TD61-7358E

ApresiaNP2000 シリーズ

AEOS-NP2000 Ver. 1.09

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
-	2020年11月30日	• TD61-7092D AEOS-NP2000 Ver. 1.08 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 • 「2.1 インターフェースコマンド」の以下を修正 - interface を修正 - interface range のパラメーターを修正 - show interfaces の使用例を修正 - show counters の対象バージョン、使用例を修正 • 「2.2 ポート設定コマンド」の以下を修正 - snmp-server enable traps sfp を追加 • 「2.3 ブザーおよびアラーム LED コマンド」の以下を修正 - alarm buzzer beep-type を修正 • 「2.5 PoE コマンド」の以下を修正 - poe power-inline を修正 - poe power-inline never の注意事項、使用例を追加 - show poe power-inline の対象バージョン、使用例を修正 • 「2.6 PD モニタリングコマンド」の以下を修正 - pd-monitoring restart-poe retry のガイドラインを修正、注意事項を追加 • 「2.7 スタックコマンド」の以下を修正 - show stack を修正 • 「3.9 システムファイル管理コマンド」の以下を修正 - backup clone を修正 - reboot を修正 - backup を修正 - restore を修正 • 「4.8 NTP コマンド」の以下を修正 - ntp update-calendar を修正 - show ntp associations の使用例を修正 • 「4.12 sFlow コマンド」の以下を修正 - show sflow の使用例を修正 • 「4.13 SNMP コマンド」の以下を修正 - snmp-server の注意事項を追加 - snmp-server enable traps snmp の制限事項を追加 - snmp-server enable traps environment を修正 - show snmp-server traps の対象バージョン、使用例を修正 • 「4.19 Zero Touch Provisioning(ZTP)コマンド」の以下を修正 - ztp enable のガイドラインを修正 - show ztp を修正 • 「4.20 タイムレンジコマンド」を追加 • 「5.6 ループ検知コマンド」の以下を修正 - loop-detection no-check-src の注意事項を修正 • 「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 を修正 - snmp-server enable traps storm-control を追加 - show storm-control を修正

No.	年　月　日	内　容
		• 「5.12 MMRP-Plus コマンド」の以下を修正 - mmrp-plus vlangroup slave-vid の注意事項を追加 • 「5.13 スパニングツリープロトコルコマンド」の以下を修正 - forward-bpdu global enable を追加 - spanning-tree global state の制限事項を追加 - spanning-tree forward-bpdu を修正 • 「7.1 優先制御(QoS)コマンド」の以下を修正 - cpu rate-limit を追加 • 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 - acl-hardware-counter の制限事項を修正 - mac access-list enable ip-packets を追加 - match ip address を修正 - match ipv6 address を修正 - match mac address を修正 - action を修正 • 「9.1 AccessDefender 共通コマンド」の以下を修正 - authentication web-mac abort-if-failure を追加 - show access-defender rule-statistics の使用例を修正 - copy (AccessDefender)を修正 - access-defender erase を修正 • 「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 authentication mac-auth を修正 - aaa authentication web-auth を修正 - show tacacs statistics の制限事項を追加 • 「9.4 IEEE 802.1X 認証コマンド」の以下を修正 - dot1x timeout server-timeout を追加 • 「9.6 Web 認証コマンド」の以下を修正 - web-authentication http-port を修正 - web-authentication https-port を修正 - web-authentication redirect proxy-port の制限事項を修正 - web-authentication interface を追加 - web-authentication snooping proxy-port の制限事項を修正 - show access-defender webpages を追加 • 「9.7 Web アクセス拒否通知コマンド」を追加 • 「10.1 デバッグコマンド」の以下を修正 - show tech-support のパラメーター、対象バージョンを追加 • 「10.5 CPU 使用率監視コマンド」の以下を修正 - snmp-server enable traps environment memory を追加
A	2021 年 1 月 29 日	• 全章を対象に誤字・脱字・体裁を修正 • 「1.2 コマンドシンタックス」を修正 • 「2.2 ポート設定コマンド」の以下を修正 - speed を修正 - duplex を修正 - speed_duplex (mgmt 0)を修正 • 「2.5 PoE コマンド」の以下を修正 - snmp-server enable traps poe のガイドラインを追加 • 「2.7 スタックコマンド」の以下を修正

No.	年　月　日	内　　容
		- stack bandwidth のガイドラインを修正 • 「3.2 ファイルシステムコマンド」の以下を修正 - dir の使用例を修正 - show storage media-info の使用例を修正 • 「3.4 アクセス管理コマンド」の以下を修正 - terminal length default のガイドラインを修正 - terminal width default のガイドラインと使用例を修正 - login (Line)を修正 - terminal length を修正 - terminal width の使用例を修正 • 「3.5 基本 IPv4 コマンド」の以下を修正 - ip address の目的とパラメーターを修正 - arp を修正 - show arp を修正 - show arp cache の使用例を修正 • 「3.6 基本 IPv6 コマンド」の以下を修正 - ipv6 address を修正 - ipv6 address eui-64 を修正 - ipv6 address dhcp を修正 - ipv6 address autoconfig を修正 - ipv6 neighbor を修正 - show ipv6 general-prefix を修正 • 「3.7 IP ユーティリティーコマンド」の以下を修正 - ping を修正 • 「4.3 DHCP サーバーコマンド」の以下を修正 - host の使用例を修正 - hardware-address を修正 - client-identifier の使用例を修正 • 「4.4 DHCPv6 クライアントコマンド」の以下を修正 - ipv6 dhcp client pd を修正 - show ipv6 dhcp interface の使用例を修正 • 「4.15 LLDP コマンド」の以下を修正 - lldp receive の使用例を修正 - lldp transmit の使用例を修正 - show lldp の使用例を修正 - show lldp interface の使用例を修正 - show lldp local interface の使用例を修正 • 「4.18 CFM コマンド」の以下を修正 - cfm mp-ltr-all を修正 - show cfm linktrace を修正 - show cfm mp-ltr-all の目的と使用例を修正 - cfm linktrace を修正 - cfm loopback test を修正 - clear cfm linktrace を修正 • 「5.1 FDB コマンド」の以下を修正 - mac-address-table static を修正 - show mac-address-table を修正

No.	年　月　日	内　容
		- clear mac-address-table を修正 • 「5.4 ポートリダンダントコマンド」の以下を修正 - redundant fdb-flush dst-mac のパラメーターを修正 • 「5.13 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 mode のガイドラインを追加 - show spanning-tree の使用例を修正 - show spanning-tree mst の使用例を修正 • 「5.17 プライベート VLAN コマンド」の以下を修正 - switchport mode private-vlan の使用例を修正 • 「5.18 VLAN トンネルコマンド」の以下を修正 - vlan mapping rule のガイドラインを追加 - switchport vlan mapping profile の制限事項を修正 • 「5.19 Voice VLAN コマンド」の以下を修正 - voice vlan mac-address のパラメーターを修正 • 「6.1 プロトコル非依存コマンド」の以下を修正 - ip route のパラメーターを修正 • 「7.1 優先制御(QoS)コマンド」の以下を修正 - match のガイドラインを修正 • 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 - permit | deny (expert access-list)のガイドラインを追加 - permit | deny (mac access-list)のガイドラインを追加 • 「9.1 AccessDefender 共通コマンド」の以下を修正 - access-defender static mac のパラメーターを修正 - access-defender deny のパラメーターを修正 - access-defender logout のパラメーターを修正
B	2021 年 3 月 31 日	• 全章を対象に誤字・脱字・体裁を修正 • 全章を対象にコマンドモード遷移に関する記載を修正 • 5.1 章の名称を「FDB コマンド」に修正 • 「3.4 アクセス管理コマンド」の以下を修正 - banner login を修正 - line の使用例を修正 - clear line を修正 • 「3.9 システムファイル管理コマンド」の以下を修正 - backup clone の注意事項を修正 - copy primary-config secondary-config を copy から分離して追加 - copy を修正 - backup の注意事項を修正 • 「4.12 sFlow コマンド」の以下を修正 - sflow receiver を修正 - sflow sampler を修正 - sflow poller を修正 - show sflow の使用例を修正 • 「4.18 CFM コマンド」の以下を修正 - cfm enable のガイドラインを修正 - cfm ma のガイドラインを修正 - cfm mep のガイドラインを修正 - show cfm mip ccm の使用例を修正

No.	年　月　日	内　　容
		- show cfm pkt-cnt interface の使用例を修正 • 「5.11 リングプロテクション(ERPS)コマンド」関連の使用例を修正 • 「5.11 リングプロテクション(ERPS)コマンド」の以下を修正 - instance (ERPS)を修正 - sub-ring を修正 - profile (ERPS)を修正 • 「5.13 スパニングツリープロトコルコマンド」の以下を修正 - show spanning-tree configuration interface の使用例を修正 • 「5.16 VLAN コマンド」の以下を修正 - vlan を修正 - name (VLAN)のデフォルトを修正 - switchport mode を修正 - show vlan の使用例を修正 • 「5.18 VLAN トンネルコマンド」の以下を修正 - vlan mapping profile のガイドラインを修正 • 「6.1 プロトコル非依存コマンド」の以下を修正 - ip route を修正 - ipv6 route を修正 - show ip route を修正 - show ipv6 route を修正 • 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 - list-remark の使用例を修正 - expert access-group を修正 - expert access-list の使用例を修正 - permit | deny (expert access-list)のパラメーターを修正、制限事項を追加 - 「拡張エキスパートアクセスリストの抽出条件」を修正 - ip access-group を修正 - ip access-list のパラメーターと使用例を修正 - permit | deny (ip access-list)のパラメーターを修正、制限事項を追加 - 「IP アクセスリストの抽出条件」を修正 - ipv6 access-group を修正 - ipv6 access-list のパラメーターと使用例を修正 - permit | deny (ipv6 access-list)のパラメーターを修正、制限事項を追加 - 「IPv6 アクセスリストの抽出条件」を修正 - mac access-group を修正 - mac access-list の使用例を修正 - 「拡張 MAC アクセスリストの抽出条件」を修正 - show access-list のパラメーターを修正 • 「9.1 AccessDefender 共通コマンド」の以下を修正 - copy (AccessDefender)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 - dot1x initialize interface の注意事項を追加 - dot1x re-authenticate interface の注意事項を追加 • 「9.6 Web 認証コマンド」の以下を修正

No.	年　月　日	内　容
		- web-authentication interface の制限事項を追加 • 「10.1 デバッグコマンド」の以下を修正 - debug stack restart のパラメーターを修正 • 「10.4 システムログコマンド」の以下を修正 - command logging enable の制限事項を追加
C	2021 年 6 月 30 日	• 「ポート設定コマンド」の記載を、「2 インターフェースとハードウェア」配下に変更 • 「Gratuitous ARP コマンド」の記載を、「3 基礎知識」配下に変更 • 「ミラーリングコマンド」「LLDP コマンド」の記載を、「4 管理」配下に変更 • 「FDB コマンド」の記載を、「5 レイヤー2」配下に変更 • コマンド記載位置の見直しに伴い、過去の制定・改訂来歴表を修正 • 全章を対象に各章の記載順序・コマンドの記載順序を変更 • 全章を対象に各コマンドの見出しを追加 • 全章を対象に誤字・脱字・体裁を修正 • 「1 はじめに」に「適応機種と対応バージョン」を追加 • 「1 はじめに」を修正 • 「1.13 本書でのコマンド説明の記載項目」を修正 • 「2.7 スタックコマンド」の以下を修正 - stack bandwidth の制限事項を修正 • 「3.3 ターミナルコマンド」を追加し、関連コマンドを配下に変更 • 「3.8 Gratuitous ARP コマンド」の以下を修正 - ip gratuitous-arps を修正 • 「4.5 DHCPv6 サーバーコマンド」の以下を修正 - address prefix の制限事項を追加 - address-assignment の制限事項を追加 - prefix-delegation pool の制限事項を追加 - prefix-delegation の制限事項を追加 • 「4.8 NTP コマンド」の以下を修正 - show ntp associations の注意事項を追加、使用例を修正 • 「4.9 TELNET コマンド」を追加し、関連コマンドを配下に変更 • 「4.10 SSH コマンド」の以下を修正 - crypto key generate の注意事項を追加 • 「4.13 SNMP コマンド」の以下を修正 - show snmp user の使用例を修正 • 「4.14 ミラーリングコマンド」の以下を修正 - monitor session source acl のパラメーターとガイドラインを修正 • 「4.18 CFM コマンド」の以下を修正 - cfm global enable の注意事項を追加 • 「5.3 ポートチャネルコマンド」の以下を修正 - channel-group を修正 - lacp port-priority を修正 - lacp timeout を修正 - lacp system-priority を修正 - port-channel load-balance を修正 - show channel-group を修正 - show channel-group channel を追加

No.	年　月　日	内　　容
		- show channel-group load-balance を追加 - show channel-group channel sys-id を追加 • 「5.4 ポートリダンダントコマンド」の以下を修正 - redundant fdb-flush send enable の注意事項を追加 - redundant fdb-flush receive enable の注意事項を追加 • 「5.6 ループ検知コマンド」の以下を修正 - loop-detection global enable の注意事項を追加 - loop-detection enable (Interface)の注意事項を追加 - loop-detection action notify-only の注意事項を追加 - loop-detection no-check-src の注意事項を追加 • 「5.7 ストームコントロールコマンド」の以下を修正 - storm-control の注意事項を追加 - storm-control action の注意事項を追加 • 「5.8 マルチキャストフィルタリングモードコマンド」を追加し、関連コマンドを配下に変更 • 「5.12 MMRP-Plus コマンド」の以下を修正 - mmrp-plus enable の注意事項を追加 - mmrp-plus ring ring-master のガイドライン、注意事項を修正 - mmrp-plus ring divided-master のガイドライン、注意事項を修正 - mmrp-plus ring divided-slave のガイドライン、注意事項を修正 - mmrp-plus ring aware のガイドライン、注意事項を修正 - debug mmrp を修正 • 「5.13 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 priority を修正 - spanning-tree (timers)を修正 - spanning-tree cost を修正 - spanning-tree port-priority を修正 - spanning-tree mst configuration のガイドラインを追加 - spanning-tree mst priority を修正 - spanning-tree mst を、spanning-tree mst cost と spanning-tree mst port-priority の 2 つに分割 - show spanning-tree を修正 - show spanning-tree configuration interface を修正 - show spanning-tree mst を修正 - clear spanning-tree detected-protocols を修正 • 「5.14 RPVST+コマンド」の以下を修正 - spanning-tree vlan を修正 - spanning-tree vlan priority を修正 - spanning-tree vlan (timers)を修正 - spanning-tree vlan cost を修正 - spanning-tree vlan port-priority を修正 - show spanning-tree vlan を修正 - show spanning-tree vlan interface を修正 • 「5.16 VLAN コマンド」の以下を修正 - switchport mode の注意事項を修正 - switchport trunk allowed vlan の注意事項を修正 - switchport hybrid allowed vlan の注意事項を修正

No.	年　月　日	内　容
		• 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 - vlan filter の注意事項を追加 - show access-list resource reserved-group の使用例を修正 - show access-list resource reserved-priority の使用例を修正 • 「9.1 AccessDefender 共通コマンド」の以下を修正 - total-client の注意事項を修正 • 「10.1 デバッグコマンド」の以下を修正 - debug reboot on-tscmoddown を追加 - debug show memory-pool を修正
D	2021 年 11 月 30 日	• 全章を対象に誤字・脱字・体裁を修正 • 「1 はじめに」を修正 • 「2.1 インターフェースコマンド」の以下を修正 - description のパラメーターを修正 - shutdown のガイドラインを修正 - show interfaces の使用例を修正 - show interfaces status の使用例を修正 - show interfaces description の使用例を修正 - show counters の使用例を修正 • 「2.2 ポート設定コマンド」の以下を修正 - speed の使用例を修正 • 「2.3 ブザーおよびアラーム LED コマンド」の以下を修正 - show alarm の使用例を修正 • 「2.5 PoE コマンド」の以下を修正 - poe pd description のパラメーターを修正 - show poe power module の使用例を修正 - show poe power-inline • 「2.6 PD モニタリングコマンド」の以下を修正 - pd-monitoring acl-mode access-list の制限事項を追加 • 「2.7 スタックコマンド」の以下を修正 - stack bandwidth を修正 - stack renumber を修正 - stack priority を修正 - stack my_box_id を修正 - stack my_box_priority を修正 - stack preempt を修正 - show stack の使用例を修正 - stack remove のガイドラインを追加 • 「3.1 基本 CLI コマンド」の以下を修正 - show unit の使用例を修正 • 「3.2 ファイルシステムコマンド」の以下を修正 - cd のガイドラインを追加 - delete のガイドライン、使用例を修正 - dir のガイドライン、使用例を修正 - mkdir のガイドラインを追加、使用例を修正 - more のガイドライン、使用例を修正 - rename のガイドライン、使用例を修正 - rmdir のガイドラインを追加、使用例を修正

No.	年　月　日	内　　容
		• 「3.4 アクセス管理コマンド」の以下を修正 - username を修正 - enable password のパラメーターを修正 - prompt を修正 - password のパラメーターを修正 - access-class を修正 • 「3.5 基本 IPv4 コマンド」の以下を修正 - ip address を修正 - show arp cache の制限事項を追加 • 「3.6 基本 IPv6 コマンド」の以下を修正 - ipv6 enable のガイドラインを追加 - ipv6 address eui-64 の制限事項を追加 - ipv6 address dhcp の制限事項を追加 - ipv6 address autoconfig のガイドライン、制限事項を追加 - show ipv6 neighbors cache の制限事項を追加 • 「3.7 IP ユーティリティーコマンド」の以下を修正 - ping access-class を修正 - ping のパラメーターを修正 - traceroute を修正 • 「3.9 システムファイル管理コマンド」の以下を修正 - boot image を修正 - boot config を修正 - show boot のガイドライン、使用例を修正 - show running-config を修正 - show startup-config を修正 - backup clone のガイドライン、対象バージョンを追加 - write を修正 - erase boot を修正 - configure replace のガイドライン、対象バージョンを追加 - copy のガイドライン、対象バージョンを追加 - backup のガイドラインを修正 - restore のガイドラインを修正 - clear running-config を修正 - reset system を修正 • 「4.1 DHCP クライアントコマンド」の以下を修正 - ip dhcp client class-id を修正 - ip dhcp client client-id を修正 - ip dhcp client hostname を修正 ip dhcp client lease を修正 • 「4.2 DHCP リレーコマンド」の以下を修正 - ip dhcp pool (DHCP Relay)のパラメーターを修正 • 「4.3 DHCP サーバーコマンド」の以下を修正 - ip dhcp pool (DHCP Server)のパラメーターを修正 - network のパラメーターを修正、注意事項を追加 - host のパラメーターを修正、注意事項を追加 - lease のパラメーターを修正 - domain-name のパラメーターを修正

No.	年　月　日	内　　容
		- option のパラメーター、使用例を修正 - ip dhcp class (DHCP Relay & Server)のパラメーターを修正 • 「4.4 DHCPv6 クライアントコマンド」の以下を修正 - ipv6 dhcp client pd のパラメーターを修正 • 「4.5 DHCPv6 サーバーコマンド」の以下を修正 - ipv6 dhcp pool のパラメーターを修正 - address prefix を修正 - address-assignment を修正 - domain-name (DHCPv6 Server)のパラメーターを修正 - prefix-delegation pool を修正 - prefix-delegation を修正 - ipv6 local pool のパラメーターを修正 • 「4.7 時刻および SNTP コマンド」の以下を修正 - show sntp の使用例を修正 • 「4.11 RMON コマンド」の以下を修正 - rmon collection stats を修正 - rmon collection history を修正 - rmon alarm を修正 - rmon event を修正 - show rmon statistics の使用例を修正 - show rmon history の使用例を修正 - show rmon alarm の使用例を修正 - show rmon events の使用例を修正 • 「4.12 sFlow コマンド」の以下を修正 - sflow receiver のパラメーターを修正 • 「4.13 SNMP コマンド」の以下を修正 - snmp-server name を修正 - snmp-server location を修正 - snmp-server contact を修正 - snmp-server community を修正 - snmp-server host を修正 - snmp-server user を修正 - snmp-server group を修正 - snmp-server view を修正 - snmp-server engineID local のガイドラインを追加 - show snmp-server の使用例を修正 • 「4.14 ミラーリングコマンド」の以下を修正 - monitor session source acl のガイドラインを修正 • 「4.15 LLDP コマンド」の以下を修正 - lldp subtype port-id の目的を修正 • 「4.16 EtherOAM コマンド」の以下を修正 - show ethernet oam event-log の使用例を修正 • 「4.18 CFM コマンド」の以下を修正 - cfm enable のガイドラインを修正 - cfm domain のパラメーターを修正 - cfm ma のパラメーターを修正 - show cfm mepid の使用例を修正

No.	年　月　日	内　　容
		• 「4.20 タイムレンジコマンド」の以下を修正 - time-range のパラメーターを修正 • 「5.4 ポートリダンダントコマンド」の以下を修正 - redundant group-number preempt のパラメーターを修正 - show redundant の使用例を修正 • 「5.7 ストームコントロールコマンド」の以下を修正 - storm-control の制限事項を修正 - storm-control action のパラメーター、制限事項を修正 • 「5.8 マルチキャストフィルタリングモードコマンド」の以下を修正 - show multicast filtering-mode の使用例を修正 • 「5.9 IGMP スヌーピングコマンド」の以下を修正 - show ip igmp snooping statistics の使用例を修正 • 「5.11 リングプロテクション(ERPS)コマンド」の以下を修正 - ethernet ring g8032 profile のパラメーターを修正 - ethernet ring g8032 のパラメーターを修正 - description (ERPS)のパラメーターを修正 • 「5.12 MMRP-Plus コマンド」の以下を修正 - mmrp-plus ring name のパラメーターを修正 - show mmrp-plus status port の使用例を修正 - show mmrp-plus status ring の使用例を修正 • 「5.13 スパニングツリープロトコルコマンド」の以下を修正 - name (MSTP)のパラメーターを修正 • 「5.16 VLAN コマンド」の以下を修正 - name (VLAN)のパラメーターを修正 - show vlan の使用例を修正 • 「5.17 プライベート VLAN コマンド」の以下を修正 - show vlan private-vlan の使用例を修正 • 「5.19 Voice VLAN コマンド」の以下を修正 - voice vlan mac-address のパラメーターを修正 - show voice vlan の使用例を修正 • 「6.1 プロトコル非依存コマンド」の以下を修正 - ip forwarding を追加 - ipv6 forwarding を追加 - show ip forwarding を追加 - show ipv6 forwarding を追加 • 「7.1 優先制御(QoS)コマンド」の以下を修正 - mls qos map dscp-mutation のパラメーターを修正 - queue rate-limit を修正 - class-map のパラメーターを修正 - match の制限事項を追加 - policy-map のパラメーターを修正 - mls qos aggregate-policer のパラメーターを修正 - show mls qos interface を削除 - show mls qos interface scheduler を追加 - show mls qos interface trust を追加 - show mls qos interface cos を追加 - show mls qos interface map dscp-cos を追加

No.	年　月　日	内　　容
		- show mls qos interface map cos-color を追加 - show mls qos interface map dscp-color を追加 - show mls qos interface dscp-mutation を追加 - show mls qos interface queue-rate-limit を追加 - show mls qos interface rate-limit を追加 - show policy-map の使用例を修正 • 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 - list-remark のパラメーター、ガイドラインを修正 - expert access-list のパラメーターを修正 - ip access-list のパラメーターを修正 - arp access-group を追加 - arp access-list を追加 - permit	deny (arp access-list)を追加 - ipv6 access-list のパラメーターを修正 - permit	deny (ipv6 access-list)を修正 - mac access-list のパラメーターを修正 - vlan access-map のパラメーター、ガイドラインを修正 - match ip address のガイドラインを修正 - match arp address を追加 - match ipv6 address のガイドラインを修正 - match mac address のガイドラインを修正 - show access-list を修正 - show access-list resource reserved-group の使用例を修正 - show access-list resource reserved-priority のガイドライン、使用例を修正 - show vlan filter を修正 • 「9.1 AccessDefender 共通コマンド」の以下を修正 - access-defender のガイドラインを追加 - logout aging-time のパラメーターを修正 - logout timeout のパラメーターを修正 - logout clock のパラメーターを修正 • 「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 - radius-server host を修正 - tacacs-server host を修正 - aaa group server radius のパラメーターを修正 - aaa group server tacacs+のパラメーターを修正 - aaa authentication login のパラメーターを修正 - aaa authentication mac-auth のガイドラインを追加 - aaa authentication dot1x のガイドラインを追加 - aaa authentication web-auth のガイドラインを追加 - aaa accounting commands のパラメーターを修正 - aaa accounting exec のパラメーターを修正 • 「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 • 「9.5 SSL コマンド」の以下を修正 - show ssl https-private-key の使用例を修正 • 「10.4 システムログコマンド」の以下を修正

No.	年　月　日	内　容
		- logging on を修正 - logging buffered を修正 - logging console を修正 - logging discriminator を修正 - logging server を修正 • 「10.5 CPU 使用率監視コマンド」の以下を修正 - cpu-protect system-memory limit-check fault-action reboot を修正 - cpu-protect system-memory limit-check threshold を修正
E	2022 年 2 月 28 日	• 全章を対象に誤字・脱字・体裁を修正 • 「2.1 インターフェースコマンド」の以下を修正 - show interfaces の使用例を修正 - show interfaces status の使用例を修正 - show interfaces utilization の使用例を修正 - show interfaces description を修正 • 「2.3 ブザーおよびアラーム LED コマンド」の以下を修正 - alarm state enable のパラメーター、ガイドラインを修正 - show alarm の使用例を修正 - debug alarm test のコマンドモード、使用例を修正 • 「2.4 省電力イーサネット(EEE)コマンド」の以下を修正 - show eee の使用例を修正 • 「2.5 PoE コマンド」の以下を修正 - poe pd priority を修正 - c-poe enable のガイドラインを追加 - show poe power module の使用例を修正 - show poe power-inline の使用例を修正 • 「2.6 PD モニタリングコマンド」の以下を修正 - show pd-monitoring の使用例を修正 • 「2.7 スタックコマンド」の以下を修正 - stack stack-port load-balance を修正 - show stack の使用例を修正 • 「3.3 ターミナルコマンド」の以下を修正 - show terminal の使用例を修正 • 「3.9 システムファイル管理コマンド」の以下を修正 - backup clone の注意事項を追加 - reboot のパラメーター、ガイドラインを修正 - copy boot の注意事項を追加 - configure replace の注意事項を追加 - backup の注意事項を追加 - restore の注意事項を追加 • 「4.10 SSH コマンド」の以下を修正 - ip ssh server のガイドライン、注意事項を追加 - show ssh の使用例を修正 - crypto key generate の注意事項を追加 • 「5.3 ポートチャネルコマンド」の以下を修正 - port-channel load-balance のガイドラインを修正、使用例を追加 • 「5.13 スパニングツリープロトコルコマンド」の以下を修正

No.	年　月　日	内　　容
		- show spanning-tree の制限事項を追加 - show spanning-tree mst の制限事項を追加 • 「5.14 RPVST+コマンド」の以下を修正 - show spanning-tree vlan の制限事項を追加 - show spanning-tree vlan interface の制限事項を追加 • 「6.1 プロトコル非依存コマンド」の以下を修正 - ip forwarding のガイドライン、注意事項を修正 - ipv6 forwarding のガイドライン、注意事項を修正 • 「7.1 優先制御(QoS)コマンド」の以下を修正 - match の制限事項を追加 - service-policy を修正 • 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 - vlan filter の注意事項を追加 - show access-group のガイドライン、制限事項を追加 • 「9.5 SSL コマンド」の以下を修正 - ssl gencsr rsakey の注意事項を追加 • 「9.6 Web 認証コマンド」の以下を修正 - web-authentication overwrite enable を修正

目次

制定・改訂来歴表 1
1 はじめに 18
1.1 本文中の表記について 20
1.2 コマンドシンタックス 21
1.3 コンソールポートへの接続 23
1.4 初めての CLI への接続 25
1.5 ユーザーアカウント 26
1.6 ユーザーアカウントの作成 27
1.7 コマンドモード 28
1.8 インターフェースの表記法 30
1.9 VLAN インターフェース 31
1.10 エラーメッセージ 32
1.11 コマンド入力の補助機能 33
1.12 表示結果出力修飾子 34
1.13 本書でのコマンド説明の記載項目 35
2 インターフェースとハードウェア 36
2.1 インターフェースコマンド 36
2.2 ポート設定コマンド 61
2.3 ブザーおよびアラーム LED コマンド 68
2.4 省電力イーサネット(EEE)コマンド 77
2.5 PoE コマンド 79
2.6 PD モニタリングコマンド 90
2.7 スタックコマンド 98
3 基礎知識 109
3.1 基本 CLI コマンド 109
3.2 ファイルシステムコマンド 123
3.3 ターミナルコマンド 131
3.4 アクセス管理コマンド 135
3.5 基本 IPv4 コマンド 146
3.6 基本 IPv6 コマンド 156
3.7 IP ユーティリティーコマンド 167
3.8 Gratuitous ARP コマンド 171
3.9 システムファイル管理コマンド 173
4 管理 202
4.1 DHCP クライアントコマンド 202
4.2 DHCP リレーコマンド 205
4.3 DHCP サーバーコマンド 219
4.4 DHCPv6 クライアントコマンド 246
4.5 DHCPv6 サーバーコマンド 250
4.6 DHCP Auto Configuration コマンド 266
4.7 時刻および SNTP コマンド 268
4.8 NTP コマンド 274
4.9 TELNET コマンド 287

4.10 SSH コマンド.....290
4.11 RMON コマンド.....298
4.12 sFlow コマンド.....307
4.13 SNMP コマンド.....315
4.14 ミラーリングコマンド.....339
4.15 LLDP コマンド.....348
4.16 EtherOAM コマンド.....377
4.17 単方向リンク検出(ULD)コマンド.....392
4.18 CFM コマンド.....396
4.19 Zero Touch Provisioning(ZTP)コマンド.....429
4.20 タイムレンジコマンド.....434
5 レイヤー2.....437
5.1 FDB コマンド.....437
5.2 ジャンボフレームコマンド.....445
5.3 ポートチャネルコマンド.....446
5.4 ポートリダンダントコマンド.....455
5.5 リンクダウン連携コマンド.....461
5.6 ループ検知コマンド.....464
5.7 ストームコントロールコマンド.....473
5.8 マルチキャストフィルタリングモードコマンド.....482
5.9 IGMP スヌーピングコマンド.....484
5.10 MLD スヌーピングコマンド.....504
5.11 リングプロテクション(ERPS)コマンド.....523
5.12 MMRP-Plus コマンド.....537
5.13 スパニングツリープロトコルコマンド.....566
5.14 RPVST+コマンド.....592
5.15 トラフィックセグメンテーションコマンド.....600
5.16 VLAN コマンド.....602
5.17 プライベート VLAN コマンド.....616
5.18 VLAN トンネルコマンド.....622
5.19 Voice VLAN コマンド.....636
6 レイヤー3.....645
6.1 プロトコル非依存コマンド.....645
6.2 IPv4 マルチキャストコマンド.....654
6.3 IPv6 マルチキャストコマンド.....655
7 優先制御(QoS).....656
7.1 優先制御(QoS)コマンド.....656
8 アクセスリスト(ACL).....696
8.1 アクセスリスト(ACL)コマンド.....696
9 セキュリティー.....739
9.1 AccessDefender 共通コマンド.....739
9.2 認証、許可、アカウンティング(AAA)コマンド.....774
9.3 MAC 認証コマンド.....803
9.4 IEEE 802.1X 認証コマンド.....807
9.5 SSL コマンド.....821

9.6 Web 認証コマンド 825
9.7 Web アクセス拒否通知コマンド 838
9.8 DHCP スヌーピングコマンド 845
10 サポート 853
10.1 デバッグコマンド 853
10.2 エラー復旧コマンド 876
10.3 メモリーエラー自動復旧コマンド 879
10.4 システムログコマンド 882
10.5 CPU 使用率監視コマンド 894
11 付録 898
11.1 システム復旧手順(パスワードのリセット) 898

1 はじめに

■本書の目的
ApresiaNP2000 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
ApresiaNP2000-24T4X	AEOS-NP2000 Ver. 1.01.01～
ApresiaNP2000-48T4X	AEOS-NP2000 Ver. 1.01.01～
ApresiaNP2000-24T4X-PoE	AEOS-NP2000 Ver. 1.05.01～
ApresiaNP2000-48T4X-PoE	AEOS-NP2000 Ver. 1.05.01～

■対象読者
ネットワーク管理の概念と用語に精通したネットワーク管理者の方を対象としています。

■製品名の表記について
本書では、ApresiaNP2000-24T4X、ApresiaNP2000-48T4X、ApresiaNP2000-24T4X-PoE、および ApresiaNP2000-48T4X-PoE を「装置」、「ブリッジ」、または「ルーター」と表記します。

■運用上のご注意
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。
ApresiaNP2000 シリーズでは以下のレイヤー3 中継機能をサポートしています。

- VLAN 間のレイヤー3 中継
- スタティックルート

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
APRESIA は、APRESIA Systems 株式会社の登録商標です。
AEOS は、APRESIA Systems 株式会社の登録商標です。
MMRP は、APRESIA Systems 株式会社の登録商標です。
AccessDefender は、APRESIA Systems 株式会社の登録商標です。
Ethernet およびイーサネットは、富士フイルムビジネスイノベーション株式会社の登録商標です。
sFlow は、米国 InMon Corp.の登録商標です。
その他ブランド名は、各所有者の商標もしくは登録商標です。

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
太字	コマンド、およびパラメーターの強調表示です。コマンドラインでは、表記のとおりにパラメーターを正確に入力してください。
大文字斜体	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。ユーザー定義のパラメーター例を示す場合にも使用します。
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。
Courier フォント	画面コンソールの表示例を示します。例えば、CLI コマンドの入力と、入力したコマンドに対応する出力を示します。
太字斜体「(1)」	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

コマンドの入力方法と値や引数の指定方法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、および 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。

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 キー	カーソルを行頭へ移動します。
Ctrl+E キー	カーソルを行末へ移動します。
Ctrl+K キー	カーソル位置の文字から行末までを削除します。
Ctrl+Z キー	グローバル設定モードまたはサブ設定モードの場合に、入力途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 キー	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 キー	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 キー	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、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。
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。

編集機能	
	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 キー、Esc キー、または Q キー：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：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: 00-40-66-B4-96-B5
  H/W Version: A

Power On Self Test: 100 %

Please Wait, Loading V1.07.01

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...
```

AEOS-NP2000 Ver. 1.07.01 以降では 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 enable**（デフォルト設定）で、startup-config が工場出荷状態の場合
- **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 ApresiaNP2000-24T4X

Firmware: Build 1.03.01

>
```

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。

- 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。
- 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。

1.5 ユーザーアカウント

セキュリティー上、装置のインターフェースに対するアクセスを管理して、制御するためのユーザーアカウントを作成することを推奨します。ユーザーアカウントは、割り当てられている特権レベルに応じて相互に区別されます。例えば、特権レベルが 15 のユーザーアカウントを作成すると、Administrator ユーザーアカウントが作成されます。

下表に示す定義済みの特権レベルを使用して、ユーザーアカウントを作成できます。

特権レベル	ユーザーアカウント	コマンドモード	説明
レベル 1	Basic User	ユーザー実行モード	すべてのユーザーアカウントの中で、最も低い特権レベルです。必要最小限のコマンドを実行できます。主に監視用の表示コマンドにアクセスするために使用します。
レベル 12	Operator	特権実行モード グローバル設定モード 制限付き設定モード	装置の CLI で使用できる表示コマンド、および設定コマンドの大半にアクセスできます。セキュリティー関連の設定は行えません。
レベル 15	Administrator	特権実行モード グローバル設定モード 任意の設定モード	装置の CLI で使用できるすべてのコマンドに、無制限にアクセスできます。

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。ユーザーは、ユーザー実行モードまたは特権実行モードのどちらかにログインします。

- Basic User アカウントは、ユーザー実行モードで装置にログインします。
- Operator アカウントと Administrator アカウントは、特権実行モードで装置にログインします。

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 ApresiaNP2000-24T4X

Firmware: Build 1.08.01

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。各コマンドモードでは、装置の特定の機能を設定するための、固有のコマンドのセットが提供されます。

ユーザーアカウント、およびユーザーアカウントの特権レベルによって、ログイン後のモードは以下のどちらかになります。

- ユーザー実行モード
- 特権実行モード

特権実行モードでは、グローバル設定モードにアクセスできます。また、グローバル設定モードでは、インターフェース設定モードなどの他の設定モードにアクセスできます。インターフェース設定モードなどの他の設定モードは、一般的にはサブ設定モードとして分類されます。サブ設定モードに分類される設定モードの例を以下に示します。

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

コマンドモードと特権レベルの説明を以下に示します。

コマンドモード	特権レベル	説明
ユーザー実行モード >	レベル 1	基本のシステム設定をチェックするための、制限された表示コマンドにアクセスできます。レベル 1 ユーザーアカウントが使用できる最上位のコマンドモードです。
特権実行モード #	レベル 12	ほとんどの表示コマンドにアクセスできます。ローカルとグローバルの端末設定を設定できます。また、制限されたシステム管理タスクを実行できます。ほとんどの clear コマンド操作は、このレベルで実行されます。
	レベル 15	このモードで提供されるすべてのコマンドにアクセスできます。
グローバル設定モード (config)#	レベル 12	ほとんどのグローバル設定操作を実行できます。また、ほとんどのサブ設定モードへのアクセスと、サブ設定モードより下位の操作を実行できます。ただし、セキュリティー関連の設定は、実行できません。
	レベル 15	このモードで提供されるすべてのコマンド、およびすべてのサブ設定モードへのアクセスが可能です。また、サブ設定モードより下位の操作を実行できます。

インターフェース設定モードの説明を以下に示します。

コマンドモード	説明
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です。
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です。
インターフェース設定モード(port-channel)	ポートチャネル関連の設定を、指定したポートチャ

コマンドモード	説明
(config-if-port-channel)#	ネルで実施する設定モードです。
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です。
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です。
インターフェース設定モード(l2vlan) (config-if-l2vlan)#	レイヤー2 VLAN インターフェース関連の設定を実施する設定モードです。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

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/空きスロットの 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 1 です。
  - 空きスロットの 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"という文字列を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"という文字列を入力した時点で[TAB]キーを押した場合は、"show environment "という文字列に補完されます。

```
# 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"という文字列を入力した時点で[?]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 "という文字列を入力した時点で[?]キーを押した場合は、"show environment "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
temperature               Display temperature status
|                         Output modifiers
<cr>

# show environment
```

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 1/0/46
interface port 1/0/46
interface port 1/0/47
interface port 1/0/48
interface port 1/0/49
interface port 1/0/50
interface port 1/0/51
interface port 1/0/52

# SSH

ip ssh server
ssh user user1 authentication-method password

#-------------------------------------------------------------------
#             End of configuration file for ApresiaNP2000-48T4X
#-------------------------------------------------------------------
```

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     10           a-full  a-1000         1000BASE-T
Port1/0/33    disabled      trunk        auto    auto           1000BASE-T
Port1/0/34    disabled      trunk        auto    auto           1000BASE-T
Port1/0/49    connected     trunk        a-full  a-10G          10GBASE-R
Port1/0/50    connected     trunk        a-full  a-10G          10GBASE-R

Total Entries: 52
```

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。
シンタックス	コマンド構文を示します。
パラメーター	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	工場出荷時のデフォルト状態とパラメーター値を示します。
コマンドモード	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	コマンドの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。
制限事項	コマンドの制限事項を示します。
注意事項	コマンドの注意事項を示します。
対象バージョン	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。

コマンド	コマンドとパラメーター
interface	interface INTERFACE-ID no interface INTERFACE-ID
interface range	interface range INTERFACE-ID [,|-]
description	description STRING no description
shutdown	shutdown no shutdown
default port-shutdown	default port-shutdown no 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。

コマンド	コマンドとパラメーター
show interfaces	show interfaces [INTERFACE-ID [,|-]]
show interfaces counters	show interfaces [INTERFACE-ID [,|-]] counters [errors]
show interfaces status	show interfaces [INTERFACE-ID [,|-]] status
show interfaces utilization	show interfaces [INTERFACE-ID [,|-]] utilization
show interfaces gbic	show interfaces [INTERFACE-ID [,|-]] gbic
show interfaces description	show interfaces [INTERFACE-ID [,|-]] description
show interfaces auto-negotiation	show interfaces [INTERFACE-ID [,|-]] auto-negotiation
show interfaces transceiver	show interfaces [INTERFACE-ID [,|-]] transceiver [detail]
show counters	show counters [interface INTERFACE-ID [,|-] | cpu-port | internal-port | stack-port]
clear counters	clear counters {all | interface INTERFACE-ID [,|-] | cpu-port | internal-port | stack-port}

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。
シンタックス	**interface** *INTERFACE-ID* **no interface** *INTERFACE-ID*

interface	
パラメーター	*INTERFACE-ID*：インターフェースを指定します。インターフェースは、インターフェースの種類とインターフェース番号から構成されます。本コマンドでは、インターフェースの種類とインターフェース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。インターフェースには以下のパラメーターを指定します。 • port：物理ポートを指定します。物理ポート番号の範囲は装置により異なります。また、スタックポートに設定した物理ポートは指定できません。 • port-channel 〈1-48〉：ポートチャネルを指定します。 • vlan 〈1-4094〉：VLAN インターフェースを指定します。設定済みの VLAN に対してのみ指定できます。 • mgmt 〈0〉：マネージメントポートを指定します。 • l2vlan 〈1-4094〉：レイヤー2 VLAN インターフェースを指定します。 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)# • 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。
コマンドモード	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	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。 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

interface	
	に削除されます。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)# 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。
シンタックス	interface range *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：範囲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。 • port：物理ポートを指定します。複数指定できます。物理ポート番号の範囲は装置により異なります。また、スタックポートに設定した物理ポートは指定できません。 • l2vlan 〈1-4094〉：レイヤー2 VLAN インターフェースを指定します。複数指定できます。 各パラメーターを指定して範囲設定の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-range)# • l2vlan 指定時：(config-if-l2vlan-range)#
デフォルト	なし
コマンドモード	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	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。

interface range	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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。
シンタックス	**description** *STRING* **no description**
パラメーター	*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
コマンドモード	インターフェース設定モード(port, range, 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**shutdown** **no shutdown**
パラメーター	なし
デフォルト	有効（**no shutdown**）
コマンドモード	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。

shutdown	
	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	default port-shutdown no default port-shutdown
パラメーター	なし
デフォルト	無効
コマンドモード	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	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
制限事項	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。
注意事項	-
対象バージョン	1.06.01

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。
シンタックス	show interfaces [*INTERFACE-ID* [,|-]]
パラメーター	*INTERFACE-ID*（省略可能）：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：物理ポートを指定します。複数指定できます。 • vlan <1-4094>：VLAN インターフェースを指定します。 • mgmt <0>：マネージメントポートを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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

```
# show interfaces vlan 1

vlan1 is enabled, link status is up ...(1)
  Interface type: VLAN ...(2)
  Interface description: ...(3)
  MAC address: 00-40-66-AF-F0-48 ...(4)
```

項番	説明
(1)	VLAN インターフェースの状態を表示します。 enabled：有効（no shutdown） disabled：無効（shutdown） <link status is> up：VLAN インターフェースがアップ状態 down：VLAN インターフェースがダウン状態
(2)	インターフェースの種類を表示します。 VLAN：VLAN インターフェース
(3)	VLAN インターフェースの説明を表示します。
(4)	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

Port1/0/1 is enabled, link status is up ...(1)
  Interface type: 1000BASE-T ...(2)
  Interface description: ...(3)
  MAC Address: 00-40-66-AF-F0-49 ...(4)
  Auto-duplex, auto-speed, auto-mdix ...(5)
  Send flow-control: off, receive flow-control: off ...(6)
  Send flow-control oper: off, receive flow-control oper: off ...(7)
  Full-duplex, 1Gb/s ...(8)
```

```
  Maximum transmit unit: 1536 bytes ...(9)
  RX rate: 2344 bits/sec, TX rate: 0 bits/sec ...(10)
  RX bytes: 916, TX bytes: 0 ...(11)
  RX rate: 3 packets/sec, TX rate: 0 packets/sec ...(12)
  RX packets: 10, TX packets: 0 ...(13)
  RX multicast: 6, RX broadcast: 4 ...(14)
  RX CRC error: 0, RX undersize: 0 ...(15)
  RX oversize: 0, RX fragment: 0 ...(16)
  RX jabber: 0, RX dropped Pkts: 3 ...(17)
  RX MTU exceeded: 0 ...(18)
  TX CRC error: 0, TX excessive deferral: 0 ...(19)
  TX single collision: 0, TX excessive collision: 0 ...(20)
  TX late collision: 0, TX collision: 0 ...(21)
```

項番	説明
(1)	ポートの状態を表示します。 enabled：有効（**no shutdown**） disabled：無効（**shutdown**） <link status is> 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 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
(2)	インターフェースの種類を表示します。 1000BASE-T：RJ-45 ポート(10BASE-T/100BASE-TX/1000BASE-T) 10GBASE-R：SFP/SFP+ポート
(3)	ポートの説明を表示します。
(4)	ポートの MAC アドレスを表示します。
(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> 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） 1000　　：1000Mbps（**speed 1000** 設定時） 1000 maste ：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）

項番	説明
	cross-mdix ：MDI モード（mdix cross 設定時）
(6)	送信時および受信時のフロー制御設定を表示します。 off：フロー制御機能は無効設定（flowcontrol off） on：フロー制御機能は有効設定（flowcontrol on）
(7)	送信時および受信時のフロー制御の実動作を表示します。 off：フロー制御機能は無効状態 on：フロー制御機能は有効状態
(8)	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, 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
(9)	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。
(10)	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。
(11)	受信バイト数、および送信バイト数を表示します。
(12)	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。
(13)	受信パケット数、および送信パケット数を表示します。
(14)	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。
(15)	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。
(16)	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。
(17)	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）。なお、ApresiaNP2000-48T4X(-PoE)は対象外で、非スタック装置の場合でもカウントしません。 • 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。

項番	説明
	• 対象が Layer3 中継パケットで、宛先ルート情報が存在しないで破棄される場合。 • 対象が Layer3 中継パケットで、不正な IP パケットの場合（例：IP チェックサムエラー）。
(18)	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。
(19)	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。
(20)	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。
(21)	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 0 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

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

項番	説明
(1)	マネージメントポートの状態を表示します。 enabled：有効（**no shutdown**） disabled：無効（**shutdown**） <link status is> up：リンクアップ状態 down：リンクダウン状態
(2)	インターフェースの種類を表示します。 Management port：マネージメントポート
(3)	マネージメントポートの説明を表示します。
(4)	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	指定したインターフェースのカウンターを表示します。
シンタックス	**show interfaces** [*INTERFACE-ID* [,|-]] **counters** [**errors**]
パラメーター	*INTERFACE-ID*（省略可能）：カウンターを表示するインターフェースを、以下の

show interfaces counters	
	パラメーターで指定します。 • port：物理ポートを指定します。複数指定できます。 • mgmt〈0〉：マネージメントポートを指定します。マネージメントポートの場合は、errors パラメーターは省略できません。 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。
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 1/0/2 の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)	受信バイ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 からポート 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。
シンタックス	show interfaces [*INTERFACE-ID* [,|-]] status
パラメーター	*INTERFACE-ID*（省略可能）：ポートの接続状態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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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         1000BASE-T
Port1/0/2      not-connected  1            auto    auto           1000BASE-T
Port1/0/3      not-connected  1            auto    auto           1000BASE-T
Port1/0/4      not-connected  1            auto    auto           1000BASE-T
Port1/0/5      not-connected  1            auto    auto           1000BASE-T
Port1/0/6      connected      1            a-full  a-1000         1000BASE-T
Port1/0/7      not-connected  1            auto    auto           1000BASE-T
Port1/0/8      not-connected  1            auto    auto           1000BASE-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(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

項番	説明
	※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。 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。
シンタックス	**show interfaces** [*INTERFACE-ID* [,|-]] **utilization**
パラメーター	*INTERFACE-ID*（省略可能）：使用率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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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。
シンタックス	**show interfaces** [*INTERFACE-ID* [,|-]] **gbic**
パラメーター	*INTERFACE-ID*（省略可能）：トランシーバーの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**：物理ポートを指定します。複数指定できます。

show interfaces gbic	
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/25 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 1/0/25 gbic

Port1/0/25 ...(1)
 Type: H-SR-SFP+ ...(2)
 Vendor PN: FTLX8571D3BCL ...(3)
 Vendor SN: ARK1CC0 ...(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。
シンタックス	show interfaces [*INTERFACE-ID* [,|-]] description
パラメーター	*INTERFACE-ID*（省略可能）：インターフェースの説明とリンク状態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：物理ポートを指定します。複数指定できます。 • vlan <1-4094>：VLAN インターフェースを指定します。 • mgmt <0>：マネージメントポートを指定します。 • l2vlan [<1-4094>]：レイヤー2 VLAN インターフェースを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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
 Port1/0/3              down      enabled
 Port1/0/4              down      disabled
～～省略～～
 Port1/0/26             down      enabled
 Port1/0/27             down      enabled
 Port1/0/28             down      enabled
 Mgmt 0                 up        enabled
 L2VLAN 1               up        enabled
 Interface vlan1        up        enabled         TEST VLAN 1 Interface

Total Entries: 31
```

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。 enabled：有効（**no shutdown**） disabled：無効（**shutdown**） なお、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。
(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。
シンタックス	**show interfaces** [*INTERFACE-ID* [,|-]] **auto-negotiation**
パラメーター	*INTERFACE-ID*（省略可能）：オートネゴシエーション情報の詳細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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 1/0/2 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 1/0/1-2 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: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full ...(6)
  Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full...(7)
  Capability Received Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full ...(8)
  RemoteFaultAdvertised: Disabled ...(9)
  RemoteFaultReceived: NoError ...(10)

