1/0/5      trust CoS
```

項番	説明
(1)	ポート番号を表示します。
(2)	受信トラフィックの分類設定を表示します。 trust CoS：受信トラフィックの CoS を信頼するモード trust DSCP：受信トラフィックの DSCP を信頼するモード

7.1.18 show mls qos interface cos

show mls qos interface cos	
目的	ポートのデフォルト CoS 値を表示します。
Command	show mls qos interface [port PORTS] cos

show mls qos interface cos	
Parameter	port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/2～1/0/5 の、デフォルト CoS 値を表示する方法を示します。

```
# show mls qos interface port 1/0/2-5 cos
 (1)             (2)    (3)
 Interface       CoS    Override
 ------------    ----   ---------
 Port1/0/2       0      No
 Port1/0/3       0      No
 Port1/0/4       0      No
 Port1/0/5       0      No
```

項番	説明
(1)	ポート番号を表示します。
(2)	デフォルトの CoS 値を表示します。
(3)	受信トラフィックの CoS を、デフォルトの CoS 値で書き換える設定を表示します。 Yes：デフォルトの CoS 値で書き換える No：デフォルトの CoS 値で書き換えない

7.1.19 show mls qos interface map dscp-cos

show mls qos interface map dscp-cos	
目的	DSCP から CoS 値へのマッピング設定を表示します。
Command	show mls qos interface [port PORTS] map dscp-cos
Parameter	port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の、DSCP から CoS 値へのマッピング設定を表示する方法を示します。

```
# show mls qos interface port 1/0/1 map dscp-cos

Port1/0/1 ...(1)
        0  1  2  3  4  5  6  7  8  9 ...(2)
   --------------------------------
   00   00 00 00 00 00 00 00 00 01 01
   10   01 01 01 01 01 01 02 02 02 02
   20   02 02 02 02 03 03 03 03 03 03
   30   03 03 04 04 04 04 04 04 04 04
   40   05 05 05 05 05 05 05 05 06 06
```

```
    50   06 06 06 06 06 06 07 07 07 07
    60   07 07 07 07
```

項番	説明
(1)	ポート番号を表示します。
(2)	DSCP から CoS 値へのマッピング設定を表形式で表示します。表の縦軸は DSCP の 10 の位を、横軸は DSCP の 1 の位を表します。交差する点に表示されている数値がマッピングする CoS 値を表します。

7.1.20 show mls qos interface map cos-color

show mls qos interface map cos-color	
目的	CoS からトラフィック初期カラーへのマッピング設定を表示します。
Command	show mls qos interface [port PORTS] map cos-color
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/3～1/0/4 の、CoS からトラフィック初期カラーへのマッピング設定を表示する方法を示します。

```
# show mls qos interface port 1/0/3-4 map cos-color

Port1/0/3 ...(1)
  CoS 0-2,5,7 are mapped to green ...(2)
  CoS 3-4 are mapped to yellow ...(3)
  CoS 6 are mapped to red ...(4)
Port1/0/4
  CoS 0-7 are mapped to green
```

項番	説明
(1)	ポート番号を表示します。
(2)	グリーントラフィックに分類される CoS を表示します。
(3)	イエロートラフィックに分類される CoS を表示します。
(4)	レッドトラフィックに分類される CoS を表示します。

7.1.21 show mls qos interface map dscp-color

show mls qos interface map dscp-color	
目的	DSCP からトラフィック初期カラーへのマッピング設定を表示します。
Command	show mls qos interface [port PORTS] map dscp-color
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1

show mls qos interface map dscp-color	
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/2 の、DSCP からトラフィック初期カラーへのマッピング設定を表示する方法を示します。

```
# show mls qos interface port 1/0/1-2 map dscp-color

Port1/0/1 ...(1)
  DSCP 0-7 are mapped to green ...(2)
  DSCP 41-63 are mapped to yellow ...(3)
  DSCP 8-40 are mapped to red ...(4)
Port1/0/2
  DSCP 0-63 are mapped to green
```

項番	説明
(1)	ポート番号を表示します。
(2)	グリーントラフィックに分類される DSCP を表示します。
(3)	イエロートラフィックに分類される DSCP を表示します。
(4)	レッドトラフィックに分類される DSCP を表示します。

7.1.22 show mls qos map dscp-mutation

show mls qos map dscp-mutation	
目的	DSCP 変換マップを表示します。
Command	show mls qos map dscp-mutation [DSCP-MAP-NAME]
Parameter	DSCP-MAP-NAME（省略可能）：DSCP 変換マップ名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべての DSCP 変換マップを表示する方法を示します。

```
# show mls qos map dscp-mutation

DSCP Mutation: mutemap1 ...(1)
Attaching interface: ...(2)
   Port1/0/1

       0  1  2  3  4  5  6  7  8  9 ...(3)
   ---------------------------------
   00  00 01 02 03 04 05 06 07 08 09
   10  10 11 12 13 14 15 16 17 18 19
   20  20 21 22 23 24 25 26 27 28 29
   30  30 31 32 33 34 35 36 37 38 39
   40  40 41 42 43 44 45 46 47 48 49
   50  50 51 52 53 54 55 56 57 58 59
   60  60 61 62 63
```

項番	説明
(1)	DSCP 変換マップ名を表示します。
(2)	DSCP 変換マップが適用されている受信ポート番号を表示します。
(3)	DSCP 変換マップを表形式で表示します。表の縦軸は DSCP の 10 の位を、横軸は DSCP の 1 の位を表します。交差する点に表示されている数値が変換後 DSCP を表します。

7.1.23 show mls qos interface dscp-mutation

show mls qos interface dscp-mutation	
目的	ポートに適用した DSCP 変換マップを表示します。
Command	show mls qos interface [port PORTS] dscp-mutation
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/2 に適用した DSCP 変換マップを表示する方法を示します。

```
# show mls qos interface port 1/0/1-2 dscp-mutation
 (1)            (2)
 Interface      DSCP Mutation Map
 ------------   --------------------
 Port1/0/1      Mutate Map TEST-MAP1
 Port1/0/2      Mutate Map
```

項番	説明
(1)	ポート番号を表示します。
(2)	DSCP 変換マップ名を表示します。"Mutate Map "の後に設定した DSCP 変換マップ名が表示されます。

7.1.24 show mls qos interface queue-rate-limit

show mls qos interface queue-rate-limit	
目的	送信キューごとの帯域設定を表示します。
Command	show mls qos interface [port PORTS] queue-rate-limit
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/2 の、送信キューごとの帯域設定を表示する方法を示します。

```
# show mls qos interface port 1/0/1-2 queue-rate-limit

Port1/0/1 ...(1)
 (2)    (3)                    (4)
 QID    Min Bandwidth          Max Bandwidth
 ----   --------------------   --------------------
 0      1000 kbps              2000 kbps
 1      No Limit               No Limit
 2      No Limit               No Limit
 3      10%(100000 kbps)       20%(200000 kbps)
 4      No Limit               No Limit
 5      No Limit               No Limit
 6      No Limit               No Limit
 7      No Limit               No Limit
Port1/0/2
 QID    Min Bandwidth          Max Bandwidth
 ----   --------------------   --------------------
 0      1000 kbps              2000 kbps
 1      No Limit               No Limit
 2      No Limit               No Limit
 3      10%                    20%
 4      No Limit               No Limit
 5      No Limit               No Limit
 6      No Limit               No Limit
 7      No Limit               No Limit
```

項番	説明
(1)	ポート番号を表示します。
(2)	送信キューの ID を表示します。
(3)	最小保証帯域(kbps)を表示します。 queue rate-limit コマンドで最小保証帯域をパーセント指定で設定した場合は、「リンクアップポート：パーセント設定値と実際の設定値(kbps)を表示」「リンクダウンポート：パーセント設定値のみ表示」となります。
(4)	最大帯域(kbps)を表示します。 queue rate-limit コマンドで最大帯域をパーセント指定で設定した場合は、「リンクアップポート：パーセント設定値と実際の設定値(kbps)を表示」「リンクダウンポート：パーセント設定値のみ表示」となります。

7.1.25 show mls qos interface rate-limit

show mls qos interface rate-limit	
目的	ポートごとの帯域制限設定を表示します。
Command	show mls qos interface [port PORTS] rate-limit
Parameter	port PORTS (省略可能)：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、すべてのポートの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/4 の、帯域制限設定を表示する方法を示します。

```
# show mls qos interface port 1/0/1-4 rate-limit
 (1)         (2)                  (3)                  (4)           (5)
 Interface   Rx Rate              TX Rate              Rx Burst      Tx Burst
 ----------- -------------------- -------------------- ------------- -------------
 Port1/0/1   1000 kbps            No Limit             64 kbyte      No Limit
 Port1/0/2   No Limit             2000 kbps            No Limit      2000 kbyte
 Port1/0/3   10%(100000 kbps)     20%(200000 kbps)     64 kbyte      64 kbyte
 Port1/0/4   2%                   2000 kbps            64 kbyte      64 kbyte
```

項番	説明
(1)	ポート番号を表示します。
(2)	受信帯域制限機能の帯域制限値(kbps)を表示します。 rate-limit input コマンドで帯域制限値をパーセント指定で設定した場合は、「リンクアップポート：パーセント設定値と実際の設定値(kbps)を表示」「リンクダウンポート：パーセント設定値のみ表示」となります。
(3)	送信帯域制限機能の帯域制限値(kbps)を表示します。 rate-limit output コマンドで帯域制限値をパーセント指定で設定した場合は、「リンクアップポート：パーセント設定値と実際の設定値(kbps)を表示」「リンクダウンポート：パーセント設定値のみ表示」となります。
(4)	受信帯域制限機能のバーストサイズ(KByte)を表示します。
(5)	送信帯域制限機能のバーストサイズ(KByte)を表示します。

7.2 ポリシーマップコマンド

ポリシーマップ関連の設定コマンドは以下のとおりです。

- class-map
- match
- policy-map
- class（Policy Map）
- set
- police
- police cir
- police aggregate
- mls qos aggregate-policer
- service-policy

ポリシーマップ関連の show コマンドは以下のとおりです。

- show class-map
- show policy-map
- show mls qos aggregate-policer

7.2.1 class-map

class-map	
目的	クラスマップを設定します。また、クラスマップ設定モードに遷移します。遷移後のプロンプトは（config-cmap)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	class-map [match-all | match-any] NAME no class-map NAME
Parameter	match-all（省略可能）：クラスマップに複数種類の一致条件（match 設定）が設定されている場合に、AND 条件で最終的な一致条件を決定する場合に指定します。 match-any（省略可能）：クラスマップに複数種類の一致条件（match 設定）が設定されている場合に、OR 条件で最終的な一致条件を決定する場合に指定します。省略した場合は match-any 指定になります。 NAME：クラスマップ名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	クラスマップ名「class-default（デフォルトクラス）」のみ作成済み
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	クラスマップでは、対象となるトラフィックを分類するための一致条件を定義します。クラスマップの match 設定が 1 種類の場合は、一致条件の決定方法は指定不要です。省略した場合は match-any 指定になります。 クラスマップに複数種類の match 設定がある場合は、設定した一致条件の決定方法に従って AND 条件または OR 条件で決定されます。 クラスマップに match access-group name 条件のみが設定されていて、指定したアクセスリストに複数ルールが存在する場合は、各ルールで定義した内容がそれぞれ異なる一致条件になります。このクラスマップにアクションとして通常のポリサーが適

class-map	
	用された場合は、それぞれの一致条件ごとに異なるポリサーが適用されます。 クラスマップの設定例については「クラスマップ(match-any)の設定例」「クラスマップ(match-all)の設定例」を参照してください。
制限・注意	• クラスマップは、デフォルトで作成済みの「class-default」を含めて、最大 255 個設定できます。 • デフォルトで作成済みの「class-default」は削除できません。 • 1 つのクラスマップにおいて、同時に設定できる match 設定は最大 64 個です。 • 一致条件の決定方法が match-all 指定のクラスマップでは、条件が競合する match 設定は同時に設定できません。設定すると、前の設定を上書きします。
バージョン	1.08.02

■ クラスマップ(match-any)の設定例

例(1) 複数の match cos コマンド設定

```
class-map match-any test-class-1
 match cos 3
 match cos 5
```

この設定の場合、クラスマップ test-class-1 の一致条件は以下の 2 種類になります。アクションとして通常のポリサーを適用した場合、以下のそれぞれに異なるポリサーが適用されます。

- CoS 値が 3 のトラフィック
- CoS 値が 5 のトラフィック

例(2) 複数の match dscp コマンド設定

```
class-map match-any test-class-2
 match dscp 0
 match dscp 46
```

この設定の場合、クラスマップ test-class-2 の一致条件は以下の 4 種類になります。アクションとして通常のポリサーを適用した場合、以下のそれぞれに異なるポリサーが適用されます。

- DSCP が 0 の IPv4 トラフィック
- DSCP が 46 の IPv4 トラフィック
- Traffic Class の上位 6bit が 0 (Traffic Class=0～3)の IPv6 トラフィック
- Traffic Class の上位 6bit が 46 (Traffic Class=184～187)の IPv6 トラフィック

例(3) 複数の match ip dscp コマンド設定

```
class-map match-any test-class-3
 match ip dscp 0
 match ip dscp 46
```

この設定の場合、クラスマップ test-class-3 の一致条件は以下の 2 種類になります。アクションとして通常のポリサーを適用した場合、以下のそれぞれに異なるポリサーが適用されます。

- DSCP が 0 の IPv4 トラフィック
- DSCP が 46 の IPv4 トラフィック

例(4) 複数ルールを定義したアクセスリストを指定時の match access-group name コマンド設定

```
ip access-list IPv4-ACL 1999
 10 permit host 192.0.2.100 any
 20 permit host 192.0.2.200 any

class-map match-any test-class-4
```

```
 match access-group name IPv4-ACL
```

この設定の場合、クラスマップ test-class-4 の一致条件は以下の 2 種類になります。アクションとして通常のポリサーを適用した場合、以下のそれぞれに異なるポリサーが適用されます。

- 送信元 IP が 192.0.2.100 の IPv4 トラフィック
- 送信元 IP が 192.0.2.200 の IPv4 トラフィック

例(5) match access-group name コマンドと match ip dscp コマンドを同時に設定

```
ip access-list IPv4-ACL 1999
 10 permit host 192.0.2.100 any
 20 permit host 192.0.2.200 any

class-map match-any test-class-5
 match access-group name IPv4-ACL
 match ip dscp 46
```

この設定の場合、クラスマップ test-class-5 の一致条件は以下の 3 種類になります。アクションとして通常のポリサーを適用した場合、以下のそれぞれに異なるポリサーが適用されます。

- 送信元 IP が 192.0.2.100 の IPv4 トラフィック
- 送信元 IP が 192.0.2.200 の IPv4 トラフィック
- DSCP が 46 の IPv4 トラフィック

■ クラスマップ(match-all)の設定例

例(1) match access-group name コマンドと match ip dscp コマンドを同時に設定

```
ip access-list IPv4-ACL 1999
 10 permit host 192.0.2.100 any
 20 permit host 192.0.2.200 any

class-map match-all test-class-6
 match access-group name IPv4-ACL
 match ip dscp 46
```

この設定の場合、クラスマップ test-class-6 の一致条件は以下の 2 種類になります。アクションとして通常のポリサーを適用した場合、以下のそれぞれに異なるポリサーが適用されます。

- 送信元 IP が 192.0.2.100 で、かつ DSCP が 46 の IPv4 トラフィック
- 送信元 IP が 192.0.2.200 で、かつ DSCP が 46 の IPv4 トラフィック

7.2.2 match

match	
目的	クラスマップの一致条件を定義します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	match access-group name ACL-NAME match cos [inner] COS-LIST match vlan [inner] VLAN-ID-LIST match [ip] dscp DSCP-LIST match [ip] precedence IP-PRECEDENCE-LIST match protocol PROTOCOL-NAME no match access-group name ACL-NAME no match cos [inner] COS-LIST no match vlan [inner] VLAN-ID-LIST

match	
	no match [ip] **dscp** DSCP-LIST **no match** [ip] **precedence** IP-PRECEDENCE-LIST **no match protocol** PROTOCOL-NAME
Parameter	access-group name ACL-NAME：一致条件とするアクセスリストを指定します。指定するアクセスリストでは、処理対象となる条件を permit ルールで設定します。deny ルールはサポートしていません。 cos [inner] COS-LIST：一致条件とする CoS（一番外側の VLAN タグの CoS）を、0～7 の範囲で指定します。inner を指定した場合は、カスタマーVLAN タグ（2 段タグ付きフレームの内側の VLAN タグ）の CoS が対象になります。複数の CoS を指定する場合はコンマで区切るか、ハイフンで範囲を指定します。 vlan [inner] VLAN-ID-LIST：一致条件とする VLAN ID を 1～4094 の範囲で指定します。inner を指定した場合は、カスタマーVLAN タグ（2 段タグ付きフレームの内側の VLAN タグ）の VLAN ID が対象になります。複数の VLAN ID を指定する場合はコンマで区切るか、ハイフンで範囲を指定します。 [ip] dscp DSCP-LIST：一致条件とする DSCP（Differentiated Service Code Point）を、0～63 の範囲で指定します。ip を指定した場合は、IPv4 パケットのみが対象になります。指定しない場合は、IPv4 パケットと IPv6 パケットの両方が対象になります。複数の DSCP を指定する場合はコンマで区切るか、ハイフンで範囲を指定します。 [ip] precedence IP-PRECEDENCE-LIST：一致条件とする IP Precedence を、0～7 の範囲で指定します。ip を指定した場合は、IPv4 パケットのみが対象になります。指定しない場合は、IPv4 パケットと IPv6 パケット（Traffic Class フィールドの上位 3bit の値）の両方が対象になります。複数の IP Precedence を指定する場合はコンマで区切るか、ハイフンで範囲を指定します。 protocol PROTOCOL-NAME：一致条件とするプロトコル名を指定します。
デフォルト	なし
モード	クラスマップ設定モード
特権レベル	レベル：12
ガイドライン	match access-group name 条件で指定するアクセスリストでは、処理対象となる条件を permit ルールで設定します。deny ルールはサポートしていません。 match protocol 条件で指定可能なパラメーターは以下のとおりです。 • arp - IP アドレス解決プロトコル（ARP） • bgp - Border Gateway Protocol • dhcp - Dynamic Host Configuration • dns - Domain Name Server ルックアップ • egp - 外部ゲートウェイプロトコル • ftp - ファイル転送プロトコル • ip - IP（バージョン 4） • ipv6 - IP（バージョン 6） • netbios - NetBIOS • nfs - ネットワークファイルシステム • ntp - 時刻プロトコル • ospf - Open Shortest Path First

match	
	• pppoe - Point-to-Point Protocol over Ethernet • rip - ルーティング情報プロトコル • rtsp - Real-Time Streaming Protocol • ssh - Secure Shell • telnet - Telnet • tftp - Trivial File Transfer Protocol (TFTP) match access-group name 条件を設定したクラスマップを含むポリシーを受信側(input)に適用した場合、指定したアクセスリストの Ingress グループのルールを設定した数使用します。同様に、このポリシーを送信側(output)に適用した場合、Egress グループのルールを設定した数使用します。なお、同一ポリシーを複数ポートに割り当てた場合、割り当てたポートごとにアクセスリストのリソースを消費します。 match cos [inner]条件、または match vlan [inner]条件を設定したクラスマップを含むポリシーを受信側(input)に適用した場合、拡張 MAC アクセスリストの Ingress グループのルールを、CoS または VLAN あたり 1 個使用します。同様に、このポリシーを送信側(output)に適用した場合、Egress グループのルールを CoS または VLAN あたり 1 個使用します。これらの場合、アクセスリスト(ACL)機能の拡張 MAC アクセスリストとは異なり、IPv4 パケットおよび IPv6 パケットに対してもポリシーが適用されます。なお、以下ケースでは、CoS または VLAN あたり 2 個使用します。 • 本条件のポリシーマップで set ip dscp を設定している場合 • 本条件のポリシーマップで set ip precedence を設定し、受信側(input)に適用している場合 match dscp 条件、または match precedence 条件を設定したクラスマップを含むポリシーを受信側(input)に適用した場合、IPv4 アクセスリストおよび IPv6 アクセスリストの Ingress グループのルールを、dscp または precedence 値あたり 1 個使用します。同様に、このポリシーを送信側(output)に適用した場合、Egress グループのルールを dscp または precedence 値あたり 1 個使用します。 match ip dscp 条件、または match ip precedence 条件を設定したクラスマップを含むポリシーを受信側(input)に適用した場合、IPv4 アクセスリストの Ingress グループのルールを、dscp または precedence 値あたり 1 個使用します。同様に、このポリシーを送信側(output)に適用した場合、Egress グループのルールを dscp または precedence 値あたり 1 個使用します。 match protocol 条件を設定した場合は、使用するアクセスリストおよびルール数は、指定されたプロトコルによって異なります。
制限・注意	• 一致条件の決定方法が match-all 指定のクラスマップでは、条件が競合する match 設定は同時に設定できません。設定すると、前の設定を上書きします。 • 同じ種類のアクセスリストを指定した match access-group name 条件は、同一クラスマップ(match-any 指定)には、それぞれ 1 個までしか設定できません。 • 本コマンドで ARP アクセスリストを指定することは未サポートです。 • match access-group name 条件において、拡張エキスパートアクセスリストの cos inner 抽出条件は、送信方向(output)では使用できません。 • match cos inner 条件と、以下の IPv4/IPv6 関連の条件を併用しているクラスマップ(match-all 指定)は、送信方向(output)では使用できません。 • match access-group name 条件で拡張エキスパートアクセスリスト、IP アク

match	
	セスリスト、IPv6 アクセスリストを指定している場合 • match [ip] dscp 条件 • match [ip] precedence 条件 • match protocol 条件(bgp, dhcp, dns, egp, ftp, ip, ipv6, netbios, nfs, ntp, ospf, rip, rtsp, ssh, telnet, tftp)
バージョン	1.08.02

使用例：クラスマップ「class-home-user」で、一致条件にアクセスリスト「acl-home-user」を設定する方法を示します。

```
# configure terminal
(config)# class-map class-home-user
(config-cmap)# match access-group name acl-home-user
(config-cmap)#
```

使用例：クラスマップ「cos」で、一致条件に CoS=1,2,3 を設定する方法を示します。

```
# configure terminal
(config)# class-map cos
(config-cmap)# match cos 1,2,3
(config-cmap)#
```

7.2.3 policy-map

policy-map	
目的	ポリシーマップを設定します。また、ポリシーマップ設定モードに遷移します。遷移後のプロンプトは（config-pmap)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	policy-map NAME no policy-map NAME
Parameter	NAME：ポリシーマップ名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	1 つのポリシーマップを、複数のインターフェースに同時に追加できます。ポリシーマップを新たに追加すると、前のポリシーマップは上書きされます。 ポリシーマップにはクラスマップが含まれています。クラスマップには、プロトコルタイプまたはアプリケーションに基づくパケットのマッチング（とグループへの編成）に使用できる match コマンドが、1 つ以上含まれています。
制限・注意	• 作成できるポリシーマップは最大 255 個です。
バージョン	1.08.02

使用例：ポリシーマップ「test-policy」を設定する方法を示します。

```
# configure terminal
(config)# policy-map test-policy
(config-pmap)#
```

7.2.4 class（Policy Map）

class（Policy Map）	
目的	ポリシーマップに関連付けるクラスマップを設定します。また、ポリシーマップクラス設定モードに遷移します。遷移後のプロンプトは（config-pmap-c)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	class NAME no class NAME
Parameter	NAME：ポリシーマップに関連付けるクラスマップ名を指定します。
デフォルト	class-default（デフォルトクラス）
モード	ポリシーマップ設定モード
特権レベル	レベル：12
ガイドライン	クラスの QoS ポリシーを定義するには、set コマンドを使用できます。 class-default は、デフォルトクラスの予約名です。定義済みクラスと一致しないトラフィックは、すべて class-default として分類されます。指定したクラスマップ名が存在しない場合、トラフィックはクラスに分類されません。
制限・注意	• 最大クラス数は 255 です。
バージョン	1.08.02

使用例：ポリシーマップ policy1 を指定して、クラス「class-dscp-red」のポリシーを定義する方法を示します。DSCP 10、12、14 と一致するパケットは、すべて DSCP 10 とマークされ、1 レートポリサーでポリシングされるように設定しています。

```
# configure terminal
(config)# class-map class-dscp-red
(config-cmap)# match ip dscp 10,12,14
(config-cmap)# exit
(config)# policy-map policy1
(config-pmap)# class class-dscp-red
(config-pmap-c)# set ip dscp 10
(config-pmap-c)# police 1000000 16384 exceed-action set-dscp-transmit 0
(config-pmap-c)#
```

7.2.5 set

set	
目的	一致条件にマッチしたパケットに対するアクションを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	set cos COS set [ip] dscp DSCP set [ip] precedence IP-PRECEDENCE set cos-queue COS-QUEUE no set cos COS no set [ip] dscp DSCP no set [ip] precedence IP-PRECEDENCE no set cos-queue COS-QUEUE
Parameter	cos COS：対象に割り当てる新しい CoS 値を、0～7 の範囲で指定します。

set	
	[ip] dscp DSCP：対象に割り当てる新しい DSCP を、0～63 の範囲で指定します。ip を指定した場合は、IPv4 パケットのみが対象になります。指定しない場合は、IPv4 パケットと IPv6 パケットの両方が対象になります。 [ip] precedence IP-PRECEDENCE：対象に割り当てる新しい IP Precedence を、0～7 の範囲で指定します。このパラメーターはポリシーを受信側(input)に適用した場合のみ動作します。ip を指定した場合は、IPv4 パケットのみが対象になります。指定しない場合は、IPv4 パケットと IPv6 パケット（Traffic Class フィールドの上位 3bit の値）の両方が対象になります。 cos-queue COS-QUEUE：対象に割り当てる送信キュー(CoS キュー)を、0～7 の範囲で指定します。このパラメーターはポリシーを受信側(input)に適用した場合のみ動作します。
デフォルト	なし
モード	ポリシーマップクラス設定モード
特権レベル	レベル：12
ガイドライン	設定が競合しない場合は、1 つのクラスマップに対して複数の set コマンドを設定できます。また、同じクラスマップに set コマンドと police コマンドを同時に設定できます。 set cos コマンドで CoS 値を変更した場合に、priority-queue cos-map コマンド（CoS 値から送信キューへのマッピング設定）によって決定される送信キューは、以下のように決定されます。 • ポリシーを受信側(input)で適用した場合は、対象の set cos コマンドによる変更後の新しい CoS 値を元に決定される。 • ポリシーを送信側(output)で適用した場合は、対象の set cos コマンドによる変更前の CoS 値を元に決定される。 set［ip］dscp コマンド、および set［ip］precedence コマンドで変更された後の値は、CoS 値の決定には影響しません。 set cos-queue コマンドは、対象に割り当てる送信キューを直接指定するコマンドです。このコマンドを適用しても、対象パケットの CoS 値は変更されません。
制限・注意	• set [ip] precedence コマンド、および set cos-queue コマンドは、ポリシーを受信側(input)に適用した場合のみ動作します。ポリシーを送信側(output)に適用した場合は動作しません。 • set [ip] precedence コマンドは、トラフィック初期カラーがグリーンの場合のみ動作します。トラフィック初期カラーがイエロー、またはレッドの場合は動作しません。 • match access-group name 条件で拡張 MAC アクセスリストを指定し、かつ mac access-list enable ip-packets が有効設定の場合に、この一致条件にマッチして対象になった IPv4 パケットに対しては、set ip dscp コマンド、および set ip precedence コマンドは動作しません。set dscp コマンド、および set precedence コマンドは動作します。 • set cos-queue コマンドによる送信キューの変更は、スタック装置を跨がない（受信ポートと同一装置のポートから送信する）トラフィックに対しては動作しますが、スタック装置を跨ぐ（受信ポートと異なるメンバー装置のポートから送信する）トラフィックに対しては動作しません。
バージョン	1.08.02

使用例：ポリシーマップ「policy1」のクラスマップ「class1」で、set ip dscp 10 を設定する方法を示します。

```
# configure terminal
(config)# policy-map policy1
(config-pmap)# class class1
(config-pmap-c)# set ip dscp 10
(config-pmap-c)#
```

7.2.6 police

police	
目的	1 レート 2 カラーポリサー、または 1 レート 3 カラーポリサーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	police KBPS [BURST [BURST-MAX]] [conform-action ACTION] exceed-action ACTION [violate-action ACTION] [color-aware] no police
Parameter	KBPS：平均レートを 0～10,000,000（Kbps）の範囲で指定します。 BURST（省略可能）：標準バーストサイズを 0～16,384（KByte）の範囲で指定します。指定しない場合、標準バーストサイズは 12KByte です。 BURST-MAX（省略可能）：1 レート 3 カラーポリサーとして使用する場合に、最大バーストサイズを 0～16,384（KByte）の範囲で指定します。指定しない場合、最大バーストサイズは 12KByte です。1 レート 2 カラーポリサーとして使用する場合は、最大バーストサイズを指定しても無視されます。 conform-action ACTION（省略可能）：グリーントラフィックに対するアクションを指定します。指定しない場合、デフォルトのアクションは transmit です。 exceed-action ACTION：イエロートラフィックに対するアクションを指定します。 violate-action ACTION（省略可能）：1 レート 3 カラーポリサーとして使用する場合に、レッドトラフィックに対するアクションを指定します。指定しない場合は 1 レート 2 カラーポリサーとして動作します。 ACTION：トラフィックに対するアクションを以下から指定します。 • drop：パケットを廃棄します。 • set-dscp-transmit VALUE：IP DSCP を設定して、新しい IP DSCP でパケットを送信します。 • set-1p-transmit VALUE：CoS 値を設定して、新しい CoS 値でパケットを送信します。 • transmit：パケットを変更せずに送信します。 color-aware（省略可能）：1 レート 3 カラーポリサーでカラーアウェアモードとして使用する場合に指定します。指定しない場合はカラーブラインドモードで動作します。1 レート 2 カラーポリサーとして使用する場合は、本パラメーターを指定しても無視されます。
デフォルト	なし
モード	ポリシーマップクラス設定モード
特権レベル	レベル：12
ガイドライン	本機能のポリサーの帯域計測仕様は、IFG（Inter Frame Gap）と Preamble を含めないで計測する仕様です。

police	
	パケットがインターフェースに到着すると、パケットはトラフィック初期カラーで初期化されます。受信インターフェースが DSCP を信頼する場合、トラフィック初期カラーは DSCP からトラフィック初期カラーへのマップに基づいてマップされます。受信インターフェースが CoS を信頼する場合、トラフィック初期カラーは CoS からトラフィック初期カラーへのマップに基づいてマップされます。 1 レート 2 カラーポリサーは、カラーブラインドモードでだけ動作します。1 レート 3 カラーポリサーは、カラーブラインドモードとカラーアウェアモードで動作します。 カラーブラインドモードでは、パケットの最終カラーは、ポリサーの計測結果だけで決定されます。 カラーアウェアモードでは、パケットの最終カラーは、トラフィック初期カラーとポリサーの計測結果で決定されます。ポリサーの計測結果によっては、トラフィック初期カラーがさらにダウングレードされる場合があります。 ポリサーの計測後は、最終カラーに基づいてアクションが実行されます。グリーントラフィックには conform-action、イエロートラフィックには exceed-action、レッドトラフィックには violate-action が実行されます。アクションを指定する場合、以下のような組み合わせの設定はサポートしていません。 • conform-action を drop に設定し、exceed-action と violate-action に drop 以外を設定する組み合わせ • exceed-action を drop に設定し、violate-action に drop 以外を設定する組み合わせ set コマンドでクラスマップに対して設定するアクションは、クラスマップに属するすべてのパケットに適用されます。 受信方向のポリサーリソースはアクセスリスト 1 グループあたり 128 個、最大で 7 グループ使用可能です。1 レート 2 カラーポリサーを作成すると、1 個のポリサーリソースを使用し、1 レート 3 カラーポリサーを作成すると、2 個のポリサーリソースを使用します。 送信方向のポリサーリソースはアクセスリスト 1 グループあたり 128 個、装置全体で最大 4 グループ使用可能ですが、アクセスリスト種別ごとに以下の上限があります。 • 拡張 MAC アクセスリストおよび IPv4 アクセスリストでは、最大 1 グループの送信方向のポリサーリソースを使用できます。1 レート 2 カラーポリサーは最大 128 個、1 レート 3 カラーポリサーは最大 64 個作成可能です。 • 拡張エキスパートアクセスリストおよび IPv6 アクセスリストでは、最大 2 グループの送信方向のポリサーリソースを使用できます。1 レート 2 カラーポリサー、1 レート 3 カラーポリサーともに最大 128 個作成可能です。
制限・注意	• ループ検知機能を併用している場合は、設定可能なポリサーの最大数が減る制限があります。エラーメッセージ「ERROR: Insufficient ACL resources.」が出力されてポリサーを含むポリシーマップを適用できない場合は、ポリサーの設定数を減らすなどの検討をしてください。 • set-1p-transmit アクションを input 側で適用した場合は、変更後の値を基に priority-queue cos-map 設定に基づいて送信キューが決定されます。output 側に適用した場合は変更前の値を基に priority-queue cos-map 設定に基づいて送信キューが決定されます。 • set-dscp-transmit アクションを input 側/output 側のいずれに適用した場合でも、変更後の値は送信キューの選択に影響しません。

police	
	• クラスマップに対して、police、police cir、または police aggregate のいずれか 1 つのみ設定できます。設定済みの状況で再度設定した場合は、後から設定した内容で上書きされます。
バージョン	1.08.02

使用例：[平均レート=5000Kbps, 標準バーストサイズ=16KByte, conform-action transmit（省略時のデフォルト）, exceed-action drop]で 1 レート 2 カラーポリサーを設定する方法を示します。以下の例では、ポリシーマップ「police-setting」内で、クラスマップ「access-match」にマッチしたパケットに対してポリサーが適用されるように設定しています。また、ポート 1/0/1 で input 側でポリシーマップ「police-setting」を適用しています。

```
# configure terminal
(config)# class-map access-match
(config-cmap)# match access-group name acl_rd
(config-cmap)# exit
(config)# policy-map police-setting
(config-pmap)# class access-match
(config-pmap-c)# police 5000 16 exceed-action drop
(config-pmap-c)# exit
(config-pmap)# exit
(config)# interface port 1/0/1
(config-if-port)# service-policy input police-setting
(config-if-port)#
```

7.2.7 police cir

police cir	
目的	保証帯域（CIR）と最大帯域（PIR）の、2 レート 3 カラーポリサーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	police cir CIR [bc CIR-BURST] pir PIR [be PIR-BURST] [conform-action ACTION] [exceed-action ACTION [violate-action ACTION]] [color-aware] no police
Parameter	CIR：保証帯域を 0～10,000,000（Kbps）の範囲で指定します。 bc CIR-BURST（省略可能）：標準バーストサイズを 0～16,384（KByte）の範囲で指定します。 PIR：最大帯域を 0～10,000,000（Kbps）の範囲で指定します。 be PIR-BURST（省略可能）：最大バーストサイズを 0～16,384（KByte）の範囲で指定します。 conform-action ACTION（省略可能）：グリーントラフィックに対するアクションを指定します。指定しない場合、デフォルトのアクションは transmit です。 exceed-action ACTION（省略可能）：イエロートラフィック（PIR には適合しても、CIR には適合しないパケット）に対するアクションを指定します。指定しない場合、デフォルトのアクションは drop です。 violate-action ACTION（省略可能）：レッドトラフィック（CIR と PIR の両方に適合しなかったパケット）に対するアクションを指定します。指定しない場合、デフォルトのアクションは exceed-action と同一です。 ACTION：トラフィックに対するアクションを以下から指定します。 • drop：パケットを廃棄します。

police cir	
	• set-dscp-transmit VALUE：IP DSCP を設定して、新しい IP DSCP でパケットを送信します。 • set-1p-transmit VALUE：CoS 値を設定して、新しい CoS 値でパケットを送信します。 • transmit：パケットを変更せずに送信します。 color-aware（省略可能）：カラーアウェアモードとして使用する場合に指定します。指定しない場合はカラーブラインドモードで動作します。
デフォルト	なし
モード	ポリシーマップクラス設定モード
特権レベル	レベル：12
ガイドライン	本機能のポリサーの帯域計測仕様は、IFG(Inter Frame Gap)と Preamble を含めないで計測する仕様です。 パケットがインターフェースに到着すると、パケットはトラフィック初期カラーで初期化されます。受信インターフェースが DSCP を信頼する場合、トラフィック初期カラーは DSCP からトラフィック初期カラーへのマップに基づいてマップされます。受信インターフェースが CoS を信頼する場合、トラフィック初期カラーは CoS からトラフィック初期カラーへのマップに基づいてマップされます。 カラーブラインドモードでは、パケットの最終カラーは、ポリサーの計測結果だけで決定されます。 カラーアウェアモードでは、パケットの最終カラーは、トラフィック初期カラーとポリサーの計測結果で決定されます。ポリサーの計測結果によっては、トラフィック初期カラーがさらにダウングレードされる場合があります。 ポリサーの計測後は、最終カラーに基づいてアクションが実行されます。グリーントラフィックには conform-action、イエロートラフィックには exceed-action、レッドトラフィックには violate-action が実行されます。アクションを指定する場合、以下のような組み合わせの設定はサポートしていません。 • conform-action を drop に設定し、exceed-action と violate-action に drop 以外を設定する組み合わせ • exceed-action を drop に設定し、violate-action に drop 以外を設定する組み合わせ set コマンドでクラスマップに対して設定するアクションは、クラスマップに属するすべてのパケットに適用されます。 受信方向のポリサーリソースはアクセスリスト 1 グループあたり 128 個、最大で 7 グループ使用可能です。2 レートポリサーを作成すると、2 個のポリサーリソースを使用します。 送信方向のポリサーリソースはアクセスリスト 1 グループあたり 128 個、装置全体で最大 4 グループ使用可能ですが、アクセスリスト種別ごとに以下の上限があります。 • 拡張 MAC アクセスリストおよび IPv4 アクセスリストでは、最大 1 グループの送信方向のポリサーリソースを使用できます。2 レートポリサーは最大 64 個作成可能です。 • 拡張エキスパートアクセスリストおよび IPv6 アクセスリストでは、最大 2 グループの送信方向のポリサーリソースを使用できます。2 レートポリサーは最大 128 個作成可能です。
制限・注意	• ループ検知機能を併用している場合は、設定可能なポリサーの最大数が減る制限が

police cir	
	あります。エラーメッセージ「ERROR: Insufficient ACL resources.」が出力されてポリサーを含むポリシーマップを適用できない場合は、ポリサーの設定数を減らすなどの検討をしてください。 • set-1p-transmit アクションを input 側で適用した場合は、変更後の値を基に priority-queue cos-map 設定に基づいて送信キューが決定されます。output 側に適用した場合は変更前の値を基に priority-queue cos-map 設定に基づいて送信キューが決定されます。 • set-dscp-transmit アクションを input 側/output 側のいずれに適用した場合でも、変更後の値は送信キューの選択に影響しません。 • クラスマップに対して、police、police cir、または police aggregate のいずれか 1 つのみ設定できます。設定済みの状況で再度設定した場合は、後から設定した内容で上書きされます。
バージョン	1.08.02

使用例：[保証帯域=500Kbps，標準バーストサイズ=10KByte，最大帯域=1000Kbps，最大バーストサイズ=10KByte, conform-action transmit（省略時のデフォルト）, exceed-action set-dscp-transmit 2，violate-action drop]で 2 レート 3 カラーポリサーを設定する方法を示します。以下の例では、ポリシーマップ「POLICY-1」内で、クラスマップ「CLASS-1」にマッチしたパケットに対してポリサーが適用されるように設定しています。また、ポート 1/0/3 で input 側でポリシーマップ「POLICY-1」を適用しています。

```
# configure terminal
(config)# class-map CLASS-1
(config-cmap)# match vlan 10
(config-cmap)# policy-map POLICY-1
(config-pmap)# class CLASS-1
(config-pmap-c)# police cir 500 bc 10 pir 1000 be 10 exceed-action set-dscp-transmit 2
violate-action drop
(config-pmap-c)# exit
(config-pmap)# exit
(config)# interface port 1/0/3
(config-if-port)# service-policy input POLICY-1
(config-if-port)#
```

7.2.8 police aggregate

police aggregate	
目的	ポリシーマップ内のクラスマップに集約ポリサーを適用します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	police aggregate AG-NAME no police
Parameter	AG-NAME：集約ポリサー名を指定します。未定義の集約ポリサー名を指定することもできます。
デフォルト	なし
モード	ポリシーマップクラス設定モード
特権レベル	レベル：12
ガイドライン	本機能のポリサーの帯域計測仕様は、IFG(Inter Frame Gap)と Preamble を含めないで計測する仕様です。 クラスマップのパケットマッチングの条件は、以下の 4 つの種類に分類できます。

police aggregate	
	police aggregate コマンドは、種類が異なるクラスマップに適用できません。 • Layer2：以下のコマンドで作成したクラスマップが分類されます。 • match access-group name ACL-NAME（拡張 MAC アクセスリスト） • match cos [inner] COS-LIST • match vlan [inner] VLAN-LIST • match protocol arp • match protocol pppoe • IPv4：以下のコマンドで作成したクラスマップが分類されます。 • match access-group name ACL-NAME（IP アクセスリスト） • match [ip] dscp DSCP-LIST • match ip precedence IP-PRECEDENCE-LIST • match protocol ip • match protocol netbios • IPv6：以下のコマンドで作成したクラスマップが分類されます。 • match access-group name ACL-NAME（IPv6 アクセスリスト） • match protocol ipv6 • expert：以下のコマンドで作成したクラスマップが分類されます。 • match access-group name ACL-NAME（拡張エキスパートアクセスリスト） クラスマップのパケットマッチングの条件に、IP プロトコルの相対条件が含まれていて、IPv4 または IPv6 パケットの比較が指定されていない場合は、police aggregate コマンドは、IPv4 および IPv6 パケットの両方を比較するまでは、クラスマップに適用できません。つまり、以下のコマンドで作成したクラスマップは、match-all が指定され、IP/IPv6 プロトコルに一致するように指定された場合に限り、police aggregate コマンドを適用できます。 • match protocol dns • match protocol egp • match protocol ftp • match protocol nfs • match protocol ntp • match protocol rip • match protocol ssh • match protocol dhcp • match dscp • match protocol ospf • match protocol rtsp • match protocol tftp • match protocol telnet • match precedence 同一名称の集約ポリサーを複数の受信ポートに適用した場合は、それぞれの受信ポートごとに異なる集約ポリサーが割り当てられて動作します。
制限・注意	• デフォルトのクラスマップ「class-default」では集約ポリサーは適用できません。 • ループ検知機能を併用している場合は、設定可能なポリサーの最大数が減る制限があります。エラーメッセージ「ERROR: Insufficient ACL resources.」が出力され

police aggregate	
	てポリサーを含むポリシーマップを適用できない場合は、ポリサーの設定数を減らすなどの検討をしてください。 • クラスマップに対して、police、police cir、または police aggregate のいずれか 1 つのみ設定できます。設定済みの状況で再度設定した場合は、後から設定した内容で上書きされます。
バージョン	1.08.02

使用例：ポリシーマップ内の複数のクラスマップに対して集約ポリサーを適用する方法を示します。以下の例では、ポリシーマップ「policy2」内のクラスマップ「class1」「class2」「class3」に集約ポリサー「agg_policer1」を適用しています。

```
# configure terminal
(config)# mls qos aggregate-policer agg_policer1 10000 16384 exceed-action drop
(config)# policy-map policy2
(config-pmap)# class class1
(config-pmap-c)# police aggregate agg_policer1
(config-pmap-c)# exit
(config-pmap)# class class2
(config-pmap-c)# police aggregate agg_policer1
(config-pmap-c)# exit
(config-pmap)# class class3
(config-pmap-c)# police aggregate agg_policer1
(config-pmap-c)#
```

7.2.9 mls qos aggregate-policer

mls qos aggregate-policer	
目的	ポリシーマップで使用する、集約ポリサーを定義します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mls qos aggregate-policer AG-NAME KBPS [BURST [BURST-MAX]] [conform-action ACTION] exceed-action ACTION [violate-action ACTION] [color-aware] mls qos aggregate-policer AG-NAME cir CIR [bc CIR-BURST] pir PIR [be PIR-BURST] [conform-action ACTION] [exceed-action ACTION [violate-action ACTION]] [color-aware] no mls qos aggregate-policer AG-NAME
Parameter	AG-NAME：集約ポリサー名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、;|？空白文字 を除いた文字を使用可能です。ただし、先頭は英字のみ指定可能です。 KBPS：平均レートを 0～10,000,000（Kbps）の範囲で指定します。 BURST（省略可能）：標準バーストサイズを 0～16,384（KByte）の範囲で指定します。指定しない場合、標準バーストサイズは 12KByte です。 BURST-MAX（省略可能）：1 レート 3 カラーポリサーとして使用する場合に、最大バーストサイズを 0～16,384（KByte）の範囲で指定します。指定しない場合、最大バーストサイズは 12KByte です。1 レート 2 カラーポリサーとして使用する場合は、最大バーストサイズを指定しても無視されます。 conform-action ACTION（省略可能）：グリーントラフィックに対するアクションを指定します。指定しない場合、デフォルトのアクションは transmit です。

mls qos aggregate-policer	
	exceed-action ACTION（省略可能）：イエロートラフィックに対するアクションを指定します。2 レートポリサーとして使用する場合は省略可能で、その場合デフォルトのアクションは drop です。 violate-action ACTION（省略可能）：レッドトラフィックに対するアクションを指定します。1 レートポリサーの場合は、標準バーストサイズと最大バーストサイズに違反するパケットに対するアクションを指定します。2 レートポリサーの場合は、CIR と PIR の両方に適合しなかったパケットに対して行うアクションを指定します。指定しない場合、1 レートポリサーでは 1 レート 2 カラーポリサーとして動作します。2 レートポリサーでは、デフォルトのアクションは exceed-action と同じです。 ACTION：トラフィックに対するアクションを以下から指定します。 • drop：パケットを廃棄します。 • set-dscp-transmit VALUE：IP DSCP を設定して、新しい IP DSCP でパケットを送信します。 • set-1p-transmit VALUE：CoS 値を設定して、新しい CoS 値でパケットを送信します。 • transmit：パケットを変更せずに送信します。 color-aware（省略可能）：1 レート 3 カラーポリサー、または 2 レート 3 カラーポリサーで、カラーアウェアモードとして使用する場合に指定します。指定しない場合はカラーブラインドモードで動作します。1 レート 2 カラーポリサーとして使用する場合は、本パラメーターを指定しても無視されます。 CIR：保証帯域を 0～10,000,000（Kbps）の範囲で指定します。 bc CIR-BURST（省略可能）：標準バーストサイズを 0～16,384（KByte）の範囲で指定します。 PIR：最大帯域を 0～10,000,000（Kbps）の範囲で指定します。 be PIR-BURST（省略可能）：最大バーストサイズを 0～16,384（KByte）の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本機能のポリサーの帯域計測仕様は、IFG（Inter Frame Gap）と Preamble を含めないで計測する仕様です。 定義できる集約ポリサーは最大 255 個です。 集約ポリサーは、同一ポリシーマップ内の異なるクラスマップ間で共有できます。異なるポリシーマップ間では共有できません。 mls qos aggregate-policer は 1 レートポリサー用、mls qos aggregate-policer cir は 2 レートポリサー用です。 集約ポリサー名に使用できる文字は、スペースを除く以下の文字になります。 • アルファベット："A"～"Z"、"a"～"z" • 数字："0"～"9" • 記号：!#$%&()+,.=@[]^_`{}~/:<>*-'\"
制限・注意	• ループ検知機能を併用している場合は、設定可能なポリサーの最大数が減る制限があります。エラーメッセージ「ERROR: Insufficient ACL resources.」が出力され

mls qos aggregate-policer	
	てポリサーを含むポリシーマップを適用できない場合は、ポリサーの設定数を減らすなどの検討をしてください。 • set-1p-transmit アクションを input 側で適用した場合は、変更後の値を基に priority-queue cos-map 設定に基づいて送信キューが決定されます。output 側に適用した場合は変更前の値を基に priority-queue cos-map 設定に基づいて送信キューが決定されます。 • set-dscp-transmit アクションを input 側/output 側のいずれに適用した場合でも、変更後の値は送信キューの選択に影響しません。 • 設定済みの集約ポリサー名を指定して設定した場合は、後から設定した内容で上書きされます。
バージョン	1.08.02

使用例：集約ポリサー「agg-policer5」を、「1 レート 2 カラーポリサー、平均レート=8000Kbps、標準バーストサイズ=32KByte、conform-action transmit（省略時のデフォルト）、exceed-action drop」で設定する方法を示します。

```
# configure terminal
(config)# mls qos aggregate-policer agg-policer5 8000 32 exceed-action drop
(config)#
```

7.2.10 service-policy

service-policy	
目的	インターフェースに適用するポリシーマップを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	service-policy {input | output} NAME no service-policy {input | output}
Parameter	input：受信方向でポリシーマップを適用する場合に指定します。 output：送信方向でポリシーマップを適用する場合に指定します。 NAME：ポリシーマップ名を指定します。
デフォルト	なし
モード	インターフェース設定モード（port, range）
特権レベル	レベル：12
ガイドライン	1 つのインターフェースには、受信方向と送信方向のそれぞれに 1 個のポリシーマップを適用できます。 すでにインターフェースにポリシーマップが適用されている状態で、別のポリシーマップを指定して再度設定すると、前の設定を上書きします。 ポリシーマップを受信方向で適用すると、match コマンドなどで設定した一致条件に従って、必要な種別のアクセスリストのルール（Ingress グループ）を消費します。 ポリシーマップを送信方向で適用すると、match コマンドなどで設定した一致条件に従って、必要な種別のアクセスリストのルール（Egress グループ）を消費します。 同じポリシーマップを複数ポートに適用した場合でも、適用したポート数分のアクセスリストのルールを消費します。
制限・注意	• 同一ポートにポリシーマップとアクセスリストを併用して設定する場合、任意のパ

service-policy	
	ケットがポリシーマップとアクセスリストの両方にマッチする可能性がありますが、その場合は最も優先順位の高い種別のアクセスリストを使用している設定が優先されます。アクセスリストの優先順位は show access-list resource reserved-priority コマンドで確認できます。 • 任意のパケットがポリシーマップとアクセスリストの両方にマッチして、それが同一種別のアクセスリストの場合は、ポリシーマップが優先されます。 • 同一ポート・同一適用方向で、アクセスリストと「class-default を設定したポリシーマップ」を同時に設定しないでください。同時に設定した場合、そのポート・適用方向では常に「class-default を設定したポリシーマップ」が優先されます。そのため、そのポート・適用方向ではアクセスリストによるパケットフィルターは動作しなくなります。 • 指定したポリシーマップが以下の条件に一致するクラスマップを含む場合は、送信方向(output)に適用することはできません。 • match cos inner 条件と IPv4/IPv6 関連の条件を併用しているクラスマップ(match-all 指定) • 本機能はアクセスリスト機能と同じハードウェアリソース (受信方向に適用時は Ingress グループ、送信方向に適用時は Egress グループ) を使用します。使用するアクセスリスト種別やルール数は設定によります。グループの利用状況は show access-list resource reserved-group コマンドで確認できます。
バージョン	1.08.02

使用例：ポート 1/0/1 で、ポリシーマップ「test-policy」を受信方向に適用する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# service-policy input test-policy
(config-if-port)#
```

7.2.11 show class-map

show class-map	
目的	クラスマップを表示します。
Command	show class-map [NAME]
Parameter	NAME (省略可能)：クラスマップ名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべてのクラスマップを表示する方法を示します。

```
# show class-map

 Class Map match-any c2 ...(1)
  Match protocol ip ...(2)

 Class Map match-any c3
  Match access-group acl_home_user
```

```
Class Map match-any class-default
 Match any
```

項番	説明
(1)	クラスマップ内の複数の match ステートメントを評価する方法、およびクラスマップ名を表示します。 match-all：論理 AND に基づく評価 match-any：論理 OR に基づく評価
(2)	クラスマップの一致条件を表示します。

7.2.12 show policy-map

show policy-map	
目的	ポリシーマップを表示します。
Command	show policy-map [NAME | interface port PORT]
Parameter	NAME（省略可能）：ポリシーマップ名を指定します。 interface port PORT（省略可能）：物理ポートを指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	パラメーター省略時は、すべてのポリシーマップが表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポリシーマップ「policy1」を表示する方法を示します。

```
# show policy-map policy1

 Policy Map policy1 ...(1)
  Class Map police ...(2)
   police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-
transmit 2 violate-action drop ...(3)
```

項番	説明
(1)	ポリシーマップ名を表示します。
(2)	ポリシーマップに割り当てられたクラスマップ名を表示します。
(3)	対象のクラスマップに一致したトラフィックに対して行う操作内容（ポリシング、マーキング）を表示します。

使用例：ポート 1/0/1 に適用したポリシーマップを表示する方法を示します。

```
# show policy-map interface port 1/0/1

 Policy Map: policy1 : output ...(1)
  Class Map police ...(2)
   police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-
transmit 2 violate-action drop ...(3)
```

項番	説明
(1)	ポリシーマップ名、およびポリシーマップの動作対象となるトラフィックの方向（受信／送信）を表示します。
(2)	ポリシーマップに割り当てられたクラスマップ名を表示します。
(3)	対象のクラスマップに一致したトラフィックに対して行う操作内容（ポリシング、マーキング）を表示します。

7.2.13 show mls qos aggregate-policer

show mls qos aggregate-policer	
目的	集約ポリサーを表示します。
Command	show mls qos aggregate-policer [AG-NAME]
Parameter	AG-NAME（省略可能）：集約ポリサー名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：集約ポリサーを表示する方法を示します。

```
# show mls qos aggregate-policer

mls qos aggregate-policer agg-policer5 10 1000 conform-action transmit exceed-action
drop ...(1)
mls qos aggregate-policer agg-policer6 cir 500 bc 10 pir 1000 be 10 conform-action
transmit exceed-action set-dscp-transmit 2 violate-action drop
```

項番	説明
(1)	集約ポリサーの設定を表示します。

8 アクセスリスト(ACL)

8.1 アクセスリスト(ACL)コマンド

アクセスリスト(ACL)関連の共通の設定コマンドは以下のとおりです。

- access-list resequence
- acl-hardware-counter
- list-remark

拡張エキスパートアクセスリスト関連の設定コマンドは以下のとおりです。

- expert access-group
- expert access-list
- permit｜deny（expert access-list）

IP アクセスリスト関連の設定コマンドは以下のとおりです。

- ip access-group
- ip access-list
- permit｜deny（ip access-list）

ARP アクセスリスト関連の設定コマンドは以下のとおりです。

- arp access-group
- arp access-list
- permit｜deny（arp access-list）

IPv6 アクセスリスト関連の設定コマンドは以下のとおりです。

- ipv6 access-group
- ipv6 access-list
- permit｜deny（ipv6 access-list）

拡張 MAC アクセスリスト関連の設定コマンドは以下のとおりです。

- mac access-list enable ip-packets
- mac access-group
- mac access-list
- permit｜deny（mac access-list）

VLAN アクセスマップ関連の設定コマンドは以下のとおりです。

- vlan access-map
- match ip address
- match arp address
- match ipv6 address
- match mac address
- action
- vlan filter

アクセスリスト(ACL)関連の show／操作コマンドは以下のとおりです。

- show access-group
- show access-list
- show access-list resource reserved-group
- show access-list resource reserved-priority
- show vlan access-map
- show vlan filter
- clear acl-hardware-counter

8.1.1 access-list resequence

access-list resequence	
目的	指定したアクセスリストのシーケンス番号の開始値と増分値を設定し、設定済みルールのシーケンス番号を一括変更します。
Command	access-list resequence {ACL-NAME | ACL-NUM} START-SEQ INCREMENT no access-list resequence
Parameter	ACL-NAME：シーケンス番号を変更するアクセスリスト名を指定します。 ACL-NUM：シーケンス番号を変更するアクセスリスト番号を指定します。 START-SEQ：シーケンス番号の開始値を 1～65535 の範囲で指定します。 INCREMENT：シーケンス番号の増分値を 1～32 の範囲で指定します。
デフォルト	開始値：10、増分値：10
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを実行すると、指定したアクセスリストの設定済みルールのシーケンス番号が一括変更されます。例えば、開始値 100、増分値 5 で実行すると、設定済みルールのシーケンス番号は「100、105、110、115、・・・」と変更されます。 特定のアクセスリストの開始値と増分値をデフォルト設定に戻すには、デフォルト設定値（開始値 10、増分値 10）で再度設定してください。 no access-list resequence コマンドを実行すると、すべてのアクセスリストの開始値と増分値がデフォルト設定に戻ります。 access-list resequence コマンド、もしくは no access-list resequence コマンド実行時は、いずれの場合も設定済みルールのシーケンス番号が一括変更されます。
制限・注意	• 本コマンドを実行して一括変更した結果シーケンス番号が最大値（65535）を超える場合には、本コマンドは実行できません。
バージョン	1.08.02

使用例：拡張 IP アクセスリスト「R&D」のシーケンス番号を、開始値=1、増分値=2 で一括変更する方法を示します。

```
# show access-list ip R&D

Extended IP access list R&D(ID: 3999)
    5 permit tcp any 10.30.0.0 0.0.255.255
    10 permit tcp any 10.20.0.0 0.0.255.255
    20 permit tcp any host 10.100.1.2
    30 permit icmp any any
```

```
#
# configure terminal
(config)# access-list resequence R&D 1 2
(config)# end
# show access-list ip R&D

Extended IP access list R&D(ID: 3999)
    1 permit tcp any 10.30.0.0 0.0.255.255
    3 permit tcp any 10.20.0.0 0.0.255.255
    5 permit tcp any host 10.100.1.2
    7 permit icmp any any
```

8.1.2 acl-hardware-counter

acl-hardware-counter	
目的	アクセスリスト機能、または VLAN フィルター機能の VLAN アクセスマップに対して、アクセスリストハードウェアカウンターを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	acl-hardware-counter {access-group {ACL-NAME | ACL-NUM} | vlan-filter MAP-NAME} no acl-hardware-counter {access-group {ACL-NAME | ACL-NUM} | vlan-filter MAP-NAME}
Parameter	access-group {ACL-NAME | ACL-NUM}：ハードウェアカウンターを有効にするアクセスリスト名、またはアクセスリスト番号を指定します。 vlan-filter MAP-NAME：ハードウェアカウンターを有効にする VLAN アクセスマップ名を指定します。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	通常のアクセスリスト（ip access-group コマンドなどでインターフェースに適用してパケットフィルターとして使用する場合）でハードウェアカウンターを有効にするには、access-group パラメーターを指定して設定します。有効にしたアクセスリストの各ルールにマッチしたパケット数がカウントされます。カウンター確認コマンドとクリアコマンドは以下になります。 • 確認コマンド：show access-list {ip | arp | mac | expert | ipv6} • クリアコマンド：clear acl-hardware-counter access-group VLAN フィルター機能の VLAN アクセスマップでハードウェアカウンターを有効にするには、vlan-filter パラメーターを指定して設定します。有効にした VLAN アクセスマップの各サブマップにマッチした受信パケット数がカウントされます。カウンター確認コマンドとクリアコマンドは以下になります。 • 確認コマンド：show vlan access-map • クリアコマンド：clear acl-hardware-counter vlan-filter
制限・注意	• VLAN アクセスマップのハードウェアカウンターでは、show vlan access-map コマンドでサブマップ単位のカウンターが使用できます。VLAN アクセスマップに関連付けたアクセスリストに複数のルールが設定されている場合に、ルールごとのカウントを確認する方法はありません。 • 同一ポートに複数種別のアクセスリストを設定していて、任意のパケットが複数種別のアクセスリストにマッチする場合、アクションは最も優先順位の高いアクセスリスト（優先順位は show access-list resource reserved-priority コマンドで確認可

acl-hardware-counter	
	能) のアクションが採用されますが、カウンターは以下のように動作します。 • 受信方向(Ingress)の場合、任意のパケットがマッチした複数種別のすべてのアクセスリストでカウント • 送信方向(Egress)の場合、アクションが採用された最も優先順位の高いアクセスリストでのみカウント • 通常のアクセスリスト使用以外の、他機能のコマンドで指定したアクセスリストの場合は、本設定を実施してもアクセスリストハードウェアカウンターを使用できません。使用できない主なケースを以下に示します。 • PD モニタリングの ACL モードで使用中のアクセスリスト • IGMP スヌーピング、MLD スヌーピング関連のコマンドで使用中のアクセスリスト • ポリシーマップ関連のコマンドで使用中のアクセスリスト • access-class コマンド、ping access-class コマンド、snmp-server community コマンド、snmp-server user コマンド、snmp-server group コマンドで指定したアクセスリスト • インターフェースに適用済みのアクセスリスト、または VLAN に適用済みの VLAN アクセスマップに対してアクセスリストハードウェアカウンターを有効／無効にする場合、一時的に対象のアクセスリストまたは VLAN アクセスマップの当該ルールが無効となります。
バージョン	1.08.02

使用例：アクセスリスト名 abc を指定して、アクセスリストハードウェアカウンターを有効にする方法を示します。

```
# configure terminal
(config)# acl-hardware-counter access-group abc
(config)#
```

8.1.3 list-remark

list-remark	
目的	指定したアクセスリストに備考情報を追加します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	list-remark STRING no list-remark
Parameter	STRING：備考情報を最大 256 文字で指定します。ASCII コードの印字可能な文字のうち、? を除いた文字を使用可能です。スペースも使用できます。
デフォルト	なし
モード	アクセスリスト設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：アクセスリストに備考情報を追加する方法を示します。

```
# configure terminal
```

```
(config)# ip access-list extended R&D
(config-ip-ext-acl)# 10 permit host 10.2.2.1 any
(config-ip-ext-acl)# 20 permit host 10.2.2.2 any
(config-ip-ext-acl)# list-remark This access-list is use to match any IP packets from
host 10.2.2.1 and 10.2.2.2.
(config-ip-ext-acl)# end
#
# show access-list ip

Extended IP access list R&D(ID: 3999)
    10 permit host 10.2.2.1 any
    20 permit host 10.2.2.2 any
  This access-list is use to match any IP packets from host 10.2.2.1 and 10.2.2.2.
```

8.1.4 expert access-group

expert access-group	
目的	インターフェースに適用する拡張エキスパートアクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	expert access-group {NAME | NUM} [in | out] no expert access-group [NAME | NUM] [in | out]
Parameter	NAME：拡張エキスパートアクセスリスト名を指定します。 NUM：拡張エキスパートアクセスリスト番号を 8000～9999 の範囲で指定します。 in（省略可能）：受信トラフィックをチェックする場合に指定します。方向を省略して設定した場合は in が適用されます。 out（省略可能）：送信トラフィックをチェックする場合に指定します。
デフォルト	なし
モード	インターフェース設定モード(port, range（in パラメーター指定時）)
特権レベル	レベル：12
ガイドライン	拡張エキスパートアクセスリストは、IPv4 パケットのみがチェック対象になります。 すでにインターフェースに設定されている状態で、別の拡張エキスパートアクセスリストを指定して再度設定すると、前の設定を上書きします。 同一インターフェースには同じ種類のアクセスリストは 1 つしか適用できませんが、異なる種類のアクセスリストは同一インターフェースに適用できます。 アクセスリストを適用すると、装置のアクセスリスト用のリソースを消費します。ApresiaNP2500 シリーズでは、装置全体で Ingress グループ用に 7 グループ（Group 1～7：各 256 リソース）、Egress グループ用に 4 グループ（Group 0～3：各 128 リソース）が用意されています。拡張エキスパートアクセスリストでの 1 ルールあたりのリソース消費量は以下になります。 • Ingress グループの場合：2 リソース(同一グループ) • Egress グループの場合：連続した 2 グループで 1 リソースずつ、合計 2 リソース使用 連続した 2 グループの使用可能パターンは以下になります。以下の組み合わせで占有できない状況では、拡張エキスパートアクセスリストを送信方向に適用できません。 • Egress グループの場合：Group(0,1)、Group(2,3) ApresiaNP2500 シリーズですべてのリソースを拡張エキスパートアクセスリストで使用する場合、最大設定可能な拡張エキスパートアクセスリストのルール数は以下に

expert access-group	
	なります。 • Ingress グループの場合：最大 896 個 • Egress グループの場合：最大 256 個 L4 ポート番号の複数指定で使用する比較演算子（lt, gt, neq）と範囲指定パラメーター（range）は、受信方向のアクセスリストでのみ使用できます。送信方向のアクセスリストに適用しても、警告メッセージが出力されて動作しません。また、この比較演算子（lt, gt, neq）と範囲指定パラメーター（range）は、装置全体で異なる指定パターンの設定を最大 32 個まで使用できます。
制限・注意	• 抽出条件「クラス ID (class)」は、受信方向のアクセスリストでのみ使用できます。送信方向のアクセスリストに適用しないでください。 • 同一名称または同一番号のアクセスリストを、複数の送信ポート(out パラメーター)に適用することはできません。 • 同じ拡張エキスパートアクセスリストを複数の受信ポート(in パラメーター)に適用した場合の構成情報の表示は以下になります。 • AEOS-NP2500 Ver. 1.12.01 以降では、同じ拡張エキスパートアクセスリストを適用した複数の受信ポートを range 表示でまとめて表示 • AEOS-NP2500 Ver. 1.12.01 より前のバージョンでは、受信ポートごとの表示 • 同一ポートに複数種別のアクセスリストを設定していると、任意のパケットが複数のアクセスリストにマッチする可能性がありますが、その場合は最も優先順位の高いアクセスリストのアクションが採用されます。アクセスリストの優先順位は show access-list resource reserved-priority コマンドで確認できます。 • 同一ポート・同一適用方向で、アクセスリストと「class-default を設定したポリシーマップ」を同時に設定しないでください。同時に設定した場合、そのポート・適用方向では常に「class-default を設定したポリシーマップ」が優先されます。そのため、そのポート・適用方向ではアクセスリストによるパケットフィルターは動作しなくなります。 • インターフェースに適用したアクセスリストを異なるアクセスリストで上書きした場合、一時的に当該ルールが無効となります。そのため、アクセスリストの設定変更時には、インターフェースへの適用が完了するまでの間、当該ルールが適用されません。
バージョン	1.08.02 1.12.01：構成情報での表示仕様変更

使用例：ポート 1/0/1 において、設定済みの拡張エキスパートアクセスリスト「EX-ACL」を、受信方向で適用する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# expert access-group EX-ACL in
(config-if-port)#
```

8.1.5 expert access-list

expert access-list	
目的	拡張エキスパートアクセスリストを設定します。また、拡張エキスパートアクセスリスト設定モードに遷移します。遷移後のプロンプトは（config-exp-nacl)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。

expert access-list	
Command	expert access-list extended NAME [NUM] no expert access-list extended {NAME | NUM}
Parameter	NAME：拡張エキスパートアクセスリスト名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、; | ? 空白文字 を除いた文字を使用可能です。ただし、先頭は英字のみ指定可能です。 NUM（省略可能）：拡張エキスパートアクセスリスト番号を手動で割り当てる場合に、8000～9999 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	アクセスリスト名は、すべての種類のアクセスリスト内で一意になるように設定してください。なお、アクセスリスト名に使用する文字は大文字と小文字が区別されます。 拡張エキスパートアクセスリスト番号を指定しない場合は、拡張エキスパートアクセスリスト番号の範囲で、未使用の番号の中から最大の値が自動的に割り当てられます。
制限・注意	-
バージョン	1.08.02

使用例：拡張エキスパートアクセスリスト「EX-ACL」を作成し、拡張エキスパートアクセスリスト設定モードに遷移する方法を示します。

```
# configure terminal
(config)# expert access-list extended EX-ACL
(config-exp-nacl)#
```

8.1.6 permit | deny (expert access-list)

permit | deny (expert access-list)	
目的	拡張エキスパートアクセスリストで、permit（抽出対象を許可するアクション）のルール、または deny（抽出対象を拒否するアクション）のルールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	[SEQ] {permit [authentication-bypass] | deny} tcp CONDITION [SEQ] {permit [authentication-bypass] | deny} udp CONDITION [SEQ] {permit [authentication-bypass] | deny} icmp CONDITION [SEQ] {permit [authentication-bypass] | deny} [PROTOCOL] CONDITION no SEQ
Parameter	SEQ（省略可能）：シーケンス番号を 1～65535 の範囲で指定します。小さい番号ほど、許可/拒否のルールの優先度が高くなります。 permit：許可するアクションのルールとして設定する場合に指定します。 permit authentication-bypass：AccessDefender 認証のための認証バイパスエントリーとして設定する場合に指定します。 deny：拒否するアクションのルールとして設定する場合に指定します。 tcp：TCP パケットを抽出対象にする場合に指定します。

permit｜deny (expert access-list)	
	udp：UDP パケットを抽出対象にする場合に指定します。 icmp：ICMP パケットを抽出対象にする場合に指定します。 PROTOCOL（省略可能）：抽出対象にする IP プロトコル番号を 0～255 の範囲で指定するか、以下の定義済みパラメーターで指定します。なお、51(Authentication Header)指定は未サポートです。 • igmp(2) gre(47) esp(50) eigrp(88) ospf(89) ipinip(94) pim(103) pcp(108) vrrp(112) CONDITION：使用する抽出条件を指定します。詳細は「拡張エキスパートアクセスリストのタイプごとの抽出条件一覧」と「拡張エキスパートアクセスリストの抽出条件」を参照。
デフォルト	なし
モード	拡張エキスパートアクセスリスト設定モード
特権レベル	レベル：12
ガイドライン	シーケンス番号を指定せずに設定した場合、開始値（デフォルト設定では 10）から増分値（デフォルト設定では 10）でインクリメントした番号のうち、まだ使用されていない一番小さい番号が自動的に割り当てられます。 開始値と増分値を変更するには、access-list resequence コマンドを使用します。なお、access-list resequence コマンドを実行した時点で、指定したアクセスリストの設定済みルールのシーケンス番号が一括変更されます。 シーケンス番号を手動で割り当てる場合、将来の拡張のためにシーケンス番号を「10、20、30、・・・」と、間を飛ばして設定することもできます。 AccessDefender 認証ポートに適用したアクセスリストで、permit ルール、または認証バイパスエントリー(permit authentication-bypass)にマッチした場合は、未認証状態でも中継は許可されます。なお、permit ルールと認証バイパスエントリーの違いは以下のとおりです。 • permit ルールに一致したパケットは、MAC 認証が有効な場合は、MAC 認証のための CPU コピーも行われます。 • 認証バイパスエントリー(permit authentication-bypass)に一致したパケットは、MAC 認証が有効な場合でも、MAC 認証のための CPU コピーは行われません。ただし、MAC 認証と関係なく CPU 宛てにコピーされるパケットは、たとえ認証バイパスエントリーにマッチしても、CPU コピーされることに注意してください。(例：IP アドレス設定時の自局 IP アドレス宛てパケットや任意宛ての ARP Request パケットなど、各機能有効時に CPU 処理やソフトウェア中継されるパケットなど) 以下の抽出条件をグループ指定する場合は、ワイルドカードビットを指定します。ワイルドカードビットを 1 で指定したビットが any 扱いになります。(例：192.0.2.0 0.0.0.255 と指定した場合は 192.0.2.0～192.0.2.255 がチェック対象になる) • 送信元 IP アドレス (SRC-IP-ADDR SRC-IP-WILDCARD) • 送信元 MAC アドレス (SRC-MAC-ADDR SRC-MAC-WILDCARD) • 宛先 IP アドレス (DST-IP-ADDR DST-IP-WILDCARD) • 宛先 MAC アドレス (DST-MAC-ADDR DST-MAC-WILDCARD) 抽出条件「送信元 MAC アドレス」と「宛先 MAC アドレス」で指定する MAC アドレスとワイルドカードビットは、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。

permit｜deny (expert access-list)	
	• 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX）
制限・注意	• IP プロトコル番号を 51(Authentication Header)で指定して使用することは未サポートです。 • シーケンス番号は、アクセスリストの領域内で一意にしてください。すでに存在するシーケンス番号を入力すると、エラーメッセージが表示されます。 • IP プロトコル番号や L4 ポート番号などを数値指定で設定しても、一致する定義済みパラメーターが存在する場合は、構成情報では定義済みパラメーターで表示されます。
バージョン	1.08.02

■ 拡張エキスパートアクセスリストのタイプごとの抽出条件一覧

タイプ	送信元			宛先			TCP Flag	ICMP	CoS	VLAN ID	フラグメント	DSCP	クラス ID
	IP	MAC	L4	IP	MAC	L4							
tcp	○	○	○	○	○	○	○	–	○	○	–	○	○
udp	○	○	○	○	○	○	–	–	○	○	–	○	○
icmp	○	○	–	○	○	–	–	○	○	○	–	○	○
PROTOCOL	○	○	–	○	○	–	–	–	○	○	○	○	○

※ 複数の抽出条件を指定する場合は、この表に記載した左側の抽出条件から順番に指定する。

■ 拡張エキスパートアクセスリストの抽出条件

抽出条件	概要
送信元 IP アドレス	any：すべての送信元 IP アドレスを指定 host SRC-IP-ADDR：特定の送信元 IP アドレスを指定 SRC-IP-ADDR SRC-IP-WILDCARD：送信元 IP アドレスのグループを指定
送信元 MAC アドレス	any：すべての送信元 MAC アドレスを指定 host SRC-MAC-ADDR：特定の送信元 MAC アドレスを指定 SRC-MAC-ADDR SRC-MAC-WILDCARD：送信元 MAC アドレスのグループを指定
送信元 L4 ポート番号 (省略可能)	{eq｜lt｜gt｜neq} SRC-L4-PORT：比較演算子を使用して送信元 L4 ポート番号を 0～65535 の範囲で指定します。lt, gt, neq は、受信方向のアクセスリストでのみ使用できます。 • eq：指定した L4 ポート番号と等しい場合にマッチ • lt：指定した L4 ポート番号より小さい場合にマッチ • gt：指定した L4 ポート番号より大きい場合にマッチ • neq：指定した L4 ポート番号と等しくない場合にマッチ range MIN-SRC-L4-PORT MAX-SRC-L4-PORT：送信元 L4 ポート番号を範囲で指定します。受信方向のアクセスリストでのみ使用できます。

抽出条件	概要
	L4 ポート番号は以下の定義済みパラメーターでも指定できます。 • tcp の場合：bgp(179) chargen(19) daytime(13) discard(9) domain(53) echo(7) finger(79) ftp(21) ftp-data(20) gopher(70) hostname(101) http(80) ident(113) irc(194) klogin(543) kshell(544) login(513) lpd(515) nntp(119) pop2(109) pop3(110) rexec(512) shell(514) smtp(25) snpp(444) sunrpc(111) tacacs(49) telnet(23) time(37) uucp(540) whois(43) • udp の場合：biff(512) bootpc(68) bootps(67) discard(9) domain(53) echo(7) irc(194) isakmp(500) mobile-ip(434) nameserver(42) nat-t(4500) netbios-dgm(138) netbios-ns(137) netbios-ss(139) ntp(123) rip(520) snmp(161) snmptrap(162) snpp(444) sunrpc(111) syslog(514) tacacs(49) talk(517) tftp(69) time(37) who(513) xdmcp(177)
宛先 IP アドレス	any：すべての宛先 IP アドレスを指定 host DST-IP-ADDR：特定の宛先 IP アドレスを指定 DST-IP-ADDR DST-IP-WILDCARD：宛先 IP アドレスのグループを指定
宛先 MAC アドレス	any：すべての宛先 MAC アドレスを指定 host DST-MAC-ADDR：特定の宛先 MAC アドレスを指定 DST-MAC-ADDR DST-MAC-WILDCARD：宛先 MAC アドレスのグループを指定
宛先 L4 ポート番号 (省略可能)	{eq｜lt｜gt｜neq} DST-L4-PORT：比較演算子を使用して宛先 L4 ポート番号を 0～65535 の範囲で指定します。lt, gt, neq は、受信方向のアクセスリストでのみ使用できます。 • eq：指定した L4 ポート番号と等しい場合にマッチ • lt：指定した L4 ポート番号より小さい場合にマッチ • gt：指定した L4 ポート番号より大きい場合にマッチ • neq：指定した L4 ポート番号と等しくない場合にマッチ range MIN-DST-L4-PORT MAX-DST-L4-PORT：宛先 L4 ポート番号を範囲で指定します。受信方向のアクセスリストでのみ使用できます。 L4 ポート番号は定義済みパラメーターでも指定できます。定義済みパラメーターは送信元 L4 ポート番号を参照。
TCP フラグ (省略可能)	TCP フラグを、ack(acknowledge), fin(finish), psh(push), rst(reset), syn(synchronize), urg(urgent)パラメーターで指定します。 同一ルールで複数の TCP フラグを指定する場合は、ack, fin, psh, rst, syn, urg の順番で有効にするパラメーターを指定して設定します。
ICMP メッセージ (省略可能)	ICMP メッセージをタイプ(0～255)とコード(0～255)で指定するか、もしくは以下の定義済みパラメーターで指定します。 alternate-address(6,-) bad-length(12,2) conversion-error(31,-) echo(8,0) echo-reply(0,0) host-isolated(3,8) host-precedence-violation(3,14) host-prohibited(3,10) host-redirect(5,1) host-tos-redirect(5,3) host-tos-unreachable(3,12) host-unknown(3,7) host-unreachable(3,1) information-reply(16,0) information-request(15,0) mask-reply(18,0)

抽出条件	概要
	mask-request(17,0) mobile-redirect(32,-) net-prohibited(3,9) net-redirect(5,0) net-tos-redirect(5,2) net-tos-unreachable(3,11) net-unknown(3,6) net-unreachable(3,0) option-missing(12,1) packet-fragment(3,4) parameter-problem(12,-) pointer-indicates-error(12,0) port-unreachable(3,3) precedence-cutoff(3,15) protocol-unreachable(3,2) reassembly-timeout(11,1) redirect-message(5,-) router-advertisement(9,0) router-solicitation(10,0) source-quench(4,0) source-route-failed(3,5) time-exceeded(11,-) timestamp-reply(14,0) timestamp-request(13,0) traceroute(30,0) ttl-expired(11,0) unreachable(3,-)
CoS (省略可能)	cos OUTER-COS [inner INNER-COS]：外側のサービス VLAN タグの CoS を 0～7 の範囲で指定します。また、内側のカスタマーVLAN タグの CoS も 0～7 の範囲で指定できます。
VLAN ID (省略可能)	vlan OUTER-VLAN [inner INNER-VLAN]：外側のサービス VLAN タグの VLAN ID を 1～4094 の範囲で指定します。また、内側のカスタマーVLAN タグの VLAN ID も 1～4094 の範囲で指定できます。
フラグメント (省略可能)	fragments：フラグメントされたパケットを指定します。
DSCP (省略可能)	precedence PRECEDENCE tos TOS｜dscp DSCP：IP ヘッダーの ToS フィールド(ip precedence(0～7), tos(0～15))、もしくは DSCP(0～63)を指定します。それぞれ以下の定義済みパラメーターでも指定できます。 • ip precedence：routine(0) priority(1) immediate(2) flash(3) flash-override(4) critical(5) internet(6) network(7) • tos：normal(0) min-monetary-cost(1) max-reliability(2) max-throughput(4) min-delay(8) • DSCP：af11(10) af12(12) af13(14) af21(18) af22(20) af23(22) af31(26) af32(28) af33(30) af41(34) af42(36) af43(38) cs1(8) cs2(16) cs3(24) cs4(32) cs5(40) cs6(48) cs7(56) default(0) ef(46)
クラス ID (省略可能)	class CLASS-ID：認証端末クラス ID を 1～4095 の範囲で指定します。受信方向のアクセスリストでのみ使用できます。

使用例：拡張エキスパートアクセスリスト「EX-ACL」で、シーケンス番号 10、deny、抽出条件「送信元 IP アドレス 192.0.2.100、送信元 MAC アドレス 00:00:5E:00:53:00 の TCP パケット」のルールを設定する方法を示します。

```
# configure terminal
(config)# expert access-list extended EX-ACL
(config-exp-nacl)# 10 deny tcp host 192.0.2.100 host 0000.5e00.5300 any any
(config-exp-nacl)#
```

8.1.7 ip access-group

ip access-group	
目的	インターフェースに適用する IP アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip access-group {NAME｜NUM} [in｜out] no ip access-group [NAME｜NUM] [in｜out]
Parameter	NAME：IP アクセスリスト名を指定します。

ip access-group	
	NUM：IP アクセスリスト番号を 1～3999 の範囲で指定します。 in（省略可能）：受信トラフィックをチェックする場合に指定します。方向を省略して設定した場合は in が適用されます。 out（省略可能）：送信トラフィックをチェックする場合に指定します。
デフォルト	なし
モード	インターフェース設定モード(port, range（in パラメーター指定時）)
特権レベル	レベル：12
ガイドライン	IP アクセスリストは、IPv4 パケットのみがチェック対象になります。 すでにインターフェースに設定されている状態で、別の IP アクセスリストを指定して再度設定すると、前の設定を上書きします。 同一インターフェースには同じ種類のアクセスリストは 1 つしか適用できませんが、異なる種類のアクセスリストは同一インターフェースに適用できます。 アクセスリストを適用すると、装置のアクセスリスト用のリソースを消費します。ApresiaNP2500 シリーズでは、装置全体で Ingress グループ用に 7 グループ（Group 1～7：各 256 リソース)、Egress グループ用に 4 グループ（Group 0～3：各 128 リソース）が用意されています。IP アクセスリストでの 1 ルールあたりのリソース消費量は以下になります。 • Ingress グループの場合：2 リソース(同一グループ) • Egress グループの場合：1 リソース ApresiaNP2500 シリーズですべてのリソースを IP アクセスリストで使用する場合、最大設定可能な IP アクセスリストのルール数は以下になります。 • Ingress グループの場合：最大 896 個 • Egress グループの場合：最大 512 個 本コマンドを適用した際には、残りのリソースをすべて IP アクセスリストで使用した場合の設定可能ルール数が表示されます。 L4 ポート番号の複数指定で使用する比較演算子（lt, gt, neq）と範囲指定パラメーター（range）は、受信方向のアクセスリストでのみ使用できます。送信方向のアクセスリストに適用しても、警告メッセージが出力されて動作しません。また、この比較演算子（lt, gt, neq）と範囲指定パラメーター（range）は、装置全体で異なる指定パターンの設定を最大 32 個まで使用できます。
制限・注意	• 抽出条件「クラス ID (class)」は、受信方向のアクセスリストでのみ使用できます。送信方向のアクセスリストに適用しないでください。 • 同一名称または同一番号のアクセスリストを、複数の送信ポート(out パラメーター)に適用することはできません。 • 同じ IP アクセスリストを複数の受信ポート(in パラメーター)に適用した場合の構成情報の表示は以下になります。 • AEOS-NP2500 Ver. 1.12.01 以降では、同じ IP アクセスリストを適用した複数の受信ポートを range 表示でまとめて表示 • AEOS-NP2500 Ver. 1.12.01 より前のバージョンでは、受信ポートごとの表示 • 同一ポートに複数種別のアクセスリストを設定していると、任意のパケットが複数のアクセスリストにマッチする可能性がありますが、その場合は最も優先順位の高いアクセスリストのアクションが採用されます。アクセスリストの優先順位は show

ip access-group	
	access-list resource reserved-priority コマンドで確認できます。 • 同一ポート・同一適用方向で、アクセスリストと「class-default を設定したポリシーマップ」を同時に設定しないでください。同時に設定した場合、そのポート・適用方向では常に「class-default を設定したポリシーマップ」が優先されます。そのため、そのポート・適用方向ではアクセスリストによるパケットフィルターは動作しなくなります。 • インターフェースに適用したアクセスリストを異なるアクセスリストで上書きした場合、一時的に当該ルールが無効となります。そのため、アクセスリストの設定変更時には、インターフェースへの適用が完了するまでの間、当該ルールが適用されません。
バージョン	1.08.02 1.12.01：構成情報での表示仕様変更

使用例：ポート 1/0/1 において、設定済みの IP アクセスリスト「IPv4-ACL」を、受信方向で適用する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ip access-group IPv4-ACL in

The remaining applicable IP related access entries are 893
(config-if-port)#
```

8.1.8 ip access-list

ip access-list	
目的	IP アクセスリストを設定します。また、IP アクセスリスト設定モードに遷移します。遷移後のプロンプトは、標準 IP アクセスリストの場合は（config-ip-acl)# に、拡張 IP アクセスリストの場合は（config-ip-ext-acl)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ip access-list [extended] NAME [NUM] no ip access-list [extended] {NAME | NUM}
Parameter	extended（省略可能）：拡張 IP アクセスリストを作成する場合に指定します。省略した場合は標準 IP アクセスリストになります。 NAME：IP アクセスリスト名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、;｜？空白文字 を除いた文字を使用可能です。ただし、先頭は英字のみ指定可能です。 NUM（省略可能）：IP アクセスリスト番号を手動で割り当てる場合に、標準 IP アクセスリストは 1～1999 の範囲で、拡張 IP アクセスリストは 2000～3999 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	アクセスリスト名は、すべての種類のアクセスリスト内で一意になるように設定してください。なお、アクセスリスト名に使用する文字は大文字と小文字が区別されます。 IP アクセスリスト番号を指定しない場合は、IP アクセスリスト番号の範囲で、未使

ip access-list	
	用の番号の中から最大の値が自動的に割り当てられます。
制限・注意	-
バージョン	1.08.02

使用例：標準 IP アクセスリスト「IPv4-ACL」を作成し、IP アクセスリスト設定モードに遷移する方法を示します。

```
# configure terminal
(config)# ip access-list IPv4-ACL
(config-ip-acl)#
```

8.1.9 permit | deny (ip access-list)

permit | deny (ip access-list)	
目的	IP アクセスリストで、permit（抽出対象を許可するアクション）のルール、または deny（抽出対象を拒否するアクション）のルールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	■ 拡張 IP アクセスリスト [SEQ] {permit [authentication-bypass] | deny} tcp CONDITION [SEQ] {permit [authentication-bypass] | deny} udp CONDITION [SEQ] {permit [authentication-bypass] | deny} icmp CONDITION [SEQ] {permit [authentication-bypass] | deny} [PROTOCOL | protocol-id ID] CONDITION ■ 標準 IP アクセスリスト [SEQ] {permit [authentication-bypass] | deny} CONDITION ■ 削除コマンド no SEQ
Parameter	SEQ（省略可能）：シーケンス番号を 1～65535 の範囲で指定します。小さい番号ほど、許可/拒否のルールの優先度が高くなります。 permit：許可するアクションのルールとして設定する場合に指定します。 permit authentication-bypass：AccessDefender 認証のための認証バイパスエントリーとして設定する場合に指定します。 deny：拒否するアクションのルールとして設定する場合に指定します。 tcp：TCP パケットを抽出対象にする場合に指定します。 udp：UDP パケットを抽出対象にする場合に指定します。 icmp：ICMP パケットを抽出対象にする場合に指定します。 PROTOCOL（省略可能）：抽出対象にする IP プロトコル番号を、以下の定義済みパラメーターで指定します。 • igmp(2) gre(47) esp(50) eigrp(88) ospf(89) ipinip(94) pim(103) pcp(108) vrrp(112) protocol-id ID（省略可能）：抽出対象にする IP プロトコル番号を 0～255 の範囲で指定します。なお、51(Authentication Header)指定は未サポートです。 CONDITION：使用する抽出条件を指定します。詳細は「IP アクセスリストのタイ

permit｜deny (ip access-list)	
	プごとの抽出条件一覧」と「IP アクセスリストの抽出条件」を参照。
デフォルト	なし
モード	IP アクセスリスト設定モード
特権レベル	レベル：12
ガイドライン	シーケンス番号を指定せずに設定した場合、開始値（デフォルト設定では 10）から増分値（デフォルト設定では 10）でインクリメントした番号のうち、まだ使用されていない一番小さい番号が自動的に割り当てられます。 開始値と増分値を変更するには、access-list resequence コマンドを使用します。なお、access-list resequence コマンドを実行した時点で、指定したアクセスリストの設定済みルールのシーケンス番号が一括変更されます。 シーケンス番号を手動で割り当てる場合、将来の拡張のためにシーケンス番号を「10、20、30、・・・」と、間を飛ばして設定することもできます。 AccessDefender 認証ポートに適用したアクセスリストで、permit ルール、または認証バイパスエントリー(permit authentication-bypass)にマッチした場合は、未認証状態でも中継は許可されます。なお、permit ルールと認証バイパスエントリーの違いは以下のとおりです。 • permit ルールに一致したパケットは、MAC 認証が有効な場合は、MAC 認証のための CPU コピーも行われます。 • 認証バイパスエントリー(permit authentication-bypass)に一致したパケットは、MAC 認証が有効な場合でも、MAC 認証のための CPU コピーは行われません。ただし、MAC 認証と関係なく CPU 宛てにコピーされるパケットは、たとえ認証バイパスエントリーにマッチしても、CPU コピーされることに注意してください。(例：IP アドレス設定時の自局 IP アドレス宛てパケットや任意宛ての ARP Request パケットなど、各機能有効時に CPU 処理やソフトウェア中継されるパケットなど) 以下の抽出条件をグループ指定する場合は、ワイルドカードビットを指定します。ワイルドカードビットを 1 で指定したビットが any 扱いになります。(例：192.0.2.0 0.0.0.255 と指定した場合は 192.0.2.0～192.0.2.255 がチェック対象になる) • 送信元 IP アドレス (SRC-IP-ADDR SRC-IP-WILDCARD) • 宛先 IP アドレス (DST-IP-ADDR DST-IP-WILDCARD)
制限・注意	• IP プロトコル番号を 51(Authentication Header)で指定して使用することは未サポートです。 • シーケンス番号は、アクセスリストの領域内で一意にしてください。すでに存在するシーケンス番号を入力すると、エラーメッセージが表示されます。 • IP プロトコル番号や L4 ポート番号などを数値指定で設定しても、一致する定義済みパラメーターが存在する場合は、構成情報では定義済みパラメーターで表示されます。
バージョン	1.08.02

■ IP アクセスリストのタイプごとの抽出条件一覧

タイプ	送信元		宛先		TCP Flag	ICMP	フラグメント	DSCP	クラス ID
	IP	L4	IP	L4					
tcp	○	○	○	○	○	–	–	○	○

タイプ	送信元		宛先		TCP Flag	ICMP	フラグメント	DSCP	クラス ID
	IP	L4	IP	L4					
udp	○	○	○	○	–	–	–	○	○
icmp	○	–	○	–	–	○	–	○	○
PROTOCOL	○	–	○	–	–	–	○	○	○
標準	○	–	○	–	–	–	–	–	○

※ 複数の抽出条件を指定する場合は、この表に記載した左側の抽出条件から順番に指定する。

■ IP アクセスリストの抽出条件

抽出条件	概要
送信元 IP アドレス	any：すべての送信元 IP アドレスを指定 host SRC-IP-ADDR：特定の送信元 IP アドレスを指定 SRC-IP-ADDR SRC-IP-WILDCARD：送信元 IP アドレスのグループを指定
送信元 L4 ポート番号 (省略可能)	{eq | lt | gt | neq} SRC-L4-PORT：比較演算子を使用して送信元 L4 ポート番号を 0～65535 の範囲で指定します。lt, gt, neq は、受信方向のアクセスリストでのみ使用できます。 • eq：指定した L4 ポート番号と等しい場合にマッチ • lt：指定した L4 ポート番号より小さい場合にマッチ • gt：指定した L4 ポート番号より大きい場合にマッチ • neq：指定した L4 ポート番号と等しくない場合にマッチ range MIN-SRC-L4-PORT MAX-SRC-L4-PORT：送信元 L4 ポート番号を範囲で指定します。受信方向のアクセスリストでのみ使用できます。 L4 ポート番号は定義済みパラメーターでも指定できます。定義済みパラメーターは「拡張エキスパートアクセスリストの抽出条件」を参照。
宛先 IP アドレス	any：すべての宛先 IP アドレスを指定 host DST-IP-ADDR：特定の宛先 IP アドレスを指定 DST-IP-ADDR DST-IP-WILDCARD：宛先 IP アドレスのグループを指定
宛先 L4 ポート番号 (省略可能)	{eq | lt | gt | neq} DST-L4-PORT：比較演算子を使用して宛先 L4 ポート番号を 0～65535 の範囲で指定します。lt, gt, neq は、受信方向のアクセスリストでのみ使用できます。 • eq：指定した L4 ポート番号と等しい場合にマッチ • lt：指定した L4 ポート番号より小さい場合にマッチ • gt：指定した L4 ポート番号より大きい場合にマッチ • neq：指定した L4 ポート番号と等しくない場合にマッチ range MIN-DST-L4-PORT MAX-DST-L4-PORT：宛先 L4 ポート番号を範囲で指定します。受信方向のアクセスリストでのみ使用できます。 L4 ポート番号は定義済みパラメーターでも指定できます。定義済みパラメーターは「拡張エキスパートアクセスリストの抽出条件」を参照。
TCP フラグ (省略可能)	TCP フラグを、ack(acknowledge), fin(finish), psh(push), rst(reset), syn(synchronize), urg(urgent)パラメーターで指定します。

抽出条件	概要
	同一ルールで複数の TCP フラグを指定する場合は、ack, fin, psh, rst, syn, urg の順番で有効にするパラメーターを指定して設定します。
ICMP メッセージ (省略可能)	ICMP メッセージをタイプ(0～255)とコード(0～255)で指定するか、もしくは定義済みパラメーターで指定します。定義済みパラメーターは「拡張エキスパートアクセスリストの抽出条件」を参照。
フラグメント (省略可能)	fragments：フラグメントされたパケットを指定します。
DSCP (省略可能)	precedence PRECEDENCE tos TOS｜dscp DSCP：IP ヘッダーの ToS フィールド(ip precedence(0～7), tos(0～15))、もしくは DSCP(0～63)を指定します。それぞれ定義済みパラメーターでも指定できます。定義済みパラメーターは「拡張エキスパートアクセスリストの抽出条件」を参照。
クラス ID (省略可能)	class CLASS-ID：認証端末クラス ID を 1～4095 の範囲で指定します。受信方向のアクセスリストでのみ使用できます。

使用例：拡張 IP アクセスリスト「IPv4-EX-ACL」で、以下のルールを設定する方法を示します。

- シーケンス番号 10、permit、抽出条件「宛先 IP アドレス 192.0.2.100 の TCP パケット」
- シーケンス番号 20、deny、抽出条件「宛先 IP アドレス 192.0.2.0/24」

```
# configure terminal
(config)# ip access-list extended IPv4-EX-ACL
(config-ip-ext-acl)# 10 permit tcp any host 192.0.2.100
(config-ip-ext-acl)# 20 deny any 192.0.2.0 0.0.0.255
(config-ip-ext-acl)#
```

使用例：標準 IP アクセスリスト「IPv4-ACL」で、シーケンス番号 10、permit、抽出条件「送信元 IP アドレス 192.168.100.0/24」のルールを設定する方法を示します。

```
# configure terminal
(config)# ip access-list IPv4-ACL
(config-ip-acl)# 10 permit 192.168.100.0 0.0.0.255 any
(config-ip-acl)#
```

8.1.10 arp access-group

arp access-group	
目的	インターフェースに適用する ARP アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	arp access-group {NAME｜NUM} [in] no arp access-group [NAME｜NUM] [in]
Parameter	NAME：ARP アクセスリスト名を指定します。 NUM：ARP アクセスリスト番号を 4000～5999 の範囲で指定します。 in（省略可能）：受信トラフィックをチェックする場合に指定します。方向を省略して設定した場合は in が適用されます。
デフォルト	なし
モード	インターフェース設定モード(port, range)
特権レベル	レベル：12
ガイドライン	ARP アクセスリストは、ARP パケットのみがチェック対象になります。

arp access-group	
	すでにインターフェースに設定されている状態で、別の ARP アクセスリストを指定して再度設定すると、前の設定を上書きします。 同一インターフェースには同じ種類のアクセスリストは 1 つしか適用できませんが、異なる種類のアクセスリストは同一インターフェースに適用できます。 アクセスリストを適用すると、装置のアクセスリスト用のリソースを消費します。ApresiaNP2500 シリーズでは、装置全体で Ingress グループ用に 7 グループ(Group 1〜7：各 256 リソース）が用意されています。ARP アクセスリストでの 1 ルールあたりのリソース消費量は以下になります。 • Ingress グループの場合：2 リソース(同一グループ) ApresiaNP2500 シリーズですべてのリソースを ARP アクセスリストで使用する場合、最大設定可能な ARP アクセスリストのルール数は以下になります。 • Ingress グループの場合：最大 896 個 本コマンドを適用した際には、残りのリソースをすべて ARP アクセスリストで使用した場合の設定可能ルール数が表示されます。

制限・注意	• ARP アクセスリストは受信方向で使用できます。送信方向では使用できません。
	
	• IPv4 アドレスが設定されている VLAN では、ARP パケットは CPU 宛てにもコピーされます。ARP アクセスリストで ARP パケットの中継が破棄された場合でも、CPU 宛てにはコピーされます。
	
	• 同じ ARP アクセスリストを複数の受信ポート(in パラメーター)に適用した場合の構成情報の表示は以下になります。
	  • AEOS-NP2500 Ver. 1.12.01 以降では、同じ ARP アクセスリストを適用した複数の受信ポートを range 表示でまとめて表示
	  • AEOS-NP2500 Ver. 1.12.01 より前のバージョンでは、受信ポートごとの表示
	
	• 同一ポートに複数種別のアクセスリストを設定していると、任意のパケットが複数のアクセスリストにマッチする可能性がありますが、その場合は最も優先順位の高いアクセスリストのアクションが採用されます。アクセスリストの優先順位は show access-list resource reserved-priority コマンドで確認できます。
	
	• 同一ポート・同一適用方向で、アクセスリストと「class-default を設定したポリシーマップ」を同時に設定しないでください。同時に設定した場合、そのポート・適用方向では常に「class-default を設定したポリシーマップ」が優先されます。そのため、そのポート・適用方向ではアクセスリストによるパケットフィルターは動作しなくなります。
	
	• インターフェースに適用したアクセスリストを異なるアクセスリストで上書きした場合、一時的に当該ルールが無効となります。そのため、アクセスリストの設定変更時には、インターフェースへの適用が完了するまでの間、当該ルールが適用されません。

バージョン	1.10.01 1.12.01：構成情報での表示仕様変更

使用例：ポート 1/0/1 において、設定済みの ARP アクセスリスト「ARP-ACL」を、受信方向で適用する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# arp access-group ARP-ACL in
```

```
The remaining applicable ARP access entries are 127
(config-if-port)#
```

8.1.11 arp access-list

arp access-list	
目的	ARP アクセスリストを設定します。また、ARP アクセスリスト設定モードに遷移します。遷移後のプロンプトは（config-arp-nacl)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	arp access-list NAME [NUM] no arp access-list {NAME | NUM}
Parameter	NAME：ARP アクセスリスト名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、;｜？空白文字 を除いた文字を使用可能です。ただし、先頭は英字のみ指定可能です。 NUM（省略可能）：ARP アクセスリスト番号を手動で割り当てる場合に、4000～5999 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	アクセスリスト名は、すべての種類のアクセスリスト内で一意になるように設定してください。なお、アクセスリスト名に使用する文字は大文字と小文字が区別されます。 ARP アクセスリスト番号を指定しない場合は、ARP アクセスリスト番号の範囲で、未使用の番号の中から最大の値が自動的に割り当てられます。
制限・注意	-
バージョン	1.10.01

使用例：ARP アクセスリスト「ARP-ACL」を作成し、ARP アクセスリスト設定モードに遷移する方法を示します。

```
# configure terminal
(config)# arp access-list ARP-ACL
(config-arp-nacl)#
```

8.1.12 permit｜deny (arp access-list)

permit｜deny (arp access-list)	
目的	ARP アクセスリストで、permit（抽出対象を許可するアクション）のルール、または deny（抽出対象を拒否するアクション）のルールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	[SEQ] {permit [authentication-bypass]｜deny} ip SENDER-IP-ADDRESS mac SRC-MAC-ADDRESS no SEQ
Parameter	SEQ（省略可能）：シーケンス番号を 1～65535 の範囲で指定します。小さい番号ほど、許可/拒否のルールの優先度が高くなります。 permit：許可するアクションのルールとして設定する場合に指定します。

permit	deny (arp access-list)	
	permit authentication-bypass：AccessDefender 認証のための認証バイパスエントリーとして設定する場合に指定します。 deny：拒否するアクションのルールとして設定する場合に指定します。 ip SENDER-IP-ADDRESS：ARP ヘッダーの Sender IP address フィールドを、以下の形式で指定します。 • any：すべての IP アドレスを指定 • host SRC-IP-ADDR：特定の IP アドレスを指定 • SRC-IP-ADDR SRC-IP-WILDCARD：IP アドレスのグループを指定 mac SRC-MAC-ADDRESS：送信元 MAC アドレス を、以下の形式で指定します。 • any：すべての送信元 MAC アドレスを指定 • host SRC-MAC-ADDR：特定の送信元 MAC アドレスを指定 • SRC-MAC-ADDR SRC-MAC-WILDCARD：送信元 MAC アドレスのグループを指定
デフォルト	なし	
モード	ARP アクセスリスト設定モード	
特権レベル	レベル：12	
ガイドライン	シーケンス番号を指定せずに設定した場合、開始値（デフォルト設定では 10）から増分値（デフォルト設定では 10）でインクリメントした番号のうち、まだ使用されていない一番小さい番号が自動的に割り当てられます。 開始値と増分値を変更するには、access-list resequence コマンドを使用します。なお、access-list resequence コマンドを実行した時点で、指定したアクセスリストの設定済みルールのシーケンス番号が一括変更されます。 シーケンス番号を手動で割り当てる場合、将来の拡張のためにシーケンス番号を「10、20、30、・・・」と、間を飛ばして設定することもできます。 AccessDefender 認証ポートに適用したアクセスリストで、permit ルール、または認証バイパスエントリー(permit authentication-bypass)にマッチした場合は、未認証状態でも中継は許可されます。なお、permit ルールと認証バイパスエントリーの違いは以下のとおりです。 • permit ルールに一致したパケットは、MAC 認証が有効な場合は、MAC 認証のための CPU コピーも行われます。 • 認証バイパスエントリー(permit authentication-bypass)に一致したパケットは、MAC 認証が有効な場合でも、MAC 認証のための CPU コピーは行われません。ただし、MAC 認証と関係なく CPU 宛てにコピーされるパケットは、たとえ認証バイパスエントリーにマッチしても、CPU コピーされることに注意してください。(例：IP アドレス設定時の自局 IP アドレス宛てパケットや任意宛ての ARP Request パケットなど、各機能有効時に CPU 処理やソフトウェア中継されるパケットなど) 以下の抽出条件をグループ指定する場合は、ワイルドカードビットを指定します。ワイルドカードビットを 1 で指定したビットが any 扱いになります。(例：192.0.2.0 0.0.0.255 と指定した場合は 192.0.2.0～192.0.2.255 がチェック対象になる) • Sender IP address フィールド (SRC-IP-ADDR SRC-IP-WILDCARD) • 送信元 MAC アドレス (SRC-MAC-ADDR SRC-MAC-WILDCARD) 抽出条件「送信元 MAC アドレス」で指定する MAC アドレスとワイルドカードビッ	

permit｜deny (arp access-list)	
	トは、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式 (例：XX-XX-XX-XX-XX-XX) • 1 バイトごとにコロン区切り形式 (例：XX:XX:XX:XX:XX:XX) • 2 バイトごとにドット区切り形式 (例：XXXX.XXXX.XXXX) • 区切り文字を使用しない形式 (例：XXXXXXXXXXXX)
制限・注意	• シーケンス番号は、アクセスリストの領域内で一意にしてください。すでに存在するシーケンス番号を入力すると、エラーメッセージが表示されます。
バージョン	1.10.01

使用例：ARP アクセスリスト「ARP-ACL」で、シーケンス番号 10、permit、抽出条件「Sender IP address フィールド 192.0.2.0/24」のルールを設定する方法を示します。

```
# configure terminal
(config)# arp access-list ARP-ACL
(config-arp-nacl)# 10 permit ip 192.0.2.0 0.0.0.255 mac any
(config-arp-nacl)#
```

8.1.13 ipv6 access-group

ipv6 access-group	
目的	インターフェースに適用する IPv6 アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 access-group {NAME｜NUM} [in｜out] no ipv6 access-group [NAME｜NUM] [in｜out]
Parameter	NAME：IPv6 アクセスリスト名を指定します。 NUM：IPv6 アクセスリスト番号を 11000～14999 の範囲で指定します。 in（省略可能）：受信トラフィックをチェックする場合に指定します。方向を省略して設定した場合は in が適用されます。 out（省略可能）：送信トラフィックをチェックする場合に指定します。
デフォルト	なし
モード	インターフェース設定モード(port, range (in パラメーター指定時))
特権レベル	レベル：12
ガイドライン	IPv6 アクセスリストは、IPv6 パケットのみがチェック対象になります。 すでにインターフェースに設定されている状態で、別の IPv6 アクセスリストを指定して再度設定すると、前の設定を上書きします。 同一インターフェースには同じ種類のアクセスリストは 1 つしか適用できませんが、異なる種類のアクセスリストは同一インターフェースに適用できます。 アクセスリストを適用すると、装置のアクセスリスト用のリソースを消費します。ApresiaNP2500 シリーズでは、装置全体で Ingress グループ用に 7 グループ（Group 1～7：各 256 リソース)、Egress グループ用に 4 グループ（Group 0～3：各 128 リソース）が用意されています。IPv6 アクセスリストでの 1 ルールあたりのリソース消費量は以下になります。 • Ingress グループの場合：連続した 2 グループで 2 リソースずつ、合計 4 リソース使用

ipv6 access-group	
	• Egress グループの場合：連続した 2 グループで 1 リソースずつ、合計 2 リソース使用 連続した 2 グループの使用可能パターンは以下になります。以下の組み合わせで占有できない状況では、IPv6 アクセスリストを適用できません。 • Ingress グループの場合：Group(2,3)、Group(4,5)、Group(6,7) • Egress グループの場合：Group(0,1)、Group(2,3) ApresiaNP2500 シリーズですべてのリソースを IPv6 アクセスリストで使用する場合、最大設定可能な IPv6 アクセスリストのルール数は以下になります。 • Ingress グループの場合：最大 384 個 • Egress グループの場合：最大 256 個 本コマンドを適用した際には、残りのリソースをすべて IPv6 アクセスリストで使用した場合の設定可能ルール数が表示されます。 L4 ポート番号の複数指定で使用する比較演算子（lt, gt, neq）と範囲指定パラメーター（range）は、受信方向のアクセスリストでのみ使用できます。送信方向のアクセスリストに適用しても、警告メッセージが出力されて動作しません。また、この比較演算子（lt, gt, neq）と範囲指定パラメーター（range）は、装置全体で異なる指定パターンの設定を最大 32 個まで使用できます。 抽出条件「フローラベル（flow-label)」は、受信方向のアクセスリストでのみ使用できます。送信方向のアクセスリストに適用しても、警告メッセージが出力されて動作しません。
制限・注意	• 抽出条件「クラス ID (class)」は、受信方向のアクセスリストでのみ使用できます。送信方向のアクセスリストに適用しないでください。 • 同一名称または同一番号のアクセスリストを、複数の送信ポート(out パラメーター)に適用することはできません。 • 同じ IPv6 アクセスリストを複数の受信ポート(in パラメーター)に適用した場合の構成情報の表示は以下になります。 • AEOS-NP2500 Ver. 1.12.01 以降では、同じ IPv6 アクセスリストを適用した複数の受信ポートを range 表示でまとめて表示 • AEOS-NP2500 Ver. 1.12.01 より前のバージョンでは、受信ポートごとの表示 • 同一ポートに複数種別のアクセスリストを設定していると、任意のパケットが複数のアクセスリストにマッチする可能性がありますが、その場合は最も優先順位の高いアクセスリストのアクションが採用されます。アクセスリストの優先順位は show access-list resource reserved-priority コマンドで確認できます。 • 同一ポート・同一適用方向で、アクセスリストと「class-default を設定したポリシーマップ」を同時に設定しないでください。同時に設定した場合、そのポート・適用方向では常に「class-default を設定したポリシーマップ」が優先されます。そのため、そのポート・適用方向ではアクセスリストによるパケットフィルターは動作しなくなります。 • インターフェースに適用したアクセスリストを異なるアクセスリストで上書きした場合、一時的に当該ルールが無効となります。そのため、アクセスリストの設定変更時には、インターフェースへの適用が完了するまでの間、当該ルールが適用されません。
バージョン	1.08.02 1.12.01：構成情報での表示仕様変更

使用例：ポート 1/0/1 において、設定済みの IPv6 アクセスリスト「IPv6-ACL」を、受信方向で適用する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# ipv6 access-group IPv6-ACL in

The remaining applicable IPv6 related access entries are 381
(config-if-port)#
```

8.1.14 ipv6 access-list

ipv6 access-list	
目的	IPv6 アクセスリストを設定します。また、IPv6 アクセスリスト設定モードに遷移します。遷移後のプロンプトは、標準 IPv6 アクセスリストの場合は（config-ipv6-acl)# に、拡張 IPv6 アクセスリストの場合は（config-ipv6-ext-acl)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	ipv6 access-list [extended] NAME [NUM] no ipv6 access-list [extended] {NAME | NUM}
Parameter	extended（省略可能）：拡張 IPv6 アクセスリストを作成する場合に指定します。省略した場合は標準 IPv6 アクセスリストになります。 NAME：IPv6 アクセスリスト名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、;|？空白文字 を除いた文字を使用可能です。ただし、先頭は英字のみ指定可能です。 NUM（省略可能）：IPv6 アクセスリスト番号を手動で割り当てる場合に、標準 IPv6 アクセスリストは 11000～12999 の範囲で、拡張 IPv6 アクセスリストは 13000～14999 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	アクセスリスト名は、すべての種類のアクセスリスト内で一意になるように設定してください。なお、アクセスリスト名に使用する文字は大文字と小文字が区別されます。 IPv6 アクセスリスト番号を指定しない場合は、IPv6 アクセスリスト番号の範囲で、未使用の番号の中から最大の値が自動的に割り当てられます。
制限・注意	-
バージョン	1.08.02

使用例：標準 IPv6 アクセスリスト「IPv6-ACL」を作成し、IPv6 アクセスリスト設定モードに遷移する方法を示します。

```
# configure terminal
(config)# ipv6 access-list IPv6-ACL
(config-ipv6-acl)#
```