 Port1/0/2
  Auto Negotiation: Enabled

  Speed auto downgrade: Disabled
  Remote Signaling: Not detected
  Configure Status: Configuring
  Capability Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
  Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
  Capability Received Bits: -
  RemoteFaultAdvertised: Disabled
  RemoteFaultReceived: NoError
```

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／無効を表示します。
(3)	speed auto-downgrade の有効／無効を表示します。
(4)	リモートシグナルの使用状況を表示します。
(5)	オートネゴシエーションの動作状況を表示します。
(6)	使用可能なスピードと duplex を表示します。
(7)	広告している Capability Bits を表示します。
(8)	受信している Capability Bits を表示します。
(9)	ローカルフォルト広告状態を表示します。
(10)	リモートフォルトの受信状態を表示します。

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。
シンタックス	**show interfaces** [*INTERFACE-ID* [,|-]] **transceiver** [**detail**]
パラメーター	*INTERFACE-ID*（省略可能）：光トランシーバーの動作状況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。
デフォルト	なし
コマンドモード	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トの情報が表示されます。
制限事項	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。
注意事項	**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。
対象バージョン	1.01.01

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)
---------- ------------ ------------ ------------ ------------
Port1/0/25 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統計情報を表示します。
シンタックス	**show counters** [**interface** *INTERFACE-ID* [,|-] | **cpu-port** | **internal-port** | **stack-port**]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：統計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**：物理ポートを指定します。複数指定できます。 **cpu-port**（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統計情報を表示する場合に指定します。 **internal-port**（省略可能）：ApresiaNP2000-48T4X および ApresiaNP2000-48T4X-PoE の内部ポートの統計情報を表示する場合に指定します。 **stack-port**（省略可能）：スタックポートの統計情報を表示する場合に指定します。
デフォルト	なし
コマンドモード	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。
制限事項	ApresiaNP2000 シリーズでは、txCoS0DropPkts～txCoS7DropPkts はカウントしません。
注意事項	-
対象バージョン	1.01.01 1.03.01：**cpu-port**、**internal-port**、**stack-port** パラメーター追加 1.09.01：**cpu-port** パラメーター指定時の表示内容変更

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。
(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。

項番	説明
(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)。なお、ApresiaNP2000-48T4X(-PoE)は対象外で、非スタック装置の場合でもカウントしません。 • 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 Layer3 中継パケットで、宛先ルート情報が存在しないで破棄される場合。 • 対象が Layer3 中継パケットで、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。
(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。 ApresiaNP2000 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。 ApresiaNP2000 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。 ApresiaNP2000 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。 ApresiaNP2000 シリーズでは、本項目はカウントしません。

項番	説明
(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。 ApresiaNP2000 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。 ApresiaNP2000 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。 ApresiaNP2000 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。 ApresiaNP2000 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：ApresiaNP2000-48T4X の内部ポートのカウンターを表示する方法を示します。

```
# show counters internal-port

Unit 2, Internal Port 1 counters
txDropPkts                          :                       0 ...(1)

Unit 2, Internal Port 2 counters
txDropPkts                          :                       0

Unit 2, Internal Port 3 counters
txDropPkts                          :                       0

Unit 2, Internal Port 4 counters
txDropPkts                          :                       0
```

項番	説明
(1)	送信パケットドロップカウンターを表示します。

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 27 counters
ifInErrors                          :                       0 ...(1)
txDropPkts                          :                       0 ...(2)

Unit 1, Stack Port 28 counters
ifInErrors                          :                       0
txDropPkts                          :                       0

Unit 2, Stack Port 27 counters
ifInErrors                          :                       0
txDropPkts                          :                       0

Unit 2, Stack Port 28 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)                (5) cpuTxDropPkts
CoS                cpuRxPkts            cpuTxDropPkts        Last occurrence
--- ----------------------- ----------------------- --------------------
0                       0                       0                       -
1                       0                       0                       -
2                       0                       0                       -
3                   19544                       0                       -
4                       0                       0                       -
5                       0                       0                       -
6                       0                       0                       -
7                       0                       0                       -

Unit 1, CPU Port counters rate (pps)
       (6)            (7)              (8)
 (2)   cpuRxPkts     Maximum          Maximum rate
CoS    rate(pps)       rate       last occurrence
--- ----------- ---------- --------------------
0             0          -                    -
1             0          -                    -
2             0          -                    -
3             0          1  2020-09-29 09:16:55
4             0          -                    -
5             0          -                    -
6             0          -                    -
7             0          -                    -
```

```
      (9)                    (10)        (11)                    (12)
 (2)  cpuTxDropPkts          Maximum     Maximum drop rate       Number of
 CoS      rate(pps)        drop rate      last occurrence      occurrences
--- -------------- -------------- -------------------- ------------
0               0              -                    -            -
1               0              -                    -            -
2               0              -                    -            -
3               0              -                    -            -
4               0              -                    -            -
5               0              -                    -            -
6               0              -                    -            -
7               0              -                    -            -

Unit 2, CPU Port counters
～～省略～～
```

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。
(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。
(5)	CoS ごとの送信パケットドロップが最後に発生した時刻を表示します。
(6)	CoS ごとの現在の受信パケットレート（pps）を表示します。
(7)	CoS ごとの受信パケットレートが最大を示したときの値（pps）を表示します。
(8)	CoS ごとの受信パケットレートが最大を示したときの時刻を表示します。
(9)	CoS ごとの現在の送信パケットドロップレート（pps）を表示します。
(10)	CoS ごとの送信パケットドロップレートが最大を示したときの値（pps）を表示します。
(11)	CoS ごとの送信パケットドロップレートが最大を示したときの時刻を表示します。
(12)	CoS ごとの送信パケットドロップが 1pps 以上を示した回数を表示します。

2.1.15 clear counters

clear counters	
目的	インターフェースのカウンターをクリアします。
シンタックス	**clear counters** {**all** ｜ **interface** *INTERFACE-ID* [,｜-] ｜ **cpu-port** ｜ **internal-port** ｜ **stack-port**}
パラメーター	**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** *INTERFACE-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**：物理ポートを指定します。複数指定できます。 • **mgmt** 〈0〉：マネージメントポートを指定します。 **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。 **internal-port**：ApresiaNP2000-48T4X、および ApresiaNP2000-48T4X-PoE の内部ポー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。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12

clear counters	
ガイドライン	-
制限事項	-
注意事項	stack-port パラメーターは、スタック構成の場合のみ有効です。
対象バージョン	1.01.01 1.03.01：cpu-port、internal-port、stack-port パラメーター追加

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

ポート設定関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
speed	speed {10 ｜ 100 ｜ 1000 [master ｜ slave] ｜ 10giga ｜ auto [SPEED-LIST] ｜ auto-downgrade} no speed [auto-downgrade]
duplex	duplex {full ｜ half ｜ auto} no duplex
mdix	mdix {auto ｜ normal ｜ cross} no mdix
flowcontrol	flowcontrol {on ｜ off} no flowcontrol
speed_duplex (mgmt 0)	speed_duplex {10_half ｜ 10_full ｜ 100_half ｜ 100_full ｜ auto} no speed_duplex
snmp-server enable traps sfp	snmp-server enable traps sfp no snmp-server enable traps sfp

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。
シンタックス	speed {10 ｜ 100 ｜ 1000 [master ｜ slave] ｜ 10giga ｜ auto [*SPEED-LIST*] ｜ auto-downgrade} no speed [auto-downgrade]

パラメーター	■ 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。

speed	
	■ 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(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）
コマンドモード	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	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(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 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**、またはアドバタイズする速度に 1000 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。
制限事項	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。
注意事項	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** 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。
対象バージョン	1.01.01

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

- ApresiaNP2000-24T4X / ApresiaNP2000-24T4X-PoE の Port 1/0/1～1/0/24
- ApresiaNP2000-48T4X / ApresiaNP2000-48T4X-PoE の Port 1/0/1～1/0/48

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
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

- ApresiaNP2000-24T4X / ApresiaNP2000-24T4X-PoE の Port 1/0/25～1/0/28
- ApresiaNP2000-48T4X / ApresiaNP2000-48T4X-PoE の Port 1/0/49～1/0/52

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）

使用方法	設定コマンド
	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。
シンタックス	duplex {full ｜ half ｜ auto} no duplex
パラメーター	■ 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
コマンドモード	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	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(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 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、またはアドバタイズする速度に 1000 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。

duplex	
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：ポート 1/0/10 を、1000Mbps/Full 固定に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/10
(config-if-port)# speed 1000
(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。
シンタックス	mdix {auto ｜ normal ｜ cross} no mdix
パラメーター	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）
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	flowcontrol {on ｜ off} no flowcontrol

flowcontrol	
パラメーター	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）
コマンドモード	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	装置のソフトウェアでフロー制御機能が設定されます。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	speed_duplex {10_half | 10_full | 100_half | 100_full | auto} no speed_duplex
パラメーター	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）
コマンドモード	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	-
制限事項	ApresiaNP2000 シリーズでは、マネージメントポートでは 1000BASE-T はサポートしていません。
注意事項	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。
対象バージョン	1.01.01

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 snmp-server enable traps sfp

snmp-server enable traps sfp	
目的	光トランシーバー関連の 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。
シンタックス	snmp-server enable traps sfp no snmp-server enable traps sfp
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.09.01

使用例：光トランシーバー関連の 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 sfp
(config)#
```

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 関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
alarm global enable	alarm [buzzer ｜ warn-led] global enable no alarm [buzzer ｜ warn-led] global enable
alarm duration	alarm [buzzer ｜ warn-led] duration {SECONDS ｜ infinite} no alarm [buzzer ｜ warn-led] duration
alarm state enable	alarm [buzzer ｜ warn-led] state enable [cause {loop-detection ｜ storm-control ｜ all}] no alarm [buzzer ｜ warn-led] state enable
alarm buzzer beep-type	alarm buzzer beep-type {default ｜ TYPE-ID} no alarm buzzer beep-type
show alarm	show alarm [buzzer ｜ warn-led] [interface INTERFACE-ID [,｜-]]
debug alarm test	debug alarm [buzzer ｜ warn-led [interface INTERFACE-ID [,｜-]]] 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。
シンタックス	alarm [buzzer ｜ warn-led] global enable no alarm [buzzer ｜ warn-led] global enable
パラメーター	buzzer（省略可能）：ブザーのグローバル設定を有効または無効にする場合に指定します。 warn-led（省略可能）：アラーム LED のグローバル設定を有効または無効にする場合に指定します。
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	alarm buzzer global enable は 1.01.01、それ以外は 1.03.01

使用例：ブザーおよびアラーム LED 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」ステータスに変化したとき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

alarm duration	
	コマンドを使用します。
シンタックス	alarm [buzzer ｜ warn-led] duration {*SECONDS* ｜ infinite} no alarm [buzzer ｜ warn-led] duration
パラメーター	buzzer（省略可能）：ブザーの動作時間を設定する場合に指定します。 warn-led（省略可能）：アラーム LED の動作時間を設定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。 infinite：ループまたはストームが解決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
コマンドモード	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	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 を有効にしたインターフェースのループ検知またはストームコントロールの結果が、正常から他のステータスに変化するときに、ブザーおよびアラーム LED が動作します。ループ検知の状態は show loop-detection コマンドで確認できます。ストームコントロールの状態は show storm-control コマンドで確認できます。
制限事項	-
注意事項	-
対象バージョン	alarm buzzer duration {SECONDS ｜ infinite}は 1.01.01、それ以外は 1.03.01

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。
シンタックス	alarm [buzzer ｜ warn-led] state enable [cause {loop-detection ｜ storm-control ｜ all}] no alarm [buzzer ｜ warn-led] state enable
パラメーター	buzzer（省略可能）：インターフェースのブザーの設定を有効または無効にする場合に指定します。 warn-led（省略可能）：インターフェースのアラーム LED の設定を有効または無効に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

alarm state enable	
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	alarm buzzer state enable は 1.01.01、それ以外は 1.03.01

使用例：ポート 1/0/1 でループ検知による警告が発生したときに、ブザーで通知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)# alarm buzzer state enable
(config-if-port)#
```

2.3.4 alarm buzzer beep-type

alarm buzzer beep-type	
目的	ブザーの種類を指定します。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。
シンタックス	alarm buzzer beep-type {default ｜ *TYPE-ID*} no alarm buzzer beep-type
パラメーター	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 秒動作し、8 秒停止することを繰り返します。 • 2：5 秒動作し、5 秒停止することを繰り返します。 • 3：8 秒動作し、2 秒停止することを繰り返します。
デフォルト	default（2 秒動作し、2 秒停止することを繰り返す）
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

使用例：ブザーの種類を 1（2 秒動作し、8 秒停止する）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。
シンタックス	show alarm [buzzer ｜ warn-led] [interface *INTERFACE-ID* [,｜-]]
パラメーター	buzzer（省略可能）：ブザーの設定を表示する場合に指定します。

show alarm	
	warn-led（省略可能）：アラーム LED の設定を表示する場合に指定します。 **interface** *INTERFACE-ID*（省略可能）：ブザーおよびアラーム LED の設定と状態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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	–
対象バージョン	**show alarm buzzer** [**interface** *INTERFACE-ID* [,|-]]は 1.01.01、それ以外は 1.03.01

使用例：ブザーおよびアラーム LED の設定と状態を表示する方法を示します。

```
# show alarm

 Alarm Buzzer:
 ----------------------------------------------------------------------
 Global State      : Enabled ...(1)
 Duration          : 30 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    Loop Detection
 Port1/0/3         Enabled    All
 Port1/0/4         Disabled   -
～～省略～～
 Port1/0/26        Disabled   -
 Port1/0/27        Disabled   -
 Port1/0/28        Disabled   -

 Alarm Warning LEDs:
 ----------------------------------------------------------------------
 Global State      : Enabled ...(8)
 Duration          : Infinite ...(9)
 (5)               (10)       (11)              (12)       (13)
 Interface         State      Cause Enabled     Current    Warning
                                                Status     Time Left
 ---------------   --------   --------------    --------   ------------
 Port1/0/1         Enabled    Storm Control     Warning    Infinite
 Port1/0/2         Enabled    All               Warning    Infinite
 Port1/0/3         Enabled    Loop Detection    Ready      0  second(s)
 Port1/0/4         Disabled   -                 Inactive   0  second(s)
～～省略～～
 Port1/0/26        Disabled   -                 Inactive   0  second(s)
 Port1/0/27        Disabled   -                 Inactive   0  second(s)
 Port1/0/28        Disabled   -                 Inactive   0  second(s)
```

```
Alarm Events:
(14)                (15)
Interface           Reason
-----------------------------------------------------------------
Port 1/0/1          Storm(BC)
Port 1/0/2          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。
(3)	ブザーが停止するまでの残り時間を表示します。
(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。
(7)	ブザーで通知するように設定した機能を表示します。 All：ループ検知またはストームコントロールによる警告 Loop Detection：ループ検知による警告 Storm Control：ストームコントロールによる警告
(8)	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。
(9)	アラーム LED の動作時間を表示します。
(10)	アラーム LED の有効(Enabled)／無効(Disabled)を表示します。
(11)	アラーム LED で通知するように設定した機能を表示します。 All：ループ検知またはストームコントロールによる警告 Loop Detection：ループ検知による警告 Storm Control：ストームコントロールによる警告
(12)	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
(13)	アラーム LED が停止するまでの残り時間を表示します。
(14)	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。
(15)	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

使用例：ポート 1/0/1 からポート 1/0/5 のブザーの設定と状態を表示する方法を示します。

```
# show alarm buzzer interface port 1/0/1-5
```

```
Alarm Buzzer:
-------------------------------------------------------------------
Global State      : Enabled ...(1)
Duration          : 30 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   -
Port1/0/5         Disabled   -

Alarm Events:
(8)               (9)
Interface         Reason
-------------------------------------------------------------------
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。
(3)	ブザーが停止するまでの残り時間を表示します。
(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。
(7)	ブザーで通知するように設定した機能を表示します。 All：ループ検知またはストームコントロールによる警告 Loop Detection：ループ検知による警告 Storm Control：ストームコントロールによる警告
(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

使用例：ポート 1/0/1 のアラーム LED の設定と状態を表示する方法を示します。

```
# show alarm warn-led interface port 1/0/1
```

```
Alarm Warning LEDs:
-------------------------------------------------------------------
Global State      : Enabled ...(1)
Duration          : Infinite ...(2)
(3)               (4)       (5)              (6)        (7)
Interface         State     Cause Enabled    Current    Warning
                                             Status     Time Left
---------------   --------  --------------   --------   ------------
Port1/0/1         Enabled   Storm Control    Warning    Infinite

Alarm Events:
(8)               (9)
Interface         Reason
-------------------------------------------------------------------
Port 1/0/1        Storm(DLF)
```

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。
(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)	アラーム LED の有効(Enabled)／無効(Disabled)を表示します。
(5)	アラーム LED で通知するように設定した機能を表示します。 All：ループ検知またはストームコントロールによる警告 Loop Detection：ループ検知による警告 Storm Control：ストームコントロールによる警告
(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。
(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

使用例：ポートチャネル 2 のブザーの設定と状態を表示する方法を示します。

```
# show alarm buzzer interface port-channel 2

Alarm Buzzer:
-------------------------------------------------------------------
Global State      : Enabled ...(1)
Duration          : 30 second(s) ...(2)
Warning Time Left: 0  second(s) ...(3)
Current Status    : Ready ...(4)
(5)               (6)       (7)
```

```
Interface        State     Cause Enabled
---------------  --------  --------------
Port-channel2    Enabled   All

Alarm Events:
(8)              (9)
Interface        Reason
---------------  ------------------------------------------------
```

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。
(3)	ブザーが停止するまでの残り時間を表示します。
(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。
(7)	ブザーで通知するように設定した機能を表示します。 All：ループ検知またはストームコントロールによる警告 Loop Detection：ループ検知による警告 Storm Control：ストームコントロールによる警告
(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

2.3.6 debug alarm test

debug alarm test	
目的	テストする目的で、ブザーおよびアラーム LED を手動でオン／オフします。
シンタックス	**debug alarm** [**buzzer** | **warn-led** [**interface** *INTERFACE-ID* [,|-]]] **test**
パラメーター	**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** *INTERFACE-ID*（省略可能）：アラーム LED をテスト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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	ブザーおよびアラーム LED がオフ

debug alarm test	
コマンドモード	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。 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。
制限事項	–
注意事項	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。
対象バージョン	**debug alarm buzzer test** は 1.01.01，それ以外は 1.03.01

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)関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
eee	eee no eee
show eee	show eee [interface INTERFACE-ID [,|-]]

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。
シンタックス	eee no eee
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	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。
注意事項	-
対象バージョン	1.04.01

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)の設定情報を表示します。
シンタックス	show eee [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID* (省略可能)：省電力イーサネット(EEE)の設定情報を表示する物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-

show eee	
対象バージョン	1.04.01

使用例：省電力イーサネット(EEE)の有効または無効を表示する方法を示します。

```
# show eee
(1)             (2)
Port            State
---------       -----------
1/0/1            Enabled
1/0/2            Enabled
1/0/3            Enabled
1/0/4            Enabled
～～省略～～
1/0/20           Enabled
1/0/21           Enabled
1/0/22           Enabled
1/0/23           Enabled
1/0/24           Enabled
1/0/25           -
1/0/26           -
```

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／無効を表示します。 Enabled：有効 Disabled：無効 -：省電力イーサネット未対応ポート

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。

コマンド	コマンドとパラメーター
poe power-inline	poe power-inline auto [max MAX-WATTAGE] [time-range TR-NAME] no poe power-inline [auto {max ｜ time-range}]
poe power-inline never	poe power-inline never no poe power-inline never
poe pd description	poe pd description TEXT no poe pd description
poe pd priority	poe pd priority {critical ｜ high ｜ low} no poe pd priority
poe usage-threshold	poe [unit UNIT-ID] usage-threshold PERCENTAGE no poe [unit UNIT-ID] usage-threshold
snmp-server enable traps poe	snmp-server enable traps poe no snmp-server enable traps poe
c-poe enable	c-poe enable no c-poe enable

PoE 関連の show／操作コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show poe power module	show poe power module [unit UNIT-ID] [detail]
show poe power-inline	show poe power-inline [INTERFACE-ID [,｜-]] {status ｜ configuration ｜ statistics ｜ lldp-classification}
clear poe statistic	clear poe statistic {all ｜ interface INTERFACE-ID [,｜-]}

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。
シンタックス	**poe power-inline auto [max** *MAX-WATTAGE*] [**time-range** *TR-NAME*] **no poe power-inline [auto {max ｜ time-range}]**
パラメーター	**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** *TR-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**）
コマンドモード	インターフェース設定モード(port, range)
特権レベル	レベル：12

poe power-inline	
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。
制限事項	本コマンドは、PoE 対応ポートでのみ使用できます。
注意事項	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。 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。
対象バージョン	1.05.01 1.07.01：never パラメーター削除 1.09.01：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。
シンタックス	poe power-inline never no poe power-inline never

poe power-inline never	
パラメーター	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）
コマンドモード	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	-
制限事項	本コマンドは、PoE 対応ポートでのみ使用できます。
注意事項	AEOS-NP2000 Ver. 1.06.02 以前では no poe power-inline never コマンドは未実装のため、以下の方法で有効にしてください。 • Ver. 1.06.02 以前では、最大電力を未指定で有効にする場合は poe power-inline auto コマンドを使用してください。 • Ver. 1.06.02 以前では、最大電力を指定して有効にする場合は poe power-inline auto max *MAX-WATTAGE* コマンドを使用してください。
対象バージョン	1.07.01

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：AEOS-NP2000 Ver. 1.07.01 以降で、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)#
```

使用例：AEOS-NP2000 Ver. 1.06.02 以前で、ポート 1/0/1 の PoE 給電を最大電力を未指定で有効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)#
```

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。
シンタックス	poe pd description *TEXT* no poe pd description
パラメーター	*TEXT*：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
コマンドモード	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	-
制限事項	本コマンドは、PoE 対応ポートでのみ使用できます。

poe pd description	
注意事項	-
対象バージョン	1.05.01

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。
シンタックス	**poe pd priority {critical ｜ high ｜ low}** **no poe pd priority**
パラメーター	**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
コマンドモード	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	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。
制限事項	本コマンドは、PoE 対応ポートでのみ使用できます。
注意事項	-
対象バージョン	1.05.01

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。
シンタックス	**poe [unit *UNIT-ID*] usage-threshold *PERCENTAGE*** **no poe [unit *UNIT-ID*] usage-threshold**

poe usage-threshold	
パラメーター	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%
コマンドモード	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	装置全体の電力使用率が設定されたしきい値を超えた場合に、pethMainPowerUsageOnNotification トラップが送信されます。また、装置全体の電力使用率が設定されたしきい値を下回った場合に、pethMainPowerUsageOffNotification トラップが送信されます。
制限事項	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。
注意事項	-
対象バージョン	1.05.01

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 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。
シンタックス	snmp-server enable traps poe no snmp-server enable traps poe
パラメーター	なし
デフォルト	有効（snmp-server enable traps poe）
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.05.01

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)#
```

2.5.7 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。
シンタックス	c-poe enable no c-poe enable
パラメーター	なし
デフォルト	無効
コマンドモード	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	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-NP2000 Ver. 1.09.01 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。
制限事項	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。
注意事項	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。
対象バージョン	1.05.01

使用例：ApresiaNP2000-24T4X-PoE において、ポート 1/0/1 からポート 1/0/24 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 1/0/1-24
(config-if-port-range)# c-poe enable
(config-if-port-range)#
```

2.5.8 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。
シンタックス	show poe power module [unit *UNIT-ID*] [detail]
パラメーター	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）：電源モジュールの詳細情報を表示する場合に指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.05.01

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)
Unit   Delivered(W)   Power Budget(W)   Usage-Threshold(%)     Trap State
----   ------------   ---------------   --------------------   ----------
1      0              370               5                      Enabled
2      140            370               99                     Enabled
3      115            370               80                     Enabled
```

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。

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)
Unit   Delivered(W)   Power Budget(W)   Usage-Threshold(%)     Trap State
----   ------------   ---------------   --------------------   ----------
1      1              370               99                     Enabled

PoE system parameters:
 (1)    (6)          (7)          (8)
Unit   Max Ports    Device ID    SW Version
----   ---------    ---------    ----------
1      24           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 を使用可能な最大ポート数を表示します。
(7)	PoE チップのハードウェアバージョンを表示します。
(8)	PoE チップのファームウェアバージョンを表示します。

2.5.9 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。
シンタックス	**show poe power-inline** [*INTERFACE-ID* [,|-]] {**status** | **configuration** | **statistics** | **lldp-classification**}
パラメーター	*INTERFACE-ID*（省略可能）：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 機能の設定情報を表示する場合に指定します。

show poe power-inline	
	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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.05.01 1.09.01：**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      30.0    0.0
Port1/0/2    searching   n/a      0.0     0.0
Port1/0/3    searching   n/a      0.0     0.0
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    searching   n/a      0.0     0.0
Port1/0/8    searching   n/a      0.0     0.0
Port1/0/9    searching   n/a      0.0     0.0
Port1/0/10   searching   n/a      0.0     0.0
Port1/0/11   searching   n/a      0.0     0.0
Port1/0/12   searching   n/a      0.0     0.0
Port1/0/13   searching   n/a      0.0     0.0
Port1/0/14   searching   n/a      0.0     0.0
Port1/0/15   searching   n/a      0.0     0.0
Port1/0/16   searching   n/a      0.0     0.0
Port1/0/17   disabled    n/a      0.0     0.0
Port1/0/18   searching   n/a      0.0     0.0
Port1/0/19   searching   n/a      0.0     0.0
Port1/0/20   searching   n/a      0.0     0.0
Port1/0/21   searching   n/a      0.0     0.0
Port1/0/22   searching   n/a      0.0     0.0
Port1/0/23   searching   n/a      0.0     0.0
Port1/0/24   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。

項番	説明
(2)	PoE 機能の状態を表示します。 disabled：PoE 機能が無効状態 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 機能の設定情報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        ip-phone
Port1/0/7    auto      low        ip-phone
Port1/0/8    auto      low        ip-phone
Port1/0/9    auto      low
Port1/0/10   auto      low
Port1/0/11   auto      low
Port1/0/12   auto      low
Port1/0/13   auto      low
Port1/0/14   auto      low
Port1/0/15   auto      low
Port1/0/16   auto      low
Port1/0/17   never     low
Port1/0/18   auto      low
Port1/0/19   auto      low
Port1/0/20   auto      low
Port1/0/21   auto      low
Port1/0/22   auto      low
Port1/0/23   auto      low
Port1/0/24   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

項番	説明
	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              88
Port1/0/2      0            0          0          0              33
Port1/0/3      0            0          0          0              30
Port1/0/4      0            0          0          0              35
Port1/0/5      0            0          0          0              46
Port1/0/6      0            0          0          0              35
Port1/0/7      0            0          0          0              149
Port1/0/8      0            0          0          0              36
Port1/0/9      0            0          0          0              24
Port1/0/10     0            0          0          0              141
Port1/0/11     0            0          0          0              143
Port1/0/12     0            0          0          0              141
Port1/0/13     0            0          0          0              48
Port1/0/14     0            0          0          0              142
Port1/0/15     0            0          0          0              175
Port1/0/16     0            0          0          0              88
Port1/0/17     0            0          0          0              114
Port1/0/18     0            0          0          0              15
Port1/0/19     0            0          0          0              120
Port1/0/20     0            0          0          0              16
Port1/0/21     0            0          0          0              71
Port1/0/22     0            0          0          0              99
Port1/0/23     0            0          0          0              111
Port1/0/24     0            0          0          0              156
```

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
(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。

2.5.10 clear poe statistic

clear poe statistic	
目的	PoE 機能の統計情報を消去します。
シンタックス	**clear poe statistic** {**all** | **interface** *INTERFACE-ID* [,|-]}
パラメーター	**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** *INTERFACE-ID*：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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	–
制限事項	–
注意事項	–
対象バージョン	1.05.01

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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
pd-monitoring global state enable	pd-monitoring global state enable no pd-monitoring global state enable
pd-monitoring period-to-start	pd-monitoring period-to-start MINUTES no pd-monitoring period-to-start
pd-monitoring restart-poe retry	pd-monitoring restart-poe retry TIMES no pd-monitoring restart-poe retry
pd-monitoring auto-recovery time	pd-monitoring auto-recovery time MINUTES no pd-monitoring auto-recovery time
pd-monitoring acl-mode	pd-monitoring acl-mode interval SECONDS threshold pps PACKET-PER-SECOND no pd-monitoring acl-mode [interval ｜ threshold]
pd-monitoring acl-mode access-list	pd-monitoring acl-mode access-list ACCESS-LIST-NAME action {restart-poe ｜ notify-only} no pd-monitoring acl-mode access-list
pd-monitoring icmp	pd-monitoring icmp interval SECONDS timeout MILLISECONDS count TIMES no pd-monitoring icmp [interval ｜ timeout ｜ count]
pd-monitoring icmp pd-ip	pd-monitoring icmp pd-ip IP-ADDRESS action {restart-poe ｜ notify-only} no pd-monitoring icmp pd-ip
pd-monitoring state	pd-monitoring {icmp ｜ acl-mode} state enable no pd-monitoring state enable
show pd-monitoring	show pd-monitoring [INTERFACE-ID [,｜-]]

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。
シンタックス	pd-monitoring global state enable no pd-monitoring global state enable
パラメーター	なし
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.05.01

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。
シンタックス	**pd-monitoring period-to-start** *MINUTES* **no pd-monitoring period-to-start**
パラメーター	*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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.05.01

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。
シンタックス	**pd-monitoring restart-poe retry** *TIMES* **no pd-monitoring restart-poe retry**
パラメーター	*TIMES*：PD モニタリングによるリスタートの上限回数を、1～3 回の範囲で指定します。
デフォルト	3 回
コマンドモード	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	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。

pd-monitoring restart-poe retry	
	AEOS-NP2000 Ver. 1.07.01 以降では、**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。
制限事項	-
注意事項	AEOS-NP2000 Ver. 1.06.02 以前では **no poe power-inline never** コマンドは未実装のため、以下の方法で有効にしてください。 • Ver. 1.06.02 以前では、最大電力を未指定で有効にする場合は **poe power-inline auto** コマンドを使用してください。 • Ver. 1.06.02 以前では、最大電力を指定して有効にする場合は **poe power-inline auto max** *MAX-WATTAGE* コマンドを使用してください。
対象バージョン	1.05.01

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。
シンタックス	**pd-monitoring auto-recovery time** *MINUTES* **no pd-monitoring auto-recovery time**
パラメーター	*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	自動復旧時間：0 分（自動復旧しない）
コマンドモード	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	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 0 の場合、PoE 機能は自動復旧しません。
制限事項	本コマンドは、PoE 対応ポートでのみ使用できます。
注意事項	-
対象バージョン	1.05.01

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。
シンタックス	**pd-monitoring acl-mode interval** *SECONDS* **threshold pps** *PACKET-PER-SECOND* **no pd-monitoring acl-mode** [**interval** ｜ **threshold**]
パラメーター	**interval** *SECONDS*：トラフィックレートの監視間隔を、5～30 秒の範囲で指定します。 **threshold pps** *PACKET-PER-SECOND*：トラフィックレートの下限しきい値を、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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.05.01

使用例：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。
シンタックス	**pd-monitoring acl-mode access-list** *ACCESS-LIST-NAME* **action** {**restart-poe** ｜ **notify-only**} **no pd-monitoring acl-mode access-list**
パラメーター	*ACCESS-LIST-NAME*：監視するアクセスリスト名を指定します。 **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
コマンドモード	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	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。
制限事項	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。

pd-monitoring acl-mode access-list	
	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
注意事項	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。
対象バージョン	1.05.01

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。
シンタックス	**pd-monitoring icmp interval** *SECONDS* **timeout** *MILLISECONDS* **count** *TIMES* **no pd-monitoring icmp** [**interval** ｜ **timeout** ｜ **count**]
パラメーター	**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** *TIMES*：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
コマンドモード	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	–
制限事項	–
注意事項	–
対象バージョン	1.05.01

使用例：ICMP による 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。
シンタックス	**pd-monitoring icmp pd-ip** *IP-ADDRESS* **action {restart-poe ｜ notify-only}** **no pd-monitoring icmp pd-ip**
パラメーター	*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
コマンドモード	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	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。
制限事項	本コマンドは、PoE 対応ポートでのみ使用できます。
注意事項	-
対象バージョン	1.05.01

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。
シンタックス	**pd-monitoring {icmp ｜ acl-mode} state enable** **no pd-monitoring state enable**
パラメーター	**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
コマンドモード	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	-
制限事項	本コマンドは、PoE 対応ポートでのみ使用できます。
注意事項	-
対象バージョン	1.05.01

使用例：ポート 1/0/1 からポート 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。
シンタックス	**show pd-monitoring** [*INTERFACE-ID* [,|-]]
パラメーター	*INTERFACE-ID*（省略可能）：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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.05.01

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 ポートの給電状態を表示します。 PoE Power supply in progress：給電中 PoE Power supply disable：給電停止中
(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 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。

コマンド	コマンドとパラメーター
stack bandwidth	stack bandwidth 10G {2-port ｜ 4-port} [chain] no stack
stack renumber	stack CURRENT-UNIT-ID renumber NEW-UNIT-ID no stack CURRENT-UNIT-ID renumber
stack priority	stack CURRENT-UNIT-ID priority NEW-PRIORITY-NUMBER no stack CURRENT-UNIT-ID priority
stack my_box_id	stack my_box_id NEW-UNIT-ID no stack my_box_id
stack my_box_priority	stack my_box_priority NEW-PRIORITY-NUMBER no stack my_box_priority
stack preempt	stack preempt no stack preempt
stack stack-port load-balance	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
stack port-channel mode partial	stack port-channel mode partial no stack port-channel mode partial
snmp-server enable traps stack	snmp-server enable traps stack no 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。

コマンド	コマンドとパラメーター
show stack	show stack
stack remove	stack remove UNIT-ID

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。
シンタックス	stack bandwidth 10G {2-port ｜ 4-port} [chain] no stack
パラメーター	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。ApresiaNP2000-48T4X または ApresiaNP2000-48T4X-PoE では、スタックポートの帯域幅を 10G 4-port で設定する場合は、chain オプションは併用できません。

<table>
<tr><th colspan="2">stack bandwidth</th></tr>
<tr><td>デフォルト</td><td>無効</td></tr>
<tr><td>コマンドモード</td><td>特権実行モード</td></tr>
<tr><td>特権レベル</td><td>レベル：12</td></tr>
<tr><td>ガイドライン</td><td>
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。
<table>
<tr><th>装置</th><th>帯域幅の設定</th><th>スタックポート 1</th><th>スタックポート 2</th></tr>
<tr><td rowspan="4">ApresiaNP 2000-24T4X (-PoE)</td><td>10G 2-port</td><td>1/0/27</td><td>1/0/28</td></tr>
<tr><td>10G 4-port</td><td>1/0/25, 1/0/26</td><td>1/0/27, 1/0/28</td></tr>
<tr><td>10G 2-port chain</td><td>1/0/27, 1/0/28</td><td>-</td></tr>
<tr><td>10G 4-port chain</td><td>1/0/25, 1/0/26, 1/0/27, 1/0/28</td><td>-</td></tr>
<tr><td rowspan="4">ApresiaNP 2000-48T4X (-PoE)</td><td>10G 2-port</td><td>1/0/51</td><td>1/0/52</td></tr>
<tr><td>10G 4-port</td><td>1/0/49, 1/0/50</td><td>1/0/51, 1/0/52</td></tr>
<tr><td>10G 2-port chain</td><td>1/0/51, 1/0/52</td><td>-</td></tr>
<tr><td>10G 4-port chain</td><td>1/0/49, 1/0/50, 1/0/51, 1/0/52</td><td>-</td></tr>
</table>
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。

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。

ファームウェアのバージョンが AEOS-NP2000 Ver. 1.09 の場合のみ、ApresiaNP2100 シリーズと ApresiaNP2000 シリーズが混在するスタックを構成できます。
</td></tr>
<tr><td>制限事項</td><td>
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
</td></tr>
</table>

stack bandwidth	
	• [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。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。
注意事項	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。 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。
対象バージョン	1.01.01 1.06.01：chain パラメーター追加

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。
シンタックス	stack *CURRENT-UNIT-ID* renumber *NEW-UNIT-ID* no stack *CURRENT-UNIT-ID* renumber
パラメーター	*CURRENT-UNIT-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-UNIT-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
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	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。

stack renumber	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	stack *CURRENT-UNIT-ID* priority *NEW-PRIORITY-NUMBER* no stack *CURRENT-UNIT-ID* priority
パラメーター	*CURRENT-UNIT-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。 *NEW-PRIORITY-NUMBER*：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）
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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

stack my_box_id	
	式のコマンドを使用します。
シンタックス	stack my_box_id *NEW-UNIT-ID* no stack my_box_id
パラメーター	*NEW-UNIT-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
コマンドモード	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-UNIT-ID* に自装置の今のボックス ID を指定して、stack *CURRENT-UNIT-ID* renumber *NEW-UNIT-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。
制限事項	-
注意事項	-
対象バージョン	1.03.01

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。
シンタックス	stack my_box_priority *NEW-PRIORITY-NUMBER* no stack my_box_priority
パラメーター	*NEW-PRIORITY-NUMBER*：優先度の値を 1～63 の範囲で指定します。
デフォルト	32
コマンドモード	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-UNIT-ID* に自装置の今のボックス ID を指定して、stack *CURRENT-UNIT-ID* priority *NEW-PRIORITY-NUMBER* 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。 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

stack my_box_priority	
	ください。
制限事項	-
注意事項	-
対象バージョン	1.03.01

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。
シンタックス	stack preempt no stack preempt
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	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
パラメーター	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 アドレスによる負荷分散 • dst-mac：宛先 MAC アドレスによる負荷分散 • src-mac：送信元 MAC アドレスによる負荷分散 • src-dst-ip：送信元 IP アドレスと宛先 IP アドレスによる負荷分散 • dst-ip：宛先 IP アドレスによる負荷分散 • src-ip：送信元 IP アドレスによる負荷分散
デフォルト	設定なし（no stack stack-port load-balance）
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	本コマンドがデフォルト設定の場合は、受信ポート番号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。
制限事項	-
注意事項	-
対象バージョン	1.06.01

■ 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	受信ポート番号
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
	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。
シンタックス	stack port-channel mode partial no stack port-channel mode partial
パラメーター	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）
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.06.01

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 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。
シンタックス	snmp-server enable traps stack no snmp-server enable traps stack
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-

snmp-server enable traps stack	
注意事項	-
対象バージョン	1.03.01

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)#
```

2.7.10 show stack

show stack	
目的	スタック情報を表示します。
シンタックス	**show stack**
パラメーター	なし
デフォルト	なし
コマンドモード	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、AEOS-NP2000 Ver. 1.07.01 以降では **show version** コマンドを使用してください。AEOS-NP2000 Ver. 1.06.02 以前では **show mac-address-table** コマンドを使用してください。
制限事項	-
注意事項	Unit Status 項目は AEOS-NP2000 Ver. 1.09.01 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。
対象バージョン	1.01.01 1.09.01：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)

Topology             : Duplex_Ring ...(6)
My Box ID            : 1 ...(7)
Master ID            : 1 ...(8)
BK Master ID         : 2 ...(9)
Box Count            : 2 ...(10)
 (11) (12)  (13)                      (14)   (15)   (16)                (17)       (18)       (19)
Box User Module                             Prio-                      Prom       Runtime    H/W
ID  Set  Name                        Exist  rity   MAC                Version    Version    Version
--- ---- ------------------------- ----- ----- ------------------ --------- --------- -------
1   User ApresiaNP2000-48T4X       Exist 0     00-40-66-B4-96-B5 1.00.00    1.09.01    A
2   User ApresiaNP2000-48T4X       Exist 20    00-40-66-B4-97-1F 1.00.00    1.09.01    A
3   -    NOT_EXIST                 No
4   -    NOT_EXIST                 No

 Stack Bandwidth and Unit Status:
 (11)    (20)         (21)           (22)           (23)
 Box     User Set     SIO1 Active    SIO2 Active    Unit
```

```
ID     Bandwidth   Bandwidth     Bandwidth     Status
----   ---------   ---------     ---------     ---------
1      2-port(10G) 1-port        1-port        Normal
2      2-port(10G) 1-port        1-port        Normal
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
(7)	装置のボックス ID を表示します。
(8)	マスターのボックス ID を表示します。
(9)	バックアップマスターのボックス ID を表示します。
(10)	スタックを構成している装置の数を表示します。
(11)	ボックス ID を表示します。
(12)	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
(13)	装置の名称を表示します。
(14)	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。
(15)	優先度を表示します。
(16)	スタックメンバーの MAC アドレスを表示します。
(17)	ブートローダーバージョンを表示します。
(18)	ファームウェアバージョンを表示します。
(19)	ハードウェアリビジョンを表示します。
(20)	スタックポート構成を表示します。 4-port(10G)：stack bacnwidth 10G 4-port 設定時 2-port(10G)：stack bacnwidth 10G 2-port 設定時
(21)	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
(22)	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

項番	説明
(23)	装置の状態を表示します。 Normal：正常状態 *Abnormal：異常状態

2.7.11 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。
シンタックス	**stack remove** *UNIT-ID*
パラメーター	*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。
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.06.01

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。

コマンド	コマンドとパラメーター
help	help
enable	enable [PRIVILEGE-LEVEL]
disable	disable [PRIVILEGE-LEVEL]
login (EXEC)	login
logout	logout
configure terminal	configure terminal
exit	exit
end	end
fan	fan {auto ｜ forceon}

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。

コマンド	コマンドとパラメーター
show version	show version
show environment	show environment [fan ｜ memory ｜ power ｜ temperature ｜ health]
show unit	show unit [UNIT-ID]
show cpu utilization	show cpu utilization [unit [UNIT-ID]]
clear cpu utilization history	clear cpu utilization history
show 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。
シンタックス	help
パラメーター	なし
デフォルト	なし
コマンドモード	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

help	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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」という文字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。

```
# conf 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。特権実行モードではプロンプトが # で表示されます。
シンタックス	**enable** [*PRIVILEGE-LEVEL*]

enable	
パラメーター	*PRIVILEGE-LEVEL*（省略可能）：ユーザーの特権レベルを 1～15 の範囲で指定します。指定しない場合、レベル 15 が指定されます。
デフォルト	なし
コマンドモード	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	特権レベルでパスワードが要求された場合、表示されたフィールドにパスワードを入力します。パスワードの入力に 3 回失敗すると、ユーザーは現在のレベルに戻されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：特権実行モードに遷移する方法を示します。

```
> enable

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

3.1.3 disable

disable	
目的	特権レベルより低いユーザーレベルに遷移します。
シンタックス	**disable** [*PRIVILEGE-LEVEL*]
パラメーター	*PRIVILEGE-LEVEL*（省略可能）：遷移する特権レベルを指定します。指定しない場合、レベル 1 が指定されます。
デフォルト	なし
コマンドモード	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	パスワードが設定されている特権レベルに disable で遷移する場合、パスワードは不要です。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：レベル 12 に遷移する方法を示します。

```
# disable 12
#
```

3.1.4 login (EXEC)

login (EXEC)	
目的	CLI でログイン処理を実施します。
シンタックス	**login**
パラメーター	なし
デフォルト	なし
コマンドモード	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

login (EXEC)	
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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	logout
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。遷移後のプロンプトは (config)# に変更されます。
シンタックス	configure terminal
パラメーター	なし
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	exit
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	end
パラメーター	なし
デフォルト	なし
コマンドモード	任意の設定モード
特権レベル	レベル：1
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 fan

fan	
目的	ApresiaNP2000-24T4X のファン回転スピードの制御において、停止する制御の有効／無効を設定します。
シンタックス	fan {auto | forceon}
パラメーター	auto：ファン回転スピードの制御で「停止する制御」を有効にする場合に指定し

fan	
	ます。 forceon：ファン回転スピードの制御で「停止する制御」を無効にする場合に指定します。
デフォルト	auto（ファン回転スピードを停止する制御は有効）
コマンドモード	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	本コマンドは ApresiaNP2000-24T4X でのみ動作します。 ApresiaNP2000-24T4X（AEOS-NP2000 Ver. 1.08.02 以降）では、ファンは停止／低速／高速の 3 段階で制御されます。本コマンドを forceon パラメーターを指定して設定すると「停止する制御」が無効になり、低速／高速の 2 段階で制御されます。
制限事項	-
注意事項	-
対象バージョン	1.08.02

使用例：ファン回転スピードの制御において、停止する制御を無効にする方法を示します。

```
# configure terminal
(config)# fan forceon

Set to Disable fan stop mode...

Success!
```

3.1.10 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。
シンタックス	show version
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
対象バージョン	1.01.01 1.07.01：System MAC Address 項目の仕様変更

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: 00-40-66-AF-F0-48 ...(1)
 (2)          (3)                              (4)
Unit ID    Module Name                        Versions
-------  ----------------------------  ----------------------
   1      ApresiaNP2000-24T4X            H/W:A
                                         Bootloader:1.00.00
                                         Runtime:1.03.01
                                         CPLD:FC
```

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、AEOS-NP2000 Ver. 1.07.01 以降では「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。AEOS-NP2000 Ver. 1.06.02 以前では「コマンド実行時点のマスター装置（自装置）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。

3.1.11 show environment

show environment	
目的	ファン、メモリー、温度、電源の可用性、および状態の情報を表示します。
シンタックス	show environment [fan ｜ memory ｜ power ｜ temperature ｜ health]
パラメーター	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。
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	–
対象バージョン	1.01.01 1.03.01：health パラメーター追加

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       28C

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

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。 ApresiaNP2000-24T4X（AEOS-NP2000 Ver. 1.08.02 以降）では、ファン停止中の初めの 1 時間は"-"と表示されます。
(4)	ファンの状態を表示します。 OK：すべてのファンが動作中 Fault：一部のファンが動作していません
(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／無効を表示します。
(8)	メモリーエラー自動復旧機能に関連付けられる通知の有効／無効を表示します。
(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／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

項番	説明
	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。

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       32C
2        Abnormal     60C

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

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        Abnormal     8                   1

Health Status:
(1)      (13)         (14)
Unit     Status       Failure Code
-----    ---------    --------------------
1        Normal       0x00000
2        Abnormal     0x00400
```

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。 ApresiaNP2000-24T4X（AEOS-NP2000 Ver. 1.08.02 以降）では、ファン停止中の初めの 1 時間は"-"と表示されます。
(4)	ファンの状態を表示します。 OK：すべてのファンが動作中 Fault：一部のファンが動作していません
(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／無効を表示します。
(8)	メモリーエラー自動復旧機能に関連付けられる通知の有効／無効を表示します。
(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／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。

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／無効を表示します。
(2)	メモリーエラー自動復旧機能に関連付けられる通知の有効／無効を表示します。
(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／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。

3.1.12 show unit

show unit	
目的	システムユニットの情報を表示します。
シンタックス	**show unit** [*UNIT-ID*]
パラメーター	*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。
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	–
対象バージョン	1.01.01

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     ApresiaNP2000-24T4X
 2     ApresiaNP2000-24T4X
(1)          (3)                            (4)          (5)
Unit         Serial-Number                  Status       Up Time
----  ---------------------------------  ---------  -----------------
 1     202410000029                        ok         0DT15H51M42S
 2     202410000040                        ok         0DT15H51M37S
(1)    (6)         (7)         (8)         (9)
Unit   Memory      Total       Used        Free
----  --------  ----------  ----------  ----------
 1     DRAM      262144 K    83632 K     178512 K
 1     FLASH      29937 K    21193 K       8744 K
 2     DRAM      262144 K    83499 K     178645 K
 2     FLASH      29937 K    19470 K      10467 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。

3.1.13 show cpu utilization

show cpu utilization	
目的	CPU 使用率を表示します。
シンタックス	**show cpu utilization** [**unit** [*UNIT-ID*]]
パラメーター	**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）：スタック構成で、ユニットを指定して CPU 使用率を表示する場合にボックス ID を指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	Maximum 項目と Minimum 項目は AEOS-NP2000 Ver. 1.08.01 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。
対象バージョン	1.01.01 1.08.01：**unit** パラメーター追加

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 -  30 %         One minute -  25 %           Five minutes -  24 %
Maximum - 31 %               Minimum - 8 %
(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:     27%      23%      23%     33%    10%
Unit 2:     28%      23%      23%     33%     9%
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:     28%      23%      23%     33%     9%
```

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。

項番	説明
(6)	CPU 使用率の最小値を表示します。

3.1.14 clear cpu utilization history

clear cpu utilization history	
目的	CPU 使用率をクリアします。
シンタックス	clear cpu utilization history
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.08.01

使用例：CPU 使用率をクリアする方法を示します。

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

3.1.15 show history

show history	
目的	現在の実行モード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。
シンタックス	show history
パラメーター	なし
デフォルト	なし
コマンドモード	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	入力したコマンドは、装置に記録されています。
制限事項	履歴バッファーのサイズは、コマンド 20 個で固定です。
注意事項	-
対象バージョン	1.01.01

使用例：コマンドバッファーの履歴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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
cd	cd [DIRECTORY-URL]
delete	delete FILE-URL
dir	dir [URL]
mkdir	mkdir DIRECTORY-NAME
more	more FILE-URL
rename	rename FILE-URL1 FILE-URL2
rmdir	rmdir DIRECTORY-NAME
show storage media-info	show storage media-info [unit UNIT-ID]

3.2.1 cd

cd	
目的	現在のディレクトリーを変更します。
シンタックス	cd [*DIRECTORY-URL*]
パラメーター	*DIRECTORY-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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 14:32:28  log
2   -rw       7208588 Dec 18 2020 14:12:39  AEOS-NP2000_R10802_sec.had
3   -rw       7208588 Dec 18 2020 12:54:38  AEOS-NP2000_R10802.had
4   -rw          1589 Dec 18 2020 14:16:08  primary.cfg
5   -rw          1589 Dec 18 2020 14:16:12  secondary.cfg
6   d--             0 Dec 18 2020 05:16:55  system

30656000 bytes total (15488512 bytes free)

# cd log
# dir
```

```
Directory of /c:/log
No files in directory
30656000 bytes total (15488512 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。
シンタックス	**delete** *FILE-URL*
パラメーター	*FILE-URL*：削除するファイルの URL を指定します。
デフォルト	なし
コマンドモード	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「**unit**X**:/**（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。
制限事項	**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。
注意事項	-
対象バージョン	1.01.01

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	指定したパス名のファイルの情報、またはファイルの一覧を表示します。
シンタックス	**dir** [*URL*]
パラメーター	*URL*（省略可能）：表示するファイルまたはディレクトリーの URL を指定します。
デフォルト	なし

dir	
コマンドモード	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	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のファイル情報を表示します。 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「**unit**X:/（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。 本装置のローカルフラッシュと外部ストレージの情報は、**show storage media-info** コマンドを使用して表示できます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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       7208588 Dec 18 2020 14:12:39  AEOS-NP2000_R10802_sec.had
2    -rw       7208588 Dec 18 2020 12:54:38  AEOS-NP2000_R10802.had
3    -rw          1589 Dec 18 2020 14:16:08  primary.cfg
4    -rw          1589 Dec 18 2020 14:16:12  secondary.cfg
5    d--             0 Dec 18 2020 05:16:55  system

30656000 bytes total (15489024 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       7208588 Dec 18 2020 14:12:39  AEOS-NP2000_R10802_sec.had
2   -rw       7208588 Dec 18 2020 12:54:38  AEOS-NP2000_R10802.had
3   -rw          1589 Dec 18 2020 14:16:08  primary.cfg
4   -rw          1589 Dec 18 2020 14:16:12  secondary.cfg
5   d--             0 Dec 18 2020 05:16:55  system

30656000 bytes total (15489024 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。
シンタックス	**mkdir** *DIRECTORY-NAME*
パラメーター	*DIRECTORY-NAME*：作成する新規ディレクトリー名を指定します。
デフォルト	なし
コマンドモード	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「**unit**X**:/**（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。
制限事項	–
注意事項	–
対象バージョン	1.01.01

使用例：現在のディレクトリーに「newdir」という名称のディレクトリー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「test_dir」という名称のディレクトリー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。
シンタックス	**more** *FILE-URL*
パラメーター	*FILE-URL*：表示するファイルの URL を指定します。
デフォルト	なし
コマンドモード	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「**unit**X**:/**（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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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


#-------------------------------------------------------------------------------
#                  ApresiaNP2000-48T4X Gigabit Ethernet Switch
#                                Configuration
#
#                            Firmware: Build 1.08.02
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------