8.1.15 permit | deny (ipv6 access-list)

permit | deny (ipv6 access-list)	
目的	IPv6 アクセスリストで、permit（抽出対象を許可するアクション）のルール、または

permit｜deny (ipv6 access-list)	
	deny（抽出対象を拒否するアクション）のルールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	■ 拡張 IPv6 アクセスリスト [SEQ] {permit [authentication-bypass]｜deny} tcp CONDITION [SEQ] {permit [authentication-bypass]｜deny} udp CONDITION [SEQ] {permit [authentication-bypass]｜deny} icmp CONDITION [SEQ] {permit [authentication-bypass]｜deny} [PROTOCOL｜protocol-id ID] CONDITION ■ 標準 IPv6 アクセスリスト [SEQ] {permit [authentication-bypass]｜deny} CONDITION ■ 削除コマンド no SEQ
Parameter	SEQ（省略可能）：シーケンス番号を 1～65535 の範囲で指定します。小さい番号ほど、許可/拒否のルールの優先度が高くなります。 permit：許可するアクションのルールとして設定する場合に指定します。 permit authentication-bypass：AccessDefender 認証のための認証バイパスエントリーとして設定する場合に指定します。 deny：拒否するアクションのルールとして設定する場合に指定します。 tcp：TCP パケットを抽出対象にする場合に指定します。 udp：UDP パケットを抽出対象にする場合に指定します。 icmp：ICMP パケットを抽出対象にする場合に指定します。 PROTOCOL（省略可能）：抽出対象にする IP プロトコル番号を、以下の定義済みパラメーターで指定します。 • esp(50) pcp(108) sctp(132) protocol-id ID（省略可能）：抽出対象にする IP プロトコル番号を 0～255 の範囲で指定します。なお、0(IPv6 Hop-by-Hop Option)、43(Routing Header for IPv6)、44(Fragment Header for IPv6)、51(Authentication Header)、60(Destination Options for IPv6)指定は未サポートです。 CONDITION：使用する抽出条件を指定します。詳細は「IPv6 アクセスリストのタイプごとの抽出条件一覧」と「IPv6 アクセスリストの抽出条件」を参照。
デフォルト	なし
モード	IPv6 アクセスリスト設定モード
特権レベル	レベル：12
ガイドライン	シーケンス番号を指定せずに設定した場合、開始値（デフォルト設定では 10）から増分値（デフォルト設定では 10）でインクリメントした番号のうち、まだ使用されていない一番小さい番号が自動的に割り当てられます。 開始値と増分値を変更するには、access-list resequence コマンドを使用します。なお、access-list resequence コマンドを実行した時点で、指定したアクセスリストの設定済みルールのシーケンス番号が一括変更されます。 シーケンス番号を手動で割り当てる場合、将来の拡張のためにシーケンス番号を

permit｜deny (ipv6 access-list)	
	「10、20、30、・・・」と、間を飛ばして設定することもできます。 AccessDefender 認証ポートに適用したアクセスリストで、permit ルール、または認証バイパスエントリー(permit authentication-bypass)にマッチした場合は、未認証状態でも中継は許可されます。なお、permit ルールと認証バイパスエントリーの違いは以下のとおりです。 • permit ルールに一致したパケットは、MAC 認証が有効な場合は、MAC 認証のための CPU コピーも行われます。 • 認証バイパスエントリー(permit authentication-bypass)に一致したパケットは、MAC 認証が有効な場合でも、MAC 認証のための CPU コピーは行われません。ただし、MAC 認証と関係なく CPU 宛てにコピーされるパケットは、たとえ認証バイパスエントリーにマッチしても、CPU コピーされることに注意してください。(例：IP アドレス設定時の自局 IP アドレス宛てパケットや任意宛ての ARP Request パケットなど、各機能有効時に CPU 処理やソフトウェア中継されるパケットなど)
制限・注意	• IP プロトコル番号を 0(IPv6 Hop-by-Hop Option)、43(Routing Header for IPv6)、44(Fragment Header for IPv6)、51(Authentication Header)、60(Destination Options for IPv6)で指定して使用することは未サポートです。 • シーケンス番号は、アクセスリストの領域内で一意にしてください。すでに存在するシーケンス番号を入力すると、エラーメッセージが表示されます。 • IP プロトコル番号や L4 ポート番号などを数値指定で設定しても、一致する定義済みパラメーターが存在する場合は、構成情報では定義済みパラメーターで表示されます。
バージョン	1.08.02 1.10.01：抽出条件を追加

■ IPv6 アクセスリストのタイプごとの抽出条件一覧

タイプ	送信元		宛先		TCP Flag	ICMP	フラグメント	DSCP	※1	※2	※3	クラス ID
	IPv6	L4	IPv6	L4								
tcp	○	○	○	○	○	–	–	○	○	○	○	○
udp	○	○	○	○	–	–	–	○	○	○	○	○
icmp	○	–	○	–	–	○	–	○	○	○	○	○
PROTOCOL	○	–	○	–	–	–	○	○	○	○	○	○
標準	○	–	○	–	–	–	–	–	–	–	–	○

※1：トラフィッククラス ※2：フローラベル ※3：ホップリミット

※ 複数の抽出条件を指定する場合は、この表に記載した左側の抽出条件から順番に指定する。

※ DSCP とトラフィッククラスは併用不可

■ IPv6 アクセスリストの抽出条件

抽出条件	概要
送信元 IPv6 アドレス	any：すべての送信元 IPv6 アドレスを指定 host SRC-IPV6-ADDR：特定の送信元 IPv6 アドレスを指定 SRC-IPV6-ADDR/LENGTH：送信元 IPv6 アドレスのプレフィックス指定

抽出条件	概要
送信元 L4 ポート番号 (省略可能)	{eq | lt | gt | neq} SRC-L4-PORT：比較演算子を使用して送信元 L4 ポート番号を 0～65535 の範囲で指定します。lt, gt, neq は、受信方向のアクセスリストでのみ使用できます。 • eq：指定した L4 ポート番号と等しい場合にマッチ • lt：指定した L4 ポート番号より小さい場合にマッチ • gt：指定した L4 ポート番号より大きい場合にマッチ • neq：指定した L4 ポート番号と等しくない場合にマッチ range MIN-SRC-L4-PORT MAX-SRC-L4-PORT：送信元 L4 ポート番号を範囲で指定します。受信方向のアクセスリストでのみ使用できます。 L4 ポート番号は定義済みパラメーターでも指定できます。定義済みパラメーターは「拡張エキスパートアクセスリストの抽出条件」を参照。
宛先 IPv6 アドレス	any：すべての宛先 IPv6 アドレスを指定 host DST-IPV6-ADDR：特定の宛先 IPv6 アドレスを指定 DST-IPV6-ADDR/LENGTH：宛先 IPv6 アドレスのプレフィックス指定
宛先 L4 ポート番号 (省略可能)	{eq | lt | gt | neq} DST-L4-PORT：比較演算子を使用して宛先 L4 ポート番号を 0～65535 の範囲で指定します。lt, gt, neq は、受信方向のアクセスリストでのみ使用できます。 • eq：指定した L4 ポート番号と等しい場合にマッチ • lt：指定した L4 ポート番号より小さい場合にマッチ • gt：指定した L4 ポート番号より大きい場合にマッチ • neq：指定した L4 ポート番号と等しくない場合にマッチ range MIN-DST-L4-PORT MAX-DST-L4-PORT：宛先 L4 ポート番号を範囲で指定します。受信方向のアクセスリストでのみ使用できます。 L4 ポート番号は定義済みパラメーターでも指定できます。定義済みパラメーターは「拡張エキスパートアクセスリストの抽出条件」を参照。
TCP フラグ (省略可能)	TCP フラグを、ack(acknowledge), fin(finish), psh(push), rst(reset), syn(synchronize), urg(urgent)パラメーターで指定します。 同一ルールで複数の TCP フラグを指定する場合は、ack, fin, psh, rst, syn, urg の順番で有効にするパラメーターを指定して設定します。
ICMP メッセージ (省略可能)	ICMP メッセージをタイプ(0～255)とコード(0～255)で指定するか、もしくは以下の定義済みパラメーターで指定します。 beyond-scope(1,2) destination-unreachable(1,3) echo-reply(129,0) echo-request(128,0) erroneous_header(4,0) hop-limit(3,0) multicast-listener-done(132,0) multicast-listener-query(130,0) multicast-listener-report(131,0) nd-na(136,0) nd-ns(135,0) next-header(4,1) no-admin(1,1) no-route(1,0) packet-too-big(2,0) parameter-option(4,2) parameter-problem(4,-) port-unreachable(1,4) reassembly-timeout(3,1) redirect(137,0) renum-command(138,0) renum-result(138,1) renum-seq-number(138,255) router-advertisement(134,0) router-renumbering(138,-) router-solicitation(133,0) time-exceeded(3,-) unreachable(1,-)
フラグメント (省略可能)	fragments：フラグメントされたパケットを指定します。

抽出条件	概要
DSCP (省略可能)	dscp DSCP：DSCP(0～63)を指定します。定義済みパラメーターでも指定できます。定義済みパラメーターは「拡張エキスパートアクセスリストの抽出条件」を参照。
トラフィッククラス (省略可能)	traffic-class TRAFFIC-CLASS：トラフィッククラスを 0～255 の範囲で指定します。
フローラベル (省略可能)	flow-label FLOW-LABEL：フローラベルを 0～1048575 の範囲で指定します。受信方向のアクセスリストでのみ使用できます。
ホップリミット (省略可能)	hop-limit-ipv6-header HOP-LIMIT：ホップリミットを 0～255 の範囲で指定します。
クラス ID (省略可能)	class CLASS-ID：認証端末クラス ID を 1～4095 の範囲で指定します。受信方向のアクセスリストでのみ使用できます。

使用例：拡張 IPv6 アクセスリスト「IPv6-EX-ACL」で、以下のルールを設定する方法を示します。

- シーケンス番号 10、permit、抽出条件「宛先 IPv6 アドレス 2001:db8::1 の TCP パケット」
- シーケンス番号 20、deny、抽出条件「宛先 IPv6 アドレス 2001:db8::/64」

```
# configure terminal
(config)# ipv6 access-list extended IPv6-EX-ACL
(config-ipv6-ext-acl)# 10 permit tcp any host 2001:db8::1
(config-ipv6-ext-acl)# 20 deny any 2001:db8::/64
(config-ipv6-ext-acl)#
```

使用例：標準 IPv6 アクセスリスト「IPv6-ACL」で、シーケンス番号 10、permit、抽出条件「送信元 IPv6 アドレス 2001:db8:50::/64」のルールを設定する方法を示します。

```
# configure terminal
(config)# ipv6 access-list IPv6-ACL
(config-ipv6-acl)# 10 permit 2001:db8:50::/64 any
(config-ipv6-acl)#
```

8.1.16 mac access-list enable ip-packets

mac access-list enable ip-packets	
目的	拡張 MAC アクセスリストにおいて、IPv4 パケットおよび IPv6 パケットをチェック対象にする IP パケット対象化機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	mac access-list enable ip-packets no mac access-list enable ip-packets
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	拡張 MAC アクセスリストでは IPv4 パケットおよび IPv6 パケットはチェック対象外ですが、本設定を有効にするとチェック対象にすることができます。 本設定を有効にした場合、同一ポートに拡張 MAC アクセスリストとそれ以外の種別のアクセスリストを設定していると、任意のパケットが複数のアクセスリストにマッチする可能性がありますが、その場合は最も優先順位の高いアクセスリストのアク

mac access-list enable ip-packets	
	ションが採用されます。アクセスリストの優先順位は show access-list resource reserved-priority コマンドで確認できます。 • IPv4 パケットの場合、受信方向に適用したアクセスリストでは、「拡張エキスパートアクセスリスト」「拡張 MAC アクセスリスト」「IP アクセスリスト」の順番にチェックされます。送信方向に適用したアクセスリストでは、「拡張 MAC アクセスリスト」「IP アクセスリスト」「拡張エキスパートアクセスリスト」の順番にチェックされます。 • IPv6 パケットの場合、「拡張 MAC アクセスリスト」「IPv6 アクセスリスト」の順番にチェックされます。
制限・注意	-
バージョン	1.10.01

使用例：拡張 MAC アクセスリストにおいて、IPv4 パケットおよび IPv6 パケットをチェック対象にする IP パケット対象化機能を有効にする方法を示します。

```
# configure terminal
(config)# mac access-list enable ip-packets
(config)#
```

8.1.17 mac access-group

mac access-group	
目的	インターフェースに適用する拡張 MAC アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mac access-group {NAME | NUM} [in | out] no mac access-group [NAME | NUM] [in | out]
Parameter	NAME：拡張 MAC アクセスリスト名を指定します。 NUM：拡張 MAC アクセスリスト番号を 6000～7999 の範囲で指定します。 in（省略可能）：受信トラフィックをチェックする場合に指定します。方向を省略して設定した場合は in が適用されます。 out（省略可能）：送信トラフィックをチェックする場合に指定します。
デフォルト	なし
モード	インターフェース設定モード(port, range（in パラメーター指定時）)
特権レベル	レベル：12
ガイドライン	拡張 MAC アクセスリストは、IPv4 パケットおよび IPv6 パケット以外の非 IP パケットのみがチェック対象になります。拡張 MAC アクセスリストの IP パケット対象化機能（mac access-list enable ip-packets）を有効にしている場合は、IPv4 パケットおよび IPv6 パケットもチェック対象になります。 すでにインターフェースに設定されている状態で、別の拡張 MAC アクセスリストを指定して再度設定すると、前の設定を上書きします。 同一インターフェースには同じ種類のアクセスリストは 1 つしか適用できませんが、異なる種類のアクセスリストは同一インターフェースに適用できます。 アクセスリストを適用すると、装置のアクセスリスト用のリソースを消費します。ApresiaNP2500 シリーズでは、装置全体で Ingress グループ用に 7 グループ（Group 1～7：各 256 リソース）、Egress グループ用に 4 グループ（Group 0～3：

mac access-group	
	各 128 リソース）が用意されています。拡張 MAC アクセスリストでの 1 ルールあたりのリソース消費量は以下になります。 • Ingress グループの場合：1 リソース • Egress グループの場合：1 リソース ApresiaNP2500 シリーズですべてのリソースを拡張 MAC アクセスリストで使用する場合、最大設定可能な拡張 MAC アクセスリストのルール数は以下になります。 • Ingress グループの場合：最大 1792 個 • Egress グループの場合：最大 512 個 本コマンドを適用した際には、残りのリソースをすべて拡張 MAC アクセスリストで使用した場合の設定可能ルール数が表示されます。
制限・注意	• 抽出条件「クラス ID (class)」は、受信方向のアクセスリストでのみ使用できます。送信方向のアクセスリストに適用しないでください。 • 同一名称または同一番号のアクセスリストを、複数の送信ポート(out パラメーター)に適用することはできません。 • 同じ拡張 MAC アクセスリストを複数の受信ポート(in パラメーター)に適用した場合の構成情報の表示は以下になります。 • AEOS-NP2500 Ver. 1.12.01 以降では、同じ拡張 MAC アクセスリストを適用した複数の受信ポートを range 表示でまとめて表示 • AEOS-NP2500 Ver. 1.12.01 より前のバージョンでは、受信ポートごとの表示 • 同一ポートに複数種別のアクセスリストを設定していると、任意のパケットが複数のアクセスリストにマッチする可能性がありますが、その場合は最も優先順位の高いアクセスリストのアクションが採用されます。アクセスリストの優先順位は show access-list resource reserved-priority コマンドで確認できます。 • 同一ポート・同一適用方向で、アクセスリストと「class-default を設定したポリシーマップ」を同時に設定しないでください。同時に設定した場合、そのポート・適用方向では常に「class-default を設定したポリシーマップ」が優先されます。そのため、そのポート・適用方向ではアクセスリストによるパケットフィルターは動作しなくなります。 • インターフェースに適用したアクセスリストを異なるアクセスリストで上書きした場合、一時的に当該ルールが無効となります。そのため、アクセスリストの設定変更時には、インターフェースへの適用が完了するまでの間、当該ルールが適用されません。
バージョン	1.08.02 1.12.01：構成情報での表示仕様変更

使用例：ポート 1/0/1 において、設定済みの拡張 MAC アクセスリスト「MAC-ACL」を、受信方向で適用する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# mac access-group MAC-ACL in

The remaining applicable MAC access entries are 1789
(config-if-port)#
```

8.1.18 mac access-list

mac access-list	
目的	拡張 MAC アクセスリストを設定します。また、拡張 MAC アクセスリスト設定モードに遷移します。遷移後のプロンプトは（config-mac-ext-acl)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	mac access-list extended NAME [NUM] no mac access-list extended {NAME | NUM}
Parameter	NAME：拡張 MAC アクセスリスト名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、;|？空白文字 を除いた文字を使用可能です。ただし、先頭は英字のみ指定可能です。 NUM（省略可能）：拡張 MAC アクセスリスト番号を手動で割り当てる場合に、6000～7999 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	アクセスリスト名は、すべての種類のアクセスリスト内で一意になるように設定してください。なお、アクセスリスト名に使用する文字は大文字と小文字が区別されます。 拡張 MAC アクセスリスト番号を指定しない場合は、拡張 MAC アクセスリスト番号の範囲で、未使用の番号の中から最大の値が自動的に割り当てられます。
制限・注意	-
バージョン	1.08.02

使用例：拡張 MAC アクセスリスト「MAC-ACL」を作成し、拡張 MAC アクセスリスト設定モードに遷移する方法を示します。

```
# configure terminal
(config)# mac access-list extended MAC-ACL
(config-mac-ext-acl)#
```

8.1.19 permit | deny (mac access-list)

permit | deny (mac access-list)	
目的	拡張 MAC アクセスリストで、permit（抽出対象を許可するアクション）のルール、または deny（抽出対象を拒否するアクション）のルールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	[SEQ] {permit [authentication-bypass] | deny} CONDITION no SEQ
Parameter	SEQ（省略可能）：シーケンス番号を 1～65535 の範囲で指定します。小さい番号ほど、許可/拒否のルールの優先度が高くなります。 permit：許可するアクションのルールとして設定する場合に指定します。 permit authentication-bypass：AccessDefender 認証のための認証バイパスエントリーとして設定する場合に指定します。 deny：拒否するアクションのルールとして設定する場合に指定します。 CONDITION：使用する抽出条件を指定します。詳細は「拡張 MAC アクセスリスト

permit｜deny (mac access-list)	
	の抽出条件」を参照。
デフォルト	なし
モード	拡張 MAC アクセスリスト設定モード
特権レベル	レベル：12
ガイドライン	シーケンス番号を指定せずに設定した場合、開始値（デフォルト設定では 10）から増分値（デフォルト設定では 10）でインクリメントした番号のうち、まだ使用されていない一番小さい番号が自動的に割り当てられます。 開始値と増分値を変更するには、access-list resequence コマンドを使用します。なお、access-list resequence コマンドを実行した時点で、指定したアクセスリストの設定済みルールのシーケンス番号が一括変更されます。 シーケンス番号を手動で割り当てる場合、将来の拡張のためにシーケンス番号を「10、20、30、・・・」と、間を飛ばして設定することもできます。 AccessDefender 認証ポートに適用したアクセスリストで、permit ルール、または認証バイパスエントリー(permit authentication-bypass)にマッチした場合は、未認証状態でも中継は許可されます。なお、permit ルールと認証バイパスエントリーの違いは以下のとおりです。 • permit ルールに一致したパケットは、MAC 認証が有効な場合は、MAC 認証のための CPU コピーも行われます。 • 認証バイパスエントリー(permit authentication-bypass)に一致したパケットは、MAC 認証が有効な場合でも、MAC 認証のための CPU コピーは行われません。ただし、MAC 認証と関係なく CPU 宛てにコピーされるパケットは、たとえ認証バイパスエントリーにマッチしても、CPU コピーされることに注意してください。(例：IP アドレス設定時の自局 IP アドレス宛てパケットや任意宛ての ARP Request パケットなど、各機能有効時に CPU 処理やソフトウェア中継されるパケットなど) 以下の抽出条件をグループ指定する場合は、ワイルドカードビットを指定します。ワイルドカードビットを 1 で指定したビットが any 扱いになります。(例：00aa.bbcc.0000 0000.0000.ffff と指定した場合は 00AA.BBCC.0000 ～ 00AA.BBCC.FFFF がチェック対象になる) • 送信元 MAC アドレス (SRC-MAC-ADDR SRC-MAC-WILDCARD) • 宛先 MAC アドレス (DST-MAC-ADDR DST-MAC-WILDCARD) 抽出条件「送信元 MAC アドレス」と「宛先 MAC アドレス」で指定する MAC アドレスとワイルドカードビットは、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式 (例：XX-XX-XX-XX-XX-XX) • 1 バイトごとにコロン区切り形式 (例：XX:XX:XX:XX:XX:XX) • 2 バイトごとにドット区切り形式 (例：XXXX.XXXX.XXXX) • 区切り文字を使用しない形式 (例：XXXXXXXXXXXX) イーサタイプ (ethernet-type TYPE MASK) 抽出条件をマスク指定する場合は、固定するビットを 1、any 扱いにするビットを 0 でマスクを指定します。(例：0x5500 0xff00 と指定した場合は 0x5500～0x55FF がチェック対象になる)
制限・注意	• シーケンス番号は、アクセスリストの領域内で一意にしてください。すでに存在するシーケンス番号を入力すると、エラーメッセージが表示されます。
バージョン	1.08.02

■ 拡張 MAC アクセスリストの抽出条件

抽出条件	概要
送信元 MAC アドレス	any：すべての送信元 MAC アドレスを指定 host SRC-MAC-ADDR：特定の送信元 MAC アドレスを指定 SRC-MAC-ADDR SRC-MAC-WILDCARD：送信元 MAC アドレスのグループを指定
宛先 MAC アドレス	any：すべての宛先 MAC アドレスを指定 host DST-MAC-ADDR：特定の宛先 MAC アドレスを指定 DST-MAC-ADDR DST-MAC-WILDCARD：宛先 MAC アドレスのグループを指定
イーサタイプ (省略可能)	ethernet-type TYPE MASK：イーサタイプを値(0x0～0xFFFF)とマスク(0x0～0xFFFF)で指定します。ビット操作後のイーサタイプは 1536 (0x0600) 以上である必要があります。また、以下の定義済みパラメーターでも指定できます。 aarp, appletalk, arp, decnet-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp
CoS (省略可能)	cos OUTER-COS [inner INNER-COS]：外側のサービス VLAN タグの CoS を 0～7 の範囲で指定します。また、内側のカスタマーVLAN タグの CoS も 0～7 の範囲で指定できます。
VLAN ID (省略可能)	vlan OUTER-VLAN [inner INNER-VLAN]：外側のサービス VLAN タグの VLAN ID を 1～4094 の範囲で指定します。また、内側のカスタマーVLAN タグの VLAN ID も 1～4094 の範囲で指定できます。
クラス ID (省略可能)	class CLASS-ID：認証端末クラス ID を 1～4095 の範囲で指定します。受信方向のアクセスリストでのみ使用できます。

※ 複数の抽出条件を指定する場合は、この表に記載した先頭の抽出条件から順番に指定する。

使用例：拡張 MAC アクセスリスト「MAC-ACL」で、シーケンス番号 10、deny、抽出条件「送信元 MAC アドレス 00:00:5E:00:53:00～00:00:5E:00:53:FF の非 IP フレーム」のルールを設定する方法を示します。

```
# configure terminal
(config)# mac access-list extended MAC-ACL
(config-mac-ext-acl)# 10 deny 00:00:5e:00:53:00 00:00:00:00:00:ff any
(config-mac-ext-acl)#
```

8.1.20 vlan access-map

vlan access-map	
目的	VLAN アクセスマップのサブマップを設定します。また、VLAN アクセスマップのサブマップ設定モードに遷移します。遷移後のプロンプトは（config-access-map)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	vlan access-map MAP-NAME [SEQ] no vlan access-map MAP-NAME [SEQ]
Parameter	MAP-NAME：VLAN アクセスマップ名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。

vlan access-map	
	SEQ（省略可能）：サブマップのシーケンス番号を 1～65535 の範囲で指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	VLAN フィルター機能は、特定の VLAN の受信パケットに対してアクセスコントロールを実施する機能です。送信パケットに対しては動作しません。本コマンドでは、VLAN アクセスマップを設定します。 各サブマップには 1 つのアクセスリスト（IP アクセスリスト、ARP アクセスリスト、IPv6 アクセスリスト、または拡張 MAC アクセスリスト）を設定可能です。また、1 つのアクションを指定できます。 サブマップのシーケンス番号を指定しない場合は、開始値 10 から増分値 10 でインクリメントした番号のうち、まだ使用されていない一番小さい番号が自動的に割り当てられます。 サブマップに一致するパケット（関連付けられたアクセスリストによって許可されたパケット）は、サブマップに指定されているアクションを実行します。以降のサブマップに対するチェックは行われません。パケットがサブマップに一致しない場合に、次のサブマップがチェックされます。 シーケンス番号を指定せずに no vlan access-map コマンドを使用すると、指定した VLAN アクセスマップのサブマップの情報がすべて削除されます。
制限・注意	-
バージョン	1.08.02

使用例：VLAN アクセスマップ「vlan-map」において、シーケンス番号 20 のサブマップ設定モードに遷移する方法を示します。

```
# configure terminal
(config)# vlan access-map vlan-map 20
(config-access-map)#
```

8.1.21 match ip address

match ip address	
目的	サブマップに関連付ける IP アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	match ip address {ACL-NAME | ACL-NUM} no match ip address {ACL-NAME | ACL-NUM}
Parameter	ACL-NAME：関連付ける IP アクセスリスト名を指定します。 ACL-NUM：関連付ける IP アクセスリスト番号を、1～3999 の範囲で指定します。
デフォルト	なし
モード	VLAN アクセスマップのサブマップ設定モード
特権レベル	レベル：12
ガイドライン	1 つのサブマップには、1 つのアクセスリスト（IP アクセスリスト、ARP アクセスリスト、IPv6 アクセスリスト、または拡張 MAC アクセスリスト）のみ関連付けることができます。

match ip address	
	関連付けるアクセスリストでは、当該サブマップの処理対象となる条件を permit ルールで設定します。deny ルールはサポートしていません。 IP アクセスリストを関連付けた IPv4 サブマップは、IPv4 パケットのみがチェック対象になります。 本コマンドが設定済みの状態で、別の IP アクセスリストを指定して設定すると上書き設定されます。また、本コマンドが設定済みの状態で match {arp | ipv6 | mac} address コマンドを設定すると、本コマンドの設定が削除されて match {arp | ipv6 | mac} address コマンドが設定されます。 フィルタリング対象のエントリー数は装置全体で 1792 個となりますが、設定可能なエントリー数は使用するアクセスリストの種別、設定順序、および当該サブマップを vlan filter コマンドで適用した VLAN の組み合わせによって変化します。
制限・注意	• 説明に記載されている種別以外のアクセスリストを指定して使用できません。
バージョン	1.08.02

使用例：VLAN アクセスマップ「vlan-map」のシーケンス番号 10 のサブマップに、IP アクセスリスト「IPv4-ACL」を関連付ける方法を示します。

```
# configure terminal
(config)# vlan access-map vlan-map 10
(config-access-map)# match ip address IPv4-ACL
(config-access-map)#
```

8.1.22 match arp address

match arp address	
目的	サブマップに関連付ける ARP アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	match arp address {ACL-NAME | ACL-NUM} no match arp address {ACL-NAME | ACL-NUM}
Parameter	ACL-NAME：関連付ける ARP アクセスリスト名を指定します。 ACL-NUM：関連付ける ARP アクセスリスト番号を、4000～5999 の範囲で指定します。
デフォルト	なし
モード	VLAN アクセスマップのサブマップ設定モード
特権レベル	レベル：12
ガイドライン	1 つのサブマップには、1 つのアクセスリスト（IP アクセスリスト、ARP アクセスリスト、IPv6 アクセスリスト、または拡張 MAC アクセスリスト）のみ関連付けることができます。 関連付けるアクセスリストでは、当該サブマップの処理対象となる条件を permit ルールで設定します。deny ルールはサポートしていません。 ARP アクセスリストを関連付けた ARP サブマップは、ARP パケットのみがチェック対象になります。 本コマンドが設定済みの状態で、別の ARP アクセスリストを指定して設定すると上書き設定されます。また、本コマンドが設定済みの状態で match {ip | ipv6 | mac} address コマンドを設定すると、本コマンドの設定が削除されて match {ip | ipv6 |

match arp address	
	mac} address コマンドが設定されます。 フィルタリング対象のエントリー数は装置全体で 1792 個となりますが、設定可能なエントリー数は使用するアクセスリストの種別、設定順序、および当該サブマップを vlan filter コマンドで適用した VLAN の組み合わせによって変化します。
制限・注意	• 説明に記載されている種別以外のアクセスリストを指定して使用できません。
バージョン	1.10.01

使用例：VLAN アクセスマップ「vlan-map」のシーケンス番号 15 のサブマップに、ARP アクセスリスト「ARP-ACL」を関連付ける方法を示します。

```
# configure terminal
(config)# vlan access-map vlan-map 15
(config-access-map)# match arp address ARP-ACL
(config-access-map)#
```

8.1.23 match ipv6 address

match ipv6 address	
目的	サブマップに関連付ける IPv6 アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	match ipv6 address {ACL-NAME | ACL-NUM} no match ipv6 address {ACL-NAME | ACL-NUM}
Parameter	ACL-NAME：関連付ける IPv6 アクセスリスト名を指定します。 ACL-NUM：関連付ける IPv6 アクセスリスト番号を、11000～14999 の範囲で指定します。
デフォルト	なし
モード	VLAN アクセスマップのサブマップ設定モード
特権レベル	レベル：12
ガイドライン	1 つのサブマップには、1 つのアクセスリスト（IP アクセスリスト、ARP アクセスリスト、IPv6 アクセスリスト、または拡張 MAC アクセスリスト）のみ関連付けることができます。 関連付けるアクセスリストでは、当該サブマップの処理対象となる条件を permit ルールで設定します。deny ルールはサポートしていません。 IPv6 アクセスリストを関連付けた IPv6 サブマップは、IPv6 パケットのみがチェック対象になります。 本コマンドが設定済みの状態で、別の IPv6 アクセスリストを指定して設定すると上書き設定されます。また、本コマンドが設定済みの状態で match {ip | arp | mac} address コマンドを設定すると、本コマンドの設定が削除されて match {ip | arp | mac} address コマンドが設定されます。 フィルタリング対象のエントリー数は装置全体で 1792 個となりますが、設定可能なエントリー数は使用するアクセスリストの種別、設定順序、および当該サブマップを vlan filter コマンドで適用した VLAN の組み合わせによって変化します。
制限・注意	• 説明に記載されている種別以外のアクセスリストを指定して使用できません。
バージョン	1.08.02

使用例：VLAN アクセスマップ「vlan-map」のシーケンス番号 20 のサブマップに、IPv6 アクセスリスト「IPv6-ACL」を関連付ける方法を示します。

```
# configure terminal
(config)# vlan access-map vlan-map 20
(config-access-map)# match ipv6 address IPv6-ACL
(config-access-map)#
```

8.1.24 match mac address

match mac address	
目的	サブマップに関連付ける拡張 MAC アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	match mac address {ACL-NAME | ACL-NUM} no match mac address {ACL-NAME | ACL-NUM}
Parameter	ACL-NAME：関連付ける拡張 MAC アクセスリスト名を指定します。 ACL-NUM：関連付ける拡張 MAC アクセスリスト番号を、6000～7999 の範囲で指定します。
デフォルト	なし
モード	VLAN アクセスマップのサブマップ設定モード
特権レベル	レベル：12
ガイドライン	1 つのサブマップには、1 つのアクセスリスト（IP アクセスリスト、ARP アクセスリスト、IPv6 アクセスリスト、または拡張 MAC アクセスリスト）のみ関連付けることができます。 関連付けるアクセスリストでは、当該サブマップの処理対象となる条件を permit ルールで設定します。deny ルールはサポートしていません。 拡張 MAC アクセスリストを関連付けた MAC サブマップは、非 IP パケットのみがチェック対象になります。拡張 MAC アクセスリストの IP パケット対象化機能(mac access-list enable ip-packets)が有効の場合は、IPv4 パケットおよび IPv6 パケットもチェック対象になります。 本コマンドが設定済みの状態で、別の拡張 MAC アクセスリストを指定して設定すると上書き設定されます。また、本コマンドが設定済みの状態で match {ip | arp | ipv6} address コマンドを設定すると、本コマンドの設定が削除されて match {ip | arp | ipv6} address コマンドが設定されます。 フィルタリング対象のエントリー数は装置全体で 1792 個となりますが、設定可能なエントリー数は使用するアクセスリストの種別、設定順序、および当該サブマップを vlan filter コマンドで適用した VLAN の組み合わせによって変化します。
制限・注意	• 説明に記載されている種別以外のアクセスリストを指定して使用できません。
バージョン	1.08.02

使用例：VLAN アクセスマップ「vlan-map」のシーケンス番号 30 のサブマップに、拡張 MAC アクセスリスト「MAC-ACL」を関連付ける方法を示します。

```
# configure terminal
(config)# vlan access-map vlan-map 30
(config-access-map)# match mac address MAC-ACL
(config-access-map)#
```

8.1.25 action

action	
目的	VLAN アクセスマップのサブマップのアクションを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	action {forward | drop | redirect port PORT} no action
Parameter	forward：マッチ条件に一致したパケットを中継する場合に指定します。 drop：マッチ条件に一致したパケットを破棄する場合に指定します。 redirect port PORT：マッチ条件に一致したパケットをリダイレクトする場合に、リダイレクト先の物理ポートを指定します。
デフォルト	forward
モード	VLAN アクセスマップのサブマップ設定モード
特権レベル	レベル：12
ガイドライン	1 つのサブマップに設定できるアクションは 1 つだけです。新たなアクションを設定すると、以前のアクションが上書きされます。 サブマップに一致するパケット（関連付けられたアクセスリストによって許可されたパケット）は、サブマップに指定されているアクションを実行します。以降のサブマップに対するチェックは行われません。パケットがサブマップに一致しない場合に、次のサブマップがチェックされます。 redirect アクションを使用する場合は、リダイレクト先ポートにも同一 VLAN の設定が必要です。redirect アクションが適用されると、指定したリダイレクト先ポートにのみ転送されるようになります。
制限・注意	• 適用済の VLAN フィルターに対してアクションを更新する際、VLAN アクセスマップのエントリー数や適用対象の VLAN 数が多いほど、設定反映時間が長くなります。以下に最悪ケースの例を示します。 　• (例) 2 台スタック構成で 1792 エントリー分のリソースが設定済みの状態で、この全エントリーのアクションを更新する場合、最大で約 240 秒程度かかることがあります。 • redirect アクションはストームコントロール機能が適用される前にリダイレクトされるため、リダイレクトされるトラフィックに対してはストームコントロール機能は適用されません。
バージョン	1.08.02

使用例：VLAN アクセスマップ「vlan-map」のシーケンス番号 10 のサブマップに、drop アクションを設定する方法を示します。

```
# configure terminal
(config)# vlan access-map vlan-map 10
(config-access-map)# action drop
(config-access-map)#
```

8.1.26 vlan filter

vlan filter	
目的	VLAN アクセスマップを適用する VLAN を設定します。新たに指定した VLAN が既存の設定に追加されます。設定を削除する場合は、no 形式のコマンドを使用します。

vlan filter	
Command	vlan filter MAP-NAME vlan-list VLAN-ID-LIST no vlan filter MAP-NAME vlan-list VLAN-ID-LIST
Parameter	MAP-NAME：VLAN アクセスマップ名を指定します。 VLAN-ID-LIST：VLAN ID リストを指定します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	VLAN フィルター機能は、特定の VLAN の受信パケットに対してアクセスコントロールを実施する機能です。送信パケットに対しては動作しません。本コマンドでは、定義した VLAN アクセスマップを適用する VLAN を設定します。

制限・注意	• 1 つの VLAN に関連付けられる VLAN アクセスマップは、1 つだけです。
	• VLAN フィルター機能を使用しているポートでは、「class-default を設定したポリシーマップ(input 方向)」を同時に設定しないでください。同時に設定した場合、そのポートでは常に「class-default を設定したポリシーマップ(input 方向)」が優先されます。そのため、そのポートでは VLAN フィルター機能によるパケットフィルターは動作しなくなります。
	• 適用する VLAN アクセスマップのエントリー数や適用対象の VLAN 数が多いほど、設定反映時間が長くなります。以下に最悪ケースの例を示します。
	  • (例) 2 台スタック構成で 896 エントリー分のリソースが設定済みの状態で、更に 896 エントリー分のリソースを消費する設定を追加する場合、 AEOS-NP2500 Ver. 1.10.01 以降のバージョンでは約 210 秒程度、AEOS-NP2500 Ver. 1.10.01 より前のバージョンでは約 55 秒程度かかることがあります。
	• AEOS-NP2500 Ver. 1.10.01 以降では、VLAN フィルターの設定が完了するまでの時間が 5 秒以上かかる場合は、CLI に進捗状況(%)が表示されます。
	• 受信トラフィックが VLAN タグ付きフレームの場合、受信ポートの VLAN 設定にかかわらず、VLAN タグの VLAN ID が本コマンドで指定した VLAN ID と一致すると、対応する VLAN アクセスマップが適用されます。そのため、受信ポートの VLAN 設定と受信トラフィックが不一致で通常は受信して中継しないトラフィックでも、VLAN アクセスマップが適用される場合があることに注意してください。このような状況を避けるには、自装置のトランクポートと対向装置のトランクポートの VLAN 設定を揃えるようにしてください。
	• 例えば、VLAN 10,20 が設定されているトランクポートで VLAN 30 のトラフィックを受信する状況を例に説明します。このポートでは通常は VLAN 30 のトラフィックを受信して中継しませんが、本コマンドで VLAN 30 に VLAN アクセスマップが適用されている場合は、以下のような動作に注意してください。
	  • 対象 VLAN アクセスマップのハードウェアカウンターでカウントする。
	  • redirect アクションが設定されている場合、本来はこのポートでは受信して中継しない VLAN 30 のトラフィックに対しても redirect アクションが動作する。

バージョン	1.08.02

使用例：VLAN 5 に VLAN アクセスマップ「vlan-map」を適用する方法を示します。

```
# configure terminal
(config)# vlan filter vlan-map vlan-list 5
```

```
(config)#
```

8.1.27 show access-group

show access-group	
目的	ポートに適用したアクセスリストの情報を表示します。
Command	show access-group [interface port PORTS]
Parameter	interface port PORTS（省略可能）：物理ポートを指定します。複数指定できます。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のポートを指定しない場合は、アクセスリストを適用したすべてのポートの情報が表示されます。
制限・注意	• interface パラメーターでアクセスリストを適用していないポートを指定して実行しても、何も表示されません。
バージョン	1.08.02

使用例：ポートに適用したすべてのアクセスリスト情報を表示する方法を示します。

```
# show access-group

Port1/0/1: ...(1)
  (2)                              (3)
  Inbound ip access-list       : simple-ip-acl(ID: 1998)
  Inbound mac access-list      : simple-mac-acl(ID: 7999)
```

項番	説明
(1)	ポート番号を表示します。
(2)	アクセスリストの種類を表示します。 Inbound ip access-list：受信方向に適用した IP アクセスリスト Inbound arp access-list：受信方向に適用した ARP アクセスリスト Inbound ipv6 access-list：受信方向に適用した IPv6 アクセスリスト Inbound expert access-list：受信方向に適用した拡張エキスパートアクセスリスト Inbound mac access-list：受信方向に適用した拡張 MAC アクセスリスト Outbound ip access-list：送信方向に適用した IP アクセスリスト Outbound ipv6 access-list：送信方向に適用した IPv6 アクセスリスト Outbound expert access-list：送信方向に適用した拡張エキスパートアクセスリスト Outbound mac access-list：送信方向に適用した拡張 MAC アクセスリスト
(3)	アクセスリスト名およびアクセスリスト番号を表示します。

8.1.28 show access-list

show access-list	
目的	アクセスリストの設定を表示します。
Command	show access-list [[ip | arp | mac | expert | ipv6] [NAME | NUM]]
Parameter	ip [NAME | NUM]（省略可能）：IP アクセスリストを表示する場合に指定します。アクセスリスト名、またはアクセスリスト番号(1～3999)を指定して表示することも可能です。

show access-list	
	arp［NAME ｜ NUM］(省略可能)：ARP アクセスリストを表示する場合に指定します。アクセスリスト名、またはアクセスリスト番号(4000～5999)を指定して表示することも可能です。 mac［NAME｜NUM］(省略可能)：拡張 MAC アクセスリストを表示する場合に指定します。アクセスリスト名、またはアクセスリスト番号(6000～7999)を指定して表示することも可能です。 expert［NAME｜NUM］(省略可能)：拡張エキスパートアクセスリストを表示する場合に指定します。アクセスリスト名、またはアクセスリスト番号(8000～9999)を指定して表示することも可能です。 ipv6［NAME ｜ NUM］(省略可能)：IPv6 アクセスリストを表示する場合に指定します。アクセスリスト名、またはアクセスリスト番号(11000～14999)を指定して表示することも可能です。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のアクセスリスト種別を指定しない場合は、すべてのアクセスリストの一覧情報が表示されます。
制限・注意	-
バージョン	1.08.02 1.10.01：arp パラメーター追加

使用例：すべてのアクセスリストの一覧情報を表示する方法を示します。

```
# show access-list
(1)                                          (2)
Access-List-Name                             Type
-------------------------------------------  ---------------
rd-ip-acl(ID: 1998)                          ip acl
simple-ip-acl(ID: 3998)                      ip ext-acl
simple-rd-acl(ID: 3999)                      ip ext-acl
rd-mac-acl(ID: 6998)                         mac ext-acl
ip6-acl(ID: 14999)                           ipv6 ext-acl

Total Entries: 5
```

項番	説明
(1)	アクセスリスト名およびアクセスリスト番号を表示します。
(2)	アクセスリストの種類を表示します。 ip acl：標準 IP アクセスリスト ip ext-acl：拡張 IP アクセスリスト arp acl：ARP アクセスリスト ipv6 acl：標準 IPv6 アクセスリスト ipv6 ext-acl：拡張 IPv6 アクセスリスト expert ext-acl：拡張エキスパートアクセスリスト mac ext-acl：拡張 MAC アクセスリスト

使用例：IP アクセスリスト「R&D」の設定を表示する方法を示します。

```
# show access-list ip R&D
```

```
Extended IP access list R&D(ID: 3999) ...(1)
     (2)
     10 permit tcp any 10.20.0.0 0.0.255.255
     20 permit tcp any host 10.100.1.2
     30 permit icmp any any
```

項番	説明
(1)	アクセスリスト名およびアクセスリスト番号を表示します。
(2)	各ルールのシーケンス番号、アクション、抽出条件を表示します。

使用例：アクセスリストハードウェアカウンターを有効にした IP アクセスリスト「simple-ip-acl」の設定を表示する方法を示します。

```
# show access-list ip simple-ip-acl

Extended IP access list simple-ip-acl(ID: 3994) ...(1)
     (2)                                          (3)                  (4)
     10 permit tcp any 10.20.0.0 0.0.255.255  (Ing: 12410 packets Egr: 85201 packets)
     20 permit tcp any host 10.100.1.2  (Ing: 6532 packets Egr: 0 packets)
     30 permit icmp any any  (Ing: 8758 packets Egr: 4214 packets)

     Counter enable on following port(s): ...(5)
     Ingress port(s): Port1/0/5-1/0/8
     Egress port(s): Port1/0/3
```

項番	説明
(1)	アクセスリスト名およびアクセスリスト番号を表示します。
(2)	各ルールのシーケンス番号、アクション、抽出条件を表示します。
(3)	アクセスリストハードウェアカウンターの受信パケット数を表示します。
(4)	アクセスリストハードウェアカウンターの送信パケット数を表示します。
(5)	アクセスリストハードウェアカウンターが有効化されているポート番号を表示します。

8.1.29 show access-list resource reserved-group

show access-list resource reserved-group	
目的	アクセスリストを利用している機能を表示します。
Command	show access-list resource reserved-group
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• 各機能がどのアクセスリストグループを使用するかは、設定時の空き状況や設定順序、装置起動時の処理などにより変わります。そのため、本コマンドの表示結果（各機能がどのアクセスリストグループを使用するか）は設定時と装置起動後で異なることがありますが、show access-list resource reserved-priority コマンドで確認できる優先度順は常に同じになります。
バージョン	1.08.02

使用例：アクセスリストを利用している機能を表示する方法を示します。

```
# show access-list resource reserved-group

Ingress ACL
 (1)              (2)
 Group            Function
-------------    ---------------------
 1/1              Access-list (IPv4)
 1/2              Access-list (Expert)
 1/3              AccessDefenderI
 1/4              AccessDefenderII
 1/5              AccessDefenderIII & Loop Detection
 1/6              AccessDefender (Client)
 1/7              AccessDefender (reserve)

Egress ACL
 (3)              (4)
 Group            Function
-------------    ---------------------
 1/0              Access-list (IPv6)
 1/1              Access-list (IPv6)
 1/2              Access-list (MAC)
 1/3              -
```

項番	説明
(1)	アクセスリストの Ingress グループ ID を表示します。
(2)	Ingress グループを利用している機能を表示します。 Access-list (Expert)：拡張エキスパートアクセスリストを使用している機能 Access-list (ARP)：ARP アクセスリストを使用している機能 Access-list (MAC)：拡張 MAC アクセスリストを使用している機能 Access-list (IPv4)：IP アクセスリストを使用している機能 Access-list (IPv6)：IPv6 アクセスリストを使用している機能 CFM：CFM (Connectivity Fault Management) MMRP (reserve)：MMRP-Plus(予約状態) MMRP：MMRP-Plus AccessDefenderI：AccessDefender 制御用 AccessDefenderII：AccessDefender 制御用 AccessDefenderIII & Loop Detection：AccessDefender 制御用、ループ検知、およびポートリダンダントの一部コマンド AccessDefender (reserve)：AccessDefender クライアント用(予約状態) AccessDefender (Client)：AccessDefender クライアント用(使用中) IGMP snooping：IGMP スヌーピングの unregistered-filter 用 MLD snooping：MLD スヌーピングの unregistered-filter 用
(3)	アクセスリストの Egress グループ ID を表示します。
(4)	Egress グループを利用している機能を表示します。 Access-list (Expert)：拡張エキスパートアクセスリストを使用している機能 Access-list (MAC)：拡張 MAC アクセスリストを使用している機能 Access-list (IPv4)：IP アクセスリストを使用している機能 Access-list (IPv6)：IPv6 アクセスリストを使用している機能

8.1.30 show access-list resource reserved-priority

show access-list resource reserved-priority	
目的	アクセスリストを利用している機能を、アクセスリストに付与された優先度順に表示します。
Command	show access-list resource reserved-priority
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	受信方向に適用したアクセスリスト（例：ip access-group TEST in）では、各アクセスリストは以下の優先度順で動作します。 優先度：高 → 拡張エキスパートアクセスリスト ｜ → ARP アクセスリスト ｜ → 拡張 MAC アクセスリスト ｜ → IP アクセスリスト 低 → IPv6 アクセスリスト 送信方向に適用したアクセスリスト（例：ip access-group TEST out）では、各アクセスリストは以下の優先度順で動作します。 優先度：高 → 拡張 MAC アクセスリスト ｜ → IP アクセスリスト ｜ → 拡張エキスパートアクセスリスト 低 → IPv6 アクセスリスト
制限・注意	-
バージョン	1.08.02

使用例：アクセスリストを利用している機能を、アクセスリストに付与された優先度順に表示する方法を示します。

```
# show access-list resource reserved-priority

Ingress ACL
 (1)              (2)
 Priority         Function
-------------    ---------------------
 1                Access-list (Expert)
 2                Access-list (IPv4)
 3                AccessDefender (Client)
 4                AccessDefenderI
 5                AccessDefenderII
 6                AccessDefenderIII & Loop Detection
 7                -

Egress ACL
 (3)              (4)
 Priority         Function
```

```
-------------   --------------------
 1              Access-list (MAC)
 2              Access-list (IPv6)
 2              Access-list (IPv6)
 4              -
```

項番	説明
(1)	アクセスリストの Ingress グループの優先度を表示します。
(2)	Ingress グループを利用している機能を表示します。 Access-list (Expert)：拡張エキスパートアクセスリストを使用している機能 Access-list (ARP)：ARP アクセスリストを使用している機能 Access-list (MAC)：拡張 MAC アクセスリストを使用している機能 Access-list (IPv4)：IP アクセスリストを使用している機能 Access-list (IPv6)：IPv6 アクセスリストを使用している機能 CFM：CFM (Connectivity Fault Management) MMRP：MMRP-Plus AccessDefenderI：AccessDefender 制御用 AccessDefenderII：AccessDefender 制御用 AccessDefenderIII & Loop Detection：AccessDefender 制御用、ループ検知、およびポートリダンダントの一部コマンド AccessDefender (Client)：AccessDefender クライアント用 IGMP snooping：IGMP スヌーピングの unregistered-filter 用 MLD snooping：MLD スヌーピングの unregistered-filter 用
(3)	アクセスリストの Egress グループの優先度を表示します。
(4)	Egress グループを利用している機能を表示します。 Access-list (Expert)：拡張エキスパートアクセスリストを使用している機能 Access-list (MAC)：拡張 MAC アクセスリストを使用している機能 Access-list (IPv4)：IP アクセスリストを使用している機能 Access-list (IPv6)：IPv6 アクセスリストを使用している機能

8.1.31 show vlan access-map

show vlan access-map	
目的	VLAN アクセスマップの設定を表示します。
Command	show vlan access-map [MAP-NAME]
Parameter	MAP-NAME (省略可能)：表示する VLAN アクセスマップ名を指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN アクセスマップの設定を表示する方法を示します。

```
# show vlan access-map

VLAN access-map vlan-map 10 ...(1)
```

```
  match ip access list: stp_ip1(ID: 1888) ...(2)
  action: forward ...(3)
  Counter enable on VLAN(s): 1-2 ...(4)
  match count: 8541 packets ...(5)
VLAN access-map vlan-map 20
  match mac access list: ext_mac(ID: 6995)
  action: redirect port 1/0/5
  Counter enable on VLAN(s): 1-2
  match count: 5647 packets
```

項番	説明
(1)	サブマップの情報 (VLAN アクセスマップ名およびシーケンス番号) を表示します。
(2)	サブマップに関連付けられたアクセスリスト名およびアクセスリスト番号を表示します。 match ip access list：IP アクセスリスト指定 (match ip address コマンド) match arp address：ARP アクセスリスト指定 (match arp address コマンド) match ipv6 access list：IPv6 アクセスリスト指定 (match ipv6 address コマンド) match mac access list：拡張 MAC アクセスリスト指定 (match mac address コマンド)
(3)	サブマップと一致したパケットに対するアクションを表示します。
(4)	アクセスリストハードウェアカウンターが有効化されている VLAN を表示します。
(5)	アクセスリストハードウェアカウンターの受信パケット数を表示します。

8.1.32 show vlan filter

show vlan filter	
目的	VLAN フィルターの設定を表示します。
Command	show vlan filter [access-map MAP-NAME | vlan VLAN-ID]
Parameter	access-map MAP-NAME (省略可能)：指定した VLAN アクセスマップを適用している VLAN を表示する場合に指定します。 vlan VLAN-ID (省略可能)：指定した VLAN に適用されている VLAN アクセスマップを表示する場合に指定します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：VLAN フィルターの設定を表示する方法を示します。

```
# show vlan filter

VLAN Map vlan-map4 ...(1)
  Configured on VLANs: 1,10,20 ...(2)
```

項番	説明
(1)	VLAN アクセスマップ名を表示します。
(2)	対象の VLAN アクセスマップを適用している VLAN を表示します。

8.1.33 clear acl-hardware-counter

clear acl-hardware-counter	
目的	アクセスリストハードウェアカウンターをクリアします。
Command	clear acl-hardware-counter access-group [ACL-NAME | ACL-NUM] clear acl-hardware-counter vlan-filter [MAP-NAME]
Parameter	ACL-NAME（省略可能）：クリア対象のアクセスリスト名を指定します。 ACL-NUM（省略可能）：クリア対象のアクセスリスト番号を指定します。 MAP-NAME（省略可能）：クリア対象の VLAN アクセスマップ名を指定します。
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	通常のアクセスリストに適用したハードウェアカウンター（show access-list {ip | arp | mac | expert | ipv6}コマンドで確認可能）をクリアする場合は、access-group パラメーターを指定して実施します。特定のアクセスリストを指定しない場合、すべてのアクセスリストのハードウェアカウンターがクリアされます。 VLAN フィルター機能の VLAN アクセスマップに適用したハードウェアカウンター（show vlan access-map コマンドで確認可能）をクリアする場合は、vlan-filter パラメーターを指定して実施します。特定の VLAN アクセスマップを指定しない場合、すべての VLAN アクセスマップのハードウェアカウンターがクリアされます。
制限・注意	-
バージョン	1.08.02

使用例：通常のアクセスリストに適用したハードウェアカウンターをクリアする方法を示します。

```
# clear acl-hardware-counter access-group
#
```

9 セキュリティー

9.1 AccessDefender 共通コマンド

AccessDefender 共通コマンド関連の設定コマンドは以下のとおりです。

- access-defender
- total-client
- authentication interface
- aaa-local-db user
- access-defender static mac
- logout aging-time
- logout timeout
- logout clock
- logout ping dst-ip
- logout ping ttl
- logout linkdown disable interface
- logout linkdown time
- logout linkdown time enable interface
- roaming enable interface
- authentication prefer-attribute
- authentication advanced-vlan-setting
- max-client interface
- max-discard
- vlan mode
- radius-server attribute mac-format

AccessDefender 共通コマンド関連の show／操作コマンドは以下のとおりです。

- show access-defender aaa-local-db
- show access-defender client
- show access-defender deny
- show access-defender port-configuration
- show access-defender port-channel-configuration
- show access-defender rule-statistics
- copy（AccessDefender）
- access-defender deny
- access-defender erase
- access-defender logout

RADIUS サーバーを使用する場合の追加情報は以下のとおりです。

- RADIUS 属性に関する情報

9.1.1 access-defender

access-defender	
目的	AccessDefender 設定モードに遷移します。遷移後のプロンプトは（config-a-def)# に変更されます。

access-defender	
Command	access-defender
Parameter	なし
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	AccessDefender のユーザー名とパスワードは最大 63 文字で指定します。ASCII コードの印字可能な文字のうち、; , | " ? 空白文字 を除いた文字のみ使用可能です。
制限・注意	• 動的 VLAN が割り当てられたクライアントを、ログアウトしていない状態で動的 VLAN とは異なる VLAN の認証無効ポートに移動させると、移動した認証無効ポートでは通信できない仕様制限があります。そのため、そのようなクライアントを認証無効ポートに移動させる場合は、ログアウトした状態にしてから移動させてください。
バージョン	1.08.02

使用例：AccessDefender 設定モードに遷移する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)#
```

9.1.2 total-client

total-client	
目的	認証クライアントの最大数を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	total-client VALUE [deny-client VALUE] [ipv6-disable] no total-client
Parameter	VALUE：認証クライアントの最大数を、1～1024 の範囲で指定します。 deny-client VALUE（省略可能）：認証を一時的に拒否するクライアントの最大数を、1～128 の範囲で指定します。 ipv6-disable（省略可能）：最大数を 769 以上で設定する場合に指定します。
デフォルト	なし
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	AccessDefender を有効にするには、本コマンドで認証クライアントの最大数を設定します。本コマンドは、すべての認証機能（Web 認証、MAC 認証、IEEE 802.1X 認証、および DHCP スヌーピング）が無効な状態で設定します。 ipv6-disable パラメーターを指定しない場合は、1～768 の範囲で設定します。この場合は、IPv6 アドレス認証の使用有無にかかわらず、IPv6 アドレス認証用のアクセスリストのリソースが、必ず 1 グループ予約されます。 ipv6-disable パラメーターを指定した場合は、IPv6 アドレス認証用のアクセスリストのリソースが予約されなくなります。これにより、1～1024 の範囲で設定できるようになります。 認証拒否クライアントを登録するには、deny-client パラメーターで認証拒否クライ

total-client	
	アントの最大数を設定してから、access-defender deny コマンドで登録します。
制限・注意	• AEOS-NP2500 Ver. 1.11.01 より前のバージョンでは、設定範囲は 1～768 です。 • 本機能はアクセスリスト機能と同じハードウェアリソース（Ingress グループ）を、複数グループ使用します。使用するグループ数は設定によります。本機能で使用中の Ingress グループは、他の機能では使用できません。なお、AccessDefender 制御用の 1 グループ、ループ検知、およびポートリダンダントの一部コマンドで使用するグループは、同じ 1 グループを共有します。グループの利用状況は show access-list resource reserved-group コマンドで確認できます。 • 複数の端末の認証が同時に行われた場合の性能を保証するものではありません。
バージョン	1.08.02 1.11.01：ipv6-disable パラメーター追加、設定範囲を拡張

使用例：認証クライアントの最大数を 500、認証拒否クライアントの最大数を 64 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# total-client 500 deny-client 64
(config-a-def)#
```

9.1.3 authentication interface

authentication interface	
目的	指定したインターフェースでの認証を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	authentication interface IF-ID [,|-] {dot1x | mac | web | gateway | static | web-mac | web-dot1x | dot1x-mac | web-dot1x-mac} no authentication interface IF-ID [, | -] {dot1x | mac | web | gateway | static | web-mac | web-dot1x | dot1x-mac | web-dot1x-mac}
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定 認証種別を以下のパラメーターで指定します。 • dot1x：IEEE 802.1X 認証 • mac：MAC 認証 • web：Web 認証 • gateway：ゲートウェイ認証 • static：スタティック認証 • web-mac：Web/MAC 認証(AND) • web-dot1x：Web/IEEE 802.1X 認証(AND) • dot1x-mac：IEEE 802.1X/MAC 認証(AND) • web-dot1x-mac：Web/IEEE 802.1X/MAC 認証(AND)
デフォルト	なし
モード	AccessDefender 設定モード
特権レベル	レベル：15

authentication interface	
ガイドライン	同一インターフェースで、IEEE 802.1X 認証、MAC 認証、Web 認証、スタティック認証の中から複数の認証機能を有効にした場合は、「OR 認証」になります。「OR 認証」では、いずれか 1 つの認証機能で認証されると、認証済みクライアントとして登録され通信が許可されます。 一方、web-mac パラメーターなどで指定する「AND 認証」では、すべての認証機能で認証されると、認証済みクライアントとして登録され通信が許可されます。 Web/MAC 認証(AND)では、MAC 認証、Web 認証の順に成功する必要があります。認証に成功したクライアントには Web 認証で取得した属性情報（VLAN ID、クラス ID）が反映されますが、authentication prefer-attribute コマンドで MAC 認証で取得した属性情報に変更することも可能です。 web-mac パラメーターと mac パラメーターの両方を指定したインターフェースでの Web/MAC 認証(AND)は、以下のような動作となります。 • クライアントから Web 認証の HTTP/HTTPS プロトコルの Web 認証要求を受信しログイン認証ページを返した後、クライアントから「Web 認証用のユーザー名とパスワード」を受信すると、装置は Web/MAC 認証(AND)の「MAC 認証用のユーザー名とパスワード」で認証の問い合わせを行います。そして、その問い合わせに成功すると、自動的に「Web 認証用のユーザー名とパスワード」で認証の問い合わせを行います。 • 「MAC 認証用のユーザー名とパスワード」で認証の問い合わせに失敗した場合は、認証処理を打ち切ります。 • 「MAC 認証用のユーザー名とパスワード」「Web 認証用のユーザー名とパスワード」のいずれの問い合わせも、aaa authentication web-auth コマンドで指定した認証方式リストを使用するように変更されます。 Web/IEEE 802.1X 認証(AND)では、IEEE 802.1X 認証、Web 認証の順に成功する必要があります。認証に成功したクライアントには Web 認証で取得した属性情報（VLAN ID、クラス ID）が反映されますが、authentication prefer-attribute コマンドで IEEE 802.1X 認証で取得した属性情報に変更することも可能です。 IEEE 802.1X/MAC 認証(AND)では、MAC 認証、IEEE 802.1X 認証の順に成功する必要があります。認証に成功したクライアントには IEEE 802.1X 認証で取得した属性情報（VLAN ID、クラス ID）が反映されますが、authentication prefer-attribute コマンドで MAC 認証で取得した属性情報に変更することも可能です。 Web/IEEE 802.1X/MAC 認証(AND)では、MAC 認証、IEEE 802.1X 認証、Web 認証の順に成功する必要があります。認証に成功したクライアントには Web 認証で取得した属性情報（VLAN ID、クラス ID）が反映されますが、authentication prefer-attribute コマンドで他の認証機能で取得した属性情報に変更することも可能です。 スタティック認証エントリーは access-defender static mac コマンドで登録します。
制限・注意	• ポートセキュリティー機能が有効なポートでは、AccessDefender による認証は併用できません。 • 同一インターフェースではゲートウェイ認証と他の認証機能は併用できません。 • ゲートウェイ認証では、ダイナミック VLAN やクラス ID の割り当てはサポートしていません。 • ポートチャネルで認証を有効にする場合は、ポートチャネルのメンバーポート（物理ポート）ではなく、ポートチャネルを指定して設定してください。 • スパニングツリープロトコル（STP/RSTP/MSTP/RPVST+）が動作しているポート

authentication interface	

	で認証を併用することは未サポートです。
	• トランクポートでのダイナミック VLAN は未サポートです。
	• ゲートウェイ認証は IP アドレスベースで動作します。そのため、ゲートウェイ認証で許可されたクライアントの IP アドレスが認証後に変更された場合は、通信ができなくなります。
	• ゲートウェイ認証、Web/MAC 認証(AND)、Web/IEEE 802.1X 認証(AND)、IEEE 802.1X/MAC 認証(AND)、および Web/IEEE 802.1X/MAC 認証(AND)は、DHCP スヌーピングとは併用できません。
	• 各認証機能の併用に関しては「認証機能の同一インターフェースでの併用可否」も参照してください。
	• 同一ポートで以下の併用をサポートしています。なお、以下以外の組み合わせでは、同一ポートで AND 認証と IEEE 802.1X 認証、MAC 認証、Web 認証は併用できません。
	  • Web/MAC 認証(AND)と MAC 認証の併用(web-mac と mac)
	  • Web/IEEE 802.1X 認証(AND)と MAC 認証の併用(web-dot1x と mac)
	• インターフェースに設定済みの認証機能を変更すると、そのポートで認証済みのすべてのクライアントはログアウトします。
	• タグ付きの IEEE 802.1X 認証フレームは認証できません。
	• AND 認証では、クライアントは、MAC 認証、IEEE 802.1X 認証、Web 認証の順に認証に成功する必要があります。

バージョン	1.08.02

■ 認証機能の同一インターフェースでの併用可否

認証機能	スタティック認証との併用 (OR)	DHCP スヌーピングとの併用 (AND)
Web 認証	可	可
IEEE 802.1X 認証	可	可
MAC 認証	可	可
Web 認証、MAC 認証 (OR 認証)	可	可
Web 認証、IEEE 802.1X 認証 (OR 認証)	可	可
IEEE 802.1X 認証、MAC 認証 (OR 認証)	可	可
Web 認証、IEEE 802.1X 認証、MAC 認証 (OR 認証)	可	可
ゲートウェイ認証	不可	不可
Web/MAC 認証(AND)	可	不可
Web/IEEE 802.1X 認証(AND)	可	不可
IEEE 802.1X/MAC 認証(AND)	可	不可
Web/IEEE 802.1X/MAC 認証(AND)	可	不可

使用例：ポート 1/0/1～1/0/10 で Web 認証を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
```

```
(config-a-def)# authentication interface port 1/0/1-10 web
(config-a-def)#
```

9.1.4 aaa-local-db user

aaa-local-db user	
目的	AccessDefender のユーザーアカウントをローカルデータベースに設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	aaa-local-db user NAME [password [0 | 7] PASS] [vlan VLAN-ID] [class CLASS-ID] no aaa-local-db [user NAME]
Parameter	NAME：ユーザー名を最大 63 文字で指定します。ASCII コードの印字可能な文字のうち、; , | " ? 空白文字 を除いた文字のみ使用可能です。 password [0 | 7] PASS（省略可能）：パスワードを指定します。 • [0 | 7]（省略可能）：後に続くパスワードの文字列の形式を明示する場合に指定します。0 の場合は平文を、7 の場合は暗号化された形式を意味します。省略した場合は、平文で入力します。 • PASS：平文で入力する場合は、パスワードを最大 63 文字で指定します。ASCII コードの印字可能な文字のうち、; , | " ? 空白文字 を除いた文字のみ使用可能です。 vlan VLAN-ID（省略可能）：VLAN ID を 1～4094 の範囲で指定します。 class CLASS-ID（省略可能）：クラス ID を 1～4095 の範囲で指定します。
デフォルト	なし
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	ユーザー名を指定せずに no aaa-local-db コマンドを使用した場合、すべてのエントリーが削除されます。 MAC 認証では、MAC アドレスをユーザー名として登録する必要があります。MAC アドレスの形式は mac-authentication username mac-format コマンドの設定に従います。
制限・注意	• エントリーは、最大 3000 件まで登録できます。
バージョン	1.08.02

使用例：AccessDefender のユーザーアカウント（ユーザー名 apresia、パスワード apresia、VLAN ID=10、クラス ID=10）を、ローカルデータベースに設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# aaa-local-db user apresia password apresia vlan 10 class 10
(config-a-def)#
```

9.1.5 access-defender static mac

access-defender static mac	
目的	スタティック認証エントリーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	access-defender static mac MAC-ADDRESS [vlan VLAN-ID] [class CLASS-

access-defender static mac	
	ID] interface IF-ID no access-defender static mac MAC-ADDRESS
Parameter	MAC-ADDRESS：スタティック認証エントリーの MAC アドレスを、以下のいずれかの形式で指定します。どの形式で指定しても構成情報ではハイフン区切りで表示されます。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） vlan VLAN-ID（省略可能）：スタティック認証エントリーに関連付ける VLAN ID を 1～4094 の範囲で指定します。 class CLASS-ID（省略可能）：スタティック認証エントリーに関連付けるクラス ID を 1～4095 の範囲で指定します。 interface IF-ID：スタティック認証エントリーを接続するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定
デフォルト	スタティックエントリーの設定なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	スタティック認証エントリーを使用する場合は、必ず authentication interface コマンドで対象ポートのスタティック認証を有効にしてください。 スタティック認証エントリー1 個につき、total-client コマンドで設定した認証クライアントのリソースを 1 個消費します。 他認証で認証済みのクライアントまたは Discard 登録されたクライアントを指定して登録した場合は、スタティック認証エントリーとして上書きされます。
制限・注意	• 登録可能なスタティック認証エントリー数は最大 64 です。 • total-client コマンドで設定した認証クライアントの最大数を超えて、スタティック認証エントリーを設定することはできません。 • スタティック認証が無効なポートに対してスタティック認証エントリーを設定した場合でも、内部のリソースは消費されます。
バージョン	1.08.02

使用例：スタティック認証エントリー「MAC アドレス=00:00:5E:00:53:01、VLAN ID=10、クラス ID=1234、ポート 1/0/1」を設定する方法を示します。

```
# configure terminal
(config)# access-defender static mac 00:00:5E:00:53:01 vlan 10 class 1234 interface port 1/0/1
(config)#
```

9.1.6 logout aging-time

logout aging-time	
目的	無通信の認証済みクライアントが自動的にログアウトするまでの経過時間（エージン

logout aging-time	
	グログアウト時間）を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	logout aging-time SECONDS [MINUTES [HOURS [DAYS]]] {web | gateway | mac | dot1x} no logout aging-time [web | gateway | mac | dot1x]
Parameter	SECONDS [MINUTES [HOURS [DAYS]]]：無通信の認証済みクライアントが自動的にログアウトするまでの経過時間（エージングログアウト時間）を指定します。 • SECONDS：0, 10～86,400 秒の範囲で指定 • MINUTES（省略可能）：0～59 分の範囲で指定 • HOURS（省略可能）：0～23 時間の範囲で指定 • DAYS（省略可能）：0～31 日の範囲で指定 本機能の対象にする認証種別を以下のパラメーターで指定します。 • web：Web 認証 • gateway：ゲートウェイ認証 • mac：MAC 認証 • dot1x：IEEE 802.1X 認証
デフォルト	0 秒（無通信の認証済みクライアントを自動ログアウトしない）
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本機能を 0 秒以外に設定すると、認証済みクライアントは無通信の時間がエージングログアウト時間経過すると自動的にログアウトします。 適用されるエージングログアウト時間は、設定したパラメーターの合計値になります。例えば、logout aging-time 40 2 0 0 と設定した場合は、エージングログアウト時間は 160 秒になります。 Web/MAC 認証(AND)、Web/IEEE 802.1X 認証(AND)、Web/IEEE 802.1X/MAC 認証(AND)で使用する場合は、web パラメーターを指定して設定してください。IEEE 802.1X/MAC 認証(AND)で使用する場合は、dot1x パラメーターを指定して設定してください。
制限・注意	-
バージョン	1.08.02

使用例：Web 認証のエージングログアウト時間を 1000 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# logout aging-time 1000 web
(config-a-def)#
```

9.1.7 logout timeout

logout timeout	
目的	認証済みクライアントが自動的にログアウトするまでの経過時間（タイムアウト時間）を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	logout timeout SECONDS [MINUTES [HOURS [DAYS]]] {web | gateway | mac | dot1x}

logout timeout	
	no logout timeout [web | gateway | mac | dot1x]
Parameter	SECONDS [MINUTES [HOURS [DAYS]]]：認証済みクライアントが自動的にログアウトするまでの経過時間（タイムアウト時間）を指定します。 • SECONDS：0, 10～86,400 秒の範囲で指定 • MINUTES（省略可能）：0～59 分の範囲で指定 • HOURS（省略可能）：0～23 時間の範囲で指定 • DAYS（省略可能）：0～31 日の範囲で指定 本機能の対象にする認証種別を以下のパラメーターで指定します。 • web：Web 認証 • gateway：ゲートウェイ認証 • mac：MAC 認証 • dot1x：IEEE 802.1X 認証
デフォルト	0 秒（認証済みクライアントを自動ログアウトしない）
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本機能を 0 秒以外に設定すると、認証済みクライアントはログインしてからの時間がタイムアウト時間経過すると自動的にログアウトします。 適用されるタイムアウト時間は、設定したパラメーターの合計値になります。例えば、logout timeout 40 2 0 0 と設定した場合は、タイムアウト時間は 160 秒になります。 Web/MAC 認証(AND)、Web/IEEE 802.1X 認証(AND)、Web/IEEE 802.1X/MAC 認証(AND)で使用する場合は、web パラメーターを指定して設定してください。IEEE 802.1X/MAC 認証(AND)で使用する場合は、dot1x パラメーターを指定して設定してください。
制限・注意	-
バージョン	1.08.02

使用例：Web 認証のタイムアウト時間を 1000 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# logout timeout 1000 web
(config-a-def)#
```

9.1.8 logout clock

logout clock	
目的	認証済みクライアントの指定時刻ログアウトを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	logout clock HH:MM {web | gateway | mac | dot1x} no logout clock [web | gateway | mac | dot1x]
Parameter	HH:MM：認証済みクライアントをログアウトさせる時刻を 時:分 形式で指定します。時は 24 時間表記で指定します。 本機能の対象にする認証種別を以下のパラメーターで指定します。 • web：Web 認証

logout clock	
	• gateway：ゲートウェイ認証 • mac：MAC 認証 • dot1x：IEEE 802.1X 認証
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本機能を設定すると、認証済みクライアントは指定した時刻にログアウトします。 Web/MAC 認証(AND)、Web/IEEE 802.1X 認証(AND)、Web/IEEE 802.1X/MAC 認証(AND)で使用する場合は、web パラメーターを指定して設定してください。IEEE 802.1X/MAC 認証(AND)で使用する場合は、dot1x パラメーターを指定して設定してください。
制限・注意	-
バージョン	1.08.02

使用例：Web 認証で、18:00 を指定して認証済みクライアントの指定時刻ログアウトを有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# logout clock 18:00 web
(config-a-def)#
```

9.1.9 logout ping dst-ip

logout ping dst-ip	
目的	宛先 IPv4/IPv6 アドレス指定の ping ログアウト機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	logout ping dst-ip {IP-ADDRESS | IPV6-ADDRESS} no logout ping dst-ip
Parameter	IP-ADDRESS：宛先 IPv4 アドレスを指定します。 IPV6-ADDRESS：宛先 IPv6 アドレスを指定します。
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本機能を有効にすると、認証済みクライアントから指定した宛先 IPv4/IPv6 アドレスの ICMP Request パケットを受信した場合に、認証済みクライアントはログアウトします。
制限・注意	• Web 認証、ゲートウェイ認証でのみ有効です。 • 宛先 IPv4/IPv6 アドレスはそれぞれ 1 個ずつ設定できます。 • 本コマンドの IPv4 アドレスと logout ping ttl コマンドを併用した場合は、2 つの条件を満たした場合のみ認証済みクライアントがログアウトします。
バージョン	1.08.02

使用例：宛先 IPv4 アドレス 192.0.2.1 指定で ping ログアウト機能を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# logout ping dst-ip 192.0.2.1
(config-a-def)#
```

使用例：宛先 IPv6 アドレス 2001:db8::1 指定で ping ログアウト機能を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# logout ping dst-ip 2001:db8::1
(config-a-def)#
```

9.1.10 logout ping ttl

logout ping ttl	
目的	TTL 指定の ping ログアウト機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	logout ping ttl VALUE no logout ping ttl
Parameter	VALUE：TTL 値を 1～255 の範囲で指定します。
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本機能を有効にすると、認証済みクライアントから指定した TTL 値の ICMP Request パケットを受信した場合に、認証済みクライアントはログアウトします。
制限・注意	• Web 認証、ゲートウェイ認証でのみ有効です。 • TTL 値は 1 個だけ設定できます。 • 本コマンドと logout ping dst-ip コマンドを併用した場合は、IPv4 の ping パケットが 2 つの条件を満たした場合のみ認証済みクライアントがログアウトします。
バージョン	1.08.02

使用例：TTL 値=1 指定で ping ログアウト機能を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# logout ping ttl 1
(config-a-def)#
```

9.1.11 logout linkdown disable interface

logout linkdown disable interface	
目的	認証ポートのリンクダウンによるログアウトを無効にします。有効にする場合は、no 形式のコマンドを使用します。
Command	logout linkdown disable interface IF-ID [,|-] no logout linkdown disable interface IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定

logout linkdown disable interface	
デフォルト	認証ポートのリンクダウンによるログアウトは有効（no logout linkdown disable interface）
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	この機能をローミング機能（roaming enable interface コマンド）と同時に使用すると、認証済みクライアントの通信ポートが変更されてもログアウトすることなく通信が継続されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/10 がリンクダウンしたときに、認証済みのクライアントがログアウトしないように設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# logout linkdown disable interface port 1/0/1-10
(config-a-def)#
```

9.1.12 logout linkdown time

logout linkdown time	
目的	リンクダウン監視時間を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	logout linkdown time SECONDS no logout linkdown time
Parameter	SECONDS：リンクダウン監視時間を、1～300 秒の範囲で指定します。
デフォルト	なし
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	リンクダウン監視時間が有効なインターフェースでは、リンクダウンしてもリンクダウン監視時間が経過するまでログアウトしなくなります。そのため、リンクダウン監視時間が経過する前にリンクアップすると、認証済みクライアントはログアウトを回避できます。
制限・注意	-
バージョン	1.08.02

使用例：リンクダウン監視時間を 10 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# logout linkdown time 10
(config-a-def)#
```

9.1.13 logout linkdown time enable interface

logout linkdown time enable interface	
目的	リンクダウン監視時間を有効にします。無効にする場合は、no 形式のコマンドを使用します。

logout linkdown time enable interface	
Command	logout linkdown time enable interface IF-ID [,|-] no logout linkdown time enable interface IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	リンクダウン監視時間が有効なインターフェースでは、リンクダウンしてもリンクダウン監視時間が経過するまでログアウトしなくなります。そのため、リンクダウン監視時間が経過する前にリンクアップすると、認証済みクライアントはログアウトを回避できます。 リンクダウン監視時間が無効になっている場合、またはリンクダウン監視時間が設定されていない場合、認証済みクライアントはリンクダウン直後にログアウトします。 リンクダウン監視時間は、logout linkdown time コマンドで設定します。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/10 のリンクダウン監視時間を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# logout linkdown time enable interface port 1/0/1-10
(config-a-def)#
```

9.1.14 roaming enable interface

roaming enable interface	
目的	指定したインターフェースのローミング機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	roaming enable interface IF-ID [,|-] no roaming enable interface IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	ローミング機能が有効で、logout linkdown disable interface コマンドでリンクダウン時のログアウトを無効に設定しているインターフェース間では、認証済みクライアントの接続ポートを変更してもログアウトしません。
制限・注意	• roaming enable interface コマンドで指定したインターフェースは、logout linkdown disable interface コマンドもあわせて設定してください。 • ローミング機能は、roaming enable interface コマンドを実行し、同じ認証機能を

roaming enable interface	
	使用する、同じデバイス上のポート間でのみ有効にできます。 • ローミング後に、ローミング前のポートがリンクダウンすると、ローミング後のポートの状態にかかわらず、リンクダウンによるログアウトが発生します。このログアウトを回避するには、ローミング前のポートに対して logout linkdown disable interface コマンドを設定してください。 • ローミングしている接続ポートが変更された場合でも、show access-defender client コマンドを使用したときに表示されるポート番号は、ログイン時のポート番号です。ローミング機能が有効になっているポートのポート番号の後ろにアスタリスク(*)が表示されます。 • ローミング時のポートの設定を変更しても変更以前にログインした端末はログアウトされません。設定変更前の設定でログイン状態を保持します。設定変更後にログインした端末は変更後の設定が反映されます。 • ローミング機能が有効なポートで端末の認証が成功し、その後 VLAN が変更された場合、ローミング機能が有効なすべてのポートにおいて、変更後の VLAN のトラフィックが中継されます。 • 認証済み端末がないローミングポートの認証が無効になっている場合、他のローミングポートで認証された端末がログアウトするまで、動的 VLAN およびクラス ID の変更は解除されません。 • 動的 VLAN およびクラス ID の変更を解除するには、装置を再起動するか、一時的に認証を無効にします。
バージョン	1.08.02

使用例：ポート 1/0/1～1/0/10 でローミング機能を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# roaming enable interface port 1/0/1-10
(config-a-def)#
```

9.1.15 authentication prefer-attribute

authentication prefer-attribute	
目的	AND 認証において、認証に成功したクライアントに反映する属性情報（VLAN ID、クラス ID）として、どの認証機能で取得した属性情報を使用するかを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	authentication {web-mac | web-dot1x | dot1x-mac | web-dot1x-mac} prefer-attribute {web | dot1x | mac} no authentication {web-mac | web-dot1x | dot1x-mac | web-dot1x-mac} prefer-attribute
Parameter	認証種別を以下のパラメーターで指定します。 • web-mac：Web/MAC 認証(AND) • web-dot1x：Web/IEEE 802.1X 認証(AND) • dot1x-mac：IEEE 802.1X/MAC 認証(AND) • web-dot1x-mac：Web/IEEE 802.1X/MAC 認証(AND) prefer-attribute：認証成功端末に適用する認証属性（VLAN ID やクラス ID）の取得元の認証機能を指定します。

authentication prefer-attribute	
	• web：Web 認証で取得した認証属性を適用 • dot1x：IEEE 802.1X 認証で取得した認証属性を適用 • mac：MAC 認証で取得した認証属性を適用
デフォルト	なし
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本コマンドを設定しない場合は、Web/MAC 認証(AND)、Web/IEEE 802.1X 認証(AND)、Web/IEEE 802.1X/MAC 認証(AND)では Web 認証で取得した認証属性が適用されます。IEEE 802.1X/MAC 認証(AND)では IEEE 802.1X 認証で取得した認証属性が適用されます。 本コマンド設定時には、以下におけるユーザー名が、本コマンドで指定した認証機能のユーザー名で表示されるようになります。 • show access-defender client コマンドで表示されるユーザー名 • ログイン成功/ログアウト成功ログで表示されるユーザー名 • ログイン成功/ログアウト成功時のアカウンティング情報のユーザー名
制限・注意	• Web/MAC 認証(AND)では、dot1x パラメーターは指定できません。 • IEEE 802.1X/MAC 認証(AND)では、web パラメーターは指定できません。 • Web/IEEE 802.1X 認証(AND)では、mac パラメーターは指定できません。
バージョン	1.08.02

使用例：Web/MAC 認証(AND)において、MAC 認証で取得した認証属性を適用する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# authentication web-mac prefer-attribute mac
(config-a-def)#
```

9.1.16 authentication advanced-vlan-setting

authentication advanced-vlan-setting	
目的	Web/MAC 認証(AND)、または Web/IEEE 802.1X 認証(AND)において、アドバンスド VLAN 設定モードを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	authentication {web-mac | web-dot1x} advanced-vlan-setting no authentication {web-mac | web-dot1x} advanced-vlan-setting
Parameter	web-mac：Web/MAC 認証(AND)において、アドバンスド VLAN 設定モードを有効にする場合に指定します。 web-dot1x：Web/IEEE 802.1X 認証(AND)において、アドバンスド VLAN 設定モードを有効にする場合に指定します。
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	アドバンスド VLAN 設定モードを有効にした Web/MAC 認証(AND)の場合、MAC 認証処理で認証に成功した時点で、通信が許可されない状態で、MAC 認証処理で取得した認証属性 (VLAN ID、クラス ID) が装置に反映されるようになります。

authentication advanced-vlan-setting	
	アドバンスド VLAN 設定モードを有効にした Web/IEEE 802.1X 認証(AND)の場合、IEEE 802.1X 認証処理で認証に成功した時点で、通信が許可されない状態で、IEEE 802.1X 認証処理で取得した認証属性（VLAN ID、クラス ID）が装置に反映されるようになります。
制限・注意	-
バージョン	1.08.02

使用例：Web/IEEE 802.1X 認証(AND)において、アドバンスド VLAN 設定モードを有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# authentication web-dot1x advanced-vlan-setting
(config-a-def)#
```

9.1.17 max-client interface

max-client interface	
目的	指定したインターフェースの認証可能なクライアントの最大数を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	max-client VALUE interface IF-ID [,|-] no max-client interface IF-ID [,|-]
Parameter	VALUE：認証可能なクライアントの最大数を、1～1024 の範囲で指定します。 IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	なし
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本コマンドで接続クライアント数を制限しない場合は、1 インターフェースにつき、装置で認証できるクライアントの最大数まで認証できます。
制限・注意	• AEOS-NP2500 Ver. 1.11.01 より前のバージョンでは、設定範囲は 1～768 です。
バージョン	1.08.02 1.11.01：設定範囲を拡張

使用例：ポート 1/0/1 で認証可能なクライアントの最大数を 500 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# max-client 500 interface port 1/0/1
(config-a-def)#
```

9.1.18 max-discard

max-discard	
目的	MAC 認証に失敗して Discard 登録されるクライアントの最大数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	max-discard VALUE

max-discard	
	no max-discard
Parameter	VALUE：最大数を 100～200 の範囲で指定します。
デフォルト	200
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	MAC 認証に失敗したクライアントのみが、Discard 登録されます。
制限・注意	• 本コマンドは、MAC 認証を無効にした状態で設定してください。
バージョン	1.08.02

使用例：Discard 登録されるクライアントの最大数を、100 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# max-discard 100
(config-a-def)#
```

9.1.19 vlan mode

vlan mode	
目的	AccessDefender の VLAN モードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	vlan mode {dynamic port-base | static} no vlan mode
Parameter	dynamic port-base：dynamic port-base モードに設定する場合に指定します。 static：static モードに設定する場合に指定します。
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	デフォルトでは、ダイナミック VLAN により同一ポートに複数の VLAN を割り当てることができます。 VLAN モードを dynamic port-base モードに設定した場合は、2 台目以降の認証クライアントのダイナミック VLAN 動作を制限するモードになります。動作概要については「dynamic port-base モードの場合の動作概要」を参照してください。 VLAN モードを static モードに設定した場合は、ダイナミック VLAN 動作を禁止することができます。認証に成功して属性値として VLAN ID が通知された場合でも、ダイナミック VLAN は動作せず、元々対象ポートに設定されていた VLAN が割り当てられます。 本コマンドを dynamic port-base モード、または static モードに設定した場合でも、スタティック認証エントリーの VLAN は access-defender static mac コマンドの設定に従います。 本コマンドを dynamic port-base モードに設定してスタティック認証エントリーを併用する場合、スタティック認証エントリーも「ログイン中のクライアント」として扱われます。
制限・注意	• 本コマンドを dynamic port-base モードに設定してスタティック認証エントリーを

vlan mode	
	併用する環境において、同一インターフェースに複数のスタティック認証エントリーを設定している場合は、一番最後に設定したスタティック認証エントリーが「ログイン中のクライアント」として扱われます。 • なお、スタティック認証エントリーは構成情報では MAC アドレスで昇順にソートされて表示されます。そのため再起動後は、構成情報のより下の行に設定されているスタティック認証エントリーが、一番最後に設定したスタティック認証エントリーになることに注意してください。
バージョン	1.08.02

■ dynamic port-base モードの場合の動作概要

ログイン中のクライアントの VLAN	同一ポートで後から認証を行うクライアント	ログイン可否
対象ポートに元々設定されている VLAN	VLAN ID の通知なし	可
	属性値として VLAN ID（ログイン中のクライアントと同じ VLAN）の通知あり	可
	属性値として VLAN ID（ログイン中のクライアントと異なる VLAN）の通知あり	不可
対象ポートに元々設定されている VLAN と異なる VLAN	VLAN ID の通知なし	不可
	属性値として VLAN ID（ログイン中のクライアントと同じ VLAN）の通知あり	可
	属性値として VLAN ID（ログイン中のクライアントと異なる VLAN）の通知あり	不可

使用例：AccessDefender の VLAN モードを static モードに設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# vlan mode static
(config-a-def)#
```

9.1.20 radius-server attribute mac-format

radius-server attribute mac-format	
目的	装置から送信される RADIUS 要求パケットの、「Calling-Station-Id」属性の MAC アドレス形式を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	radius-server attribute mac-format case {lowercase | uppercase} delimiter {{hyphen | colon | dot} number {1 | 2 | 5} | none} no radius-server attribute mac-format
Parameter	case：「Calling-Station-Id」属性の MAC アドレスの大文字／小文字の設定を指定します。 • lowercase：小文字指定（例：aabbccddeeff） • uppercase：大文字指定（例：AABBCCDDEEFF） delimiter：区切り文字を指定します。 • hyphen：ハイフン指定（例：aa-bb-cc-dd-ee-ff） • colon：コロン指定（例：aa:bb:cc:dd:ee:ff）

radius-server attribute mac-format	
	• dot：ドット指定（例：aa.bb.cc.dd.ee.ff） • none：区切り文字を使用しない場合に指定（例：aabbccddeeff） number：区切り文字の数を指定します。 • 1：区切り文字 1 個指定（例：aabbcc-ddeeff） • 2：区切り文字 2 個指定（例：aabb-ccdd-eeff） • 5：区切り文字 5 個指定（例：aa-bb-cc-dd-ee-ff）
デフォルト	小文字、区切り文字を使用しない形式（例：aabbccddeeff）
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：装置から送信される RADIUS 要求パケットの、「Calling-Station-Id」属性の MAC アドレス形式を、大文字で、区切り文字としてハイフンを 5 つ使用する形式に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# radius-server attribute mac-format case uppercase delimiter hyphen
number 5
(config-a-def)#
```

9.1.21 show access-defender aaa-local-db

show access-defender aaa-local-db	
目的	AccessDefender のローカルデータベースの情報を表示します。
Command	show access-defender aaa-local-db
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：AccessDefender のローカルデータベースの情報を表示する方法を示します。

```
# show access-defender aaa-local-db
(1)   (2)                                                          (3)  (4)
-------------------------------------------------------------------------------
No.  Username                                                     VID Class
-------------------------------------------------------------------------------
1    user1                                                         50
2    user2                                                         20
3    user3                                                         30
4    user4                                                         40    40
5    user5                                                         50
6    user6                                                         60    60
```

項番	説明
(1)	通し番号を表示します。
(2)	ユーザー名を表示します。
(3)	VLAN ID を表示します。
(4)	クラス ID を表示します。

9.1.22 show access-defender client

show access-defender client	
目的	認証済みクライアントと、MAC 認証に失敗して Discard 登録されたクライアントを表示します。
Command	show access-defender client [interface IF-ID [,|-]] [type {dhcp-snooping | disc | dot1x | gateway | mac | static | web}]
Parameter	interface IF-ID（省略可能）：クライアント情報を表示するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定 type（省略可能）：表示するクライアント種別を以下のパラメーターで指定します。 • dhcp-snooping：DHCP スヌーピングの登録済みクライアント。 • disc：MAC 認証に失敗して Discard 登録されたクライアント。 • dot1x：IEEE 802.1X 認証の認証済みクライアント。 • gateway：ゲートウェイ認証の認証済みクライアント。 • mac：MAC 認証の認証済みクライアント。 • static：スタティック認証の登録済みクライアント。 • web：Web 認証の認証済みクライアント。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：認証済みクライアントと、Discard 登録されたクライアントを表示する方法を示します。

```
# show access-defender client

Total number of Clients           :    3 ...(1)
Total number of Discarded Clients :    1 ...(2)

   Codes: W = Web authentication, G = Gateway authentication,
          M = MAC authentication, - = MAC authentication (discard),
          X = IEEE802.1X, D(S) = DHCP snooping (static),
          S = Static authentication
    Port: C = port-channel, * = roaming,
(3) (4)              (5)                                    (6)    (7)   (8)
T   MAC address      IP                                     Port   VID   Cls
(9)                                                           (10)   (11)
User                                                          Time   Aging
-------------------------------------------------------------------------------
-   00-17-A4-F6-D3-04                                    1/0/3
0017a4f6d304                                              0:00:21 0:00:00
```

```
WD  00-17-A4-D6-B3-A4 172.170.100.100                          1/0/1 4094   10
webuser01                                                       0:20:39 0:00:00

WM  00-17-A4-D6-F3-C4 172.170.1.1                              1/0/2 4094   10
webuser03                                                       0:20:39 0:00:15

D   00-17-29-7F-6F-2A 172.170.2.100                              C/1
N/A                                                             0:00:36 0:00:00
```

項番	説明
(1)	認証済みクライアントの数を表示します。
(2)	MAC 認証に失敗して Discard 登録されたクライアントの数を表示します。
(3)	認証済みクライアント、または MAC 認証に失敗して Discard 登録されたクライアントのタイプコードを表示します。タイプコードが複数ある場合は、そのクライアントが AND 認証に成功したことを意味します。 W：Web 認証 G：ゲートウェイ認証 M：MAC 認証 -：MAC 認証に失敗して Discard 登録されたクライアント X：IEEE 802.1X 認証 D：DHCP スヌーピング S：スタティック認証
(4)	クライアントの MAC アドレスを表示します。
(5)	クライアントの IP アドレスを表示します。
(6)	クライアントが接続されたポート番号またはポートチャネル番号を表示します。
(7)	クライアントが所属する VLAN ID を表示します。
(8)	クライアントに関連付けられたクラス ID を表示します。クラス ID が関連付けられていない場合は表示されません。
(9)	クライアントのユーザー名を表示します。
(10)	クライアントが認証されてからの経過時間、または MAC 認証に失敗して Discard 登録されてからの経過時間を表示します。 経過時間が 10 時間より短い場合は（時):(分):(秒）形式で表示され、10 時間以上の場合は(日)d(時)hr 形式で表示されます。
(11)	認証済みクライアントの無通信時間（最後に通信してからの経過時間）を表示します。 経過時間が 10 時間より短い場合は（時):(分):(秒）形式で表示され、10 時間以上の場合は(日)d(時)hr 形式で表示されます。

9.1.23 show access-defender deny

show access-defender deny	
目的	認証拒否クライアントの情報を表示します。
Command	show access-defender deny
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1

show access-defender deny	
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：認証拒否クライアントの情報を表示する方法を示します。

```
# show access-defender deny

Total number of Denied Clients     :    2 ...(1)
(2)                 (3)                                          (4)
MAC address         IP                                           Timer
-------------------------------------------------------------------------
00-00-11-11-22-22 -                                              0:29:04
-                   100.100.100.100                              0:29:04
```

項番	説明
(1)	認証拒否クライアントの数を表示します。
(2)	認証拒否クライアントの MAC アドレスを表示します。
(3)	認証拒否クライアントの IP アドレスを表示します。
(4)	認証拒否クライアントの、認証を拒否する残り時間を表示します。

9.1.24 show access-defender port-configuration

show access-defender port-configuration	
目的	ポートの AccessDefender 設定を表示します。
Command	show access-defender port-configuration
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポートの AccessDefender 設定を表示する方法を示します。

```
# show access-defender port-configuration

AccessDefender Port Configuration:
  mac = mac-authentication, 802.1X = IEEE802.1X,
  web = web-authentication, gateway = web-authentication gateway,
  web/mac = web/mac authentication,
  web/.1X = web/IEEE802.1X authentication,
  .1X/mac = IEEE802.1X/mac authentication,
  w/.1X/m = web/IEEE802.1X/mac authentication,
  DHCPSNP = DHCP snooping,
  linkdown = linkdown logout, TTL = web-authentication ttl filter,
  ld time = logout linkdown time,
  o = enable, x = disable
(1)
Type      C Port
            1       8 9
```

```
            +------+ +---
mac       1 ..oo..oo ....
802.1X    1 ......oo ....
web       1 oo....oo ....
gateway   1 ........ oo..
web/mac   1 ........ ....
web/.1X   1 ....oo.. ....
.1X/mac   1 ........ ....
w/.1X/m   1 ........ ....
DHCPSNP   1 ........ ....
roaming   1 oo...... ....
static    1 ........ ....
linkdown  1 xxxx.... ....
ld time   1 ....oooo ....
TTL       1 oo...... ....
```

項番	説明
(1)	ポートごとに、AccessDefender 設定の各機能の有効／無効を表示します。 mac：MAC 認証 802.1X：IEEE 802.1X 認証 web：Web 認証 gateway：ゲートウェイ認証 web/mac：Web/MAC 認証(AND) web/.1X：Web/IEEE 802.1X 認証(AND) .1X/mac：IEEE 802.1X/MAC 認証(AND) w/.1X/m：Web/IEEE 802.1X/MAC 認証(AND) DHCPSNP：DHCP スヌーピング roaming：ローミング機能 static：スタティック認証 linkdown：x 表示の場合、リンクダウンによるログアウトが無効 ld time：リンクダウン監視時間の設定 TTL：Web 認証の TTL フィルター機能 "C"列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。

9.1.25 show access-defender port-channel-configuration

show access-defender port-channel-configuration	
目的	ポートチャネルの AccessDefender 設定を表示します。
Command	show access-defender port-channel-configuration
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポートチャネルの AccessDefender 設定を表示する方法を示します。

```
# show access-defender port-channel-configuration
```

```
AccessDefender Port-channel Configuration:
  mac = mac-authentication, 802.1X = IEEE802.1X,
  web = web-authentication, gateway = web-authentication gateway,
  web/mac = web/mac authentication,
  web/.1X = web/IEEE802.1X authentication,
  .1X/mac = IEEE802.1X/mac authentication,
  w/.1X/m = web/IEEE802.1X/mac authentication,
  DHCPSNP = DHCP snooping,
  linkdown = linkdown logout, TTL = web-authentication ttl filter,
  ld time = logout linkdown time,
  o = enable, x = disable
(1)
Type      C Port-channel ID
            1       8 9     16 17    24 25    32 33    40 41    48
            +-------+ +------+ +------+ +------+ +------+ +------+
mac       1 oooooo.. ........ ........ ........ ........ ........
802.1X    1 ........ ........ ........ ........ ........ ........
web       1 oooooo.. ........ ........ ........ ........ ........
gateway   1 ........ ........ ........ ........ ........ ........
web/mac   1 ......o. ........ ........ ........ ........ ........
web/.1X   1 .......o ........ ........ ........ ........ ........
.1X/mac   1 ........ o....... ........ ........ ........ ........
w/.1X/m   1 ........ ........ ........ ........ ........ ........
DHCPSNP   1 ........ ........ ........ ........ ........ ........
roaming   1 ........ ........ ........ ........ ........ ........
static    1 ........ ........ ........ ........ ........ ........
linkdown  1 xxxxxx.. ........ ........ ........ ........ ........
ld time   1 ........ ........ ........ ........ ........ ........
TTL       1 oooooo.. ........ ........ ........ ........ ........
```

項番	説明
(1)	ポートチャネルごとに、AccessDefender 設定の各機能の有効／無効を表示します。 mac：MAC 認証 802.1X：IEEE 802.1X 認証 web：Web 認証 gateway：ゲートウェイ認証 web/mac：Web/MAC 認証(AND) web/.1X：Web/IEEE 802.1X 認証(AND) .1X/mac：IEEE 802.1X/MAC 認証(AND) w/.1X/m：Web/IEEE 802.1X/MAC 認証(AND) DHCPSNP：DHCP スヌーピング roaming：ローミング機能 static：スタティック認証 linkdown：x 表示の場合、リンクダウンによるログアウトが無効 ld time：リンクダウン監視時間の設定 TTL：Web 認証の TTL フィルター機能 "C"列はスタックのボックス ID を示しますが、本コマンドでは常に 1 が表示されます。

9.1.26 show access-defender rule-statistics

show access-defender rule-statistics	
目的	AccessDefender に関連するアクセスリストルールの使用状態を表示します。
Command	show access-defender rule-statistics

show access-defender rule-statistics	
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：AccessDefender に関連するアクセスリストルールの使用状態を表示する方法を示します。

```
# show access-defender rule-statistics

 Total Rules   :  768 ...(1)
 Unused Rules  :  767 ...(2)
 Used Rules    :    1 ...(3)              (4)     (5)
                                         Rule    Client
               ----------------------------------------
                web-authentication           1         1
                web-authentication gateway   0         0
                mac-authentication           0         0
                static-authentication        0         0
                IEEE802.1X                   0         0
                DHCPv4 snooping              0         0
                DHCPv6 snooping              0         0
               ----------------------------------------

 Total Discard Rules  :  200 ...(6)
 Unused Discard Rules :  199 ...(7)
 Used Discard Rules   :    1 ...(8)       (9)     (10)
                                         Rule    Client
               ----------------------------------------
                Discarded MAC address        1         1
               ----------------------------------------

 Total VFP Rules          :  512 ...(11)
 Unused VFP Rules         :  512 ...(12)
 Authorization VFP Rules  :    0 ...(13)
```

項番	説明
(1)	ルール数を表示します。
(2)	未使用のルール数を表示します。
(3)	使用済みルール数を表示します。
(4)	認証機能ごとのルール数を表示します。
(5)	認証機能ごとのクライアント数を表示します。
(6)	Discard クライアント用のルール数を表示します。
(7)	未使用の Discard クライアント用のルール数を表示します。
(8)	使用済みの Discard クライアント用のルール数を表示します。
(9)	MAC 認証に失敗して Discard 登録されたクライアント用のルール数を表示します。
(10)	MAC 認証に失敗して Discard 登録されたクライアント数を表示します。
(11)	VFP テーブルのルール数を表示します。
(12)	未使用の VFP ルール数を表示します。

項番	説明
(13)	認証済みの VFP ルール数を表示します。VFP ルールはクラス ID を使用すると消費します。

9.1.27 copy (AccessDefender)

copy (AccessDefender)	
目的	TFTP、SFTP、または SD カードを使用して、AccessDefender のシステムファイルをダウンロードまたはアップロードします。
Command	■ 装置へのダウンロード **copy** {**flash:** [URL] | **tftp:** [URL] | **sftp:** [URL]} SYSTEM-FILE ■ 装置からのアップロード **copy** SYSTEM-FILE {**flash:** [URL] | **tftp:** [URL] | **sftp:** [URL]}

Parameter	flash: [URL]：装置のローカルフラッシュまたは SD カードを使用する場合に指定します。URL は省略可能です。
	tftp: [URL]：TFTP を使用する場合に指定します。URL は省略可能です。
	sftp: [URL]：SFTP を使用する場合に指定します。URL は省略可能です。
	URL（省略可能）：ダウンロード元ファイル、またはアップロード先ファイルを指定します。省略可能ですが、指定した場合は、コマンド実行後の入力ダイアログがあらかじめ入力された状態になります。以下に入力書式例を示します。
	• flash: c:/FILE：装置のローカルフラッシュ上(c:)のファイルパス指定
	• flash: d:/FILE：SD カード上(d:)のファイルパス指定
	• tftp: //IP/FILE：TFTP サーバー上のファイルパス指定
	  • IP：TFTP サーバーの IP アドレス
	  • FILE：ファイルパス名
	• sftp: //USER:PASS@IP:TCP/FILE：SFTP サーバー上のファイルパス指定
	  • USER：ユーザー名
	  • PASS：パスワード
	  • IP：SFTP サーバーの IP アドレス
	  • TCP：TCP ポート番号、省略可能
	  • FILE：ファイルパス名
	SYSTEM-FILE：AccessDefender のシステムファイルを、以下のいずれかのパラメーターで指定します。
	• login-page：ログイン認証ページ
	• login-success-page：認証成功ページ
	• login-failure-page：認証失敗ページ
	• logout-success-page：ログアウト成功ページ
	• logout-failure-page：ログアウト失敗ページ
	• redirect-error-page：リダイレクト失敗ページ
	• aaa-local-db：AccessDefender のローカルデータベース
	• https-certificate：SSL サーバー証明書
	• https-private-key：SSL サーバーの秘密鍵
	• csr-certificate：CSR（証明書署名要求）
	• csr-private-key：CSR の秘密鍵
	• webpage-image01～webpage-image10：Web ページの画像 01～10

<table>
<tr><th colspan="2">copy (AccessDefender)</th></tr>
<tr><td>モード</td><td>特権実行モード</td></tr>
<tr><td>特権レベル</td><td>レベル：15</td></tr>
<tr><td>ガイドライン</td><td>
システムファイルには、Web 認証に使用する Web ページ、AccessDefender のローカルデータベースファイル、SSL サーバー証明書、SSL サーバーの秘密鍵、および Web ページで使用する画像ファイルが含まれます。

Web 認証に使用する Web ページでは、ダウンロード可能なファイルの最大サイズは、5KB（5,120 バイト）です。ダウンロードした Web ページを削除するには、access-defender erase コマンドを使用します。ダウンロードした Web ページが削除された場合は、デフォルトの Web ページを使用します。

Web 認証で使用する各ページの用途は以下のとおりです。
<table>
<tr><th>Web ページの種類</th><th>内容</th></tr>
<tr><td>ログイン認証ページ</td><td>ユーザー名、パスワードを入力する認証ページ</td></tr>
<tr><td>認証成功ページ</td><td>認証が成功したときに表示されるページ</td></tr>
<tr><td>認証失敗ページ</td><td>認証が失敗したときに表示されるページ</td></tr>
<tr><td>ログアウト成功ページ</td><td>ログアウトに成功したときに表示されるページ</td></tr>
<tr><td>ログアウト失敗ページ</td><td>ログアウトに失敗したときに表示されるページ</td></tr>
<tr><td>リダイレクト失敗ページ</td><td>リダイレクトに失敗したときに表示されるページ</td></tr>
</table>
AccessDefender のローカルデータベースのフォーマットは、以下のとおりです。ユーザー名、パスワード、VLAN ID、クラス ID の指定例を示します。
• CSV 形式（userid, password,[vid],[classid][,*]）
• userid および password は、最大 63 文字で指定します。
• 最大 3,000 行
<pre>
temp01,temp01,10
temp02,temp02
temp03,temp03,,30
00096b82c51e,1q2w3d,100,10
01010102,*@&foe2zgl6pwJiXjVe0+amVwAAAAC+RzmF,1002,1002,*
</pre>
AccessDefender のローカルデータベースファイル：
• ローカルデータベースに改行だけの行が含まれている場合は、ダウンロードできません。
• MAC 認証では、MAC アドレスをユーザー名として登録する必要があります。MAC アドレスの形式は mac-authentication username mac-format コマンドの設定に従います。
• ローカルデータベースの最終行に改行コードを入力してください。
• 重複するユーザー名を含むローカルデータベースはデバイスに保存できません。
• vid 未指定で classid のみを指定する場合は、上記の例の 3 行目のようにコンマ(,)を追加する必要があります。
• ファイルのエントリーのパスワード部分がパスワード暗号化機能により暗号化されている場合は、上記の例の 5 行目のようにエントリーの末尾にコンマおよびアスタリスク(,*)が追加されます。

SSL サーバー証明書と秘密鍵：
• 秘密鍵ファイルが暗号化されている場合は、パスフレーズを入力してください。対応している暗号化形式は DES/3DES/AES-128/AES-192/AES-256 で
</td></tr>
</table>

copy (AccessDefender)	
	す。 • 誤った秘密鍵がダウンロードされた場合は、パスフレーズを入力しても復号に失敗します。秘密鍵も有効になりません。 • 暗号化された秘密鍵ファイルをダウンロードする際にパスフレーズの入力を求められない場合は、事前にパスフレーズを解除してからダウンロードしてください。 • 中間証明書には、証明書チェーン（第三の証明書および第二の証明書を結合したもの）を使用してください。 • SSL サーバー証明書（https-certificate）と秘密鍵（https-private-key）は Privacy Enhanced Mail（PEM）形式で使用してください。 • ダウンロード済みの SSL サーバー証明書および秘密鍵が装置上に存在する場合、access-defender erase ssl-files コマンドで既存のファイルを削除してから証明書、秘密鍵をダウンロードしてください。 • SD カードブート利用時は、装置起動時に SD カードに保存された証明書を装置にダウンロードします。証明書、秘密鍵を変更する場合、access-defender erase ssl-files コマンドで既存の証明書、秘密鍵を削除してから新しい証明書、秘密鍵をダウンロードしてください。 • SSL サーバー証明書は 12KB（12,288 バイト）、秘密鍵は 2KB（2,048 バイト）のファイルサイズまでダウンロード可能です。 CSR（証明書署名要求）は装置からのアップロードのみ可能です。アップロード元に csr-certificate, csr-privatekey を指定して TFTP サーバーにアップロードできます。 Web ページで使用する画像ファイルは、1 ファイルにつき 1 メガバイト未満としてください。
制限・注意	• ファイル名には、&:;`'\"|*?~<>^()[]{}$ の各文字は使用できません。 • ファイル名には、「../」の文字列は使用できません。 • スラッシュ文字（/）は、ディレクトリーを識別するために使用します。 • デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在する TFTP サーバーを指定して本コマンドを実施する場合、宛先判定にはデフォルトルートよりもデフォルトゲートウェイ設定が優先され、宛先(1)(2)のいずれの場合も TFTP パケットはマネージメントポートから送信されます。 • 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク • 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク • VLAN インターフェース経由でのみ管理する場合は、送信元 IP アドレス設定(ip tftp source-interface)を VLAN インターフェース指定で設定することにより、このような状況でも宛先(1)への TFTP パケットが VLAN インターフェースから送信されるようになりますが、この設定をすると宛先(2)の場合も VLAN インターフェースから送信されるようになることに注意してください。 • Web 認証に使用する Web ページとして、UTF-16(BE、LE)、UTF-32(BE、LE)形式で保存された Web ページは正常に表示できませんので、使用しないでください。UTF-8、EUC-JP、Shift-JIS については動作確認済みのためこちらを使用してください。 • Web 認証が有効な状態では、SSL サーバー証明書と秘密鍵はダウンロードできませ

copy (AccessDefender)	
	ん。 • Web 認証に使用する Web ページまたは画像ファイルをダウンロードする際、ファイルサイズが仕様制限より大きくてダウンロードに失敗した場合のエラーメッセージは、"ERROR: Not a valid file." と表示されます。 • 本コマンドでは FTP サーバーの使用は未サポートです。
バージョン	1.08.02 1.13.01：sftp:パラメーター追加

使用例：TFTP サーバー(192.0.2.100)から、ファイル「custom-page.html」を認証成功ページ(login-success-page)としてダウンロードする方法を示します。

```
# copy tftp: login-success-page

Address of remote host []? 192.0.2.100
Source filename []? custom-page.html
Destination filename login-success-page? [y/n]:  y

 Accessing tftp://192.0.2.100/custom-page.html...
 Transmission start...
 Transmission finished, file length 1,336 bytes.
 Please wait, programming flash.............. Done.
```

使用例：SD カード(d:/)から、ファイル「custom-page.html」を認証成功ページ(login-success-page)としてコピーする方法を示します。

```
# copy flash: d:/custom-page.html login-success-page

Source filename [d:/custom-page.html]?
Destination filename login-success-page? [y/n]:  y

 Copy in progress............................ 100 %
```

使用例：TFTP サーバー(192.0.2.100)から、ファイル「local-db.txt」を AccessDefender のローカルデータベースファイル(aaa-local-db)としてダウンロードする方法を示します。

```
# copy tftp: //192.0.2.100/local-db.txt aaa-local-db

Address of remote host [192.0.2.100]?
Source filename [local-db.txt]?
Destination filename aaa-local-db? [y/n]:  y

 Accessing tftp://192.0.2.100/local-db.txt...
 Transmission start...
 Transmission finished, file length 259,973 bytes.
 Set aaa DB success.
```

使用例：SD カード(d:/)から、ファイル「local-db.txt」を AccessDefender のローカルデータベースファイル(aaa-local-db)としてコピーする方法を示します。

```
# copy flash: aaa-local-db

Source filename []? d:/local-db.txt
Destination filename aaa-local-db? [y/n]:  y

 Transmission start...
 Transmission finished, file length 259,973 bytes.
 Set aaa DB success.
```

使用例：TFTP サーバー(192.0.2.100)から、ファイル「key.prv」を SSL サーバーの秘密鍵(https-private-key)としてダウンロードする方法を示します。

```
# copy tftp: //192.0.2.100/key.prv https-private-key

Address of remote host [192.0.2.100]?
Source filename [key.prv]?
Destination filename https-privatekey? [y/n]:  y

% Importing private key PEM file...
Reading file from tftp://192.0.2.100/key.prv
Loading key.prv from 192.0.2.100 (via Port1/0/24):!
[OK - 1675 bytes]
```

使用例：TFTP サーバー(192.0.2.100)から、ファイル「cert.crt」を SSL サーバー証明書(https-certificate)としてダウンロードする方法を示します。

```
# copy tftp: https-certificate

Address of remote host []? 192.0.2.100
Source filename []? cert.crt
Destination filename https-certificate? [y/n]:  y

% Importing certificate PEM file...
Reading file from tftp://192.0.2.100/cert.crt
Loading cert.crt from 192.0.2.100 (via Port1/0/24):!
[OK - 1403 bytes]
```

使用例：AccessDefender のローカルデータベースファイル(aaa-local-db)を、TFTP サーバー(192.0.2.100)にファイル名「local-db.txt」でアップロードする方法を示します。

```
# copy aaa-local-db tftp: //192.0.2.100/local-db.txt

Address of remote host [192.0.2.100]?
Destination filename [local-db.txt]?