# Date: Sat Sep 05 14:26:14 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

# AAA
```

```
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


#-------------------------------------------------------------------------------
#                  ApresiaNP2000-24T4X Gigabit Ethernet Switch
#                                Configuration
#
#                            Firmware: Build 1.08.02
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------

# Date: Sat Sep 05 14:26:20 2020


# STACK

##  stacking config information
##   #Box                                Prio-
##   #ID  Type                       Exist rity
##   #--- ------------------------- ----- -----
##   #  1 ApresiaNP2000-48T4X      exist 10
##   #  2 ApresiaNP2000-24T4X      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。
シンタックス	**rename** *FILE-URL1 FILE-URL2*
パラメーター	*FILE-URL1*：名前を変更するファイルの URL を指定します。 *FILE-URL2*：名前変更後のファイルの URL を指定します。
デフォルト	なし
コマンドモード	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「**unit**X**:/**（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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**rmdir** *DIRECTORY-NAME*
パラメーター	*DIRECTORY-NAME*：削除するディレクトリー名を指定します。
デフォルト	なし
コマンドモード	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「**unit**X**:/**（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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**show storage media-info** [**unit** *UNIT-ID*]
パラメーター	**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。
デフォルト	なし

show storage media-info	
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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        29 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)	ローカルフラッシュまたは外部ストレージの種類を表示します。 Flash：ローカルフラッシュ SD Card：外部ストレージ
(4)	ローカルフラッシュまたは外部ストレージの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。

コマンド	コマンドとパラメーター
terminal length default	terminal length default NUMBER no terminal length default
terminal width default	terminal width default NUMBER no terminal width default
terminal speed	terminal speed BPS no 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。

コマンド	コマンドとパラメーター
show terminal	show terminal
terminal length	terminal length NUMBER no terminal length
terminal width	terminal width NUMBER no terminal width

3.3.1 terminal length default

terminal length default	
目的	端末画面に表示され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。
シンタックス	terminal length default *NUMBER* no terminal length default
パラメーター	*NUMBER*：画面に表示する行数を 0～512 行の範囲で指定します。0 を指定した場合、末尾に達するまで表示は停止しません。0 以外の値を指定した場合、指定した行数ごとに停止します。50 を指定した場合、表示は 50 行ごとに停止します。
デフォルト	24 行
コマンドモード	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	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。 コマンドからの出力を 1 つの画面に表示しきれない場合、出力の後にプロンプトが表示されます。プロンプトで Ctrl+C キー、q キー、または Esc キーを押すと、出力を中断してプロンプトに戻ります。スペースキーを押すと出力の追加画面が表示されます。Enter キーを押すと次の 1 行を表示します。画面の長さを 0 に設定すると、スクロール機能がオフになり、出力全体が一度に表示されます。
制限事項	本コマンドは、構成情報では CLI コマンド（ラベル# CLI）で表示されます。
注意事項	コマンドからの出力の表示幅が、画面の表示幅の設定を超えた場合、自動的に次の行に表示されます。
対象バージョン	1.01.01

使用例：端末画面に表示される行数のデフォルト値を 60 行に変更する方法を示します。

```
(config)# terminal length default 60
(config)#
```

3.3.2 terminal width default

terminal width default	
目的	端末画面の 1 行の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。
シンタックス	**terminal width default** *NUMBER* **no terminal width default**
パラメーター	*NUMBER*：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
コマンドモード	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	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。
制限事項	本コマンドは、構成情報では CLI コマンド（ラベル# CLI）で表示されます。
注意事項	コマンドからの出力の表示幅が、画面の表示幅の設定を超えた場合、超えた部分の情報を表示するために、自動的に次の行に表示されます。
対象バージョン	1.01.01

使用例：端末画面の 1 行の文字数のデフォルト値を 120 文字に設定する方法を示します。

```
# configure terminal
(config)# terminal width default 120
(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。
シンタックス	**terminal speed** *BPS* **no terminal speed**
パラメーター	*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。
デフォルト	9600(bps)
コマンドモード	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	-
制限事項	本コマンドは、構成情報では BASIC 関連（ラベル# BASIC）で表示されます。
注意事項	-
対象バージョン	1.01.01

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	現在の端末の設定情報を取得します。
シンタックス	show terminal
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：現在の端末の設定情報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、端末画面に表示される行数を設定します。デフォルト設定に戻すには、no terminal length コマンドを使用します。
シンタックス	terminal length *NUMBER* no terminal length
パラメーター	*NUMBER*：画面に表示する行数を 0～512 行の範囲で指定します。0 を指定した場合、末尾に達するまで表示は停止しません。0 以外の値を指定した場合、指定した行数ごとに停止します。50 を指定した場合、表示は 50 行ごとに停止します。
デフォルト	24 行
コマンドモード	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。 コマンドからの出力を 1 つの画面に表示しきれない場合、出力の後にプロンプトが表示されます。プロンプトで Ctrl+C キー、q キー、または Esc キーを押すと、出力を中断してプロンプトに戻ります。スペースキーを押すと出力の追加画面が表示されます。Enter キーを押すと次の 1 行を表示します。

terminal length	
制限事項	–
注意事項	コマンドからの出力の表示幅が、画面の表示幅の設定を超えた場合、自動的に次の行に表示されます。
対象バージョン	1.01.01

使用例：現在のセッションの端末画面に表示される行数を 60 行に設定する方法を示します。

```
# terminal length 60
#
```

3.3.6 terminal width

terminal width	
目的	現在のセッションで、端末画面の 1 行の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。
シンタックス	**terminal width** *NUMBER* **no terminal width**
パラメーター	*NUMBER*：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
コマンドモード	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。
制限事項	–
注意事項	コマンドからの出力の表示幅が、画面の表示幅の設定を超えた場合、超えた部分の情報を表示するために、自動的に次の行に表示されます。
対象バージョン	1.01.01

使用例：現在のセッションの端末画面の 1 行の文字数を 120 文字に設定する方法を示します。

```
# terminal width 120
#
```

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。

コマンド	コマンドとパラメーター
username	username NAME [privilege LEVEL] [nopassword | password [0 | 7] PASSWORD] no username [NAME]
enable password	enable password [level PRIVILEGE-LEVEL] [0 | 7] PASSWORD no enable password [level PRIVILEGE-LEVEL]
service user-account encryption	service user-account encryption no service user-account encryption
prompt	prompt STRING no prompt
banner login	banner login cMESSAGEc no banner login
line	line {console | telnet | ssh}
login (Line)	login [local] no login
password	password [0 | 7] PASSWORD no password
session-timeout	session-timeout MINUTES no session-timeout
access-class	access-class IP-ACL-NAME no access-class IP-ACL-NAME

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。

コマンド	コマンドとパラメーター
show users	show users
show privilege	show privilege
clear line	clear line LINE-ID

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。
シンタックス	**username** *NAME* [**privilege** *LEVEL*] [**nopassword** | **password** [**0** | **7**] *PASSWORD*] **no username** [*NAME*]
パラメーター	*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。

username	
	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] *PASSWORD*（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。 • *PASSWORD*：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
コマンドモード	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。レベル 1 のユーザーは、ユーザー実行モードへのアクセスが許可されます。また、特権実行モードに遷移する場合は、enable コマンドを実行してください。 2 以上のレベルにログインしたユーザーは、特権実行モードを使用できます。レベル 2～15 にログインしたユーザーは、特権実行モードにアクセスできます。 ユーザー名を指定せずに no username コマンドを実行した場合、すべてのユーザーが削除されます。 デフォルトでは、ユーザーアカウントはありません。ユーザーアカウントがないときは、ユーザーはレベル 1 のユーザー実行モードに直接配置されます。特権実行モードに遷移する場合は、enable コマンドを実行します。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	enable password [level *PRIVILEGE-LEVEL*] [0 ｜ 7] *PASSWORD* no enable password [level *PRIVILEGE-LEVEL*]
パラメーター	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。

enable password	
	[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。 *PASSWORD*：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）
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	service user-account encryption no service user-account encryption
パラメーター	なし
デフォルト	無効
コマンドモード	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

service user-account encryption	
	• 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 プロンプトを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	prompt *STRING* no prompt
パラメーター	*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
コマンドモード	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	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。 • >：ユーザーレベルを表します。 • #：特権ユーザーレベルを表します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：CLI プロンプトを「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。
シンタックス	banner login *cMESSAGEc* no banner login
パラメーター	*c*：ログインバナーメッセージの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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。区切り文字「#」、メッセージ「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。区切り文字「%」、メッセージ 1 行目「#####################################」、2 行目「### 2F-L2-05, Apresia Systems LAN ###」、3 行目「###　　Location: TNTC-2Fb01 ###」とします。

```
# 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。
シンタックス	line {console | telnet | ssh}
パラメーター	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。 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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	login [local] no login
パラメーター	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）
コマンドモード	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。

login (Line)	
	• 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。 • 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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**password** [0 ｜ 7] *PASSWORD* **no password**
パラメーター	[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。 *PASSWORD*：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	パスワードなし
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**session-timeout** *MINUTES* **no session-timeout**
パラメーター	*MINUTES*：タイムアウト時間を 0～1439 分の範囲で指定します。0 を指定した場合は、タイムアウト処理は無効になります。
デフォルト	3 分
コマンドモード	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**

session-timeout	
	authentication-retries コマンドで設定します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	access-class *IP-ACL-NAME* no access-class *IP-ACL-NAME*
パラメーター	*IP-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
コマンドモード	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。
制限事項	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。
注意事項	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

access-class	
	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。
対象バージョン	1.01.01

使用例：標準 IP アクセスリスト「vty-filter（10.1.1.1 のみ許可）」を指定して、Telnet によるアクセスの制限を有効にする方法を示します。

```
# configure terminal
(config)# ip access-list vty-filter
(config-ip-acl)# permit 10.1.1.1 0.0.0.0
(config-ip-acl)# exit
(config)# line telnet
(config-line)# access-class vty-filter
(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。
シンタックス	show users
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
ID   Type      User-Name       Privilege Login-Time          IP address
--------------------------------------------------------------------------------
0    * console Anonymous       15        3M14S

Total Entries: 1
```

3.4.12 show privilege

show privilege	
目的	現在の特権レベルを表示します。
シンタックス	show privilege
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-

show privilege	
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**clear line** *LINE-ID*
パラメーター	*LINE-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。
デフォルト	なし
コマンドモード	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。
制限事項	ラインセッション(コンソール)は手動で切断できません。
注意事項	-
対象バージョン	1.01.01

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。

コマンド	コマンドとパラメーター
ip address	ip address {{IP-ADDRESS SUBNET-MASK | IP-ADDRESS/PREFIX-LENGTH} [secondary] | dhcp} no ip address [IP-ADDRESS SUBNET-MASK | IP-ADDRESS/PREFIX-LENGTH | dhcp]
ip default-gateway (mgmt 0)	ip default-gateway IP-ADDRESS no ip default-gateway IP-ADDRESS
ip proxy-arp	ip proxy-arp no ip proxy-arp
ip local-proxy-arp	ip local-proxy-arp no ip local-proxy-arp
arp	arp IP-ADDRESS MAC-ADDRESS no arp IP-ADDRESS MAC-ADDRESS
arp timeout	arp timeout MINUTES no arp timeout

基本 IPv4 関連の show／操作コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show ip interface	show ip interface [INTERFACE-ID] [brief]
show arp	show arp [ARP-TYPE | IP-ADDRESS [MASK] | interface INTERFACE-ID | MAC-ADDRESS]
show arp cache	show arp cache [IP-ADDRESS [MASK] | interface INTERFACE-ID]
show arp timeout	show arp timeout [interface vlan VLAN-ID]
clear arp-cache	clear arp-cache {all | interface INTERFACE-ID | IP-ADDRESS}

3.5.1 ip address

ip address	
目的	VLAN インターフェースのプライマリー／セカンダリーIPv4 アドレスを設定します。また、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。
シンタックス	**ip address** {{*IP-ADDRESS SUBNET-MASK* | *IP-ADDRESS/PREFIX-LENGTH*} [secondary] | dhcp} **no ip address** [*IP-ADDRESS SUBNET-MASK* | *IP-ADDRESS/PREFIX-LENGTH* | dhcp]
パラメーター	*IP-ADDRESS SUBNET-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/PREFIX-LENGTH*：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) **secondary**（省略可能）：セカンダリーIPv4 アドレスとして設定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。

ip address	
	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
コマンドモード	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	1 つの VLAN インターフェースに複数の異なるセグメントの IPv4 アドレスを設定できます。複数の IPv4 アドレスを設定する場合は、1 つをプライマリーIPv4 アドレスとして設定し、残りはセカンダリーIPv4 アドレスとして設定します。 プライマリーIPv4 アドレスは、VLAN インターフェースから送信される SNMP トラップメッセージや SYSLOG メッセージなどの送信元 IPv4 アドレスとして使用されます。
制限事項	IPv4 アドレスおよび IPv6 アドレスを設定可能な VLAN インターフェース数は 64 個です。同一 VLAN インターフェースで、IPv4 アドレスと IPv6 アドレスの併用も可能です。 装置全体に設定可能な IPv4 アドレス数は、セカンダリーIPv4 アドレスを含めて 64 個です。IPv6 アドレスと併用する場合は、IPv4 アドレスと IPv6 アドレスをそれぞれ 64 個まで設定可能です。 マネージメントポートでは、セカンダリーIPv4 アドレスの設定、**ip address dhcp** コマンドの設定はできません。
注意事項	**ip address dhcp** コマンドを設定した VLAN インターフェースでは、セカンダリーIPv4 アドレスを設定することは未サポートです。 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。
対象バージョン	1.01.01

使用例：VLAN 100 インターフェースにおいて、プライマリーIPv4 アドレスとして 192.0.2.254/24 を、セカンダリーIPv4 アドレスとして 172.16.0.20/24 と 192.168.50.30/24 を設定する方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# ip address 192.0.2.254/24
(config-if-vlan)# ip address 172.16.0.20/24 secondary
(config-if-vlan)# ip address 192.168.50.30/24 secondary
(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。
シンタックス	**ip default-gateway** *IP-ADDRESS* **no ip default-gateway** *IP-ADDRESS*
パラメーター	*IP-ADDRESS*：IPv4 アドレスを指定します。
デフォルト	0.0.0.0
コマンドモード	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

ip default-gateway (mgmt 0)	
	トゲートウェイ宛てに送信されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 ip proxy-arp

ip proxy-arp	
目的	プロキシ ARP 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。
シンタックス	ip proxy-arp no ip proxy-arp
パラメーター	なし
デフォルト	無効
コマンドモード	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	プロキシ ARP を有効にした VLAN インターフェースでは、以下に一致する ARP リクエストを受信した場合に、自身の MAC アドレスを使用して代理で ARP リプライを応答します。 • 自装置に直接接続されているネットワークで、その ARP リクエストを受信した VLAN インターフェース以外のネットワーク宛て • ルーティングテーブルに経路情報が登録されているネットワーク宛て
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 100 インターフェースで、プロキシ ARP を有効にする方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# ip proxy-arp
(config-if-vlan)#
```

3.5.4 ip local-proxy-arp

ip local-proxy-arp	
目的	ローカルプロキシ ARP 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。
シンタックス	ip local-proxy-arp no ip local-proxy-arp
パラメーター	なし
デフォルト	無効

ip local-proxy-arp	
コマンドモード	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	ローカルプロキシ ARP を有効にする場合は、**ip proxy-arp** コマンドでプロキシ ARP も有効にする必要があります。 ローカルプロキシ ARP を有効にした VLAN インターフェースでは、そのサブネット内の ARP リクエストを受信した場合に、ARP Reply を代理応答することができるようになります。これにより、同一サブネット内のホストが直接通信できないような特殊なネットワーク（例えば、プライベート VLAN を使用しているネットワークのセカンダリーVLAN 間や、独立ポート間など）でも、ローカルプロキシ ARP を有効にした装置を経由して、通信させることができるようになります。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 100 インターフェースで、ローカルプロキシ ARP を有効にする方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# ip local-proxy-arp
(config-if-vlan)#
```

3.5.5 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。
シンタックス	**arp** *IP-ADDRESS MAC-ADDRESS* **no arp** *IP-ADDRESS MAC-ADDRESS*
パラメーター	*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 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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式）
デフォルト	スタティックエントリーの設定なし
コマンドモード	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	-
制限事項	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。 ApresiaNP2000 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。
注意事項	-
対象バージョン	1.01.01

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)#
```

3.5.6 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。
シンタックス	**arp timeout** *MINUTES* **no arp timeout**
パラメーター	*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
コマンドモード	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ければ、ダイナミックエントリーはエージアウトされます。 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消去されません。ルートのネクストホップの ARP エントリーを消去するには、**clear arp-cache** コマンドを使用します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

3.5.7 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。
シンタックス	**show ip interface** [*INTERFACE-ID*] [**brief**]
パラメーター	*INTERFACE-ID*（省略可能）：情報を表示する 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**：マネージメントポートを指定します。 • **vlan**：VLAN インターフェースを指定します。 **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。
デフォルト	なし
コマンドモード	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。

show ip interface	
制限事項	-
注意事項	-
対象バージョン	1.01.01

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        0.0.0.0           up
mgmt_ipif    0.0.0.0           down

Total Entries: 2
```

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

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 0.0.0.0/0 (Manual) ...(3)
  ARP timeout is 240 minutes ...(4)
  Proxy ARP is disabled ...(5)
  IP Local Proxy ARP is disabled ...(6)
  Gratuitous-send is disabled, interval is 0 seconds ...(7)
```

項番	説明
(1)	インターフェース ID を表示します。
(2)	リンク状態を表示します。
(3)	IPv4 アドレスを表示します。
(4)	ARP エージングタイムを表示します。
(5)	プロキシ ARP の有効／無効を表示します。
(6)	ローカルプロキシ ARP の有効／無効を表示します。
(7)	GARP リクエスト送信の有効／無効、および送信間隔を表示します。

3.5.8 show arp

show arp	
目的	ARP テーブルのエントリーを表示します。
シンタックス	**show arp** [*ARP-TYPE* | *IP-ADDRESS* [*MASK*] | **interface** *INTERFACE-ID* | *MAC-ADDRESS*]
パラメーター	*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。

show arp	
	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** *INTERFACE-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。 • **mgmt**：マネージメントポートを指定します。 • **vlan**：VLAN インターフェースを指定します。 *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。 • XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン"-"で区切る形式) • XX:XX:XX:XX:XX:XX (1 バイトごとにコロン":"で区切る形式) • XXXX.XXXX.XXXX (2 バイトごとにドット"."で区切る形式) • XXXXXXXXXXXX (区切り文字を使用しない形式)
デフォルト	なし
コマンドモード	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、ARP テーブルのすべてのエントリーが表示されます。
制限事項	-
注意事項	*ARP-TYPE* に **static** を指定した場合、未使用のスタティックエントリーも表示されます。未使用のスタティックエントリーは、IPv4 インターフェースが表示されません。
対象バージョン	1.01.01

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)            (5)
IP Address         Hardware Addr      IP Interface   Age (min)
-----------------  -----------------  -------------  ---------------
  172.16.20.100    00-00-5E-00-53-33  vlan20         240
  172.16.20.254    00-40-66-A8-CC-36  vlan20         forever
  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      00-40-66-A8-CC-36  vlan10         forever

Total Entries: 6
```

項番	説明
(1)	表示されているエントリーの種類を表示します。 S - Static Entry：スタティックエントリー
(2)	IPv4 アドレスを表示します。
(3)	MAC アドレスを表示します。
(4)	エントリーを学習した IPv4 インターフェースを表示します。
(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。マネージメントポートで学習したダイナミック

項番	説明
	エントリーの場合は 0 と表示されます。

3.5.9 show arp cache

show arp cache	
目的	ARP キャッシュテーブルを表示します。
シンタックス	**show arp cache** [*IP-ADDRESS* [*MASK*] ｜ **interface** *INTERFACE-ID*]
パラメーター	*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** *INTERFACE-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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。 • **vlan**：VLAN インターフェースを指定します。
デフォルト	なし
コマンドモード	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、ARP キャッシュテーブルのすべてのエントリーが表示されます。
制限事項	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。
注意事項	AEOS-NP2000 Ver. 1.07.01 以降では、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
対象バージョン	1.04.01 1.07.01：**mgmt** パラメーター削除、表示対象の仕様変更

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
---------------  ----  ------------------  -------------  --------
172.16.20.100      20  00-00-5E-00-53-33   1/0/2          240
172.16.20.254      20  00-40-66-A8-CC-36   CPU            forever
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  00-40-66-A8-CC-36   CPU            forever

Total Entries: 6
```

項番	説明
(1)	IPv4 アドレスを表示します。

項番	説明
(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。

3.5.10 show arp timeout

show arp timeout	
目的	ARP エージングタイムを表示します。
シンタックス	**show arp timeout** [**interface vlan** *VLAN-ID*]
パラメーター	**vlan** *VLAN-ID*（省略可能）：ARP エージングタイムを表示する VLAN インターフェースを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ARP エージングタイム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。
(2)	ARP エージングタイムの設定値を表示します。

3.5.11 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消去します。
シンタックス	**clear arp-cache** {**all** | **interface** *INTERFACE-ID* | *IP-ADDRESS*}
パラメーター	**all**：すべてのダイナミックエントリーを消去する場合に指定します。 **interface** *INTERFACE-ID*：ダイナミックエントリーをすべて消去する 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。 • **vlan**：VLAN インターフェースを指定します。 • **mgmt**：マネージメントポートを指定します。

clear arp-cache	
	IP-ADDRESS：ダイナミックエントリーを消去する IPv4 アドレスを指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：すべてのダイナミックエントリーを ARP テーブルから消去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。

コマンド	コマンドとパラメーター
ipv6 enable	ipv6 enable no ipv6 enable
ipv6 address	ipv6 address {IPV6-ADDRESS/PREFIX-LENGTH | PREFIX-NAME SUB-BITS/PREFIX-LENGTH | IPV6-ADDRESS link-local} no ipv6 address {IPV6-ADDRESS/PREFIX-LENGTH | PREFIX-NAME SUB-BITS/PREFIX-LENGTH | IPV6-ADDRESS link-local}
ipv6 address eui-64	ipv6 address IPV6-PREFIX/PREFIX-LENGTH eui-64 no ipv6 address IPV6-PREFIX/PREFIX-LENGTH eui-64
ipv6 address dhcp	ipv6 address dhcp [rapid-commit] no ipv6 address dhcp
ipv6 address autoconfig	ipv6 address autoconfig [default] no ipv6 address autoconfig
ipv6 nd ns-interval	ipv6 nd ns-interval MILLI-SECONDS no ipv6 nd ns-interval
ipv6 neighbor	ipv6 neighbor IPV6-ADDRESS INTERFACE-NAME MAC-ADDRESS no ipv6 neighbor IPV6-ADDRESS INTERFACE-NAME

基本 IPv6 関連の show／操作コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show ipv6 interface	show ipv6 interface [INTERFACE-ID] [brief]
show ipv6 general-prefix	show ipv6 general-prefix [PREFIX-NAME]
show ipv6 neighbors	show ipv6 neighbors [INTERFACE-NAME] [IPV6-ADDRESS]
show ipv6 neighbors cache	show ipv6 neighbors cache [IPV6-ADDRESS | interface INTERFACE-ID]
clear ipv6 neighbors	clear ipv6 neighbors {all | interface INTERFACE-ID}

3.6.1 ipv6 enable

ipv6 enable	
目的	IPv6 アドレスが明示的に設定されていないインターフェースで、IPv6 の処理を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	ipv6 enable no ipv6 enable
パラメーター	なし
デフォルト	無効
コマンドモード	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	ipv6 enable は、インターフェースで IPv6 リンクローカルアドレスを自動出力して、IPv6 の処理を開始するコマンドです。

ipv6 enable	
	ApresiaNP2000 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。ApresiaNP2000 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**ipv6 address** {*IPV6-ADDRESS/PREFIX-LENGTH* | *PREFIX-NAME SUB-BITS/PREFIX-LENGTH* | *IPV6-ADDRESS* **link-local**} **no ipv6 address** {*IPV6-ADDRESS/PREFIX-LENGTH* | *PREFIX-NAME SUB-BITS/PREFIX-LENGTH* | *IPV6-ADDRESS* **link-local**}
パラメーター	*IPV6-ADDRESS/PREFIX-LENGTH*：IPv6 アドレスとプレフィックス長を指定します。 *PREFIX-NAME SUB-BITS/PREFIX-LENGTH*：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。 • *PREFIX-LENGTH*：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
コマンドモード	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	インターフェースには、手動設定、ステートレスアドレス設定、ステートフルアドレス設定などの方法で、複数の IPv6 アドレスを割り当てることができます。ただし、同じプレフィックス内で設定できる IPv6 アドレスは 1 つだけです。 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。
制限事項	IPv4 アドレスおよび IPv6 アドレスを設定可能な VLAN インターフェース数は 64 個です。同一 VLAN インターフェースで、IPv4 アドレスと IPv6 アドレスの併用も可能です。 装置全体に設定可能な IPv6 アドレス数は 64 個です。IPv4 アドレスと併用する場合は、IPv4 アドレスと IPv6 アドレスをそれぞれ 64 個まで設定可能です。 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。

ipv6 address	
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 インターフェースで IPv6 アドレス 2001:db8:1:2::5555/64 を設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 address 2001:db8:1:2::5555/64
(config-if-vlan)#
```

使用例：VLAN 1 インターフェースで IPv6 アドレス 2001:db8:1:2::5555/64 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:db8:1:2::5555/64
(config-if-vlan)#
```

使用例：VLAN 1 インターフェースで、DHCPv6-PD によって取得したプレフィックスを使用して、IPv6 アドレスを設定する方法を示します。この例では、DHCPv6-PD によって「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 によって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。
シンタックス	**ipv6 address** *IPV6-PREFIX/PREFIX-LENGTH* **eui-64** **no ipv6 address** *IPV6-PREFIX/PREFIX-LENGTH* **eui-64**
パラメーター	*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。 *PREFIX-LENGTH*：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
コマンドモード	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	本設定を実施すると、**ipv6 enable** も自動的に設定されます。
制限事項	IPv4 アドレスおよび IPv6 アドレスを設定可能な VLAN インターフェース数は 64 個です。同一 VLAN インターフェースで、IPv4 アドレスと IPv6 アドレスの併用も可能です。 装置全体に設定可能な IPv6 アドレス数は 64 個です。IPv4 アドレスと併用する

ipv6 address eui-64	
	場合は、IPv4 アドレスと IPv6 アドレスをそれぞれ 64 個まで設定可能です。 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。
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**ipv6 address dhcp [rapid-commit]** **no ipv6 address dhcp**
パラメーター	**rapid-commit**（省略可能）：2 メッセージの交換を使用して、アドレス委譲を進める場合に指定します。
デフォルト	なし
コマンドモード	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	**rapid-commit** パラメーターを指定した場合、アドレス委譲のためにメッセージ交換の個数を 4 個から 2 個に減らすことを要求するために、Solicit メッセージ内に Rapid Commit オプションを含めて送信します。 本設定を実施すると、**ipv6 enable** も自動的に設定されます。
制限事項	IPv4 アドレスおよび IPv6 アドレスを設定可能な VLAN インターフェース数は 64 個です。同一 VLAN インターフェースで、IPv4 アドレスと IPv6 アドレスの併用も可能です。 装置全体に設定可能な IPv6 アドレス数は 64 個です。IPv4 アドレスと併用する場合は、IPv4 アドレスと IPv6 アドレスをそれぞれ 64 個まで設定可能です。 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。
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 インターフェースで、DHCPv6 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 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

ipv6 address autoconfig	
	る場合は、no 形式のコマンドを使用します。
シンタックス	**ipv6 address autoconfig** [default] **no ipv6 address autoconfig**
パラメーター	**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
コマンドモード	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	本設定を実施すると、**ipv6 enable** も自動的に設定されます。 ApresiaNP2000 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。ApresiaNP2000 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。
制限事項	IPv4 アドレスおよび IPv6 アドレスを設定可能な VLAN インターフェース数は 64 個です。同一 VLAN インターフェースで、IPv4 アドレスと IPv6 アドレスの併用も可能です。 装置全体に設定可能な IPv6 アドレス数は 64 個です。IPv4 アドレスと併用する場合は、IPv4 アドレスと IPv6 アドレスをそれぞれ 64 個まで設定可能です。 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。
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 インターフェースで、ステートレス自動構成を使用して 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 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指定します。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。
シンタックス	**ipv6 nd ns-interval** *MILLI-SECONDS* **no ipv6 nd ns-interval**
パラメーター	*MILLI-SECONDS*：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）
コマンドモード	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。

ipv6 nd ns-interval	
制限事項	-
注意事項	**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。
対象バージョン	1.01.01

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。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**ipv6 neighbor** *IPV6-ADDRESS INTERFACE-NAME MAC-ADDRESS* **no ipv6 neighbor** *IPV6-ADDRESS INTERFACE-NAME*
パラメーター	*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。 *INTERFACE-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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式）
デフォルト	スタティックエントリーの設定なし
コマンドモード	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	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。
制限事項	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。 スタティック IPv6 ネイバーキャッシュ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。 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 個まで設定できます。
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**show ipv6 interface** [*INTERFACE-ID*] [**brief**]
パラメーター	*INTERFACE-ID*（省略可能）：情報を表示する 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**：VLAN インターフェースを指定します。 **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。
デフォルト	なし
コマンドモード	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 インターフェースの情報が表示されます。
制限事項	–
注意事項	–
対象バージョン	1.01.01

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)
vlan10 is up, link status is up
  IPv6 is enabled, ...(3)
  Link-local address: ...(4)
      fe80::240:66ff:feb4:96b5
  Global unicast address: ...(5)
      2001:db8:1:1::1001/64 (Manual)
  NS messages retransmit interval is 0 milliseconds ...(6)

vlan20 is up, link status is up
  IPv6 is enabled,
  Link-local address:
      fe80::240:66ff:feb4:96b5
  Global unicast address:
      2001:db8:2222:3333:240:66ff:feb4:96b5/64 (Stateless)
  NS messages retransmit interval is 0 milliseconds


Total Entries: 2
```

項番	説明
(1)	インターフェース ID を表示します。
(2)	リンク状態を表示します。
(3)	IPv6 の有効／無効を表示します。
(4)	リンクローカルアドレスを表示します。

項番	説明
(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。

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)
vlan10 is up, link status is up
    fe80::240:66ff:feb4:96b5 ...(3)
    2001:db8:1:1::1001

vlan20 is up, link status is up
    fe80::240:66ff:feb4:96b5
    2001:db8:2222:3333:240:66ff:feb4:96b5


Total Entries: 2
```

項番	説明
(1)	インターフェース ID を表示します。
(2)	リンク状態を表示します。
(3)	IPv6 アドレスを表示します。

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。
シンタックス	**show ipv6 general-prefix** [*PREFIX-NAME*]
パラメーター	*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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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-pd01 ...(1)
 Acquired via DHCPv6 PD ...(2)
```

```
    vlan10: 2001:db8:1111:1::/64
        Valid lifetime 2592000, preferred lifetime 604800
    Apply to interfaces ...(3)
      vlan201: ::1:2:3:4/64

 IPv6 prefix test-pd02 ...(1)
  Acquired via DHCPv6 PD ...(2)
    vlan20: 2001:db8:2222:1::/64
        Valid lifetime 2592000, preferred lifetime 604800

 Total Entries: 2
```

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。
シンタックス	**show ipv6 neighbors** [*INTERFACE-NAME*] [*IPV6-ADDRESS*]
パラメーター	*INTERFACE-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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
2001:db8:12:0:aaaa:bbbb:cccc:dddd      00-03-33-34-44-44 vlan12     D    REACH
fe80::203:33ff:fe34:4444               00-03-33-34-44-44 vlan12     D    REACH

Total Entries: 4
```

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。

項番	説明
(4)	エントリーの種類を表示します。 D：ダイナミックエントリー S：スタティックエントリー
(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。
シンタックス	**show ipv6 neighbors cache** [*IPV6-ADDRESS* | **interface** *INTERFACE-ID*]
パラメーター	*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** *INTERFACE-ID*（省略可能）：IPv6 ネイバーキャッシュ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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。 • **vlan**：VLAN インターフェースを指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	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。
注意事項	AEOS-NP2000 Ver. 1.06.02 以前では、装置に設定したグローバル IPv6 アドレスのエントリーは本コマンドでは表示されません。 AEOS-NP2000 Ver. 1.07.01 以降では、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
対象バージョン	1.04.01 1.07.01：表示対象の仕様変更

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:db8:12:0:aaaa:bbbb:cccc:dddd         12 00-03-33-34-44-44 C/5      REACH
2001:db8:11:0:1:2:3:4                     11 00-40-66-A8-CC-36 CPU
2001:db8:12::1                            12 00-40-66-A8-CC-36 CPU

Total Entries: 4
```

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消去します。
シンタックス	**clear ipv6 neighbors** {**all** | **interface** *INTERFACE-ID*}
パラメーター	**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消去する場合に指定します。 **interface** *INTERFACE-ID*：IPv6 ネイバーキャッシュのダイナミックエントリー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。 • **vlan**：VLAN インターフェースを指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	–
制限事項	–
注意事項	–
対象バージョン	1.01.01

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消去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。

コマンド	コマンドとパラメーター
ping access-class	ping access-class IP-ACL-NAME no ping access-class IP-ACL-NAME
ping	ping {[ip] IP-ADDRESS | [ipv6] IPV6-ADDRESS} [count TIMES] [timeout SECONDS] [source {IP-ADDRESS | IPV6-ADDRESS}] [size LENGTH] [interval SECONDS]
traceroute	traceroute {[ip] IP-ADDRESS | [ipv6] IPV6-ADDRESS} [probe NUMBER] [timeout SECONDS] [max-ttl TTL] [port DEST-PORT]

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。
シンタックス	**ping access-class** *IP-ACL-NAME* **no ping access-class** *IP-ACL-NAME*
パラメーター	*IP-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
コマンドモード	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	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。
制限事項	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。

ping access-class	
注意事項	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。
対象バージョン	1.01.01

使用例：標準 IP アクセスリスト「ping-filter（10.1.1.1 のみ許可）」を指定して、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。

```
# configure terminal
(config)# ip access-list ping-filter
(config-ip-acl)# permit 10.1.1.1 0.0.0.0
(config-ip-acl)# exit
(config)# ping access-class ping-filter
(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。
シンタックス	**ping** {[**ip**] *IP-ADDRESS* ｜ [**ipv6**] *IPV6-ADDRESS*} [**count** *TIMES*] [**timeout** *SECONDS*] [**source** {*IP-ADDRESS* ｜ *IPV6-ADDRESS*}] [**size** *LENGTH*] [**interval** *SECONDS*]
パラメーター	[**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。IPv6 アドレスが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*%*INTERFACE-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** *TIMES*（省略可能）：ping パケット(Echo Request)の送信数を 1～255 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 パケットで使用される送信元 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 バイトの範囲で指定します。 **interval** *SECONDS*（省略可能）：ping パケットの送信間隔を、1～3600 秒の範囲で指定します。
デフォルト	送信数：5 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
コマンドモード	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。
制限事項	宛先 IP アドレスを directed broadcast アドレスで指定する際に、その宛先ネットワークへの経路がデフォルトルート(0.0.0.0/0)情報によって解決される場合は、応答表示できない仕様制限があります。そのため、そのような使い方をする

ping	
	場合は、宛先ネットワークへのスタティックルートを設定し、デフォルトルート(0.0.0.0/0)情報以外で経路解決されるようにしてから実施してください。
注意事項	コマンドシンタックスのパラメーター指定は順不同ではありません。パラメーターの指定は、シンタックス欄の記載順に指定してください。パラメーター省略時は、省略したパラメーター以降が指定できます。
対象バージョン	1.01.01

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：VLAN 110 インターフェース経由で IPv6 マルチキャストアドレス ff02::1 宛てに ping 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。
シンタックス	**traceroute** {[**ip**] *IP-ADDRESS* ｜ [**ipv6**] *IPV6-ADDRESS*} [**probe** *NUMBER*] [**timeout** *SECONDS*] [**max-ttl** *TTL*] [**port** *DEST-PORT*]
パラメーター	[**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** *NUMBER*（省略可能）：ホップあたりのプローブ数を 1～1000 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** *TTL*（省略可能）：送信 UDP データグラムの最大 TTL 値を、1～255 の範囲で指定します。 **port** *DEST-PORT*（省略可能）：送信 UDP データグラムで使用される宛先 UDP ポート番号のベースとなる値を、1～65535 の範囲で指定します。宛先 UDP ポート番

traceroute	
	号は、UDP データグラムが送信されるたびに指定した値から加算されます。
デフォルト	初期 TTL が 1 の 40 バイト UDP データグラムを 3 つ送信 最大 TTL：30 タイムアウト時間：5 秒 宛先 UDP ポート番号のベースの値：33434 各 TTL のクエリー数：3
コマンドモード	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。
制限事項	**traceroute** を同時に使用できる最大セッション数は 3 個です。
注意事項	コマンドシンタックスのパラメーター指定は順不同ではありません。パラメーターの指定は、シンタックス欄の記載順に指定してください。パラメーター省略時は、省略したパラメーター以降が指定できます。
対象バージョン	1.01.01

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。

コマンド	コマンドとパラメーター
ip arp gratuitous	ip arp gratuitous no ip arp gratuitous
ip gratuitous-arps	ip gratuitous-arps [dad-reply] no ip gratuitous-arps [dad-reply]
arp gratuitous-send	arp gratuitous-send interval SECONDS no 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。
シンタックス	ip arp gratuitous no ip arp gratuitous
パラメーター	なし
デフォルト	有効
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	ip gratuitous-arps [dad-reply] no ip gratuitous-arps [dad-reply]
パラメーター	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
コマンドモード	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	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

ip gratuitous-arps	
	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。 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。
制限事項	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 形式のコマンドを実行してください。
注意事項	-
対象バージョン	1.01.01

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、インターフェースに設定します。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	**arp gratuitous-send interval** *SECONDS* **no arp gratuitous-send**
パラメーター	*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	無効
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01 1.04.01：インターフェース設定モード(mgmt)に追加

使用例：GARP メッセージの送信を有効にし、VLAN 100 インターフェースから 300 秒ごとに定期的に送信する方法を示します。

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

システムファイル管理関連の設定コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
boot image	boot image [check] URL [primary ｜ secondary]
boot config	boot config URL [primary ｜ secondary]
ip tftp source-interface	ip tftp source-interface INTERFACE-ID no ip tftp source-interface
ip ftp source-interface	ip ftp source-interface INTERFACE-ID no ip ftp 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。

コマンド	コマンドとパラメーター
show boot	show boot [unit UNIT-ID]
show running-config	show running-config [effective ｜ all] [interface INTERFACE-ID ｜ function [MODULE-TITLE]]
show startup-config	show startup-config
show config differences	show config differences {flash: URL1 ｜ running-config ｜ startup-config} {flash: URL2 ｜ running-config ｜ startup-config}
backup clone	backup clone
write	write [memory [secondary]]
copy primary-config secondary-config	copy primary-config secondary-config
reboot	reboot [unit UNIT-ID] [force_agree] [cold]
copy boot	copy boot
erase boot	erase boot
configure replace	configure replace {tftp: //location/filename ｜ ftp: //username:password@location:tcpport/filename ｜ flash: FILENAME} [force]
copy	copy SOURCE-URL DESTINATION-URL copy SOURCE-URL {tftp: [//LOCATION/DESTINATION-URL] ｜ ftp: [//USER-NAME:PASSWORD@LOCATION:TCP-PORT/DESTINATION-URL]} copy {tftp: [//LOCATION/SOURCE-URL] ｜ ftp: [//USER-NAME:PASSWORD@LOCATION:TCP-PORT/SOURCE-URL]} DESTINATION-URL
backup	backup {tftp: [//LOCATION[/PATH]] ｜ ftp: [//USER-NAME:PASSWORD@LOCATION:TCP-PORT[/PATH]] ｜ memory-card: [/PATH]} prefix BASENAME [no-software] [no-access-defender]
restore	restore {tftp: [//LOCATION[/PATH]] ｜ ftp: [//USER-NAME:PASSWORD@LOCATION:TCP-PORT[/PATH]] ｜ memory-card: [/PATH]} prefix BASENAME [no-software] [no-access-defender] [reboot]
clear running-config	clear running-config

コマンド	コマンドとパラメーター
reset system	reset system [factory-default] [ztp-disable]

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。
シンタックス	boot image [check] *URL* [primary ｜ secondary]
パラメーター	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：その装置のローカルフラッシュ上のファイルを使用する場合に指定します。例えば、c:/switch-image.had と入力します。 • d:/URL：その装置の SD カード上のファイルを使用する場合に指定します。例えば、d:/switch-image.had と入力します。 〈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）：その装置のローカルフラッシュ上のファイルを使用する場合に指定します。例えば、unit2:/c:/switch-image.had と入力します。 • unitX:/d:/URL（X はボックス ID）：その装置の SD カード上のファイルを使用する場合に指定します。例えば、unit2:/d:/switch-image.had と入力します。 primary（省略可能）：ファイル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場合に指定します。 secondary（省略可能）：ファイルを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
コマンドモード	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すると、ファイル情報を検証して、指定したファイルがブートイメージファイルとして適切かどうかを確認します。 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

boot image	
	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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：「c:/switch-image.had」という名前のブートイメージファイルを検証する方法を示します。検証されたブートイメージファイルのチェックサムは正常であることが示されています。また、ブートイメージファイルの情報が表示されています。

```
# 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：「c:/switch-image.had」という名前のブートイメージファイルを検証する方法を示します。ブートイメージファイルのチェックサムに異常があり、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。
シンタックス	**boot config** *URL* [**primary** ｜ **secondary**]
パラメーター	*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：その装置のローカルフラッシュ上のファイルを使用する場合に指定します。例えば、c:/switch-config.cfg と入力します。 • **d:**/URL：その装置の SD カード上のファイルを使用する場合に指定します。例えば、d:/switch-config.cfg と入力します。 〈対象がスタックマスター以外の装置の場合〉 • **unit**X**:/c:**/URL（X はボックス ID）：その装置のローカルフラッシュ上のファイルを使用する場合に指定します。例えば、unit2:/c:/switch-config.cfg と入力します。 • **unit**X**:/d:**/URL（X はボックス ID）：その装置の SD カード上のファイルを使用する場合に指定します。例えば、unit2:/d:/switch-config.cfg と入力します。 **primary**（省略可能）：ファイルを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）：ファイルを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
コマンドモード	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。 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「primary.cfg」が設定されています。 AEOS-NP2000 Ver.1.09.05 以降では、本コマンドの対象として、ApresiaNP2000 シリーズの構成情報ファイルを、同系統の ApresiaNP2100 シリーズでも使用できるように変更しました。なお、逆のケース（ApresiaNP2100 シリーズの構成情報ファイルを、同系統の ApresiaNP2000 シリーズで使用すること）はできません。（例：ApresiaNP2100-24T4X の場合は、ApresiaNP2000-24T4X の構成情報ファイルを使用可能）
制限事項	-
注意事項	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

boot config	
	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。
対象バージョン	1.01.01 1.09.05：ApresiaNP2100 シリーズにおいて、ApresiaNP2000 シリーズの構成情報ファイルを使用可能に変更

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 パケットの送信元アドレスとして使用される IP アドレスが設定されたインターフェースを指定します。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。
シンタックス	**ip tftp source-interface** *INTERFACE-ID* **no ip tftp source-interface**
パラメーター	*INTERFACE-ID*：TFTP パケットの送信元アドレスとして使用される IP アドレスが設定された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**：VLAN インターフェースを指定します。 • **mgmt**：マネージメントポートを指定します。
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
コマンドモード	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	-
制限事項	-
注意事項	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

ip tftp source-interface	
	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。
対象バージョン	1.01.01

使用例：TFTP パケットの送信元 IP アドレスに、マネージメントポートの IP アドレスを指定する方法を示します。

```
# configure terminal
(config)# ip tftp source-interface mgmt0
(config)#
```

3.9.4 ip ftp source-interface

ip ftp source-interface	
目的	FTP パケットの送信元アドレスとして使用される IP アドレスが設定されたインターフェースを指定します。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。
シンタックス	ip ftp source-interface *INTERFACE-ID* no ip ftp source-interface
パラメーター	*INTERFACE-ID*：FTP パケットの送信元アドレスとして使用される IP アドレスが設定された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：VLAN インターフェースを指定します。 • mgmt：マネージメントポートを指定します。
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
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：FTP パケットの送信元 IP アドレスに、マネージメントポートの IP アドレスを指定する方法を示します。

```
# configure terminal
(config)# ip ftp source-interface mgmt0
(config)#
```

3.9.5 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。
シンタックス	show boot [unit *UNIT-ID*]
パラメーター	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。

show boot	
デフォルト	なし
コマンドモード	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	「apresia-loader.conf」が保存されている SD カードを挿入した場合は、その中に記録されているブートスクリプト情報も表示されます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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:/image1.had ...(2)
 Primary boot config: /c:/config1.cfg ...(3)
 Secondary boot image: No valid boot image. ...(4)
 Secondary boot config: No valid boot config. ...(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。

3.9.6 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。
シンタックス	**show running-config** [**effective** | **all**] [**interface** *INTERFACE-ID* | **function** [*MODULE-TITLE*]]
パラメーター	**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）：デフォルト設定を含めて、すべての設定を表示する場合に指定

show running-config	
	します。 **interface** *INTERFACE-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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。 • **vlan**：VLAN インターフェースを指定します。 • **mgmt**：マネージメントポートを指定します。 **function** [*MODULE-TITLE*]（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（*MODULE-TITLE*）を省略した場合は、入力可能な機能名の一覧が表示されます。機能名は一覧で確認できる大文字文字列で、省略せずに入力する必要があります。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 : 2360 bytes ...(1)

#-------------------------------------------------------------------------------
#                  ApresiaNP2000-24T4X Gigabit Ethernet Switch
#                                Configuration
#
#                            Firmware: Build 1.03.01
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------

# Date: Wed Nov 09 10:44:28 2016


# STACK

##  stacking config information
##   #Box                    Prio-
##   #ID    Type       Exist rity
##   #--- ----------- ----- -----
```

```
##   #  1 ApresiaNP2000-24T4X exist 32
##   #  2 ApresiaNP2000-24T4X no
##   #  3 NOT_EXIST no
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 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 : 157 bytes


# IP

interface vlan 10
 ip address 192.168.10.251/24
interface vlan 20
 ip address 192.168.20.251/24
 ipv6 enable
 ipv6 address 2001:db8:12::1/64
```

3.9.7 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。
シンタックス	**show startup-config**
パラメーター	なし
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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

#-------------------------------------------------------------------------------
#                  ApresiaNP2000-24T4X Gigabit Ethernet Switch
#                                Configuration
#
#                            Firmware: Build 1.03.01
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------

# Date: Wed Feb 24 16:32:19 2016


# STACK

no stack
```

```
no stack my_box_id
stack my_box_priority 32
no stack preempt

# PRIVMGMT

username 15 password 0 15
username 15 privilege 15
line console
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.9.8 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。
シンタックス	**show config differences {flash:** *URL1* **| running-config | startup-config} {flash:** *URL2* **| running-config | startup-config}**
パラメーター	**flash:** *URL1*：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:/***URL1*：装置のローカルフラッシュ上のファイルを使用する場合に指定します。例えば、c:/switch-config.cfg と入力します。 • **d:/***URL1*：SD カード上のファイルを使用する場合に指定します。例えば、d:/switch-config.cfg と入力します。 • *UNIT-ID***:/c:/***URL1*：スタックメンバーのローカルフラッシュ上のファイルを使用する場合に指定します。例えば、unit2:/c:/switch-config.cfg と入力します。 **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。 **flash:** *URL2*：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:/***URL2*：装置のローカルフラッシュ上のファイルを使用する場合に指定します。例えば、c:/switch-config.cfg と入力します。 • **d:/***URL2*：SD カード上のファイルを使用する場合に指定します。例えば、d:/switch-config.cfg と入力します。 • *UNIT-ID***:/c:/***URL2*：スタックメンバーのローカルフラッシュ上のファイルを使用する場合に指定します。例えば、unit2:/c:/switch-config.cfg と入力します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.04.02

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 1/0/25
```

```
+ 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

3.9.9 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。
シンタックス	**backup clone**
パラメーター	なし
デフォルト	なし
コマンドモード	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 • 個別 Web 認証ページ • 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 AEOS-NP2000 Ver.1.09.05 以降では、ApresiaNP2000 シリーズで本コマンドで作成された startup-config ファイル「apresia-startup-config.txt」を、同系統

backup clone	
	の ApresiaNP2100 シリーズでも使用できるように変更しました。以下に使用可能な組み合わせを示します。なお、逆のケース（ApresiaNP2100 シリーズで作成された startup-config ファイルを、同系統の ApresiaNP2000 シリーズで使用すること）はできません。 • ApresiaNP2100-24T4X の場合は、ApresiaNP2000-24T4X で作成された startup-config ファイルを使用可能 • ApresiaNP2100-48T4X の場合は、ApresiaNP2000-48T4X で作成された startup-config ファイルを使用可能 • ApresiaNP2100-24T4X-PoE の場合は、ApresiaNP2000-24T4X-PoE で作成された startup-config ファイルを使用可能 • ApresiaNP2100-48T4X-PoE の場合は、ApresiaNP2000-48T4X-PoE で作成された startup-config ファイルを使用可能 これにより、AEOS-NP2000 Ver.1.09.05 以降の ApresiaNP2000 シリーズで作成された SD カードブート用の SD カードなら、ファームウェアも含めて同系統の ApresiaNP2100 シリーズで利用可能になり、故障などの理由で ApresiaNP2000 シリーズを同系統の ApresiaNP2100 シリーズに交換する際に、その SD カードを挿入して起動するだけで交換できるようになります。 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-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。

backup clone	
制限事項	-
注意事項	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。 AEOS-NP2000 Ver. 1.09.01 以降では、個別 Web 認証ページ(180 ファイル)、Web アクセス拒否通知ページも処理対象になります。なお、同一装置で個別 Web 認証ページと SD カードブートを併用する場合は、すべてのファイルを SD カードに保存できないことがあります。詳細は **web-authentication interface** コマンドを参照してください。 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(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。
対象バージョン	1.01.01 1.02.01：バックアップ対象ファイル追加（Web ページ画像は未サポート） 1.03.01：Web ページ画像をサポート 1.09.01：バックアップ対象ファイル追加（個別 Web 認証ページ、Web アクセス拒否通知ページ） 1.09.05：ApresiaNP2100 シリーズにおいて、ApresiaNP2000 シリーズで作成された startup-config ファイルを使用可能に変更

使用例：AEOS-NP2000 Ver. 1.09.01 より前のバージョンで、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.
```

使用例：AEOS-NP2000 Ver. 1.09.01 以降で、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)........... Done.
  Uploading SSH DSA key file (apresia-dsa-key)........... Fail.
  Uploading web authentication login-page file (apresia-login-page)........... Done.
  Uploading web authentication 01-login-page file (apresia-01-login-page)........... Fail.
  Uploading web authentication 02-login-page file (apresia-02-login-page)........... Fail.
  Uploading web authentication 03-login-page file (apresia-03-login-page)........... Fail.
  Uploading web authentication 04-login-page file (apresia-04-login-page)........... Fail.
  Uploading web authentication 05-login-page file (apresia-05-login-page)........... Done.
  Uploading web authentication 06-login-page file (apresia-06-login-page)........... Fail.
  Uploading web authentication 07-login-page file (apresia-07-login-page)........... Fail.
  Uploading web authentication 08-login-page file (apresia-08-login-page)........... Fail.
  Uploading web authentication 09-login-page file (apresia-09-login-page)........... Fail.
  Uploading web authentication 10-login-page file (apresia-10-login-page)........... Fail.
  Uploading web authentication 11-login-page file (apresia-11-login-page)........... Fail.
  Uploading web authentication 12-login-page file (apresia-12-login-page)........... Fail.
  Uploading web authentication 13-login-page file (apresia-13-login-page)........... Fail.
  Uploading web authentication 14-login-page file (apresia-14-login-page)........... Fail.
  Uploading web authentication 15-login-page file (apresia-15-login-page)........... Fail.
～～省略～～
```

3.9.10 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。
シンタックス	write [memory [secondary]]
パラメーター	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。
デフォルト	なし
コマンドモード	特権実行モード

write	
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。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。**secondary** パラメーターは AEOS-NP2000 Ver. 1.05.01 以降でサポートしています。
制限事項	**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。
注意事項	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。
対象バージョン	1.01.01 1.05.01：**secondary** パラメーター追加

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.
```

3.9.11 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。
シンタックス	**copy primary-config secondary-config**
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.05.01

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
```

3.9.12 reboot

reboot	
目的	装置を再起動します。

reboot	
シンタックス	reboot [unit *UNIT-ID*] [force_agree] [cold]
パラメーター	unit *UNIT-ID*（省略可能）：再起動する装置のボックス 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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	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、本コマンドを実行ください。
対象バージョン	1.01.01 1.03.01：unit パラメーター追加 1.09.01：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...
```

3.9.13 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。
シンタックス	copy boot
パラメーター	なし
デフォルト	なし
コマンドモード	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、装置が起動する際に「apresia-loader.conf」のブートスクリプトが参照されます。

copy boot	
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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.
```

3.9.14 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。
シンタックス	erase boot
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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.
```

3.9.15 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。
シンタックス	configure replace {tftp: *//location/filename* | ftp: *//username:password@location:tcpport/filename* | flash: *FILENAME*} [force]
パラメーター	tftp:：TFTP サーバー上の構成情報をダウンロードする場合に指定します。

configure replace	
	//location/filename：TFTP サーバー上の構成情報の URL を指定します。 **ftp:**：FTP サーバー上の構成情報を指定します。 *//username:password@location:tcpport/filename*：FTP サーバー上の構成情報の URL を指定します。 **flash:**：装置の NVRAM に格納されている構成情報をコピーする場合に指定します。 *FILENAME*：装置の NVRAM に格納されている構成情報名を指定します。 **force**（省略可能）：確認せずに、直ちにコマンドを実行する場合に指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	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。 AEOS-NP2000 Ver.1.09.05 以降では、本コマンドの対象として、ApresiaNP2000 シリーズの構成情報ファイルを、同系統の ApresiaNP2100 シリーズでも使用できるように変更しました。なお、逆のケース（ApresiaNP2100 シリーズの構成情報ファイルを、同系統の ApresiaNP2000 シリーズで使用すること）はできません。（例：ApresiaNP2100-24T4X の場合は、ApresiaNP2000-24T4X の構成情報ファイルを使用可能） 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。
対象バージョン	1.01.01 1.09.05：ApresiaNP2100 シリーズにおいて、ApresiaNP2000 シリーズの構成情報ファイルを使用可能に変更

使用例：TFTP サーバーから「config.cfg」をダウンロードして、現在の running-config を「config.cfg」に置き換える方法を示します。

```
# configure replace tftp: //10.0.0.66/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://10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
```

```
  Executing script file config.cfg ......
  Executing done
```

使用例：FTP サーバーから「config.cfg」をダウンロードして、現在の running-config を「config.cfg」に置き換える方法を示します。確認なしで、コマンドを直ちに実行する例を示しています。

```
# configure replace ftp: //User:123@10.0.0.66:80/config.cfg force

 Accessing ftp: //10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done
```

使用例：装置の NVRAM に格納されている指定の構成情報「config.cfg」で、現在の running-config を置き換える方法を示します。確認なしで、コマンドを直ちに実行する例を示しています。

```
# configure replace flash: config.cfg force

 Executing script file config.cfg ......
 Executing done
```

3.9.16 copy

copy	
目的	ファイルを別のファイルにコピーします。
シンタックス	**copy** *SOURCE-URL DESTINATION-URL* **copy** *SOURCE-URL* {**tftp:** [*//LOCATION/DESTINATION-URL*] | **ftp:** [*//USER-NAME:PASSWORD@LOCATION:TCP-PORT/DESTINATION-URL*]} **copy** {**tftp:** [*//LOCATION/SOURCE-URL*] | **ftp:** [*//USER-NAME:PASSWORD@LOCATION:TCP-PORT/SOURCE-URL*]} *DESTINATION-URL*
パラメーター	*SOURCE-URL*：コピー元ファイルのコピー元 URL を指定します。以下のパラメーターが使用できます。 • **startup-config**：startup-config をコピー（アップロード）する場合に指定します。 • **running-config**：running-config をコピー（アップロード）する場合に指定します。 • **flash:** [*PATH-FILE-NAME*]：特定のファイルをコピーする場合に、コピー元ファイルを指定します。 • **log**：システムログをコピーする場合に指定します。 *DESTINATION-URL*：コピー先ファイルのコピー先 URL を指定します。以下のパラメーターが使用できます。 • **running-config**：running-config へ適用する場合に指定します。 • **startup-config** [**secondary**]：startup-config へ適用する場合に指定します。次回起動時の設定を保存します。現在の設定は NVRAM に保管され、ファイル名は、**boot config** コマンドで指定されるファイル名と同じになります。**secondary** パラメーターは、セカンダリー構成情報が存在する場合に、**copy running-config startup-config** コマンドでのみ使用できます。 • **flash:** [*PATH-FILE-NAME*]：特定のファイルへコピーする場合に、コピー先ファイルを指定します。相対パスを指定した場合、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、各ユニットの現在のパス

copy	
	に格納されます。絶対パスを指定した場合、絶対パスが示す場所にファイルがダウンロードされます。絶対パスにユニット情報が存在しない場合、マスター装置が割り当てられます。 *LOCATION*：TFTP/FTP サーバーの IPv4 アドレス、または IPv6 アドレスを指定します。 *USER-NAME*：FTP サーバーのユーザー名を指定します。 *PASSWORD*：上記ユーザーのパスワードを指定します。
デフォルト	なし
コマンドモード	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。 **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 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。 AEOS-NP2000 Ver.1.09.05 以降では、本コマンドのコピー元ファイルとして、ApresiaNP2000 シリーズの構成情報ファイルを、同系統の ApresiaNP2100 シリーズでも使用できるように変更しました。なお、逆のケース（ApresiaNP2100 シリーズの構成情報ファイルを、同系統の ApresiaNP2000 シリーズで使用すること）はできません。（例：ApresiaNP2100-24T4X の場合は、ApresiaNP2000-24T4X の構成情報ファイルを使用可能）
制限事項	**copy tftp: startup-config** コマンドと **copy ftp: 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。
注意事項	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

copy	
	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。
対象バージョン	1.01.01 1.05.01：**secondary** パラメーター追加 1.09.05：ApresiaNP2100 シリーズにおいて、ApresiaNP2000 シリーズの構成情報ファイルを使用可能に変更

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.
```

3.9.17 backup

backup	
目的	ユーザー定義のプレフィックス文字列を持つ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 TFTP/FTP サーバーまたは SD カードにバックアップします。
シンタックス	backup {tftp: [//*LOCATION*[/*PATH*]] | ftp: [//*USER-NAME*:*PASSWORD*@*LOCATION*:*TCP-PORT*[/*PATH*]] | memory-card: [/*PATH*]} prefix *BASENAME* [no-software] [no-access-defender]
パラメーター	tftp:：装置のローカルフラッシュから TFTP サーバーに、動作に必要なファイルをバックアップする場合に指定します。 • *LOCATION*（省略可能）：TFTP サーバーの IPv4/IPv6 アドレスを指定します。 • *PATH*（省略可能）：TFTP サーバー上のバックアップ先パスを指定します。 ftp:：装置のローカルフラッシュから FTP サーバーに、動作に必要なファイルをバックアップする場合に指定します。 • *USER-NAME*（省略可能）：FTP サーバーの FTP アカウントのユーザー名を指定します。 • *PASSWORD*（省略可能）：FTP サーバーの FTP アカウントのパスワードを指定します。 • *LOCATION*（省略可能）：FTP サーバーの IPv4/IPv6 アドレスを指定します。 • *TCP-PORT*（省略可能）：FTP サーバーで使用する TCP ポート番号を指定します。 • *PATH*（省略可能）：FTP サーバー上のバックアップ先パスを指定します。 memory-card:：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場合に指定します。 • *PATH*（省略可能）：SD カード上のバックアップ先パスを指定します。 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。 no-software（省略可能）：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します。

backup	
	no-access-defender（省略可能）：AccessDefender の Web 認証ページ(6 ファイル)、AccessDefender の個別 Web 認証ページ(180 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します。
デフォルト	なし
コマンドモード	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 • 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 • 個別 Web 認証ページ • 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 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。
制限事項	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。
注意事項	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。 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

backup	
	集してください。 AEOS-NP2000 Ver. 1.09.01 以降では、個別 Web 認証ページ(180 ファイル)、Web アクセス拒否通知ページも処理対象になります。なお、同一装置で個別 Web 認証ページと **backup memory-card: prefix** コマンドを併用する場合は、すべてのファイルを SD カードに保存できないことがあります。詳細は **web-authentication interface** コマンドを参照してください。 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。
対象バージョン	1.01.01 1.02.01：バックアップ対象ファイル追加（Web ページ画像は未サポート)、プレフィックス文字列の最大数変更（13 文字から 12 文字へ) 1.03.01：Web ページ画像をサポート 1.07.01：**no-software** パラメーター、**no-access-defender** パラメーター追加 1.09.01：バックアップ対象ファイル追加（個別 Web 認証ページ、Web アクセス拒否通知ページ)

使用例：AEOS-NP2000 Ver. 1.09.01 より前のバージョンで、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.
```

使用例：AEOS-NP2000 Ver. 1.09.01 以降で、プレフィックス文字列を「test」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 test

 Uploading firmware image file (test-software.had)........... Done.
 Uploading start-up configuration file (test-startup-config.txt)........... Done.
 Uploading running configuration file (test-running-config.txt)........... Done.
 Uploading system name file (test-system-name.txt)........... Done.
 Uploading SSH RSA key file (test-rsa-key)........... Done.
 Uploading SSH DSA key file (test-dsa-key)........... Fail.
 Uploading web authentication login-page file (test-login-page)........... Done.
```

```
  Uploading web authentication 01-login-page file (test-01-login-page)........... Fail.
  Uploading web authentication 02-login-page file (test-02-login-page)........... Fail.
  Uploading web authentication 03-login-page file (test-03-login-page)........... Fail.
  Uploading web authentication 04-login-page file (test-04-login-page)........... Fail.
  Uploading web authentication 05-login-page file (test-05-login-page)........... Done.
  Uploading web authentication 06-login-page file (test-06-login-page)........... Fail.
  Uploading web authentication 07-login-page file (test-07-login-page)........... Fail.
  Uploading web authentication 08-login-page file (test-08-login-page)........... Fail.
  Uploading web authentication 09-login-page file (test-09-login-page)........... Fail.
  Uploading web authentication 10-login-page file (test-10-login-page)........... Fail.
  Uploading web authentication 11-login-page file (test-11-login-page)........... Fail.
  Uploading web authentication 12-login-page file (test-12-login-page)........... Fail.
  Uploading web authentication 13-login-page file (test-13-login-page)........... Fail.
  Uploading web authentication 14-login-page file (test-14-login-page)........... Fail.
  Uploading web authentication 15-login-page file (test-15-login-page)........... Fail.
 ～～省略～～
```

3.9.18 restore

restore	
目的	TFTP/FTP 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。
シンタックス	**restore** {**tftp:** [//*LOCATION*[/*PATH*]] ｜ **ftp:** [//*USER-NAME*:*PASSWORD*@*LOCATION*:*TCP-PORT*[/*PATH*]] ｜ **memory-card:** [/*PATH*]} **prefix** *BASENAME* [**no-software**] [**no-access-defender**] [**reboot**]
パラメーター	**tftp:**：TFTP サーバー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する場合に指定します。 • *LOCATION*（省略可能）：TFTP サーバーの IPv4/IPv6 アドレスを指定します。 • *PATH*（省略可能）：TFTP サーバー上のバックアップ先パスを指定します。 **ftp:**：FTP サーバー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する場合に指定します。 • *USER-NAME*（省略可能）：FTP サーバーの FTP アカウントのユーザー名を指定します。 • *PASSWORD*（省略可能）：FTP サーバーの FTP アカウントのパスワードを指定します。 • *LOCATION*（省略可能）：FTP サーバーの IPv4/IPv6 アドレスを指定します。 • *TCP-PORT*（省略可能）：FTP サーバーで使用する TCP ポート番号を指定します。 • *PATH*（省略可能）：TFTP サーバー上のバックアップ先パスを指定します。 **memory-card:**：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する場合に指定します。 • *PATH*（省略可能）：SD カード上のバックアップ先パスを指定します。 **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。 **no-software**（省略可能）：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します。 **no-access-defender**（省略可能）：AccessDefender の Web 認証ページ(6 ファイル)、AccessDefender の個別 Web 認証ページ(180 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

restore	
	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します。 reboot（省略可能）：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します。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ません。
デフォルト	なし
コマンドモード	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 　• 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 • 個別 Web 認証ページ • 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。
制限事項	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。
注意事項	AEOS-NP2000 Ver. 1.09.01 以降では、個別 Web 認証ページ(180 ファイル)、Web

restore	
	アクセス拒否通知ページも処理対象になります。 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。
対象バージョン	1.01.01 1.02.01：リストア対象ファイル追加（Web ページ画像は未サポート)、プレフィックス文字列の最大数変更（13文字から12文字へ) 1.03.01：Webページ画像をサポート 1.07.01：**no-software** パラメーター、**no-access-defender** パラメーター、**reboot** パラメーター追加 1.09.01：リストア対象ファイル追加（個別 Web 認証ページ、Web アクセス拒否通知ページ)

使用例：AEOS-NP2000 Ver. 1.09.01より前のバージョンで、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.
```

使用例：AEOS-NP2000 Ver. 1.09.01以降で、プレフィックス文字列を「test」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 test

 Downloading firmware image file (test-software.had)........... Done.
 Downloading start-up configuration file (test-startup-config.txt)........... Done.
 Downloading system name file (test-system-name.txt)........... Done.
 Downloading SSH RSA key file (test-rsa-key)........... Done.
 Downloading SSH DSA key file (test-dsa-key)........... Fail.
 Downloading web authentication login-page file (test-login-page)........... Done.
 Downloading web authentication 01-login-page file (test-01-login-page)........... Fail.
 Downloading web authentication 02-login-page file (test-02-login-page)........... Fail.
 Downloading web authentication 03-login-page file (test-03-login-page)........... Fail.
 Downloading web authentication 04-login-page file (test-04-login-page)........... Fail.
 Downloading web authentication 05-login-page file (test-05-login-page)........... Done.
 Downloading web authentication 06-login-page file (test-06-login-page)........... Fail.
 Downloading web authentication 07-login-page file (test-07-login-page)........... Fail.
 Downloading web authentication 08-login-page file (test-08-login-page)........... Fail.
 Downloading web authentication 09-login-page file (test-09-login-page)........... Fail.
```

```
  Downloading web authentication 10-login-page file (test-10-login-page)..... Fail.
  Downloading web authentication 11-login-page file (test-11-login-page)..... Fail.
  Downloading web authentication 12-login-page file (test-12-login-page)..... Fail.
  Downloading web authentication 13-login-page file (test-13-login-page)..... Fail.
  Downloading web authentication 14-login-page file (test-14-login-page)..... Fail.
  Downloading web authentication 15-login-page file (test-15-login-page)..... Fail.
  Downloading web authentication 16-login-page file (test-16-login-page)..... Fail.
～～省略～～
```

3.9.19 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。
シンタックス	**clear running-config**
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	**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。
注意事項	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。
対象バージョン	1.01.01

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
```

3.9.20 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。
シンタックス	**reset system [factory-default] [ztp-disable]**
パラメーター	**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。 **ztp-disable**（省略可能）：ZTP 機能を無効設定にする場合に指定します。
デフォルト	なし
コマンドモード	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

reset system	
	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 **ztp-disable** パラメーターを指定すると、ZTP 機能を無効にした状態で再起動します。なお、初期化された後の構成情報（running-config と startup-config の両方）には、**no ztp enable** が設定されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01 1.04.01：**factory-default** パラメーター 1.09.05：**ztp-disable** パラメーター追加

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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ip dhcp client class-id	ip dhcp client class-id {STRING | hex HEX-STRING} no ip dhcp client class-id
ip dhcp client client-id	ip dhcp client client-id INTERFACE-ID no ip dhcp client client-id
ip dhcp client hostname	ip dhcp client hostname HOST-NAME no ip dhcp client hostname
ip dhcp client lease	ip dhcp client lease DAYS [HOURS [MINUTES]] no 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。
シンタックス	**ip dhcp client class-id** {*STRING* | **hex** *HEX-STRING*} **no ip dhcp client class-id**
パラメーター	*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, LtdApresiaNP2000-24T4X)
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**ip dhcp client client-id** *INTERFACE-ID* **no ip dhcp client client-id**
パラメーター	*INTERFACE-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**：VLAN インターフェースを指定します。
デフォルト	対象 VLAN インターフェースの MAC アドレス
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**ip dhcp client hostname** *HOST-NAME* **no ip dhcp client hostname**
パラメーター	*HOST-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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**ip dhcp client lease** *DAYS* [*HOURS* [*MINUTES*]] **no ip dhcp client lease**
パラメーター	*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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 リレーコマンド

DHCP リレー関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ip dhcp pool (DHCP Relay)	ip dhcp pool POOL-NAME no ip dhcp pool POOL-NAME
relay destination	relay destination IP-ADDRESS no relay destination IP-ADDRESS
relay source	relay source {NETWORK-PREFIX PREFIX-MASK | NETWORK-ADDRESS/MASK-LENGTH} no relay source {NETWORK-PREFIX PREFIX-MASK | NETWORK-ADDRESS/MASK-LENGTH}
relay target	relay target IP-ADDRESS no relay target IP-ADDRESS
ip dhcp relay unicast	ip dhcp relay unicast no ip dhcp relay unicast
ip dhcp relay information check	ip dhcp relay information check no ip dhcp relay information check
ip dhcp relay information check-reply	ip dhcp relay information check-reply [none] no ip dhcp relay information check-reply [none]
ip dhcp relay information option	ip dhcp relay information option no ip dhcp relay information option
ip dhcp relay information option-insert	ip dhcp relay information option-insert [none] no ip dhcp relay information option-insert [none]
ip dhcp relay information policy	ip dhcp relay information policy {drop | keep | replace} no ip dhcp relay information policy
ip dhcp relay information policy-action	ip dhcp relay information policy-action {drop | keep | replace} no ip dhcp relay information policy-action
ip dhcp relay information trust-all	ip dhcp relay information trust-all no ip dhcp relay information trust-all
ip dhcp relay information trusted	ip dhcp relay information trusted no ip dhcp relay information trusted
service dhcp (DHCP Relay)	service dhcp no service dhcp
show ip dhcp relay information trusted-sources	show ip dhcp relay information trusted-sources
show ip dhcp relay information option-insert	show ip dhcp relay information option-insert
show ip dhcp relay information policy-action	show ip dhcp relay information policy-action

4.2.1 ip dhcp pool (DHCP Relay)

ip dhcp pool (DHCP Relay)	
目的	DHCP リレー機能のための DHCP リレー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。
シンタックス	**ip dhcp pool** *POOL-NAME* **no ip dhcp pool** *POOL-NAME*
パラメーター	*POOL-NAME*：DHCP リレープール名を最大 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
コマンドモード	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	DHCP リレー機能を使用する場合は、以下の設定を実施します。 • **ip dhcp pool** コマンドで、DHCP リレープールを設定します。 • **relay source** コマンドで、DHCP リレー対象の送信元サブネットを設定します。 • **relay destination** コマンドで、リレー先 DHCP サーバーの IP アドレスを設定します。 **class** コマンドと **relay target** コマンドを使用すると、DHCP クラスで指定したオプションに一致した場合のリレー先 DHCP サーバーを設定することができます。 DHCP クラス（**relay target** コマンド）と **relay destination** コマンドの両方を設定している場合、DHCP クラスに一致した対象パケットは **relay target** コマンドで指定した宛先にリレーされ、一致しなかった対象パケットは **relay destination** コマンドで指定した宛先にリレーされます。 DHCP リレー機能を使用する場合も、**service dhcp** コマンドを有効に設定する必要があります。
制限事項	DHCP リレープールは最大 16 個設定できます。
注意事項	-
対象バージョン	1.08.01

使用例：DHCP リレープール「pool1」を設定し、DHCP リレー対象の送信元サブネットを 172.16.10.0/24 に、リレー先 DHCP サーバーの IP アドレスを 192.168.1.100 に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# relay source 172.16.10.0/24
(config-dhcp-pool)# relay destination 192.168.1.100
(config-dhcp-pool)#
```

4.2.2 relay destination

relay destination	
目的	DHCP リレー機能のリレー先 DHCP サーバーの 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。
シンタックス	**relay destination** *IP-ADDRESS* **no relay destination** *IP-ADDRESS*

relay destination	
パラメーター	*IP-ADDRESS*：リレー先 DHCP サーバーの IP アドレスを指定します。
デフォルト	なし
コマンドモード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	リレー先 DHCP サーバーの IP アドレスを複数設定した場合、対象の DHCP パケットはすべてのリレー先にリレーされます。
制限事項	**relay destination** コマンドで設定するリレー先 DHCP サーバーの IP アドレスは、1 つの DHCP リレープールにつき最大 4 個まで設定できます。
注意事項	-
対象バージョン	1.08.01

使用例：DHCP リレープール「pool1」を設定し、DHCP リレー対象の送信元サブネットを 172.16.10.0/24 に、リレー先 DHCP サーバーの IP アドレスを 192.168.1.100 と 192.168.2.200 に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# relay source 172.16.10.0/24
(config-dhcp-pool)# relay destination 192.168.1.100
(config-dhcp-pool)# relay destination 192.168.2.200
(config-dhcp-pool)#
```

4.2.3 relay source

relay source	
目的	DHCP リレー機能のリレー対象の送信元サブネットを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**relay source** {*NETWORK-PREFIX PREFIX-MASK* | *NETWORK-ADDRESS/MASK-LENGTH*} **no relay source** {*NETWORK-PREFIX PREFIX-MASK* | *NETWORK-ADDRESS/MASK-LENGTH*}
パラメーター	*NETWORK-PREFIX PREFIX-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-ADDRESS/MASK-LENGTH*：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
コマンドモード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	リレー対象の送信元サブネットを設定する場合、装置に設定した IP アドレスのサブネットマスク（プレフィックス長）と一致するように設定してください。複数のサブネットをサマリー指定でまとめて設定することはできません。
制限事項	リレー対象の送信元サブネットは、1 つの DHCP リレープールにつき最大 4 個まで設定できます。 セカンダリーIP アドレスで指定したサブネットをリレー対象の送信元サブネットに設定しても、DHCP リレー機能は動作しません。
注意事項	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。
対象バージョン	1.08.01

使用例：DHCP リレープール「pool1」「pool2」を以下の内容で設定する方法を示します。

- pool1：DHCP リレー対象の送信元サブネットを 172.16.10.0/24、172.16.11.0/24 に、リレー先 DHCP サーバーの IP アドレスを 192.168.1.100 に設定
- pool2：DHCP リレー対象の送信元サブネットを 172.16.20.0/24、172.16.21.0/24 に、リレー先 DHCP サーバーの IP アドレスを 192.168.1.100 に設定

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# relay source 172.16.10.0/24
(config-dhcp-pool)# relay source 172.16.11.0/24
(config-dhcp-pool)# relay destination 192.168.1.100
(config-dhcp-pool)# exit
(config)# ip dhcp pool pool2
(config-dhcp-pool)# relay source 172.16.20.0/24
(config-dhcp-pool)# relay source 172.16.21.0/24
(config-dhcp-pool)# relay destination 192.168.1.100
(config-dhcp-pool)#
```

4.2.4 relay target

relay target	
目的	DHCP クラスで指定したオプションに一致した場合のリレー先 DHCP 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。
シンタックス	**relay target** *IP-ADDRESS* **no relay target** *IP-ADDRESS*
パラメーター	*IP-ADDRESS*：DHCP クラスのリレー先 DHCP サーバーの IP アドレスを指定します。
デフォルト	なし
コマンドモード	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	**class** コマンドと **relay target** コマンドを使用すると、DHCP クラスで指定したオプションに一致した場合のリレー先 DHCP サーバーを設定することができます。DHCP リレープールで DHCP クラスを使用する場合は、必ず **relay target** コマンドも設定してください。 リレー先 DHCP サーバーの IP アドレスを複数設定した場合、対象の DHCP パケットはすべてのリレー先にリレーされます。 DHCP クラスに一致しない場合、**relay destination** コマンドが設定されていれば、**relay destination** コマンドで指定した DHCP サーバーにリレーされます。
制限事項	**relay target** コマンドで設定するリレー先 DHCP サーバーの IP アドレスは、1 つの DHCP クラスにつき最大 4 個まで設定できます。
注意事項	-
対象バージョン	1.08.01

使用例：DHCP リレープール「pool1」を設定し、DHCP リレー対象の送信元サブネットを 172.16.10.0/24 に、DHCP クラス「Service-A」のリレー先 DHCP サーバーの IP アドレスを 192.168.1.100 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)# exit
(config)#
(config)# ip dhcp pool pool1
```

```
(config-dhcp-pool)# relay source 172.16.10.0/24
(config-dhcp-pool)# class Service-A
(config-dhcp-pool-class)# relay target 192.168.1.100
(config-dhcp-pool-class)#
```

4.2.5 ip dhcp relay unicast

ip dhcp relay unicast	
目的	DHCP クライアントユニキャストパケットを DHCP リレー機能で処理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。
シンタックス	**ip dhcp relay unicast** **no ip dhcp relay unicast**
パラメーター	なし
デフォルト	有効（DHCP クライアントユニキャストパケットは、DHCP リレー機能で処理される）
コマンドモード	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	本コマンドは、DHCP クライアントユニキャストパケットを DHCP リレー機能で処理するかどうかを決定します。無効にすると、DHCP リレー機能ではなく通常のレイヤー3 中継として処理されます。 ユニキャストには、DHCP クライアント用のすべての DHCP メッセージタイプ（DHCP Renew、Release、その他）が含まれます。 ネットワークの複数の装置で DHCP リレーが有効の場合は、DHCP ユニキャストパケットの処理方法は同一にしてください。 パケットの中継時、DHCP リレーは、装置の VRRP 役割がマスターとスレーブのどちらなのかはチェックしません。
制限事項	-
注意事項	-
対象バージョン	1.08.01

使用例：DHCP クライアントユニキャストパケットを、DHCP リレー機能で処理することを無効にする方法を示します。

```
# configure terminal
(config)# no ip dhcp relay unicast
(config)#
```

4.2.6 ip dhcp relay information check

ip dhcp relay information check	
目的	サーバーから応答された DHCP パケットの Relay Agent Information（Option 82）チェック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。
シンタックス	**ip dhcp relay information check** **no ip dhcp relay information check**
パラメーター	なし
デフォルト	Relay Agent Information（Option 82）のチェックは無効
コマンドモード	グローバル設定モード
特権レベル	レベル：12

ip dhcp relay information check	
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、サーバーから応答された DHCP パケットの Relay Agent Information（Option 82）はチェックされません。 本コマンドが有効の場合は、すべての VLAN インターフェースでチェックが有効になります。サーバーから応答された DHCP パケットの Relay Agent Information（Option 82）をチェックし、元の情報と内容が異なる場合は、その DHCP パケットを破棄します。 本コマンドが無効（デフォルト設定）でも、インターフェースごとの設定が有効（**ip dhcp relay information check-reply**）の場合は、対象 VLAN インターフェースでは有効になります。 本コマンドが有効でも、インターフェースごとの設定が無効（**ip dhcp relay information check-reply none**）の場合は、対象 VLAN インターフェースでは無効になります。
制限事項	-
注意事項	本コマンドの設定を確認する場合は、**show running-config function DHCP-RELAY** コマンドなどで構成情報を直接確認してください。
対象バージョン	1.08.01

使用例：Relay Agent Information（Option 82）チェックのグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# ip dhcp relay information check
(config)#
```

4.2.7 ip dhcp relay information check-reply

ip dhcp relay information check-reply	
目的	サーバーから応答された DHCP パケットの Relay Agent Information（Option 82）のチェックを、インターフェースごとに有効または無効にします。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**ip dhcp relay information check-reply [none]** **no ip dhcp relay information check-reply [none]**
パラメーター	**none**（省略可能）：サーバーから応答された DHCP パケットの Relay Agent Information（Option 82）のチェックを無効にする場合に指定します。
デフォルト	なし
コマンドモード	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の場合は、グローバル設定（**ip dhcp relay information check**）に従います。 本コマンドが有効設定（**ip dhcp relay information check-reply**）の VLAN インターフェースでは、グローバル設定にかかわらず有効になります。 本コマンドが無効設定（**ip dhcp relay information check-reply none**）の VLAN インターフェースでは、グローバル設定にかかわらず無効になります。
制限事項	設定を削除する場合は、**no ip dhcp relay information check-reply** コマンド、または **no ip dhcp relay information check-reply none** コマンドのどちらの形式で実行しても、本設定は削除されます。
注意事項	本コマンドの設定を確認する場合は、**show running-config function DHCP-**

ip dhcp relay information check-reply	
	RELAY コマンドなどで構成情報を直接確認してください。
対象バージョン	1.08.01

使用例：Relay Agent Information (Option 82) チェックのグローバル設定は無効に、VLAN 100 インターフェースでは有効にする方法を示します。

```
# configure terminal
(config)# no ip dhcp relay information check
(config)# interface vlan 100
(config-if-vlan)# ip dhcp relay information check-reply
```

4.2.8 ip dhcp relay information option

ip dhcp relay information option	
目的	クライアントからの DHCP パケットをリレーする際の、Relay Agent Information (Option 82) 挿入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。
シンタックス	**ip dhcp relay information option** **no ip dhcp relay information option**
パラメーター	なし
デフォルト	Relay Agent Information (Option 82) の挿入は無効
コマンドモード	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	本コマンドが無効（デフォルト設定）の場合は、リレーする際に Relay Agent Information (Option 82) は挿入されません。 本コマンドが有効の場合は、すべての VLAN インターフェースでリレーする際に Relay Agent Information (Option 82) が挿入されるようになります。 本コマンドが無効（デフォルト設定）でも、インターフェースごとの設定が有効（**ip dhcp relay information option-insert**）の場合は、対象 VLAN インターフェースでは有効になります。 本コマンドが有効でも、インターフェースごとの設定が無効（**ip dhcp relay information option-insert none**）の場合は、対象 VLAN インターフェースでは無効になります。
制限事項	-
注意事項	本コマンドの設定を確認する場合は、**show running-config function DHCP-RELAY** コマンドなどで構成情報を直接確認してください。
対象バージョン	1.08.01

使用例：Relay Agent Information (Option 82) 挿入のグローバル設定を有効にする方法を示します。

```
# configure terminal
(config)# ip dhcp relay information option
(config)#
```

4.2.9 ip dhcp relay information option-insert

ip dhcp relay information option-insert	
目的	クライアントからの DHCP パケットをリレーする際の、Relay Agent Information (Option 82) 挿入を、インターフェースごとに有効または無効にします。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 relay information option-insert	
シンタックス	ip dhcp relay information option-insert [none] no ip dhcp relay information option-insert [none]
パラメーター	none（省略可能）：クライアントからの DHCP パケットをリレーする際の、Relay Agent Information（Option 82）の挿入を無効にする場合に指定します。
デフォルト	なし
コマンドモード	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の場合は、グローバル設定（ip dhcp relay information option）に従います。 本コマンドが有効設定（ip dhcp relay information option-insert）の VLAN インターフェースでは、グローバル設定にかかわらず有効になります。 本コマンドが無効設定（ip dhcp relay information option-insert none）の VLAN インターフェースでは、グローバル設定にかかわらず無効になります。
制限事項	設定を削除する場合は、no ip dhcp relay information option-insert コマンド、または no ip dhcp relay information option-insert none コマンドのどちらの形式で実行しても、本設定は削除されます。
注意事項	-
対象バージョン	1.08.01

使用例：Relay Agent Information（Option 82）挿入のグローバル設定は有効に、VLAN 100 インターフェースでは無効にする方法を示します。

```
# configure terminal
(config)# ip dhcp relay information option
(config)# interface vlan 100
(config-if-vlan)# ip dhcp relay information option-insert none
(config-if-vlan)#
```

4.2.10 ip dhcp relay information policy

ip dhcp relay information policy	
目的	すでに Relay Agent Information（Option 82）が付与されたクライアントからの DHCP パケットを受信した場合の、リレー時の処理ポリシー（グローバル設定）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。
シンタックス	ip dhcp relay information policy {drop | keep | replace} no ip dhcp relay information policy
パラメーター	drop：対象の DHCP パケットを破棄する場合に指定します。 keep：対象の DHCP パケットの Relay Agent Information（Option 82）を変更せずに、そのままリレー処理する場合に指定します。 replace：対象の DHCP パケットの Relay Agent Information（Option 82）を、新しい内容に置き換えてリレー処理する場合に指定します。
デフォルト	replace
コマンドモード	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	本機能を使用する場合は、ip dhcp relay information option コマンド、または ip dhcp relay information option-insert コマンドを有効にする必要があります。

ip dhcp relay information policy	
	また、クライアントからの DHCP パケット（GIADDR フィールドが 0）に Relay Agent Information（Option 82）が付与されていても信頼するように、**ip dhcp relay information trust-all** コマンド、または **ip dhcp relay information trusted** コマンドを有効にする必要があります。 インターフェースごとの設定（**ip dhcp relay information policy-action**）が未設定の場合は、リレー時の処理ポリシーは本コマンドの設定で動作します。 インターフェースごとの設定（**ip dhcp relay information policy-action**）が設定されている VLAN インターフェースでは、その設定が優先されます。
制限事項	-
注意事項	本コマンドの設定を確認する場合は、**show running-config function DHCP-RELAY** コマンドなどで構成情報を直接確認してください。
対象バージョン	1.08.01

使用例：リレー時の処理ポリシー（グローバル設定）を **keep** に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp relay information policy keep
(config)#
```

4.2.11 ip dhcp relay information policy-action

ip dhcp relay information policy-action	
目的	すでに Relay Agent Information（Option 82）が付与されたクライアントからの DHCP パケットを受信した場合の、リレー時の処理ポリシー（インターフェースごと設定）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。
シンタックス	**ip dhcp relay information policy-action {drop | keep | replace}** **no ip dhcp relay information policy-action**
パラメーター	**drop**：対象の DHCP パケットを破棄する場合に指定します。 **keep**：対象の DHCP パケットの Relay Agent Information（Option 82）を変更せずに、そのままリレー処理する場合に指定します。 **replace**：対象の DHCP パケットの Relay Agent Information（Option 82）を、新しい内容に置き換えてリレー処理する場合に指定します。
デフォルト	なし
コマンドモード	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	本機能を使用する場合は、**ip dhcp relay information option** コマンド、または **ip dhcp relay information option-insert** コマンドを有効にする必要があります。 また、クライアントからの DHCP パケット（GIADDR フィールドが 0）に Relay Agent Information（Option 82）が付与されていても信頼するように、**ip dhcp relay information trust-all** コマンド、または **ip dhcp relay information trusted** コマンドを有効にする必要があります。 本コマンドが未設定の場合は、リレー時の処理ポリシーはグローバル設定（**ip dhcp relay information trust-all**）に従います。 本コマンドが設定されている VLAN インターフェースでは、グローバル設定にか

ip dhcp relay information policy-action	
	かわらず本コマンドの設定で動作します。
制限事項	-
注意事項	VLAN インターフェース設定専用のコマンドです。
対象バージョン	1.08.01

使用例：リレー時の処理ポリシー（グローバル設定）を keep に設定し、VLAN 100 インターフェースでは drop に設定する方法を示します。

```
# configure terminal
(config)# ip dhcp relay information policy keep
(config)# interface vlan 100
(config-if-vlan)# ip dhcp relay information policy-action drop
(config-if-vlan)#
```

4.2.12 ip dhcp relay information trust-all

ip dhcp relay information trust-all	
目的	Relay Agent Information（Option 82）が付与されたクライアントからの DHCP パケットを信頼する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。
シンタックス	**ip dhcp relay information trust-all** **no ip dhcp relay information trust-all**
パラメーター	なし
デフォルト	無効（すべての VLAN インターフェースで信頼しない）
コマンドモード	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	本コマンドが無効（デフォルト設定）の場合は、クライアントからの DHCP パケット（GIADDR フィールドが 0）に Relay Agent Information（Option 82）が付与されていると、その DHCP パケットは信頼されず破棄されます。 本コマンドが有効の場合は、すべての VLAN インターフェースで信頼してリレーするようになります。 本コマンドが無効（デフォルト設定）でも、インターフェースごとの設定が有効（**ip dhcp relay information trusted**）の場合は、対象 VLAN インターフェースでは有効になります。
制限事項	-
注意事項	-
対象バージョン	1.08.01

使用例：Relay Agent Information（Option 82）が付与されたクライアントからの DHCP パケットを信頼する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)# ip dhcp relay information trust-all
(config)#
```

4.2.13 ip dhcp relay information trusted

ip dhcp relay information trusted	
目的	Relay Agent Information（Option 82）が付与されたクライアントからの DHCP パケットを信頼する設定を、インターフェースごとに有効にします。設定を削除

ip dhcp relay information trusted	
	する場合は、no 形式のコマンドを使用します。
シンタックス	ip dhcp relay information trusted no ip dhcp relay information trusted
パラメーター	なし
デフォルト	なし
コマンドモード	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の場合は、グローバル設定（ip dhcp relay information trust-all）に従います。 本コマンドが有効設定（ip dhcp relay information trusted）の VLAN インターフェースでは、グローバル設定にかかわらず信頼してリレーするようになります。
制限事項	-
注意事項	-
対象バージョン	1.08.01

使用例：Relay Agent Information（Option 82）が付与されたクライアントからの DHCP パケットを信頼する機能のグローバル設定は無効に、VLAN 100 インターフェースでは有効にする方法を示します。

```
# configure terminal
(config)# no ip dhcp relay information trust-all
(config)# interface vlan 100
(config-if-vlan)# ip dhcp relay information trusted
(config-if-vlan)#
```

4.2.14 service dhcp (DHCP Relay)

service dhcp (DHCP Relay)	
目的	DHCP サーバー機能、または DHCP リレ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。
シンタックス	service dhcp no service dhcp
パラメーター	なし
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	DHCP リレー機能のみ使用する場合でも本設定が必要です。
対象バージョン	1.08.01

使用例：DHCP サーバー機能、または DHCP リレー機能を有効にする方法を示します。

```
# configure terminal
(config)# service dhcp
(config)#
```

4.2.15 show ip dhcp relay information trusted-sources

show ip dhcp relay information trusted-sources	
目的	Relay Agent Information (Option 82) が付与されたクライアントからの DHCP パケットを信頼するインターフェースを表示します。
シンタックス	show ip dhcp relay information trusted-sources
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.08.01

使用例：Relay Agent Information (Option 82) が付与されたクライアントからの DHCP パケットを信頼するインターフェースを表示する方法を示します。

```
# show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
vlan100     vlan200     vlan300     vlan400     vlan500     vlan600
vlan700     vlan800

Total Entries: 8
```

使用例：すべてのインターフェースが信頼するインターフェースの場合は、以下のように表示されます。

```
# show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option
```

4.2.16 show ip dhcp relay information option-insert

show ip dhcp relay information option-insert	
目的	クライアントからの DHCP パケットをリレーする際の、Relay Agent Information (Option 82) の挿入設定を表示します。
シンタックス	show ip dhcp relay information option-insert
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.08.01

使用例：クライアントからの DHCP パケットをリレーする際の、Relay Agent Information (Option 82) の挿入設定を表示する方法を示します。

```
# show ip dhcp relay information option-insert
```

```
 (1)            (2)
Interface     Option-Insert
------------- ---------
vlan1         Enabled
vlan2         Disabled
vlan3         Not Configured

Total Entries: 3
```

項番	説明
(1)	インターフェース名を表示します。
(2)	Relay Agent Information (Option 82) の挿入設定を表示します。 Enabled：有効 Disabled：無効 Not Configured：未設定

4.2.17 show ip dhcp relay information policy-action

show ip dhcp relay information policy-action	
目的	すでに Relay Agent Information (Option 82) が付与されたクライアントからの DHCP パケットを受信した場合の、リレー時の処理ポリシーを表示します。
シンタックス	**show ip dhcp relay information policy-action**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.08.01

使用例：すでに Relay Agent Information (Option 82) が付与されたクライアントからの DHCP パケットを受信した場合の、リレー時の処理ポリシーを表示する方法を示します。

```
# show ip dhcp relay information policy-action
 (1)            (2)
Interface     Policy
------------- ---------
vlan1         Keep
vlan2         Drop
vlan3         Replace
vlan4         Not configured

Total Entries: 4
```

項番	説明
(1)	インターフェース名を表示します。
(2)	すでに Relay Agent Information (Option 82) が付与されたクライアントからの DHCP パケットを受信した場合の、リレー時の処理ポリシーを表示します。 Drop：対象の DHCP パケットを破棄 Keep：対象の DHCP パケットをそのままリレー処理 Replace：Relay Agent Information (Option 82) を置き換えてリレー処理

項番	説明
	Not configured：未設定

4.3 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。

コマンド	コマンドとパラメーター
ip dhcp pool (DHCP Server)	ip dhcp pool POOL-NAME no ip dhcp pool POOL-NAME
network	network {NETWORK-ADDRESS MASK | NETWORK-ADDRESS/PREFIX-LENGTH} no network
class (DHCP Relay & Server)	class CLASS-NAME no class CLASS-NAME
address range	address range START-IP-ADDRESS END-IP-ADDRESS no address range START-IP-ADDRESS END-IP-ADDRESS
host	host {IP-ADDRESS MASK | IP-ADDRESS/PREFIX-LENGTH} no host
hardware-address	hardware-address MAC-ADDRESS no hardware-address
client-identifier	client-identifier IDENTIFIER no client-identifier
lease	lease {DAYS [HOURS [MINUTES [SECONDS]]] | infinite} no lease
default-router	default-router IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8] no default-router IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]
domain-name (DHCP Server)	domain-name NAME no domain-name
dns-server (DHCP Server)	dns-server IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8] no dns-server IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]
netbios-node-type	netbios-node-type {b-node | h-node | m-node | p-node} no netbios-node-type
netbios-name-server	netbios-name-server IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8] no netbios-name-server IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]
next-server	next-server IP-ADDRESS no next-server
bootfile	bootfile URL no bootfile
option	option CODE {ascii STRING | hex {HEX-STRING | none} | ip IP-ADDRESS [IP-ADDRESS2...IP-ADDRESS8]} no option CODE
ip dhcp class (DHCP Relay & Server)	ip dhcp class CLASS-NAME no ip dhcp class CLASS-NAME
option hex (DHCP Relay & Server)	option CODE hex PATTERN [*] [bitmask MASK] no option CODE hex PATTERN [*] [bitmask MASK]

コマンド	コマンドとパラメーター
ip dhcp use class	ip dhcp use class no ip dhcp use class
ip dhcp excluded-address	ip dhcp excluded-address START-IP-ADDRESS END-IP-ADDRESS no ip dhcp excluded-address START-IP-ADDRESS END-IP-ADDRESS
ip dhcp ping packets	ip dhcp ping packets COUNT no ip dhcp ping packets
ip dhcp ping timeout	ip dhcp ping timeout MILLI-SECONDS no ip dhcp ping timeout
service dhcp (DHCP Server)	service dhcp no 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。

コマンド	コマンドとパラメーター
show ip dhcp binding	show ip dhcp binding [IP-ADDRESS]
show ip dhcp conflict	show ip dhcp conflict [IP-ADDRESS]
show ip dhcp pool	show ip dhcp pool [POOL-NAME]
show ip dhcp server	show ip dhcp server
show ip dhcp server statistics	show ip dhcp server statistics
clear ip dhcp binding	clear ip dhcp {all | pool POOL-NAME} binding {* | IP-ADDRESS}
clear ip dhcp conflict	clear ip dhcp {all | pool POOL-NAME} conflict {* | IP-ADDRESS}
clear ip dhcp server statistics	clear ip dhcp server statistics

4.3.1 ip dhcp pool (DHCP Server)

ip dhcp pool (DHCP Server)	
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。
シンタックス	**ip dhcp pool** *POOL-NAME* **no ip dhcp pool** *POOL-NAME*
パラメーター	*POOL-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
コマンドモード	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	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

ip dhcp pool (DHCP Server)	
	は hardware-address コマンドと host コマンドを実行してください。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.2 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。
シンタックス	network {*NETWORK-ADDRESS MASK* | *NETWORK-ADDRESS/PREFIX-LENGTH*} no network
パラメーター	*NETWORK-ADDRESS 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-ADDRESS/PREFIX-LENGTH*：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
コマンドモード	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

network	
	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.3 class (DHCP Relay & Server)

class (DHCP Relay & Server)	
目的	DHCP アドレスプール、または DHCP リレープールで使用する 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。
シンタックス	**class** *CLASS-NAME* **no class** *CLASS-NAME*
パラメーター	*CLASS-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
コマンドモード	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。

class (DHCP Relay & Server)	
	DHCP リレー機能の DHCP リレープールで使用する場合は、**relay target** コマンドで DHCP クラスに関連付けるリレー先 DHCP サーバーの IP アドレスを設定します。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リレー先にリレーされます。
制限事項	DHCP クラスは最大 10 個設定できます。
注意事項	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。
対象バージョン	1.01.01

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)#
```

使用例：DHCP リレープール「Relay-pool」で使用する DHCP クラスとして「Relay-class」を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp class Relay-class
(config-dhcp-class)# exit
(config)#
(config)# ip dhcp pool Relay-pool
(config-dhcp-pool)# relay source 192.168.20.0/24
(config-dhcp-pool)# class Relay-class
(config-dhcp-pool-class)#
```

4.3.4 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。
シンタックス	**address range** *START-IP-ADDRESS END-IP-ADDRESS* **no address range** *START-IP-ADDRESS END-IP-ADDRESS*
パラメーター	*START-IP-ADDRESS*：IP アドレス範囲の最初の IP アドレスを指定します。 *END-IP-ADDRESS*：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
コマンドモード	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。 **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。

address range	
	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。
制限事項	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。 **address range** 設定を削除する場合は、一部の範囲だけを削除することはできません。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.5 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 アドレスを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**host** {*IP-ADDRESS MASK* | *IP-ADDRESS/PREFIX-LENGTH*} **no host**
パラメーター	*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/PREFIX-LENGTH*：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
コマンドモード	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。
制限事項	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。
注意事項	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。 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。

host	
対象バージョン	1.01.01

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)#
```

4.3.6 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 アドレスを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**hardware-address** *MAC-ADDRESS* **no hardware-address**
パラメーター	*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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式）
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.7 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 を指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	client-identifier *IDENTIFIER* no client-identifier
パラメーター	*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
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.8 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。
シンタックス	lease {*DAYS* [*HOURS* [*MINUTES* [*SECONDS*]]] | infinite} no lease
パラメーター	*DAYS* [*HOURS* [*MINUTES* [*SECONDS*]]]：IP アドレスのリース期間を設定します。 • *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。

lease	
	• *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
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01 1.01.03：*SECONDS* パラメーター追加

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
```

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
```

4.3.9 default-router

default-router	
目的	DHCP クライアントのデフォルトルーターを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**default-router** *IP-ADDRESS* [*IP-ADDRESS2... IP-ADDRESS8*] **no default-router** *IP-ADDRESS* [*IP-ADDRESS2... IP-ADDRESS8*]
パラメーター	*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
コマンドモード	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、デフォルトインターフェースリストに追加されます。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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
```

4.3.10 domain-name (DHCP Server)

domain-name (DHCP Server)	
目的	DHCP クライアントのドメイン名を指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**domain-name** *NAME* **no domain-name**
パラメーター	*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
コマンドモード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	指定できるドメイン名は 1 つだけです。
注意事項	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。
対象バージョン	1.01.01

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
```

4.3.11 dns-server (DHCP Server)

dns-server (DHCP Server)	
目的	DHCP クライアントの DNS サーバーを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**dns-server** *IP-ADDRESS* [*IP-ADDRESS2... IP-ADDRESS8*] **no dns-server** *IP-ADDRESS* [*IP-ADDRESS2... IP-ADDRESS8*]
パラメーター	*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
コマンドモード	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。

dns-server (DHCP Server)	
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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
```

4.3.12 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。
シンタックス	**netbios-node-type {b-node | h-node | m-node | p-node}** **no netbios-node-type**
パラメーター	**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
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.13 netbios-name-server

netbios-name-server	
目的	Microsoft DHCP クライアントに WINS サーバーを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**netbios-name-server** *IP-ADDRESS* [*IP-ADDRESS2...IP-ADDRESS8*] **no netbios-name-server** *IP-ADDRESS* [*IP-ADDRESS2...IP-ADDRESS8*]
パラメーター	*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
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.14 next-server

next-server	
目的	DHCP クライアントのブートサーバーを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**next-server** *IP-ADDRESS* **no next-server**
パラメーター	*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
コマンドモード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	指定できるブートサーバーは 1 つだけです。
注意事項	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。

next-server	
対象バージョン	1.01.01

使用例：pool1 という名前のプールで、DHCP クライアントのブートプロセス内の、次のサーバーの IP アドレスとして、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
```

4.3.15 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指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**bootfile** *URL* **no bootfile**
パラメーター	*URL*：ブートイメージファイルの URL を、最大 64 文字で指定します。
デフォルト	なし
コマンドモード	DHCP プール設定モード
特権レベル	レベル：12
ガイドライン	**next-server** コマンドで、ブートイメージファイルがあるサーバーの場所を指定します。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：DHCP プール 1 のブートイメージファイルの名前として「dhcpbootfile.bin」を指定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# bootfile \bootimage\dhcpbootfile.bin
(config-dhcp-pool)#
```

4.3.16 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。
シンタックス	**option** *CODE* {**ascii** *STRING* | **hex** {*HEX-STRING* | **none**} | **ip** *IP-ADDRESS* [*IP-ADDRESS2*...*IP-ADDRESS8*]} **no option** *CODE*
パラメーター	*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。

option	
	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
コマンドモード	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） 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）
制限事項	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。
注意事項	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。

option	
対象バージョン	1.01.01

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)#
```