 Uploading aaa-local-db to tftp://192.0.2.100/local-db.txt...
 Transmission start...
 Transmission finished, file length 259,973 bytes.
```

9.1.28 access-defender deny

access-defender deny	
目的	認証を一時的に拒否するクライアントを登録します。登録を削除する場合は、no access-defender deny コマンドを使用します。
Command	access-defender deny {ip IP-ADDRESS | mac MAC-ADDRESS} timer MINUTES no access-defender deny {ip IP-ADDRESS | mac MAC-ADDRESS}
Parameter	ip IP-ADDRESS：認証を一時的に拒否するクライアントの IPv4 アドレスを指定します。 mac MAC-ADDRESS：認証を一時的に拒否するクライアントの MAC アドレスを、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式 (例：XX-XX-XX-XX-XX-XX) • 1 バイトごとにコロン区切り形式 (例：XX:XX:XX:XX:XX:XX) • 2 バイトごとにドット区切り形式 (例：XXXX.XXXX.XXXX)

access-defender deny	
	• 区切り文字を使用しない形式（例：XXXXXXXXXXXX） timer MINUTE：認証を一時的に拒否する時間を、1～60 分の範囲で指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	認証拒否クライアントとして登録された場合は、登録中は認証が拒否されます。 認証を一時的に拒否するクライアントの登録可能数は、total-client コマンドの deny-client パラメーターで設定します。
制限・注意	• スタック機能と併用時にマスターの切り替わりが発生した場合、本コマンドで登録した認証拒否クライアントの情報は削除されます。 • 認証済みクライアントを認証拒否クライアントとして登録しても、そのクライアントからの通信は可能です。
バージョン	1.08.02

使用例：IPv4 アドレスが 10.0.0.1 のクライアントからの認証を 10 分間拒否する方法を示します。

```
# access-defender deny ip 10.0.0.1 timer 10
#
```

9.1.29 access-defender erase

access-defender erase	
目的	AccessDefender のシステムファイルを削除します。
Command	access-defender erase [SYSTEM-FILE]
Parameter	SYSTEM-FILE（省略可能）：削除する AccessDefender のシステムファイルを、以下のパラメーターで指定します。 • login-page：ログイン認証ページ • login-success-page：認証成功ページ • login-failure-page：認証失敗ページ • logout-success-page：ログアウト成功ページ • logout-failure-page：ログアウト失敗ページ • redirect-error-page：リダイレクト失敗ページ • aaa-local-db：AccessDefender のローカルデータベース • ssl-files：SSL サーバー証明書、秘密鍵、および ssl gencsr rsakey コマンドで作成したファイル • webpage-image01～webpage-image10：Web ページの画像 01～10
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	削除するシステムファイルを指定しない場合は、AccessDefender に関連するすべてのシステムファイルが削除されます。システムファイルが削除された場合は、デフォルト設定に戻ります。
制限・注意	• Web 認証が有効な状態では、SSL サーバー証明書と秘密鍵は削除できません。 • 削除するシステムファイルを指定しない場合は、Web アクセス拒否通知用のカスタム Web ページも削除されます。
バージョン	1.08.02

使用例：認証成功ページを削除してデフォルト設定に戻す方法を示します。

```
# access-defender erase login-success-page
Erasing Web authentication login-success-page in FLASH..... Done.
```

使用例：すべてのシステムファイルを削除してデフォルト設定に戻す方法を示します。

```
# access-defender erase
Erasing Web authentication login-page in FLASH..... Done.
Erasing Web authentication login-success-page in FLASH..... Done.
Erasing Web authentication login-failure-page in FLASH..... Done.
Erasing Web authentication logout-success-page in FLASH..... Done.
Erasing Web authentication logout-failure-page in FLASH..... Done.
Erasing Web authentication redirect-error-page in FLASH..... Done.
Erasing web-access-deny-page in FLASH..... Done.
Erasing Access Defender local database settings..... Done.
Erasing SSL files in FLASH..... Done.
Erasing Web authentication webpage-image01 in FLASH..... Done.
Erasing Web authentication webpage-image02 in FLASH..... Done.
Erasing Web authentication webpage-image03 in FLASH..... Done.
Erasing Web authentication webpage-image04 in FLASH..... Done.
Erasing Web authentication webpage-image05 in FLASH..... Done.
Erasing Web authentication webpage-image06 in FLASH..... Done.
Erasing Web authentication webpage-image07 in FLASH..... Done.
Erasing Web authentication webpage-image08 in FLASH..... Done.
Erasing Web authentication webpage-image09 in FLASH..... Done.
Erasing Web authentication webpage-image10 in FLASH..... Done.
```

9.1.30 access-defender logout

access-defender logout	
目的	認証済みのクライアントを手動で強制的にログアウトします。または Discard 登録されたクライアントを手動で削除します。
Command	access-defender logout {ip IP-ADDRESS | mac MAC-ADDRESS | user NAME}
Parameter	ip IP-ADDRESS：強制的にログアウトする認証済みクライアントの IPv4 アドレスを指定します。 mac MAC-ADDRESS：強制的にログアウトする認証済みクライアントの MAC アドレス、または手動で削除する Discard 登録されたクライアントの MAC アドレスを、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX） user NAME：強制的にログアウトする認証済みクライアントのユーザー名を指定します。または、手動で削除する Discard 登録されたクライアントのユーザー名を指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：IPv4 アドレスが 10.0.0.1 の認証済みクライアントを強制的にログアウトする方法を示します。

```
# access-defender logout ip 10.0.0.1
#
```

使用例：MAC アドレスが 00:00:00:10:00:77 の認証済みクライアントを強制的にログアウトする方法を示します。

```
# access-defender logout mac 00:00:00:10:00:77
#
```

使用例：ユーザー名が「web-user」の認証済みクライアントを強制的にログアウトする方法を示します。

```
# access-defender logout user web-user
#
```

9.1.31 RADIUS 属性に関する情報

RADIUS サーバーへ送信する認証要求に含まれる RADIUS 属性については、以下コマンドのガイドラインを参照してください。

- MAC 認証の場合：aaa authentication mac-auth コマンド
- IEEE 802.1X 認証の場合：aaa authentication dot1x コマンド
- Web 認証の場合：aaa authentication web-auth コマンド

認証成功後に動的に VLAN を変更する場合やクラス ID を割り当てる場合は、認証成功時に ApresiaNP シリーズに引き渡す VLAN ID およびクラス ID を、あらかじめ RADIUS サーバーに登録しておく必要があります。VLAN ID およびクラス ID として登録するベンダー独自属性（Vendor Specific Attribute）を以下に示します。

属性	属性値	動的な VLAN 変更の設定値	クラス ID 割り当ての設定値
Vendor-Specific	ベンダーID	278	278
	ベンダー属性番号	192 ※1	193
	値	割り当てる VLAN ID	割り当てるクラス ID
	属性の型	整数（INTEGER）	整数（INTEGER）

- ※1：ベンダー独自属性による動的な VLAN 変更は、MAC 認証と Web 認証でのみサポートしています。IEEE 802.1X 認証の場合は Tunnel-Private-Group-Id を使用してください。

MAC 認証、Web 認証、および IEEE 802.1X 認証において、Tunnel-Private-Group-Id により動的に VLAN を変更する機能をサポートしています。認証成功後に動的に VLAN を変更する場合は、認証成功時に ApresiaNP シリーズに引き渡す VLAN ID または VLAN 名称を、あらかじめ RADIUS サーバーに登録しておく必要があります。RADIUS サーバーに登録する属性を以下に示します。

属性	属性値	設定値	備考
Tunnel-Type	使用するトンネリングプロトコル	13（VLAN）	固定
Tunnel-Medium-Type	データ転送媒体のプロトコル	6（IEEE 802）	固定
Tunnel-Private-Group-Id	トンネルが属するグループ ID	割り当てる VLAN ID または VLAN 名称	変更可能

9.2 認証、許可、アカウンティング(AAA)コマンド

認証、許可、アカウンティング(AAA)関連の設定コマンドは以下のとおりです。

- aaa new-model
- radius-server host
- radius-server deadtime
- tacacs-server host
- ip radius source-interface
- ip tacacs source-interface
- ipv6 radius source-interface
- aaa group server radius
- server (RADIUS)
- aaa group server tacacs+
- server (TACACS+)
- aaa authentication login
- login authentication
- aaa authentication enable
- aaa authentication mac-auth
- aaa authentication dot1x
- aaa authentication web-auth
- aaa authentication control sufficient
- aaa default class
- aaa accounting system
- aaa accounting network
- aaa accounting commands
- accounting commands
- aaa accounting exec
- accounting exec

認証、許可、アカウンティング(AAA)関連の show／操作コマンドは以下のとおりです。

- show aaa
- show radius statistics
- show tacacs statistics
- clear aaa counters servers

9.2.1 aaa new-model

aaa new-model	
目的	認証またはアカウンティングのための AAA 機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	aaa new-model no aaa new-model
Parameter	なし
デフォルト	無効
モード	グローバル設定モード

aaa new-model	
特権レベル	レベル：15
ガイドライン	AAA 機能を有効にすると、各ラインセッション(コンソール、Telnet、SSH)へのログイン方法は以下のコマンドによって決定されます。デフォルト設定の場合は、ログイン認証方式が「username コマンドで作成したユーザーアカウント」になります。 • aaa authentication login • login authentication AAA 機能が無効な場合の各ラインセッション(コンソール、Telnet、SSH)へのログイン方法については、login (Line)コマンドを参照してください。 AAA 機能を有効にすると、enable パスワードの認証方式は以下のコマンドによって決定されます。デフォルト設定の場合は、認証方式が「enable password コマンドで設定したパスワード」になります。 • aaa authentication enable
制限・注意	• AAA 機能が有効、ログイン認証方式がデフォルト設定、かつ「username コマンドで作成したユーザーアカウント」設定がまだない状態では、コンソールの場合のみ「ユーザー名／パスワードを未入力で Enter 実施、または任意の文字列を入力して Enter 実施」でログインできます。 • AAA 機能が有効、enable パスワードの認証方式がデフォルト設定、かつ enable password コマンドがまだ未設定の状態では、コンソールの場合のみ「enable パスワードを未入力で Enter 実施、または任意の文字列を入力して Enter 実施」で特権レベル 15 に遷移できます。
バージョン	1.08.02

使用例：AAA 機能を有効にする方法を示します。

```
# configure terminal
(config)# aaa new-model
(config)#
```

9.2.2 radius-server host

radius-server host	
目的	RADIUS サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	radius-server host {IP-ADDRESS | IPV6-ADDRESS} [auth-port UDP-PORT] [acct-port UDP-PORT] [timeout SECONDS] [retransmit VALUE] key [0 | 7] KEY-STRING no radius-server host {IP-ADDRESS | IPV6-ADDRESS}
Parameter	IP-ADDRESS：RADIUS サーバーの IPv4 アドレスを指定します。 IPV6-ADDRESS：RADIUS サーバーの IPv6 アドレスを指定します。 auth-port UDP-PORT（省略可能）：認証で使用する UDP ポート番号を 1～65535 の範囲で指定します。デフォルト設定は 1812 です。 acct-port UDP-PORT（省略可能）：アカウンティングで使用する UDP ポート番号を 1～65535 の範囲で指定します。デフォルト設定は 1813 です。 timeout SECONDS（省略可能）：応答タイムアウト時間を 1～255 秒の範囲で指定します。デフォルト設定は 5 秒です。

radius-server host	
	retransmit VALUE（省略可能）：サーバーから応答がない場合のリクエスト再送回数を、0～20 回の範囲で指定します。デフォルト設定は 2 回です。 key [0 | 7] KEY-STRING：サーバーとの通信に使用する共有鍵（Shared Secret）を指定します。 • [0 | 7]（省略可能）：後に続く共有鍵（Shared Secret）の文字列の形式を明示する場合に指定します。0 の場合は平文を、7 の場合は暗号化された形式を意味します。省略した場合は、平文で入力します。 • KEY-STRING：平文で入力する場合は、共有鍵（Shared Secret）を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? を除いた文字を使用可能です。
デフォルト	RADIUS サーバーの設定なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	設定した RADIUS サーバーは、デフォルトの RADIUS サーバーグループ「radius」に登録されます。また、aaa group server radius コマンドで作成した任意の RADIUS サーバーグループに server コマンドで登録することもできます。 以下の条件をすべて満たす環境の場合、 • RADIUS サーバー(IPv4)が、自装置に直接接続されているネットワーク以外の、ユーザーポート経由で到達可能（VLAN インターフェースに設定した IPv4 アドレスからアクセス可能）なネットワークに存在する。 • RADIUS サーバー(IPv4)への経路が、デフォルトルート情報(0.0.0.0/0)によって解決される。 • マネージメントポートのデフォルトゲートウェイ設定（ip default-gateway）を併用している。 以下のいずれかの設定が必要になります。 • ip radius source-interface service user-account encryption でパスワード暗号化機能を有効にすると、共有鍵（Shared Secret）が暗号化されます。
制限・注意	• RADIUS サーバー（radius-server host）と TACACS+サーバー（tacacs-server host）は、合わせて最大 16 個まで設定できます。 • radius-server host コマンドの設定順序を変更する場合には、すべての radius-server host コマンドの設定を削除してから、優先する RADIUS サーバーから順番に再設定してください。 • auth-port パラメーターをデフォルト値(1812)以外に指定する場合、acct-port パラメーターをデフォルト値(1813)以外に指定する場合は、以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 161(snmp), 162(snmptrap), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • ip ssh service-port • snmp-server service-port

radius-server host	
	• snmp-server host • web-authentication http-port • web-authentication https-port • web-authentication redirect proxy-port • web-authentication snooping proxy-port • web-deny-notify http-port • web-deny-notify https-port • tacacs-server host • 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。 • MAC 認証において、本コマンドの timeout と retransmit の設定値を掛け合わせた値が 400 秒以上となる設定を行い、かつ、RADIUS サーバーへの問い合わせの応答待ち時間が 400 秒以上となった場合、MAC 認証処理を打ち切り、MAC 認証用のデータベース (MacAuthDB) も削除されます。そのため、以後の当該認証処理に関係するログは出力されず、Discard 状態の端末としても登録されません。
バージョン	1.08.02

使用例：「IPv4 アドレス=192.0.2.100、共有鍵（Shared Secret）：testtest」で、RADIUS サーバーを設定する方法を示します。

```
# configure terminal
(config)# radius-server host 192.0.2.100 key testtest
(config)#
```

9.2.3 radius-server deadtime

radius-server deadtime	
目的	問い合わせした RADIUS サーバーから応答がない場合に、その RADIUS サーバーをオフラインとみなす期間 (デッドタイム) を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	radius-server deadtime MINUTES no radius-server deadtime
Parameter	MINUTES：RADIUS サーバーのデッドタイムを 0～1,440 分(24 時間)の範囲で指定します。
デフォルト	0 分
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	デフォルト設定(0 分)の場合は、RADIUS サーバーから応答がない場合でも、その RADIUS サーバーをオフラインとみなしません。 デッドタイムを設定して応答のない RADIUS サーバーでの認証をキャンセルすることで、認証処理に要する時間を低減できます。システムが認証サーバーによる認証を実行するときは、1 回で 1 つのサーバーに対して認証を試みます。認証を試みたサーバーから応答がない場合、システムは次のサーバーに対して認証を試行します。応答のないサーバーをシステムが発見すると、サーバーがダウンしているとみなし、デッドタイムタイマーが開始され、応答のないサーバーに対してデッドタイムが満了するまで認証のためのリクエストをキャンセルします。

radius-server deadtime	
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：デッドタイムを 10 分に設定する方法を示します。

```
# configure terminal
(config)# radius-server deadtime 10
(config)#
```

9.2.4 tacacs-server host

tacacs-server host	
目的	TACACS+サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	tacacs-server host IP-ADDRESS [port TCP-PORT] [timeout SECONDS] key [0 | 7] KEY-STRING no tacacs-server host IP-ADDRESS
Parameter	IP-ADDRESS：TACACS+サーバーの IPv4 アドレスを指定します。 port TCP-PORT（省略可能）：TACACS+サーバーとの通信で使用する TCP ポート番号を 1～65535 の範囲で指定します。デフォルト設定は 49 です。 timeout SECONDS（省略可能）：応答タイムアウト時間を 1～255 秒の範囲で指定します。デフォルト設定は 5 秒です。 key [0 | 7] KEY-STRING：サーバーとの通信に使用する共有鍵（Shared Secret）を指定します。 • [0 | 7]（省略可能）：後に続く共有鍵（Shared Secret）の文字列の形式を明示する場合に指定します。0 の場合は平文を、7 の場合は暗号化された形式を意味します。省略した場合は、平文で入力します。 • KEY-STRING：平文で入力する場合は、共有鍵（Shared Secret）を最大 254 文字で指定します。ASCII コードの印字可能な文字のうち、? を除いた文字を使用可能です。
デフォルト	TACACS+サーバーの設定なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	設定した TACACS+サーバーは、デフォルトの TACACS+サーバーグループ「tacacs+」に登録されます。また、aaa group server tacacs コマンドで作成した任意の TACACS+サーバーグループに server コマンドで登録することもできます。 以下の条件をすべて満たす環境の場合、 • TACACS+サーバーが、自装置に直接接続されているネットワーク以外の、ユーザーポート経由で到達可能（VLAN インターフェースに設定した IPv4 アドレスからアクセス可能）なネットワークに存在する。 • TACACS+サーバーへの経路が、デフォルトルート情報(0.0.0.0/0)によって解決される。 • マネージメントポートのデフォルトゲートウェイ設定（ip default-gateway）を併用している。 以下のいずれかの設定が必要になります。

tacacs-server host	
	• ip tacacs source-interface service user-account encryption でパスワード暗号化機能を有効にすると、共有鍵(Shared Secret)が暗号化されます。
制限・注意	• RADIUS サーバー(radius-server host)と TACACS+サーバー(tacacs-server host)は、合わせて最大 16 個まで設定できます。 • port パラメーターをデフォルト値(49)以外に指定する場合は、以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 23(telnet), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 161(snmp), 162(snmptrap), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • ip ssh service-port • snmp-server service-port • snmp-server host • web-authentication http-port • web-authentication https-port • web-authentication redirect proxy-port • web-authentication snooping proxy-port • web-deny-notify http-port • web-deny-notify https-port • radius-server host • 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例:「IPv4 アドレス=192.0.2.100、共有鍵(Shared Secret):testtest」で、TACACS+サーバーを設定する方法を示します。

```
# configure terminal
(config)# tacacs-server host 192.0.2.100 key testtest
(config)#
```

9.2.5 ip radius source-interface

ip radius source-interface	
目的	RADIUS パケットの送信元 IPv4 アドレスとして使用するインターフェースを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip radius source-interface IF-ID no ip radius source-interface
Parameter	IF-ID:インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>:VLAN インターフェース指定
デフォルト	最も近いインターフェースの IPv4 アドレスを使用
モード	グローバル設定モード、RADIUS サーバーグループ設定モード

ip radius source-interface	
特権レベル	レベル：15
ガイドライン	グローバル設定モードと RADIUS サーバーグループ設定モードの両方で送信元インターフェースを指定した場合、RADIUS サーバーグループ設定モードでの設定が優先されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：グローバル設定モードで、RADIUS パケットの送信元 IPv4 アドレスとして、VLAN 1 インターフェースの IPv4 アドレスを設定する方法を示します。

```
# configure terminal
(config)# ip radius source-interface vlan 1
(config)#
```

9.2.6 ip tacacs source-interface

ip tacacs source-interface	
目的	TACACS+パケットの送信元 IPv4 アドレスとして使用するインターフェースを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ip tacacs source-interface IF-ID no ip tacacs source-interface
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定
デフォルト	最も近いインターフェースの IPv4 アドレスを使用
モード	グローバル設定モード、TACACS+サーバーグループ設定モード
特権レベル	レベル：15
ガイドライン	グローバル設定モードと TACACS+サーバーグループ設定モードの両方で送信元インターフェースを指定した場合、TACACS+サーバーグループ設定モードでの設定が優先されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：グローバル設定モードで、TACACS+パケットの送信元 IPv4 アドレスとして、VLAN 1 インターフェースの IPv4 アドレスを設定する方法を示します。

```
# configure terminal
(config)# ip tacacs source-interface vlan 1
(config)#
```

9.2.7 ipv6 radius source-interface

ipv6 radius source-interface	
目的	RADIUS パケットの送信元 IPv6 アドレスとして使用するインターフェースを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	ipv6 radius source-interface IF-ID no ipv6 radius source-interface

ipv6 radius source-interface	
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定
デフォルト	最も近いインターフェースの IPv6 アドレスを使用
モード	グローバル設定モード、RADIUS サーバーグループ設定モード
特権レベル	レベル：15
ガイドライン	グローバル設定モードと RADIUS サーバーグループ設定モードの両方で送信元インターフェースを指定した場合、RADIUS サーバーグループ設定モードでの設定が優先されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：グローバル設定モードで、RADIUS パケットの送信元 IPv6 アドレスとして、VLAN 1 インターフェースの IPv6 アドレスを設定する方法を示します。

```
# configure terminal
(config)# ipv6 radius source-interface vlan 1
(config)#
```

9.2.8 aaa group server radius

aaa group server radius	
目的	RADIUS サーバーグループを設定します。また、RADIUS サーバーグループ設定モードに遷移します。遷移後のプロンプトは（config-sg-radius)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	aaa group server radius NAME no aaa group server radius NAME
Parameter	NAME：サーバーグループ名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	RADIUS サーバーグループの設定なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	aaa authentication コマンドの認証方式リスト、または aaa accounting コマンドのアカウンティング方式リストで使用する RADIUS サーバーグループを作成します。サーバーグループは aaa group server radius コマンドと aaa group server tacacs+ コマンドで合わせて最大 8 グループまで作成できます。なお、8 グループには 2 つのデフォルトのサーバーグループ「radius」「tacacs+」も含まれます。 サーバーグループ名「radius」は、デフォルトの RADIUS サーバーグループとして予約されています。「radius」サーバーグループは、radius-server host コマンドで作成したすべての RADIUS サーバーを対象として、設定した順に処理されます。 本コマンドで作成した RADIUS サーバーグループには、server コマンドを使用して RADIUS サーバーを登録できます。1 つの RADIUS サーバーグループには最大 16 個の RADIUS サーバーを登録でき、設定した順に処理されます。 複数の RADIUS サーバーが対象になる場合には、先頭の RADIUS サーバーから処理が実施されます。タイムアウト等で処理がエラーになった場合には、次に登録されて

aaa group server radius	
	いる RADIUS サーバーで処理が実施されます。 aaa authentication コマンドの認証方式リストとして使用するケースにおいて、RADIUS サーバーから認証拒否応答を受信して認証失敗になった場合には、次に登録されている RADIUS サーバーが存在してもそのサーバーで認証は実施されません。ただし、aaa authentication control sufficient コマンドが有効に設定されている場合には、認証失敗になった場合でも次に登録されている RADIUS サーバーで認証が実施されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：RADIUS サーバーグループの作成方法、および作成した RADIUS サーバーグループに RADIUS サーバーを登録する方法を示します。

```
# configure terminal
(config)# aaa group server radius group1
(config-sg-radius)# server 172.19.10.100
(config-sg-radius)#
```

9.2.9 server (RADIUS)

server (RADIUS)	
目的	RADIUS サーバーグループに RADIUS サーバーを登録するコマンドです。設定を削除する場合は、no 形式のコマンドを使用します。
Command	server {IP-ADDRESS | IPV6-ADDRESS} no server {IP-ADDRESS| IPV6-ADDRESS}
Parameter	IP-ADDRESS：RADIUS サーバーグループに登録する RADIUS サーバーの IPv4 アドレスを指定します。 IPV6-ADDRESS：RADIUS サーバーグループに登録する RADIUS サーバーの IPv6 アドレスを指定します。
デフォルト	RADIUS サーバーグループに RADIUS サーバーの登録なし
モード	RADIUS サーバーグループ設定モード
特権レベル	レベル：15
ガイドライン	aaa group server radius コマンドで RADIUS サーバーグループ設定モードに遷移し、server コマンドで RADIUS サーバーグループに RADIUS サーバーを登録します。RADIUS サーバーグループは、aaa authentication コマンドの認証方式リスト、または aaa accounting コマンドのアカウンティング方式リストで使用するサーバーグループとして指定できます。 RADIUS サーバーグループに登録した RADIUS サーバーは、登録した順に処理されます。 1 つの RADIUS サーバーグループには、最大 16 個の RADIUS サーバーを登録できます。
制限・注意	事前に radius-server host コマンドで RADIUS サーバーを作成してください。RADIUS サーバーは IP アドレスで識別されます。
バージョン	-
目的	1.08.02

使用例：2 つの RADIUS サーバーを作成し、RADIUS サーバーグループ「group1」に登録する方法を説明します。

```
# configure terminal
(config)# radius-server host 172.19.10.100 auth-port 1500 timeout 8 retransmit 3 key
ABCDE
(config)# radius-server host 172.19.10.101 auth-port 1600 timeout 3 retransmit 1 key
ABCDE
(config)# aaa group server radius group1
(config-sg-radius)# server 172.19.10.100
(config-sg-radius)# server 172.19.10.101
(config-sg-radius)#
```

9.2.10 aaa group server tacacs+

aaa group server tacacs+	
目的	TACACS+サーバーグループを設定します。また、TACACS+サーバーグループ設定モードに遷移します。遷移後のプロンプトは（config-sg-tacacs+)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
Command	aaa group server tacacs+ NAME no aaa group server tacacs+ NAME
Parameter	NAME：サーバーグループ名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。
デフォルト	TACACS+サーバーグループの設定なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	aaa authentication コマンドの認証方式リスト、または aaa accounting コマンドのアカウンティング方式リストで使用する TACACS+サーバーグループを作成します。サーバーグループは aaa group server radius コマンドと aaa group server tacacs+ コマンドで合わせて最大 8 グループまで作成できます。なお、8 グループには 2 つのデフォルトのサーバーグループ「radius」「tacacs+」も含まれます。 サーバーグループ名「tacacs+」は、デフォルトの TACACS+サーバーグループとして予約されています。「tacacs+」サーバーグループは、tacacs-server host コマンドで作成したすべての TACACS+サーバーを対象として、設定した順に処理されます。 本コマンドで作成した TACACS+サーバーグループには、server コマンドを使用して TACACS+サーバーを登録できます。1 つの TACACS+サーバーグループには最大 16 個の TACACS+サーバーを登録でき、設定した順に処理されます。 複数の TACACS+サーバーが対象になる場合には、先頭の TACACS+サーバーから処理が実施されます。タイムアウト等で処理がエラーになった場合には、次に登録されている TACACS+サーバーで処理が実施されます。 aaa authentication コマンドの認証方式リストとして使用するケースにおいて、TACACS+サーバーから認証拒否応答を受信して認証失敗になった場合には、次に登録されている TACACS+サーバーが存在してもそのサーバーで認証は実施されません。ただし、aaa authentication control sufficient コマンドが有効に設定されている場合には、認証失敗になった場合でも次に登録されている TACACS+サーバーで認証が実施されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。

aaa group server tacacs+	
バージョン	1.08.02

使用例：TACACS+サーバーグループの作成方法、および作成した TACACS+サーバーグループに TACACS+サーバーを登録する方法を示します。

```
# configure terminal
(config)# aaa group server tacacs+ group1
(config-sg-tacacs+)# server 172.19.10.100
(config-sg-tacacs+)# server 172.19.11.20
(config-sg-tacacs+)#
```

9.2.11 server (TACACS+)

server (TACACS+)	
目的	TACACS+サーバーグループに TACACS+サーバーを登録するコマンドです。設定を削除する場合は、no 形式のコマンドを使用します。
Command	server IP-ADDRESS no server IP-ADDRESS
Parameter	IP-ADDRESS：TACACS+サーバーグループに登録する TACACS+サーバーの IPv4 アドレスを指定します。
デフォルト	TACACS+サーバーグループに TACACS+サーバーの登録なし
モード	TACACS+サーバーグループ設定モード
特権レベル	レベル：15
ガイドライン	aaa group server tacacs+コマンドで TACACS+サーバーグループ設定モードに遷移し、server コマンドで TACACS+サーバーグループに TACACS+サーバーを登録します。TACACS+サーバーグループは、aaa authentication コマンドの認証方式リスト、または aaa accounting コマンドのアカウンティング方式リストで使用するサーバーグループとして指定できます。 TACACS+サーバーグループに登録した TACACS+サーバーは、登録した順に処理されます。 1 つの TACACS+サーバーグループには、最大 16 個の TACACS+サーバーを登録できます。
制限・注意	• 事前に tacacs-server host コマンドで TACACS+サーバーを作成してください。 TACACS+サーバーは IP アドレスで識別されます。
バージョン	1.08.02

使用例：2 つの TACACS+サーバーを作成し、TACACS+サーバーグループ「group2」に登録する方法を説明します。

```
# configure terminal
(config)# tacacs-server host 172.19.10.100 port 1500 timeout 8 key ABCDE
(config)# tacacs-server host 172.19.122.3 port 1600 timeout 3 key ABCDE
(config)# aaa group server tacacs+ group2
(config-sg-tacacs+)# server 172.19.10.100
(config-sg-tacacs+)# server 172.19.122.3
(config-sg-tacacs+)#
```

9.2.12 aaa authentication login

aaa authentication login	
目的	ログイン認証で使用する認証方式リストを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	aaa authentication login {default | LIST-NAME} METHOD1 [METHOD2...] no aaa authentication login {default | LIST-NAME}
Parameter	default：デフォルトの認証方式リストを使用する場合に指定します。 LIST-NAME：デフォルト以外の認証方式リストを使用する場合に、認証方式リスト名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字を除いた文字を使用可能です。 METHOD1 [METHOD2...]：ここで指定した順序で試行される認証方式のリストを、以下のパラメーターを指定します。認証方式は少なくとも 1 つは指定する必要があり、最大で 4 つまで指定できます。 • local：username コマンドで作成したユーザーアカウント • group radius：デフォルトの RADIUS サーバーグループ「radius」 • group tacacs+：デフォルトの TACACS+サーバーグループ「tacacs+」 • group NAME：aaa group server コマンドで設定したサーバーグループ • none：認証なしで許可
デフォルト	local
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはログイン認証で使用する認証方式リストを設定します。本コマンド以外に login authentication コマンドの設定も必要です。 本コマンドで認証方式リストを設定しない場合は、username コマンドで作成したユーザーアカウントで認証されます。 none パラメーターは、先に処理された認証方式で明示的に判定されなかった場合でも、認証なしで許可できるようにすることを想定しています。そのため、通常は認証方式の最後に指定します。 複数の認証方式が指定されている場合には、先頭の認証方式から処理が実施されます。タイムアウト等で処理がエラーになり明示的に許可もしくは拒否が判定されなかった場合には、次に登録されている認証方式で処理が実施されます。 明示的に認証拒否と判定されて認証失敗になった場合には、次に登録されている認証方式が存在してもその認証方式では実施されません。ただし、aaa authentication control sufficient login コマンドが有効に設定されている場合には、認証失敗になった場合でも次に登録されている認証方式で認証が実施されます。 aaa authentication control sufficient login コマンドを有効に設定している場合でも、他の認証方式で明示的に認証拒否と判定されて認証失敗になった場合には、認証なし(none)では認証が許可されません。 認証方式として指定したサーバーグループが存在しない場合は、そのサーバーグループは処理対象から外されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：ログイン認証で使用する認証方式リストを設定する方法を示します。認証方式としてサーバーグループ「group2」と local を指定しています。

```
# configure terminal
(config)# aaa authentication login default group group2 local
(config)#
```

9.2.13 login authentication

login authentication	
目的	ラインでのログイン認証に使用する認証方式リストを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	login authentication {default | LIST-NAME} no login authentication
Parameter	default：デフォルトの認証方式リストで認証する場合に指定します。 LIST-NAME：使用する認証方式リストの名前を指定します。
デフォルト	デフォルトの認証方式リストを認証に使用
モード	ライン設定モード
特権レベル	レベル：15
ガイドライン	最初に aaa authentication login コマンドで認証方式リストを作成します。 認証方式リストが存在しない場合、コマンドは無効になり、デフォルトのログイン認証方式リストで認証が行われます。
制限・注意	• 本設定は構成情報ではアクセス管理関連（ラベル# PRIVMGMT）で表示されます。 • 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：ローカルコンソールラインでのログイン認証に使用する認証方式リストとして、「CONSOLE-LINE-METHOD」を設定する方法を示します。

```
# configure terminal
(config)# aaa authentication login CONSOLE-LINE-METHOD group group2 local
(config)# line console
(config-line)# login authentication CONSOLE-LINE-METHOD
(config-line)#
```

9.2.14 aaa authentication enable

aaa authentication enable	
目的	enable パスワードの認証で使用する認証方式リストを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	aaa authentication enable default METHOD1 [METHOD2...] no aaa authentication enable default
Parameter	METHOD1 [METHOD2...]：ここで指定した順序で試行される認証方式のリストを、以下のパラメーターを指定します。認証方式は少なくとも 1 つは指定する必要があり、最大で 4 つまで指定できます。 • enable：enable password コマンドで設定したパスワード

aaa authentication enable	
	• group radius：デフォルトの RADIUS サーバーグループ「radius」 • group tacacs+：デフォルトの TACACS+サーバーグループ「tacacs+」 • group NAME：aaa group server コマンドで設定したサーバーグループ • none：認証なしで許可
デフォルト	enable
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	本コマンドは enable［PRIVILEGE-LEVEL］コマンドを実行した際に、特権レベルへのアクセスを判定するために使用する認証方式リストを設定します。認証方式として RADIUS サーバーを使用する場合には、"enable12"または"enable15"のような特権レベルに基づいたユーザー名で認証が行われます。 本コマンドで認証方式リストを設定しない場合は、enable password コマンドで設定したパスワードで認証されます。 none パラメーターは、先に処理された認証方式で明示的に判定されなかった場合でも、認証なしで許可できるようにすることを想定しています。そのため、通常は認証方式の最後に指定します。 複数の認証方式が指定されている場合には、先頭の認証方式から処理が実施されます。タイムアウト等で処理がエラーになり明示的に許可もしくは拒否が判定されなかった場合には、次に登録されている認証方式で処理が実施されます。 明示的に認証拒否と判定されて認証失敗になった場合には、次に登録されている認証方式が存在してもその認証方式では実施されません。 認証方式として指定したサーバーグループが存在しない場合は、そのサーバーグループは処理対象から外されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：enable パスワードの認証で使用する認証方式リストを設定する方法を示します。認証方式としてサーバーグループ「group2」を指定しています。

```
# configure terminal
(config)# aaa authentication enable default group group2
(config)#
```

9.2.15 aaa authentication mac-auth

aaa authentication mac-auth	
目的	MAC 認証で使用する認証方式リストを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	aaa authentication mac-auth default METHOD1 [METHOD2...] no aaa authentication mac-auth default
Parameter	METHOD1［METHOD2...］：ここで指定した順序で試行される認証方式のリストを、以下のパラメーターを指定します。認証方式は少なくとも 1 つは指定する必要があり、最大で 4 つまで指定できます。 • local：AccessDefender のローカルデータベース

<table>
<tr><th colspan="2">aaa authentication mac-auth</th></tr>
<tr><td></td><td>• group radius：デフォルトの RADIUS サーバーグループ「radius」
• group NAME：aaa group server コマンドで設定したサーバーグループ
• force [vlan VLAN-ID]：強制認証、認証後に変更する VLAN ID を 1～4094 の範囲で指定可能</td></tr>
<tr><td>デフォルト</td><td>local</td></tr>
<tr><td>モード</td><td>グローバル設定モード</td></tr>
<tr><td>特権レベル</td><td>レベル：15</td></tr>
<tr><td>ガイドライン</td><td>複数の認証方式が指定されている場合には、先頭の認証方式から処理が実施されます。タイムアウト等で処理がエラーになり明示的に許可もしくは拒否が判定されなかった場合には、次に登録されている認証方式で処理が実施されます。

明示的に認証拒否と判定されて認証失敗になった場合には、次に登録されている認証方式が存在してもその認証方式では実施されません。ただし、aaa authentication control sufficient mac コマンドが有効に設定されている場合には、認証失敗になった場合でも次に登録されている認証方式で認証が実施されます。

aaa authentication control sufficient mac コマンドを有効に設定している場合でも、他の認証方式で明示的に認証拒否と判定されて認証失敗になった場合には、強制認証(force)では認証が許可されません。

認証方式として指定したサーバーグループが存在しない場合は、そのサーバーグループは処理対象から外されます。

MAC 認証の認証時に RADIUS サーバーへ送信する認証要求に含まれる RADIUS 属性は以下です。
<table>
<tr><th>属性</th><th>属性値</th></tr>
<tr><td>User-Name</td><td>認証されるユーザー名</td></tr>
<tr><td>User-Password</td><td>パスワード</td></tr>
<tr><td>NAS-IP-Address</td><td>認証要求している RADIUS クライアントの IP アドレス(IPv4 のみ)</td></tr>
<tr><td>Calling-Station-Id</td><td>認証端末の MAC アドレス</td></tr>
<tr><td>NAS-Identifier</td><td>認証された端末が属している VLAN ID</td></tr>
<tr><td>NAS-Port</td><td>認証端末が接続されているインターフェース番号</td></tr>
</table>
AccessDefender のユーザー名とパスワードは最大 63 文字で指定します。ASCII コードの印字可能な文字のうち、; , | " ? 空白文字 を除いた文字のみ使用可能です。</td></tr>
<tr><td>制限・注意</td><td>• 認証方式として、TACACS+サーバーグループは指定できません。

• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。

• ローカルデータベース認証(local)よりも後に強制認証(force)を設定することもできますが、基本的にはローカルデータベース認証がタイムアウト等でエラーになることがないため強制認証(force)では認証されません。</td></tr>
<tr><td>バージョン</td><td>1.08.02</td></tr>
</table>

使用例：MAC 認証で使用する認証方式リストを設定する方法を示します。認証方式として RADIUS サーバーグループ「radius」を指定しています。

```
# configure terminal
```

```
(config)# aaa authentication mac-auth default group radius
(config)#
```

9.2.16 aaa authentication dot1x

aaa authentication dot1x	
目的	IEEE 802.1X 認証で使用する認証方式リストを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	aaa authentication dot1x default METHOD1 [METHOD2...] no aaa authentication dot1x default
Parameter	METHOD1 [METHOD2...]：ここで指定した順序で試行される認証方式のリストを、以下のパラメーターを指定します。認証方式は少なくとも 1 つは指定する必要があり、最大で 4 つまで指定できます。 • local：AccessDefender のローカルデータベース • group radius：デフォルトの RADIUS サーバーグループ「radius」 • group NAME：aaa group server コマンドで設定したサーバーグループ • force [vlan VLAN-ID]：強制認証、認証後に変更する VLAN ID を 1～4094 の範囲で指定可能
デフォルト	local
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	複数の認証方式が指定されている場合には、先頭の認証方式から処理が実施されます。タイムアウト等で処理がエラーになり明示的に許可もしくは拒否が判定されなかった場合には、次に登録されている認証方式で処理が実施されます。 明示的に認証拒否と判定されて認証失敗になった場合には、次に登録されている認証方式が存在してもその認証方式では実施されません。 認証方式として指定したサーバーグループが存在しない場合は、そのサーバーグループは処理対象から外されます。 IEEE 802.1X 認証の認証時に RADIUS サーバーへ送信する認証要求に含まれる RADIUS 属性は以下です。

属性	属性値
User-Name	認証されるユーザー名
NAS-IP-Address	認証要求しているオーセンティケーターの IP アドレス(IPv4 のみ)
Framed-MTU	サプリカントとオーセンティケーター間の最大フレームサイズ(1466 固定)
NAS-Port	サプリカントが接続されているオーセンティケーターのインターフェース番号
NAS-Port-Type	ユーザー認証に使用しているインターフェースのタイプ(Ethernet(15)固定)
Service-Type	提供するサービスタイプ(Framed(2)固定)
Calling-Station-Id	サプリカントの MAC アドレス
EAP-Message	EAP メッセージの送受信に使用
Message-Authenticator	RADIUS パケットの内容を保証するために使用

aaa authentication dot1x	
	State: オーセンティケーターと RADIUS サーバー間の State 情報の保持 AccessDefender のユーザー名とパスワードは最大 63 文字で指定します。ASCII コードの印字可能な文字のうち、; , | " ? 空白文字 を除いた文字のみ使用可能です。
制限・注意	• IEEE 802.1X 認証において、ローカルデータベースでの認証は未サポートです。必ず他の認証方式を指定してください。 • 認証方式として、TACACS+サーバーグループは指定できません。 • 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：IEEE 802.1X 認証で使用する認証方式リストを設定する方法を示します。認証方式として RADIUS サーバーグループ「radius」を指定しています。

```
# configure terminal
(config)# aaa authentication dot1x default group radius
(config)#
```

9.2.17 aaa authentication web-auth

aaa authentication web-auth	
目的	Web 認証で使用する認証方式リストを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	aaa authentication web-auth ID default METHOD1 [METHOD2...] no aaa authentication web-auth ID default
Parameter	ID：Web 認証 ID を、1～4 の範囲で指定します。デフォルトのログインページのように Web 認証 ID を使用しない場合は、ID に 1 を指定します。 METHOD1 [METHOD2...]：ここで指定した順序で試行される認証方式のリストを、以下のパラメーターを指定します。認証方式は少なくとも 1 つは指定する必要があり、最大で 4 つまで指定できます。 • local：AccessDefender のローカルデータベース • group radius：デフォルトの RADIUS サーバーグループ「radius」 • group NAME：aaa group server コマンドで設定したサーバーグループ • force [vlan VLAN-ID]：強制認証、認証後に変更する VLAN ID を 1～4094 の範囲で指定可能
デフォルト	local
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	複数の認証方式が指定されている場合には、先頭の認証方式から処理が実施されます。タイムアウト等で処理がエラーになり明示的に許可もしくは拒否が判定されなかった場合には、次に登録されている認証方式で処理が実施されます。 明示的に認証拒否と判定されて認証失敗になった場合には、次に登録されている認証方式が存在してもその認証方式では実施されません。ただし、aaa authentication control sufficient web コマンドが有効に設定されている場合には、認証失敗になった場合でも次に登録されている認証方式で認証が実施されます。

aaa authentication web-auth	
	aaa authentication control sufficient web コマンドを有効に設定している場合でも、他の認証方式で明示的に認証拒否と判定されて認証失敗になった場合には、強制認証(force)では認証が許可されません。 認証方式として指定したサーバーグループが存在しない場合は、そのサーバーグループは処理対象から外されます。 Web 認証の認証時に RADIUS サーバーへ送信する認証要求に含まれる RADIUS 属性は以下です。 属性 / 属性値 User-Name / 認証されるユーザー名 User-Password / パスワード NAS-IP-Address / 認証要求している RADIUS クライアントの IP アドレス(IPv4 のみ) Calling-Station-Id / 認証端末の MAC アドレス NAS-Identifier / 認証された端末が属している VLAN ID NAS-Port / 認証端末が接続されているインターフェース番号 AccessDefender のユーザー名とパスワードは最大 63 文字で指定します。ASCII コードの印字可能な文字のうち、; , | " ? 空白文字 を除いた文字のみ使用可能です。
制限・注意	• 認証方式として、TACACS+サーバーグループは指定できません。 • 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。 • ローカルデータベース認証(local)よりも後に強制認証(force)を設定することもできますが、基本的にはローカルデータベース認証がタイムアウト等でエラーになることがないため強制認証(force)では認証されません。
バージョン	1.08.02

使用例:Web 認証で使用する認証方式リストを設定する方法を示します。認証方式として RADIUS サーバーグループ「radius」を指定しています。

```
# configure terminal
(config)# aaa authentication web-auth 1 default group radius
(config)#
```

9.2.18 aaa authentication control sufficient

aaa authentication control sufficient	
目的	認証方式の移行条件変更機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	aaa authentication control sufficient {web ID | mac | login} no aaa authentication control sufficient {web ID | mac | login}
Parameter	web ID:Web 認証で本機能を使用する場合に指定します。Web 認証 ID を 1〜4 の範囲で指定します。 mac:MAC 認証で本機能を使用する場合に指定します。 login:ログイン認証で本機能を使用する場合に指定します。

aaa authentication control sufficient	
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	通常は、明示的に認証拒否と判定されて認証失敗になった場合には、次に登録されている認証方式が存在してもその認証方式では実施されません。ただし、本コマンドが有効に設定されている場合には、認証失敗になった場合でも次に登録されている認証方式で認証が実施されます。 本コマンドを有効に設定している場合でも、他の認証方式で明示的に認証拒否と判定されて認証失敗になった場合には、強制認証(force)または認証なし(none)では認証が許可されません。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：Web 認証 ID 1 の認証方式の移行条件変更機能を有効にする方法を示します。

```
# configure terminal
(config)# aaa authentication control sufficient web 1
(config)#
```

9.2.19 aaa default class

aaa default class	
目的	認証されたクライアントターミナルが、RADIUS サーバーやローカルデータベースによって割り当てられたクラス ID を持たない場合に使用する、デフォルトクラスの ID を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	aaa default class CLASS-ID no aaa default class
Parameter	CLASS-ID：デフォルトクラスの ID を 1～4095 の範囲で指定します。
デフォルト	ID は設定されていません。0 が表示されます。
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	RADIUS サーバーまたはローカルデータベースによってクラス ID が設定されていない場合は、認証されたクライアントターミナルでは、クラス ID は使用できません。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：デフォルトクラスの ID を 100 に設定する方法を示します。

```
# configure terminal
(config)# aaa default class 100
(config)#
```

9.2.20 aaa accounting system

aaa accounting system	
目的	システムイベントのアカウンティングで使用するアカウンティング方式リストを設定

aaa accounting system	
	します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	aaa accounting system default {none | start-stop METHOD1 [METHOD2...]} no aaa accounting system default
Parameter	none：アカウンティングを実行しない場合に指定します。 start-stop：アカウンティングを有効にする場合に指定します。 METHOD1 [METHOD2...]：ここで指定した順序で試行されるアカウンティング方式のリストを、以下のパラメーターを指定します。アカウンティング方式は少なくとも 1 つは指定する必要があり、最大で 4 つまで指定できます。 • group radius：デフォルトの RADIUS サーバーグループ「radius」 • group tacacs+：デフォルトの TACACS+サーバーグループ「tacacs+」 • group NAME：aaa group server コマンドで設定したサーバーグループ
デフォルト	アカウンティング方式リストの設定なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはシステムイベントのアカウンティングを有効にするために使用します。再起動やリセットといったシステムイベントの際にアカウンティングメッセージを送信します。 アカウンティング方式として指定したサーバーグループが存在しない場合は、そのサーバーグループは処理対象から外されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。 • アクセスできない RADIUS/TACACS+サーバーが存在している場合、再起動やリセット実施時にアカウンティングメッセージを送信できないことがあります。
バージョン	1.08.02

使用例：システムイベントのアカウンティングを有効にする方法を示します。アカウンティング方式として RADIUS サーバーグループ「radius」を指定しています。

```
# configure terminal
(config)# aaa accounting system default start-stop group radius
(config)#
```

9.2.21 aaa accounting network

aaa accounting network	
目的	AccessDefender のアカウンティングで使用するアカウンティング方式リストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	aaa accounting network default {none | start-stop METHOD1 [METHOD2...]} no aaa accounting network default
Parameter	none：アカウンティングを実行しない場合に指定します。 start-stop：AccessDefender の認証エントリーのログイン、ログアウト時にアカウンティングメッセージを送信する場合に指定します。 METHOD1 [METHOD2...]：ここで指定した順序で試行されるアカウンティング方

aaa accounting network	
	式のリストを、以下のパラメーターを指定します。アカウンティング方式は少なくとも 1 つは指定する必要があり、最大で 4 つまで指定できます。 • group radius：デフォルトの RADIUS サーバーグループ「radius」 • group tacacs+：デフォルトの TACACS+サーバーグループ「tacacs+」 • group NAME：aaa group server コマンドで設定したサーバーグループ
デフォルト	アカウンティング方式リストの設定なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	本コマンドは、IEEE 802.1X 認証、MAC 認証、Web 認証、ゲートウェイ認証でのアカウンティングを有効にするために使用します。 アカウンティング方式として指定したサーバーグループが存在しない場合は、そのサーバーグループは処理対象から外されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：AccessDefender のアカウンティングを有効にする方法を示します。動作モードとして start-stop パラメーターを指定し、アカウンティング方式として RADIUS サーバーグループ「radius」を指定しています。

```
# configure terminal
(config)# aaa accounting network default start-stop group radius
(config)#
```

9.2.22 aaa accounting commands

aaa accounting commands	
目的	指定した特権レベル内のコマンドのアカウンティングで使用するアカウンティング方式リストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	aaa accounting commands LEVEL {default | LIST-NAME} {none | start-stop METHOD1 [METHOD2...]} no aaa accounting commands LEVEL {default | LIST-NAME}
Parameter	LEVEL：特権レベルを 1～15 の範囲で指定します。指定した特権レベル内のすべてのコマンドのアカウンティングが設定されます。 default：デフォルトのアカウンティング方式リストを使用する場合に指定します。 LIST-NAME：デフォルト以外のアカウンティング方式リストを使用する場合に、リスト名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 none：アカウンティングを実行しない場合に指定します。 start-stop：アカウンティングを有効にする場合に指定します。 METHOD1 [METHOD2...]：ここで指定した順序で試行されるアカウンティング方式のリストを、以下のパラメーターを指定します。アカウンティング方式は少なくとも 1 つは指定する必要があり、最大で 4 つまで指定できます。 • group tacacs+：デフォルトの TACACS+サーバーグループ「tacacs+」 • group NAME：aaa group server tacacs+コマンドで設定した TACACS+サー

aaa accounting commands	
	バーグループ
デフォルト	アカウンティング方式リストの設定なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	指定した特権レベルのコマンド実行時にアカウンティングメッセージを送信します。有効にする場合は本コマンド以外に accounting commands コマンドの設定も必要です。 アカウンティング方式として指定した TACACS+サーバーグループが存在しない場合は、その TACACS+サーバーグループは処理対象から外されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：特権レベル 15 のコマンドのアカウンティングのための方式リスト「list-1」を設定する方法を示します。アカウンティング方式として TACACS+サーバーグループ「tacacs+」を指定しています。

```
# configure terminal
(config)# aaa accounting commands 15 list-1 start-stop group tacacs+
(config)#
```

9.2.23 accounting commands

accounting commands	
目的	ラインでのコマンドのアカウンティングに使用するアカウンティング方式リストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	accounting commands LEVEL {default | LIST-NAME} no accounting commands LEVEL
Parameter	LEVEL：特権レベルを 1～15 の範囲で指定します。指定した特権レベルのすべての設定コマンドにアカウンティングが設定されます。 default：デフォルトのアカウンティング方式リストを使用する場合に指定します。 LIST-NAME：使用するアカウンティング方式リストの名前を指定します。
デフォルト	無効
モード	ライン設定モード
特権レベル	レベル：15
ガイドライン	最初に aaa accounting commands コマンドでアカウンティング方式リストを作成します。アカウンティング方式リストが存在しない場合、コマンドは無効です。異なる特権レベルには異なるアカウンティング方式リストを指定できます。
制限・注意	• 1 つの特権レベルに指定できるアカウンティング方式リストは 1 つだけです。 • 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：コンソール接続において、アカウンティング方式リスト「cmd-15」を使用してコマンドのアカウンティングを有効にする方法を示します。

```
# configure terminal
(config)# aaa accounting commands 15 cmd-15 start-stop group tacacs+
(config)# line console
(config-line)# accounting commands 15 cmd-15
(config-line)#
```

9.2.24 aaa accounting exec

aaa accounting exec	
目的	ユーザーEXEC ターミナルセッションのアカウンティングで使用するアカウンティング方式リストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	aaa accounting exec {default | LIST-NAME} {none | start-stop METHOD1 [METHOD2...]} no aaa accounting exec {default | LIST-NAME}
Parameter	default：デフォルトのアカウンティング方式リストを使用する場合に指定します。 LIST-NAME：デフォルト以外のアカウンティング方式リストを使用する場合に、リスト名を最大 32 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 none：アカウンティングを実行しない場合に指定します。 start-stop：アカウンティングを有効にする場合に指定します。 METHOD1 [METHOD2...]：ここで指定した順序で試行されるアカウンティング方式のリストを、以下のパラメーターを指定します。アカウンティング方式は少なくとも 1 つは指定する必要があり、最大で 4 つまで指定できます。 • group radius：デフォルトの RADIUS サーバーグループ「radius」 • group tacacs+：デフォルトの TACACS+サーバーグループ「tacacs+」 • group NAME：aaa group server コマンドで設定したサーバーグループ
デフォルト	アカウンティング方式リストの設定なし
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	ユーザーのログイン、ログアウト時にアカウンティングメッセージを送信します。セッションタイムアウトによるログアウト時にもアカウンティングメッセージを送信します。有効にする場合は本コマンド以外に accounting exec コマンドの設定も必要です。 アカウンティング方式として指定したサーバーグループが存在しない場合は、そのサーバーグループは処理対象から外されます。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：ユーザーEXEC ターミナルセッションのアカウンティングのための方式リスト「list-1」を設定する方法を示します。アカウンティング方式として RADIUS サーバーグループ「radius」を指定しています。

```
# configure terminal
```

```
(config)# aaa accounting exec list-1 start-stop group radius
(config)#
```

9.2.25 accounting exec

accounting exec	
目的	ラインでのユーザーEXEC ターミナルセッションのアカウンティングに使用するアカウンティング方式リストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	accounting exec {default | LIST-NAME} no accounting exec
Parameter	default：デフォルトのアカウンティング方式リストを使用する場合に指定します。 LIST-NAME：使用するアカウンティング方式リストの名前を指定します。
デフォルト	無効
モード	ライン設定モード
特権レベル	レベル：15
ガイドライン	最初に aaa accounting commands コマンドでアカウンティング方式リストを作成します。アカウンティング方式リストが存在しない場合、コマンドは無効です。
制限・注意	• 本コマンドを実行するには、事前に aaa new-model コマンドで AAA を有効化する必要があります。
バージョン	1.08.02

使用例：コンソール接続において、アカウンティング方式リスト「list-1」を使用してユーザーEXECターミナルセッションのアカウンティングを有効にする方法を示します。

```
# configure terminal
(config)# aaa accounting exec list-1 start-stop group radius
(config)# line console
(config-line)# accounting exec list-1
(config-line)#
```

9.2.26 show aaa

show aaa	
目的	AAA 機能の有効／無効を表示します。
Command	show aaa
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：AAA 機能の有効／無効を表示する方法を示します。

```
# show aaa

 AAA is enabled. ...(1)
```

項番	説明
(1)	AAA 機能の有効(enabled)／無効(disabled)を表示します。

9.2.27 show radius statistics

show radius statistics	
目的	RADIUS サーバーの状態を表示します。
Command	show radius statistics
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：RADIUS サーバーの状態と統計情報を表示する方法を示します。

```
# show radius statistics
                 (1)              (2)              (3)
 RADIUS Server: 172.19.192.80: Auth-Port 1645, Acct-Port 1646
 State is Up ...(4)       (5)          (6)
                          Auth.        Acct.
 Round Trip Time:         10           10 ...(7)
 Access Requests:         4            NA ...(8)
 Access Accepts:          0            NA ...(9)
 Access Rejects:          4            NA ...(10)
 Access Challenges:       0            NA ...(11)
 Acct Request:            NA           3 ...(12)
 Acct Response:           NA           3 ...(13)
 Retransmissions:         0            0 ...(14)
 Malformed Responses:     0            0 ...(15)
 Bad Authenticators:      0            0 ...(16)
 Pending Requests:        0            0 ...(17)
 Timeouts:                0            0 ...(18)
 Unknown Types:           0            0 ...(19)
 Packets Dropped:         0            0 ...(20)
```

項番	説明
(1)	RADIUS サーバーの IP アドレスを表示します。
(2)	RADIUS サーバーの認証用の UDP ポート番号を表示します。
(3)	RADIUS サーバーのアカウンティング用の UDP ポート番号を表示します。
(4)	RADIUS サーバーの状態を表示します。 Up：問い合わせ対象として使用可能な状態 Down：オフラインとみなして、問い合わせ対象から除外している状態
(5)	認証パケットの統計情報を表示します。
(6)	アカウンティングパケットの統計情報を表示します。
(7)	RADIUS サーバーからの直近の応答と、応答と一致した要求との間の時間間隔（100 分の 1 秒単位）を表示します。

項番	説明
(8)	サーバーに送信された RADIUS アクセス要求パケットの数を表示します。再送されたパケットは含まれません。
(9)	サーバーから受信した RADIUS Access-Accept パケットの数を表示します。
(10)	サーバーから受信した RADIUS Access-Reject パケットの数を表示します。
(11)	サーバーから受信した RADIUS Access-Challenge パケットの数を表示します。
(12)	送信された RADIUS Accounting-Request パケットの数を表示します。再送されたパケットは含まれません。
(13)	アカウンティングポートで受信したサーバーからの RADIUS パケットの数を表示します。
(14)	RADIUS サーバーに再送された RADIUS 要求パケットの数を表示します。再送には、識別子と Acct-Delay が更新されたリトライ状態が同じままのリトライが含まれます。
(15)	サーバーから受信した誤った形式の RADIUS 応答パケットの数を表示します。長さが無効なパケットも数に含まれます。なお、誤った Authenticator、署名属性、または不明なタイプは、誤った形式の応答の数には含まれません。
(16)	サーバーから受信した無効な Authenticator または署名属性を含んだ RADIUS 応答パケットの数を表示します。
(17)	サーバー宛てでタイムアウト前または応答未受信の RADIUS 要求パケットの数を表示します。要求の送信によって増えます。また、要求の受信、タイムアウト、または再送によって減少します。
(18)	サーバーのタイムアウト回数を表示します。タイムアウト後のクライアントに想定される動作は、同じサーバーへのリトライ、別のサーバーへの送信、または断念のいずれかです。同じサーバーへのリトライは、再送とタイムアウトとしてカウントします。別のサーバーへの送信は、要求とタイムアウトとしてカウントします。
(19)	サーバーから受信したタイプ不明の RADIUS パケットの数を表示します。
(20)	サーバーから受信し、何らかの理由で廃棄された RADIUS パケットの数を表示します。

9.2.28 show tacacs statistics

show tacacs statistics	
目的	TACACS+サーバーの状態を表示します。
Command	show tacacs statistics
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• スタック構成でマスターの切り替わりが発生した場合、本コマンドの統計情報は引き継がれません。 • 本コマンドの統計情報は TACACS+サーバーによる認証時にのみカウントします。アカウンティングで使用している場合はカウントしません。
バージョン	1.08.02

使用例：TACACS+サーバーの状態と統計情報を表示する方法を示します。