4.3.17 ip dhcp class (DHCP Relay & Server)

ip dhcp class (DHCP Relay & Server)	
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。
シンタックス	**ip dhcp class** *CLASS-NAME* **no ip dhcp class** *CLASS-NAME*
パラメーター	*CLASS-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
コマンドモード	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	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。
制限事項	DHCP クラスは最大 10 個設定できます。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.18 option hex (DHCP Relay & Server)

option hex (DHCP Relay & Server)	
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。
シンタックス	**option** *CODE* **hex** *PATTERN* [*****] [**bitmask** *MASK*] **no option** *CODE* **hex** *PATTERN* [*****] [**bitmask** *MASK*]
パラメーター	*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
コマンドモード	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。 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)
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.19 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。
シンタックス	ip dhcp use class no ip dhcp use class
パラメーター	なし
デフォルト	無効
コマンドモード	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	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 IP アドレスの範囲を設定します。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。 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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.20 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。
シンタックス	**ip dhcp excluded-address** *START-IP-ADDRESS END-IP-ADDRESS* **no ip dhcp excluded-address** *START-IP-ADDRESS END-IP-ADDRESS*
パラメーター	*START-IP-ADDRESS*：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-ADDRESS*：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
コマンドモード	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	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。
制限事項	除外対象の IP アドレスの範囲は最大 5 個設定できます。
注意事項	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。
対象バージョン	1.01.01

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
```

4.3.21 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。
シンタックス	**ip dhcp ping packets** *COUNT* **no ip dhcp ping packets**
パラメーター	*COUNT*：ping パケットの数を 0～10 の範囲で指定します。
デフォルト	2
コマンドモード	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	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。 送信する ping パケットの数を 0 に設定すると、ping による事前確認は無効にな

ip dhcp ping packets	
	ります。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.22 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。
シンタックス	**ip dhcp ping timeout** *MILLI-SECONDS* **no ip dhcp ping timeout**
パラメーター	*MILLI-SECONDS*：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）
コマンドモード	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	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.3.23 service dhcp (DHCP Server)

service dhcp (DHCP Server)	
目的	DHCP サーバー機能、または DHCP リレ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。
シンタックス	**service dhcp**

service dhcp (DHCP Server)	
	no service dhcp
パラメーター	なし
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	DHCP サーバーが有効状態で DHCP サーバー関連の設定を変更しても即反映されないため、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。
対象バージョン	1.01.01

使用例：DHCP サーバー機能、または DHCP リレー機能を有効にする方法を示します。

```
# configure terminal
(config)# service dhcp
(config)#
```

4.3.24 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。
シンタックス	**show ip dhcp binding** [*IP-ADDRESS*]
パラメーター	*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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

項番	説明
(4)	IP アドレスの割り当て方法を表示します。 Automatic：自動割り当て Manual：固定割り当て

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を表示します。 Automatic：自動割り当て Manual：固定割り当て

4.3.25 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。
シンタックス	**show ip dhcp conflict** [*IP-ADDRESS*]
パラメーター	*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。
デフォルト	なし
コマンドモード	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、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。
制限事項	–
注意事項	–
対象バージョン	1.01.01

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 クライアントが送信する 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。

4.3.26 show ip dhcp pool

show ip dhcp pool	
目的	DHCP アドレスプールに関する設定情報を表示します。
シンタックス	**show ip dhcp pool** [*POOL-NAME*]
パラメーター	*POOL-NAME*（省略可能）：表示する DHCP アドレスプールを指定します。
デフォルト	なし
コマンドモード	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情報が表示されます。
制限事項	-
注意事項	本コマンドでは DHCP リレープールも表示されますが、リレー対象の送信元サブネットやリレー先 DHCP サーバーの IP アドレスは表示されません。DHCP リレープールの設定を確認する場合は、**show running-config function DHCP-RELAY** コマンドなどで構成情報を直接確認してください。
対象バージョン	1.01.01

使用例：すべての DHCP アドレスプールの設定情報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。

項番	説明
(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。

4.3.27 show ip dhcp server

show ip dhcp server	
目的	DHCP サーバーの設定情報を表示します。
シンタックス	**show ip dhcp server**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：DHCP サーバーの設定情報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 サーバーまたは DHCP リレーの有効／無効を表示します。
(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、DHCP リレーのための DHCP リレープール）を表示します。

4.3.28 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。
シンタックス	show ip dhcp server statistics
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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、DHCP リレーのための DHCP リレープール）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。
(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。

4.3.29 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

clear ip dhcp binding	
	ます。
シンタックス	clear ip dhcp {all | pool *POOL-NAME*} binding {* | *IP-ADDRESS*}
パラメーター	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 *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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

4.3.30 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。
シンタックス	clear ip dhcp {all | pool *POOL-NAME*} conflict {* | *IP-ADDRESS*}
パラメーター	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 *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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

4.3.31 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。

clear ip dhcp server statistics	
シンタックス	clear ip dhcp server statistics
パラメーター	なし
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

4.4 DHCPv6 クライアントコマンド

DHCPv6 クライアント関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ipv6 dhcp client pd	ipv6 dhcp client pd {PREFIX-NAME [rapid-commit] | hint IPV6-PREFIX} no ipv6 dhcp client pd
show ipv6 dhcp	show ipv6 dhcp
show ipv6 dhcp interface	show ipv6 dhcp interface [INTERFACE-NAME]
clear ipv6 dhcp client	clear ipv6 dhcp client INTERFACE-NAME

4.4.1 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。
シンタックス	**ipv6 dhcp client pd** {*PREFIX-NAME* [**rapid-commit**] | **hint** *IPV6-PREFIX*} **no ipv6 dhcp client pd**
パラメーター	*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）：プレフィックスを委譲する際のメッセージ交換の個数を 4 個から 2 個に減らすことを許可する場合に指定します。 **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
コマンドモード	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。 **rapid-commit** パラメーターを指定した場合、プレフィックス委譲のための 2 つのメッセージ交換の要求メッセージに Rapid Commit オプションが書き込まれます。 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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 インターフェースで、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。関連付けるプレフィックス名は「test-prefix」とします。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 dhcp client pd test-prefix
(config-if-vlan)#
```

4.4.2 show ipv6 dhcp

show ipv6 dhcp	
目的	自装置の DUID（DHCP Unique Identifier）を表示します。
シンタックス	**show ipv6 dhcp**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 00030006004066040608 ...(1)
```

項番	説明
(1)	DUID（DHCP Unique Identifier）を表示します。

4.4.3 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。
シンタックス	**show ipv6 dhcp interface** [*INTERFACE-NAME*]
パラメーター	*INTERFACE-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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 インターフェースが、DHCPv6 サーバーとして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 関連の設定情報を表示します。 〈*INTERFACE-NAME*〉 is not in DHCPv6 mode：DHCPv6 関連の設定が未設定 〈*INTERFACE-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を表示します。 allowed：ヒントを利用する ignored：ヒントを無視する
(5)	メッセージ交換の個数を 4 個から 2 個に減らすことを許可する機能の有効／無効を表示します。

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 関連の設定情報を表示します。 〈*INTERFACE-NAME*〉 is not in DHCPv6 mode：DHCPv6 関連の設定が未設定 〈*INTERFACE-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。

項番	説明
(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。
(7)	IPv6 アドレスプレフィックス名を表示します。
(8)	メッセージ交換の個数を 4 個から 2 個に減らすことを許可する機能の有効／無効を表示します。
(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。

4.4.4 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。
シンタックス	**clear ipv6 dhcp client** *INTERFACE-NAME*
パラメーター	*INTERFACE-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。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

4.5 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。

コマンド	コマンドとパラメーター
ipv6 dhcp pool	ipv6 dhcp pool POOL-NAME no ipv6 dhcp pool POOL-NAME
address prefix	address prefix IPV6-PREFIX/PREFIX-LENGTH [lifetime VALID-LIFETIME PREFERRED-LIFETIME] no address prefix
address-assignment	address-assignment IPV6-ADDRESS CLIENT-DUID [iaid IAID] [lifetime VALID-LIFETIME PREFERRED-LIFETIME] no address-assignment IPV6-ADDRESS CLIENT-DUID [iaid IAID]
domain-name (DHCPv6 Server)	domain-name DOMAIN-NAME no domain-name
dns-server (DHCPv6 Server)	dns-server IPV6-ADDRESS no dns-server IPV6-ADDRESS
prefix-delegation pool	prefix-delegation pool LOCAL-POOL-NAME [lifetime VALID-LIFETIME PREFERRED-LIFETIME] no prefix-delegation pool LOCAL-POOL-NAME
prefix-delegation	prefix-delegation IPV6-PREFIX/PREFIX-LENGTH CLIENT-DUID [iaid IAID] [lifetime VALID-LIFETIME PREFERRED-LIFETIME] no prefix-delegation IPV6-PREFIX/PREFIX-LENGTH CLIENT-DUID [iaid IAID]
ipv6 dhcp excluded-address	ipv6 dhcp excluded-address LOW-ADDRESS [HIGH-ADDRESS] no ipv6 dhcp excluded-address LOW-ADDRESS [HIGH-ADDRESS]
ipv6 local pool	ipv6 local pool LOCAL-POOL-NAME IPV6-PREFIX/PREFIX-LENGTH ASSIGNED-LENGTH no ipv6 local pool LOCAL-POOL-NAME
ipv6 dhcp server	ipv6 dhcp server POOL-NAME [rapid-commit] [preference VALUE] [allow-hint] no ipv6 dhcp server
service ipv6 dhcp	service ipv6 dhcp no 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。

コマンド	コマンドとパラメーター
show ipv6 dhcp binding	show ipv6 dhcp binding [IPV6-ADDRESS]
show ipv6 dhcp pool	show ipv6 dhcp pool [POOL-NAME]
show ipv6 excluded-address	show ipv6 excluded-address
show ipv6 local pool	show ipv6 local pool [LOCAL-POOL-NAME]
show ipv6 dhcp operation	show ipv6 dhcp operation

コマンド	コマンドとパラメーター
clear ipv6 dhcp binding	clear ipv6 dhcp binding {all | IPV6-ADDRESS}

4.5.1 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。
シンタックス	**ipv6 dhcp pool** *POOL-NAME* **no ipv6 dhcp pool** *POOL-NAME*
パラメーター	*POOL-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
コマンドモード	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	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.5.2 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。
シンタックス	**address prefix** *IPV6-PREFIX/PREFIX-LENGTH* [**lifetime** *VALID-LIFETIME PREFERRED-LIFETIME*] **no address prefix**
パラメーター	*IPV6-PREFIX/PREFIX-LENGTH*：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-LIFETIME PREFERRED-LIFETIME*（省略可能）：VALID-LIFETIME（有効期間）と PREFERRED-LIFETIME（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-LIFETIME（有効期間）未指定時：2,592,000 秒（30 日）

address prefix	
	PREFERRED-LIFETIME（推奨期間）未指定時：604,800 秒（7 日）
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.5.3 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。
シンタックス	**address-assignment** *IPV6-ADDRESS CLIENT-DUID* [**iaid** *IAID*] [**lifetime** *VALID-LIFETIME PREFERRED-LIFETIME*] **no address-assignment** *IPV6-ADDRESS CLIENT-DUID* [**iaid** *IAID*]
パラメーター	*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。 *CLIENT-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-LIFETIME PREFERRED-LIFETIME*（省略可能）：VALID-LIFETIME（有効期間）と PREFERRED-LIFETIME（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-LIFETIME（有効期間）未指定時：2,592,000 秒（30 日）

address-assignment	
	PREFERRED-LIFETIME（推奨期間）未指定時：604,800 秒（7 日）
コマンドモード	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）。
制限事項	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。
注意事項	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。 コマンドシンタックスのパラメーター指定は順不同ではありません。パラメーターの指定は、シンタックス欄の記載順に指定してください。パラメーター省略時は、省略したパラメーター以降が指定できます。
対象バージョン	1.01.01

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)#
```

4.5.4 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。
シンタックス	**domain-name** *DOMAIN-NAME* **no domain-name**
パラメーター	*DOMAIN-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
コマンドモード	DHCPv6 プール設定モード

domain-name (DHCPv6 Server)	
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。
制限事項	ドメイン名は 1 つだけ設定できます。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.5.5 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。
シンタックス	**dns-server** *IPV6-ADDRESS* **no dns-server** *IPV6-ADDRESS*
パラメーター	*IPV6-ADDRESS*：DNS サーバーの IPv6 アドレスを指定します。
デフォルト	なし
コマンドモード	DHCPv6 プール設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	DNS サーバーは最大 2 個設定できます。
注意事項	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。
対象バージョン	1.01.01

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 2001:0db8:3000:3000::42
(config-dhcp)#
```

4.5.6 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。
シンタックス	**prefix-delegation pool** *LOCAL-POOL-NAME* [**lifetime** *VALID-LIFETIME PREFERRED-LIFETIME*]

prefix-delegation pool	
	no prefix-delegation pool *LOCAL-POOL-NAME*
パラメーター	*LOCAL-POOL-NAME*：ローカル IPv6 プレフィックスプール名を指定します。 **lifetime** *VALID-LIFETIME PREFERRED-LIFETIME*（省略可能）：VALID-LIFETIME（有効期間）と PREFERRED-LIFETIME（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-LIFETIME（有効期間）未指定時：2,592,000 秒（30 日） PREFERRED-LIFETIME（推奨期間）未指定時：604,800 秒（7 日）
コマンドモード	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。
制限事項	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** 設定も削除されます。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.5.7 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。
シンタックス	**prefix-delegation** *IPV6-PREFIX/PREFIX-LENGTH CLIENT-DUID* [**iaid** *IAID*] [**lifetime** *VALID-LIFETIME PREFERRED-LIFETIME*] **no prefix-delegation** *IPV6-PREFIX/PREFIX-LENGTH CLIENT-DUID* [**iaid** *IAID*]
パラメーター	*IPV6-PREFIX/PREFIX-LENGTH*：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。 *CLIENT-DUID*：DHCPv6 クライアントの DUID（DHCP Unique Identifier）を指定します。

prefix-delegation	
	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-LIFETIME PREFERRED-LIFETIME*（省略可能）：VALID-LIFETIME（有効期間）と PREFERRED-LIFETIME（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-LIFETIME（有効期間）未指定時：2,592,000 秒（30 日） PREFERRED-LIFETIME（推奨期間）未指定時：604,800 秒（7 日）
コマンドモード	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 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）。
制限事項	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。
注意事項	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。 コマンドシンタックスのパラメーター指定は順不同ではありません。パラメーターの指定は、シンタックス欄の記載順に指定してください。パラメーター省略時は、省略したパラメーター以降が指定できます。
対象バージョン	1.01.01

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)#
```

4.5.8 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

ipv6 dhcp excluded-address	
	形式のコマンドを使用します。
シンタックス	**ipv6 dhcp excluded-address** *LOW-ADDRESS* [*HIGH-ADDRESS*] **no ipv6 dhcp excluded-address** *LOW-ADDRESS* [*HIGH-ADDRESS*]
パラメーター	*LOW-ADDRESS*：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。 *HIGH-ADDRESS*（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
コマンドモード	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	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.5.9 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。
シンタックス	**ipv6 local pool** *LOCAL-POOL-NAME IPV6-PREFIX/PREFIX-LENGTH ASSIGNED-LENGTH* **no ipv6 local pool** *LOCAL-POOL-NAME*
パラメーター	*LOCAL-POOL-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/PREFIX-LENGTH*：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

ipv6 local pool	
コマンドモード	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	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.5.10 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。
シンタックス	**ipv6 dhcp server** *POOL-NAME* [**rapid-commit**] [**preference** *VALUE*] [**allow-hint**] **no ipv6 dhcp server**
パラメーター	*POOL-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）：メッセージ交換の個数を 4 個から 2 個に減らすことを許可する場合に指定します。デフォルトでは、2 個のメッセージ交換は許可されていません。 **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
コマンドモード	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。 コマンド実行時に **rapid-commit** パラメーターを指定して、クライアントが要求メッセージに Rapid Commit オプションを含めている場合、プレフィックス委譲やその他の構成で、サーバーは 2 つのメッセージ交換を使用します。

ipv6 dhcp server	
	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.5.11 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。
シンタックス	**service ipv6 dhcp** **no service ipv6 dhcp**
パラメーター	なし
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.5.12 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。

show ipv6 dhcp binding	
シンタックス	**show ipv6 dhcp binding** [*IPV6-ADDRESS*]
パラメーター	*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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 ...(6)
```

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。
(6)	アドレスバインディングエントリーの総数を表示します。

4.5.13 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情報を表示します。
シンタックス	**show ipv6 dhcp pool** [*POOL-NAME*]
パラメーター	*POOL-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。
デフォルト	なし
コマンドモード	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情報が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
(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。

4.5.14 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。
シンタックス	**show ipv6 excluded-address**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 ...(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。
(2)	リースする範囲から除外する IPv6 アドレス設定の総数を表示します。

4.5.15 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。
シンタックス	**show ipv6 local pool** [*LOCAL-POOL-NAME*]
パラメーター	*LOCAL-POOL-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

show ipv6 local pool	
	指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 ...(5)
```

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。
(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。
(5)	ローカル IPv6 プレフィックスプール設定の総数を表示します。

4.5.16 show ipv6 dhcp operation

show ipv6 dhcp operation	
目的	DHCPv6 サーバーの設定を表示します。
シンタックス	**show ipv6 dhcp operation**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

4.5.17 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。
シンタックス	**clear ipv6 dhcp binding** {**all** | *IPV6-ADDRESS*}
パラメーター	**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。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

4.6 DHCP Auto Configuration コマンド

DHCP Auto Configuration 関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
autoconfig enable	autoconfig enable no autoconfig enable
show autoconfig	show autoconfig

4.6.1 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。
シンタックス	autoconfig enable no autoconfig enable
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.6.2 show autoconfig

show autoconfig	
目的	DHCP Auto Configuration の設定を表示します。
シンタックス	show autoconfig
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：DHCP Auto Configuration の設定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 の利用設定を表示します。 Enabled：有効 Disabled：無効

4.7 時刻および SNTP コマンド

時刻および SNTP (Simple Network Time Protocol) 関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
clock set	clock set HH:MM:SS DAY MONTH YEAR
clock summer-time	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
clock timezone	clock timezone {+ | -} HOURS-OFFSET [MINUTES-OFFSET] no clock timezone
sntp server	sntp server {IP-ADDRESS | IPV6-ADDRESS} no sntp server {IP-ADDRESS | IPV6-ADDRESS}
sntp interval	sntp interval SECONDS no sntp interval
sntp enable	sntp enable no sntp enable
show clock	show clock
show sntp	show sntp

4.7.1 clock set

clock set	
目的	システムの時刻を手動で設定します。
シンタックス	**clock set** *HH:MM:SS DAY MONTH YEAR*
パラメーター	*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
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	システムが NTP/SNTP を利用して外部の信頼できる情報源と時刻同期している場合は、本コマンドを使用する必要はありません。本コマンドは、NTP/SNTP による時刻同期が利用できない場合に使用してください。 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。

clock set	
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

4.7.2 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。
シンタックス	**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**
パラメーター	**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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.7.3 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。
シンタックス	**clock timezone** {+ ｜ -} *HOURS-OFFSET* [*MINUTES-OFFSET*] **no clock timezone**
パラメーター	+ : 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 +09:00
コマンドモード	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	時刻は、UTC 時間、タイムゾーン、およびサマータイム設定に基づいて算出されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：UTC からのオフセットが-8:00 の太平洋標準時(PST)にタイムゾーンを設定する方法を示します。

```
# configure terminal
(config)# clock timezone - 8
(config)#
```

4.7.4 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。
シンタックス	**sntp server** {*IP-ADDRESS* ｜ *IPV6-ADDRESS*} **no sntp server** {*IP-ADDRESS* ｜ *IPV6-ADDRESS*}
パラメーター	*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
コマンドモード	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	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）

sntp server	
	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.7.5 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。
シンタックス	**sntp interval** *SECONDS* **no sntp interval**
パラメーター	*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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.7.6 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。
シンタックス	**sntp enable** **no sntp enable**
パラメーター	なし
デフォルト	無効

sntp enable	
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.7.7 show clock

show clock	
目的	日時情報を表示します。
シンタックス	**show clock**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 を有効にして、時刻が同期されている場合 NTP(Synchronized)：NTP サービスを有効にして時刻が同期されている場合 NTP(Unsynchronized)：NTP サービスを有効にしているが、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。
(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

項番	説明
	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

4.7.8 show sntp

show sntp	
目的	SNTP の情報を表示します。
シンタックス	**show sntp**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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／無効を表示します。 Enabled：有効 Disabled：無効
(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。

4.8 NTP コマンド

NTP (Network Time Protocol) 関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ntp server	ntp server {IP-ADDRESS | IPV6-ADDRESS} [version NUMBER] [key KEY-ID] [prefer] [min-poll INTERVAL] [max-poll INTERVAL] no ntp server {IP-ADDRESS | IPV6-ADDRESS}
ntp peer	ntp peer {IP-ADDRESS | IPV6-ADDRESS} [version NUMBER] [key KEY-ID] [prefer] [min-poll INTERVAL] [max-poll INTERVAL] no ntp peer {IP-ADDRESS | IPV6-ADDRESS}
ntp update-calendar	ntp update-calendar no ntp update-calendar
ntp authenticate	ntp authenticate no ntp authenticate
ntp authentication-key	ntp authentication-key KEY-ID md5 VALUE no ntp authentication-key KEY-ID
ntp trusted-key	ntp trusted-key KEY-ID no ntp trusted-key KEY-ID
ntp control-key	ntp control-key KEY-ID no ntp control-key
ntp request-key	ntp request-key KEY-ID no ntp request-key
ntp disable	ntp disable no ntp disable
ntp access-group	ntp access-group {default | IP-ADDRESS [IP-MASK] | IPV6-ADDRESS | IPV6-ADDRESS/PREFIX-LENGTH} [ignore] [nomodify] [noquery] [nopeer] [noserve] [notrust] [version] no ntp access-group {default | IP-ADDRESS [IP-MASK] | IPV6-ADDRESS | IPV6-ADDRESS/PREFIX-LENGTH}
ntp max-associations	ntp max-associations NUMBER no ntp max-associations
ntp master	ntp master STRATUM no ntp master
service ntp	service ntp no service ntp
show ntp associations	show ntp associations [detail]
show ntp status	show ntp status

4.8.1 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。
シンタックス	**ntp server** {*IP-ADDRESS* | *IPV6-ADDRESS*} [**version** *NUMBER*] [**key** *KEY-ID*]

ntp server	
	[prefer] [min-poll *INTERVAL*] [max-poll *INTERVAL*] no ntp server {*IP-ADDRESS* | *IPV6-ADDRESS*}
パラメーター	*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 *NUMBER*（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
コマンドモード	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	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。
制限事項	-
注意事項	複数のパラメーターを設定する場合は、コマンドシンタックスの記載順で指定してください。
対象バージョン	1.01.01

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)#
```

4.8.2 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。
シンタックス	ntp peer {*IP-ADDRESS* | *IPV6-ADDRESS*} [version *NUMBER*] [key *KEY-ID*] [prefer] [min-poll *INTERVAL*] [max-poll *INTERVAL*] no ntp peer {*IP-ADDRESS* | *IPV6-ADDRESS*}
パラメーター	*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 *NUMBER*（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。

ntp peer	
	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
コマンドモード	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	-
制限事項	-
注意事項	複数のパラメーターを設定する場合は、コマンドシンタックスの記載順で指定してください。
対象バージョン	1.01.01

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)#
```

4.8.3 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。
シンタックス	**ntp update-calendar** **no ntp update-calendar**
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.4 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。
シンタックス	**ntp authenticate** **no ntp authenticate**
パラメーター	なし
デフォルト	NTP 認証は有効（**ntp authenticate**）
コマンドモード	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	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.8.5 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。
シンタックス	**ntp authentication-key** *KEY-ID* **md5** *VALUE* **no ntp authentication-key** *KEY-ID*
パラメーター	*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
コマンドモード	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	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 authentication-key	
	• 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.6 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。
シンタックス	**ntp trusted-key** *KEY-ID* **no ntp trusted-key** *KEY-ID*
パラメーター	*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
コマンドモード	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	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。
制限事項	**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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.7 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。
シンタックス	**ntp control-key** *KEY-ID* **no ntp control-key**
パラメーター	*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
コマンドモード	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	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。
制限事項	**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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.8 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。
シンタックス	**ntp request-key** *KEY-ID* **no ntp request-key**
パラメーター	*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
コマンドモード	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	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。
制限事項	**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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.9 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。
シンタックス	ntp disable no ntp disable
パラメーター	なし
デフォルト	NTP サービスは有効（no ntp disable）
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.10 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。
シンタックス	ntp access-group {default | *IP-ADDRESS* [*IP-MASK*] | *IPV6-ADDRESS* | *IPV6-ADDRESS/PREFIX-LENGTH*} [ignore] [nomodify] [noquery] [nopeer] [noserve] [notrust] [version] no ntp access-group {default | *IP-ADDRESS* [*IP-MASK*] | *IPV6-ADDRESS* | *IPV6-ADDRESS/PREFIX-LENGTH*}
パラメーター	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 IP-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/PREFIX-LENGTH*：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。

ntp access-group	
	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
コマンドモード	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	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.11 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。
シンタックス	ntp max-associations *NUMBER* no ntp max-associations
パラメーター	*NUMBER*：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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.12 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。
シンタックス	**ntp master** *STRATUM* **no ntp master**
パラメーター	*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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.13 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。
シンタックス	**service ntp** **no service ntp**
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.8.14 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。
シンタックス	show ntp associations [detail]
パラメーター	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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
(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。
(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。

項番	説明
(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。

4.8.15 show ntp status

show ntp status	
目的	NTP の状態を表示します。
シンタックス	**show ntp status**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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

項番	説明
(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。

4.9 TELNET コマンド

TELNET 関連の設定コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ip telnet server	ip telnet server no ip telnet server
ip telnet service-port	ip telnet service-port TCP-PORT no ip telnet service-port
ip telnet source-interface	ip telnet source-interface INTERFACE-ID no ip telnet source-interface

TELNET 関連の show／操作コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show ip telnet server	show ip telnet server
telnet	telnet {IP-ADDRESS | IPV6-ADDRESS} [TCP-PORT]

4.9.1 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。
シンタックス	**ip telnet server** **no ip telnet server**
パラメーター	なし
デフォルト	有効（**ip telnet server**）
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.9.2 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。
シンタックス	**ip telnet service-port** *TCP-PORT* **no ip telnet service-port**
パラメーター	*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

ip telnet service-port	
	競合する場合があります。
デフォルト	23
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.9.3 ip telnet source-interface

ip telnet source-interface	
目的	Telnet 接続を開始するインターフェースを指定します。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。
シンタックス	**ip telnet source-interface** *INTERFACE-ID* **no ip telnet source-interface**
パラメーター	*INTERFACE-ID*：Telnet 接続で使用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。 • **vlan**：VLAN インターフェースを指定します。 • **mgmt**：マネージメントポートを指定します。
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
コマンドモード	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	指定したインターフェースの IP アドレスが Telnet パケットの送信元アドレスとして使用されます。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：Telnet 接続を開始する Telnet パケットの送信元インターフェースとして、VLAN 100 インターフェースを設定する方法を示します。

```
# configure terminal
(config)# ip telnet source-interface vlan 100
(config)#
```

4.9.4 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。

show ip telnet server	
シンタックス	**show ip telnet server**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：Telnet サーバーの状態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／無効を表示します。

4.9.5 telnet

telnet	
目的	Telnet をサポートする別のデバイスにログインします。
シンタックス	**telnet** {*IP-ADDRESS* | *IPV6-ADDRESS*} [*TCP-PORT*]
パラメーター	*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。Telnet プロトコルのウェルノウン TCP ポート番号は、23 です。
デフォルト	なし
コマンドモード	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	本装置では、複数の Telnet セッションを確立できます。確立した Telnet セッションでは、それぞれで Telnet クライアントソフトウェアを同時に使用できます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：デフォルトの TCP ポート番号 23 で、IP アドレスが 10.0.0.103 の装置(ApresiaNP7000-48X6L)に Telnet する方法を示します。

```
# telnet 10.0.0.103

Ethernet Switch ApresiaNP7000-48X6L

Firmware: Build 1.06.01

User Verification Access
Username:
```

4.10 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。

コマンド	コマンドとパラメーター
ip ssh server	ip ssh server no ip ssh server
ip ssh service-port	ip ssh service-port TCP-PORT no ip ssh service-port
ip ssh timeout	ip ssh timeout SECONDS no ip ssh timeout
ip ssh authentication-retries	ip ssh authentication-retries NUMBER no ip ssh authentication-retries
ssh user authentication-method	ssh user NAME authentication-method {password | publickey URL | hostbased URL host-name HOSTNAME [IP-ADDRESS | IPV6-ADDRESS]} no ssh user NAME authentication-method

SSH (Secure Shell) 関連の show／操作コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show ip ssh	show ip ssh
show ssh	show ssh
show crypto key mypubkey	show crypto key mypubkey {rsa | dsa}
crypto key generate	crypto key generate {rsa [modulus MODULUS-SIZE] | dsa}
crypto key zeroize	crypto key zeroize {rsa | dsa}

4.10.1 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。
シンタックス	**ip ssh server** **no ip ssh server**
パラメーター	なし
デフォルト	無効
コマンドモード	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	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をサポートしています。 〈暗号化方式〉 aes256-cbc, aes192-cbc, aes128-cbc, 3des-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

ip ssh server	
	<メッセージ認証符号> HMAC-SHA1, HMAC-SHA1-96, HMAC-MD5, HMAC-MD5-96
制限事項	-
注意事項	鍵交換アルゴリズムの diffie-hellman-group-exchange-sha256 は、AEOS-NP2000 Ver. 1.07.01 以降でサポートしています。
対象バージョン	1.01.01

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)#
```

4.10.2 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。
シンタックス	**ip ssh service-port** *TCP-PORT* **no ip ssh service-port**
パラメーター	*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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.10.3 ip ssh timeout

ip ssh timeout	
目的	SSH セッション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。
シンタックス	**ip ssh timeout** *SECONDS* **no ip ssh timeout**
パラメーター	*SECONDS*：SSH セッションタイムアウト時間（SSH クライアントの応答を待つ時間）を 30～600 秒の範囲で指定します。
デフォルト	120 秒
コマンドモード	グローバル設定モード
特権レベル	レベル：12

ip ssh timeout	
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：SSH セッションタイムアウト時間を 160 秒に設定する方法を示します。

```
# configure terminal
(config)# ip ssh timeout 160
(config)#
```

4.10.4 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。
シンタックス	ip ssh authentication-retries *NUMBER* no ip ssh authentication-retries
パラメーター	*NUMBER*：SSH 認証の再試行回数を 1～32 の範囲で指定します。
デフォルト	3
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.10.5 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。
シンタックス	ssh user *NAME* authentication-method {password | publickey *URL* | hostbased *URL* host-name *HOSTNAME* [*IP-ADDRESS* | *IPV6-ADDRESS*]} no ssh user *NAME* authentication-method
パラメーター	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 *HOSTNAME*：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	password
コマンドモード	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	管理者がユーザーの認証方式を指定するコマンドです。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.10.6 show ip ssh

show ip ssh	
目的	SSH サーバーの設定を表示します。
シンタックス	**show ip ssh**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 サーバーの状態を表示します。
(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。

4.10.7 show ssh

show ssh	
目的	SSH 接続の情報を表示します。
シンタックス	show ssh
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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   3des-cbc/sha1-96            user1            192.168.0.100
1   V2   3des-cbc/hmac-sha1          user2            2000::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とメッセージ認証符号を表示します。 〈暗号化方式〉 aes256-cbc, aes192-cbc, aes128-cbc, 3des-cbc, arcfour, blowfish-cbc, cast128-cbc, twofish-cbc, twofish256-cbc, twofish192-cbc, twofish128-cbc 〈メッセージ認証符号〉 HMAC-SHA1, HMAC-SHA1-96, HMAC-MD5, HMAC-MD5-96

項番	説明
(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。

4.10.8 show crypto key mypubkey

show crypto key mypubkey	
目的	RSA 公開鍵、または DSA 公開鍵を表示します。
シンタックス	**show crypto key mypubkey {rsa | dsa}**
パラメーター	**rsa**：RSA 公開鍵を表示する場合に指定します。 **dsa**：DSA 公開鍵を表示する場合に指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：RSA 公開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: 09:48:40, 2016-03-01 ...(1)
Key Size: 768 bits ...(2)
Key Data: ...(3)
AAAAB3Nz aC1yc2EA AAADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s7l9H/bh jG/oqkwj SlUJSGqR e/sj6Ws=
```

項番	説明
(1)	RSA 公開鍵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 公開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 公開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 公開鍵のサイズを表示します。
(3)	RSA 公開鍵を表示します。

使用例：DSA 公開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 公開鍵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 公開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 公開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 公開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 公開鍵を表示します。

4.10.9 crypto key generate

crypto key generate	
目的	RSA 鍵対または DSA 鍵対を生成します。
シンタックス	**crypto key generate** {**rsa** [**modulus** *MODULUS-SIZE*] ｜ **dsa**}
パラメーター	**rsa**：RSA 鍵対を生成する場合に指定します。 **modulus** *MODULUS-SIZE*（省略可能）：RSA の鍵長を指定します。有効な値は 360、512、768、1024、および 2048 ビットです。 **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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：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：DSA 鍵対の生成方法を示します。

```
# crypto key generate dsa

Generating DSA key...Done.
```

4.10.10 crypto key zeroize

crypto key zeroize	
目的	RSA 鍵対または DSA 鍵対を削除します。
シンタックス	crypto key zeroize {rsa | dsa}
パラメーター	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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：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：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
```

4.11 RMON コマンド

RMON (Remote Network Monitoring) 関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
rmon collection stats	rmon collection stats STATS-ID [owner NAME] no rmon collection stats STATS-ID
rmon collection history	rmon collection history HISTORY-ID [owner NAME] [buckets NUM] [interval SECONDS] no rmon collection history HISTORY-ID
rmon alarm	rmon alarm ALARM-ID VARIABLE INTERVAL {absolute | delta} rising-threshold VALUE [RISING-EVENT-ID] falling-threshold VALUE [FALLING-EVENT-ID] [owner NAME] no rmon alarm ALARM-ID
rmon event	rmon event EVENT-ID [log] [trap COMMUNITY] [owner NAME] [description STRING] no rmon event EVENT-ID
snmp-server enable traps rmon	snmp-server enable traps rmon [rising-alarm | falling-alarm] no snmp-server enable traps rmon [rising-alarm | falling-alarm]
show rmon statistics	show rmon statistics
show rmon history	show rmon history
show rmon alarm	show rmon alarm
show rmon events	show rmon events

4.11.1 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。
シンタックス	**rmon collection stats** *STATS-ID* [**owner** *NAME*] **no rmon collection stats** *STATS-ID*
パラメーター	*STATS-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
コマンドモード	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。
制限事項	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)では実施できません。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.11.2 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。
シンタックス	rmon collection history *HISTORY-ID* [owner *NAME*] [buckets *NUM*] [interval *SECONDS*] no rmon collection history *HISTORY-ID*
パラメーター	*HISTORY-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 *NUM*（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
コマンドモード	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。
制限事項	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)では実施できません。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.11.3 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。
シンタックス	rmon alarm *ALARM-ID VARIABLE INTERVAL* {absolute | delta} rising-threshold *VALUE* [*RISING-EVENT-ID*] falling-threshold *VALUE* [*FALLING-EVENT-ID*] [owner *NAME*]

rmon alarm	
	no rmon alarm *ALARM-ID*
パラメーター	*ALARM-ID*：アラームエントリーID を 1～65535 の範囲で指定します。 *VARIABLE*：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。 **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
コマンドモード	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	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.11.4 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 形式のコマンドを使用します。
シンタックス	**rmon event** *EVENT-ID* [**log**] [**trap** *COMMUNITY*] [**owner** *NAME*] [**description** *STRING*] **no rmon event** *EVENT-ID*
パラメーター	*EVENT-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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.11.5 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。

snmp-server enable traps rmon	
シンタックス	snmp-server enable traps rmon [rising-alarm | falling-alarm] no snmp-server enable traps rmon [rising-alarm | falling-alarm]
パラメーター	rising-alarm（省略可能）：上昇しきい値イベント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通知を有効にする場合に指定します。
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.11.6 show rmon statistics

show rmon statistics	
目的	RMON 統計情報を表示します。
シンタックス	show rmon statistics
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
  (4)                          (5)
  Received octets: 518394321, Received packets: 5228964
  (6)                          (7)
  Broadcast packets: 2559743, Multicast packets: 988945
  (8)                    (9)
  Undersized packets: 0, Oversized packets: 0
  (10)          (11)
  Fragments: 0, Jabbers: 0
  (12)                      (13)
```

```
  CRC alignment errors: 0, Collisions: 0
  Drop events: 887 ...(14)
  (15)
  Packets in 64 octets: 4255288, Packets in 65-127 octets: 128250
  Packets in 128-255 octets: 576077, Packets in 256-511 octets: 102826
  Packets in 512-1023 octets: 165799, Packets in 1024-1518 octets: 724
```

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)	受信オクテット数を表示します。
(5)	受信パケット数を表示します。
(6)	ブロードキャストパケット数を表示します。
(7)	マルチキャストパケット数を表示します。
(8)	フレーム長が 64 オクテットよりも小さいパケット数を表示します。
(9)	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。
(10)	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 (Frame Check Sequence) エラーを伴うパケット数を表示します。
(11)	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 (Frame Check Sequence) 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 (Frame Check Sequence) エラーを伴うパケット数を表示します。
(13)	コリジョンの推定値を表示します。
(14)	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。
(15)	フレーム長ごとの受信パケット数を表示します。

4.11.7 show rmon history

show rmon history	
目的	RMON 統計情報の履歴を表示します。
シンタックス	**show rmon history**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)
  (7)                    (8)
```

```
    Received octets: 9303, Received packets: 107
     (9)                    (10)
    Broadcast packets: 37, Multicast packets: 14
    Estimated utilization: 100 ...(11)
     (12)                   (13)
    Undersized packets: 0, Oversized packets: 0
     (14)          (15)
    Fragments: 0, Jabbers: 0
     (16)                     (17)
    CRC alignment errors: 0, Collisions: 0
    Drop events: 0 ...(18)
   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。
(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)	受信オクテット数を表示します。
(8)	受信パケット数を表示します。
(9)	ブロードキャストパケット数を表示します。
(10)	マルチキャストパケット数を表示します。
(11)	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。
(12)	フレーム長が 64 オクテットよりも小さいパケット数を表示します。
(13)	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。
(14)	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（Frame Check Sequence）エラーを伴うパケット数を表示します。
(15)	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（Frame Check Sequence）エラーを伴うパケット数を表示します。
(16)	フレーム長が 64～1,518 オクテットのパケットのうち、FCS（Frame Check Sequence）エラーを伴うパケット数を表示します。
(17)	コリジョンの推定値を表示します。
(18)	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。

4.11.8 show rmon alarm

show rmon alarm	
目的	アラームエントリーを表示します。

show rmon alarm	
シンタックス	show rmon alarm
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
  (7)                        (8)
 Rising threshold is 2000, assigned to event 12
  (9)                         (10)
 Falling threshold is 1100, assigned to event 12
 On startup enable rising or falling alarm ...(11)
```

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。
(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）を表示します。
(8)	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。
(9)	下降しきい値（下限値）を表示します。
(10)	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。
(11)	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。

4.11.9 show rmon events

show rmon events	
目的	イベントエントリーを表示します。
シンタックス	show rmon events
パラメーター	なし
デフォルト	なし

show rmon events	
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
(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。

4.12 sFlow コマンド

sFlow 関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
sflow receiver	sflow receiver INDEX [owner NAME] [expiry {SECONDS | infinite}] [max-datagram-size SIZE] [host {IP-ADDRESS | IPV6-ADDRESS}] [udp-port PORT] no sflow receiver INDEX
sflow sampler	sflow sampler INSTANCE [receiver RECEIVER] [inbound | outbound] [sampling-rate RATE] [max-header-size SIZE] no sflow sampler INSTANCE
sflow poller	sflow poller INSTANCE [receiver RECEIVER] [interval SECONDS] no sflow poller INSTANCE
show sflow	show sflow [agent | receiver | sampler | poller]

4.12.1 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。
シンタックス	**sflow receiver** *INDEX* [**owner** *NAME*] [**expiry** {*SECONDS* | **infinite**}] [**max-datagram-size** *SIZE*] [**host** {*IP-ADDRESS* | *IPV6-ADDRESS*}] [**udp-port** *PORT*] **no sflow receiver** *INDEX*
パラメーター	*INDEX*：レシーバーID を 1～4 の範囲で指定します。 **owner** *NAME*（省略可能）：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。ユーザーは所有者名に空の文字列を指定できません。 **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。指定しない場合は **infinite** が設定されます。 • *SECONDS*：有効期限を 1～2,000,000 秒の範囲で指定します。 • **infinite**：有効期限を無期限にする場合に指定します。 **max-datagram-size** *SIZE*（省略可能）：1 つの 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。指定しない場合は 1400 が設定されます。 **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。指定しない場合は 0.0.0.0 が設定されます。 **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。指定しない場合は 6343 が設定されます。
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： • 所有者名：空の文字列 • 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

sflow receiver	
	• UDP ポート番号：6343
コマンドモード	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	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。 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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.12.2 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。
シンタックス	**sflow sampler** *INSTANCE* [**receiver** *RECEIVER*] [**inbound** | **outbound**] [**sampling-rate** *RATE*] [**max-header-size** *SIZE*] **no sflow sampler** *INSTANCE*
パラメーター	*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** *RECEIVER*（省略可能）：レシーバーID を 1～4 の範囲で指定します。指定しない場合は 0 が設定されます。 サンプリング対象（省略可能）：サンプリング対象を、以下のパラメーターで指定します。指定しない場合は inbound が設定されます。 • inbound：受信パケットをサンプリング対象にする。 • outbound：送信パケットをサンプリング対象にする。 **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 を指定した場合はサンプラーが無効になります。指定しない場合は 0 が設定されます。（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）

sflow sampler	
	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タの最大バイト数を、18～256 の範囲で指定します。指定しない場合は 128 が設定されます。
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
コマンドモード	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	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, ・・・)
制限事項	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。
注意事項	複数のパラメーターを同時に設定する場合は、コマンドシンタックスの記載順で指定してください。
対象バージョン	1.01.01

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)#
```

4.12.3 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。
シンタックス	**sflow poller** *INSTANCE* [**receiver** *RECEIVER*] [**interval** *SECONDS*] **no sflow poller** *INSTANCE*
パラメーター	*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** *RECEIVER*（省略可能）：レシーバーID を 1～4 の範囲で指定します。指定しない場合は 0 が設定されます。 **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 を指定した場合はポーラーが無効になります。指定しない場合は 0 が設定されます。
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
コマンドモード	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	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。
制限事項	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。
注意事項	複数のパラメーターを同時に設定する場合は、コマンドシンタックスの記載順で指定してください。
対象バージョン	1.01.01

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)#
```

4.12.4 show sflow

show sflow	
目的	sFlow 情報を表示します。
シンタックス	**show sflow** [**agent** | **receiver** | **sampler** | **poller**]
パラメーター	**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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)	サンプラーの動作モードを表示します。 inbound：受信パケット用 outbound：送信パケット用
(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)	サンプラーの動作モードを表示します。 inbound：受信パケット用 outbound：送信パケット用
(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。

4.13 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。

コマンド	コマンドとパラメーター
snmp-server	snmp-server no snmp-server
snmp-server name	snmp-server name SYSTEM-NAME no snmp-server name
snmp-server location	snmp-server location SYSTEM-LOCATION no snmp-server location
snmp-server contact	snmp-server contact SYSTEM-CONTACT no snmp-server contact
snmp-server service-port	snmp-server service-port PORT-NUMBER no snmp-server service-port
snmp-server response broadcast-request	snmp-server response broadcast-request no snmp-server response broadcast-request
snmp-server community	snmp-server community [0 | 7] COMMUNITY-STRING [view VIEW-NAME] [ro | rw] [access IP-ACL-NAME] no snmp-server community [0 | 7] COMMUNITY-STRING
snmp-server host	snmp-server host {IP-ADDRESS | IPV6-ADDRESS} [version {1 | 2c | 3 {auth | noauth | priv}}] [0 | 7] COMMUNITY-STRING [port PORT-NUMBER] no snmp-server host {IP-ADDRESS | IPV6-ADDRESS}
snmp-server enable traps	snmp-server enable traps no snmp-server enable traps
snmp-server enable traps snmp	snmp-server enable traps snmp [authentication | linkup | linkdown | coldstart | warmstart] no snmp-server enable traps snmp [authentication | linkup | linkdown | coldstart | warmstart]
snmp-server enable traps environment	snmp-server enable traps environment [fan] [power] [temperature] [memory] no snmp-server enable traps environment [fan | power | temperature | memory]
snmp-server source-interface traps	snmp-server source-interface traps INTERFACE-ID no snmp-server source-interface traps
snmp-server trap-sending disable	snmp-server trap-sending disable no snmp-server trap-sending disable
snmp trap link-status	snmp trap link-status no snmp trap link-status
snmp-server user	snmp-server user USER-NAME [0 | 7] GROUP-NAME v3 [encrypted] [auth {md5 | sha} AUTH-PASSWORD [priv PRIV-PASSWORD]] [access IP-ACL-NAME] no snmp-server user USER-NAME [0 | 7] GROUP-NAME v3

コマンド	コマンドとパラメーター
snmp-server group	snmp-server group [0 | 7] GROUP-NAME {v1 | v2c | v3 {auth | noauth | priv}} [read READ-VIEW] [write WRITE-VIEW] [notify NOTIFY-VIEW] [access IP-ACL-NAME] no snmp-server group [0 | 7] GROUP-NAME {v1 | v2c | v3 {auth | noauth | priv}}
snmp-server view	snmp-server view VIEW-NAME OID-TREE {included | excluded} no snmp-server view VIEW-NAME
snmp-server engineID local	snmp-server engineID local ENGINEID-STRING no 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。

コマンド	コマンドとパラメーター
show snmp-server	show snmp-server
show snmp community	show snmp community
show snmp host	show snmp host
show snmp-server traps	show snmp-server traps
show snmp-server trap-sending	show snmp-server trap-sending [interface INTERFACE-ID [,|-]]
show snmp trap link-status	show snmp trap link-status [interface INTERFACE-ID [,|-]]
show snmp user	show snmp user [USER-NAME]
show snmp group	show snmp group
show snmp view	show snmp view
show snmp engineID	show snmp engineID

4.13.1 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。
シンタックス	snmp-server no snmp-server
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	AEOS-NP2000 Ver. 1.09.01 以降では、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

snmp-server	
	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。
対象バージョン	1.01.01

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)#
```

4.13.2 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。
シンタックス	**snmp-server name** *SYSTEM-NAME* **no snmp-server name**
パラメーター	*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
コマンドモード	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	**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。
制限事項	-
注意事項	システム名（sysName）の先頭に数字を指定できるのは AEOS-NP2000 Ver. 1.03.06 以降です。それより前のバージョンでは指定できません。
対象バージョン	1.01.01 1.03.06：設定可能文字列の仕様変更

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)#
```

4.13.3 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。
シンタックス	**snmp-server location** *SYSTEM-LOCATION* **no snmp-server location**
パラメーター	*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。スペースも使用できます。
デフォルト	なし
コマンドモード	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	-

snmp-server location	
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.13.4 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。
シンタックス	**snmp-server contact** *SYSTEM-CONTACT* **no snmp-server contact**
パラメーター	*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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.13.5 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。
シンタックス	**snmp-server service-port** *PORT-NUMBER* **no snmp-server service-port**
パラメーター	*PORT-NUMBER*：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。
デフォルト	161
コマンドモード	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	-
制限事項	-
注意事項	-

snmp-server service-port	
対象バージョン	1.01.01

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)#
```

4.13.6 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。
シンタックス	snmp-server response broadcast-request no snmp-server response broadcast-request
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.13.7 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。
シンタックス	snmp-server community [0 | 7] *COMMUNITY-STRING* [view *VIEW-NAME*] [ro | rw] [access *IP-ACL-NAME*] no snmp-server community [0 | 7] *COMMUNITY-STRING*
パラメーター	[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。 *COMMUNITY-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 *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。

snmp-server community	
	[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 *IP-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）
コマンドモード	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	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

使用例：SNMP ビュー「interfacesMibView」を設定し、interfacesMibView に read-write アクセスができる SNMP コミュニティー名「comaccess」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)# snmp-server community comaccess view interfacesMibView rw
(config)#
```

4.13.8 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。
シンタックス	**snmp-server host** {*IP-ADDRESS* | *IPV6-ADDRESS*} [**version** {1 | 2c | 3 {auth | noauth | priv}}] [0 | 7] *COMMUNITY-STRING* [**port** *PORT-NUMBER*] **no snmp-server host** {*IP-ADDRESS* | *IPV6-ADDRESS*}

パラメーター	*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-STRING：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 *PORT-NUMBER*（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
コマンドモード	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	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。
制限事項	-
注意事項	-

snmp-server host	
対象バージョン	1.01.01

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)#
```

4.13.9 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。
シンタックス	snmp-server enable traps no snmp-server enable traps
パラメーター	なし
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.13.10 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。
シンタックス	snmp-server enable traps snmp [authentication | linkup | linkdown | coldstart | warmstart] no snmp-server enable traps snmp [authentication | linkup | linkdown | coldstart | warmstart]
パラメーター	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。正常に認証が行われなかったという SNMP メッセージを装置が受信すると、authenticationFailuretrap が出力されます。認証方式は、使用している SNMP のバージョンによって異なります。SNMPv1 または SNMPv2c では、パケットが不適切な SNMP コミュニティー名の場合に認証が失敗します。SNMPv3 では、パケットが不適切な 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。

snmp-server enable traps snmp	
	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。 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
コマンドモード	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	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.13.11 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。
シンタックス	snmp-server enable traps environment [fan] [power] [temperature] [memory] no snmp-server enable traps environment [fan | power | temperature | memory]
パラメーター	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。 memory（省略可能）：システムメモリー使用率監視機能の通知を有効にする場合に指定します。
デフォルト	fan、power、temperature パラメーターは無効 memory パラメーターは有効
コマンドモード	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	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。
制限事項	本コマンドは、構成情報ではデバイス関連（ラベル# DEVICE）で表示されます。
注意事項	-
対象バージョン	1.03.01 1.09.01：memory パラメーター追加

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)#
```

4.13.12 snmp-server source-interface traps

snmp-server source-interface traps	
目的	SNMP トラップパケットの送信元 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。
シンタックス	snmp-server source-interface traps *INTERFACE-ID* no snmp-server source-interface traps
パラメーター	*INTERFACE-ID*：SNMP トラップパケットの送信元 IP アドレスとして使用するインターフェースを、以下のパラメーターで指定します。 • vlan：VLAN インターフェースを指定します。 • mgmt：マネージメントポートを指定します。
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
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：SNMP トラップパケットの送信元 IP アドレスとして使用するインターフェースを、VLAN 100 インターフェースに設定する方法を示します。

```
# configure terminal
(config)# snmp-server source-interface traps vlan100
(config)#
```

4.13.13 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。
シンタックス	snmp-server trap-sending disable no snmp-server trap-sending disable
パラメーター	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）
コマンドモード	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	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。
制限事項	-

snmp-server trap-sending disable	
注意事項	-
対象バージョン	1.01.01

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)#
```