```
# show tacacs statistics
                  (1)                (2)
```

```
TACACS+ Server: 172.19.192.80/49, State is Up
Socket Opens: 0 ...(3)
Socket Closes: 0 ...(4)
Total Packets Sent: 0 ...(5)
Total Packets Recv: 0 ...(6)
Reference Count: 0 ...(7)
```

項番	説明
(1)	TACACS+サーバーの IP アドレスを表示します。
(2)	TACACS+サーバーの状態を表示します。
(3)	TACACS+サーバーへの TCP ソケット接続に成功した回数を表示します。
(4)	TCP ソケットを閉じようとして成功した回数を表示します。
(5)	TACACS+サーバーに送信されたパケットの数を表示します。
(6)	TACACS+サーバーから受信したパケットの数を表示します。
(7)	TACACS+サーバーからの認証要求の数を表示します。

9.2.29 clear aaa counters servers

clear aaa counters servers	
目的	認証とアカウンティングで使用するサーバーの統計情報を消去します。
Command	clear aaa counters servers {all | radius {IP-ADDRESS | IPV6-ADDRESS | all} | tacacs {IP-ADDRESS | all} | sg NAME}
Parameter	all：すべてのサーバーの統計情報を消去する場合に指定します。 radius：統計情報を消去する RADIUS サーバーを指定します。 • IP-ADDRESS：RADIUS サーバーの IPv4 アドレスを指定 • IPV6-ADDRESS：RADIUS サーバーの IPv6 アドレスを指定 • all：すべての RADIUS サーバーを対象にする場合に指定 tacacs：統計情報を消去する TACACS+サーバーを指定します。 • IP-ADDRESS：TACACS+サーバーの IPv4 アドレスを指定 • all：すべての TACACS+サーバーを対象にする場合に指定 sg NAME：サーバーグループに登録されたすべてのサーバーの統計情報を消去する場合に、サーバーグループ名を指定します。
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：認証とアカウンティングで使用するすべてのサーバーの統計情報を消去する方法を示します。

```
# clear aaa counters servers all
#
```

使用例：サーバーグループ「server-farm」に登録されたすべてのサーバーの統計情報を消去する方法を示します。

```
# clear aaa counters servers sg server-farm
#
```

9.3 MAC 認証コマンド

MAC 認証関連の設定コマンドは以下のとおりです。

- mac-authentication enable
- mac-authentication discard-time
- mac-authentication ignore-dhcp
- mac-authentication password
- mac-authentication username mac-format

9.3.1 mac-authentication enable

mac-authentication enable	
目的	MAC 認証を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	mac-authentication enable no mac-authentication enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	MAC 認証は、クライアントの MAC アドレスを使用して認証を行う機能です。 MAC 認証を有効にする前に、total-client コマンドで認証クライアントの最大数を設定してください。 アクセスリストの認証バイパスエントリー(permit authentication-bypass)にマッチした場合は、未認証状態でも中継は許可されます。これにより、認証前に未認証クライアントからの通信を許可することができます（認証バイパス)。 認証に成功して属性値として VLAN ID が通知された場合は、認証に成功したクライアントごとに、受信する VLAN をダイナミックに割り当てることができます（ダイナミック VLAN)。なお、同一ポートに複数の VLAN を割り当てることができます。 MAC 認証に失敗した場合は、Discard 端末として一定時間（デフォルト設定は 300 秒）登録されます。Discard 端末として登録されている間は、その端末から任意のパケットを受信しても MAC 認証は行われず破棄されます。 Discard 端末を手動で削除する場合は、access-defender logout コマンドで Discard 登録されたクライアントの MAC アドレスまたはユーザー名を指定して削除します。
制限・注意	• ダイナミックに割り当てる VLAN は、あらかじめ作成しておく必要があります。 • ダイナミック VLAN を使用する際、設定した最大認証端末数に満たない場合でも、VLAN 割り当て時にテーブルのエントリーが重複して、ログインに失敗する可能性があります。 • MAC 認証有効ポートで認証バイパスを使用する際、MAC 認証と関係なく CPU 宛てにコピーされるパケットは、たとえ認証バイパスにマッチしても CPU コピーされるため、MAC 認証が動作します。(例：IP アドレス設定時の自局 IP アドレス宛てパケットや任意宛ての ARP Request パケットなど、各機能有効時に CPU 処理やソフトウェア中継されるパケットなど) • この状況で MAC 認証に失敗して Discard 登録された場合でも、認証バイパスにマッチするため通信可能ですが、Discard 登録の解除と MAC 認証の失敗が定期的に

mac-authentication enable	
	繰り返され、不要なログが出力される可能性があることに注意してください。
バージョン	1.08.02

使用例：MAC 認証を有効にする方法を示します。

```
# configure terminal
(config)# mac-authentication enable
(config)#
```

9.3.2 mac-authentication discard-time

mac-authentication discard-time	
目的	MAC 認証の認証破棄時間（Discard 端末として登録している時間）を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mac-authentication discard-time SECONDS no mac-authentication discard-time
Parameter	SECONDS：MAC 認証の認証破棄時間を 10～86,400 秒の範囲で指定します。
デフォルト	300 秒
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	MAC 認証に失敗した場合は、Discard 端末として一定時間（デフォルト設定は 300 秒）登録されます。Discard 端末として登録されている間は、その端末から任意のパケットを受信しても MAC 認証は行われず破棄されます。
制限・注意	• AEOS-NP2500 Ver. 1.10.02 より前のバージョンでは、設定範囲は 300～86,400 秒です。
バージョン	1.08.02 1.10.02：設定範囲を 10～86,400 秒に拡張

使用例：MAC 認証の認証破棄時間を 600 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# mac-authentication discard-time 600
(config-a-def)#
```

9.3.3 mac-authentication ignore-dhcp

mac-authentication ignore-dhcp	
目的	MAC 認証において、認証端末から送信される DHCP 関連パケット、DHCPv6 関連パケット、および近隣要請メッセージ（ICMPv6 NS）を MAC 認証の対象外とします。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mac-authentication ignore-dhcp no mac-authentication ignore-dhcp
Parameter	なし
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15

mac-authentication ignore-dhcp	
ガイドライン	MAC 認証において、認証端末から送信される UDP ポート 67（DHCP サーバー）、547（DHCPv6 サーバー）および 135（ICMPv6 NS）宛てのパケットを MAC 認証の対象外とします。本機能を有効にすると、これらのパケットを MAC 認証インターフェースで受信しても MAC 認証は動作しません。パケットの中継動作は MAC 認証の認証結果に従います。
制限・注意	-
バージョン	1.08.02

使用例：クライアントからの UDP ポート 67（DHCP サーバー）、547（DHCPv6 サーバー）および 135（ICMPv6 NS）宛ての破棄パケットを無視するように MAC 認証を設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# mac-authentication ignore-dhcp
(config-a-def)#
```

9.3.4 mac-authentication password

mac-authentication password	
目的	MAC 認証で使用するパスワードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mac-authentication password [0 | 7] PASS {mac | web-mac | dot1x-mac | web-dot1x-mac} no mac-authentication password {mac | web-mac | dot1x-mac | web-dot1x-mac}
Parameter	[0 | 7] PASS：MAC 認証で使用するパスワードを指定します。 • 0：パスワードを平文で入力する場合に指定します。0 および 7 を省略した場合のデフォルト設定です。 • 7：パスワードを暗号化した形式で入力する場合に指定します。 • PASS：MAC 認証で使用するパスワードを入力します。平文で入力する場合は最大 63 文字で指定します。暗号化した形式で入力する場合は最大 44 文字で指定します。 認証種別を以下のパラメーターで指定します。 • mac：MAC 認証 • web-mac：Web/MAC 認証(AND) • dot1x-mac：IEEE 802.1X/MAC 認証(AND) • web-dot1x-mac：Web/IEEE 802.1X/MAC 認証(AND)
デフォルト	端末の MAC アドレスが MAC 認証パスワードとして使用されます。 MAC アドレスの形式は mac-authentication username mac-format コマンドの設定に従います。
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：Web/MAC 認証(AND)で使用するパスワードを「password1」に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# mac-authentication password password1 web-mac
(config-a-def)#
```

9.3.5 mac-authentication username mac-format

mac-authentication username mac-format	
目的	MAC 認証で使用するユーザー名の形式を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	mac-authentication username mac-format case {lowercase | uppercase} delimiter {{hyphen | colon | dot} number {1 | 2 | 5} | none} no mac-authentication username mac-format
Parameter	case：MAC 認証用のユーザー名として使用する MAC アドレスの大文字／小文字の設定を指定します。 • lowercase：小文字指定（例：aabbccddeeff） • uppercase：大文字指定（例：AABBCCDDEEFF） delimiter：区切り文字を指定します。 • hyphen：ハイフン指定（例：aa-bb-cc-dd-ee-ff） • colon：コロン指定（例：aa:bb:cc:dd:ee:ff） • dot：ドット指定（例：aa.bb.cc.dd.ee.ff） • none：区切り文字を使用しない場合に指定（例：aabbccddeeff） number：区切り文字の数を指定します。 • 1：区切り文字 1 個指定（例：aabbcc-ddeeff） • 2：区切り文字 2 個指定（例：aabb-ccdd-eeff） • 5：区切り文字 5 個指定（例：aa-bb-cc-dd-ee-ff）
デフォルト	小文字、区切り文字を使用しない形式（例：aabbccddeeff）
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	MAC 認証のユーザー名には端末の MAC アドレスが使用されます。デフォルト設定では「小文字、区切り文字を使用しない形式」がユーザー名になります。
制限・注意	-
バージョン	1.08.02

使用例：ユーザー名として使用する MAC アドレスの形式を、大文字で、区切り文字としてハイフンを 5 つ使用する形式に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# mac-authentication username mac-format case uppercase delimiter hyphen
number 5
(config-a-def)#
```

9.4 IEEE 802.1X 認証コマンド

IEEE 802.1X 認証関連の設定コマンドは以下のとおりです。

- dot1x enable
- dot1x ignore-eapol-start interface
- dot1x mode mac-authentication-fail
- dot1x reauthentication interface
- dot1x timeout quiet-period
- dot1x timeout re-authperiod
- dot1x timeout supp-timeout
- dot1x timeout server-timeout
- dot1x timeout tx-period
- fwd-eapol enable

IEEE 802.1X 認証関連の show／操作コマンドは以下のとおりです。

- show access-defender dot1x
- show access-defender dot1x interface
- show access-defender dot1x statistics
- dot1x initialize interface
- dot1x re-authenticate interface

9.4.1 dot1x enable

dot1x enable	
目的	IEEE 802.1X 認証を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	dot1x enable no dot1x enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	IEEE 802.1X 認証を有効にする前に、total-client コマンドで認証クライアントの最大数を設定してください。 アクセスリストの認証バイパスエントリー(permit authentication-bypass)にマッチした場合は、未認証状態でも中継は許可されます。これにより、認証前に未認証クライアントからの通信を許可することができます（認証バイパス)。 認証に成功して属性値として VLAN ID が通知された場合は、認証に成功したクライアントごとに、受信する VLAN をダイナミックに割り当てることができます（ダイナミック VLAN)。なお、同一ポートに複数の VLAN を割り当てることができます。
制限・注意	• クライアントのユーザー名が 64 文字以上の場合、認証済みクライアントの登録時に 64 文字以降は切り捨てられます。 • ダイナミックに割り当てる VLAN は、あらかじめ作成しておく必要があります。 • ダイナミック VLAN を使用する際、設定した最大認証端末数に満たない場合でも、

dot1x enable	
	VLAN 割り当て時にテーブルのエントリーが重複して、ログインに失敗する可能性があります。
バージョン	1.08.02

使用例：IEEE 802.1X 認証を有効にする方法を示します。

```
# configure terminal
(config)# dot1x enable
(config)#
```

9.4.2 dot1x ignore-eapol-start interface

dot1x ignore-eapol-start interface	
目的	EAPOL-Start 受信による認証の抑止機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	dot1x ignore-eapol-start interface IF-ID [,|-] no dot1x ignore-eapol-start interface IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本設定を有効にしたインターフェースでは、サプリカントから EAPOL-Start を受信しても、EAP-Request/EAP-Identity を応答せず、認証を抑止することができます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で EAPOL-Start 受信による認証の抑止機能を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dot1x ignore-eapol-start interface port 1/0/1
(config-a-def)#
```

9.4.3 dot1x mode mac-authentication-fail

dot1x mode mac-authentication-fail	
目的	MAC 認証と IEEE 802.1X 認証の「OR 認証」で、MAC 認証が失敗した場合のみ IEEE 802.1X 認証を開始するモードを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	dot1x mode mac-authentication-fail no dot1x mode mac-authentication-fail
Parameter	なし
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15

dot1x mode mac-authentication-fail	
ガイドライン	本機能を有効にすると、MAC 認証と IEEE 802.1X 認証の「OR 認証」で MAC 認証を先に行い、MAC 認証が失敗した場合のみ IEEE 802.1X 認証を開始するようになります。MAC 認証が成功した場合は IEEE 802.1X 認証は行いません。
制限・注意	-
バージョン	1.08.02

使用例：MAC 認証と IEEE 802.1X 認証の「OR 認証」で、MAC 認証が失敗した場合のみ IEEE 802.1X 認証を開始するモードを有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dot1x mode mac-authentication-fail
(config-a-def)#
```

9.4.4 dot1x reauthentication interface

dot1x reauthentication interface	
目的	IEEE 802.1X 認証の再認証を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	dot1x reauthentication interface IF-ID [,|-] no dot1x reauthentication interface IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で IEEE 802.1X 認証の再認証を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dot1x reauthentication interface port 1/0/1
(config-a-def)#
```

9.4.5 dot1x timeout quiet-period

dot1x timeout quiet-period	
目的	認証が失敗したときのステータスの保持時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	dot1x timeout quiet-period SECONDS interface IF-ID [,|-] no dot1x timeout quiet-period interface IF-ID [,|-]
Parameter	SECONDS：ステータスの保持時間を、0 または 5～65,535 秒の範囲で指定します。0 指定時は、認証が失敗したときにステータスは保持されません。

dot1x timeout quiet-period	
	interface IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	60 秒
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で認証が失敗したときのステータスの保持時間を 10 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dot1x timeout quiet-period 10 interface port 1/0/1
(config-a-def)#
```

9.4.6 dot1x timeout re-authperiod

dot1x timeout re-authperiod	
目的	再認証の間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	dot1x timeout re-authperiod SECONDS interface IF-ID [,|-] no dot1x timeout re-authperiod interface IF-ID [,|-]
Parameter	SECONDS：再認証の間隔を 5～2,147,483,647 秒の範囲で指定します。 interface IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	3600 秒
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で再認証の間隔を 7200 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dot1x timeout re-authperiod 7200 interface port 1/0/1
(config-a-def)#
```

9.4.7 dot1x timeout supp-timeout

dot1x timeout supp-timeout	
目的	RADIUS サーバーからの EAP メッセージを受信後、サプリカントからの応答がない

dot1x timeout supp-timeout	
	場合に EAP-Request を再送信する間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	dot1x timeout supp-timeout SECONDS interface IF-ID [,|-] no dot1x timeout supp-timeout interface IF-ID [,|-]
Parameter	SECONDS：EAP-Request を再送信する間隔を 5～65,535 秒の範囲で指定します。 interface IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	30 秒
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で EAP-Request を再送信する間隔を 60 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dot1x timeout supp-timeout 60 interface port 1/0/1
(config-a-def)#
```

9.4.8 dot1x timeout server-timeout

dot1x timeout server-timeout	
目的	サプリカントが接続されて RADIUS サーバーに認証問い合わせを実施する際の、RADIUS サーバーからの応答待ち時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	dot1x timeout server-timeout SECONDS interface IF-ID [,|-] no dot1x timeout server-timeout interface IF-ID [,|-]
Parameter	SECONDS：RADIUS サーバーからの応答待ち時間を 5～65,535 秒の範囲で指定します。 interface IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	30 秒
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.10.01

使用例：ポート 1/0/1 で RADIUS サーバーの応答待ち時間を 310 秒に設定する方法を示します。

```
# configure terminal
```

```
(config)# access-defender
(config-a-def)# dot1x timeout server-timeout 310 interface port 1/0/1
(config-a-def)#
```

9.4.9 dot1x timeout tx-period

dot1x timeout tx-period	
目的	EAP-Request/EAP-Identity をサプリカントに送信する間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	dot1x timeout tx-period SECONDS interface IF-ID [,|-] no dot1x timeout tx-period interface IF-ID [,|-]
Parameter	SECONDS：EAP-Request/EAP-Identity をサプリカントに送信する間隔を、0 または 5～65,535 秒の範囲で指定します。 interface IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	30 秒
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 で EAP-Request/EAP-Identity をサプリカントに送信する間隔を 60 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dot1x timeout tx-period 60 interface port 1/0/1
(config-a-def)#
```

9.4.10 fwd-eapol enable

fwd-eapol enable	
目的	IEEE 802.1X 認証が無効なインターフェースで受信した EAPOL フレームを転送する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	fwd-eapol enable no fwd-eapol enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本設定が無効の場合は、IEEE 802.1X 認証が無効なインターフェースで EAPOL フレームを受信しても転送しません。
制限・注意	-
バージョン	1.08.02

使用例：IEEE 802.1X 認証が無効なインターフェースで受信した EAPOL フレームを、転送する機能を有効にする方法を示します。

```
# configure terminal
(config)# fwd-eapol enable
(config)#
```

9.4.11 show access-defender dot1x

show access-defender dot1x	
目的	登録されたサプリカントの情報を表示します。
Command	show access-defender dot1x
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：登録されたサプリカントの情報を表示する方法を示します。

```
# show access-defender dot1x

802.1X Port-Based Authentication Enabled ...(1)
802.1X info for Port-channel1 ...(2)
  Supplicant name: user1 ...(3)
  Supplicant address: 00-0C-29-8F-8F-2A ...(4)
  portEnabled: true - portControl: Auto ...(5)
  portStatus: authorized - currentId: 1 ...(6)
  protocol version: 2 ...(7)
  reAuthenticate: Disabled ...(8)
  reAuthPeriod: 3600 ...(9)
       (10)                    (11)
  PAE: state:Authenticated - portMode: Auto
  PAE: reAuthCount: 0 ...(12)
       (13)                (14)            (15)
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle ...(16)
      (17)                (18)
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: In - operControlledDirections: In
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

項番	説明
(1)	IEEE 802.1X 認証の有効(Enabled)／無効(Disabled)を表示します。
(2)	情報を表示するポート番号またはポートチャネル番号を表示します。
(3)	サプリカントのユーザー名を表示します。
(4)	サプリカントの MAC アドレスを表示します。
(5)	リンクステータス(true 固定)、ポートコントロール(Auto 固定)を表示します。
(6)	認証状態（authorized：認証済／unauthorized：未認証）と、現在の認証セッション ID を

項番	説明
	表示します。
(7)	IEEE 802.1X/EAPOL プロトコルバージョンを表示します。
(8)	IEEE 802.1X 認証の再認証の有効(Enabled)／無効(Disabled)を表示します。
(9)	再認証の間隔(秒)を表示します。
(10)	Port Access Entity (PAE) のステータスを表示します。 Down：ダウン状態 Initialize：初期化中 Disconnecting：接続なし Connecting：接続済み Authenticating：認証中 Aborting：中断中 Held：EAP-Failure 送信
(11)	PAE のポートモード (Auto 固定) を表示します。
(12)	サプリカントへのリクエスト ID 送信リトライ回数を表示します。
(13)	認証が失敗したときのステータスの保持時間(秒)を表示します。
(14)	EAP-Request/EAP-Identity をサプリカントに再送信する回数 (2 回固定) を表示します。
(15)	EAP-Request/EAP-Identity をサプリカントに送信する間隔(秒)を表示します。
(16)	バックエンド認証のステータスを表示します。 Invalid：無効 Request：リクエスト送信 Response：応答受信 Success：認証成功 Fail：認証失敗 Timeout：応答タイムアウト Idle：待機中 Initialize：初期化
(17)	RADIUS サーバーからの EAP メッセージを受信後、サプリカントからの応答がない場合に EAP-Request を再送信する間隔(秒)を表示します。
(18)	RADIUS サーバーからの応答待ち時間(秒)を表示します。

9.4.12 show access-defender dot1x interface

show access-defender dot1x interface	
目的	IEEE 802.1X 認証の設定を表示します。
Command	show access-defender dot1x interface IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-

show access-defender dot1x interface	
バージョン	1.08.02

使用例：ポート 1/0/1 の IEEE 802.1X 認証の設定を表示する方法を示します。

```
# show access-defender dot1x interface port 1/0/1

Interface          : Port1/0/1 ...(1)
PAE                : Authenticator ...(2)
Port Control       : Auto ...(3)
Ignore EAPOL start: Disabled ...(4)
Quiet Period       : 60     sec ...(5)
Tx Period          : 30     sec ...(6)
Supp Timeout       : 30     sec ...(7)
Server Timeout     : 30     sec ...(8)
Max-req            : 2      times ...(9)
Re-Authenticate    : Enabled ...(10)
Re-Auth Period     : 3600   sec ...(11)
```

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	Port Access Entity (PAE) の現在の状態を表示します。
(3)	ポートコントロール (Auto 固定) を表示します。
(4)	EAPOL-Start 受信による認証の抑止機能の有効(Enabled)／無効(Disabled)を表示します。
(5)	認証が失敗したときのステータスの保持時間(秒)を表示します。
(6)	EAP-Request/EAP-Identity をサプリカントに送信する間隔(秒)を表示します。
(7)	RADIUS サーバーからの EAP メッセージを受信後、サプリカントからの応答がない場合に EAP-Request を再送信する間隔(秒)を表示します。
(8)	RADIUS サーバーからの応答待ち時間(秒)を表示します。
(9)	EAP-Request/EAP-Identity をサプリカントに再送信する回数 (2 回固定) を表示します。
(10)	IEEE 802.1X 認証の再認証の有効(Enabled)／無効(Disabled)を表示します。
(11)	再認証の間隔(秒)を表示します。

9.4.13 show access-defender dot1x statistics

show access-defender dot1x statistics	
目的	IEEE 802.1X 認証に関する統計情報を表示します。
Command	show access-defender dot1x statistics [interface IF-ID [,|-]]
Parameter	interface IF-ID (省略可能)：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	特定のインターフェースを指定しない場合は、すべてのインターフェースの情報が表示されます。
制限・注意	-
バージョン	1.08.02

使用例：ポート 1/0/1 の IEEE 802.1X 認証に関する統計情報を表示する方法を示します。

```
# show access-defender dot1x statistics interface port 1/0/1

Port1/0/1 dot1x statistics information:
EAPOL Frames RX                          : 1  ...(1)
EAPOL Frames TX                          : 4  ...(2)
EAPOL-Start Frames RX                    : 0  ...(3)
EAPOL-Req/Id Frames TX                   : 6  ...(4)
EAPOL-Logoff Frames RX                   : 0  ...(5)
EAPOL-Req Frames TX                      : 0  ...(6)
EAPOL-Resp/Id Frames RX                  : 0  ...(7)
EAPOL-Resp Frames RX                     : 0  ...(8)
Invalid EAPOL Frames RX                  : 0  ...(9)
EAP-Length Error Frames RX               : 0  ...(10)
Last EAPOL Frame Version                 : 0  ...(11)
Last EAPOL Frame Source                  : 00-10-28-00-19-78  ...(12)
```

項番	説明
(1)	受信した EAPOL フレームのフレーム数を表示します。
(2)	送信した EAPOL フレームのフレーム数を表示します。
(3)	受信した EAPOL-Start フレームのフレーム数を表示します。
(4)	送信した EAP-Request/EAP-Identity フレームのフレーム数を表示します。
(5)	受信した EAPOL-Logoff フレームのフレーム数を表示します。
(6)	送信した EAP-Request フレームのフレーム数を表示します。
(7)	受信した EAP-Response/EAP-Identity フレームのフレーム数を表示します。
(8)	受信した EAP-Response フレームのフレーム数を表示します。
(9)	受信した無効な EAPOL フレームのフレーム数を表示します。
(10)	受信した EAP フレームのうち、Length に誤りがあるフレームのフレーム数を表示します。
(11)	最後に送受信した EAPOL フレームのプロトコルバージョンを表示します。
(12)	最後に送受信した EAPOL フレームの送受信相手の MAC アドレスを表示します。

9.4.14 dot1x initialize interface

dot1x initialize interface	
目的	指定したインターフェースの IEEE 802.1X 認証を初期化して、認証済みクライアントを削除します。
Command	dot1x initialize interface IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	• 本コマンドは AccessDefender 設定モードで実施する実行コマンドで、実施しても構成情報には残りません。
バージョン	1.08.02

使用例：ポート 1/0/1 で IEEE 802.1X 認証を初期化する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dot1x initialize interface port 1/0/1
(config-a-def)#
```

9.4.15 dot1x re-authenticate interface

dot1x re-authenticate interface	
目的	指定したインターフェースで IEEE 802.1X 認証の再認証を実行します。
Command	dot1x re-authenticate interface IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	• 本コマンドは AccessDefender 設定モードで実施する実行コマンドで、実施しても構成情報には残りません。
バージョン	1.08.02

使用例：ポート 1/0/1 で IEEE 802.1X 認証の再認証を実行する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dot1x re-authenticate interface port 1/0/1
(config-a-def)#
```

9.5 SSL コマンド

SSL（SECURE SOCKETS LAYER）関連の show／操作コマンドは以下のとおりです。

- show ssl https-certificate
- show ssl https-private-key
- show ssl csr
- ssl gencsr rsakey

9.5.1 show ssl https-certificate

show ssl https-certificate	
目的	SSL サーバー証明書情報を表示します。
Command	show ssl https-certificate
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• SSL サーバーの秘密鍵は、SSL サーバー証明書（https-certificate）と秘密鍵（https-private-key）の両方が装置内にある場合にのみ有効です。そのため、秘密鍵なしで SSL サーバー証明書情報を表示することはできません。ダウンロードした SSL サーバー証明書と一致する秘密鍵をダウンロードしてください。
バージョン	1.08.02

使用例：SSL サーバー証明書情報を表示する方法を示します。

```
# show ssl https-certificate

Certificate Information:
Certificate Version :3 ...(1)
Serial Number :00:80:2D:5E:A8:BD:8D:53:C3 ...(2)
Issuer Name   :C=JP, ST=Tokyo, L=Chiyoda-ku, O=Example Domain., OU=Example Group.,
CN=Apresia, emailAddress=example@example.com ...(3)
Subject Name  :C=JP, ST=Tokyo, L=Chiyoda-ku, O=Example Domain., OU=Example Group.,
CN=Apresia, emailAddress=example@example.com ...(4)
Not Before    :2017-02-16 06:54:58 ...(5)
Not After     :2037-02-11 06:54:58 ...(6)
Public Key Alg:rsaEncryption ...(7)
Signed Using  :RSA+SHA256 ...(8)
RSA Key Size  :2048 bits ...(9)
```

項番	説明
(1)	バージョンを表示します。
(2)	シリアル番号を表示します。
(3)	発行者を表示します。
(4)	サブジェクトを表示します。
(5)	有効期間の開始日時を表示します。
(6)	有効期間の終了日時を表示します。
(7)	公開鍵アルゴリズムを表示します。

項番	説明
(8)	署名アルゴリズムを表示します。
(9)	公開鍵 (RSA キー) のサイズを表示します。

9.5.2 show ssl https-private-key

show ssl https-private-key	
目的	SSL サーバーの秘密鍵情報を表示します。
Command	show ssl https-private-key
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• SSL サーバーの秘密鍵は、SSL サーバー証明書 (https-certificate) と秘密鍵 (https-private-key) の両方が装置内にある場合にのみ有効です。そのため、秘密鍵なしで SSL サーバー証明書情報を表示することはできません。ダウンロードした SSL サーバー証明書と一致する秘密鍵をダウンロードしてください。
バージョン	1.08.02

使用例：SSL サーバーの秘密鍵情報を表示する方法を示します。

```
# show ssl https-private-key

Private key is embedded in firmware. ...(1)
```

項番	説明
(1)	SSL サーバーの証明書と、その証明書に一致する秘密鍵の両方をユーザーがダウンロードした状態では、「Private key is installed by user.」と表示されます。

9.5.3 show ssl csr

show ssl csr	
目的	CSR (証明書署名要求) を表示します。
Command	show ssl csr
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：CSR (証明書署名要求) を表示する方法を示します。

```
# show ssl csr

Certificate Request: ...(1)
    Data:
        Version: 1 (0x1)
```

```
        Subject: C=jp, ST=tokyo, L=chiyoda-ku, O=apresia, OU=network,
CN=www.apresia.jp/emailAddress=xxx@apresia.jp
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:9d:f3:98:37:f2:c5:7f:e0:89:b3:6a:6f:b6:9a:
                    f3:b1:76:48:c3:91:20:9f:b4:7c:d8:91:ac:6a:a3:
                    6b:df:da:7a:2e:93:9e:0e:56:92:6f:01:84:6f:bd:
                    c5:61:21:7a:a0:29:42:c7:5b:79:22:7c:cb:2e:4a:
                    9a:8a:5a:c0:45:9e:43:b4:8e:6b:2f:11:6d:a1:12:
                    17:d7:bf:ec:ca:72:ca:ea:2b:2f:df:e4:e7:03:14:
                    ee:e8:97:4a:a7:ba:67:b9:2b:ce:a2:f5:28:1c:fa:
                    a7:67:b3:59:96:0a:6f:91:fd:fc:bd:1c:86:79:b8:
                    41:d9:04:74:01:d5:b3:63:61
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
        8c:c6:69:d7:65:56:e8:80:5d:3b:58:fa:3f:86:91:01:aa:97:
        aa:92:58:ba:1f:8c:b8:e4:99:77:f8:b1:c3:1e:1e:29:7a:e2:
        98:ad:f1:59:28:3b:df:50:32:a5:d7:9a:db:65:01:a4:26:c8:
        28:db:a4:d3:6a:2b:7b:53:44:0d:c9:22:d7:16:39:fa:bf:ec:
        2d:54:4d:bd:33:03:ec:c1:4e:c6:f9:8d:ac:8b:9d:c8:71:ba:
        99:48:e9:a2:85:db:59:22:35:e5:f0:2e:e6:dd:19:76:dd:25:
        5a:b1:d3:95:41:c4:bf:9e:47:82:e1:98:82:c3:14:95:ac:e3:
        cf:ce
```

項番	説明
(1)	CSR (証明書署名要求) を表示します。

9.5.4 ssl gencsr rsakey

ssl gencsr rsakey	
目的	CSR (証明書署名要求) および CSR の秘密鍵を作成します。
Command	ssl gencsr rsakey [KEY-LENGTH]
Parameter	KEY-LENGTH (省略可能)：RSA 鍵の長さを、512～2048 の範囲で指定します。
デフォルト	RSA 鍵の長さは 2048
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	• 本コマンドを実行して情報を入力する際に、Common Name は省略できません。 • RSA の鍵長が大きいほど、コマンド実行完了までの時間が長くなります。RSA の鍵長を 2048 ビット (省略指定の場合も含む) で指定した場合は、本コマンドの実行完了までに約 2～6 分程度の時間がかかることがあります。
バージョン	1.08.02

使用例：CSR (証明書署名要求) および CSR の秘密鍵を作成する方法を示します。

```
# ssl gencsr rsakey

Country Name (2 letter code) [JP]: JP
State or Province Name (full name) [Some-State]: Tokyo
Locality Name (eg, city) [Some-City]: chiyoda-ku
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]: apresia
Organizational Unit Name (eg, section) []: network
Common Name (YOUR domain name) []: www.apresia.jp
Email Address []: xxx@apresia.jp

 Start generating key ...

 Start generating Certificate Signing Request ...

 Done.
```

9.6 Web 認証コマンド

Web 認証関連の設定コマンドは以下のとおりです。

- web-authentication enable
- web-authentication http-ip
- web-authentication http-port
- web-authentication https-port
- web-authentication redirect disable
- web-authentication redirect url
- web-authentication http-session-timeout
- web-authentication overwrite enable
- web-authentication ttl
- web-authentication redirect-target-url enable
- web-authentication redirect-target-url delay
- web-authentication redirect proxy-port
- web-authentication snooping proxy-port
- web-authentication logging web-access on

9.6.1 web-authentication enable

web-authentication enable	
目的	Web 認証を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	web-authentication enable no web-authentication enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	Web 認証は、ユーザー名とパスワードに基づいて認証を行う機能です。 Web 認証を有効にする前に、以下の設定を行ってください。 • total-client コマンドで認証クライアントの最大数を設定する。 • web-authentication http-ip コマンドで、Web 認証用の Web サーバーの IP アドレスを設定する。 アクセスリストの認証バイパスエントリー(permit authentication-bypass)にマッチした場合は、未認証状態でも中継は許可されます。これにより、認証前に未認証クライアントからの通信を許可することができます（認証バイパス)。 認証に成功して属性値として VLAN ID が通知された場合は、認証に成功したクライアントごとに、受信する VLAN をダイナミックに割り当てることができます（ダイナミック VLAN)。なお、同一ポートに複数の VLAN を割り当てることができます。 その他の Web 認証コマンドは、Web 認証を有効にしている場合のみ使用できます。
制限・注意	• Web 認証を使用する場合は、少なくとも 1 つは IP アドレスを設定した任意の VLAN インターフェースを作成してください。また、IP アドレスを設定した VLAN インターフェースが 1 つもアップしていない場合は認証ページを応答できません。 • ダイナミックに割り当てる VLAN は、あらかじめ作成しておく必要があります。

web-authentication enable	
	• ダイナミック VLAN を使用する際、設定した最大認証端末数に満たない場合でも、VLAN 割り当て時にテーブルのエントリーが重複して、ログインに失敗する可能性があります。
バージョン	1.08.02

使用例：Web 認証を有効にする方法を示します。

```
# configure terminal
(config)# web-authentication enable
(config)#
```

9.6.2 web-authentication http-ip

web-authentication http-ip	
目的	Web 認証用の Web サーバーの IPv4 アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	web-authentication http-ip ipv4 IP-ADDRESS no web-authentication http-ip ipv4
Parameter	ipv4 IP-ADDRESS：Web 認証用の Web サーバーの IPv4 アドレスを設定する場合に指定します。
デフォルト	なし
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	Web 認証用の Web サーバーの IP アドレスは、Web 認証時に認証クライアントが参照する IP アドレスです。
制限・注意	-
バージョン	1.08.02

使用例：Web 認証用の Web サーバーの IPv4 アドレスを 3.3.3.3 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication http-ip ipv4 3.3.3.3
(config-a-def)#
```

9.6.3 web-authentication http-port

web-authentication http-port	
目的	Web 認証用の Web サーバーの、HTTP プロトコルの TCP ポート番号を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	web-authentication http-port TCP-PORT no web-authentication http-port
Parameter	TCP-PORT：Web 認証用の Web サーバーの、追加する HTTP プロトコルの TCP ポート番号を 1～65535 の範囲で指定します。
デフォルト	80
モード	AccessDefender 設定モード
特権レベル	レベル：15

web-authentication http-port	
ガイドライン	デフォルトの TCP ポート番号(80)以外に追加できる HTTP プロトコルの TCP ポート番号は 1 個です。
制限・注意	• 本設定で HTTP プロトコルの TCP ポート番号を追加した場合は、デフォルトの TCP ポート番号(80)と、追加した TCP ポート番号の両方で動作します。 • 以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 123(ntp), 161(snmp), 162(snmptrap), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • ip ssh service-port • snmp-server service-port • snmp-server host • web-authentication https-port • web-authentication redirect proxy-port • web-authentication snooping proxy-port • web-deny-notify http-port • web-deny-notify https-port • radius-server host • tacacs-server host
バージョン	1.08.02

使用例：Web 認証用の Web サーバーの、追加する HTTP プロトコルの TCP ポート番号を 8080 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication http-port 8080
(config-a-def)#
```

9.6.4 web-authentication https-port

web-authentication https-port	
目的	Web 認証用の Web サーバーの、HTTPS プロトコルの TCP ポート番号を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	web-authentication https-port TCP-PORT no web-authentication https-port
Parameter	TCP-PORT：Web 認証用の Web サーバーの、追加する HTTPS プロトコルの TCP ポート番号を 1～65535 の範囲で指定します。
デフォルト	443
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	デフォルトの TCP ポート番号(443)以外に追加できる HTTPS プロトコルの TCP ポート番号は 1 個です。
制限・注意	• 本設定で HTTPS プロトコルの TCP ポート番号を追加した場合は、デフォルトの

web-authentication https-port	
	TCP ポート番号(443)と、追加した TCP ポート番号の両方で動作します。 • 以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 161(snmp), 162(snmptrap), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • ip ssh service-port • snmp-server service-port • snmp-server host • web-authentication http-port • web-authentication redirect proxy-port • web-authentication snooping proxy-port • web-deny-notify http-port • web-deny-notify https-port • radius-server host • tacacs-server host
バージョン	1.08.02

使用例：Web 認証用の Web サーバーの、追加する HTTPS プロトコルの TCP ポート番号を 8443 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication https-port 8443
(config-a-def)#
```

9.6.5 web-authentication redirect disable

web-authentication redirect disable	
目的	Web 認証のログイン認証ページのリダイレクト機能を無効にします。有効にする場合は、no 形式のコマンドを使用します。
Command	web-authentication redirect disable [http | https] no web-authentication redirect disable
Parameter	http（省略可能）：HTTP（TCP ポート 80）パケットのリダイレクトを無効にする場合に指定します。 https（省略可能）：HTTPS（TCP ポート 443）パケットのリダイレクトを無効にする場合に指定します。 http、および https の両方を指定しない場合、HTTP（TCP ポート 80)、および HTTPS（TCP ポート 443）パケットのリダイレクトを無効にします。
デフォルト	ログイン認証ページのリダイレクト機能は有効（no web-authentication redirect disable）
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	リダイレクト機能が有効の場合、ブラウザー以外からの HTTP、HTTPS 通信負荷に

web-authentication redirect disable	
	よって認証性能が著しく低下する可能性があります。
制限・注意	-
バージョン	1.08.02

使用例：Web 認証のログインページのリダイレクト機能を無効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect disable
(config-a-def)#
```

使用例：Web 認証のログインページのリダイレクト機能のうち、HTTPS（TCP ポート 443）パケットのリダイレクトを無効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect disable https
(config-a-def)#
```

9.6.6 web-authentication redirect url

web-authentication redirect url	
目的	Web 認証のログイン認証ページのリダイレクト先 URL を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	web-authentication redirect url URL no web-authentication redirect url
Parameter	URL：リダイレクト先 URL を、最大 255 文字で指定します。
デフォルト	装置の Web 認証用の Web サーバーにリダイレクトされます。
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本機能は、HTTP(80)，HTTPS(443)プロトコルで任意の URL を参照した場合、および web-authentication redirect proxy-port コマンドで指定したプロキシを参照した場合に、強制的に指定した認証ページへリダイレクトさせる機能です。 Web 認証用の Web サーバーの IP アドレスは web-authentication http-ip コマンドで設定します。

制限・注意	• 一度に指定できる URL は 1 つだけです。
	• URL を指定しておらず、クライアントが Web 認証ポートを使用してインターネットにアクセスする場合は、クライアントは web-authentication http-ip コマンドで指定した装置内 Web サーバーの Web 認証ページにリダイレクトされます。
	• デフォルトのリダイレクト先の Web 認証ページは以下のとおりです。
	  • http://<http-ip>:<http-port>/www/AuthLogin.html
	  • https://<http-ip>:<https-port>/www/AuthLogin.html
	• デフォルトでは、HTTP のアクセスは HTTP に、HTTPS のアクセスは HTTPS にリダイレクトされます。
	• 装置の Web 認証ページを明示的に設定する際は、認証 Web サーバーの IP アドレスと TCP ポート番号に加えて、ログインページのパス ("/www/AuthLogin.html") まで指定してください。

web-authentication redirect url	
バージョン	1.08.02

使用例：リダイレクト先を装置の Web 認証ページに設定します（認証 Web サーバーの IP アドレスが 3.3.3.3、HTTP の TCP ポート番号が 8080 の場合）。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect url http://3.3.3.3:8080/www/AuthLogin.html
(config-a-def)#
```

使用例：リダイレクト先 URL を「http://website.com:8081」に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect url http://website.com:8081
(config-a-def)#
```

9.6.7 web-authentication http-session-timeout

web-authentication http-session-timeout	
目的	Web 認証の Web サーバーの、HTTP セッションのタイムアウト時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	web-authentication http-session-timeout SECONDS no web-authentication http-session-timeout
Parameter	SECONDS：タイムアウト時間を 5～60 秒の範囲で指定します。
デフォルト	30 秒
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	• 認証された HTTP クライアントのセッションがタイムアウトすると、TCP 接続が自動的にクリアされます。 • Web 認証で HTTP クライアント用に予約されたセッションは制限されているため、すべてのセッションが占有されている場合は、新しいクライアントは Web 認証を開始できません。タイムアウト時間を設定することで、アイドル状態の TCP 接続を自動的にクリアして、新しいクライアントにセッションを提供できます。
バージョン	1.08.02

使用例：HTTP セッションのタイムアウト時間を 60 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication http-session-timeout 60
(config-a-def)#
```

9.6.8 web-authentication overwrite enable

web-authentication overwrite enable	
目的	Web 認証の上書きログイン機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	web-authentication overwrite enable

web-authentication overwrite enable	
	no web-authentication overwrite enable
Parameter	なし
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本コマンドが無効（デフォルト設定）の場合は、認証済みクライアントから装置の認証ページにアクセスすると認証成功ページが表示されます。 本コマンドを有効にすると、認証済みクライアントから装置の認証ページにアクセスした際に、認証成功ページではなくログインページを表示させて、ユーザー名の上書きログインが行えるように変更できます。 • 同一ユーザー名で上書きログインに成功すると、上書きログイン理由で一度ログアウトしてから、再度ログインします。これにより、ログイン経過時間をリセットできます。 • 異なるユーザー名で上書きログインに成功すると、既存ユーザー名でのログイン状態は上書きログイン理由でログアウトされ、新たに入力したユーザー名でログインします。
制限・注意	• 上書きログイン実行時は、パスワード不一致などで上書きログインの認証に失敗した場合でも、既存ユーザー名でのログイン状態はログアウトされます。
バージョン	1.08.02

使用例：Web 認証の上書きログイン機能を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication overwrite enable
(config-a-def)#
```

9.6.9 web-authentication ttl

web-authentication ttl	
目的	TTL フィルター機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	web-authentication ttl VALUE interface IF-ID [,|-] no web-authentication ttl [VALUE] [interface IF-ID [,|-]]
Parameter	VALUE：IP ヘッダーで使用される TTL 値を、1～255 の範囲で指定します。 interface IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	指定された TTL 値を持つ IP パケットだけが Web 認証を使用して認証を受けることができます。 指定可能 TTL 値はインターフェースごとに最大 8 個です。
制限・注意	-

web-authentication ttl	
バージョン	1.08.02

使用例：ポート 1/0/1 で TTL フィルター機能の TTL 値を 255 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication ttl 255 interface port 1/0/1
(config-a-def)#
```

9.6.10 web-authentication redirect-target-url enable

web-authentication redirect-target-url enable	
目的	Web 認証のログイン認証ページを開く前にアクセスした URL に、Web 認証成功後に自動的にリダイレクトする機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	web-authentication redirect-target-url enable no web-authentication redirect-target-url enable
Parameter	なし
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	AEOS-NP2500 Ver. 1.10.01 以降では、デフォルトのログイン認証ページにコメント文字列 <!-- TARGET_URL --> が追加されています。同様に、認証成功ページにコメント文字列 <!-- REDIRECT_URL --> が追加されています。 カスタマイズした認証ページを利用している環境で本機能を使用する場合、ログイン認証ページと認証成功ページで以下のカスタマイズが必要になります。 • ログイン認証ページ：ログイン用の form タグにおいて、「input type="submit"（送信ボタン）」の次にコメント文字列 <!-- TARGET_URL --> を追加する。 • 認証成功ページ：head タグにおいて、title タグの前にコメント文字列 <!-- REDIRECT_URL --> を追加する。 ■ ログイン認証ページのカスタマイズ例 <form method="POST" action="/cgi-bin/adeflogin.cgi"> 〜〜省略〜〜 <input type="submit" value="login"> <!-- TARGET_URL --> 〜〜省略〜〜 </form> ■ 認証成功ページのカスタマイズ例 <head> 〜〜省略〜〜 <!-- REDIRECT_URL --> <title>APRESIA AccessDefender</title> </head> 認証ページとして外部 Web サーバーを利用している環境で本機能を使用する場合、Web サーバーで以下のカスタマイズが必要です。Web サーバーのカスタマイズはお

web-authentication redirect-target-url enable	
	客様の責任で実施してください。 • 認証端末は、URL パラメーター "target-url" に最初の URL 情報を付与してアクセスしてきます。Web サーバーでは、この URL 情報を読み取り応答する認証ページに反映させるようにカスタマイズ。 • 応答する認証ページでは、ログイン用の form タグにおいて、「input type="submit"(送信ボタン)」の次に、以下属性の input タグを記載 • type 属性：hidden • name 属性："target-url" • value 属性：URL パラメーターから取得した最初の URL 情報 • 例えば、取得した最初の URL 情報が http://www.apresia.jp/ の場合、「input type="submit"(送信ボタン)」の次に <input type=hidden name="target-url" value="http://www.apresia.jp/"> が記載された認証ページを、対象の認証端末に応答するようにカスタマイズします。
制限・注意	• 端末やブラウザーの機能によって自動的にアクセスが発生して認証ページが開いた場合は、その認証ページでの最初の URL は、自動的にアクセスした際の URL 情報になることに注意してください。
バージョン	1.10.01

使用例：Web 認証のログイン認証ページを開く前にアクセスした URL に、Web 認証成功後に自動的にリダイレクトする機能を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect-target-url enable
(config-a-def)#
```

9.6.11 web-authentication redirect-target-url delay

web-authentication redirect-target-url delay	
目的	Web 認証のログイン認証ページを開く前にアクセスした URL に、Web 認証成功後に自動的にリダイレクトする際の遅延時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	web-authentication redirect-target-url delay SECONDS no web-authentication redirect-target-url delay
Parameter	SECONDS：Web 認証成功後に、最初にアクセスした URL に自動的にリダイレクトするまでの遅延時間を、0～60 秒の範囲で指定します。
デフォルト	5 秒
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.10.01

使用例：Web 認証のログイン認証ページを開く前にアクセスした URL に、Web 認証成功後に自動的にリダイレクトする際の遅延時間を、2 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
```

```
(config-a-def)# web-authentication redirect-target-url delay 2
(config-a-def)#
```

9.6.12 web-authentication redirect proxy-port

web-authentication redirect proxy-port	
目的	Web 認証のプロキシリダイレクト機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	web-authentication redirect proxy-port PROXY-PORT no web-authentication redirect proxy-port
Parameter	PROXY-PORT：プロキシポート番号を 1～65535 の範囲で指定します。
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	HTTP プロキシを設定した認証クライアントがプロキシ経由で任意の Web ページに HTTP アクセスした場合に、認証ページへリダイレクトさせます。リダイレクト先は、web-authentication redirect url コマンドの設定に従います。 Web 認証のプロキシリダイレクト機能を有効にする場合は、リダイレクト先の URL がプロキシ経由にならないように、Web ブラウザーのプロキシ設定で例外指定する必要があります。
制限・注意	• 本機能を有効にしても、プロキシ経由（指定したプロキシポート番号宛て）の HTTPS アクセスの場合は、リダイレクトできません。 • 以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 161(snmp), 162(snmptrap), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • ip ssh service-port • snmp-server service-port • snmp-server host • web-authentication http-port • web-authentication https-port • web-authentication snooping proxy-port • web-deny-notify http-port • web-deny-notify https-port • radius-server host • tacacs-server host
バージョン	1.08.02

使用例：Web 認証のプロキシリダイレクト機能を有効にして、プロキシポート番号を 8080 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect proxy-port 8080
```

```
(config-a-def)#
```

9.6.13 web-authentication snooping proxy-port

web-authentication snooping proxy-port	
目的	Web 認証のスヌーピングプロキシ機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	web-authentication snooping proxy-port PROXY-PORT no web-authentication snooping proxy-port
Parameter	PROXY-PORT：プロキシポート番号を 1～65535 の範囲で指定します。
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	HTTP プロキシを設定した認証クライアントがプロキシ経由で任意の Web ページに HTTP アクセスした場合に、自装置の認証ページを直接応答して強制的に表示します。なお、外部サーバーの認証ページは表示できません。 プロキシリダイレクト機能とは異なり、Web ブラウザーのプロキシ設定でリダイレクト先を例外指定しなくても、自装置の認証ページを表示してログイン処理することができます。
制限・注意	• 本機能を有効にしても、プロキシ経由（指定したプロキシポート番号宛て）の HTTPS アクセスの場合は、認証ページを応答できません。 • 以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 161(snmp), 162(snmptrap), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • ip ssh service-port • snmp-server service-port • snmp-server host • web-authentication http-port • web-authentication https-port • web-authentication redirect proxy-port • web-deny-notify http-port • web-deny-notify https-port • radius-server host • tacacs-server host • Web 認証に成功してログインした認証済みクライアントから、プロキシ経由の自装置の認証ページ宛ての HTTP アクセスパケットを受信しても、直接応答することはできません。そのため、本機能を使用する場合でも、自装置の認証ページ宛ての HTTP アクセスがプロキシ経由にならないように、Web ブラウザーのプロキシ設定で例外指定してください。
バージョン	1.08.02

使用例：Web 認証のスヌーピングプロキシ機能を有効にして、プロキシポート番号を 8080 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication snooping proxy-port 8080
(config-a-def)#
```

9.6.14 web-authentication logging web-access on

web-authentication logging web-access on	
目的	Web 認証用の Web サーバーのアクセスログを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	web-authentication logging web-access on no web-authentication logging web-access on
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	アクセスログが有効な場合、Web 認証用の Web サーバーへのアクセスが発生するごとにログエントリーが生成されます。
制限・注意	• ログメッセージの長さは最大 512 文字です。それ以降の文字はすべて破棄されます。 • この機能は、問題のトラブルシューティングを行う際に役に立ちます。通常の動作中は、この機能を無効にすることをお勧めします。
バージョン	1.08.02

使用例：Web 認証用の Web サーバーのアクセスログを有効にする方法を示します。

```
# configure terminal
(config)# web-authentication logging web-access on
(config)#
```

9.7 Web アクセス拒否通知コマンド

Web アクセス拒否通知機能関連の設定コマンドは以下のとおりです。

- web-deny-notify (expert access-list)
- web-deny-notify http-port
- web-deny-notify https-port
- web-deny-notify redirect url

Web アクセス拒否通知機能関連の操作コマンドは以下のとおりです。

- copy (web-deny-notify)
- access-defender erase web-access-deny-page

9.7.1 web-deny-notify (expert access-list)

<table>
<tr><th colspan="2">web-deny-notify (expert access-list)</th></tr>
<tr><td>目的</td><td>拡張エキスパートアクセスリストにおいて、特定端末に対する Web アクセスを拒否し、端末へ拒否されたことを通知するルールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。</td></tr>
<tr><td>Command</td><td>[SEQ] web-deny-notify tcp CONDITION</td></tr>
<tr><td>Parameter</td><td>SEQ (省略可能)：シーケンス番号を 1～65535 の範囲で指定します。小さい番号ほどルールの優先度が高くなります。

tcp：TCP パケットを抽出対象にする場合に指定します。本機能を使用するルールでは必ず指定してください。

CONDITION：使用する抽出条件を指定します。詳細は「Web アクセス拒否通知機能用 拡張エキスパートアクセスリストのタイプごとの抽出条件一覧」と「Web アクセス拒否通知機能用 拡張エキスパートアクセスリストの抽出条件」を参照。</td></tr>
<tr><td>デフォルト</td><td>なし</td></tr>
<tr><td>モード</td><td>拡張エキスパートアクセスリスト設定モード</td></tr>
<tr><td>特権レベル</td><td>レベル：12</td></tr>
<tr><td>ガイドライン</td><td>本ルールにマッチした HTTP、および HTTPS パケットを受信した場合、そのパケットを他のポートへ転送せずに、パケット送信元の端末に対し、Web アクセスができないことを通知する Web ページへリダイレクトさせます。

本機能がサポートする送信元アドレス条件の組み合わせを示します。
<table>
<tr><th colspan="2">送信元</th><th rowspan="2">サポート可否</th></tr>
<tr><th>IP</th><th>MAC</th></tr>
<tr><td>指定なし(any)</td><td>指定なし(any)</td><td>未サポート</td></tr>
<tr><td>指定なし(any)</td><td>特定端末指定</td><td>host 指定の場合のみサポート、マスク指定は未サポート</td></tr>
<tr><td>特定端末指定</td><td>指定なし(any)</td><td>host 指定の場合のみサポート、マスク指定は未サポート</td></tr>
<tr><td>特定端末指定</td><td>特定端末指定</td><td>host 指定の場合のみサポート、マスク指定は未サポート</td></tr>
</table>
本機能では、宛先 IP アドレス条件と宛先 MAC アドレス条件は any で指定してください。</td></tr>
</table>

web-deny-notify (expert access-list)	
	本機能は、受信パケットの宛先 TCP ポート番号が、web-deny-notify http-port、および web-deny-notify https-port で指定された宛先 TCP ポート番号と一致する場合のみ動作します。 本機能を使用し、かつ Web 認証機能を使用しない場合は、HTTP/HTTPS パケットを受信する VLAN に IP アドレスを設定してください。 シーケンス番号を指定せずに設定した場合、開始値（デフォルト設定では 10）から増分値（デフォルト設定では 10）でインクリメントした番号のうち、まだ使用されていない一番小さい番号が自動的に割り当てられます。 開始値と増分値を変更するには、access-list resequence コマンドを使用します。なお、access-list resequence コマンドを実行した時点で、指定したアクセスリストの設定済みルールのシーケンス番号が一括変更されます。 シーケンス番号を手動で割り当てる場合、将来の拡張のためにシーケンス番号を「10、20、30、・・・」と、間を飛ばして設定することもできます。
制限・注意	• CPU が過負荷になることを防止するため、リダイレクトさせるトラフィックのレートは、各ルール毎に最大 256Kbps に制限されています。 • 本設定は構成情報ではアクセスリスト関連（ラベル# ACL）で表示されます。 • シーケンス番号は、アクセスリストの領域内で一意にしてください。すでに存在するシーケンス番号を入力すると、エラーメッセージが表示されます。 • IP プロトコル番号や L4 ポート番号などを数値指定で設定しても、一致する定義済みパラメーターが存在する場合は、構成情報では定義済みパラメーターで表示されます。
バージョン	1.10.01

■ Web アクセス拒否通知機能用 拡張エキスパートアクセスリストのタイプごとの抽出条件一覧

タイプ	送信元			宛先			TCP Flag	ICMP	CoS	VLAN ID	フラグメント	DSCP	クラス ID
	IP	MAC	L4	IP	MAC	L4							
tcp	○	○	○	any	any	○	−	−	○	○	−	○	○

※ 複数の抽出条件を指定する場合は、この表に記載した左側の抽出条件から順番に指定する。
※ 本機能では、宛先 IP アドレス条件、宛先 MAC アドレス条件は any 指定のみサポート。

■ Web アクセス拒否通知機能用 拡張エキスパートアクセスリストの抽出条件
「8.1.6 permit｜deny (expert access-list)」コマンドの「拡張エキスパートアクセスリストの抽出条件」を参照。

使用例：拡張エキスパートアクセスリスト「exp_acl」において、シーケンス番号=11 で「送信元 MAC アドレスが 00-00-5E-00-53-22 からの TCP ポート 80 番の Web アクセスに対して、拒否されたことを示す Web ページを返すためのルール」を設定し、老番のシーケンス番号=12 で「送信元 MAC アドレスが 00-00-5E-00-53-22 からの IPv4 パケットを拒否するルール」を設定する方法を示します。