4.13.14 snmp trap link-status

snmp trap link-status	
目的	対象ポートのリンクアップ通知およびリンクダウン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。
シンタックス	snmp trap link-status no snmp trap link-status
パラメーター	なし
デフォルト	リンクアップ通知およびリンクダウン通知は有効（snmp trap link-status）
コマンドモード	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	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通知およびリンクダウン通知を無効にするには、no snmp trap link-status を設定します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 で、リンクアップ通知およびリンクダウン通知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)#
```

4.13.15 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。
シンタックス	snmp-server user *USER-NAME* [0 | 7] *GROUP-NAME* v3 [encrypted] [auth {md5 | sha} *AUTH-PASSWORD* [priv *PRIV-PASSWORD*]] [access *IP-ACL-NAME*] no snmp-server user *USER-NAME* [0 | 7] *GROUP-NAME* v3
パラメーター	*USER-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-NAME*：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。

snmp-server user	
	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。 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-PASSWORD*：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-PASSWORD*（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 *IP-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
コマンドモード	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	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-PASSWORD)、または暗号化パスワード(PRIV-PASSWORD)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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

使用例：SNMP ユーザー名「user1」、設定済みの SNMP グループ名「test-group」、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)#
```

4.13.16 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。
シンタックス	**snmp-server group** [0 | 7] *GROUP-NAME* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *READ-VIEW*] [**write** *WRITE-VIEW*] [**notify** *NOTIFY-VIEW*] [**access** *IP-ACL-NAME*] **no snmp-server group** [0 | 7] *GROUP-NAME* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}
パラメーター	[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-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** *IP-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）

snmp-server group	
	private (SNMPv1, N/A, CommunityView, CommunityView, CommunityView) private (SNMPv2c, N/A, CommunityView, CommunityView, CommunityView) initial (SNMPv3, noauth, restricted, N/A, restricted)
コマンドモード	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	SNMP グループは、許可される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の許可の内容を定義します。 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。
制限事項	**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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.13.17 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。
シンタックス	**snmp-server view** *VIEW-NAME OID-TREE* {**included** | **excluded**} **no snmp-server view** *VIEW-NAME*
パラメーター	*VIEW-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。

snmp-server view	
	OID-TREE：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-TREE, 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）
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.13.18 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。
シンタックス	**snmp-server engineID local** *ENGINEID-STRING* **no snmp-server engineID local**
パラメーター	*ENGINEID-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
コマンドモード	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	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。
制限事項	-

snmp-server engineID local	
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.13.19 show snmp-server

show snmp-server	
目的	SNMP エージェントの設定を表示します。
シンタックス	show snmp-server
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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     : 50000 ...(5)
SNMP Response Broadcast Request     : Enabled ...(6)
```

項番	説明
(1)	SNMP エージェントの有効／無効を表示します。
(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 に対する応答設定を表示します。

4.13.20 show snmp community

show snmp community	
目的	SNMP コミュニティー名を表示します。

show snmp community	
シンタックス	show snmp community
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)

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。

4.13.21 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。
シンタックス	show snmp host
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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     : V1 ...(2)
Community Name   : public ...(3)
UDP Port         : 50001 ...(4)
```

```
Host IP Address  : 10.10.10.1
SNMP Version     : V3 noauthnopriv
SNMPv3 User Name : user1 ...(5)
UDP Port         : 50001

Host IPv6 Address: 2001:db8::100 ...(6)
SNMP Version     : V3 noauthnopriv
SNMPv3 User Name : user2
UDP Port         : 162

Total Entries: 3
```

項番	説明
(1)	SNMP トラップの宛先ホストの IPv4 アドレスを表示します。
(2)	SNMP トラップの送信に使用する SNMP のバージョンを表示します。 V1：SNMPv1 V2C：SNMPv2c 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。
(6)	SNMP トラップの宛先ホストの IPv6 アドレスを表示します。

4.13.22 show snmp-server traps

show snmp-server traps	
目的	SNMP トラップ関連設定を表示します。
シンタックス	show snmp-server traps
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01 1.09.01：表示内容を拡張

使用例：SNMP トラップ関連設定を表示する方法を示します。

```
# show snmp-server traps

Global Trap State : Enabled ...(1)
Individual Trap State:
  STACK
    Stack                    : Disabled ...(2)
  Environment
    Fan                      : Disabled ...(3)
    Power                    : Disabled ...(4)
    Temperature              : Disabled ...(5)
```

```
    Memory                    : Enabled ...(6)
  SYSTEM
    CPU-Protect               : Disabled ...(7)
  STORM
    Storm-control             : Disabled ...(8)
  PORT
    SFP                       : Disabled ...(9)
  STP
    New-root                  : Disabled ...(10)
    Topology-change           : Disabled ...(11)
  PoE
    PoE                       : Enabled ...(12)
  SNMP
    Authentication            : Disabled ...(13)
    Linkup                    : Disabled ...(14)
    Linkdown                  : Disabled ...(15)
    Coldstart                 : Disabled ...(16)
    Warmstart                 : Disabled ...(17)
  LLDP
    LLDP                      : Disabled ...(18)
    LLDP-MED                  : Disabled ...(19)
  RMON
    Rising-alarm              : Disabled ...(20)
    Falling-alarm             : Disabled ...(21)
```

項番	説明
(1)	SNMP トラップのグローバル設定の有効／無効を表示します。
(2)	スタック機能の SNMP トラップの有効／無効を表示します。
(3)	ファン関連の SNMP トラップの有効／無効を表示します。
(4)	電源関連の SNMP トラップの有効／無効を表示します。
(5)	温度関連の SNMP トラップの有効／無効を表示します。
(6)	システムメモリー使用率監視機能の SNMP トラップの有効／無効を表示します。
(7)	CPU 使用率監視機能の SNMP トラップの有効／無効を表示します。
(8)	ストームコントロール機能の SNMP トラップの有効／無効を表示します。
(9)	光トランシーバー関連の SNMP トラップの有効／無効を表示します。
(10)	スパニングツリープロトコル機能の、新ルートブリッジ SNMP トラップの有効／無効を表示します。
(11)	スパニングツリープロトコル機能の、トポロジー変更 SNMP トラップの有効／無効を表示します。
(12)	PoE 機能の SNMP トラップの有効／無効を表示します。PoE 対応機種でのみ表示されます。
(13)	SNMP 認証失敗 SNMP トラップの有効／無効を表示します。
(14)	リンクアップ SNMP トラップのグローバル設定の有効／無効を表示します。
(15)	リンクダウン SNMP トラップのグローバル設定の有効／無効を表示します。
(16)	コールドスタート SNMP トラップの有効／無効を表示します。
(17)	ウォームスタート SNMP トラップの有効／無効を表示します。
(18)	LLDP 機能の SNMP トラップの有効／無効を表示します。
(19)	LLDP-MED 機能の SNMP トラップの有効／無効を表示します。
(20)	RMON 機能の、上限値超過 SNMP トラップの有効／無効を表示します。
(21)	RMON 機能の、下限値超過 SNMP トラップの有効／無効を表示します。

4.13.23 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または送信禁止ポートを表示します。
シンタックス	show snmp-server trap-sending [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID*（省略可能）：自装置の SNMP トラップの送信可否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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 1/0/9 の、自装置の SNMP トラップの送信可否を表示する方法を示します。

```
# show snmp-server trap-sending interface port 1/0/1-1/0/9
 (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
Port1/0/6           Disabled
Port1/0/7           Enabled
Port1/0/8           Enabled
Port1/0/9           Enabled
```

項番	説明
(1)	ポート番号を表示します。
(2)	自装置の SNMP トラップの送信可否を表示します。 Enabled：送信可能ポート Disabled：送信禁止ポート

4.13.24 show snmp trap link-status

show snmp trap link-status	
目的	ポートのリンクアップ通知およびリンクダウン通知の設定を表示します。
シンタックス	show snmp trap link-status [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID*（省略可能）：ポートのリンクアップ通知およびリンクダウン通知の有効／無効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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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 snmp trap link-status	
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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 1/0/9 の、リンクアップ通知およびリンクダウン通知の有効／無効を表示する方法を示します。

```
# show snmp trap link-status interface port 1/0/1-1/0/9
 (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
Port1/0/6            Enabled
Port1/0/7            Enabled
Port1/0/8            Enabled
Port1/0/9            Enabled
```

項番	説明
(1)	ポート番号を表示します。
(2)	リンクアップ通知およびリンクダウン通知の有効／無効を表示します。 Enabled：有効（リンクアップ通知およびリンクダウン通知可能） Disabled：無効（リンクアップ通知およびリンクダウン通知不可）

4.13.25 show snmp user

show snmp user	
目的	SNMP ユーザーを表示します。
シンタックス	**show snmp user** [*USER-NAME*]
パラメーター	*USER-NAME*（省略可能）：SNMP ユーザー名を指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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を表示します。 3：SNMPv3
(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。 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を表示します。 None：なし DES：Data Encryption Standard
(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 アクセスリストを表示します。

4.13.26 show snmp group

show snmp group	
目的	SNMP グループを表示します。
シンタックス	**show snmp group**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)
  (3)                                                  (4)
  ReadView      : CommunityView                        WriteView     :
  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)	グループと関連付ける標準 IP アクセスリストを表示します。

4.13.27 show snmp view

show snmp view	
目的	SNMP ビューを表示します。
シンタックス	**show snmp view**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
(2)	OID ツリーを SNMP ビューに含めるか除外するかを表示します。 included：OID ツリーを SNMP ビューに含める excluded：OID ツリーを SNMP ビューから除外する
(3)	OID ツリーの頂点のオブジェクト識別子を表示します。

4.13.28 show snmp engineID

show snmp engineID	
目的	SNMP エンジン ID を表示します。
シンタックス	**show snmp engineID**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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: 800001160300406670450000 ...(1)
```

項番	説明
(1)	SNMP エンジン ID を表示します。

4.14 ミラーリングコマンド

ミラーリング関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
monitor session destination interface	monitor session SESSION-NUMBER destination interface INTERFACE-ID no monitor session SESSION-NUMBER destination interface INTERFACE-ID
monitor session destination remote vlan	monitor session SESSION-NUMBER destination remote vlan VLAN-ID interface INTERFACE-ID no monitor session SESSION-NUMBER destination remote vlan
monitor session source interface	monitor session SESSION-NUMBER source interface {INTERFACE-ID [,|-] [both | rx | tx] | cpu rx} no monitor session SESSION-NUMBER source interface {INTERFACE-ID [,|-] | cpu rx}
monitor session source acl	monitor session SESSION-NUMBER source acl ACCESS-LIST-NAME no monitor session SESSION-NUMBER source acl ACCESS-LIST-NAME
monitor session source remote vlan	monitor session SESSION-NUMBER source remote vlan VLAN-ID no monitor session SESSION-NUMBER source remote vlan
remote-span	remote-span no remote-span
no monitor session	no monitor session SESSION-NUMBER
show monitor session	show monitor session [SESSION-NUMBER | remote | local]

4.14.1 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、ミラーリングしたパケット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。
シンタックス	**monitor session** *SESSION-NUMBER* **destination interface** *INTERFACE-ID* **no monitor session** *SESSION-NUMBER* **destination interface** *INTERFACE-ID*
パラメーター	*SESSION-NUMBER*：セッション番号を、1～4 の範囲で指定します。 *INTERFACE-ID*：モニターセッションのための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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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	1 つのモニターセッションには、1 つの宛先インターフェースのみ設定できます。 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。

monitor session destination interface	
制限事項	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。 ApresiaNP2000 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。
注意事項	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パケット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。
対象バージョン	1.01.01

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 からポート 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)#
```

4.14.2 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、ミラーリングしたパケット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。
シンタックス	monitor session *SESSION-NUMBER* destination remote vlan *VLAN-ID* interface *INTERFACE-ID* no monitor session *SESSION-NUMBER* destination remote vlan
パラメーター	*SESSION-NUMBER*：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。 interface *INTERFACE-ID*：ミラーリングしたパケットを送信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：物理ポートを指定します。 • port-channel：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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	1 つのモニターセッションには、1 つのリモートモニターVLAN と宛先インターフェースのみ設定できます。 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

monitor session destination remote vlan	
	くても、ミラーリングされたパケット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。
制限事項	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ん。 ApresiaNP2000 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。
注意事項	-
対象バージョン	1.01.01

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ポート 1/0/2 からポート 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 source interface port 1/0/2-4
(config)# monitor session 2 destination remote vlan 100 interface port 1/0/6
(config)#
```

4.14.3 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。
シンタックス	**monitor session** *SESSION-NUMBER* **source interface** {*INTERFACE-ID* [,|-] [**both** | **rx** | **tx**] | **cpu rx**} **no monitor session** *SESSION-NUMBER* **source interface** {*INTERFACE-ID* [,|-] | **cpu rx**}
パラメーター	*SESSION-NUMBER*：セッション番号を、1～4 の範囲で指定します。 *INTERFACE-ID*：ミラーリングする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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。 **both**（省略可能）：送受信するパケットを対象にする場合に指定します。 **rx**（省略可能）：受信するパケットを対象にする場合に指定します。 **tx**（省略可能）：送信するパケットを対象にする場合に指定します。 **cpu rx**：CPU が受信したすべてのパケットをミラーリングする場合に指定します。
デフォルト	なし

monitor session source interface	
コマンドモード	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	1 つのモニターセッションには、複数の送信元インターフェースを設定できます。 both, rx, tx パラメーターを指定しない場合は、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。
制限事項	送信パケットがミラーリング対象になる場合は、送信されるフレームのタグの有無にかかわらず、タグ付きフレームとしてミラーリングされます。 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。 ApresiaNP2000 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。
注意事項	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。
対象バージョン	1.01.01

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 からポート 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)#
```

4.14.4 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。
シンタックス	monitor session *SESSION-NUMBER* source acl *ACCESS-LIST-NAME* no monitor session *SESSION-NUMBER* source acl *ACCESS-LIST-NAME*
パラメーター	*SESSION-NUMBER*：セッション番号を、1～4 の範囲で指定します。 *ACCESS-LIST-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ます。受信方向のミラーリングのみサポートされています。
デフォルト	なし

monitor session source acl	
コマンドモード	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	1 つのモニターセッションには、1 つの送信元アクセスリストのみ設定できます。アクセスリストでは複数のエントリーを設定できます。 permit で設定したエントリーだけでなく、deny で設定したエントリー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。
制限事項	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。 ApresiaNP2000 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。
注意事項	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。
対象バージョン	1.01.01

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拡張 MAC アクセスリストの 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)#
```

4.14.5 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。
シンタックス	**monitor session** *SESSION-NUMBER* **source remote vlan** *VLAN-ID* **no monitor session** *SESSION-NUMBER* **source remote vlan**
パラメーター	*SESSION-NUMBER*：セッション番号を、1～4 の範囲で指定します。 *VLAN-ID*：ミラーリング元のリモートモニターVLAN を、2～4094 の範囲で指定します。
デフォルト	なし
コマンドモード	グローバル設定モード
特権レベル	レベル：12

monitor session source remote vlan	
ガイドライン	1 つのモニターセッションには、1 つのリモートモニターVLAN 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、monitor session source remote vlan 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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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パケットはポート 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)#
```

4.14.6 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。
シンタックス	remote-span no remote-span
パラメーター	なし
デフォルト	なし
コマンドモード	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。

remote-span	
	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。
制限事項	-
注意事項	リモートモニターセッションに関係する中継装置の、モニターされたパケットを受信するポートと、モニターされたパケットを送信するポートは、リモートモニターVLAN のタグ付きのメンバーポートとして設定してください。
対象バージョン	1.01.01

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)#
```

4.14.7 no monitor session

no monitor session	
目的	モニターセッションを削除します。
シンタックス	**no monitor session** *SESSION-NUMBER*
パラメーター	*SESSION-NUMBER*：削除するセッション番号を、1～4 の範囲で指定します。
デフォルト	なし
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.14.8 show monitor session

show monitor session	
目的	すべての、または特定のモニターセッションの設定情報を表示します。
シンタックス	**show monitor session** [*SESSION-NUMBER* | **remote** | **local**]

show monitor session	
パラメーター	*SESSION-NUMBER*（省略可能）：表示するセッション番号を、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。
デフォルト	なし
コマンドモード	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情報が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：セッション番号 1 のモニターセッションの設定情報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情報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: Port1/0/19 ...(4)
     Source Ports: ...(5)
         Both:
             Port1/0/10

 Session 4 ...(1)
     Session Type: remote destination session ...(2)
     Source Remote VLAN: VLAN 4090 ...(6)
     Destination Port: Port1/0/48 ...(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。

4.15 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。

コマンド	コマンドとパラメーター
lldp run	lldp run no lldp run
lldp transmit	lldp transmit no lldp transmit
lldp receive	lldp receive no lldp receive
lldp forward	lldp forward no lldp forward
lldp tx-delay	lldp tx-delay SECONDS no lldp tx-delay
lldp tx-interval	lldp tx-interval SECONDS no lldp tx-interval
lldp hold-multiplier	lldp hold-multiplier VALUE no hold-multiplier
lldp reinit	lldp reinit SECONDS no lldp reinit
lldp fast-count	lldp fast-count VALUE no lldp fast-count
lldp subtype port-id	lldp subtype port-id {mac-address | local}
lldp tlv-select	lldp tlv-select [port-description | system-capabilities | system-description | system-name] no lldp tlv-select [port-description | system-capabilities | system-description | system-name]
lldp management-address	lldp management-address [IP-ADDRESS | IPV6-ADDRESS] no lldp management-address [IP-ADDRESS | IPV6-ADDRESS]
lldp dot1-tlv-select	lldp dot1-tlv-select {port-vlan | protocol-vlan VLAN-ID [,|-] | vlan-name [VLAN-ID [,|-]] | protocol-identity [PROTOCOL-NAME]} no lldp dot1-tlv-select {port-vlan | protocol-vlan [VLAN-ID [,|-]] | vlan-name [VLAN-ID [,|-]] | protocol-identity [PROTOCOL-NAME]}
lldp dot3-tlv-select	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]
lldp med-tlv-select	lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management] no lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]

コマンド	コマンドとパラメーター
lldp err-disable	lldp err-disable no lldp err-disable
lldp notification enable	lldp notification enable no lldp notification enable
lldp med notification enable	lldp med notification enable no lldp med notification enable
snmp-server enable traps lldp	snmp-server enable traps lldp no snmp-server enable traps lldp
snmp-server enable traps lldp med	snmp-server enable traps lldp med no 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。

コマンド	コマンドとパラメーター
show lldp	show lldp
show lldp interface	show lldp interface INTERFACE-ID [,|-]
show lldp local interface	show lldp local interface INTERFACE-ID [,|-] [brief | detail]
show lldp management-address	show lldp management-address [IP-ADDRESS | IPV6-ADDRESS]
show lldp neighbors interface	show lldp neighbors interface INTERFACE-ID [,|-] [brief | detail]
show lldp traffic	show lldp traffic
show lldp traffic interface	show lldp traffic interface INTERFACE-ID [,|-]
clear lldp table	clear lldp table {all | interface INTERFACE-ID [,|-]}
clear lldp counters	clear lldp counters [all | interface INTERFACE-ID [,|-]]

4.15.1 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。
シンタックス	**lldp run** **no lldp run**
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	-

lldp run	
対象バージョン	1.01.01

使用例：LLDP 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)# lldp run
(config)#
```

4.15.2 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。
シンタックス	lldp transmit no lldp transmit
パラメーター	なし
デフォルト	有効（lldp transmit）
コマンドモード	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	-
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.15.3 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。
シンタックス	lldp receive no lldp receive
パラメーター	なし
デフォルト	有効（lldp receive）
コマンドモード	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	-
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.15.4 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。
シンタックス	**lldp forward** **no lldp forward**
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.5 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。
シンタックス	**lldp tx-delay** *SECONDS* **no lldp tx-delay**
パラメーター	*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
コマンドモード	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	-
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.6 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。
シンタックス	**lldp tx-interval** *SECONDS* **no lldp tx-interval**
パラメーター	*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
コマンドモード	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	-
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.7 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。
シンタックス	**lldp hold-multiplier** *VALUE* **no hold-multiplier**
パラメーター	*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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.8 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。
シンタックス	**lldp reinit** *SECONDS* **no lldp reinit**
パラメーター	*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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.9 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。
シンタックス	**lldp fast-count** *VALUE* **no lldp fast-count**
パラメーター	*VALUE*：LLDP-MED fast start 処理の実行回数を 1～10 の範囲で設定します。
デフォルト	4
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.10 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。

lldp subtype port-id	
シンタックス	lldp subtype port-id {mac-address | local}
パラメーター	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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.11 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。
シンタックス	lldp tlv-select [port-description | system-capabilities | system-description | system-name] no lldp tlv-select [port-description | system-capabilities | system-description | system-name]
パラメーター	port-description（省略可能）：Port Description TLV を通知する場合に指定します。 system-capabilities（省略可能）：System Capabilities TLV を通知する場合に指定します。 system-description（省略可能）：System Description TLV を通知する場合に指定します。 system-name（省略可能）：System Name TLV を通知する場合に指定します。
デフォルト	IEEE 802.1AB basic management set のオプション TLV は未選択
コマンドモード	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	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 lldp tlv-select を実行した場合は、すべての lldp tlv-select 設定が有効になります。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 lldp tlv-select 設定が削除され

lldp tlv-select	
	ます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.12 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。
シンタックス	**lldp management-address** [*IP-ADDRESS* | *IPV6-ADDRESS*] **no lldp management-address** [*IP-ADDRESS* | *IPV6-ADDRESS*]
パラメーター	*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。
デフォルト	設定なし（Management Address TLV は通知されない）
コマンドモード	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	**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。
制限事項	-
注意事項	「管理用 IP アドレスを指定した **lldp management-address** 設定」と「管理用 IP アドレスを指定しない **lldp management-address** 設定」を同時に設定した場合は、「管理用 IP アドレスを指定した **lldp management-address** 設定」のみ動作します。

lldp management-address	
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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 からポート 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)#
```

4.15.13 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。
シンタックス	**lldp dot1-tlv-select** {**port-vlan** | **protocol-vlan** *VLAN-ID* [,|-] | **vlan-name** [*VLAN-ID* [,|-]] | **protocol-identity** [*PROTOCOL-NAME*]} **no lldp dot1-tlv-select** {**port-vlan** | **protocol-vlan** [*VLAN-ID* [,|-]] | **vlan-name** [*VLAN-ID* [,|-]] | **protocol-identity** [*PROTOCOL-NAME*]}
パラメーター	**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 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 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** [*PROTOCOL-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
コマンドモード	インターフェース設定モード(port, range)
特権レベル	レベル：12

lldp dot1-tlv-select	
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。
制限事項	-
注意事項	**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。
対象バージョン	1.01.01

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)#
```

4.15.14 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。
シンタックス	**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]**
パラメーター	**mac-phy-cfg**（省略可能）：MAC/PHY Configuration/Status TLV を通知する場合

lldp dot3-tlv-select	
	に指定します。 link-aggregation（省略可能）：Link Aggregation TLV を通知する場合に指定します。 power（省略可能）：Power Via MDI TLV を通知する場合に指定します。PoE 対応ポートでのみ設定できます。 max-frame-size（省略可能）：Maximum Frame Size TLV を通知する場合に指定します。
デフォルト	IEEE 802.3 Organizationally Specific TLV は未選択
コマンドモード	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	パラメーターを指定しないで lldp dot3-tlv-select を実行した場合は、すべての lldp dot3-tlv-select 設定が有効になります。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 lldp dot3-tlv-select 設定が削除されます。
制限事項	-
注意事項	AEOS-NP2000 Ver. 1.05.01 以降では、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。
対象バージョン	1.01.01 1.05.01：power パラメーター追加

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)#
```

4.15.15 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。
シンタックス	lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management] no lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]
パラメーター	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）を通知する場合に指定します。 inventory-management（省略可能）：LLDP-MED Inventory Management TLV（LLDP-MED 対応機器の管理情報）を通知する場合に指定します。 network-policy（省略可能）：LLDP-MED Network Policy TLV を通知する場合に指定します。 power-management（省略可能）：LLDP-MED Extended Power-via-MDI TLV を通知する場合に指定します。PoE 対応ポートでのみ設定できます。
デフォルト	LLDP-MED TLV は未選択
コマンドモード	インターフェース設定モード(port, range)

lldp med-tlv-select	
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 **lldp med-tlv-select** を実行した場合は、すべての **lldp med-tlv-select** 設定が有効になります。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 **lldp med-tlv-select** 設定が削除されます。
制限事項	-
注意事項	AEOS-NP2000 Ver. 1.05.01 以降では、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。
対象バージョン	1.01.01 1.05.01：**power-management** パラメーター追加 1.08.02：**network-policy** パラメーター追加

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)#
```

4.15.16 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。
シンタックス	**lldp err-disable** **no lldp err-disable**

lldp err-disable	
パラメーター	なし
デフォルト	無効
コマンドモード	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	隣接するポート間の通信状態は、LLDPDU を使用してポートのリンク情報をネイバーに通知すること、および LLDPDU の受信状態と受信内容を判断することで確認できます。LLDP 疑似リンクダウン機能を有効にすると、リンクに障害が発生したことやリンクが復旧したことを、LLDPDU により検知した場合に、ポートを LLDP 疑似リンクダウン状態にしたり復旧したりできます。 Port-channel 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には、**show channel-group** 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には、**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)は errDis と表示され、その MMRP-Plus リングポートはダウンします。 LLDP 疑似リンクダウン状態の物理ポートでは、**show interfaces status** コマンドのステータスは connected と表示され、**show interfaces port** コマンド、もしくは **show interfaces description** コマンドのステータスは errDis と表示されます。
制限事項	-
注意事項	物理ポートの設定用のコマンドです。 LLDP 疑似リンクダウン機能と LACP をポートで併用することはできません。 物理ポートで LLDP 疑似リンクダウン機能と STP/RSTP/MSTP/RPVST+/ERPS 機能を併用することはできません。 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。
対象バージョン	1.03.01

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)#
```

4.15.17 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。
シンタックス	**lldp notification enable** **no lldp notification enable**
パラメーター	-
デフォルト	無効
コマンドモード	インターフェース設定モード(port, range)

lldp notification enable	
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.15.18 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。
シンタックス	lldp med notification enable no lldp med notification enable
パラメーター	-
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.15.19 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。
シンタックス	snmp-server enable traps lldp no snmp-server enable traps lldp
パラメーター	-
デフォルト	無効
コマンドモード	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	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

snmp-server enable traps lldp	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.20 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。
シンタックス	**snmp-server enable traps lldp med** **no snmp-server enable traps lldp med**
パラメーター	-
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.15.21 show lldp

show lldp	
目的	装置の一般的な LLDP 設定を表示します。
シンタックス	**show lldp**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-

show lldp	
制限事項	-
注意事項	-
対象バージョン	1.01.01

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                  : 00-40-66-B4-94-07 ...(2)
    System Name                 : Switch ...(3)
    System Description          : ApresiaNP2000-24T4X-PoE Gigabit Ethernet Switch
                                  Ver.1.09.01 ...(4)
    System Capabilities Supported: Bridge, Router ...(5)
    System Capabilities Enabled  : Bridge, Router ...(6)
LLDP-MED System Information:
    Device Class                : Network Connectivity Device ...(7)
    Hardware Revision           : A ...(8)
    Firmware Revision           : 1.00.00 ...(9)
    Software Revision           : 1.09.01 ...(10)
    Serial Number               : 188770000009 ...(11)
    Manufacturer Name           : APRESIA Systems, Ltd ...(12)
    Model Name                  : ApresiaNP2100-24T4X-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。
(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。

項番	説明
(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。PoE 機種でのみ表示されます。
(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。PoE 機種でのみ表示されます。
(17)	装置全体の LLDP 設定の有効／無効を表示します。
(18)	LLDP 転送の有効／無効を表示します。
(19)	LLDPDU の送信間隔を表示します。
(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を表示します。
(22)	LLDPDU の送信遅延間隔を設定します。
(23)	LLDP-MED fast start 処理の実行回数を表示します。

4.15.22 show lldp interface

show lldp interface	
目的	物理ポートの LLDP 設定を表示します。
シンタックス	**show lldp interface** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：LLDP 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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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	–
制限事項	–
注意事項	–
対象バージョン	1.01.01

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／無効を表示します。
(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／無効を表示します。
(7)	System Name TLV 付加の有効／無効を表示します。
(8)	System Description TLV 付加の有効／無効を表示します。
(9)	System Capabilities TLV 付加の有効／無効を表示します。
(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／無効を表示します。
(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／無効を表示します。
(16)	Power Via MDI TLV 付加の有効／無効を表示します。PoE 対応ポートでのみ表示されます。
(17)	Link Aggregation TLV 付加の有効／無効を表示します。

項番	説明
(18)	Maximum Frame Size TLV 付加の有効／無効を表示します。
(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／無効を表示します。
(20)	LLDP-MED Capabilities TLV 付加の有効／無効を表示します。
(21)	LLDP-MED Network Policy TLV 付加の有効／無効を表示します。
(22)	LLDP-MED Extended Power-via-MDI TLV 付加の有効／無効を表示します。
(23)	LLDP-MED Inventory Management TLV 付加の有効／無効を表示します。

4.15.23 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。
シンタックス	**show lldp local interface** *INTERFACE-ID* [,|-] [brief | detail]
パラメーター	*INTERFACE-ID*：物理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。
デフォルト	なし
コマンドモード	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	要約モードと詳細モードのどちらも指定しない場合、情報は標準モードで表示されます。
制限事項	–
注意事項	–
対象バージョン	1.01.01

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
                                               ApresiaNP2000-24T4X-PoE HW A
                                               firmware 1.09.01 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 ...(9)
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。
(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。
(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
                                                  ApresiaNP2000-24T4X-PoE HW A
                                                  firmware 1.09.01 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。
(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
                                                 ApresiaNP2000-24T4X-PoE HW A
                                                 firmware 1.09.01 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                                    : 1.3.6.1.4.1.278.1.42.3

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     : 6c01(hex)
    Auto-Negotiation Operational MAU Type      : 0000(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   :Not 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。
(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。
(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。

4.15.24 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。
シンタックス	**show lldp management-address** [*IP-ADDRESS* | *IPV6-ADDRESS*]
パラメーター	*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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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                                  : 1.3.6.1.4.1.278.1.42.3 ...(4)
    Advertising Ports                    : - ...(5)

Address 2 :
-----------------------------------------------
    Subtype                              : IPv4
    Address                              : 192.0.2.100
    IF Type                              : IfIndex
    OID                                  : 1.3.6.1.4.1.278.1.42.3
    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を表示します。 IPv4：IPv4 アドレス IPv6：IPv6 アドレス
(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。

4.15.25 show lldp neighbors interface

show lldp neighbors interface	
目的	隣接装置の LLDP 情報を表示します。
シンタックス	**show lldp neighbors interface** *INTERFACE-ID* [,|-] [brief | detail]
パラメーター	*INTERFACE-ID*：隣接装置の LLDP 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。
デフォルト	なし
コマンドモード	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	要約モードと詳細モードのどちらも指定しない場合、情報は標準モードで表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/15 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 1/0/15
```

```
Port ID: Port1/0/15 ...(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。
(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。

項番	説明
(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。
(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 1/0/15 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 1/0/15 brief

Port ID: Port1/0/15 ...(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。
(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 1/0/15 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 1/0/15 detail

Port ID: Port1/0/15 ...(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。

項番	説明
(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。
(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。

4.15.26 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。
シンタックス	show lldp traffic
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

項番	説明
(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。

4.15.27 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。
シンタックス	**show lldp traffic interface** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：LLDP 統計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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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	–
制限事項	–
注意事項	–
対象バージョン	1.01.01

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。

4.15.28 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。
シンタックス	clear lldp table {all | interface *INTERFACE-ID* [,|-]}
パラメーター	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 *INTERFACE-ID*：LLDP 情報を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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

4.15.29 clear lldp counters

clear lldp counters	
目的	LLDP 統計情報を消去します。
シンタックス	clear lldp counters [all | interface *INTERFACE-ID* [,|-]]
パラメーター	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 *INTERFACE-ID*（省略可能）：LLDP 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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	パラメーターを指定しない場合は、グローバルな LLDP 統計情報のみが消去されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

4.16 EtherOAM コマンド

EtherOAM 関連の設定コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ethernet oam	ethernet oam no ethernet oam
ethernet oam mode	ethernet oam mode {active | passive} no ethernet oam mode
ethernet oam link-monitor error-symbol	ethernet oam link-monitor error-symbol [threshold NUMBER] [window DECISECONDS] no ethernet oam link-monitor error-symbol [threshold | window]
ethernet oam link-monitor error-frame	ethernet oam link-monitor error-frame [threshold NUMBER] [window DECISECONDS] no ethernet oam link-monitor error-frame [threshold | window]
ethernet oam link-monitor error-frame-seconds	ethernet oam link-monitor error-frame-seconds [threshold NUMBER] [window DECISECONDS] no ethernet oam link-monitor error-frame-seconds [threshold | window]
ethernet oam link-monitor error-frame-period	ethernet oam link-monitor error-frame-period [threshold NUMBER] [window NUMBER] no ethernet oam link-monitor error-frame-period [threshold | window]
ethernet oam remote-failure critical-event	ethernet oam remote-failure critical-event no ethernet oam remote-failure critical-event

EtherOAM 関連の show／操作コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show ethernet oam configuration	show ethernet oam configuration [interface INTERFACE-ID [,|-]]
show ethernet oam status	show ethernet oam status [interface INTERFACE-ID [,|-]]
show ethernet oam statistics	show ethernet oam statistics [interface INTERFACE-ID [,|-]]
show ethernet oam event-log	show ethernet oam event-log [interface INTERFACE-ID [,|-]]
clear ethernet oam statistics	clear ethernet oam statistics [interface INTERFACE-ID [,|-]]
clear ethernet oam event-log	clear ethernet oam event-log [interface INTERFACE-ID [,|-]]
ethernet oam remote-loopback	ethernet oam remote-loopback {start | stop} interface INTERFACE-ID [,|-]
ethernet oam received-remote-loopback	ethernet oam received-remote-loopback {process | ignore}

4.16.1 ethernet oam

ethernet oam	
目的	指定したインターフェースで EtherOAM 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。
シンタックス	ethernet oam no ethernet oam
パラメーター	なし
デフォルト	無効
コマンドモード	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	インターフェースの EtherOAM 機能を有効にすると、インターフェースは EtherOAM ディスカバリーを開始します。EtherOAM 機能を有効にしたインターフェースの EtherOAM の動作モードがアクティブな場合、インターフェースはディスカバリーを開始します。インターフェースの EtherOAM の動作モードがアクティブではない場合、インターフェースは隣接装置から受信したディスカバリーを受けて動作します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 で EtherOAM 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)#
```

4.16.2 ethernet oam mode

ethernet oam mode	
目的	指定したインターフェースで EtherOAM の動作モードを構成します。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。
シンタックス	ethernet oam mode {active | passive} no ethernet oam mode
パラメーター	active：インターフェースの EtherOAM の動作モードをアクティブモードに設定する場合に指定します。 passive：インターフェースの EtherOAM の動作モードを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
コマンドモード	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	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。 • EtherOAM ディスカバリーの開始 • リモートループバックの開始または停止
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の EtherOAM の動作モードをアクティブに構成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)#
```

4.16.3 ethernet oam link-monitor error-symbol

ethernet oam link-monitor error-symbol	
目的	エラーシンボルイベントの通知を有効にして、指定したインターフェースの監視上限値とウィンドウを構成します。イベントの通知を無効にして、パラメーターを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。
シンタックス	ethernet oam link-monitor error-symbol [threshold *NUMBER*] [window *DECISECONDS*] no ethernet oam link-monitor error-symbol [threshold | window]
パラメーター	threshold *NUMBER*（省略可能）：シンボルエラー回数を 0～4,294,967,295 の範囲で指定します。window で指定した期間内のシンボルエラー回数が上限値を超えた場合、エラーシンボルイベントが発行されます。 window *DECISECONDS*（省略可能）：上限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。指定した期間内のシンボルエラー回数が上限値を超えた場合、エラーシンボルイベント通知がエラーシンボル期間イベント TLV と合わせて発行されます。
デフォルト	エラーシンボルイベント：通知 エラーシンボル監視上限値：1 エラーシンボル監視ウィンドウ：10（1 秒）
コマンドモード	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	リンク監視機能は、指定したウィンドウ期間中に発生したシンボルエラーの数をカウントします。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 でエラーシンボ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 link-monitor error-symbol
(config-if-port)#
```

使用例：ポート 1/0/1 でエラーシンボルイベントの通知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 のエラーシンボル監視上限値を、100 に構成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
(config-if-port)#
```

使用例：ポート 1/0/1 のエラーシンボル監視ウィンドウを、100（10 秒）に構成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 window 100
(config-if-port)#
```

使用例：ポート 1/0/1 のエラーシンボル監視上限値を、デフォルトに構成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 threshold
(config-if-port)#
```

4.16.4 ethernet oam link-monitor error-frame

ethernet oam link-monitor error-frame	
目的	エラーフレームイベントの通知を有効にして、指定したインターフェースの監視上限値とウィンドウを構成します。イベントの通知を無効にして、パラメーターを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。
シンタックス	**ethernet oam link-monitor error-frame** [**threshold** *NUMBER*] [**window** *DECISECONDS*] **no ethernet oam link-monitor error-frame** [**threshold** | **window**]
パラメーター	**threshold** *NUMBER*（省略可能）：フレームエラー回数を 0～4,294,967,295 の範囲で指定します。**window** で指定した期間内のフレームエラー回数が上限値を超えた場合、エラーフレームイベントが発行されます。 **window** *DECISECONDS*（省略可能）：上限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。指定した期間内のフレームエラー回数が上限値を超えた場合、エラーフレームイベント通知がエラーフレームイベント TLV と合わせて発行されます。
デフォルト	エラーフレームイベント：通知 エラーフレーム監視上限値：1 エラーフレーム監視ウィンドウ：10（1 秒）
コマンドモード	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	リンク監視機能は、指定したウィンドウ期間中に検知されたエラーフレームの数をカウントします。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 でエラーフレーム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 link-monitor error-frame
(config-if-port)#
```

使用例：ポート 1/0/1 でエラーフレームイベントの通知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 のエラーフレーム監視上限値を、100 に構成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
(config-if-port)#
```

使用例：ポート 1/0/1 のエラーフレーム監視ウィンドウを、100（10 秒）に構成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 window 100
(config-if-port)#
```

使用例：ポート 1/0/1 のエラーフレーム監視ウィンドウを、デフォルトに構成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 window
(config-if-port)#
```

4.16.5 ethernet oam link-monitor error-frame-seconds

ethernet oam link-monitor error-frame-seconds	
目的	エラーフレーム秒イベントの通知を有効にして、指定したインターフェースの監視上限値とウィンドウを構成します。イベントの通知を無効にして、パラメーターを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。
シンタックス	ethernet oam link-monitor error-frame-seconds [threshold *NUMBER*] [window *DECISECONDS*] no ethernet oam link-monitor error-frame-seconds [threshold | window]
パラメーター	threshold *NUMBER*（省略可能）：フレームエラー秒数を 1～900 秒の範囲で指定します。window で指定した期間内のフレームエラー秒数が上限値を超えた場合、エラーフレーム秒イベントが発行されます。 window *DECISECONDS*（省略可能）：上限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。指定した期間内のフレームエラー秒数が上限値を超えた場合、エラーフレーム秒イベント通知がエラーフレーム秒要約イベント TLV と合わせて発行されます。
デフォルト	エラーフレーム秒イベント：通知 エラーフレーム秒監視上限値：1 エラーフレーム秒監視ウィンドウ：600（60 秒）
コマンドモード	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	リンク監視機能は、指定したウィンドウ期間中に発生したエラーフレームの数をカウントします。エラーフレームの数が指定したウィンドウ期間の上限値以上になった場合、イベントが出力されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 でエラーフレーム秒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 link-monitor error-frame-seconds
```

```
(config-if-port)#
```

使用例：ポート 1/0/1 でエラーフレーム秒イベントの通知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 のエラーフレーム秒監視上限値を、100 に構成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 100
(config-if-port)#
```

使用例：ポート 1/0/1 のエラーフレーム秒監視ウィンドウを、100（10 秒）に構成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 window 100
(config-if-port)#
```

使用例：ポート 1/0/1 のエラーフレーム秒監視上限値を、デフォルトに構成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 threshold
(config-if-port)#
```

4.16.6 ethernet oam link-monitor error-frame-period

ethernet oam link-monitor error-frame-period	
目的	エラーフレーム期間イベントの通知を有効にして、指定したインターフェースの監視上限値とウィンドウを構成します。イベントの通知を無効にして、パラメーターを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。
シンタックス	ethernet oam link-monitor error-frame-period [threshold *NUMBER*] [window *NUMBER*] no ethernet oam link-monitor error-frame-period [threshold | window]
パラメーター	threshold *NUMBER*（省略可能）：フレームエラー回数を、0～4,294,967,295 の範囲で指定します。window で指定したフレーム数内のフレームエラー回数が上限値を超えた場合、エラーフレーム期間イベントが発行されます。 window *NUMBER*（省略可能）：上限値を定義する対象のフレーム数を指定します。指定したフレーム数内のフレームエラー回数が上限値を超えた場合、エラーフレーム期間イベント通知がエラーフレーム期間イベント TLV と合わせて発行されます。設定範囲は、「基盤となる物理レイヤーで 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」～「基盤となる物理レイヤーで 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	エラーフレーム期間イベント：通知 エラーフレーム期間監視上限値：1 ウィンドウ値は基盤となる物理レイヤーで 1 秒間に受信できる最小フレームサイズのフレーム数
コマンドモード	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	リンク監視機能は、指定した期間中に検知されたエラーフレームの数をカウントします。

ethernet oam link-monitor error-frame-period	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 でエラーフレーム期間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 link-monitor error-frame-period
(config-if-port)#
```

使用例：ポート 1/0/1 でエラーフレーム期間イベントの通知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 のエラーフレーム期間監視上限値を、100 に構成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
(config-if-port)#
```

使用例：ポート 1/0/1 のエラーフレーム期間監視ウィンドウを、1488100 フレームに構成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 window 1488100
(config-if-port)#
```

使用例：ポート 1/0/1 のエラーフレーム期間監視上限値を、デフォルトに構成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 threshold
(config-if-port)#
```

4.16.7 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。
シンタックス	ethernet oam remote-failure critical-event no ethernet oam remote-failure critical-event
パラメーター	なし
デフォルト	有効（ethernet oam remote-failure critical-event）
コマンドモード	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	クリティカルイベントの機能が無効の場合、未指定のクリティカルイベントが発生したときに、インターフェースはクリティカルイベントビットがセットされた EtherOAM フレームを送出しません。
制限事項	-

ethernet oam remote-failure critical-event	
注意事項	-
対象バージョン	1.01.01

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)#
```

4.16.8 show ethernet oam configuration

show ethernet oam configuration	
目的	EtherOAM 機能の構成を表示します。
シンタックス	**show ethernet oam configuration** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：構成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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の EtherOAM 構成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)	EtherOAM の有効／無効を表示します。
(3)	EtherOAM の動作モードを表示します。 Active：アクティブ Passive：パッシブ
(4)	Dying Gasp イベント通知の有効／無効を表示します。
(5)	クリティカルイベント通知の有効／無効を表示します。
(6)	リモートループバック要求に対する動作を表示します。 Processed：応答 Not Processed：無視
(7)	エラーシンボルイベントに関する情報を表示します。
(8)	通知の有効／無効を表示します。
(9)	数量を監視する単位時間を表示します。
(10)	上限値を表示します。
(11)	エラーフレームイベントに関する情報を表示します。
(12)	エラーフレーム期間イベントに関する情報を表示します。
(13)	エラーフレーム秒イベントに関する情報を表示します。

4.16.9 show ethernet oam status

show ethernet oam status	
目的	EtherOAM のプライマリー制御と状態の情報を表示します。
シンタックス	**show ethernet oam status** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：状態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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の EtherOAM 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)	ローカルの装置の情報を表示します。
(3)	EtherOAM の有効／無効を表示します。
(4)	EtherOAM の動作モードを表示します。 Active：アクティブ Passive：パッシブ
(5)	EtherOAM フレームの最大サイズを表示します。 EtherOAM フレームの最大サイズを交換して、隣接装置間の最大サイズのうち、小さい方が使用されます。
(6)	リモートループバック機能の対応状況を表示します。 Supported：対応 Not supported：非対応
(7)	単方向リンクにおける EtherOAM フレーム送信機能の対応状況を表示します。 Supported：対応 Not supported：非対応
(8)	イベント通知機能の対応状況を表示します。 Supported：対応 Not supported：非対応
(9)	Ethernet MIB で記述されている属性値の参照機能の対応状況を表示します。 Supported：対応 Not supported：非対応
(10)	EtherOAM フレームのリビジョンを表示します。 リビジョンは、構成が変更されたか、隣接装置間の接続が許可された際、再評価の必要性を示すために使用される値です。
(11)	インターフェースの EtherOAM に関するステータスを表示します。 Disable：EtherOAM が無効 LinkFault：リンク障害を検知 PassiveWait：インターフェースがパッシブで、隣接装置が EtherOAM に対応しているか確認中 ActiveSendLocal：インターフェースがアクティブで、情報を送信中 SendLocalAndRemote：隣接装置を検出済み（設定待ち） SendLocalAndRemoteOk：隣接装置を検出済み（設定済み） PeeringLocallyRejected：隣接装置から受信したリモートループバックモード設定要求をローカルの装置が拒否 PeeringRemotelyRejected：ローカルの装置から送信したリモートループバックモード設

項番	説明
	定要求を隣接装置が拒否 Operational：EtherOAM を利用可能（装置自身と隣接装置の両方が接続を受け入れたことを学習） NonOperHalfDuplex：EtherOAM を利用可能（インターフェースが半二重動作のため不完全動作）
(12)	ループバックのステータスを表示します。
(13)	隣接装置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。

4.16.10 show ethernet oam statistics

show ethernet oam statistics	
目的	EtherOAM 機能の統計情報を表示します。
シンタックス	**show ethernet oam statistics** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：統計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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	–
対象バージョン	1.01.01

使用例：ポート 1/0/1 の EtherOAM 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。

項番	説明
(2)	情報フレームの送信フレーム数を表示します。
(3)	情報フレームの受信フレーム数を表示します。
(4)	ユニークなイベント通知フレームの送信フレーム数を表示します。
(5)	ユニークなイベント通知フレームの受信フレーム数を表示します。
(6)	重複したイベント通知フレームの送信フレーム数を表示します。
(7)	重複したイベント通知フレームの受信フレーム数を表示します。
(8)	ループバック制御フレームの送信フレーム数を表示します。
(9)	ループバック制御フレームの受信フレーム数を表示します。
(10)	MIB 変数要求フレームの送信フレーム数を表示します。
(11)	MIB 変数要求フレームの受信フレーム数を表示します。
(12)	MIB 変数応答フレームの送信フレーム数を表示します。
(13)	MIB 変数応答フレームの受信フレーム数を表示します。
(14)	ベンダー独自フレームの送信フレーム数を表示します。
(15)	ベンダー独自フレームの受信フレーム数を表示します。
(16)	非対応フレームの送信フレーム数を表示します。
(17)	非対応フレームの受信フレーム数を表示します。
(18)	EtherOAM によって廃棄されたフレーム数を表示します。

4.16.11 show ethernet oam event-log

show ethernet oam event-log	
目的	EtherOAM 機能のイベントログを表示します。
シンタックス	**show ethernet oam event-log** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：イベントログ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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の EtherOAM 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
```

```
      0 Critical Event records

    Local event logs: ...(7)
    -------------
      0 Errored Symbol records ...(8)
      0 Errored Frame records ...(9)
      0 Errored Frame Period records ...(10)
      0 Errored Frame Second records ...(11)

    Remote event logs: ...(12)
    -------------
      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)	ローカルの装置における失敗ログの数を表示します。
(3)	リンクエラーログの数を表示します。
(4)	Dying Gasp ログの数を表示します。
(5)	クリティカルイベントログの数を表示します。
(6)	隣接装置における失敗ログの数を表示します。
(7)	ローカルの装置におけるイベントログの数を表示します。
(8)	エラーシンボルイベントログの数を表示します。
(9)	エラーフレームイベントログの数を表示します。
(10)	エラーフレーム期間イベントログの数を表示します。
(11)	エラーフレーム秒イベントログの数を表示します。
(12)	隣接装置におけるイベントログの数を表示します。

4.16.12 clear ethernet oam statistics

clear ethernet oam statistics	
目的	EtherOAM 機能の統計情報を消去します。
シンタックス	**clear ethernet oam statistics** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の EtherOAM 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
#
```

4.16.13 clear ethernet oam event-log

clear ethernet oam event-log	
目的	EtherOAM 機能のイベントログを消去します。
シンタックス	clear ethernet oam event-log [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID*（省略可能）：イベントログ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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の EtherOAM イベントログを消去する方法を示します。

```
# clear ethernet oam event-log interface port 1/0/1
#
```

4.16.14 ethernet oam remote-loopback

ethernet oam remote-loopback	
目的	指定したインターフェースでリモートループバックのアクションを設定します。
シンタックス	ethernet oam remote-loopback {start | stop} interface *INTERFACE-ID* [,|-]
パラメーター	start：隣接装置へループバックモードの開始を要求する場合に指定します。 stop：隣接装置へループバックモードの終了（通常動作モードへの変更）を要求する場合に指定します。 interface *INTERFACE-ID*：リモートループバックアクションを実行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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	EtherOAM リモートループバックモードの開始を隣接装置に要求する場合、ethernet oam remote-loopback start コマンドを使用します。 EtherOAM リモートループバックモードの終了を隣接装置に要求する場合、ethernet oam remote-loopback stop コマンドを使用します。 リモートループバック要求を無視するように隣接装置が構成されている場合、隣接装置は要求を受信しても、リモートループバックモードを開始または終了しません。
制限事項	-
注意事項	隣接装置でリモートループバックモードが開始されるようにするには、ローカルクライアントがアクティブモードで、EtherOAM 接続が確立されていることを管理者が確認してください。ローカルクライアントがすでにリモートループバックモードの場合、コマンドは適用できません。

ethernet oam remote-loopback	
対象バージョン	1.01.01

使用例：ポート 1/0/1 で EtherOAM リモートループバックを開始する方法を示します。

```
# ethernet oam remote-loopback start interface port 1/0/1
```

4.16.15 ethernet oam received-remote-loopback

ethernet oam received-remote-loopback	
目的	指定したインターフェースで、隣接装置から受信したリモートループバック要求の動作を構成します。
シンタックス	ethernet oam received-remote-loopback {process | ignore}
パラメーター	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要求を無視）
コマンドモード	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	ethernet oam remote-loopback コマンドを処理または無視するように、クライアントを構成するコマンドです。 リモートループバックモードでは、すべてのユーザートラフィックは処理されません。ethernet oam remote-loopback コマンドを無視した場合、指定したインターフェースでリモートループバックモードが開始されません。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 で ethernet oam remote-loopback コマンドの処理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 received-remote-loopback process
(config-if-port)#
```

4.17 単方向リンク検出(ULD)コマンド

単方向リンク検出(ULD)関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
uld enable	uld enable no uld enable
uld action	uld action shutdown no uld action
uld discovery-time	uld discovery-time SECONDS no uld discovery-time
errdisable recovery cause uld	errdisable recovery cause uld [interval SECONDS] no errdisable recovery cause uld [interval]
show uld	show uld [interface INTERFACE-ID [,|-]]