```
# configure terminal
(config)# expert access-list extended exp_acl
(config-exp-nacl)# 11 web-deny-notify tcp any host 00-00-5E-00-53-22 any any eq 80
(config-exp-nacl)# 12 deny any host 00-00-5E-00-53-22 any any
(config-exp-nacl)#
```

9.7.2 web-deny-notify http-port

web-deny-notify http-port	
目的	Web アクセス拒否通知用 Web サーバーの、HTTP プロトコルの TCP ポート番号を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	web-deny-notify http-port TCP-PORT no web-deny-notify http-port
Parameter	TCP-PORT：Web アクセス拒否通知用 Web サーバーで使用する HTTP プロトコルの TCP ポート番号を 1～65535 の範囲で指定します。
デフォルト	TCP ポート番号：80
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	HTTP プロトコルの TCP ポート番号は 1 個のみ指定できます。本コマンドで HTTP プロトコルの TCP ポート番号を指定すると、デフォルトの TCP ポート番号(80)は使用できなくなります。
制限・注意	• 以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 123(ntp), 161(snmp), 162(snmptrap), 443(HTTPS), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • ip ssh service-port • snmp-server service-port • snmp-server host • web-authentication http-port • web-authentication https-port • web-authentication redirect proxy-port • web-authentication snooping proxy-port • web-deny-notify https-port • radius-server host • tacacs-server host • 本設定は構成情報では Web 認証関連（ラベル# WEB-AUTHENTICATION）で表示されます。
バージョン	1.10.01

使用例：Web アクセス拒否通知用 Web サーバーの、 HTTP プロトコルの TCP ポート番号を 8080 に設定する方法を示します。

```
# configure terminal
(config)# web-deny-notify http-port 8080
(config)#
```

9.7.3 web-deny-notify https-port

web-deny-notify https-port	
目的	Web アクセス拒否通知用 Web サーバーの、HTTPS プロトコルの TCP ポート番号を

web-deny-notify https-port	
	設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	web-deny-notify https-port TCP-PORT no web-deny-notify https-port
Parameter	TCP-PORT：Web アクセス拒否通知用 Web サーバーで使用する HTTPS プロトコルの TCP ポート番号を 1～65535 の範囲で指定します。
デフォルト	TCP ポート番号：443
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	HTTPS プロトコルの TCP ポート番号は 1 個のみ指定できます。本コマンドで HTTPS プロトコルの TCP ポート番号を指定すると、デフォルトの TCP ポート番号(443)は使用できなくなります。
制限・注意	• 以下に示す TCP/UDP ポート番号は指定しないでください。 • 21(ftp), 22(ssh), 23(telnet), 49(tacacs), 67(bootps), 68(bootpc), 69(tftp), 80(http), 123(ntp), 161(snmp), 162(snmptrap), 514(syslog), 546(dhcpv6-client), 547(dhcpv6-server), 520(rip), 521(ripng), 179(BGP), 1812(radius), 1813(radius-acct), 8021, 8022 • 以下コマンドで指定した TCP/UDP ポート番号 • ip telnet service-port • ip ssh service-port • snmp-server service-port • snmp-server host • web-authentication http-port • web-authentication https-port • web-authentication redirect proxy-port • web-authentication snooping proxy-port • web-deny-notify http-port • radius-server host • tacacs-server host • 本設定は構成情報では Web 認証関連（ラベル# WEB-AUTHENTICATION）で表示されます。
バージョン	1.10.01

使用例：Web アクセス拒否通知用 Web サーバーの、HTTPS プロトコルの TCP ポート番号を 8443 に設定する方法を示します。

```
# configure terminal
(config)# web-deny-notify https-port 8443
(config)#
```

9.7.4 web-deny-notify redirect url

web-deny-notify redirect url	
目的	Web アクセス拒否通知ページのリダイレクト先 URL を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	web-deny-notify redirect url URL

web-deny-notify redirect url	
	no web-deny-notify redirect url
Parameter	URL：リダイレクト先 URL を、最大 255 文字で指定します。
デフォルト	装置の Web アクセス拒否通知ページ用の Web サーバーにリダイレクトされます。
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	本コマンドは、web-deny-notify（expert access-list）コマンドで設定したルールに対して応答する、リダイレクト先 URL を設定します。 リダイレクト先として外部サーバーの URL を指定する場合は、拡張エキスパートアクセスリストの web-deny-notify で指定したルールよりも先にマッチするシーケンス番号で、リダイレクト先 URL の外部サーバー宛ての通信を permit もしくは permit authentication-bypass で許可してください。

制限・注意	• 一度に指定できる URL は 1 つだけです。
	• 本設定は構成情報では Web 認証関連（ラベル# WEB-AUTHENTICATION）で表示されます。
	• デフォルトのリダイレクト先の Web アクセス拒否通知ページは以下のとおりです。
	  • http://<パケットを受信した VLAN の IP アドレス>:<web-deny-notify http-port>/www/web-deny-notify.html
	  • https://<パケットを受信した VLAN の IP アドレス>:<web-deny-notify https-port>/www/web-deny-notify.html
	• デフォルトでは、HTTP のアクセスは HTTP に、HTTPS のアクセスは HTTPS にリダイレクトされます。
	• web-authentication http-ip ipv4 コマンドを設定して、装置の Web アクセス拒否通知ページを明示的に指定することもできます。
	  • http://<web-authentication http-ip ipv4 で指定した IP アドレス>:<web-deny-notify http-port>/www/web-deny-notify.html
	  • https://<web-authentication http-ip ipv4 で指定した IP アドレス>:<web-deny-notify https-port>/www/web-deny-notify.html

バージョン	1.10.01

使用例：パケットを受信した VLAN の IP アドレスが 192.168.100.100 の場合に、リダイレクト先を装置の Web アクセス拒否通知ページ（TCP ポート番号：8080）に設定する方法を示します。

```
# configure terminal
(config)# web-deny-notify redirect url http://192.168.100.100:8080/www/web-deny-notify.html
(config)#
```

使用例：リダイレクト先 URL を「http://webdeny.com:8081」に設定する方法を示します。

```
# configure terminal
(config)# web-deny-notify redirect url http://webdeny.com:8081
(config)#
```

9.7.5 copy（web-deny-notify）

copy（web-deny-notify）	
目的	TFTP、SFTP、または SD カードを使用して、Web アクセス拒否通知ページをダウン

copy (web-deny-notify)	
	ロードまたはアップロードします。
Command	■ 装置へのダウンロード copy {flash: [URL] | tftp: [URL] | sftp: [URL]} web-access-deny-page ■ 装置からのアップロード copy web-access-deny-page {flash: [URL] | tftp: [URL] | sftp: [URL]}
Parameter	flash: [URL]：装置のローカルフラッシュまたは SD カードを使用する場合に指定します。URL は省略可能です。 tftp: [URL]：TFTP を使用する場合に指定します。URL は省略可能です。 sftp: [URL]：SFTP を使用する場合に指定します。URL は省略可能です。 URL（省略可能）：ダウンロード元ファイル、またはアップロード先ファイルを指定します。省略可能ですが、指定した場合は、コマンド実行後の入力ダイアログがあらかじめ入力された状態になります。以下に入力書式例を示します。 • flash: c:/FILE：装置のローカルフラッシュ上(c:)のファイルパス指定 • flash: d:/FILE：SD カード上(d:)のファイルパス指定 • tftp: //IP/FILE：TFTP サーバー上のファイルパス指定 • IP：TFTP サーバーの IP アドレス • FILE：ファイルパス名 • sftp: //USER:PASS@IP:TCP/FILE：SFTP サーバー上のファイルパス指定 • USER：ユーザー名 • PASS：パスワード • IP：SFTP サーバーの IP アドレス • TCP：TCP ポート番号、省略可能 • FILE：ファイルパス名
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	Web アクセス拒否通知ページのダウンロード可能な最大ファイルサイズは、5KB (5,120 バイト) です。 ダウンロードしたカスタム Web ページを削除するには、access-defender erase コマンドを使用します。カスタム Web ページが削除された場合は、デフォルトの Web ページを使用します。
制限・注意	• ファイル名には、&:;`'\"|*?~<>^()[]{}$ の各文字は使用できません。 • ファイル名には、「../」の文字列は使用できません。 • スラッシュ文字 (/) は、ディレクトリーを識別するために使用します。 • Web アクセス拒否通知ページでは、画像ファイルは使用できません。 • Web アクセス拒否通知ページでは、UTF-16(BE, LE)、UTF-32(BE, LE)形式で保存された Web ページは正常に表示できないため、使用しないでください。 • Web アクセス拒否通知ページをダウンロードする際、ファイルサイズが仕様制限より大きくてダウンロードに失敗した場合のエラーメッセージは、"ERROR: Not a valid file." と表示されます。
バージョン	1.10.01 1.13.01：sftp:パラメーター追加

使用例：IP アドレス 192.168.1.110 の TFTP サーバーから「my-deny-page.html」ファイルを Web アクセス拒否通知ページとしてダウンロードする方法を示します。

```
# copy tftp: //192.168.1.110/my-deny-page.html web-access-deny-page

Address of remote host [192.168.1.110]?
Source filename [my-deny-page.html]?
Destination filename web-access-deny-page? [y/n]:  y

 Accessing tftp://192.168.1.110/my-deny-page.html...
 Transmission start...
 Transmission finished, file length 72 bytes.
 Please wait, programming flash.............. Done.
```

使用例：IP アドレス 192.168.1.110 の TFTP サーバーに、装置内の Web アクセス拒否通知ページをアップロードして、ファイル名を「my-deny-page.html」に変更する方法を示します。

```
# copy web-access-deny-page tftp: //192.168.1.110/my-deny-page.html

Address of remote host [192.168.1.110]?
Destination filename [my-deny-page.html]?
 Accessing tftp://192.168.1.110/my-deny-page.html...
 Transmission start...
 Transmission finished, file length 72 bytes.
```

9.7.6 access-defender erase web-access-deny-page

access-defender erase web-access-deny-page	
目的	ダウンロードした Web アクセス拒否通知用のカスタム Web ページを削除します。
Command	access-defender erase web-access-deny-page
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	ダウンロードしたカスタム Web ページが削除された場合は、デフォルトの Web ページを使用します。
制限・注意	-
バージョン	1.10.01

使用例：ダウンロードした Web アクセス拒否通知用のカスタム Web ページを削除する方法を示します。

```
# access-defender erase web-access-deny-page
Erasing web-access-deny-page in FLASH.......... Done.
```

9.8 DHCP スヌーピングコマンド

DHCP スヌーピング関連の設定コマンドは以下のとおりです。

- dhcp-snooping enable
- dhcp-snooping interface
- dhcp-snooping mode deny
- dhcp-snooping mode timer
- dhcp-snooping mode mac-authentication
- dhcp-snooping static-entry

DHCP スヌーピング関連の show コマンドは以下のとおりです。

- show access-defender dhcp-snooping configuration
- show access-defender dhcp-snooping mode-status
- show access-defender dhcp-snooping status

9.8.1 dhcp-snooping enable

dhcp-snooping enable	
目的	DHCP スヌーピングを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	dhcp-snooping enable no dhcp-snooping enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	DHCP スヌーピングを有効にすると、未登録のクライアントからの通信（IPv4,ARP）を制限できます。非 IP パケットの通信を制限するには、他の認証機能（MAC 認証、Web 認証、または IEEE 802.1X 認証）と DHCP スヌーピングを同時に使用します。 DHCP スヌーピングを有効にする前に、total-client コマンドで認証クライアントの最大数を設定してください。 登録された DHCP スヌーピングエントリーは、クライアントから DHCP Release パケットを受信するか、DHCP サーバーから払い出されたリース期間が経過すると削除されます。なお、リンクダウンしても DHCP スヌーピングエントリーは削除されません。
制限・注意	• DHCP スヌーピングで登録可能なクライアントの最大数は 400 です。クライアントの最大数は、ダイナミックエントリーとスタティックエントリーで共有です。 • DHCPv6 スヌーピングは未サポートです。
バージョン	1.08.02

使用例：DHCP スヌーピングを有効にする方法を示します。

```
# configure terminal
(config)# dhcp-snooping enable
(config)#
```

9.8.2 dhcp-snooping interface

dhcp-snooping interface	
目的	インターフェースの DHCP スヌーピングを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	dhcp-snooping interface IF-ID [,|-] no dhcp-snooping interface IF-ID [,|-]
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • port-channel <1-48>：ポートチャネル指定
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	DHCP スヌーピングを有効にしたインターフェースでは、動作モードにかかわらず DHCP サーバーからの DHCP offer パケットを破棄します。これにより、不正に設置された DHCP サーバーによる IP アドレスの配布を防止します。
制限・注意	• DHCP スヌーピングとゲートウェイ認証は併用できません。 • ポートチャネルで DHCP スヌーピングを有効にする場合は、ポートチャネルを指定して設定します。ポートチャネルのメンバーポート（物理ポート）を指定して設定しないでください。
バージョン	1.08.02

使用例：ポート 1/0/1 で DHCP スヌーピングを有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping interface port 1/0/1
(config-a-def)#
```

9.8.3 dhcp-snooping mode deny

dhcp-snooping mode deny	
目的	DHCP スヌーピングの動作モードを DENY モードに設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	dhcp-snooping mode deny no dhcp-snooping mode deny
Parameter	なし
デフォルト	無効（PERMIT モードに設定）
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	DENY モードの場合は、登録されたクライアントからの通信（IPv4,ARP）が許可され、それ以外のクライアントからの通信（IPv4,ARP）が制限されます。 PERMIT モードの場合は、登録されたクライアントだけでなく、未登録クライアントからの通信（IPv4,ARP）も許可されます。
制限・注意	-
バージョン	1.08.02

使用例：DHCP スヌーピングの動作モードを DENY モードに設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping mode deny
(config-a-def)#
```

9.8.4 dhcp-snooping mode timer

dhcp-snooping mode timer	
目的	DHCP スヌーピングの動作モード自動切り替えタイマーを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	dhcp-snooping mode timer SECONDS no dhcp-snooping mode timer
Parameter	SECONDS：DHCP スヌーピングの動作モード自動切り替えタイマーを、0 または 30～604,800 秒の範囲で指定します。0 指定時は PERMIT モード固定になります。
デフォルト	1800 秒
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本コマンドでタイマーを設定すると、DHCP スヌーピングの動作モードは PERMIT モードになり、自動切り替えタイマーが指定した値で開始されます。 自動切り替えタイマーが満了すると、DHCP スヌーピングの動作モードは DENY モードに切り替わります。
制限・注意	-
バージョン	1.08.02

使用例：DHCP スヌーピングの動作モード自動切り替えタイマーを 600 秒に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping mode timer 600
(config-a-def)#
```

9.8.5 dhcp-snooping mode mac-authentication

dhcp-snooping mode mac-authentication	
目的	DHCP スヌーピングの MAC 認証モードを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	dhcp-snooping mode mac-authentication no dhcp-snooping mode mac-authentication
Parameter	なし
デフォルト	無効
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	本コマンドは、DHCP スヌーピングと MAC 認証の両方が有効になっているインターフェースで動作します。DHCP スヌーピングの MAC 認証モードを有効にすると、クライアントの DHCP パケットは、MAC 認証に成功するまで、DHCP スヌーピングお

dhcp-snooping mode mac-authentication	
	よび DHCP サーバーの対象になることはできません。 インターフェースで有効になっている認証機能が MAC 認証だけでない場合は、クライアントの DHCP パケットは、認証に成功する前に DHCP スヌーピングと DHCP サーバーの対象になることができます。
制限・注意	-
バージョン	1.08.02

使用例：DHCP スヌーピングの MAC 認証モードを有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping mode mac-authentication
(config-a-def)#
```

9.8.6 dhcp-snooping static-entry

dhcp-snooping static-entry	
目的	DHCP スヌーピングのスタティックエントリーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	**dhcp-snooping static-entry interface** IF-ID IP-ADDRESS **no dhcp-snooping static-entry** [**interface** IF-ID] [IP-ADDRESS]
Parameter	interface IF-ID：スタティックエントリーを接続するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 IP-ADDRESS：スタティックエントリーの IP アドレスを指定します。
デフォルト	スタティックエントリーの設定なし
モード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	インターフェースおよび IP アドレスが同一のスタティックエントリーが、すでにダイナミックエントリーに登録済みの場合は、そのスタティックエントリーはダイナミックエントリーを上書きします。 スタティックエントリーを登録している状態で別の認証機能と併用する場合は、その認証機能を有効にした後に、DHCP スヌーピングを有効にします。 パラメーターを指定せずに no dhcp-snooping static-entry コマンドを使用すると、すべてのスタティックエントリーを削除します。パラメーターを指定して no dhcp-snooping static-entry コマンドを使用すると、指定したスタティックエントリーのみを削除します。
制限・注意	• DHCP スヌーピングで登録可能なクライアントの最大数は、ダイナミックエントリーとスタティックエントリーで共有です。 • DHCP スヌーピングのスタティックエントリー設定がある状態では、total-client 設定は変更できません。 • DHCPv6 スヌーピングは未サポートです。
バージョン	1.08.02

使用例：ポート 1/0/1、IP アドレス 192.0.2.1 のスタティックエントリーを設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping static-entry interface port 1/0/1 192.0.2.1
(config-a-def)#
```

9.8.7 show access-defender dhcp-snooping configuration

show access-defender dhcp-snooping configuration	
目的	DHCP スヌーピングの設定を表示します。
Command	show access-defender dhcp-snooping configuration
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCP スヌーピングの設定を表示する方法を示します。

```
# show access-defender dhcp-snooping configuration

 Port configuration (o: snooping ON) ...(1)
         C Port
           1       8 9
           +-------+ +---
         1 oooo.... ....

 Snooping : ENABLE ...(2)
 Mode     : PERMIT ...(3)
 Mode     : MAC Authentication Mode ...(4)
 Timer    : 1800 ...(5)

 Port-channel configuration (o: snooping ON) ...(6)
                  C Port-channel ID
                    1       8 9      16 17    24 25    32 33    40 41    48
                    +-------+ +-------+ +-------+ +-------+ +-------+ +-------+
 Port-channel      1 o....... ........ ........ ........ ........ ........
 (7)
 Static Entry :
 Port            IP Address
 ------------------------------------------------------
 Port1/0/1       192.0.2.100
 Port-channel1   192.0.2.200
```

項番	説明
(1)	ポートごとの DHCP スヌーピングの有効／無効を表示します。 "C"列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。
(2)	DHCP スヌーピングの有効(ENABLE)／無効(DISABLE)を表示します。
(3)	DHCP スヌーピングの動作モード手動切り替えコマンド（dhcp-snooping mode deny）の設定（DENY：コマンド設定時／PERMIT：コマンド未設定時）を表示します。
(4)	DHCP スヌーピングの MAC 認証モードが有効な場合に表示されます。無効な場合には表示されません。

項番	説明
(5)	DHCP スヌーピングの動作モード自動切り替えタイマーの設定を表示します。
(6)	ポートチャネルごとの DHCP スヌーピングの有効／無効を表示します。 "C"列はスタックのボックス ID を示しますが、ここでは常に 1 が表示されます。
(7)	スタティックエントリーを表示します。

9.8.8 show access-defender dhcp-snooping mode-status

show access-defender dhcp-snooping mode-status	
目的	DHCP スヌーピングの動作モードを表示します。
Command	show access-defender dhcp-snooping mode-status
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCP スヌーピングの動作モードを表示する方法を示します。

```
# show access-defender dhcp-snooping mode-status
 (1)         (2)             (3)
 Mode        Timer           Remaining time
 ------------------------------------
 PERMIT      0:00:30:00      0:00:05:20
 MAC AUTH    -:--:--:--      -:--:--:--
```

項番	説明
(1)	DHCP スヌーピングの動作モードを表示します。MAC AUTH 行は DHCP スヌーピングの MAC 認証モードが有効な場合に表示されます。無効な場合には表示されません。
(2)	DHCP スヌーピングの動作モード自動切り替えタイマーの設定を表示します。
(3)	PERMIT モードから DENY モードに自動的に切り替えるまでの残り時間を表示します。

9.8.9 show access-defender dhcp-snooping status

show access-defender dhcp-snooping status	
目的	DHCP スヌーピングエントリーを表示します。
Command	show access-defender dhcp-snooping status
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：DHCP スヌーピングエントリーを表示する方法を示します。

```
# show access-defender dhcp-snooping status

 Snooping : ENABLE ...(1)
 Mode     : DENY ...(2)
 Mode     : MAC Authentication Mode ...(3)

 C = port-channel, LE = Lease Expiration

 Total : 3 (static 1, dynamic 2) ...(4)
 (5)          (6)                                    (7)                (8)
 Port         IP Address                             MAC Address        LE
 ------------------------------------------------------------------------------
 Port1/0/2    192.0.2.100                            00-00-5E-00-53-22  0d23hr
 C/1          192.0.2.101                            00-00-5E-00-53-11  0:04:57
 Port1/0/5    192.0.2.250                            N/A                -
```

項番	説明
(1)	DHCP スヌーピングの有効(ENABLE)／無効(DISABLE)を表示します。
(2)	DHCP スヌーピングの動作モードを表示します。 DENY：DENY モード（登録されたクライアントからの通信は許可、それ以外は制限） PERMIT：PERMIT モード（未登録クライアントからの通信も許可）
(3)	DHCP スヌーピングの MAC 認証モードが有効な場合に表示されます。無効な場合には表示されません。
(4)	DHCP スヌーピングのエントリー数（スタティックエントリー数とダイナミックエントリー数）を表示します。
(5)	DHCP スヌーピングエントリーのポート番号またはポートチャネル番号を表示します。
(6)	DHCP サーバーによって提供されるクライアント IP アドレスを表示します。
(7)	DHCP スヌーピングエントリーの MAC アドレスを表示します。スタティックエントリーでは、MAC アドレスは表示されません。
(8)	DHCP スヌーピングエントリーのリース期間を表示します。スタティックエントリーではリース期間は表示されません。 10 時間未満の場合は、9:33:12 のように（時):(分):(秒）の形式で表示されます。10 時間を超える場合は、3d5hr のように（日)d(時)hr の形式で表示されます。

9.9 ARP スヌーピングコマンド

ARP スヌーピング関連の設定コマンドは以下のとおりです。

- arp snooping global enable
- arp snooping enable
- arp snooping probe interval
- arp snooping probe count
- arp snooping max-entry
- aaa accounting delay-start

ARP スヌーピング関連の show／操作コマンドは以下のとおりです。

- show arp snooping configuration
- show arp snooping
- clear arp snooping

9.9.1 arp snooping global enable

arp snooping global enable	
目的	ARP スヌーピングのグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	arp snooping global enable no arp snooping global enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ARP スヌーピングを有効にすると、受信した ARP パケットから IP アドレス情報を取得して ARP スヌーピングエントリーを登録します。1 つの ARP スヌーピングエントリーには以下の情報が含まれます。 • IPv4 アドレス（ARP ヘッダーの Sender IP address フィールド） • MAC アドレス（ARP ヘッダーの Sender hardware address フィールド） • 受信ポート番号、もしくは受信ポートチャネル番号 • 受信した VLAN ID 「ARP スヌーピング」「アカウンティング遅延設定(aaa accounting delay-start)」「AccessDefender のアカウンティング(aaa accounting network)」を併用することで、MAC 認証、IEEE 802.1X 認証、IEEE 802.1X/MAC 認証(AND)のログイン成功ログ(A-Def : <auth-type> : login succeeded)、およびこのログに付随して出力されるアカウンティングパケットに、IPv4 アドレス情報を付与することができるようになります。
制限・注意	-
バージョン	1.10.02

使用例：ARP スヌーピングのグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# arp snooping global enable
(config)#
```

9.9.2 arp snooping enable

arp snooping enable	
目的	ARP スヌーピングのインターフェースごとの設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	arp snooping enable no arp snooping enable
Parameter	なし
デフォルト	無効
モード	インターフェース設定モード(port, range, port-channel)
特権レベル	レベル：12
ガイドライン	ポートチャネルで設定する場合は、対象ポートチャネルのインターフェース設定モード（interface port-channel コマンド）で設定してください。
制限・注意	-
バージョン	1.10.02

使用例：ポート 1/0/1 で、ARP スヌーピングを有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# arp snooping enable
(config-if-port)#
```

9.9.3 arp snooping probe interval

arp snooping probe interval	
目的	ARP プローブの送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	arp snooping probe interval SECONDS no arp snooping probe interval
Parameter	SECONDS：ARP プローブの送信間隔を 30～1,814,400 秒の範囲で指定します。
デフォルト	30 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• 運用中に ARP プローブの送信間隔が変更された場合は、変更前の送信間隔で次のタイミングの ARP プローブを送信した後に、新たに設定した送信間隔で動作するようになります。
バージョン	1.10.02

使用例：ARP プローブの送信間隔を 1800 秒に設定する方法を示します。

```
# configure terminal
(config)# arp snooping probe interval 1800
(config)#
```

9.9.4 arp snooping probe count

arp snooping probe count	
目的	ARP プローブの受信タイムアウト回数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	arp snooping probe count VALUE no arp snooping probe count
Parameter	VALUE：ARP プローブの受信タイムアウト回数を 1～255 回の範囲で指定します。
デフォルト	3 回
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ARP プローブは、指定した送信間隔でエントリーごとに送信し監視されます。送信した ARP プローブに対する応答が無い状況が、指定した受信タイムアウト回数連続した場合に、対象エントリーが削除されます。
制限・注意	• 運用中に ARP プローブの受信タイムアウト回数が変更された場合は、登録済みエントリーの受信タイムアウト回数は 0 回にリセットされます。
バージョン	1.10.02

使用例：ARP プローブの受信タイムアウト回数を 2 回に設定する方法を示します。

```
# configure terminal
(config)# arp snooping probe count 2
(config)#
```

9.9.5 arp snooping max-entry

arp snooping max-entry	
目的	ARP スヌーピングエントリーの最大数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	arp snooping max-entry VALUE no arp snooping max-entry
Parameter	VALUE：ARP スヌーピングエントリーの最大数を 1～1024 の範囲で指定します。
デフォルト	1024
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドは ARP スヌーピングのグローバル設定が無効な状態で設定します。
制限・注意	-
バージョン	1.10.02

使用例：ARP スヌーピングエントリーの最大数を 256 に設定する方法を示します。

```
# configure terminal
(config)# arp snooping max-entry 256
(config)#
```

9.9.6 aaa accounting delay-start

aaa accounting delay-start	
目的	アカウンティング遅延設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	aaa accounting delay-start [delay SECONDS] [retry VALUE] no aaa accounting delay-start
Parameter	delay SECONDS（省略可能）：遅延時間を 1～3 秒の範囲で指定します。指定しない場合は 2 秒に設定されます。 retry VALUE（省略可能）：ARP スヌーピングエントリーから IP アドレス情報を取得する処理のリトライ回数を、0～3 回の範囲で指定します。指定しない場合は 1 回に設定されます。
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	本コマンドは、「ARP スヌーピング」と「AccessDefender のアカウンティング(aaa accounting network)」を併用して使用します。 本機能を有効にすると、MAC 認証、IEEE 802.1X 認証、IEEE 802.1X/MAC 認証(AND)のログイン成功ログ(A-Def：<auth-type>：login succeeded)、およびこのログに付随して出力されるアカウンティングパケットに、IPv4 アドレス情報を付与することができるようになります。 MAC 認証、IEEE 802.1X 認証、IEEE 802.1X/MAC 認証(AND)でログインに成功すると、対象クライアントの MAC アドレスに関連付けられた IPv4 アドレスを、ARP スヌーピングエントリーから取得することを試みます。指定した遅延時間とリトライ回数が満了するまでの間に取得できた場合には、以下に IPv4 アドレス情報が付与されます。 • show access-defender client のクライアントの IP アドレス。 • ログイン成功ログ(A-Def : <auth-type> : login succeeded)に IPv4 アドレス情報が付与される。また、このログイン成功ログに付随して出力されるアカウンティングパケットに、IPv4 アドレス情報 (Framed-IP-Address 属性) が付与される。 • ログアウトログ(A-Def : <auth-type> : logout (<reason>))に IPv4 アドレス情報が付与される。また、このログアウトログに付随して出力されるアカウンティングパケットに、IPv4 アドレス情報 (Framed-IP-Address 属性) が付与される。 なお、ARP スヌーピングエントリーから IPv4 アドレス情報を取得できなかった場合には、IPv4 アドレス情報は付与されません。 本機能を有効にすると、MAC 認証、IEEE 802.1X 認証、IEEE 802.1X/MAC 認証(AND)のログイン成功ログ(A-Def：<auth-type>：login succeeded)に、ログインに成功した時間情報も付与されるようになります。
制限・注意	• 本設定は構成情報では AAA 関連 (ラベル# AAA) で表示されます。
バージョン	1.10.02

使用例：アカウンティング遅延設定を、遅延時間 3 秒、リトライ回数 3 回で設定する方法を示します。

```
# configure terminal
(config)# aaa accounting delay-start delay 3 retry 3
```

```
(config)#
```

9.9.7 show arp snooping configuration

show arp snooping configuration	
目的	ARP スヌーピングの構成情報を表示します。
Command	show arp snooping configuration
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.10.02

使用例：ARP スヌーピングの構成情報を表示する方法を示します。

```
# show arp snooping configuration

ARP Snooping Global Configuration
        Status          : Enabled ...(1)
        Max Entries     : 256 ...(2)
        Probe Count     : 2 ...(3)
        Probe Interval  : 1800s ...(4)

ARP Snooping Port Configuration
 (5)                (6)
 Interface          Status
 ------------       ----------
 Port1/0/1          Enabled
 Port1/0/2          Enabled
 Port1/0/3          Enabled
 Port1/0/4          Disabled
 Port1/0/5          Disabled
～～省略～～
```

項番	説明
(1)	ARP スヌーピングのグローバル設定の有効(Enabled)／無効(Disabled)を表示します。
(2)	ARP スヌーピングエントリーの最大数を表示します。
(3)	ARP プローブの受信タイムアウト回数を表示します。
(4)	ARP プローブの送信間隔(秒)を表示します。
(5)	ポート番号またはポートチャネル番号を表示します。
(6)	ARP スヌーピングのインターフェースごとの設定の有効(Enabled)／無効(Disabled)を表示します。

9.9.8 show arp snooping

show arp snooping	
目的	ARP スヌーピングエントリーを表示します。
Command	show arp snooping [IP-ADDRESS [MASK] | interface {IF-ID | vlan VLAN-ID} | MAC-ADDRESS]

show arp snooping	
Parameter	IP-ADDRESS［MASK］（省略可能）：表示するエントリーの IPv4 アドレスを指定します。サブネットマスクを指定することにより、ネットワークアドレスを指定することも可能です。 interface IF-ID（省略可能）：エントリーを表示するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 interface vlan VLAN-ID（省略可能）：エントリーを表示する VLAN ID を指定します。 MAC-ADDRESS（省略可能）：表示するエントリーの MAC アドレスを、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX）
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	オプションパラメーターを指定しない場合は、すべての ARP スヌーピングエントリーが表示されます。
制限・注意	-
バージョン	1.10.02

使用例：すべての ARP スヌーピングエントリーを表示する方法を示します。

```
# show arp snooping
(1)              (2)                (3)            (4)
IP Address       Hardware Addr      Interface      VID
---------------- ------------------ -------------- ----
10.1.100.123     00-00-5E-00-53-87 1/0/2          50
192.0.2.101      00-00-5E-00-53-23 1/0/1          10

Total Entries: 2
```

項番	説明
(1)	IPv4 アドレス（ARP ヘッダーの Sender IP address フィールド）を表示します。
(2)	MAC アドレス（ARP ヘッダーの Sender hardware address フィールド）を表示します。
(3)	ポート番号またはポートチャネル番号を表示します。
(4)	VLAN ID を表示します。

9.9.9 clear arp snooping

clear arp snooping	
目的	ARP スヌーピングエントリーを削除します。
Command	clear arp snooping {all | IP-ADDRESS | interface {IF-ID | vlan VLAN-ID} | MAC-ADDRESS}
Parameter	all：すべての ARP スヌーピングエントリーを削除する場合に指定します。

clear arp snooping	
	IP-ADDRESS：削除するエントリーの IPv4 アドレスを指定します。 interface IF-ID：エントリーをすべて削除するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定 • port-channel <1-48>：ポートチャネル指定 interface vlan VLAN-ID：エントリーをすべて削除する VLAN ID を指定します。 MAC-ADDRESS：削除するエントリーの MAC アドレスを、以下のいずれかの形式で指定します。 • 1 バイトごとにハイフン区切り形式（例：XX-XX-XX-XX-XX-XX） • 1 バイトごとにコロン区切り形式（例：XX:XX:XX:XX:XX:XX） • 2 バイトごとにドット区切り形式（例：XXXX.XXXX.XXXX） • 区切り文字を使用しない形式（例：XXXXXXXXXXXX）
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.10.02

使用例：すべての ARP スヌーピングエントリーを削除する方法を示します。

```
# clear arp snooping all
#
```

10 サポート

10.1 デバッグコマンド

デバッグ関連のコマンドは以下のとおりです。

- debug enable
- debug clear buffer
- debug clear cpu port
- debug clear error-log
- debug copy
- debug output
- debug reboot on-error
- debug show access-defender internal-resource
- debug show buffer
- debug show cpu port
- debug show cpu utilization
- debug show error-log
- debug show inetstat
- debug show memory-pool
- debug show netstat
- debug show output
- debug show ps
- debug show tcpstat
- debug show udpstat
- debug show wd-error-log
- debug stack restart
- show tech-support
- debug show tech-support

10.1.1 debug enable

debug enable	
目的	デバッグメッセージ出力オプションを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	debug enable no debug enable
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：デバッグメッセージ出力オプションを有効にして、その後、無効にする方法を示します。

```
# configure terminal
(config)# debug enable
(config)#
(config)# no debug enable
(config)#
```

10.1.2 debug clear buffer

debug clear buffer	
目的	デバッグバッファーの情報を削除します。
Command	debug clear buffer
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：デバッグバッファーの情報を削除する方法を示します。

```
# debug clear buffer
Clear debug-buffer? (y/n) [n]  y
```

10.1.3 debug clear cpu port

debug clear cpu port	
目的	CPU にトラップされたパケットのうち、各プロトコル処理に伝搬された制御パケットの統計情報を消去します。
Command	debug clear cpu port
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：CPU にトラップされたパケットのうち、各プロトコル処理に伝搬された制御パケットの統計情報を消去する方法を示します。

```
# debug clear cpu port
#
```

10.1.4 debug clear error-log

debug clear error-log	
目的	エラーログの情報を削除します。
Command	debug clear error-log
Parameter	なし

debug clear error-log	
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：エラーログの情報を削除する方法を示します。

```
# debug clear error-log
Clear error-log? (y/n) [n]  y
```

10.1.5 debug copy

debug copy	
目的	宛先ファイル名のファイルにデバッグ情報をコピーします。
Command	**debug copy** SOURCE **tftp:** //IP/FILE **debug copy** SOURCE **ftp:** //USER:PASS@IP:TCP/FILE **debug copy** SOURCE **sftp:** //USER:PASS@IP:TCP/FILE **debug copy** SOURCE {**c:**/FILE | **d:**/FILE}
Parameter	SOURCE：コピー元を、以下のいずれかのパラメーターで指定します。 • buffer：デバッグバッファー • error-log：エラーログ ※SFTP ではコピー不可 • tech-support：技術サポート情報 ※FTP/SFTP ではコピー不可 • cpu-trace-history：平均 CPU 使用率がしきい値を上回った場合に採取された CPU に関する履歴ログ ※FTP ではコピー不可 tftp: //IP/FILE：TFTP サーバーをコピー先に指定します。 • IP：TFTP サーバーの IP アドレス • FILE：ファイルパス名 ftp: //USER:PASS@IP:TCP/FILE：FTP サーバーをコピー先に指定します。 sftp: //USER:PASS@IP:TCP/FILE：SFTP サーバーをコピー先に指定します。 • USER：ユーザー名 • PASS：パスワード • IP：FTP/SFTP サーバーの IP アドレス • TCP：TCP ポート番号、省略可能 • FILE：ファイルパス名 c:/FILE：装置のローカルフラッシュ(c:)をコピー先に指定します。 d:/FILE：SD カード(d:)をコピー先に指定します。 • FILE：ファイルパス名
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	なし
制限・注意	• スタック構成において tech-support 指定で本コマンドを実行する場合、マスター以外の装置の出力結果は約 4 メガバイトに制限されます。超過した以降の部分は出力

debug copy	

	されません。
	• 本装置では 4 メガバイト以上の構成情報は使用できません。超過した状態で tech-support 指定で本コマンドを実行すると、先頭から約 4 メガバイトまでの構成情報は出力結果に含まれますが、超過した以降の部分は含まれません。
	• デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在するサーバーを指定して本コマンドを実施する場合、TFTP と FTP/SFTP で動作が異なります。詳細については copy コマンドの制限事項と同等のため、そちらを参照してください。
	  • 宛先(1):デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク
	  • 宛先(2):デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク
	• 本コマンドを SFTP で使用する場合は、IPv6 アドレスでの使用は未サポートです。SFTP を使用する場合は IPv4 アドレスで使用してください。

バージョン	1.08.02 1.10.01:cpu-trace-history パラメーター追加 1.13.01:sftp:パラメーター追加

使用例:デバッグのエラーログ情報を TFTP サーバー (10.90.90.99) にコピーする方法を示します。

```
# debug copy error-log tftp: //10.90.90.99/abc.txt

Address of remote host [10.90.90.99]?
Destination filename [abc.txt]?
 Accessing tftp://10.90.90.99/abc.txt...
Transmission starts...
Finished network upload(65739) bytes.
```

使用例:デバッグバッファーの情報をローカルフラッシュにコピーする方法を示します。

```
# debug copy buffer c:/abc.txt

Copy debug-buffer to /c:/abc.txt? (y/n) [n]  y

Please wait, copy debug buffer to flash.............. 100 %
```

使用例:デバッグバッファーの情報を SD カードにコピーする方法を示します。

```
# debug copy buffer d:/abc.txt

Copy debug-buffer to /d:/abc.txt? (y/n) [n]  y

Please wait, copy debug buffer to flash.............. 100 %
```

10.1.6 debug output

debug output	
目的	デバッグメッセージを出力するモジュールを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	debug output {module MODULE-LIST | all} {buffer | console} no debug output {module MODULE-LIST | all}

debug output	
Parameter	MODULE-LIST：デバッグメッセージを出力するモジュールのリストを指定します。各モジュールの間には、スペースを挿入してください。また、モジュールのリストの先頭と末尾には、ダブルクォーテーションを挿入してください。（例："MMRP"） all：全モジュールのデバッグメッセージを出力する場合に指定します。 buffer：デバッグメッセージをデバッグバッファーに出力する場合に指定します。 console：デバッグメッセージをローカルコンソールに出力する場合に指定します。
デフォルト	バッファー
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	指定したモジュールのデバッグメッセージの出力先を指定するコマンドです。出力先として、バッファー、またはローカルコンソールを指定できます。モジュールの文字列情報を表示する場合、debug show output コマンドを使用します。デフォルトでは、モジュールのデバッグメッセージはデバッグバッファーに出力されます。 モジュールのデバッグメッセージは、モジュールのデバッグ設定が有効で、グローバルモードの debug enable コマンドが有効の場合に出力されます。
制限・注意	-
バージョン	1.08.02

使用例：全モジュールのデバッグメッセージをデバッグバッファーに出力する方法を示します。

```
# debug output all buffer
#
```

使用例：指定したモジュール（MMRP）のデバッグメッセージを、デバッグコンソールに出力する方法を示します。

```
# debug output module "MMRP" console
#
```

10.1.7 debug reboot on-error

debug reboot on-error	
目的	重大なエラーが発生した場合に、装置を再起動させる機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	debug reboot on-error no debug reboot on-error
Parameter	なし
デフォルト	有効（debug reboot on-error）
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：重大なエラーが発生した場合に、装置を再起動させる機能を有効にする方法を示します。

```
# configure terminal
(config)# debug reboot on-error
(config)#
```

10.1.8 debug show access-defender internal-resource

debug show access-defender internal-resource	
目的	AccessDefender の内部リソースの情報を表示します。
Command	debug show access-defender internal-resource
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはトラブルシューティング用のコマンドとなります。技術サポート担当者が問題の分析を行うために収集をお願いすることがあります。
制限・注意	-
バージョン	1.08.02

使用例：AccessDefender の内部リソースの情報を表示する方法を示します。

※AEOS-NP2500 Ver. 1.12.01 時点の表示例

```
# debug show access-defender internal-resource

Name: Resource name
Current: Used number of each resource
Max: Maximum(Total) number of each resource
Count: Count that number of used resource has reached the maximum
Time: The latest time when number of used resource has reached the maximum

Name                    Current/   Max  Count Time
-------------------------------------------------------------
MacAuthDB                     0/  4000      0
802.1x AuthDB                 0/  4096      0
802.1x VirtualPortDB          0/  4096      0
DHCPSNP-BSTEntryDB            0/  1024      0
DHCPSNP-BindEntryDB           0/   400      0
IP-BindInfoDB                 0/   400      0
DHCPV6SNP-BSTEntryDB          0/   511      0
IPV6SNP-BindEntryDB           0/   400      0
IPV6-BindInfoDB               0/   400      0
AD-ACL                        0/     -      0
Author-DB                     0/ 12400      0
WebAuth-HostDB                0/  4000      0
WebAuth-ConnectionDB          0/  1024      0
WebAuth-TcpPortDB             0/  1024      0
Web-Connection                0/   128      0
Web-ConnectionV6              0/   128      0
Security-client-DB            0/  4096      0
Security-client-cache         0/    64      0
Security-client-p-cache       0/  4096      0
```

10.1.9 debug show buffer

debug show buffer	
目的	デバッグバッファーの内容、または使用情報を表示します。

debug show buffer	
Command	debug show buffer [utilization]
Parameter	utilization（省略可能）：デバッグバッファーの使用率を表示する場合に指定します。指定しない場合、バッファーの内容が表示されます。
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：デバッグバッファーの情報を表示する方法を示します。

```
# debug show buffer

Debug buffer is empty
```

使用例：デバッグバッファーの使用率を表示する方法を示します。

```
# debug show buffer utilization

Allocate from       : System memory pool
Total size          : 2.0 MB
Utilization rate    : 30%
```

10.1.10 debug show cpu port

debug show cpu port	
目的	CPU にトラップされたパケットのうち、各プロトコル処理に伝搬された制御パケットの統計情報を表示します。
Command	debug show cpu port [l2 | l3 [unicast | multicast] | protocol NAME | security]
Parameter	l2（省略可能）：レイヤー2 関連の処理に伝搬された制御パケットの統計情報を表示する場合に指定します。 l3（省略可能）：レイヤー3 関連の処理に伝搬された制御パケットの統計情報を表示する場合に指定します。 • unicast（省略可能）：ユニキャストルーティングプロトコル、およびその他のレイヤー3 機能関連の制御パケットの統計情報を表示する場合に指定します。 • multicast（省略可能）：レイヤー3 マルチキャスト関連の制御パケットの統計情報を表示する場合に指定します。 protocol NAME（省略可能）：統計情報を表示するプロトコル名を指定します。大文字と小文字は区別されます。 security（省略可能）：セキュリティー関連の処理に伝搬された制御パケットの統計情報を表示する場合に指定します。
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはトラブルシューティング用のコマンドとなります。技術サポート担当者が問題の分析を行うために収集をお願いすることがあります。
制限・注意	-

debug show cpu port	
バージョン	1.08.02

使用例：CPU にトラップされたパケットのうち、各プロトコル処理に伝搬された制御パケットの統計情報を表示する方法を示します。

```
# debug show cpu port

Type                              PPS         Total       Drop
--------------------------------- ---------- ----------- -----------
LACP                                        0           0           0
802.1X                                      0           0           0
Stacking                                    0           0           0
STP                                         0           0           0
CFM                                         0           0           0
LLDP                                        0           0           0
CTP                                         0           0           0
DHCPv6                                      0           0           0
ERPS                                        0           0           0
OAM                                         0           0           0
ARP                                         0          22          14
ICMP                                        0           0           0
NDP                                         0           0           0
ICMPv6                                      0           0           0
SNTP                                        0           0           0
TFTP                                        0           0           0
Telnet                                      0           0           0
MMRP                                        0           0           0
MAC-auth                                    0           0           0
WEB-auth                                    0           0           0
RADIUS                                      0           0           0
```

使用例：CPU にトラップされたパケットのうち、レイヤー2 関連の処理に伝搬された制御パケットの統計情報を表示する方法を示します。

```
# debug show cpu port l2

Type                              PPS         Total       Drop
--------------------------------- ---------- ----------- -----------
LACP                                        0           0           0
Stacking                                    0           0           0
STP                                         0           0           0
CFM                                         0           0           0
LLDP                                        0           0           0
CTP                                         0           0           0
ERPS                                        0           0           0
OAM                                         0           0           0
MMRP                                        0           0           0
```

使用例：CPU にトラップされたパケットのうち、セキュリティー関連の処理に伝搬された制御パケットの統計情報を表示する方法を示します。

```
# debug show cpu port security

Type                              PPS         Total       Drop
--------------------------------- ---------- ----------- -----------
802.1X                                      0           0           0
MAC-auth                                    0           0           0
WEB-auth                                    0           0           0
RADIUS                                      0           0           0
```

10.1.11 debug show cpu utilization

debug show cpu utilization	
目的	プロセスごとの CPU 使用率を表示します。
Command	debug show cpu utilization
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはトラブルシューティング用のコマンドとなります。技術サポート担当者が問題の分析を行うために収集をお願いすることがあります。
制限・注意	-
バージョン	1.08.02

使用例：プロセスごとの CPU 使用率を表示する方法を示します。

```
# debug show cpu utilization
 (1)                          (2)                          (3)
Five seconds -   7 %         One minute -   6 %         Five minutes -   7 %
 (4)                    (5)       (6)       (7)
Process Name           5Sec      1Min      5Min
-----------------    ------    ------    ------
OS_UTIL                93 %      93 %      93 %
bcmLINK.0               1 %       1 %       1 %
bcmCNTR.0               0 %       1 %       1 %
GBIC_Pooling            0 %       0 %       0 %
HISR1                   0 %       0 %       0 %
bcmL2X.0                0 %       0 %       0 %
NICRX                   0 %       0 %       0 %
CLI                     0 %       0 %       0 %
socdmadesc.0            0 %       0 %       0 %
CNT_TASK                0 %       0 %       0 %
8021xCtrl               0 %       0 %       0 %
MAUMIB_TASK             0 %       0 %       0 %
radius_reader           0 %       0 %       0 %
SYS_Ctr                 0 %       0 %       0 %
cpuprotect              0 %       0 %       0 %
SYSLOGTASK              0 %       0 %       0 %
IP-Msg                  0 %       0 %       0 %
bcmRX                   0 %       0 %       0 %
DLKtimer                0 %       0 %       0 %
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

項番	説明
(1)	5 秒間の平均の CPU 使用率を表示します。
(2)	1 分間の平均の CPU 使用率を表示します。
(3)	5 分間の平均の CPU 使用率を表示します。
(4)	プロセス名を表示します。
(5)	5 秒間の平均の CPU 使用率を表示します。
(6)	1 分間の平均の CPU 使用率を表示します。
(7)	5 分間の平均の CPU 使用率を表示します。

10.1.12 debug show error-log

debug show error-log	
目的	エラーログの情報を表示します。
Command	debug show error-log
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：エラーログの情報を表示する方法を示します。

```
# debug show error-log

# Error level: FATAL (1)
# Firmware version: 1.08.02
# Clock: 868580 ms
# Overflow: No
# UTC 2021/02/10 05:12:58

Force Exception: ERROR_FATAL

Task: 0x630E4A94 "ssh_mgmt"
Back Trace:
->6125A088
->61C463E8
->61A2B5C0
->618EF0CC
->614C6AD0
->614BBA14
->614BA020
->6154FA54
->61468720
->61468630

Spinlock Name             Accessed Owner
6317C004 OsExt            0331769E none
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

10.1.13 debug show inetstat

debug show inetstat	
目的	IP プロトコルに関する詳細情報を表示します。
Command	debug show inetstat
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはトラブルシューティング用のコマンドとなります。技術サポート担当者が問題の分析を行うために収集をお願いすることがあります。
制限・注意	-
バージョン	1.08.02

使用例：IP プロトコルに関する詳細情報を表示する方法を示します。

```
# debug show inetstat

IP MIB:
ipForwarding:                          1
ipDefaultTTL:                         30
ipInReceives:                          2
ipInHdrErrors:                         0
ipInAddrErrors:                        0
ipForwDatagrams:                       0
ipInUnknownProtos:                     0
ipInDiscards:                          0
ipInDelivers:                          2
ipOutRequests:                         2
ipOutDiscards:                         0
ipOutNoRoutes:                         2
ipReasmTimeout:                       60
ipReasmReqds:                          0
ipReasmOKs:                            0
ipReasmFails:                          0
ipFragOKs:                             0
ipFragFails:                           0
ipFragCreates:                         0
ipRoutingDiscards:                     0
ipv6IpForwarding:                      1
ipv6IpDefaultHopLimit:                64
ipv4InterfaceTableLastChange:       6586
ipv6InterfaceTableLastChange:      65860
ipIfStatsTableLastChange:              0

ipAddrTable:
Addr               Index     NetMask           BcastAddr         ReasmMaxSize
----------------  --------  ----------------  ----------------  ------------
         0.0.0.0      5121           0.0.0.0           0.0.0.1         65535
    10.249.25.33       257     255.255.254.0           0.0.0.1         65535

ipAddrTable:
IfIndex   PhysAddress          NetAddress        Type
--------  ------------------  ----------------  --------
       6  FF-FF-FF-FF-FF-FF       10.249.24.0     OTHER
       6  00-40-66-13-09-69       10.249.24.1   DYNAMIC
       6  00-40-66-B9-2B-4F      10.249.25.33     OTHER
       6  54-EE-75-03-9C-B9     10.249.25.212   DYNAMIC
       6  00-02-2B-21-26-46     10.249.25.217   DYNAMIC
       6  54-EE-75-53-DC-06     10.249.25.219   DYNAMIC
       6  54-EE-75-03-03-7A     10.249.25.220   DYNAMIC
       6  54-EE-75-18-04-B7     10.249.25.222   DYNAMIC
       6  54-EE-75-18-04-D7     10.249.25.224   DYNAMIC
       6  54-EE-75-03-9F-AB     10.249.25.225   DYNAMIC
       6  54-EE-75-03-9B-C4     10.249.25.226   DYNAMIC
       6  54-EE-75-17-84-DD     10.249.25.231   DYNAMIC
       6  54-EE-75-09-FD-DD     10.249.25.233   DYNAMIC
       6  FF-FF-FF-FF-FF-FF     10.249.25.255     OTHER

(省略)
```

10.1.14 debug show memory-pool

debug show memory-pool	
目的	メモリーバッファーの詳細情報を表示します。

debug show memory-pool	
Command	debug show memory-pool MEMORY
Parameter	MEMORY：メモリーバッファーのキーワードを入力します。
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはトラブルシューティング用のコマンドとなります。技術サポート担当者が問題の分析を行うために収集をお願いすることがあります。
制限・注意	-
バージョン	1.08.02

使用例：メモリーバッファー「SYS_HUGE」の詳細情報を表示する方法を示します。

```
# debug show memory-pool SYS_HUGE

SYS_HUGE Detail:

MEMORY   NAME        BASE      SIZE MAX_REQ   ALLOC  BLKS    FREE N_FRE MAX_BLK
01D5FA58 SYS_HUGE  04F01E84  A00800  800844       0     0  A007E4    1  A007E4
-------------------------------------------------------------------------------
        <=32  <=64 <=128 <=256 <=512 <=1024 <=1536 <=2048 <=5120 <=10240 >10240
Alloc:     0     0     0     0     0     0      0      0      0      0       0
Free:      0     0     0     0     0     0      0      0      0      0       1

Alloc fail times 0.
```

使用例：メモリーバッファー「SYS_MEM」の詳細情報を表示する方法を示します。

```
# debug show memory-pool SYS_MEM

SYS_MEM Detail:

MEMORY   NAME        BASE      SIZE MAX_REQ   ALLOC  BLKS    FREE N_FRE MAX_BLK
01E3A8E8 SYS_MEM   03AE2EE4  D00000  409B58  401004   229  8FE73C   1D  8FD9D4
-------------------------------------------------------------------------------
        <=32  <=64 <=128 <=256 <=512 <=1024 <=1536 <=2048 <=5120 <=10240 >10240
Alloc:    52     1    30   441     1     0      2      1      3      2      20
Free:      0     1    24     1     1     1      0      0      0      0       1

Alloc fail times 0.

 ALLOC     SIZE     SN   Magic      Task          File(Line)
-------- ------- --------  -   ---------------- ---------------
03AE2EFC      52 00000000  Y   Root             drv_spi_iproc.c(215)
03AE2F4C   51200 00000014  Y   Root             debug_core.c(529)
03AEF764       8 00000015  Y   Root             drv_arl.c(7060)
03AEF784   90464 00000016  Y   Root             oam_db.c(2104)
03B058FC    3404 00000017  Y   Root             qospolicy_db.c(636)
03B06664    1232 00000018  Y   Root             st_lac.c(522)
03B06B4C      28 00000019  Y   Root             utl_avlt.c(50)
03B06B84      28 0000001A  Y   Root             utl_avlt.c(50)
03B06BBC      28 0000001B  Y   Root             utl_avlt.c(50)
03B06BF4      28 0000001C  Y   Root             utl_queue.c(89)
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

10.1.15 debug show netstat

debug show netstat	
目的	OS のメモリー使用量を表示します。
Command	debug show netstat
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：OS のメモリー使用量を表示する方法を示します。

```
# debug show netstat
(1)                (2)        (3)        (4)        (5)
Memory             Size       Max.       Current    Allocated
  Sub-memory                  Allocate   Allocate   Blocks
----------------- --------- --------- --------- ---------
KERNEL               B5D9D00   A67D290   A66D8E4         359
  ssl_timer             4E20         0         0           0
  ssl_lib              4B000         0         0           0
  web_mem             580000      6B628      6B628         418
  CRYPT               200000       9E80       8768          2A
  LLDP_RMIB_MEM_P      64000          0          0           0
  LLDP_MIB_MEM_PO      66800       DD20       DD20          E8
  LLDP_MEM_POOL         1B800          0          0           0
  SEC_MEM            1400000       2AD8        144           9
  NTP                 100000       3B0C       3B0C          17
  stp                249E000      20398      20398         772
  STG                  40000        200        200           C
  rmon                6E1204       6130C      8554         12F
  agent               1FA000       297D0      297D0         57A
  CLI2-MEMORY         200000      15F27C     146164        1703
  syslog_remote_a      251C0          0          0           0
  syslog_attack        251C0          0          0           0
  syslog_regular      173180       64D4       64D4          C7
  STK_PKT               C800        124          0           0
  fs                  300000      1F910      1EB00         256
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

項番	説明
(1)	メモリー名を表示します。
(2)	合計メモリーサイズを 16 進数（バイト）で表示します。
(3)	装置が起動してからの最大割り当てメモリーサイズを 16 進数（バイト）で表示します。
(4)	現在の割り当てメモリーサイズを 16 進数（バイト）で表示します。
(5)	現在の割り当てメモリーブロック数を 16 進数で表示します。

10.1.16 debug show output

debug show output	
目的	モジュールのデバッグメッセージ出力情報を表示します。

debug show output	
Command	debug show output
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：モジュールのデバッグメッセージ出力情報を表示する方法を示します。

```
# debug show output

Debug Global State  : Disabled

Module name           Output    Enabled
----------------      --------  -------------------------------------
MMRP                  buffer    No
```

10.1.17 debug show ps

debug show ps	
目的	OS のプロセスを表示します。
Command	debug show ps
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：OS のプロセスを表示する方法を示します。

```
# debug show ps
(1)                (2)    (3)       (4)
Process Name      MEM.  CPU Tic  Status
---------------   ----  -------  ------------------------
OS_UTIL            39%   80AF08  Ready
bcmLINK.0        !100%    18450  S:bcm_link_SLEEP
bcmCNTR.0          12%    167C2  S:counter_trigger
HISR1              36%     FB0A  Pend
bcmL2X.0           16%     F49E  S:l2xmsg timer
GBIC_Pooling     !100%     EB62  Q:PORT_RGBIC_QUEU
NICRX               7%     DEFB  S:NIC-RX-Sem
socdmadesc.0        8%     59FF  S:Desc DMA interr
CNT_TASK           64%     55A4  Delay
8021xCtrl          25%     401D  Q:1X_8021xCtrl
MAUMIB_TASK        29%     38AB  E:MAU EVENT
radius_reader      35%     268E  Q:radius_reader
SYS_Ctr            18%     21EB  E:SYS_ENT
cpuprotect         11%     1F64  Q:CPU Protect
CLI                42%     156B  Run
bcmRX              13%     11DC  S:RX pkt ntfy
```

```
FAN_Polling        16%      11A8  E:SYS_ENT
IP-Msg              5%       F14  Q:IPMQ
DLKtimer           24%       E8F  Delay
IP6-Tic             5%       AA6  E:IP6TIC
OS_TIMER           24%       59E  Pend
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

項番	説明
(1)	プロセス名を表示します。
(2)	装置が起動してからプロセスに割り当てられた最大メモリー使用率を表示します。
(3)	装置が起動してからプロセスで使用された合計 CPU カウンターを表示します。
(4)	現在の状態を表示します。

10.1.18 debug show tcpstat

debug show tcpstat	
目的	TCP 接続の詳細情報を表示します。
Command	debug show tcpstat
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはトラブルシューティング用のコマンドとなります。技術サポート担当者が問題の分析を行うために収集をお願いすることがあります。
制限・注意	-
バージョン	1.08.02

使用例：TCP 接続の詳細情報を表示する方法を示します。

```
# debug show tcpstat

rfc2988 tcpRtoAlgorithm
500 tcpRtoMin
32000 tcpRtoMax
-1 tcpMaxConn
0 tcpActiveOpens
0 tcpPassiveOpens
0 tcpAttemptFails
0 tcpEstabResets
0 tcpCurrEstab
0 tcpInSegs
0 tcpOutSegs
0 tcpRetransSegs
0 tcpInErrs
0 tcpOutRsts
0 tcpHCInSegs
0 tcpHCOutSegs

tcpConnTable:
Local Address          Remote Address         State
---------------------- ---------------------- -----------
0.0.0.0:23             0.0.0.0:0              listen

Total Entries: 1
```

```
tcpConnectionTable:
Process Local Type  Local Address                                    State
        Remote Type Remote Address
------- ----------- ---------------------------------------------- -----------

Total Entries (V4/V6): 0/0

tcpListenerTable:
Process Local Type  Local Address
------- ----------- ----------------------------------------------
0       IPv4        0.0.0.0:23
0       IPv6        [::]:23

Total Entries (V4/V6): 1/1
```

10.1.19 debug show udpstat

debug show udpstat	
目的	UDP 接続の詳細情報を表示します。
Command	debug show udpstat
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはトラブルシューティング用のコマンドとなります。技術サポート担当者が問題の分析を行うために収集をお願いすることがあります。
制限・注意	-
バージョン	1.08.02

使用例：UDP 接続の詳細情報を表示する方法を示します。

```
# debug show udpstat

0 udpInDatagrams
7 udpNoPorts
2 udpInErrors
0 udpOutDatagrams
0 udpHCInDatagrams
0 udpHCOutDatagrams

udpTable:
Local Address   Local Port
--------------- ----------
0.0.0.0         161
0.0.0.0         520
0.0.0.0         8021
0.0.0.0         8022

Total Entries: 4

udpEndpointTable:
Instance Process Local Type  Local Address
                 Remote Type Remote Address
-------- ------- ----------- ---------------------------------------------
1        0       IPv4        0.0.0.0:161
                 IPv4        0.0.0.0:0
1        0       IPv4        0.0.0.0:520
                 IPv4        0.0.0.0:0
1        0       IPv4        0.0.0.0:8021
```

```
                IPv4        0.0.0.0:0
1       0       IPv4        0.0.0.0:8022
                IPv4        0.0.0.0:0
1       0       IPv6        [::]:161
                IPv6        [::]:0
1       0       IPv6        [::]:162
                IPv6        [::]:0
1       0       IPv6        [::]:546
                IPv6        [::]:0
1       0       IPv6        [::]:8021
                IPv6        [::]:0
1       0       IPv6        [::]:8022
                IPv6        [::]:0

Total Entries (V4/V6): 4/5
```

10.1.20 debug show wd-error-log

debug show wd-error-log	
目的	ウォッチドッグタイマーによる再起動が発生した際の障害解析情報を表示します。
Command	debug show wd-error-log
Parameter	なし
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	本コマンドはトラブルシューティング用のコマンドとなります。技術サポート担当者が問題の分析を行うために収集をお願いすることがあります。
制限・注意	-
バージョン	1.08.02

使用例：ウォッチドッグタイマーの障害解析情報を表示する方法を示します。

```
# debug show wd-error-log

WDT_ERRLOG Entry 1:

Trigger time : 2022/2/1 4:5:42

Current TASK : HISR1

ISR Info:
DEVICE    LISR     HISR     PRI COOKIE   IRQ  LISR_CNT HISR_CNT  HISR_ACT
UART0                                     N           0        0
UART1                                     N           0        0
NIC0      81180F00 81180EA8 1   null     Y          BD4       BD4  N
NIC1                                      N           0        0
SW0       81120B04 81120AD8 1   832704EC Y    1908C2D0 1908C2D0  N
SW1                                       N           0        0
COMA      81180800 8118077C 1   null     Y          247        2  Y

CPU Utilization Info:
Five seconds -   8 %         One minute -   8 %         Five minutes -   7 %

Process Name          5Sec      1Min      5Min
-----------------   ------    ------    ------
OS_UTIL               92 %      92 %      93 %
bcmLINK.0              1 %       1 %       1 %
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

10.1.21 debug stack restart

debug stack restart	
目的	指定したスタックポートのリンクをリスタートします。
Command	debug stack restart unit UNIT-ID stack-port PORTNO
Parameter	UNIT-ID：対象装置のボックス ID を 1～4 の範囲で指定します。 PORTNO：リスタートするスタックポートのポート番号を、以下の範囲で指定します。複数指定はできません。 • ApresiaNP2500-8MT4X-PoE：9～12 • ApresiaNP2500-16MT4X-PoE：17～20
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	本コマンドを実行すると、指定したスタックポートのリンクが一時的にダウンし、再度アップします。 スタックポート以外のポート番号を指定しても動作しません。
制限・注意	-
バージョン	1.08.02

使用例：ボックス ID 1 のスタックポート（ポート 12）のリンクをリスタートする方法を示します。

```
# debug stack restart unit 1 stack-port 12
#
```

10.1.22 show tech-support

show tech-support	
目的	技術サポート情報を表示します。
Command	show tech-support [MODULE | system-dump | unit UNIT-ID | interface {IF-ID [,|-] | stack-port} system-dump]
Parameter	MODULE（省略可能）：技術サポート情報を表示する機能を、以下のパラメーターで指定します。指定しない場合はすべての情報が表示されます。 • access-defender：AccessDefender 機能 • cpu-trace-history：平均 CPU 使用率がしきい値を上回った場合に採取された CPU に関する履歴ログ • dhcp-server：DHCP サーバー機能 • dhcpv6-client：DHCPv6 クライアント機能 • dhcpv6-server：DHCPv6 サーバー機能 • ether-oam：Ethernet OAM 機能 • ethernet-ring-g8032：リングプロテクション（ERPS）機能 • ipv6-multicast：IPv6 マルチキャスト関連 • loop-detection：ループ検知機能 • memory-error：メモリーエラー自動復旧関連 • mmrp-plus：MMRP-Plus 機能 • ntp：NTP 機能 • poe：PoE 機能

show tech-support	
	• port-channel：ポートチャネル機能 • rmon：RMON 機能 • snmpv3：SNMP 機能 • sntp：SNTP 機能 • spanning-tree：スパニングツリー機能 • stack：スタック機能 system-dump（省略可能）：詳細な装置内部のシステムダンプ情報を表示する場合に指定します。 unit UNIT-ID（省略可能）：情報を表示する装置のボックス ID を 1～4 の範囲で指定します。 interface IF-ID system-dump（省略可能）：インターフェースに関連する技術サポート情報を表示するインターフェースを、以下のパラメーターで指定します。 • port：物理ポート指定、複数指定可能 • stack-port：スタックポート指定
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	問題のトラブルシューティングや分析を技術サポート担当者が行うために必要な装置の情報を、収集して表示します。
制限・注意	• unit 指定でマスター以外の装置を指定して本コマンドを実行すると、出力結果は約 4 メガバイトに制限されます。超過した以降の部分は出力されません。 • 本装置では 4 メガバイト以上の構成情報は使用できません。超過した状態で本コマンドを実行すると、先頭から約 4 メガバイトまでの構成情報は出力結果に含まれますが、超過した以降の部分は含まれません。 • スタック構成で interface IF-ID system-dump パラメーターを使用して物理ポートの技術サポート情報を表示する場合、マスター装置の物理ポートが取得対象です。マスター以外の装置の物理ポートを指定しても一部のハードウェア情報が表示されません。 • system-dump パラメーターを指定した場合、装置の性能、および通信に対して影響を及ぼす可能性があります。使用する場合には、必ず事前にサポート対応窓口へご相談のうえ、指示に従ってください。
バージョン	1.08.02 1.10.01：cpu-trace-history パラメーター追加

使用例：すべての技術サポート情報を表示する方法を示します。

```
# show tech-support

#------------------------------------------------------------------------------
#                ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
#                         Technical Support Information
#
#                              Firmware: Build 1.08.02
#   Copyright(C) 2016  APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------


********************   Basic System Information   ********************
```

```
[SYS 2021-1-8 15:33:51]

Boot Time           : 6 Jan 2021  10:44:36
RTC Time            : 2021/01/08 06:33:51
Boot PROM Version   : Build 1.00.00
Firmware Version    : Build 1.08.02
Hardware Version    : A
Serial number       : 304210000053
MAC Address         : FC-6D-D1-F2-82-1F
MAC Address Number  : 13

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

使用例：MMRP-Plus 関連の技術サポート情報を表示する方法を示します。

```
# show tech-support mmrp-plus

#------------------------------------------------------------------------------
#                ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
#                         Technical Support Information
#
#                             Firmware: Build 1.08.02
#   Copyright(C) 2016  APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------

[MMRP 2021-1-8 15:34:53]

##MMRP Global Information:
  Total Ring     : 0
  Total Ring Port: 0
  Status         : Disable
  Hello interval :    100ms Operating:      0ms
  Polling rate   :     10   Operating:      0

##MMRP VlanGroup STG Status:
  GroupID:0 ring_count[0] masterStgID[0] slaveStgID[0]
    Master VID   : 1-4094
    Slave VID    :
  GroupID:1 ring_count[0] masterStgID[0] slaveStgID[0]
    Master VID   : 1-4094
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

使用例：AccessDefender 関連の技術サポート情報を表示する方法を示します。

```
# show tech-support access-defender

#------------------------------------------------------------------------------
#                ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
#                         Technical Support Information
#
#                             Firmware: Build 1.08.02
#   Copyright(C) 2016  APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------

[ACCESS_DEFENDER 2021-1-8 15:35:09]


#DHCP-snooping entry

 Snooping : DISABLE
 Mode: 0 (0:permit,1:deny)
```

```
 Total : 0 (static 0, dynamic 0)

 Binding Entry

 BST Entry

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

使用例：メモリーエラー自動復旧関連の技術サポート情報を表示する方法を示します。

```
# show tech-support memory-error

#------------------------------------------------------------------------------
#                ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
#                         Technical Support Information
#
#                              Firmware: Build 1.08.02
#   Copyright(C) 2016  APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------

[MEAR 2021-1-8 15:35:25]

Detail Memory-Error Auto-Recovery Status:
-----------------------------------------------------------
Auto Recovery Mode         : Enabled
Auto Recovery Notification : Enabled
Fault Action Configuration : -

 Unit : 1
 Status : Normal
 Recovery Counters
 ---------------------------------------------
 L2Xm                                :          0
 L2MCm                               :          0
 EGR_VLANm                           :          0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

10.1.23 debug show tech-support

debug show tech-support	
目的	show tech-support で取得できる技術サポート情報の一部を表示します。
Command	debug show tech-support CATEGORY [unit UNIT-ID]
Parameter	CATEGORY：技術サポート情報を表示するカテゴリーを、以下のパラメーターで指定します。 • aaa：AAA 機能 • access-defender：AccessDefender 機能 • arp：ARP エントリー情報関連 • cfm：CFM 機能 • cnt：カウンター情報関連 • config：構成情報関連 • cpu-counter：CPU にトラップされたパケットのうち、各プロトコル処理に伝搬された制御パケットの統計情報関連 • cpu-protect：CPU 使用率監視機能 • dhcp-server：DHCP サーバー機能

debug show tech-support	
	• dhcpv6-client：DHCPv6 クライアント機能 • dhcpv6-server：DHCPv6 サーバー機能 • err-disable：err-disabled 状態のポートの自動復旧機能 • error-log：エラーログ情報関連 • ether-oam：Ethernet OAM 機能 • ethernet-ring-g8032：リングプロテクション(ERPS)機能 • fdb：MAC アドレスエントリー情報関連 • file-system-management：ファイルシステム情報関連 • firmware：ブート情報関連 • igmp-snooping：IGMP スヌーピング機能 • l3-system：IP プロトコル情報関連 • loop-detection：ループ検知機能 • memory-error：メモリーエラー自動復旧関連 • mirror：ミラーリング情報関連 • mld-snooping：MLD スヌーピング機能 • mmrp-plus：MMRP-Plus 機能 • nd6：IPv6 ネイバー情報関連 • ntp：NTP 機能 • os：OS 情報関連 • poe：PoE 機能 • port-channel：ポートチャネル機能 • port-configuration：ポート情報関連 • port-security：ポートセキュリティー機能 • privelege-management：ラインセッション情報関連 • rmon：RMON 機能 • routing-table：IPv4 ルーティングテーブル情報関連 • sflow：sFlow 機能 • snmpv3：SNMP 機能 • sntp：SNTP 機能 • spanning-tree：スパニングツリー機能 • stack：スタック機能 • static-ipv6-route：IPv6 スタティックルート情報関連 • storm-control：ストームコントロール機能 • system：システム情報関連 • system-log：システムログ関連 unit UNIT-ID（省略可能）：情報を表示する装置のボックス ID を 1～4 の範囲で指定します。
モード	特権実行モード、任意の設定モード
特権レベル	レベル：15
ガイドライン	問題のトラブルシューティングや分析を技術サポート担当者が行うために必要な装置の情報を、収集して表示します。
制限・注意	-
バージョン	1.13.01

使用例：システム情報関連の技術サポート情報を表示する方法を示します。

```
# debug show tech-support system

#------------------------------------------------------------------------------
-
#                ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch
#                         Technical Support Information
#
#                            Firmware: Build 1.13.01
#   Copyright(C) 2021  APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------
-


********************   Basic System Information   ********************

[SYS 2025-1-24 11:06:44]

Boot Time           : 24 Jan 2025  09:25:06
RTC Time            : 2025/01/24 02:06:43
Boot PROM Version   : Build 1.00.00
Firmware Version    : Build 1.13.01
Hardware Version    : A
Serial number       : 304210000053
MAC Address         : 00-40-66-F2-82-1F
MAC Address Number  : 13

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

10.2 メモリーエラー自動復旧コマンド

メモリーエラー自動復旧関連のコマンドは以下のとおりです。

- memory-error auto-recovery mode disable
- memory-error auto-recovery notify disable
- memory-error fault-action shutdown-all
- clear memory-error

10.2.1 memory-error auto-recovery mode disable

memory-error auto-recovery mode disable	
目的	メモリーエラー自動復旧機能を無効にします。有効にする場合は、no 形式のコマンドを使用します。
Command	memory-error auto-recovery mode disable no memory-error auto-recovery mode disable
Parameter	なし
デフォルト	メモリーエラー自動復旧機能は有効（no memory-error auto-recovery mode disable）
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	メモリーエラー自動復旧機能が有効の場合は、スイッチの大規模集積回路(LSI)のメモリーが監視対象になります。メモリーエラーが検出されると、自動的に復旧アクションが動作します。 以下のメモリー領域は監視対象外となり、show environment memory コマンドで表示される SW-LSI メモリーの状態が「Abnormal」になります。 • メモリーエラーの検出と復旧アクションが 10 回以上動作したメモリー領域 • 復旧不能なメモリーエラーが検出されたメモリー領域
制限・注意	-
バージョン	1.08.02

使用例：メモリーエラー自動復旧機能を無効にする方法を示します。

```
# configure terminal
(config)# memory-error auto-recovery mode disable
(config)#
```

10.2.2 memory-error auto-recovery notify disable

memory-error auto-recovery notify disable	
目的	メモリーエラー自動復旧機能に関連する通知を無効にします。有効にする場合は、no 形式のコマンドを使用します。
Command	memory-error auto-recovery notify disable no memory-error auto-recovery notify disable
Parameter	なし
デフォルト	メモリーエラー自動復旧機能に関連する通知は有効（no memory-error auto-recovery notify disable）

memory-error auto-recovery notify disable	
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	デフォルト状態では、メモリーエラーが検出され自動的に復旧したときに、システムログエントリーが出力されます。
制限・注意	-
バージョン	1.08.02

使用例：メモリーエラー自動復旧機能に関連付いている通知を無効にする方法を示します。

```
# configure terminal
(config)# memory-error auto-recovery notify disable
(config)#
```

10.2.3 memory-error fault-action shutdown-all

memory-error fault-action shutdown-all	
目的	SW-LSI メモリーの状態が「Abnormal」になった場合に、すべてのポートを自動的にシャットダウンする機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	memory-error fault-action shutdown-all no memory-error fault-action shutdown-all
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：15
ガイドライン	本機能が無効の場合は、SW-LSI メモリーの状態が「Abnormal」になった場合でもポートのシャットダウンは実行されません。 本機能でシャットダウンされたポートのリンク状態は、show interfaces コマンドでは "link status is down (cause: Memory Error)" と表示されます。また、show interfaces status コマンドの Status 項目では "memory-error" と表示されます。 シャットダウンされたポートを復旧するには、clear memory-error コマンド、または no memory-error fault-action shutdown-all コマンドを使用します。
制限・注意	-
バージョン	1.08.02

使用例：SW-LSI メモリーの状態が「Abnormal」になった場合に、すべてのポートを自動的にシャットダウンする機能を有効にする方法を示します。

```
# configure terminal
(config)# memory-error fault-action shutdown-all
(config)#
```

10.2.4 clear memory-error

clear memory-error	
目的	メモリーエラー自動復旧機能の状態をリストアします。
Command	clear memory-error

clear memory-error	
Parameter	なし
モード	特権実行モード
特権レベル	レベル：15
ガイドライン	本コマンドを実行すると、SW-LSI メモリーの状態が「Normal」に戻り、記録されたメモリーエラーカウンターがクリアされて、監視対象のメモリー領域のキャッシュ設定がリストアされます。
制限・注意	• SW-LSI の復旧不能なメモリーエラーを検出している状態では、本コマンドを実行してもリストアされません。
バージョン	1.08.02

使用例：メモリーエラー自動復旧機能の状態をリストアする方法を示します。

```
# clear memory-error
#
```

10.3 システムログコマンド

システムログ関連の設定コマンドは以下のとおりです。

- logging on
- logging buffered
- logging console
- logging discriminator
- logging server
- logging source-interface
- command logging enable

システムログ関連の show／操作コマンドは以下のとおりです。

- show logging
- show logging sram
- clear logging

10.3.1 logging on

logging on	
目的	システムメッセージのロギングを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	logging on no logging on
Parameter	なし
デフォルト	有効（logging on）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドはロギング全体の有効・無効を設定します。そのため、本コマンドを無効にすると、以下のそれぞれの宛先へのロギング設定が有効でも、ロギングされなくなります。 • ローカルメッセージバッファーへのロギング設定（logging buffered） • ローカルコンソールへのロギング設定（logging console） • SYSLOG サーバーへのロギング設定（logging server） ローカルメッセージバッファーへのロギング設定が無効（no logging buffered）の状態で本コマンドを有効に設定すると、ローカルメッセージバッファーへのロギング設定も有効になります。
制限・注意	• ローカルメッセージバッファーでのログの最大保存数は約 10,000 件です。また、SRAM でのログの最大保存数は約 3,000 件です。 • 装置起動後に SYSLOG サーバーに送信されるログは、SYSLOG サーバーと通信可能になった後、まとめて送信されます。その際、通信可能になる前に装置起動後からロギングされたシステムメッセージも送信されます。
バージョン	1.08.02

使用例：システムメッセージのロギングを有効にする方法を示します。

```
# configure terminal
```

```
(config)# logging on

 WARNING: The command takes effect and the logging buffered is enabled at the same time.
(config)#
```

10.3.2 logging buffered

logging buffered	
目的	ローカルメッセージバッファーへのシステムメッセージのロギングを有効にします。無効にする場合は、no logging buffered コマンドを使用します。デフォルト設定に戻すには、default logging buffered コマンドを使用します。
Command	logging buffered [severity SEVERITY] [discriminator NAME] [write-delay {SECONDS | infinite}] no logging buffered default logging buffered
Parameter	severity SEVERITY（省略可能）：システムメッセージの重要度を、レベルまたは名称で指定します。指定しない場合は重要度は informational(6) になります。 • レベル指定の場合は 0～7 の範囲で指定 • 名称指定の場合は emergencies(0), alerts(1), critical(2), errors(3), warnings(4), notifications(5), informational(6), debugging(7) のいずれかを指定 ※(数値)は入力不要 discriminator NAME（省略可能）：ロギングするメッセージのフィルタリングに使用する discriminator 名を指定します。 write-delay（省略可能）：ローカルメッセージバッファーの SRAM への周期的書き込み間隔を指定します。 SECONDS：周期的書き込み間隔（秒単位）を 0～65,535 秒の範囲で指定します。 infinite：周期的書き込みを無効にします。
デフォルト	重要度：informational(6) 周期的書き込み間隔：0 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	ローカルメッセージバッファーの内容は、write-delay パラメーターで指定した間隔で SRAM に保存されます。 以下の操作時には、SRAM とフラッシュメモリーの両方にローカルメッセージバッファーの内容が保存されます。 • write コマンド、copy running-config startup-config コマンド（設定保存） • logout コマンド、exit コマンドによるログアウト • reboot コマンド等による再起動 装置起動時には、フラッシュメモリーに保存された内容がローカルメッセージバッファーに再読み込みされます。 ローカルメッセージバッファーにロギングされるシステムメッセージは、指定した重要度レベル以上のメッセージがロギングされます。 ローカルメッセージバッファーの空きがなくなった場合、最も古いログエントリーが削除されます。

logging buffered	
	重要度の名称と対応するレベル、および説明を以下に示します。(数値)は対応するレベルです。 • emergencies(0)：システムが不安定な状態になったことを示す。 • alerts(1)：システムを運用するためにただちに処置を施す必要のある問題が発生したことを示す。 • critical(2)：クリティカルなイベントが発生したことを示す。 • errors(3)：エラーイベントが発生したことを示す。 • warnings(4)：警告イベントが発生したことを示す。 • notifications(5)：正常だが、重要なイベントが発生したことを示す。 • informational(6)：情報メッセージ。 • debugging(7)：デバッグメッセージ。 discriminator を使用してフィルタリングを行う場合は、先に discriminator を設定してから指定します。また、適用済みの discriminator の設定内容を変更した場合は、適用が解除され discriminator パラメーターの設定が削除されます。
制限・注意	• ローカルメッセージバッファーでのログの最大保存数は約 10,000 件です。また、SRAM でのログの最大保存数は約 3,000 件です。 • コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。 • SEVERITY パラメーターは、構成情報では名称で表示されます。
バージョン	1.08.02

使用例：errors(3)以上の重要度(0～3)のメッセージを対象にして、ローカルメッセージバッファーへのロギングを有効にする方法を示します。

```
# configure terminal
(config)# logging buffered severity errors
(config)#
```

10.3.3 logging console

logging console	
目的	ローカルコンソールへのシステムメッセージのロギングを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	logging console [severity SEVERITY] [discriminator NAME] no logging console
Parameter	severity SEVERITY（省略可能）：システムメッセージの重要度を、レベルまたは名称で指定します。指定しない場合は重要度は warnings(4) になります。 • レベル指定の場合は 0～7 の範囲で指定 • 名称指定の場合は emergencies(0), alerts(1), critical(2), errors(3), warnings(4), notifications(5), informational(6), debugging(7) のいずれかを指定 ※(数値)は入力不要 discriminator NAME（省略可能）：ロギングするメッセージのフィルタリングに使用する discriminator 名を指定します。
デフォルト	無効
モード	グローバル設定モード

logging console	
特権レベル	レベル：12
ガイドライン	本設定により、ローカルメッセージバッファーにシステムメッセージがロギングされた後、ローカルコンソールに送られます。 ローカルコンソールにロギングされるシステムメッセージは、指定した重要度レベル以上のメッセージがロギングされます。 重要度の名称と対応するレベル、および説明を以下に示します。(数値)は対応するレベルです。 • emergencies(0)：システムが不安定な状態になったことを示す。 • alerts(1)：システムを運用するためにただちに処置を施す必要のある問題が発生したことを示す。 • critical(2)：クリティカルなイベントが発生したことを示す。 • errors(3)：エラーイベントが発生したことを示す。 • warnings(4)：警告イベントが発生したことを示す。 • notifications(5)：正常だが、重要なイベントが発生したことを示す。 • informational(6)：情報メッセージ。 • debugging(7)：デバッグメッセージ。 discriminator を使用してフィルタリングを行う場合は、先に discriminator を設定してから指定します。また、適用済みの discriminator の設定内容を変更した場合は、適用が解除され discriminator パラメーターの設定が削除されます。
制限・注意	• コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。 • SEVERITY パラメーターは、構成情報では名称で表示されます。
バージョン	1.08.02

使用例：errors(3)以上の重要度(0～3)のメッセージを対象にして、ローカルコンソールへのロギングを有効にする方法を示します。

```
# configure terminal
(config)# logging console severity errors
(config)#
```

10.3.4 logging discriminator

logging discriminator	
目的	ロギングするシステムメッセージのフィルタリングに使用する、discriminator を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	logging discriminator NAME [facility {drops STRING | includes STRING}] [severity {drops SEVERITY-LIST | includes SEVERITY-LIST}] no logging discriminator NAME
Parameter	NAME：discriminator 名を最大 15 文字で指定します。ASCII コードの印字可能な文字のうち、? 空白文字 を除いた文字を使用可能です。 facility {drops STRING | includes STRING}（省略可能）：フィルタリングの対象となる機能名を、次の文字列のいずれかで指定します。複数指定する場合は、コンマ(,)で間を空けないで区切ります。 • SYS, STACKING, PORT, STP, LAC, VOICE_VLAN, FDB, LLDP, ACL, QOS, DHCP, DHCPV6, STORM_CTRL, SSH, CLI, SNMP, CFM, ALARM, ERPS,

logging discriminator	
	DDM, AAA, DEVICE, RADIUS, DOT1X, POE, MAC, ULD, CFG, FIRMWARE, MGMTPORT, MEAR, MMRP, PD_Monitoring • drops パラメーターで指定した場合は、指定した機能のログはフィルタリングされ、それ以外のログはフィルタリングされません。 • includes パラメーターで指定した場合は、指定した機能のログはフィルタリングされず、それ以外のログがフィルタリングされます。 severity {drops SEVERITY-LIST | includes SEVERITY-LIST}（省略可能）：フィルタリングの対象となる重要度レベルを 0～7 の範囲で指定します。複数指定する場合は、コンマ(,)で間を空けないで区切ります。 • drops パラメーターで指定した場合は、指定した重要度レベルのログはフィルタリングされ、それ以外のログはフィルタリングされません。 • includes パラメーターで指定した場合は、指定した重要度レベルのログはフィルタリングされず、それ以外のログがフィルタリングされます。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	設定した discriminator を使用してフィルタリングを行う場合は、logging buffered コマンド、logging console コマンド、logging server コマンドにおいて、適用する discriminator 名を指定します。それぞれのコマンドで指定する前に discriminator を設定する必要があります。 discriminator の設定内容を変更すると、以前の設定は上書きされます。 すでに適用済みの discriminator の設定内容を変更した場合は、logging buffered コマンド、logging console コマンド、logging server コマンドでの適用が解除され、discriminator パラメーターの設定が削除されます。
制限・注意	• コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。
バージョン	1.08.02

使用例：discriminator 名を「buffer-filter」とし、フィルタリング対象を「drops 指定、機能名=STP,CLI」として設定する方法を示します。

```
# configure terminal
(config)# logging discriminator buffer-filter facility drops STP,CLI
(config)#
```

10.3.5 logging server

logging server	
目的	SYSLOG サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	logging server {IP-ADDRESS | IPV6-ADDRESS} [severity SEVERITY] [facility FACILITY] [discriminator NAME] [port UDP-PORT] no logging server {IP-ADDRESS | IPV6-ADDRESS}
Parameter	IP-ADDRESS：SYSLOG サーバーの IPv4 アドレスを指定します。 IPV6-ADDRESS：SYSLOG サーバーの IPv6 アドレスを指定します。

logging server	
	severity SEVERITY（省略可能）：システムメッセージの重要度を、レベルまたは名称で指定します。指定しない場合は重要度は warnings(4) になります。 • レベル指定の場合は 0～7 の範囲で指定 • 名称指定の場合は emergencies(0), alerts(1), critical(2), errors(3), warnings(4), notifications(5), informational(6), debugging(7) のいずれかを指定 ※(数値)は入力不要 facility FACILITY（省略可能）：ファシリティを、数字コードまたは名称で指定します。指定しない場合はファシリティは 23(local7) になります。 • 数字コード指定の場合は 0～23 の範囲で指定 • 名称指定の場合は kern(0), user(1), mail(2), daemon(3), auth1(4), syslog(5), lpr(6), news(7), uucp(8), clock1(9), auth2(10), ftp(11), ntp(12), logaudit(13), logalert(14), clock2(15), local0(16), local1(17), local2(18), local3(19), local4(20), local5(21), local6(22), local7(23) のいずれかを指定 ※(数値)は入力不要 discriminator NAME（省略可能）：ロギングするメッセージのフィルタリングに使用する discriminator 名を指定します。 port UDP-PORT（省略可能）：SYSLOG サーバーへの通信に使用する UDP ポート番号を、514 または 1024～65535 の範囲で指定します。指定しない場合は 514 になります。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本設定により、ローカルメッセージバッファーにシステムメッセージがロギングされた後、ロギングサーバーに転送されます。 重要度の名称と対応するレベル、および説明を以下に示します。(数値)は対応するレベルです。 • emergencies(0)：システムが不安定な状態になったことを示す。 • alerts(1)：システムを運用するためにただちに処置を施す必要のある問題が発生したことを示す。 • critical(2)：クリティカルなイベントが発生したことを示す。 • errors(3)：エラーイベントが発生したことを示す。 • warnings(4)：警告イベントが発生したことを示す。 • notifications(5)：正常だが、重要なイベントが発生したことを示す。 • informational(6)：情報メッセージ。 • debugging(7)：デバッグメッセージ。 discriminator を使用してフィルタリングを行う場合は、先に discriminator を設定してから指定します。また、適用済みの discriminator の設定内容を変更した場合は、適用が解除され discriminator パラメーターの設定が削除されます。
制限・注意	• SYSLOG サーバーは、最大 4 個設定できます。 • デフォルトルート情報(0.0.0.0/0)とマネージメントポートのデフォルトゲートウェイ設定(ip default-gateway)の両方が存在する装置において、以下の宛先に存在する SYSLOG サーバーを指定して設定した場合、宛先判定にはデフォルトルートよりもデフォルトゲートウェイ設定が優先され、宛先(1)(2)のいずれの場合も SYSLOG パケットはマネージメントポートから送信されます。

logging server	
	• 宛先(1)：デフォルトルートで経路が解決されて VLAN インターフェースからアクセス可能なネットワーク • 宛先(2)：デフォルトゲートウェイ設定で経路が解決されてマネージメントポートからアクセス可能なネットワーク • VLAN インターフェース経由でのみ管理する場合は、送信元 IP アドレス設定(logging source-interface)を VLAN インターフェース指定で設定することにより、このような状況でも宛先(1)への SYSLOG パケットが VLAN インターフェースから送信されるようになりますが、この設定をすると宛先(2)の場合も VLAN インターフェースから送信されるようになることに注意してください。 • コマンド実行時のパラメーター指定は順不同ではありません。パラメーター指定の順序はコマンド構文に記載の順序で指定してください。 • SEVERITY パラメーターは、構成情報では名称で表示されます。 • FACILITY パラメーターは、構成情報では数字コードで表示されます。
バージョン	1.08.02

使用例：warnings(4)以上の重要度(0～4)のメッセージを対象にして、SYSLOG サーバー 192.0.2.100 へのロギングを有効にする方法を示します。

```
# configure terminal
(config)# logging server 192.0.2.100 severity warnings
(config)#
```

10.3.6 logging source-interface

logging source-interface	
目的	SYSLOG パケットの送信元 IP アドレスとして使用するインターフェースを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	logging source-interface IF-ID no logging source-interface
Parameter	IF-ID：インターフェースを以下のパラメーターで指定します。 • vlan <1-4094>：VLAN インターフェース指定 • mgmt 0：マネージメントポート指定
デフォルト	最も近いインターフェースの IP アドレスを使用
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	• マネージメントポート経由で管理する場合は、vlan パラメーターを指定して本コマンドを設定しないでください。 • VLAN インターフェース経由で管理する場合は、mgmt パラメーターを指定して本コマンドを設定しないでください。
バージョン	1.08.02

使用例：SYSLOG パケットの送信元 IP アドレスとして、VLAN 1 インターフェース IP アドレスを設定する方法を示します。

```
# configure terminal
```

```
(config)# logging source-interface vlan 1
(config)#
```

10.3.7 command logging enable

command logging enable	
目的	コマンドロギング機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	command logging enable no command logging enable
Parameter	なし
デフォルト	有効（command logging enable）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	コマンドロギング機能は、装置に対して実行されたコマンドをロギングします。コマンドを実行したユーザーアカウントの情報とともに、コマンド自体をシステムログにロギングします。 show logging コマンドを使用して表示されるコマンド文字列部分は、最大 255 文字です。
制限・注意	• 本設定は構成情報では CLI 関連（ラベル# CLI）で表示されます。
バージョン	1.08.02

使用例：コマンドロギング機能を有効にする方法を示します。

```
# configure terminal
(config)# command logging enable
(config)#
```

10.3.8 show logging

show logging	
目的	ローカルメッセージバッファーにロギングされたシステムメッセージを表示します。オプションパラメーターを指定しないで実行した場合には、最新メッセージから 200 個のログが表示されます。
Command	show logging [all | [REF-SEQ] [+ NN | - NN]]
Parameter	all（省略可能）：すべてのログエントリーを最新メッセージから順に表示する場合に指定します。 REF-SEQ（省略可能）：表示を開始するシーケンス番号を指定します。指定したシーケンス番号以降の新しいメッセージが順に表示されます。 + NN（省略可能）：REF-SEQ で指定したシーケンス番号から表示する新しいメッセージの数を指定します。「+」と「NN」の間には半角空白が必要です。REF-SEQ を指定しないで「+ NN」だけを指定した場合は、最も古いメッセージから表示します。 - NN（省略可能）：REF-SEQ で指定したシーケンス番号から表示する古いメッセージの数を指定します。「-」と「NN」の間には半角空白が必要です。REF-SEQ を指定しないで「- NN」だけを指定した場合は、最も新しいメッセージから表示します。
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1

show logging	
ガイドライン	ローカルメッセージバッファーにロギングされる各メッセージは、シーケンス番号と関連付けられます。メッセージがロギングされるとき、1 から始まるシーケンス番号が割り当てられます。シーケンス番号は、100000 に達すると 1 に戻ります。
制限・注意	-
バージョン	1.08.02

使用例：ローカルメッセージバッファーに保存されたシステムメッセージを表示する方法を示します。

```
# show logging

Total number of buffered messages:6 ... (1)
(2)
#6      2016-03-03 14:49:36 INFO(6) "exit" executed by 15 from Console
#5      2016-03-03 14:49:35 INFO(6) "configure terminal" executed by 15 from Console
#4      2016-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#3      2016-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#2      2016-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
#1      2016-03-03 14:49:22 INFO(6) "clear logging" executed by 15 from Console
```

項番	説明
(1)	システムメッセージ数を表示します。
(2)	オプションパラメーターを指定しないで実行した場合は、最新メッセージから最大 200 個のログが表示されます。

使用例：シーケンス番号 3 から開始して、新しいメッセージを順に表示する方法を示します。

```
# show logging 3

Total number of buffered messages:7 ... (1)
(2)
#3      2016-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#4      2016-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#5      2016-03-03 14:49:35 INFO(6) "configure terminal" executed by 15 from Console
#6      2016-03-03 14:49:36 INFO(6) "exit" executed by 15 from Console
#7      2016-03-03 14:49:40 INFO(6) "show logging" executed by 15 from Console
```

項番	説明
(1)	システムメッセージ数を表示します。
(2)	表示を開始するシーケンス番号を指定した場合は、指定したシーケンス番号以降の新しいメッセージが順に表示されます。

使用例：シーケンス番号 2 から開始して、4 個の新しいメッセージを表示する方法を示します。

```
# show logging 2 + 4

Total number of buffered messages:8 ... (1)
(2)
#2      2016-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
#3      2016-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#4      2016-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#5      2016-03-03 14:49:35 INFO(6) "configure terminal" executed by 15 from Console
```

項番	説明
(1)	システムメッセージ数を表示します。
(2)	表示を開始するシーケンス番号と「+」指定の表示数を指定した場合は、指定したシーケンス番号以降の新しいメッセージが指定した数だけ表示されます。

使用例：シーケンス番号 4 から開始して、3 個の古いメッセージを表示する方法を示します。

```
# show logging 4 - 3

Total number of buffered messages:9 ... (1)
(2)
#4      2016-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#3      2016-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#2      2016-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
```

項番	説明
(1)	システムメッセージ数を表示します。
(2)	表示を開始するシーケンス番号と「-」指定の表示数を指定した場合は、指定したシーケンス番号以前の古いメッセージが指定した数だけ表示されます。

10.3.9 show logging sram

show logging sram	
目的	SRAM に保存されたシステムメッセージを表示します。
Command	show logging sram
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	• 装置起動時には、フラッシュメモリーに保存された内容がローカルメッセージバッファーに再読み込みされ、そこから連続したシーケンス番号で新たにシステムメッセージがロギングされます。ローカルメッセージバッファーの内容を SRAM またはフラッシュメモリーに保存するトリガーの違いにより、タイミングによっては SRAM に保存されたシステムメッセージとフラッシュメモリーに保存されたシステムメッセージには差異があります。そのため、停電などで装置の電源が落ちてから起動すると、本コマンドで表示される SRAM に保存されたシステムメッセージのシーケンス番号が、連番でなくなることがあります。
バージョン	1.08.02

使用例：SRAM に保存されたシステムメッセージを表示する方法を示します。

```
# show logging sram

Total number of buffered messages:6 ... (1)
(2)
#6      2016-03-03 14:49:36 INFO(6) "exit" executed by 15 from Console
#5      2016-03-03 14:49:35 INFO(6) "configure terminal" executed by 15 from Console
#4      2016-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#3      2016-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#2      2016-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
#1      2016-03-03 14:49:22 INFO(6) "clear logging" executed by 15 from Console
```

項番	説明
(1)	システムメッセージ数を表示します。
(2)	システムメッセージを新しい順に表示します。

10.3.10 clear logging

clear logging	
目的	ローカルメッセージバッファー、フラッシュメモリー、SRAM に保存されたログメッセージを削除します。
Command	clear logging
Parameter	なし
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02

使用例：すべてのログメッセージを削除する方法を示します。

```
# clear logging
Clear logging? (y/n) [n]  y
```

10.4 システムメモリー使用率監視コマンド

システムメモリー使用率監視関連の設定コマンドは以下のとおりです。

- cpu-protect system-memory limit-check fault-action reboot
- cpu-protect system-memory limit-check threshold

10.4.1 cpu-protect system-memory limit-check fault-action reboot

cpu-protect system-memory limit-check fault-action reboot	
目的	AEOS-NP2500 Ver. 1.08.04 以降では、本コマンドは削除され、デフォルトで有効設定相当の動作に仕様変更されています。また、監視対象のシステムメモリーも追加されています。 AEOS-NP2500 Ver. 1.08.04 より前のバージョンでは、システムメモリー（SYS_MEM、SYS_HUGE、または SEC_MEM）を割り当てることができない状態が 1 分間続いた場合に、装置を再起動する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	cpu-protect system-memory limit-check fault-action reboot no cpu-protect system-memory limit-check fault-action reboot
Parameter	なし
デフォルト	AEOS-NP2500 Ver. 1.08.04 より前のバージョン：無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02 1.08.04：本コマンドは削除され、デフォルトで有効設定相当の動作に変更

使用例：AEOS-NP2500 Ver. 1.08.04 より前のバージョンにおいて、システムメモリー（SYS_MEM、SYS_HUGE、または SEC_MEM）を割り当てることができない状態が 1 分間続いた場合に、装置を再起動する機能を有効にする方法を示します。

```
# configure terminal
(config)# cpu-protect system-memory limit-check fault-action reboot
(config)#
```

10.4.2 cpu-protect system-memory limit-check threshold

cpu-protect system-memory limit-check threshold	
目的	システムメモリー（SYS_MEM、SYS_HUGE、SEC_MEM、その他監視対象のメモリー）の使用率を 60 秒ごとにチェックし、指定したしきい値を超えた場合に、ログとトラップを出力する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	cpu-protect system-memory limit-check threshold [VALUE] no cpu-protect system-memory limit-check
Parameter	VALUE（省略可能）：システムメモリーの使用率のしきい値を 80～100(%)の範囲で指定します。
デフォルト	無効、有効時のしきい値：90%

cpu-protect system-memory limit-check threshold	
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.08.02 1.08.04：監視対象のシステムメモリーを追加

使用例：システムメモリー（SYS_MEM、SYS_HUGE、SEC_MEM、その他監視対象のメモリー）の使用率を 60 秒ごとにチェックし、使用率が 90%を超えた場合に、ログとトラップを出力する機能を有効にする方法を示します。

```
# configure terminal
(config)# cpu-protect system-memory limit-check threshold 90
(config)#
```

10.5 CPU 使用率監視コマンド

CPU 使用率監視関連の設定コマンドは以下のとおりです。

- cpu-protect trace trigger
- cpu-protect trace history mode disable
- dynamic cpu-receive suppression disable
- dynamic cpu-receive suppression interval
- snmp-server enable traps cpu-protect

CPU 使用率監視関連の show／操作コマンドは以下のとおりです。

- show cpu-protect trace
- clear cpu-protect trace history

10.5.1 cpu-protect trace trigger

cpu-protect trace trigger	
目的	指定した監視間隔の平均 CPU 使用率がしきい値を上回った場合に、障害解析用ログ(error-log)、およびしきい値上昇前後の CPU に関する履歴ログ(cpu-trace-history)を採取して、ログおよびトラップを出力する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	cpu-protect trace trigger THRESHOLD [polling SECONDS] no cpu-protect trace trigger
Parameter	THRESHOLD：しきい値を 50～100(%)の範囲で指定します。 polling SECONDS (省略可能)：監視間隔を 10～180(秒)の範囲で指定します。
デフォルト	無効、CPU 使用率監視間隔は未指定時は 10 秒
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	指定した監視間隔の平均 CPU 使用率がしきい値を下回った場合にも、ログおよびトラップが出力されます。 トラップを出力する場合には、snmp-server enable traps cpu-protect コマンドを有効にする必要があります。 CPU に関する履歴ログには、タスクごとの CPU 使用率、機能ごとのプロトコルパケット受信数、受信ポートかつ CPU CoS ごとの CPU 宛てパケット統計情報が含まれます。この履歴ログの採取機能を無効にする場合は、cpu-protect trace history mode disable コマンドを使用します。
制限・注意	• CPU に関する履歴ログ(cpu-trace-history)は最大 10 件保存されます。10 件登録された状態では、平均 CPU 使用率がしきい値を上回った場合でも履歴ログの採取は行われません。この状態で履歴ログの採取を再開するには、clear cpu-protect trace history コマンドを実行して履歴ログを削除してください。 • CPU に関する履歴ログの採取機能は、AEOS-NP2500 Ver. 1.10.01 以降でサポートしています。
バージョン	1.08.02

使用例：CPU 使用率監視機能を、しきい値 100%、監視間隔 60 秒で有効にする方法を示します。

```
# configure terminal
```

```
(config)# cpu-protect trace trigger 100 polling 60
(config)#
```

10.5.2 cpu-protect trace history mode disable

cpu-protect trace history mode disable	
目的	指定した監視間隔の平均 CPU 使用率がしきい値を上回った場合に、CPU に関する履歴ログを採取する機能を無効にします。有効にする場合は、no 形式のコマンドを使用します。
Command	cpu-protect trace history mode disable no cpu-protect trace history mode disable
Parameter	なし
デフォルト	CPU に関する履歴ログの採取機能は有効（no cpu-protect trace history mode disable）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	-
制限・注意	-
バージョン	1.10.01

使用例：CPU に関する履歴ログの採取機能を無効にする方法を示します。

```
# configure terminal
(config)# cpu-protect trace history mode disable
(config)#
```

10.5.3 dynamic cpu-receive suppression disable

dynamic cpu-receive suppression disable	
目的	CPU 高負荷状態における CPU ポートでのパケット受信量を抑制する機能を無効にします。有効にする場合は、no 形式のコマンドを使用します。
Command	dynamic cpu-receive suppression disable no dynamic cpu-receive suppression disable
Parameter	なし
デフォルト	CPU 高負荷状態における CPU ポートでのパケット受信量を抑制する機能は有効（no dynamic cpu-receive suppression disable）
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	設定した監視間隔の平均 CPU 使用率が 99%以上になると CPU 宛てパケットの受信レート抑制が開始され、94%以下になると受信レート抑制が終了します。
制限・注意	• CPU 高負荷状態における CPU ポートでのパケット受信量を抑制する機能が有効の場合、構成や使用機能によっては、通常運用中でも「CPU 宛てパケットの受信レート抑制が行われていたことを示すログ（CPU dynamic receive rate suppression finish）」が出力されることがありますが、一時的なものであれば動作に問題はありません。
バージョン	1.10.01

使用例：CPU 高負荷状態における CPU ポートでのパケット受信量を抑制する機能を無効にする方法を示します。

```
# configure terminal
(config)# dynamic cpu-receive suppression disable
(config)#
```

10.5.4 dynamic cpu-receive suppression interval

dynamic cpu-receive suppression interval	
目的	CPU 高負荷状態における CPU ポートでのパケット受信量を抑制する機能の監視間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
Command	dynamic cpu-receive suppression interval SECONDS no dynamic cpu-receive suppression interval
Parameter	SECONDS：監視間隔を 1～3 秒の範囲で指定します。
デフォルト	1 秒 (dynamic cpu-receive suppression interval 1)
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	通常運用中でも「CPU 宛てパケットの受信レート抑制が行われていたことを示すログ (CPU dynamic receive rate suppression finish)」が頻繁に出力される場合は、監視間隔を長く設定することでログ出力を減らす効果が期待できます。
制限・注意	-
バージョン	1.11.01

使用例：CPU 高負荷状態における CPU ポートでのパケット受信量を抑制する機能の監視間隔を 3 秒に設定する方法を示します。

```
# configure terminal
(config)# dynamic cpu-receive suppression interval 3
(config)#
```

10.5.5 snmp-server enable traps cpu-protect

snmp-server enable traps cpu-protect	
目的	CPU 使用率監視機能の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
Command	snmp-server enable traps cpu-protect no snmp-server enable traps cpu-protect
Parameter	なし
デフォルト	無効
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	本コマンドを有効にする場合は、snmp-server enable traps コマンドでグローバル設定も有効にしてください。
制限・注意	-
バージョン	1.08.02

使用例：CPU 使用率監視機能の SNMP トラップを有効にする方法を示します。

```
# configure terminal
(config)# snmp-server enable traps cpu-protect
(config)#
```

10.5.6 show cpu-protect trace

show cpu-protect trace	
目的	CPU 使用率監視機能の情報を表示します。
Command	show cpu-protect trace
Parameter	なし
モード	ユーザー実行モード、特権実行モード、任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限・注意	-
バージョン	1.08.02 1.10.01：表示項目の仕様変更

使用例：CPU 使用率監視機能の情報を表示する方法を示します。

```
# show cpu-protect trace

CPU Protect Trace Trigger State     : Enabled ...(1)
CPU Protect Trace Trigger Status    : Exhausted ...(2)
Utilization Thresholds              : 100% ...(3)
Utilization polling                 : 60s ...(4)
CPU Protect Trace History State     : Enabled ...(5)
Traced log                          : Collected ...(6)
[2020-06-26 15:17:55]CPU Utilization: 65% ...(7)
[2020-06-26 15:23:16]CPU Utilization: 62%
[2020-06-26 15:24:05]CPU Utilization: 75%
```

項番	説明
(1)	CPU 使用率監視機能の有効(Enabled)／無効(Disabled)を表示します。
(2)	CPU 使用率監視機能の状態を表示します。 Normal：CPU 使用率がしきい値を上回っていない状態 Exhausted：CPU 使用率がしきい値を上回っている状態
(3)	CPU 使用率のしきい値(%)を表示します。
(4)	CPU 使用率の監視間隔(秒)を表示します。
(5)	CPU に関する履歴ログの採取機能の有効(Enabled)／無効(Disabled)を表示します。
(6)	CPU に関する履歴ログの記録状態を表示します。 No collection：履歴ログが記録されていない状態 Collected：履歴ログが記録されている状態
(7)	指定した監視間隔の平均 CPU 使用率がしきい値を上回った履歴を表示します。

10.5.7 clear cpu-protect trace history

clear cpu-protect trace history	
目的	平均 CPU 使用率がしきい値を上回った場合に採取された、CPU に関する履歴ログを

clear cpu-protect trace history	
	削除します。
Command	clear cpu-protect trace history
Parameter	なし
モード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドを実行すると、show tech-support cpu-trace-history コマンドや show cpu-protect trace コマンドで表示される CPU に関する履歴ログが削除されます。
制限・注意	-
バージョン	1.10.01

使用例：CPU に関する履歴ログを削除する方法を示します。

```
# clear cpu-protect trace history
#
```

10.6 CPU 保護コマンド

CPU 保護関連の設定コマンドは以下のとおりです。

- cpu-protect type dhcp

10.6.1 cpu-protect type dhcp

cpu-protect type dhcp	
目的	CPU 宛ての DHCP パケットに対してレート制限を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
Command	cpu-protect type dhcp pps RATE no cpu-protect type dhcp
Parameter	RATE：レート制限値を 0～1024(pps)の範囲で指定します。0 指定時は対象パケットをすべて破棄します。
デフォルト	なし
モード	グローバル設定モード
特権レベル	レベル：12
ガイドライン	DHCP リレー機能を使用するケースにおいて DHCP パケットトラフィックが多く到着すると、CPU の受信処理に時間をとられて、装置機能に悪影響を及ぼす可能性があります。この影響を軽減するために、本コマンドで CPU 宛てレート制限をすることができます。
制限・注意	• cpu-protect type コマンドで、コマンドリファレンスに記載されている以外のパラメーターを指定して使用することは未サポートです。
バージョン	1.12.01

使用例：DHCP パケットの CPU 宛てレート制限を 150pps に設定する方法を示します。

```
# configure terminal
(config)# cpu-protect type dhcp pps 150
(config)#
```

11 付録

11.1 システム復旧手順(パスワードのリセット)

ネットワーク管理者は、システム復旧機能を利用してパスワードをリセットできます。システム復旧手順を実行すると、保存されている設定はデフォルト設定に戻ります。また、SSH サーバーの RSA 鍵対と DSA 鍵対も削除されます。なお、装置のコンソールポートに直接接続が可能な場合だけ、システム復旧機能を利用できます。

■ 装置にユーザーアカウントが存在する場合

装置にユーザーアカウントが存在する場合のシステム復旧手順を以下に示します。

1. パラメーター設定端末を、装置のコンソールポートに接続します。
2. 装置の電源を入れます。
3. ログイン画面が表示されたら、Username フィールドに「ap_recovery」と入力して、Enter キーを押します。
4. 装置が再起動した後は設定がデフォルト設定に戻されているため、ユーザーアカウントおよびパスワードを入力せずにユーザー実行モードで CLI にアクセスが許可されます。

```
Ethernet Switch ApresiaNP2500-8MT4X-PoE

Firmware: Build 1.08.02


User Verification Access
Username:ap_recovery
System will be reset, save and reboot!
Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

■ 装置にユーザーアカウントが存在しない場合

装置にユーザーアカウントが存在しないが、enable パスワードが設定されている場合のシステム復旧手順を以下に示します。

1. パラメーター設定端末を、装置のコンソールポートに接続します。
2. 装置の電源を入れます。
3. ユーザー実行モードにログインしたら、enable コマンドを使用し、Password フィールドに「ap_recovery」と入力して、Enter キーを押します。
4. 装置が再起動した後は設定がデフォルト設定に戻されているため、enable パスワード設定もデフォルトの未設定になります。

```
Ethernet Switch ApresiaNP2500-8MT4X-PoE

Firmware: Build 1.08.02

> enable
Password:ap_recovery          <-- 実際は**********と表示されます

System will be reset, save and reboot!
Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

AEOS-NP2500 Ver. 1.13 コマンドリファレンス

2025 年 3 月 初版

APRESIA Systems 株式会社
東京都中央区築地二丁目 3 番 4 号
メトロシティ築地新富町
https://www.apresiasystems.co.jp/