4.17.1 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。
シンタックス	uld enable no uld enable
パラメーター	なし
デフォルト	無効
コマンドモード	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	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 EtherOAM 機能を有効にしてください。 単方向リンク検出は、802.3ah EtherOAM の拡張機能です。検出にはベンダー固有のメッセージ（Organization Specific Information TLV）が使用されます。 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 プロセスが完了しなくても指定した時間経過した後に開始されます。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：ポート 1/0/1 で、EtherOAM 機能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)#
```

4.17.2 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。
シンタックス	uld action shutdown no uld action
パラメーター	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）
コマンドモード	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	本コマンドが無効の場合でも、単方向リンクを検出するとシャットダウンはされませんがログは出力されます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.17.3 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。
シンタックス	uld discovery-time *SECONDS* no uld discovery-time
パラメーター	*SECONDS*：Discovery プロセスの完了待機時間を、5～65,535 秒の範囲で指定します。
デフォルト	5 秒
コマンドモード	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	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 EthernetOAM フレームを受信すると、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

uld discovery-time	
	リンク検出プロセスは開始されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.17.4 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。
シンタックス	**errdisable recovery cause uld** [**interval** *SECONDS*] **no errdisable recovery cause uld** [**interval**]
パラメーター	**interval** *SECONDS*（省略可能）：err-disabled 状態になってから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
コマンドモード	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	本コマンドの詳細や関連する show コマンドは「10.2 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。また、**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。
制限事項	本コマンドは、構成情報ではエラー復旧コマンド（ラベル# ERRDISABLE）で表示されます。
注意事項	**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。
対象バージョン	1.07.01

使用例：単方向リンク検出機能によって err-disabled 状態に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)#
```

4.17.5 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。
シンタックス	show uld [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID*（省略可能）：単方向リンク検出機能の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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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／無効を表示します。 Enabled：有効 Disabled：無効
(3)	動作状態を表示します。 Enabled：対応した EthernetOAM フレームを受信している状態 Disabled：対応した EthernetOAM フレームを未受信の状態
(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対象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：受信方向の単方向リンク（双方向通信不可の場合も含む）を検出した状態 TX Fault：送信方向の単方向リンクを検出した状態 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。

4.18 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。

コマンド	コマンドとパラメーター
cfm global enable	cfm global enable no cfm global enable
cfm enable	cfm enable no cfm enable
cfm domain	cfm domain DOMAIN-NAME level LEVEL no cfm domain DOMAIN-NAME
mip creation (MD)	mip creation {none | auto | explicit} no mip creation
sender-id (MD)	sender-id {none | chassis | manage | chassis-manage} no sender-id
cfm ma	cfm ma name MA-NAME [vlan VLAN-ID] no cfm ma name MA-NAME
mepid-list	mepid-list {add | delete} MEPID-LIST
ccm interval	ccm interval INTERVAL no ccm interval
mip creation (MA)	mip creation {none | auto | explicit | defer} no mip creation
sender-id (MA)	sender-id {none | chassis | manage | chassis-manage | defer} no sender-id
cfm mep	cfm mep mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME [direction {up | down}] no cfm mep mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME
mep enable	mep enable no mep enable
ccm enable	ccm enable no ccm enable
pdu-priority	pdu-priority COS-VALUE no pdu-priority
fault-alarm	fault-alarm {none | all | mac-status | remote-ccm | error-ccm | xcon-ccm} no fault-alarm
alarm-time	alarm-time {delay CENTISECOND | reset CENTISECOND} no alarm-time {delay | reset}
ais	ais [period PERIOD] [level LEVEL] no ais [period | level]
lck	lck [period PERIOD] [level LEVEL] no lck [period | level]

コマンド	コマンドとパラメーター
cfm mp-ltr-all	cfm mp-ltr-all no 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。

コマンド	コマンドとパラメーター
show cfm	show cfm
show cfm interface	show cfm interface [INTERFACE-ID [,|-]]
show cfm domain	show cfm domain DOMAIN-NAME
show cfm ma	show cfm ma name MA-NAME domain DOMAIN-NAME
show cfm mepid	show cfm mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME
show cfm mep fault	show cfm mep fault
show cfm counter ccm	show cfm counter ccm
show cfm remote-mep	show cfm remote-mep mepid LOCAL-MEP-ID ma name MA-NAME domain DOMAIN-NAME [remote-mepid REMOTE-MEPID]
show cfm mip ccm	show cfm mip ccm
show cfm pkt-cnt interface	show cfm pkt-cnt interface [INTERFACE-ID [,|-]] [rx] [tx]
show cfm mp-ltr-all	show cfm mp-ltr-all
cfm lck start / cfm lck stop	cfm lck start mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME cfm lck stop mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME
clear cfm counter ccm	clear cfm counter ccm
clear cfm pkt-cnt interface	clear cfm pkt-cnt interface {INTERFACE-ID [,|-] | all} [rx] [tx]

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。

コマンド	コマンドとパラメーター
cfm loopback test	cfm loopback test {MAC-ADDRESS | remote-mepid REMOTE-MEPID} mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME [num NUMBER] [length LENGTH | pattern STRING] [pdu-priority COS-VALUE]
cfm linktrace	cfm linktrace MAC-ADDRESS mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME [ttl TTL] [pdu-priority COS-VALUE]
show cfm linktrace	show cfm linktrace [mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME [trans-id ID]]
clear cfm linktrace	clear cfm linktrace {mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME | all}

4.18.1 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。

cfm global enable	
シンタックス	cfm global enable no cfm global enable
パラメーター	なし
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.18.2 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。
シンタックス	cfm enable no cfm enable
パラメーター	なし
デフォルト	無効
コマンドモード	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	CFM 機能で使用する各 CFM パケットは VLAN タグが付与された形式で送信されるため、CFM 機能を使用する場合、CFM パケットを送受信するポートはトランクポート(switchport mode trunk)に設定してください。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.18.3 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。

cfm domain	
シンタックス	**cfm domain** *DOMAIN-NAME* **level** *LEVEL* **no cfm domain** *DOMAIN-NAME*
パラメーター	**domain** *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** *LEVEL*：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
コマンドモード	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	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。
制限事項	リングプロテクション(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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.18.4 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。
シンタックス	**mip creation {none | auto | explicit}** **no mip creation**
パラメーター	**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 と同一 VLAN ID でより低い MD レベルの MA が存在しない場合に、対象 MA のポートに MIP を作成します。対象 MA と同一 VLAN ID でより低い MD レベルの MA が存在する場合には、以下のすべての条件を満たす対象 MA のポートに MIP を作成します。 • 対象 MA と同一 VLAN ID で、対象の MD レベルより次に低い MD レベルの MA のポートに MEP が設定されている。 • 対象 MA のポートに MEP が設定されていない。 • 対象 MA と同一 VLAN ID で、対象の MD レベルより高い MD レベルの MA が存在する場合には、その MA のポートに MEP が設定されていない。 **explicit**：対象 MA と同一 VLAN ID でより低い MD レベルの MA が存在し、さらに以下のすべての条件を満たす場合に対象 MA のポートに MIP を作成します。 • 対象 MA と同一 VLAN ID で、対象の MD レベルより次に低い MD レベルの

mip creation (MD)	
	MA のポートに MEP が設定されている。 • 対象 MA のポートに MEP が設定されていない。 • 対象 MA と同一 VLAN ID で、対象の MD レベルより高い MD レベルの MA が存在する場合には、その MA のポートに MEP が設定されていない。
デフォルト	none
コマンドモード	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。
制限事項	MA 内の中間装置では、装置上で MIP が作成できるように **auto** を指定してください。 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。
注意事項	-
対象バージョン	1.01.01

使用例：MIP 作成を「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)#
```

4.18.5 sender-id (MD)

sender-id (MD)	
目的	CFM MD 設定モードにおける、CFM パケットへの 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。
シンタックス	**sender-id {none | chassis | manage | chassis-manage}** **no sender-id**
パラメーター	**none**：CFM パケットに Sender ID TLV を付加しない場合に指定します。 **chassis**：CFM パケットに Chassis ID 情報を含んだ Sender ID TLV を付加する場合に指定します。 **manage**：CFM パケットに Management Address 情報を含んだ Sender ID TLV を付加する場合に指定します。 **chassis-manage**：CFM パケットに Chassis ID 情報と Management Address 情報を含んだ Sender ID TLV を付加する場合に指定します。
デフォルト	none
コマンドモード	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かは、CFM MA 設定モードの **sender-id** コマンドで設定します。
制限事項	-

sender-id (MD)	
注意事項	-
対象バージョン	1.01.01

使用例：MD 名が op-domain の MD において、CFM パケットに Chassis ID 情報を含んだ 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)#
```

4.18.6 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。
シンタックス	**cfm ma name** *MA-NAME* [**vlan** *VLAN-ID*] **no cfm ma name** *MA-NAME*
パラメーター	**name** *MA-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
コマンドモード	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** パラメーターの指定は不要です。 同一 MD に複数の MA を設定する場合は、一意の MA 名を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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.18.7 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。

mepid-list	
シンタックス	**mepid-list** {**add** | **delete**} *MEPID-LIST*
パラメーター	**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。 *MEPID-LIST*：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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.18.8 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。
シンタックス	**ccm interval** *INTERVAL* **no ccm interval**
パラメーター	*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**
コマンドモード	CFM MA 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

4.18.9 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。
シンタックス	mip creation {none | auto | explicit | defer} no mip creation
パラメーター	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 と同一 VLAN ID でより低い MD レベルの MA が存在しない場合に、対象 MA のポートに MIP を作成します。対象 MA と同一 VLAN ID でより低い MD レベルの MA が存在する場合には、以下のすべての条件を満たす対象 MA のポートに MIP を作成します。 • 対象 MA と同一 VLAN ID で、対象の MD レベルより次に低い MD レベルの MA のポートに MEP が設定されている。 • 対象 MA のポートに MEP が設定されていない。 • 対象 MA と同一 VLAN ID で、対象の MD レベルより高い MD レベルの MA が存在する場合には、その MA のポートに MEP が設定されていない。 explicit：対象 MA と同一 VLAN ID でより低い MD レベルの MA が存在し、さらに以下のすべての条件を満たす場合に対象 MA のポートに MIP を作成します。 • 対象 MA と同一 VLAN ID で、対象の MD レベルより次に低い MD レベルの MA のポートに MEP が設定されている。 • 対象 MA のポートに MEP が設定されていない。 • 対象 MA と同一 VLAN ID で、対象の MD レベルより高い MD レベルの MA が存在する場合には、その MA のポートに MEP が設定されていない。 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
コマンドモード	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。
制限事項	MA 内の中間装置では、装置上で MIP が作成できるように auto を指定してください。 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。
注意事項	-
対象バージョン	1.01.01

使用例：MA の MIP 作成を「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)#
```

4.18.10 sender-id (MA)

sender-id (MA)	
目的	CFM MA 設定モードにおける、CFM パケットへの 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。
シンタックス	**sender-id** {**none** | **chassis** | **manage** | **chassis-manage** | **defer**} **no sender-id**
パラメーター	**none**：CFM パケットに Sender ID TLV を付加しない場合に指定します。 **chassis**：CFM パケットに Chassis ID 情報を含んだ Sender ID TLV を付加する場合に指定します。 **manage**：CFM パケットに Management Address 情報を含んだ Sender ID TLV を付加する場合に指定します。 **chassis-manage**：CFM パケットに Chassis ID 情報と Management Address 情報を含んだ 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**
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MD 名が op-domain で MA 名が op-ma1 の MA において、CFM パケットに Chassis ID 情報を含んだ 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)#
```

4.18.11 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。
シンタックス	**cfm mep mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**direction** {**up** | **down**}] **no cfm mep mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*
パラメーター	**mepid** *MEP-ID*：MEP ID を 1～8191 の範囲で指定します。 **name** *MA-NAME*：MA 名を指定します。 **domain** *DOMAIN-NAME*：MD 名を指定します。 **direction**（省略可能）：MEP の方向を指定します。以下のいずれかを選択しま

cfm mep	
	す。MEP の作成時には MEP の方向を指定してください。指定しない場合、存在していた MEP の CFM MEP 設定モードに遷移します。 • up：対象ポートの装置内部方向で CFM パケットを送受信する 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 パケットを送受信する Down MEP を作成する場合に指定します。
デフォルト	なし
コマンドモード	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 パラメーターの指定は不要です。 同一 MA に複数の MEP を設定する場合は、一意の MEP ID を設定する必要があります。 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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

4.18.12 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。
シンタックス	mep enable no mep enable
パラメーター	なし
デフォルト	無効
コマンドモード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	-

mep enable	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MEP 状態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 mep mepid 1 ma name op1 domain op-domain
(config-cfm-mep)# mep enable
(config-cfm-mep)#
```

4.18.13 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。
シンタックス	**ccm enable** **no ccm enable**
パラメーター	なし
デフォルト	無効
コマンドモード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MEP の CCM 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 mep mepid 1 ma name op1 domain op-domain
(config-cfm-mep)# ccm enable
(config-cfm-mep)#
```

4.18.14 pdu-priority

pdu-priority	
目的	MEP によって送信される CCM とその他の CFM パケットで設定する IEEE 802.1p 優先度を定義します。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。
シンタックス	**pdu-priority** *COS-VALUE* **no pdu-priority**
パラメーター	*COS-VALUE*：MEP によって送信される CCM とその他の CFM パケットの IEEE 802.1p 優先度を 0～7 の範囲で指定します。
デフォルト	7
コマンドモード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	-

pdu-priority	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MEP によって送信される CCM と LTM メッセージで設定する IEEE 802.1p 優先度の定義方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name op1 domain op-domain
(config-cfm-mep)# pdu-priority 2
(config-cfm-mep)#
```

4.18.15 fault-alarm

fault-alarm	
目的	MEP によって送信される障害アラームのタイプを制御します。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。
シンタックス	fault-alarm {none | all | mac-status | remote-ccm | error-ccm | xcon-ccm} no fault-alarm
パラメーター	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
コマンドモード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	障害の優先度は以下のとおりです。 • （最低）*DefRDICCM*：リモート MEP からこの MEP が最後に受信した、RDI ビットが設定された CCM を受信しています。 • *DefMACstatus*：リモート MEP からこの MEP が最後に受信した CCM は、リモート MEP の関連する MAC がポートステータス TLV またはインターフェースステータス TLV で障害を報告していることを示しています。 • *DefRemoteCCM*：この MEP は、設定したリスト内の他の MEP から CCM を受信していません。 • *DefErrorCCM*：この MEP は無効な CCM を受信しています。 • （最高）*DefXconCCM*：この MEP は他の MA からの CCM を受信しています。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：すべてのタイプの障害アラームを送信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 op1 domain op-domain
(config-cfm-mep)# fault-alarm all
(config-cfm-mep)#
```

4.18.16 alarm-time

alarm-time	
目的	障害アラームを送信するまでの期間、および障害アラームをリセットするまでの期間を定義します。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。
シンタックス	**alarm-time** {**delay** *CENTISECOND* | **reset** *CENTISECOND*} **no alarm-time** {**delay** | **reset**}
パラメーター	**delay** *CENTISECOND*：MEP で障害が検出されてから、障害アラームを送信するまでの期間を、250～1000 の範囲で指定します。単位は 100 分の 1 秒です。 **reset** *CENTISECOND*：MEP で検出され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期間を、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	MEP アラーム遅延期間：250、MEP アラームリセット期間：1000
コマンドモード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	障害アラームは、MEP で障害が検出されてから MEP アラーム遅延期間タイマーが満了するまで常に障害が存在し続けた場合に、送信されます。なお、MEP アラーム遅延期間タイマーが満了するまでに、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、新たな障害が検出されると、新たな障害がその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。一方、新たな障害がその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 で検出されたすべての障害がなくなると、MEP アラームリセット期間タイマーが開始され、タイマーの期限が切れたときに障害がない場合は、障害アラームがリセットされます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MEP アラーム遅延期間の設定方法を示します。MEP アラーム遅延期間に 250 を割り当てます。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name op1 domain op-domain
(config-cfm-mep)# alarm-time delay 250
(config-cfm-mep)#
```

使用例：MEP アラームリセット期間の設定方法を示します。MEP アラームリセット期間に 1000 を割り当てます。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# cfm mep mepid 1 ma name op1 domain op-domain
```

```
(config-cfm-mep)# alarm-time reset 1000
(config-cfm-mep)#
```

4.18.17 ais

ais	
目的	Alarm Indication Signal (AIS) 機能を有効にして、パラメ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。
シンタックス	**ais** [**period** *PERIOD*] [**level** *LEVEL*] **no ais** [**period** | **level**]
パラメーター	**period** *PERIOD* (省略可能) : AIS Protocol Data Unit (AIS アラーム) の送信間隔を、**1sec** (1 秒) または **1min** (1 分) で指定します。 **level** *LEVEL* (省略可能) : メンテナンスエンドポイント(MEP)が AIS アラ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。デフォルトのドメインレベルは、メンテナンス中間ポイント(MIP)と MEP が存在する最も近いクライアントレイヤーです。
デフォルト	無効、送信間隔 : **1sec**、レベル : 未指定
コマンドモード	CFM MEP 設定モード
特権レベル	レベル : 12
ガイドライン	パラメーターを設定しないで実行した場合は、AIS 機能が有効になります。 ドメインレベルを指定しない場合は、MIP と MEP が存在する最も近いクライアントレイヤーの MD レベルと同じレベルに設定されます。デフォルトのクライアントレイヤーの MD レベルは、固定されていません。そのため、より上位の MD と MA を装置上で作成したり、削除したりすると、レベルが変わる可能性があります。 MEP は、不備条件の検出時に、設定済みのドメインレベルで ETH-AIS 情報を含む周期フレームを即時に出力できます。MEP は、不備条件が取り除かれるまで、ETH-AIS 情報を含む周期フレームを送信し続けます。 クライアント (サブ) レイヤーの MEP は、ETH-AIS 情報を含むフレームをサーバー (サブ) レイヤーから受信すると AIS 条件を検出して、すべての対向 MEP に関連するアラームを抑制します。MEP は、AIS 条件がクリアされると、不備条件の検出時にアラーム出力を再開します。
制限事項	-
注意事項	最も近いクライアントレイヤーMIP と MEP が存在しない場合、デフォルトのドメインレベルが計算できません。デフォルトのドメインレベルが計算できず、また、ドメインレベルを指定しない場合は、AIS アラームを送信できません。この場合、ドメインレベルを指定してください。
対象バージョン	1.01.01

使用例 : AIS 機能のドメインレベルを 5 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 op1 domain op-domain
(config-cfm-mep)# ais level 5
(config-cfm-mep)#
```

4.18.18 lck

lck	
目的	管理ロックを有効にし、パラメ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。
シンタックス	lck [period *PERIOD*] [level *LEVEL*] no lck [period | level]
パラメーター	period *PERIOD*（省略可能）：ロックフレームの送信間隔を指定します。1sec または 1min を指定できます。デフォルトは 1sec です。 level *LEVEL*（省略可能）：MEP がロック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	無効、送信間隔：1sec、レベル：未指定
コマンドモード	CFM MEP 設定モード
特権レベル	レベル：12
ガイドライン	パラメーターをすべて省略した場合は、管理ロックが有効になります。 ドメインレベルを指定しない場合は、MIP と MEP が存在する最も近いクライアントレイヤーの MD レベルと同じレベルに設定されます。このクライアントレイヤーの MD レベルは、固定されていません。そのため、より上位の MD と MA を装置上で作成したり、削除したりすると、レベルが変わる可能性があります。
制限事項	-
注意事項	最も近いクライアントレイヤーMIP と MEP が存在しない場合、デフォルトのドメインレベルが計算できません。デフォルトのドメインレベルが計算できず、また、ドメインレベルを指定しない場合は、ロックフレームを送信できません。この場合、ドメインレベルを指定してください。
対象バージョン	1.01.01

使用例：管理ロックのドメインレベルを 5 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 op1 domain op-domain
(config-cfm-mep)# lck level 5
(config-cfm-mep)#
```

4.18.19 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。
シンタックス	cfm mp-ltr-all no cfm mp-ltr-all
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。

cfm mp-ltr-all	
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

4.18.20 show cfm

show cfm	
目的	CFM のグローバル状態を表示します。
シンタックス	**show cfm**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：CFM のグローバル状態を表示する方法を示します。

```
# show cfm

CFM State: Enabled ...(1)
(2)                                  (3)
Domain Name: md5                     Level: 5
Domain Name: md6                     Level: 2
```

項番	説明
(1)	CFM の有効／無効を表示します。
(2)	MD 名を表示します。
(3)	ドメインレベルを表示します。

4.18.21 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。
シンタックス	**show cfm interface** [*INTERFACE-ID* [,|-]]
パラメーター	*INTERFACE-ID*（省略可能）：CFM 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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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 cfm interface	
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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/12 の CFM 情報を表示する方法を示します。

```
# show cfm interface port 1/0/12

Port1/0/12 ...(1)
CFM is enabled ...(2)
MAC Address: 00-40-66-A8-D5-62 ...(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 の有効／無効を表示します。
(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。
(9)	サービス方向を表示します。

4.18.22 show cfm domain

show cfm domain	
目的	MD 情報を表示します。
シンタックス	**show cfm domain** *DOMAIN-NAME*
パラメーター	*DOMAIN-NAME*：MD 名を指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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-ma1
```

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。

4.18.23 show cfm ma

show cfm ma	
目的	MA 情報を表示します。
シンタックス	**show cfm ma name** *MA-NAME* **domain** *DOMAIN-NAME*
パラメーター	**ma name** *MA-NAME* **domain** *DOMAIN-NAME*：MA 名と MD 名を指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)	サービス方向を表示します。

4.18.24 show cfm mepid

show cfm mepid	
目的	MEP 情報を表示します。
シンタックス	**show cfm mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*
パラメーター	**mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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: 00-40-66-20-24-0D ...(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)
(24)                                        (25)
Error CCMs Received: 0                      Normal CCMs Received: 0
(26)                                        (27)
Port Status CCMs Received: 0                If Status CCMs Received: 0
(28)                                        (29)
CCMs transmitted: 14813                     In-order LBRs Received: 0
(30)                                        (31)
Out-of-order LBRs Received: 0               Next LTM Trans ID: 1
(32)                                        (33)
Unexpected LTRs Received: 0                 LBMs Transmitted: 0
(34)                                        (35)
AIS PDUs Received: 0                        AIS PDUs Transmitted: 0
(36)                                        (37)
LCK PDUs Received: 0                        LCK PDUs Transmitted: 0
```

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)	サービス方向を表示します。
(4)	CFM ポートの有効／無効を表示します。
(5)	MAC アドレスを表示します。
(6)	MEP の有効／無効を表示します。
(7)	CCM の有効／無効を表示します。
(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する Some Remote MEP MAC Status Error：「DefMACstatus」以上の障害に対して送信する Some Remote MEP Down：「DefRemoteCCM」以上の障害に対して送信する Error CCM Received：「DefErrorCCM」以上の障害に対して送信する Cross-connect CCM Received：「DefXconCCM」の障害アラームだけを送信する
(10)	障害アラームを送信するまでの送信待機時間を表示します。
(11)	障害アラームのリセット時間を表示します。最後の障害を検知してから、リセット時間を経過すると、障害が解消したことが検知されます。
(12)	MEP で検出された最高優先度の障害を表示します。 None：最後の FNG_RESET 状態以降、障害なし Some Remote MEP Defect Indication：リモート MEP に障害あり Some Remote MEP MAC Status Error：リモート MEP が関係する MAC フレームにエラーあり Some Remote MEP Down：CCM が送信されていないリモート MEP あり

項番	説明
	Error CCM Received：無効な CCM の受信あり Cross-connect CCM Received：他の MA から送信された CCM の受信あり
(13)	AIS の有効／無効を表示します。
(14)	AIS アラームの送信間隔を表示します。
(15)	AIS アラームで送信するドメインレベルを表示します。 Invalid：無効
(16)	AIS アラームの受信状況を表示します。 Not Detected：未検出 Detected：検出
(17)	ロックフレームの有効／無効を表示します。
(18)	ロックフレームの送信間隔を表示します。
(19)	ロックフレームで送信するドメインレベルを表示します。
(20)	ロックフレームの受信状況を表示します。 Not Detected：未検出 Detected：検出
(21)	ロックフレームの送信状況を表示します。 Stop：停止 Start：開始
(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 アラームの数を表示します。
(35)	送信した AIS アラームの数を表示します。
(36)	受信したロックフレームの数を表示します。
(37)	送信したロックフレームの数を表示します。

4.18.25 show cfm mep fault

show cfm mep fault	
目的	障害がある MEP の概要を表示します。
シンタックス	**show cfm mep fault**
パラメーター	なし
デフォルト	なし
コマンドモード	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 cfm mep fault	
ガイドライン	MEP が検出した、すべての障害が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：障害がある MEP の表示方法を示します。

```
# 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)

Domain Name: md6
MA Name: ma6
MEPID: 3
Status: Some Remote MEP Down
AIS Status: Normal
LCK Status: Normal
```

項番	説明
(1)	MD 名を表示します。
(2)	MA 名を表示します。
(3)	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：最後の FNG_RESET 状態以降、障害なし Some Remote MEP Defect Indication：リモート MEP に障害あり Some Remote MEP MAC Status Error：リモート MEP が関係する MAC フレームにエラーあり Some Remote MEP Down：CCM が送信されていないリモート MEP あり Error CCM Received：無効な CCM の受信あり Cross-connect CCM Received：他の MA から送信された CCM の受信あり
(5)	AIS アラームの受信状況を表示します。 AIS Received：AIS アラーム受信済み Normal：AIS アラーム未受信
(6)	ロックフレームの受信状況を表示します。 LCK Received：ロックフレーム受信済み Normal：ロックフレーム未受信

4.18.26 show cfm counter ccm

show cfm counter ccm	
目的	すべての MEP の CCM パケットカウンターを表示します。
シンタックス	**show cfm counter ccm**
パラメーター	なし
デフォルト	なし
コマンドモード	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 cfm counter ccm	
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：すべての MEP の CCM パケット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: 1000  Level: 2     Direction: Up    Port: 1/0/1
 (6)                (7)                (8)
 XCON: 0           Error: 0           Normal: 0

Total:
 (9)                (10)               (11)
 XCON: 0           Error: 0           Normal: 0
```

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)	サービス方向を表示します。
(5)	ポート番号を表示します。
(6)	他の MA から受信した CCM のパケット数を表示します。
(7)	無効な CCM のパケット数を表示します。
(8)	正常な CCM のパケット数を表示します。
(9)	他の MA から受信した CCM の合計を表示します。
(10)	無効な CCM の合計を表示します。
(11)	正常な CCM の合計を表示します。

4.18.27 show cfm remote-mep

show cfm remote-mep	
目的	リモート MEP 情報を表示します。
シンタックス	**show cfm remote-mep mepid** *LOCAL-MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**remote-mepid** *REMOTE-MEPID*]
パラメーター	**mepid** *LOCAL-MEP-ID* **ma name** *MA-NAME* **domain** *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** *REMOTE-MEPID*（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。
デフォルト	なし
コマンドモード	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	-
制限事項	-

show cfm remote-mep	
注意事項	-
対象バージョン	1.01.01

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)	リモート機器の MEP ID を表示します。
(2)	リモート機器の MAC アドレスを表示します。
(3)	リモート MEP の CCM の受信状態を表示します。 IDLE：CCM の待受中（リセット中） START：CCM の受信中（リセット後にタイマーが期限切れになっていない、かつ有効な CCM を受信していない） FAILED：CCM の受信に失敗（リセット後にタイマーが期限切れになっている、または有効な CCM を受信後にタイマーが期限切れになっている） OK：CCM の受信に成功（タイマーが期限切れになる前に有効な CCM を受信した）
(4)	最後に受信した CCM の RDI ビット（リモート MEP の障害検知状態）を表示します。 Yes：RDI ビットが設定されている（障害が検知されている） No：RDI ビットが設定されていない、または有効な CCM を受信していない（障害が検知されていない）
(5)	リモート MEP が存在するポートにおいて、MAC フレームの状態にかかわらず、元データを通過させるかどうかを表示します。 No：CCM が受信されていない、または最後に受信した CCM にポートの状態に関する情報がない Blocked：元データを通過させない Up：元データを通過させる
(6)	CCM を送信するように設定されているリモート MEP が設定されているインターフェース（必ずしもそのインターフェースが常駐するインターフェースではない）または、IETF RFC 2863 IF-MIB における次の下層のインターフェースの状態を表示します。 No：CCM が受信されていない、または最後に受信した CCM にインターフェースの状態に関

項番	説明
	する情報がない Up：パケットを送信可能 Down：パケットを送信できない Testing：テスト実行中 Unknown：不明 Dormant：休止中（パケットを送信できないが、外部イベントを待機中） Notpresent：コンポーネント不足（パケットを送信できない） Lowerlayerdown：下層のインターフェースがパケットを送信できない（他のインターフェースの最も上層で稼働中だが、下層のインターフェースがパケットを送信できないため、このインターフェースもパケットを送信できない）
(7)	最後に受信した CCM のシリアル番号を表示します。
(8)	リモート MEP のシャーシ ID を表示します。
(9)	リモート MEP の管理アドレスを表示します。
(10)	最後に受信した CCM の検出時間を表示します。

4.18.28 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。
シンタックス	**show cfm mip ccm**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

4.18.29 show cfm pkt-cnt interface

show cfm pkt-cnt interface	
目的	ポートの CFM パケットカウンターを表示します。
シンタックス	show cfm pkt-cnt interface [*INTERFACE-ID* [,|-]] [rx] [tx]
パラメーター	*INTERFACE-ID*（省略可能）：カウンタ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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の CFM パケット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 ...(2)
    AllPkt:0 ...(3)      CCM:0 ...(4)
    LBR:0 ...(5)         LBM:0 ...(6)
    LTR:0 ...(7)         LTM:0 ...(8)
    VidDrop:0 ...(9)     OpcoDrop:0 ...(10)
  CFM TX Statistics ...(11)
    AllPkt:0             CCM:0
    LBR:0                LBM:0
    LTR:0                LTM:0
```

項番	説明
(1)	ポート番号を表示します。
(2)	受信パケットに関する情報を表示します。
(3)	すべての CFM パケット数を表示します。
(4)	CCM のパケット数を表示します。
(5)	LBR のパケット数を表示します。
(6)	LBM のパケット数を表示します。
(7)	LTR のパケット数を表示します。
(8)	LTM のパケット数を表示します。
(9)	監視対象 VLAN で受信できなくて廃棄されたパケット数を表示します。
(10)	予期しない OP コードのために廃棄されたパケット数を表示します。
(11)	送信パケットに関する情報を表示します。

使用例：ポート 1/0/1 の CFM パケットの RX 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 rx

Port1/0/1 ...(1)
```

```
  CFM RX Statistics ...(2)
    AllPkt:0 ...(3)     CCM:0 ...(4)
    LBR:0 ...(5)        LBM:0 ...(6)
    LTR:0 ...(7)        LTM:0 ...(8)
    VidDrop:0 ...(9)    OpcoDrop:0 ...(10)
```

項番	説明
(1)	ポート番号を表示します。
(2)	受信パケットに関する情報を表示します。
(3)	すべての CFM パケット数を表示します。
(4)	CCM のパケット数を表示します。
(5)	LBR のパケット数を表示します。
(6)	LBM のパケット数を表示します。
(7)	LTR のパケット数を表示します。
(8)	LTM のパケット数を表示します。
(9)	監視対象 VLAN で受信できなくて廃棄されたパケット数を表示します。
(10)	予期しない OP コードのために廃棄されたパケット数を表示します。

使用例：ポート 1/0/1 の CFM パケットの TX 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 tx

Port1/0/1 ...(1)
  CFM TX Statistics ...(2)
    AllPkt:0 ...(3)     CCM:0 ...(4)
    LBR:0 ...(5)        LBM:0 ...(6)
    LTR:0 ...(7)        LTM:0 ...(8)
```

項番	説明
(1)	ポート番号を表示します。
(2)	送信パケットに関する情報を表示します。
(3)	すべての CFM パケット数を表示します。
(4)	CCM のパケット数を表示します。
(5)	LBR のパケット数を表示します。
(6)	LBM のパケット数を表示します。
(7)	LTR のパケット数を表示します。
(8)	LTM のパケット数を表示します。

4.18.30 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。
シンタックス	**show cfm mp-ltr-all**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-

show cfm mp-ltr-all	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：すべてのメンテナンスポイントが LTR を応答する機能の状態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／無効を表示します。 Enabled：有効 Disabled：無効

4.18.31 cfm lck start / cfm lck stop

cfm lck start / cfm lck stop	
目的	管理ロックを開始します。管理ロックを停止する場合は、**cfm lck stop** コマンドを使用します。
シンタックス	**cfm lck start mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **cfm lck stop mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*
パラメーター	**mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *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。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：管理ロックの開始方法を示します。

```
# cfm lck start mepid 1 ma name op-ma domain op-domain
#
```

4.18.32 clear cfm counter ccm

clear cfm counter ccm	
目的	すべての MEP の CCM パケットカウンターをクリアします。
シンタックス	**clear cfm counter ccm**
パラメーター	なし
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-

clear cfm counter ccm	
注意事項	-
対象バージョン	1.01.01

使用例：すべての MEP の CCM パケットカウンターをクリアする方法を示します。

```
# clear cfm counter ccm
#
```

4.18.33 clear cfm pkt-cnt interface

clear cfm pkt-cnt interface	
目的	ポートの CFM パケットカウンターをクリアします。
シンタックス	clear cfm pkt-cnt interface {*INTERFACE-ID* [,|-] | all} [rx] [tx]
パラメーター	*INTERFACE-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：物理ポートを指定します。複数指定できます。 all：すべてのポートの CFM パケット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。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の CFM パケットの TX カウンターをクリアする方法を示します。

```
# clear cfm pkt-cnt interface port 1/0/1 tx
#
```

4.18.34 cfm loopback test

cfm loopback test	
目的	CFM ループバックテストを実施します。
シンタックス	cfm loopback test {*MAC-ADDRESS* | remote-mepid *REMOTE-MEPID*} mepid *MEP-ID* ma name *MA-NAME* domain *DOMAIN-NAME* [num *NUMBER*] [length *LENGTH* | pattern *STRING*] [pdu-priority *COS-VALUE*]
パラメーター	*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。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式） remote-mepid *REMOTE-MEPID*：宛先 MEP ID を指定します。 mepid *MEP-ID* ma name *MA-NAME* domain *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

cfm loopback test	
	ます。 **num** *NUMBER*（省略可能）：送信する LBM の数を指定します。指定しない場合、デフォルトは 4 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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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).
```

4.18.35 cfm linktrace

cfm linktrace	
目的	CFM リンクトレースを実施します。
シンタックス	**cfm linktrace** *MAC-ADDRESS* **mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**ttl** *TTL*] [**pdu-priority** *COS-VALUE*]
パラメーター	*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。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式）

cfm linktrace	
	• XXXXXXXXXXXX（区切り文字を使用しない形式） **mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *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** *TTL*（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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
```

4.18.36 show cfm linktrace

show cfm linktrace	
目的	CFM リンクトレース結果を表示します。
シンタックス	**show cfm linktrace** [**mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**trans-id** *ID*]]
パラメーター	**mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *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。
デフォルト	なし

show cfm linktrace	
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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を表示します。 Yes：転送状態 No：非転送状態
(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。

4.18.37 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。
シンタックス	**clear cfm linktrace {mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **| all}**
パラメーター	**mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*：CFM リンクトレース結果

clear cfm linktrace	
	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。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

4.19 Zero Touch Provisioning(ZTP)コマンド

Zero Touch Provisioning(ZTP)関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ztp enable	ztp enable [force] no ztp enable
show ztp	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。
シンタックス	**ztp enable [force]** **no ztp enable**
パラメーター	**force**（省略可能）：startup-config が工場出荷状態以外の場合でも、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
コマンドモード	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	ApresiaNP2000 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 enable**（デフォルト設定）で、startup-config が工場出荷状態の場合 • **ztp enable force** 設定の場合 ApresiaNP2000 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 enable**（デフォルト設定）でも、startup-config が工場出荷状態以外の場合 • **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。 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。この ZTP 処理中は、スタック ID LED が[10]で点滅します。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、スタック ID LED を[14]で 3 分間点滅させます。 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。 • 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。

ztp enable	
	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。この ZTP 処理中は、スタック ID LED が[11]で点滅します。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、スタック ID LED を[15]で 3 分間点滅させます。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。この ZTP 処理中は、スタック ID LED が[12]で点滅します。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、スタック ID LED を[16]で 3 分間点滅させます。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。この ZTP 処理中は、スタック ID LED が[13]で点滅します。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。 AEOS-NP2000 Ver. 1.09.01 以降では、DHCP オプション 125 を利用した以下のオプションも対応しています。 • ダウンロード一覧ファイル情報（subopt-code 2） • ZTP 処理中の SNMP トラップ対応 　• 宛先 IP アドレス情報（subopt-code 3） 　• SNMP コミュニティー名情報（subopt-code 4） 　• SNMP トラップ：SNMP バージョン情報（subopt-code 5）
制限事項	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。
注意事項	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。
対象バージョン	1.07.01

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。
シンタックス	show ztp
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	以下の項目は AEOS-NP2000 Ver. 1.09.01 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。 • Download Other Files • SNMP Server Address 1 • SNMP Comminity Name 1 • SNMP Server Version 1 • SNMP Server Address 2 • SNMP Comminity Name 2 • SNMP Server Version 2
対象バージョン	1.07.01 1.09.01：表示項目の追加

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:/AEOS-NP2000_R10901.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)
  Download Other Files  : - ...(13)
  SNMP Server Address 1: - ...(14)
  SNMP Comminity Name 1: - ...(15)
  SNMP Server Version 1: - ...(16)
  SNMP Server Address 2: - ...(17)
  SNMP Comminity Name 2: - ...(18)
  SNMP Server Version 2: - ...(19)
```

```
Result of this time: ...(20)
  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)
  Download Other Files : - ...(13)
  SNMP Server Address 1: 10.1.1.200 ...(14)
  SNMP Comminity Name 1: public ...(15)
  SNMP Server Version 1: 2c ...(16)
  SNMP Server Address 2: - ...(17)
  SNMP Comminity Name 2: - ...(18)
  SNMP Server Version 2: - ...(19)
```

項番	説明
(1)	起動時の ZTP 設定を表示します。 Enabled：ztp enable 設定 Enabled Force：ztp enabe force 設定 Disabled：no ztp enable 設定
(2)	現在の ZTP 設定を表示します。 Enabled：ztp enable 設定 Enabled Force：ztp enabe force 設定 Disabled：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（ダウンロードした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 • Fail (IMAGE <file> file name size over)：ファームウェアファイル名が 33 文字以上 • Fail (IMAGE <file> TFTP connection failed)：TFTP サーバーへの接続に失敗 • Fail (IMAGE <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 (IMAGE <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 (IMAGE <file> TFTP timeout)：転送途中にタイムアウト発生 • Fail (IMAGE <file> invalid file)：ダウンロードしたファームウェアファイルが不適切

項番	説明
	• Fail (IMAGE <file> disk full or allocation exceeded)：装置のフラッシュメモリーの空き容量不足で保存に失敗 • Fail (IMAGE <file> flash access error)：装置のフラッシュメモリーへの書き込みアクセスに失敗 • Fail (CONFIG <file> file name size over)：構成情報ファイル名が 33 文字以上 • Fail (CONFIG <file> TFTP connection failed)：TFTP サーバーへの接続に失敗 • Fail (CONFIG <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 (CONFIG <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 (CONFIG <file> TFTP timeout)：転送途中にタイムアウト発生 • Fail (CONFIG <file> invalid file)：ダウンロードした構成情報ファイルが不適切 • Fail (CONFIG <file> disk full or allocation exceeded)：装置のフラッシュメモリーの空き容量不足で保存に失敗 • Fail (CONFIG <file> flash access error)：装置のフラッシュメモリーへの書き込みアクセスに失敗 • Fail (OTHER <file> file name size over)：ファイル名サイズオーバー • Fail (OTHER <file> TFTP connection failed)：TFTP サーバーへの接続に失敗 • Fail (OTHER <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 (OTHER <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 (OTHER <file> TFTP timeout)：転送途中にタイムアウト発生 • Fail (OTHER <file> invalid file)：ダウンロードしたファイルが不適切 • Fail (OTHER <file> disk full or allocation exceeded)：装置のフラッシュメモリーの空き容量不足で保存に失敗 • Fail (OTHER <file> flash access error)：装置の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)	ダウンロード一覧ファイル情報
(14)	ZTP 処理中の SNMP トラップ用 宛先 IP アドレス情報(1)
(15)	ZTP 処理中の SNMP トラップ用 SNMP コミュニティー名情報(1)
(16)	ZTP 処理中の SNMP トラップ用 SNMP バージョン情報(1)
(17)	ZTP 処理中の SNMP トラップ用 宛先 IP アドレス情報(2)
(18)	ZTP 処理中の SNMP トラップ用 SNMP コミュニティー名情報(2)
(19)	ZTP 処理中の SNMP トラップ用 SNMP バージョン情報(2)
(20)	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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
time-range	time-range TR-NAME no time-range TR-NAME
periodic	periodic {daily HH:MM to HH:MM | weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM} no periodic {daily HH:MM to HH:MM | weekly WEEKLY-DAY HH:MM to [WEEKLY-DAY] HH:MM}
show time-range	show time-range [TR-NAME]

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。
シンタックス	**time-range** *TR-NAME* **no time-range** *TR-NAME*
パラメーター	*TR-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
コマンドモード	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	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。
制限事項	**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。
注意事項	-
対象バージョン	1.09.01

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。
シンタックス	**periodic** {**daily** *HH:MM* **to** *HH:MM* | **weekly** *WEEKLY-DAY HH:MM* **to** [*WEEKLY-DAY*] *HH:MM*} **no periodic** {**daily** *HH:MM* **to** *HH:MM* | **weekly** *WEEKLY-DAY HH:MM* **to** [*WEEKLY-DAY*] *HH:MM*}

periodic	
パラメーター	**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。 • *WEEKLY-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** [*WEEKLY-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
コマンドモード	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）
制限事項	タイムレンジは、装置全体で最大 64 個まで設定できます。 *WEEKLY-DAY* で指定するキーワードは、[TAB]キーによるコマンド補完は動作しません。
注意事項	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。
対象バージョン	1.09.01

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。
シンタックス	show time-range [TR-NAME]
パラメーター	*TR-NAME*（省略可能）：タイムレンジプロファイル名を指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.09.01

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。

コマンド	コマンドとパラメーター
mac-address-table aging-time	mac-address-table aging-time SECONDS no mac-address-table aging-time
mac-address-table aging destination-hit	mac-address-table aging destination-hit no mac-address-table aging destination-hit
mac-address-table learning	mac-address-table learning interface INTERFACE-ID [,|-] no mac-address-table learning interface INTERFACE-ID [,|-]
mac-address-table static	mac-address-table static MAC-ADDRESS vlan VLAN-ID {interface INTERFACE-ID [,|-] | drop} no mac-address-table static {all | MAC-ADDRESS vlan VLAN-ID [interface INTERFACE-ID] [,|-]}

FDB 関連の show／操作コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show mac-address-table	show mac-address-table [dynamic | static] [address MAC-ADDRESS | interface INTERFACE-ID | vlan VLAN-ID]
show mac-address-table aging-time	show mac-address-table aging-time
show mac-address-table learning	show mac-address-table learning [interface INTERFACE-ID [,|-]]
clear mac-address-table	clear mac-address-table dynamic {all | address MAC-ADDRESS | interface INTERFACE-ID | vlan VLAN-ID}

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。
シンタックス	**mac-address-table aging-time** *SECONDS* **no mac-address-table aging-time**
パラメーター	*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は無効化されます。
デフォルト	300 秒
コマンドモード	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	-
制限事項	-
注意事項	実際に MAC アドレステーブルからエントリーが消去されるのは設定値～設定値×2 の時間になります。

mac-address-table aging-time	
対象バージョン	1.01.01

使用例：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。
シンタックス	mac-address-table aging destination-hit no mac-address-table aging destination-hit
パラメーター	なし
デフォルト	無効
コマンドモード	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	MAC アドレスエントリーのエージング時間は、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。 宛先 MAC アドレスによる更新機能によって、MAC アドレスエントリーのエージング時間がリセットされる契機が増加します。これにより、MAC アドレスエントリーのエージングタイムアウトによるトラフィックフラッディングが減少します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	mac-address-table learning interface *INTERFACE-ID* [,|-] no mac-address-table learning interface *INTERFACE-ID* [,|-]
パラメーター	interface *INTERFACE-ID*：MAC アドレスの学習を有効に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
コマンドモード	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	-

mac-address-table learning	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MAC アドレスの学習を有効にする方法を示します。

```
# configure terminal
(config)# mac-address-table learning interface port 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。
シンタックス	mac-address-table static *MAC-ADDRESS* vlan *VLAN-ID* {interface *INTERFACE-ID* [,|-] | drop} no mac-address-table static {all | *MAC-ADDRESS* vlan *VLAN-ID* [interface *INTERFACE-ID*] [,|-]}
パラメーター	*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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式） 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 *INTERFACE-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：物理ポートを指定します。複数指定できます。 • port-channel：ポートチャネルを指定します。 drop：指定 VLAN で受信した送信元 MAC アドレスが一致したフレーム、または指定 VLAN で受信した宛先 MAC アドレスが一致した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
コマンドモード	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	スタティック MAC アドレスエントリーを設定すると、指定 VLAN で宛先 MAC アドレスが一致したフレームを受信した場合に、指定したインターフェースに転送されます。 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。 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。

mac-address-table static	
	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。
制限事項	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 レイヤー3 中継後のトラフィックは、drop パラメーターを指定したエントリーと一致しても破棄されません。
注意事項	設定したすべてのインターフェースを含むコマンド型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型式で実施してください。
対象バージョン	1.01.01

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。
シンタックス	**show mac-address-table** [**dynamic** | **static**] [**address** *MAC-ADDRESS* | **interface** *INTERFACE-ID* | **vlan** *VLAN-ID*]
パラメーター	**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。

show mac-address-table	
	• XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式） **interface** *INTERFACE-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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。 **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。
デフォルト	なし
コマンドモード	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 MAC アドレスエントリーが表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MAC アドレスが 00-00-5E-00-53-F2 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 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を表示します。 Static：スタティックエントリー dynamic：ダイナミックエントリー
(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  00-40-66-B4-96-B5   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を表示します。 Static：スタティックエントリー dynamic：ダイナミックエントリー
(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を表示します。 Static：スタティックエントリー dynamic：ダイナミックエントリー
(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を表示します。
シンタックス	**show mac-address-table aging-time**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MAC アドレステーブルのエージングタイム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 アドレスの学習状態を表示します。
シンタックス	show mac-address-table learning [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID*（省略可能）：MAC アドレスの学習状態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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 1/0/10 上での MAC アドレスの学習状況を表示する方法を示します。

```
# show mac-address-table learning interface port 1/0/1-10
 (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
Port1/0/7                   Enabled
Port1/0/8                   Enabled
Port1/0/9                   Enabled
Port1/0/10                  Enabled
```

項番	説明
(1)	ポート番号を表示します。
(2)	MAC アドレス学習状態の有効／無効を表示します。

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消去します。
シンタックス	clear mac-address-table dynamic {all | address *MAC-ADDRESS* | interface *INTERFACE-ID* | vlan *VLAN-ID*}
パラメーター	all：すべてのダイナミック MAC アドレスエントリーを消去する場合に指定します。 address *MAC-ADDRESS*：消去するダイナミック 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。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式）

clear mac-address-table	
	interface *INTERFACE-ID*：ダイナミック MAC アドレスエントリーをすべて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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。 **vlan** *VLAN-ID*：ダイナミック MAC アドレスエントリーをすべて消去する VLAN ID を 1～4094 の範囲で指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MAC アドレスが 00-00-5E-00-53-F2 のダイナミック MAC アドレスエントリーを、MAC アドレステーブルから消去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。

コマンド	コマンドとパラメーター
max-rcv-frame-size	max-rcv-frame-size BYTES no max-rcv-frame-size

5.2.1 max-rcv-frame-size

max-rcv-frame-size	
目的	許容する最大の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。
シンタックス	**max-rcv-frame-size** *BYTES* **no max-rcv-frame-size**
パラメーター	*BYTES*：許容するイーサネットフレームサイズの最大値を 64～12,288 バイトの範囲で指定します。
デフォルト	1536 バイト
コマンドモード	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	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。サーバー間のやりとりを最適化するために、装置システムを介してラージフレームまたはジャンボフレームを転送する場合に、本コマンドを実行してください。
制限事項	ApresiaNP2000 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。
注意事項	タグなしフレームの場合は、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。 タグ付きフレームの場合は、宛先 MAC アドレス～FCS が「設定値＋8 バイト」のサイズまで送受信できます。 トンネルポートでカスタマーVLAN タグ付きフレームを送受信する場合は、受信は宛先 MAC アドレス～FCS が「設定値＋8 バイト」のサイズまで、送信は「設定値＋4 バイト」のサイズまで可能です。
対象バージョン	1.01.01

使用例：ポート 1/0/1 で、受信イーサネットフレームサイズを最大 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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
channel-group	channel-group CHANNEL-NO mode {on | active | passive} no channel-group
lacp port-priority	lacp port-priority PRIORITY no lacp port-priority
lacp timeout	lacp timeout {short | long} no lacp timeout
lacp system-priority	lacp system-priority PRIORITY no lacp system-priority
port-channel load-balance	port-channel load-balance {src-dst-mac | dst-mac | src-mac | src-dst-ip | dst-ip | src-ip} no port-channel load-balance
show channel-group	show channel-group
show channel-group channel	show channel-group channel [CHANNEL-NO] {detail | neighbor}
show channel-group load-balance	show channel-group load-balance
show channel-group sys-id	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。
シンタックス	**channel-group** *CHANNEL-NO* **mode {on | active | passive}** **no channel-group**
パラメーター	*CHANNEL-NO*：チャネルグループ ID を 1～48 の範囲で指定します。なお、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。 **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
コマンドモード	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	設定可能なチャネルグループ数は、AEOS-NP2000 Ver. 1.03.01 以降では最大 48 個です。それより前のバージョンでは最大 32 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

channel-group	
	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。 本装置では、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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01 1.03.01：サポート対象のチャネルグループ数を 32 から 48 に拡張

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。
シンタックス	**lacp port-priority** *PRIORITY* **no lacp port-priority**
パラメーター	*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
コマンドモード	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	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。
制限事項	-
注意事項	本装置では、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。
対象バージョン	1.01.01

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。
シンタックス	**lacp timeout {short | long}** **no lacp timeout**
パラメーター	**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。本パラメーターを指定した場合は、キープアライブのために送信される 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。本パラメーターを指定した場合は、キープアライブのために送信される 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）
コマンドモード	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	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	lacp system-priority *PRIORITY* no lacp system-priority
パラメーター	*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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	port-channel load-balance {src-dst-mac | dst-mac | src-mac | src-dst-ip | dst-ip | src-ip} no port-channel load-balance
パラメーター	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 アドレスによる負荷分散 • dst-mac：宛先 MAC アドレスによる負荷分散 • src-mac：送信元 MAC アドレスによる負荷分散 • src-dst-ip：送信元 IP アドレスと宛先 IP アドレスによる負荷分散 • dst-ip：宛先 IP アドレスによる負荷分散 • src-ip：送信元 IP アドレスによる負荷分散
デフォルト	src-dst-mac（宛先 MAC アドレスと送信元 MAC アドレスによる負荷分散）
コマンドモード	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	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

port-channel load-balance	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

■ 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、イーサータイプ
		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、イーサータイプ
		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、イーサータイプ
		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、イーサータイプ
	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、イーサータイプ
	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、イーサータイプ
	すべて	未学習	送信元 MAC アドレス

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。
シンタックス	**show channel-group**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-

show channel-group	
注意事項	-
対象バージョン	1.01.01

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: 32768,00-40-66-03-04-00 ...(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 アドレスによる負荷分散 dst-mac：宛先 MAC アドレスによる負荷分散 src-mac：送信元 MAC アドレスによる負荷分散 src-dst-ip：送信元 IP アドレスと宛先 IP アドレスによる負荷分散 dst-ip：宛先 IP アドレスによる負荷分散 src-ip：送信元 IP アドレスによる負荷分散
(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)	ポートチャネルの動作モードを表示します。 Static：スタティックモード LACP：LACP モード

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。
シンタックス	**show channel-group channel** [*CHANNEL-NO*] {**detail** | **neighbor**}
パラメーター	*CHANNEL-NO*（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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01 1.03.01：サポート対象のチャネルグループ数を 32 から 48 に拡張

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.
  indep:    Port is in an independent state(not bundled but able to switch data
            traffic)
  down:     Port is down.

Channel Group 3 ...(3)
  Member Ports: 2, Maxports = 8, Protocol: LACP ...(4)
  (5)            (6)     (7)          (8)         (9)
                         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)	メンバーポートのポート番号を表示します。
(6)	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)	LACP の状態を表示します。
(8)	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。
(9)	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。

項番	説明
(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。
シンタックス	show channel-group load-balance
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 アドレスによる負荷分散 dst-mac：宛先 MAC アドレスによる負荷分散 src-mac：送信元 MAC アドレスによる負荷分散 src-dst-ip：送信元 IP アドレスと宛先 IP アドレスによる負荷分散 dst-ip：宛先 IP アドレスによる負荷分散 src-ip：送信元 IP アドレスによる負荷分散

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。
シンタックス	show channel-group sys-id
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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: 32768,00-40-66-03-04-00 ...(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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
redundant group-number	redundant group-number REDUNDANT-NO {primary | secondary} no redundant group-number
redundant group-number preempt	redundant group-number REDUNDANT-NO preempt {disable | delay SECONDS} no redundant group-number REDUNDANT-NO preempt
redundant mac-address-table-update	redundant mac-address-table-update count COUNT no redundant mac-address-table-update
redundant fdb-flush send enable	redundant fdb-flush send enable count COUNT no redundant fdb-flush send enable
redundant fdb-flush receive enable	redundant fdb-flush receive enable no redundant fdb-flush receive enable
redundant fdb-flush vid	redundant fdb-flush vid VLAN-ID no redundant fdb-flush vid
redundant fdb-flush dst-mac	redundant fdb-flush dst-mac MAC-ADDRESS no redundant fdb-flush dst-mac
show redundant	show redundant [portbase]

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。
シンタックス	**redundant group-number** *REDUNDANT-NO* {**primary** | **secondary**} **no redundant group-number**
パラメーター	*REDUNDANT-NO*：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
コマンドモード	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。
制限事項	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スパニングツリー、RPVST+、ERPS、MMRP-Plus、ループ検知機能（**loop-detection action notify-only** コマンド設定時を除く）と併用することはできません。
注意事項	-

redundant group-number	
対象バージョン	1.04.02

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)# 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。
シンタックス	**redundant group-number** *REDUNDANT-NO* **preempt** {**disable** | **delay** *SECONDS*} **no redundant group-number** *REDUNDANT-NO* **preempt**
パラメーター	*REDUNDANT-NO*：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*：プリエンプトモードのディレイ時間を、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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.07.01

使用例：リダンダントグループ ID 3 に対して、プリエンプトモードを無効に設定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

redundant mac-address-table-update	
	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。
シンタックス	**redundant mac-address-table-update count** *COUNT* **no redundant mac-address-table-update**
パラメーター	*COUNT*：送信回数を 1～3 の範囲で指定します。
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.04.02

使用例：MAC アドレス再学習フレームの送信を、送信回数を 3 回に指定して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。
シンタックス	**redundant fdb-flush send enable count** *COUNT* **no redundant fdb-flush send enable**
パラメーター	*COUNT*：送信回数を 1～3 の範囲で指定します。
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	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。
対象バージョン	1.04.02

使用例：FDB フラッシュフレームの送信を、送信回数を 3 回に指定して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。
シンタックス	**redundant fdb-flush receive enable** **no redundant fdb-flush receive enable**
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	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。
対象バージョン	1.04.02

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。
シンタックス	**redundant fdb-flush vid** *VLAN-ID* **no redundant fdb-flush vid**
パラメーター	*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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.04.02

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。
シンタックス	**redundant fdb-flush dst-mac** *MAC-ADDRESS* **no redundant fdb-flush dst-mac**
パラメーター	*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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式）
デフォルト	01:40:66:C0:4F:44
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.04.02

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。
シンタックス	**show redundant** [portbase]
パラメーター	**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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.04.02 1.07.01：表示項目の仕様変更

使用例：すべてのポートリダンダントの詳細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     16 17    24 25    32 33    40 41    48 49
GrpNo       +------+ +------+ +------+ +------+ +------+ +------+ +---
  1   1  -  A....... ........ ........ ........ ........ ........ ..
  1   2     R....... ........ ........ ........ ........ ........ ..
  2   1 Dis .A...... ........ ........ ........ ........ ........ ..
  2   2     .R...... ........ ........ ........ ........ ........ ..
  3   1 180 ........ ..aa.... ........ ........ ........ ........ ..
  3   2     ........ ..rr.... ........ ........ ........ ........ ..
```

項番	説明
(1)	MAC アドレス再学習フレーム送信の有効／無効を表示します。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／無効を表示します。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／無効を表示します。
(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。
(2)	ポートリダンダントの動作状態を表示します。
(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。

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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
link-relay	link-relay id INSTANCE-ID track-port interface INTERFACE-ID [,|-] relay-port interface INTERFACE-ID [,|-] no link-relay id INSTANCE-ID
show link-relay	show link-relay
show link-relay status	show link-relay status

5.5.1 link-relay

link-relay	
目的	リンクダウン連携インスタンスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**link-relay id** *INSTANCE-ID* **track-port interface** *INTERFACE-ID* [,|-] **relay-port interface** *INTERFACE-ID* [,|-] **no link-relay id** *INSTANCE-ID*
パラメーター	**id** *INSTANCE-ID*：リンクダウン連携インスタンスの識別子を 1～32 の範囲で指定します。 **track-port interface** *INTERFACE-ID*：監視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**：物理ポートを指定します。複数指定できます。 **relay-port interface** *INTERFACE-ID*：強制的にリンクダウンまたはリンクアップ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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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	1 つのリンクダウン連携インスタンスにおいて、監視するポートとして指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指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。また、監視するポートとして指定したすべてのポートがリンクダウンしている状態で、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指定したすべてのポートが強制的にリンクアップされます。 1 つのリンクダウン連携インスタンスにおいてリレーポートとして指定したポートを、他のリンクダウン連携インスタンスにおいても、リレーポートとして指定できます。複数のリンクダウン連携インスタンスにおいてリレーポートと指定した場合、その中の 1 つのリンクダウン連携インスタンスにおいて、監視するポートとして指定したすべてのポートがリンクダウンすると、そ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指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。このとき、複数のリンクダウン連携インスタンスに属するリレーポートをリンクダウンから復旧するには、リレーポートが属するすべてのリンクダウン連携インスタンスにおいて、リレーポートが強制的にリンクアップする条件を満たす必要があります。 ポートは、1 つのリンクダウン連携インスタンスにおいて、監視するポートまた

link-relay	
	はリレーポートとして指定できます。
制限事項	-
注意事項	監視するポートとして指定したポートは、他のリンクダウン連携インスタンスにおいて、監視するポートおよびリレーポートとして指定できません。 リレーポートとして指定したポートは、他のリンクダウン連携インスタンスにおいて監視するポートとして指定できません。
対象バージョン	1.03.01

使用例：ポート 1/0/1 からポート 1/0/5 がリンクダウンしたときに、ポート 1/0/10 およびポート 1/0/15 が強制的にリンクダウンするように設定する方法を示します。

```
# configure terminal
(config)# link-relay id 1 track-port interface port1/0/1-5 relay-port interface
port1/0/10,1/0/15
(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。
シンタックス	**show link-relay**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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     16 17    24 25
ID    +------+ +------+ +------+ +---
1  1  TTTTT... .R....R. ........ ..
32 1  ......Rr ........ TTT..... ..
```

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。
シンタックス	show link-relay status
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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       5
2    Down     0
32   Up       3
```

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：すべての監視するポートがリンクダウンしています。 Up：監視するポートとして設定したポートのうち、少なくとも 1 つのポートがリンクアップしています。
(3)	監視するポートのうち、リンクアップしているポートの数を表示します。

5.6 ループ検知コマンド

ループ検知関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
loop-detection global enable	loop-detection global enable no loop-detection global enable
loop-detection enable (Interface)	loop-detection enable no loop-detection enable
loop-detection interval	loop-detection interval SECONDS no loop-detection interval
loop-detection mode	loop-detection mode {port-based | vlan-based} no loop-detection mode
loop-detection vlan	loop-detection vlan VLAN-LIST [,|-] no loop-detection vlan VLAN-LIST [,|-]
loop-detection action notify-only	loop-detection action notify-only no loop-detection action notify-only
loop-detection no-check-src	loop-detection no-check-src no loop-detection no-check-src
errdisable recovery cause loop-detection	errdisable recovery cause loop-detection [interval SECONDS] no errdisable recovery cause loop-detection [interval]
show loop-detection	show loop-detection [interface INTERFACE-ID [,|-]]

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。
シンタックス	**loop-detection global enable** **no loop-detection global enable**
パラメーター	なし
デフォルト	無効
コマンドモード	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	-
制限事項	ループ検知機能（**loop-detection action notify-only** コマンド設定時を除く）は、同一インターフェースでスパニングツリー、RPVST+、ERPS、MMRP-Plus、ポートリダンダント機能と併用することはできません。 同一インターフェース（ポート、ポートチャネル）上で 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）上で MMRP-Plus、ERPS、MSTP、RPVST+機能と併用する場合は、**loop-detection mode** コマンドで動作モードを VLAN ベースに変更した上で、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。

loop-detection global enable	
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	loop-detection enable no loop-detection enable
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	ループ検知機能（loop-detection action notify-only コマンド設定時を除く）は、同一インターフェースでスパニングツリー、RPVST+、ERPS、MMRP-Plus、ポートリダンダント機能と併用することはできません。 同一インターフェース（ポート、ポートチャネル）上で 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）上で MMRP-Plus、ERPS、MSTP、RPVST+機能と併用する場合は、loop-detection mode コマンドで動作モードを VLAN ベースに変更した上で、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。
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	loop-detection interval *SECONDS* no loop-detection interval
パラメーター	interval *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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 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。
シンタックス	loop-detection mode {port-based | vlan-based} no loop-detection mode
パラメーター	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
コマンドモード	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ループ検知フレームを受信した場合は、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（ループ検知有効）でループ検知フレームを受信した場合は、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（ループ検知無効）でループ検知フレームを受信した場合は、そのループ検知フレーム

loop-detection mode	
	を送信したポート（ループ検知有効）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ループ検知フレームを受信した場合は、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（ループ検知有効）でループ検知フレームを受信した場合は、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（ループ検知無効）でループ検知フレームを受信した場合は、そのループ検知フレームを送信したポート（ループ検知有効）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。 エラーで無効にされたポートを復旧する方法は 2 つあります。 • **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無効に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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.6.5 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。
シンタックス	**loop-detection vlan** *VLAN-LIST* [,|-] **no loop-detection vlan** *VLAN-LIST* [,|-]
パラメーター	*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

loop-detection vlan	
	を有効にする VLAN 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
コマンドモード	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	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 コマンドを実行するか、もしくは loop-detection vlan 1-4094 を実行すると、デフォルト設定に戻ります。
制限事項	1 度に送信可能なループ検知フレーム数は 100 フレームです。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.6.6 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。
シンタックス	loop-detection action notify-only no loop-detection action notify-only
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.04.01

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)#
```

5.6.7 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。
シンタックス	loop-detection no-check-src no loop-detection no-check-src
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.04.01

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)#
```

5.6.8 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。
シンタックス	errdisable recovery cause loop-detection [interval *SECONDS*] no errdisable recovery cause loop-detection [interval]
パラメーター	interval *SECONDS*（省略可能）：err-disabled 状態になってから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。

errdisable recovery cause loop-detection	
デフォルト	無効
コマンドモード	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	本コマンドの詳細や関連する show コマンドは「10.2 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、ループ検知機能によって err-disabled 状態にされたポートを、指定した時間で自動復旧することができます。 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。また、**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。
制限事項	本コマンドは、構成情報ではエラー復旧コマンド（ラベル# ERRDISABLE）で表示されます。
注意事項	**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。
対象バージョン	1.01.01

使用例：ループ検知機能によって err-disabled 状態に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 loop-detection interval 200
(config)#
```

5.6.9 show loop-detection

show loop-detection	
目的	現在のループ検知設定を表示します。
シンタックス	**show loop-detection** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：ループ検知機能の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**：物理ポートを指定します。 • **range port**：物理ポートを範囲で指定します。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	noChkSrc 項目と Action 項目は AEOS-NP2000 Ver. 1.04.01 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。
対象バージョン	1.01.01

show loop-detection	
	1.04.01：表示項目の仕様変更

使用例：現在のループ検知の設定と状態を表示する方法を表示します。

```
# show loop-detection

 Loop Detection        : Disabled ...(1)
 Detection Mode        : port-based ...(2)
 Enabled VLAN          : all VLANs ...(3)
 Interval              : 10 seconds ...(4)
 (5)              (6)        (7)           (8)       (9)                 (10)
 Interface        noChkSrc   Action        State     Result              Time Left
 ---------------  --------   -----------   --------  ------------------  ----------
 Port1/0/1        Enabled    shutdown      Enabled   Normal              -
 Port1/0/2        Disabled   notify-only   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              -
 Port1/0/13       Disabled   shutdown      Disabled  Normal              -
 Port1/0/14       Disabled   shutdown      Disabled  Normal              -
 Port1/0/15       Disabled   shutdown      Disabled  Normal              -
 Port1/0/16       Disabled   shutdown      Disabled  Normal              -
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

項番	説明
(1)	ループ検知の有効／無効を表示します。
(2)	ループ検知の動作モードを表示します。
(3)	ループ検知が有効な VLAN を表示します。 all VLANs：すべての VLAN に対してループ検知が有効な場合
(4)	ループ検知フレームの送信間隔を表示します。
(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)	no-check-src オプションの有効／無効を表示します。
(7)	ループ検知したときの動作 shutdown/notify-only を表示します。
(8)	ループ検知の有効／無効を表示します。
(9)	ループ検知の結果を表示します。 Normal：ループが検知されていません Loop：ループが検知されています（ポートベースモード） Loop on VLAN XX：VLAN XX でループが検知されています（VLAN ベースモード）
(10)	ループ検知により err-disabled 状態になったインターフェースが自動復旧されるまでの残り時間を表示します。

使用例：ポート 1/0/1 のループ検知状態を表示する方法を示します。

```
# show loop-detection interface port 1/0/1
 (1)              (2)        (3)           (4)       (5)                 (6)
 Interface        noChkSrc   Action        State     Result              Time Left
 ---------------  --------   -----------   --------  ------------------  ----------
 Port1/0/1        Enabled    shutdown      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／無効を表示します。
(3)	ループ検知したときの動作 shutdown/notify-only を表示します。
(4)	ループ検知の有効／無効を表示します。
(5)	ループ検知の結果を表示します。 Normal：ループが検知されていません loop：ループが検知されています（ポートベースモード） loop on VLAN XX：VLAN XX でループが検知されています（VLAN ベースモード）
(6)	ループ検知により err-disabled 状態になったインターフェースが自動復旧されるまでの残り時間を表示します。

使用例：ポートチャネル 2 の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／無効を表示します。
(3)	ループ検知したときの動作 shutdown/notify-only を表示します。
(4)	ループ検知の有効／無効を表示します。
(5)	ループ検知の結果を表示します。 Normal：ループが検知されていません loop：ループが検知されています（ポートベースモード） loop on VLAN XX：VLAN XX でループが検知されています（VLAN ベースモード）
(6)	ループ検知により err-disabled 状態になったインターフェースが自動復旧されるまでの残り時間を表示します。

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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
storm-control	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}
storm-control action	storm-control action {shutdown | drop | none} no storm-control action
storm-control polling interval	storm-control polling interval SECONDS no storm-control polling interval
storm-control polling retries	storm-control polling retries {NUMBER | infinite} no storm-control polling retries
errdisable recovery cause storm-control	errdisable recovery cause storm-control [interval SECONDS] no errdisable recovery cause storm-control [interval]
snmp-server enable traps storm-control	snmp-server enable traps storm-control no snmp-server enable traps storm-control
show storm-control	show storm-control interface INTERFACE-ID [,|-] [broadcast | multicast | unicast]

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。
シンタックス	**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**}
パラメーター	**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、Unknwon 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 秒あたりの受信フレーム数で指定します。 • *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。 • *KBPS-RISE*：上限値を 0～2,147,483,647 の範囲で 64Kbps 単位で指定します。

storm-control	
	• *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。 • *LEVEL-RISE*：上限値を 0～100 の範囲で指定します。 • *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
コマンドモード	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。 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。
制限事項	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。
注意事項	ポートチャネルでのストームコントロールは、AEOS-NP2000 Ver. 1.09.01 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。
対象バージョン	1.01.01 1.09.01：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。
シンタックス	storm-control action {shutdown | drop | none} no storm-control action
パラメーター	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）
コマンドモード	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。
制限事項	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

storm-control action	
	として扱われる仕様制限があります。 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、Unknwon 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（Unknwon 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。
注意事項	ポートチャネルでのストームコントロールは、AEOS-NP2000 Ver. 1.09.01 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。
対象バージョン	1.01.01 1.09.01：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。
シンタックス	storm-control polling interval *SECONDS* no storm-control polling interval
パラメーター	*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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	storm-control polling retries {*NUMBER* | infinite} no storm-control polling retries
パラメーター	*NUMBER*：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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	errdisable recovery cause storm-control [interval *SECONDS*] no errdisable recovery cause storm-control [interval]
パラメーター	interval *SECONDS*（省略可能）：err-disabled 状態になってから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
コマンドモード	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	本コマンドの詳細や関連する show コマンドは「10.2 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。また、show interfaces status コマンドの Status 項目では "err-disabled" と表示されます。

errdisable recovery cause storm-control	
	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。
制限事項	本コマンドは、構成情報ではエラー復旧コマンド（ラベル# ERRDISABLE）で表示されます。
注意事項	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。
対象バージョン	1.01.01

使用例：ストームコントロール機能によって err-disabled 状態に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。
シンタックス	snmp-server enable traps storm-control no snmp-server enable traps storm-control
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.09.01

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。
シンタックス	show storm-control interface *INTERFACE-ID* [,|-] [broadcast | multicast | unicast]
パラメーター	interface *INTERFACE-ID*：ストームコントロールの状態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：物理ポートを指定します。 • range port：物理ポートを範囲で指定します。 • port-channel：ポートチャネルを指定します。

show storm-control	
	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）：Unknwon 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。
デフォルト	なし
コマンドモード	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	-
制限事項	ユニキャストのストームコントロールでは、Unknwon 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 Unknwon 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。
注意事項	-
対象バージョン	1.01.01 1.09.01：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 からポート 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)	上限値、下限値、およびトラフィックの流量の単位を表示します。単位の表示の意味は以下のとおりです。 pps：パケット数 kbps：受信トラフィックのビット数 %：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)	現在の値を表示します。
(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 状態に変更） Inactive：ストームコントロール無効

使用例：ポート 1/0/1 からポート 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 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)	上限値、下限値、およびトラフィックの流量の単位を表示します。単位の表示の意味は以下のとおりです。 pps：パケット数 kbps：受信トラフィックのビット数 %：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)	現在の値を表示します。
(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 状態に変更） 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)	上限値、下限値、およびトラフィックの流量の単位を表示します。単位の表示の意味は以下のとおりです。 pps：パケット数 kbps：受信トラフィックのビット数 %：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)	現在の値を表示します。
(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 状態に変更） Inactive：ストームコントロール無効

5.8 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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
multicast filtering-mode	multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered} no multicast filtering-mode
show multicast filtering-mode	show multicast filtering-mode [vlan VLAN-ID]

5.8.1 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。
シンタックス	multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered} no multicast filtering-mode
パラメーター	forward-all：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の設定にかかわらず、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：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：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
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	このフィルタリングモードの適用対象は、マルチキャストアドレスのために予約されたアドレス以外のアドレス宛てのマルチキャストパケットだけです。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 100 に対して、未登録のマルチキャストパケットをフィルタリングするようにマルチキャストフィルタリングモードを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)#
```

5.8.2 show multicast filtering-mode

show multicast filtering-mode	
目的	受信したマルチキャストパケットを処理するフィルタリングモードを表示しま

show multicast filtering-mode	
	す。
シンタックス	**show multicast filtering-mode** [**vlan** *VLAN-ID*]
パラメーター	**vlan** *VLAN-ID*：マルチキャストフィルタリングモードの設定を表示する VLAN ID を 1～4094 の範囲で指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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設定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パケットをフラッディング forward-unregistered：登録されたマルチキャストパケットを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パケットをフラッディング filter-unregistered：登録されたマルチキャストパケットを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パケットをフィルタリング

5.9 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。

コマンド	コマンドとパラメーター
ip igmp snooping	ip igmp snooping no ip igmp snooping
ip igmp snooping (VLAN)	ip igmp snooping no ip igmp snooping
ip igmp snooping dyn-mr-aging-time	ip igmp snooping dyn-mr-aging-time SECONDS no ip igmp snooping dyn-mr-aging-time
ip igmp snooping fast-leave	ip igmp snooping fast-leave [group-list ACCESS-LIST-NAME] no ip igmp snooping fast-leave
ip igmp snooping ignore-topology-change-notification	ip igmp snooping ignore-topology-change-notification no ip igmp snooping ignore-topology-change-notification
ip igmp snooping last-member-query-interval	ip igmp snooping last-member-query-interval SECONDS no ip igmp snooping last-member-query-interval
ip igmp snooping mrouter	ip igmp snooping mrouter [forbidden] interface INTERFACE-ID [,|-] no ip igmp snooping mrouter [forbidden] interface INTERFACE-ID [,|-]
ip igmp snooping proxy-reporting	ip igmp snooping proxy-reporting [source IP-ADDRESS] no ip igmp snooping proxy-reporting
ip igmp snooping querier	ip igmp snooping querier no ip igmp snooping querier
ip igmp snooping query-interval	ip igmp snooping query-interval SECONDS no ip igmp snooping query-interval
ip igmp snooping query-max-response-time	ip igmp snooping query-max-response-time SECONDS no ip igmp snooping query-max-response-time
ip igmp snooping query-version	ip igmp snooping query-version {1 | 2 | 3} no ip igmp snooping query-version
ip igmp snooping report-suppression	ip igmp snooping report-suppression no ip igmp snooping report-suppression
ip igmp snooping robustness-variable	ip igmp snooping robustness-variable VALUE no ip igmp snooping robustness-variable
ip igmp snooping static-group	ip igmp snooping static-group GROUP-ADDRESS interface INTERFACE-ID [,|-] no ip igmp snooping static-group GROUP-ADDRESS [interface INTERFACE-ID [,|-]]
ip igmp snooping suppression-time	ip igmp snooping suppression-time SECONDS no ip igmp snooping suppression-time
ip igmp snooping minimum-version	ip igmp snooping minimum-version {2 | 3} no ip igmp snooping minimum-version

コマンド	コマンドとパラメーター
ip igmp snooping unknown-data expiry-time	ip igmp snooping unknown-data expiry-time SECONDS no ip igmp snooping unknown-data expiry-time
ip igmp snooping unknown-data learn	ip igmp snooping unknown-data learn no ip igmp snooping unknown-data learn
ip igmp snooping unknown-data limit	ip igmp snooping unknown-data limit NUMBER no ip igmp snooping unknown-data limit

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。

コマンド	コマンドとパラメーター
show ip igmp snooping	show ip igmp snooping [vlan VLAN-ID [,|-]]
show ip igmp snooping groups	show ip igmp snooping groups [vlan VLAN-ID [,|-] | GROUP-ADDRESS]
show ip igmp snooping mrouter	show ip igmp snooping mrouter [vlan VLAN-ID [,|-]]
show ip igmp snooping statistics	show ip igmp snooping statistics {interface [INTERFACE-ID [,|-]] | vlan [VLAN-ID [,|-]]}
show ip igmp snooping static-group	show ip igmp snooping static-group [GROUP-ADDRESS | vlan VLAN-ID [,|-]]
clear ip igmp snooping groups	clear ip igmp snooping groups {all | GROUP-ADDRESS [vlan VLAN-ID]}
clear ip igmp snooping statistics	clear ip igmp snooping statistics {all | vlan VLAN-ID | interface INTERFACE-ID}
clear ip igmp snooping unknown-data	clear ip igmp snooping unknown-data {all | vlan VLAN-ID | group GROUP-ADDRESS}

5.9.1 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。
シンタックス	**ip igmp snooping** **no ip igmp snooping**
パラメーター	なし
デフォルト	装置全体の IGMP スヌーピング機能は無効
コマンドモード	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	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。
制限事項	-
注意事項	IGMP スヌーピングで学習したマルチキャストグループへの中継は、MAC アドレスベースで処理されます。例えば、224.1.2.3 と 225.1.2.3 のマルチキャスト MAC アドレスは、どちらも 01:00:5E:01:02:03 となるので、224.1.2.3 宛てのマルチキャストデータを中継する際、225.1.2.3 で学習したメンバーポートにも中継さ

ip igmp snooping	
	れます。
対象バージョン	1.01.01

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)#
```

5.9.2 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。
シンタックス	**ip igmp snooping** **no ip igmp snooping**
パラメーター	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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.9.3 ip igmp snooping dyn-mr-aging-time

ip igmp snooping dyn-mr-aging-time	
目的	IGMP スヌーピングで学習したマルチキャストルーターポートのエージングアウト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。
シンタックス	**ip igmp snooping dyn-mr-aging-time** *SECONDS* **no ip igmp snooping dyn-mr-aging-time**
パラメーター	*SECONDS*：学習したマルチキャストルーターポートのエージングアウトタイムを 10～65,535 秒の範囲で指定します。
デフォルト	300 秒
コマンドモード	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	IGMP スヌーピングが有効の場合、マルチキャストパケット（PIM コントロールメッセージ、DVMRP コントロールメッセージ、IGMP クエリーメッセージ）を受信すると、マルチキャストルーターに接続されているインターフェースを装置が認

ip igmp snooping dyn-mr-aging-time	
	識します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：学習したマルチキャストルーターポートのエージングアウトタイムを 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)#
```

5.9.4 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。
シンタックス	**ip igmp snooping fast-leave** [**group-list** *ACCESS-LIST-NAME*] **no ip igmp snooping fast-leave**
パラメーター	**group-list** *ACCESS-LIST-NAME*（省略可能）：IGMP メンバーシップの即時脱退を有効にするアクセスリスト名を指定します。
デフォルト	無効
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	本コマンドが無効の場合、マルチキャストメンバーから IGMP 脱退メッセージを受信後、以下の計算式に基づいて算出された時間内に他のマルチキャストメンバーから IGMP report メッセージを受信しなかった場合に、所属するマルチキャストグループから離脱します。 • 装置が代表クエリアの場合の計算式：Last member query interval×Robustness value • 装置が非代表クエリアの場合の計算式：MaxResponseTime（代表クエリアから送信される GroupSpecificQuery 内の値）×Robustness value ただし、代表クエリアが存在しない場合は、IGMP 脱退メッセージを受信してもマルチキャストグループから離脱しません。
対象バージョン	1.01.01 1.06.01：**group-list** パラメーター追加

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)#
```

5.9.5 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て、誘発されるクエ

ip igmp snooping ignore-topology-change-notification	
	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。
シンタックス	**ip igmp snooping ignore-topology-change-notification** **no ip igmp snooping ignore-topology-change-notification**
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.9.6 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が Group-Specific クエリーメッセージ、または Group-Source-Specific クエリーメッセージを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。
シンタックス	**ip igmp snooping last-member-query-interval** *SECONDS* **no ip igmp snooping last-member-query-interval**
パラメーター	*SECONDS*：Group-Specific クエリーメッセージの送信間隔を 1～25 秒の範囲で指定します。
デフォルト	1 秒
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	IGMP 脱退メッセージを受信すると、IGMP スヌーピングクエリアは、応答期間が経過しても何もレポートを受信しなければ、インターフェース上にローカルメンバーが存在しないとみなします。期間を短く設定すれば、装置がグループ最後のメンバーの離脱を検知するまでの時間を短縮できます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、Group-Specific クエリーメッセージの送信間隔を 3 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ip igmp snooping last-member-query-interval 3
(config-vlan)#
```

5.9.7 ip igmp snooping mrouter

ip igmp snooping mrouter	
目的	指定したインターフェースをマルチキャストルーターポートとして設定します。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設定もできます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**ip igmp snooping mrouter** [**forbidden**] **interface** *INTERFACE-ID* [,|-] **no ip igmp snooping mrouter** [**forbidden**] **interface** *INTERFACE-ID* [,|-]
パラメーター	**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ポートとして設定する場合に指定します。 **interface** *INTERFACE-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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	IGMP スヌーピングマルチキャストルーターポートの設定なし
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	マルチキャストルーターポートは、設定する VLAN に所属しているポートまたはポートチャネルを指定して設定します。 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。 マルチキャストルーターポートは、動的な学習によるものと、静的に設定するものどちらでも構いません。IGMP スヌーピングエンティティーは、IGMP または PIM パケットを動的に学習し、マルチキャストルーターポートを識別します。
制限事項	-
注意事項	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、WARNING メッセージが表示されます。
対象バージョン	1.01.01

使用例：スタティックなマルチキャストルーターポートとして、VLAN 1 のポート 1/0/1 を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)#
```

5.9.8 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。

ip igmp snooping proxy-reporting	
シンタックス	**ip igmp snooping proxy-reporting** [**source** *IP-ADDRESS*] **no ip igmp snooping proxy-reporting**
パラメーター	**source** *IP-ADDRESS*（省略可能）：プロキシレポーティングの送信元 IP アドレスを指定します。デフォルトは 0.0.0.0 です。
デフォルト	無効
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	**source** *IP-ADDRESS* で指定した IP アドレスは、レポートの送信元 IP として使用されます。プロキシレポーティングの送信元 IP が設定されていないと、0.0.0.0 が使用されます。IP インターフェース MAC は、レポートの送信元 MAC として使用されます。VLAN に IP アドレスが設定されていない場合は、システム MAC が使用されます。
制限事項	-
注意事項	本コマンドを設定した VLAN インターフェースに IP アドレスを設定して使用してください。
対象バージョン	1.01.01

使用例：VLAN 1 で 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て、プロキシレポーティングメッセージの送信元 IP を 1.2.2.2 に設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping proxy-reporting source 1.2.2.2
(config-vlan)#
```

5.9.9 ip igmp snooping querier

ip igmp snooping querier	
目的	IGMP クエリア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。
シンタックス	**ip igmp snooping querier** **no ip igmp snooping querier**
パラメーター	なし
デフォルト	無効
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	IGMP クエリア機能を有効にすると、他の装置から送信された IGMP クエリーメッセージを確認します。IGMP クエリーメッセージが受信されると、IP アドレスの値が小さい方の装置がクエリアになります。
制限事項	IGMP クエリア機能を有効にするには、VLAN インターフェースが必要です。また、インターフェースに IP 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。
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 で、IGMP クエリア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 querier
(config-vlan)#
```

5.9.10 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 IGMP スヌーピングの一般クエリーメッセージ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。
シンタックス	**ip igmp snooping query-interval** *SECONDS* **no ip igmp snooping query-interval**
パラメーター	*SECONDS*：IGMP スヌーピングのクエリアが一般クエリーメッセージを送信する間隔を 1～31,744 秒の範囲で指定します。
デフォルト	125 秒
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、一般クエリーメッセージの送信間隔を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ip igmp snooping query-interval 300
(config-vlan)#
```

5.9.11 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ー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。
シンタックス	**ip igmp snooping query-max-response-time** *SECONDS* **no ip igmp snooping query-max-response-time**
パラメーター	*SECONDS*：IGMP スヌーピングのクエリーで通知される最大応答時間を 1～25 秒の範囲で指定します。
デフォルト	10 秒
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、クエリーで通知される最大応答時間を 20 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ip igmp snooping query-max-response-time 20
(config-vlan)#
```

5.9.12 ip igmp snooping query-version

ip igmp snooping query-version	
目的	IGMP スヌーピングのクエリアにより送信される一般クエリー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。
シンタックス	ip igmp snooping query-version {1 | 2 | 3} no ip igmp snooping query-version
パラメーター	1：IGMP スヌーピングのクエリアによって送信される一般クエリーのバージョンを 1 にする場合に指定します。 2：IGMP スヌーピングのクエリアによって送信される一般クエリーのバージョンを 2 にする場合に指定します。 3：IGMP スヌーピングのクエリアによって送信される一般クエリーのバージョンを 3 にする場合に指定します。
デフォルト	3
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	クエリーのバージョン番号は、クエリアの選択に反映されます。バージョン 1 に設定すると、IGMP スヌーピングは常にクエリアとして動作し、どのような IGMP 一般クエリーを受信しても、新しいクエリアの選択を開始しません。バージョン 2 またはバージョン 3 に設定した状態で、IGMPv2 または IGMPv3 の一般クエリーを受信すると、IGMP スヌーピングは新しいクエリアの選択を開始します。IGMPv1 の一般クエリーを受信した場合、IGMP スヌーピングは、新しいクエリアの選択を開始しません。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、一般クエリーのバージョンを 2 に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ip igmp snooping query-version 2
(config-vlan)#
```

5.9.13 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。
シンタックス	ip igmp snooping report-suppression no ip igmp snooping report-suppression
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	-

ip igmp snooping report-suppression	
対象バージョン	1.01.01

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)#
```

5.9.14 ip igmp snooping robustness-variable

ip igmp snooping robustness-variable	
目的	IGMP スヌーピングで使用する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。
シンタックス	**ip igmp snooping robustness-variable** *VALUE* **no ip igmp snooping robustness-variable**
パラメーター	*VALUE*：ロバストネス変数の値を 1～7 の範囲で指定します。
デフォルト	2
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	ロバストネス変数の値は、以下の IGMP メッセージ間隔の計算に使用されます。 • **Group member interval**：マルチキャストルーターが、現在のグループメンバー以外には、ネットワーク上にグループのメンバーが存在しないと判断するまでの時間です。 　• 計算式：(ロバストネス変数×クエリー間隔)＋(1×クエリー応答間隔) • **Other querier present interval**：マルチキャストルーターが、クエリアである別のマルチキャストルーターが存在しないと判断するまでの時間です。 　• 計算式：(ロバストネス変数×クエリー間隔)＋(0.5×クエリー応答間隔) • **Last member query count**：ルーターが、グループのローカルリスナーが存在しないとみなすまでに送信される、Group-Specific Query の数です。デフォルトの数はロバストネス変数の値です。 パケットロスが高いネットワークでは、この値を大きくすることにより IGMP の動作を安定させることができます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、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 1000
(config-vlan)# ip igmp snooping robustness-variable 3
(config-vlan)#
```

5.9.15 ip igmp snooping static-group

ip igmp snooping static-group	
目的	IGMP スヌーピングのスタティックグループを設定します。設定を削除する場合

ip igmp snooping static-group	
	は、no 形式のコマンドを使用します。
シンタックス	**ip igmp snooping static-group** *GROUP-ADDRESS* **interface** *INTERFACE-ID* [,|-] **no ip igmp snooping static-group** *GROUP-ADDRESS* [**interface** *INTERFACE-ID* [,|-]]
パラメーター	*GROUP-ADDRESS*：IP マルチキャストグループアドレスを指定します。 **interface** *INTERFACE-ID*：IGMP スヌーピングのスタティックグループに追加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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	スタティックグループの設定なし
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 で、IGMP スヌーピングのスタティックグループを設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping static-group 226.1.2.3 interface port 1/0/5
(config-vlan)#
```

5.9.16 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。
シンタックス	**ip igmp snooping suppression-time** *SECONDS* **no ip igmp snooping suppression-time**
パラメーター	*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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.9.17 ip igmp snooping minimum-version

ip igmp snooping minimum-version	
目的	インターフェース上で許容される IGMP ホスト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。
シンタックス	**ip igmp snooping minimum-version {2 | 3}** **no ip igmp snooping minimum-version**
パラメーター	**2**：IGMPv1 メッセージを除去する場合に指定します。 **3**：IGMPv1 メッセージと IGMPv2 メッセージを除去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
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	IGMP メンバーシップレポートの除去だけに適用されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 で、すべての IGMPv1 ホストの参加を制限する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping minimum-version 2
(config-vlan)#
```

使用例：VLAN 1 で、すべての IGMPv1 ホストと IGMPv2 ホストの参加を制限する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ip igmp snooping minimum-version 3
(config-vlan)#
```

使用例：VLAN 1 に設定された制限を削除する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# no ip igmp snooping minimum-version
(config-vlan)#
```

5.9.18 ip igmp snooping unknown-data expiry-time

ip igmp snooping unknown-data expiry-time	
目的	リスナーが存在しないマルチキャストパケットを受信したときに IGMP スヌーピングで学習したグループ情報の有効期限を指定します。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。
シンタックス	**ip igmp snooping unknown-data expiry-time** *SECONDS* **no ip igmp snooping unknown-data expiry-time**
パラメーター	*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
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-

ip igmp snooping unknown-data expiry-time	
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、リスナーが存在しないマルチキャストパケットを受信して学習したグループ情報の有効期限を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ip igmp snooping unknown-data expiry-time 300
(config-vlan)#
```

5.9.19 ip igmp snooping unknown-data learn

ip igmp snooping unknown-data learn	
目的	リスナーが存在しないマルチキャストパケットを受信したときにグループ情報を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。
シンタックス	**ip igmp snooping unknown-data learn** **no ip igmp snooping unknown-data learn**
パラメーター	なし
デフォルト	有効（**ip igmp snooping unknown-data learn**）
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	この機能が有効な場合、IGMP スヌーピングは、受信したマルチキャストパケットのグループ情報を学習します。グループ情報の学習は、メンバーシップ情報に登録されたことによって行われるのではなく、マルチキャストパケットを受信したことによって行われます。リスナーが存在しないマルチキャストパケットは、記録され、転送されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、リスナーが存在しないマルチキャストパケットを受信したときにグループ情報を学習する機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ip igmp snooping unknown-data learn
(config-vlan)#
```

5.9.20 ip igmp snooping unknown-data limit

ip igmp snooping unknown-data limit	
目的	IGMP スヌーピングによって、未知のマルチキャストパケットから学習するグループ情報の最大数を指定します。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。
シンタックス	**ip igmp snooping unknown-data limit** *NUMBER* **no ip igmp snooping unknown-data limit**
パラメーター	*NUMBER*：学習するグループ情報の最大数を、1～128 の範囲で指定します。
デフォルト	128

ip igmp snooping unknown-data limit	
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：未知のマルチキャストパケットから学習するグループ情報の最大数を 100 に設定する方法を示します。

```
# configure terminal
(config)# ip igmp snooping unknown-data limit 100
(config)#
```

5.9.21 show ip igmp snooping

show ip igmp snooping	
目的	IGMP スヌーピングの設定情報を表示します。
シンタックス	**show ip igmp snooping** [**vlan** *VLAN-ID* [,|-]]
パラメーター	**vlan** *VLAN-ID*（省略可能）：IGMP スヌーピングの設定情報を表示する VLAN を指定します。複数指定できます。
デフォルト	なし
コマンドモード	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情報を表示します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：IGMP スヌーピングの設定状態の表示方法を示します。

```
# show ip igmp snooping

IGMP snooping global state        : Disabled ...(1)
Dynamic mrouter aging time        : 300 seconds ...(2)
Unknown data limit                : 128 ...(3)

VLAN #1 configuration
    IGMP snooping state               : Enabled ...(4)
    Minimum version                   : v3 ...(5)
    Fast leave                        : Enabled (host-based) ...(6)
    Report suppression                : Enabled ...(7)
    Suppression time                  : 10 seconds ...(8)
    Querier state                     : Enabled (Non-active) ...(9)
    Query version                     : v3 ...(10)
    Query interval                    : 125 seconds ...(11)
    Max response time                 : 10 seconds ...(12)
    Robustness value                  : 2 ...(13)
    Last member query interval        : 1 seconds ...(14)
    Proxy reporting                   : Enabled (Source 1.2.3.4) ...(15)
    Unknown data learning             : Enabled ...(16)
    Unknown data expiry time          : Infinity ...(17)
    Ignore topology change            : Disabled ...(18)
```

```
Total Entries: 1
```

項番	説明
(1)	グローバル設定モードの IGMP スヌーピング機能の有効／無効を表示します。
(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アウトタイムを表示します。
(3)	未知のマルチキャストパケットから学習する最大グループ数を表示します。
(4)	VLAN 上の IGMP スヌーピング機能の有効／無効を表示します。
(5)	インターフェース上で許容される IGMP ホストの最小バージョンを表示します。
(6)	IGMP スヌーピングの高速離脱機能の有効／無効を表示します。 Enabled (host-based)：高速離脱が有効 Disabled (host-based)：高速離脱が無効
(7)	IGMP スヌーピングのレポート抑制機能の有効／無効を表示します。
(8)	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。
(9)	IGMP クエリア機能の有効／無効を表示します。
(10)	IGMP スヌーピングのクエリアによって送信される一般クエリーパケットのバージョンを表示します。
(11)	IGMP スヌーピングのクエリアが一般クエリーメッセージを定期的に送信する間隔を表示します。
(12)	IGMP スヌーピングのクエリーで通知される最大応答時間を表示します。
(13)	IGMP スヌーピングで使用するロバストネス変数の値を表示します。
(14)	脱退メッセージを受信したときに送信するクエリーの送信間隔を表示します。
(15)	IGMP スヌーピングのプロキシレポーティング機能の有効／無効を表示します。
(16)	リスナーが存在しないマルチキャストパケットを受信したときにグループ情報を学習する機能の有効／無効を表示します。
(17)	リスナーが存在しないマルチキャストパケットを受信したときに学習したグループ情報の有効期限を表示します。
(18)	スパニングツリープロトコルに起因するクエリーの送信禁止の設定を表示します。

5.9.22 show ip igmp snooping groups

show ip igmp snooping groups	
目的	学習した IGMP スヌーピンググループ情報を表示します。
シンタックス	**show ip igmp snooping groups** [**vlan** *VLAN-ID* [,|-] | *GROUP-ADDRESS*]
パラメーター	**vlan** *VLAN-ID*（省略可能）：IGMP スヌーピンググループ情報を表示する VLAN を指定します。複数指定できます。 *GROUP-ADDRESS*（省略可能）：IGMP スヌーピンググループ情報を表示するグループ IP アドレスを指定します。
デフォルト	なし
コマンドモード	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 スヌーピンググループ情報が表示されます。 IP アドレスを指定しない場合、すべての IGMP スヌーピンググループ情報が表示されます。
制限事項	-

show ip igmp snooping groups	
注意事項	-
対象バージョン	1.01.01

使用例：IGMP スヌーピンググループ情報の表示方法を示します。

```
# 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
-------  ---------------  ---------------  --   --------  ---------
1        239.255.255.250        *          EX   382       1/0/7

Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	グループアドレスを表示します。
(3)	送信元 IP アドレスを表示します。
(4)	FM グループフィルターモードを表示します。 EX：exclude IN：include
(5)	IGMP スヌーピングでの学習を終了する時間を表示します。
(6)	ポート番号またはポートチャネル番号を表示します。

5.9.23 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。
シンタックス	**show ip igmp snooping mrouter** [**vlan** *VLAN-ID* [,|-]]
パラメーター	**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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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の表示方法を示します。

```
# show ip igmp snooping mrouter
(1)    (2)
VLAN   Ports
-----  ----------------------------
1      1/0/4,1/0/8 (static)
       1/0/10 (forbidden)
       1/0/12 (dynamic)
2      1/0/14 (static)
       1/0/15 (dynamic)
```

```
Total Entries: 2
```

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。

5.9.24 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。
シンタックス	**show ip igmp snooping statistics {interface [*INTERFACE-ID* [,|-]] | vlan [*VLAN-ID* [,|-]]}**
パラメーター	**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。 *INTERFACE-ID*（省略可能）：IGMP スヌーピングの統計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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。 **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。
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	–
対象バージョン	1.01.01

使用例：IGMP スヌーピングの統計情報の表示方法を示します。

```
# show ip igmp snooping statistics interface port 1/0/1

Interface Port1/0/1 ...(1)
  IGMPv1 Rx: Report 0, Query 0
  IGMPv2 Rx: Report 0, Query 0, Leave 0
  IGMPv3 Rx: Report 0, Query 0
  IGMPv1 Tx: Report 0, Query 0
  IGMPv2 Tx: Report 1, Query 0, Leave 0
  IGMPv3 Tx: Report 0, Query 0

Total Entries: 1

# show ip igmp snooping statistics vlan 10


VLAN 10 Statistics: ...(2)
```

```
    IGMPv1 Rx: Report 0, Query 0
    IGMPv2 Rx: Report 1, Query 0, Leave 0
    IGMPv3 Rx: Report 0, Query 0
    IGMPv1 Tx: Report 0, Query 0
    IGMPv2 Tx: Report 1, Query 0, Leave 0
    IGMPv3 Tx: Report 0, Query 0

  Total Entries: 1
```

項番	説明
(1)	インターフェースの IGMP スヌーピングの統計情報を表示します。
(2)	VLAN の IGMP スヌーピングの統計情報を表示します。

5.9.25 show ip igmp snooping static-group

show ip igmp snooping static-group	
目的	スタティックに設定された IGMP スヌーピンググループ情報を表示します。
シンタックス	**show ip igmp snooping static-group** [*GROUP-ADDRESS* | **vlan** *VLAN-ID* [,|-]]
パラメーター	*GROUP-ADDRESS*（省略可能）：IGMP スヌーピンググループ情報を表示するグループ IP アドレスを指定します。 **vlan** *VLAN-ID*（省略可能）：IGMP スヌーピンググループ情報を表示する VLAN を指定します。複数指定できます。
デフォルト	なし
コマンドモード	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	グループ IP アドレスまたは VLAN を指定しない場合、スタティックに設定されたすべての IGMP スヌーピンググループ情報が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：スタティックに設定された IGMP スヌーピンググループ情報の表示方法を示します。

```
# show ip igmp snooping static-group
 (1)       (2)              (3)
VLAN ID  Group address    Interface
-------  ---------------  ------------------------
1        224.1.1.1        1/0/1

Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	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。

5.9.26 clear ip igmp snooping groups

clear ip igmp snooping groups	
目的	IGMP スヌーピングで動的に登録したグループのメンバーシップ情報をクリアします。

clear ip igmp snooping groups	
シンタックス	**clear ip igmp snooping groups** {**all** | *GROUP-ADDRESS* [**vlan** *VLAN-ID*]}
パラメーター	**all**：すべての動的な IGMP スヌーピンググループのメンバーシップ情報を削除する場合に指定します。 *GROUP-ADDRESS*：メンバーシップ情報を削除する動的な IGMP スヌーピンググループのグループ IP アドレスを指定します。 **vlan** *VLAN-ID*（省略可能）：メンバーシップ情報を削除する動的な IGMP スヌーピンググループの VLAN ID を指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：すべての動的な IGMP スヌーピンググループのメンバーシップ情報を削除する方法を示します。

```
# clear ip igmp snooping groups all
#
```

5.9.27 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。
シンタックス	**clear ip igmp snooping statistics** {**all** | **vlan** *VLAN-ID* | **interface** *INTERFACE-ID*}
パラメーター	**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** *INTERFACE-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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

5.9.28 clear ip igmp snooping unknown-data

clear ip igmp snooping unknown-data	
目的	リスナーが存在しないマルチキャストパケットを受信したときに IGMP スヌーピングが学習したグループ情報を削除します。
シンタックス	**clear ip igmp snooping unknown-data** {**all** | **vlan** *VLAN-ID* | **group** *GROUP-ADDRESS*}
パラメーター	**all**：すべての VLAN の関連するグループ情報を削除する場合に指定します。 **vlan** *VLAN-ID*：特定の VLAN の関連するグループ情報を削除する場合に指定します。 **group** *GROUP-ADDRESS*：特定のマルチキャストグループアドレスのグループ情報を削除する場合に指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：すべての VLAN の関連するグループ情報を削除する方法を示します。

```
# clear ip igmp snooping unknown-data all
#
```

5.10 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。

コマンド	コマンドとパラメーター
ipv6 mld snooping	ipv6 mld snooping no ipv6 mld snooping
ipv6 mld snooping (VLAN)	ipv6 mld snooping no ipv6 mld snooping
ipv6 mld snooping fast-leave	ipv6 mld snooping fast-leave [group-list ACCESS-LIST-NAME] no ipv6 mld snooping fast-leave
ipv6 mld snooping last-listener-query-interval	ipv6 mld snooping last-listener-query-interval SECONDS no ipv6 mld snooping last-listener-query-interval
ipv6 mld snooping mrouter	ipv6 mld snooping mrouter {interface INTERFACE-ID [,|-] | forbidden interface INTERFACE-ID [,|-] | learn pimv6} no ipv6 mld snooping mrouter {interface INTERFACE-ID [,|-] | forbidden interface INTERFACE-ID [,|-] | learn pimv6}
ipv6 mld snooping ignore-topology-change-notification	ipv6 mld snooping ignore-topology-change-notification no ipv6 mld snooping ignore-topology-change-notification
ipv6 mld snooping proxy-reporting	ipv6 mld snooping proxy-reporting [source IPV6-ADDRESS] no ipv6 mld snooping proxy-reporting
ipv6 mld snooping querier	ipv6 mld snooping querier no ipv6 mld snooping querier
ipv6 mld snooping query-interval	ipv6 mld snooping query-interval SECONDS no ipv6 mld snooping query-interval
ipv6 mld snooping query-max-response-time	ipv6 mld snooping query-max-response-time SECONDS no ipv6 mld snooping query-max-response-time
ipv6 mld snooping query-version	ipv6 mld snooping query-version {1 | 2} no ipv6 mld snooping query-version
ipv6 mld snooping report-suppression	ipv6 mld snooping report-suppression no ipv6 mld snooping report-suppression
ipv6 mld snooping robustness-variable	ipv6 mld snooping robustness-variable VALUE no ipv6 mld snooping robustness-variable
ipv6 mld snooping static-group	ipv6 mld snooping static-group IPV6-ADDRESS interface INTERFACE-ID [,|-] no ipv6 mld snooping static-group IPV6-ADDRESS [interface INTERFACE-ID [,|-]]
ipv6 mld snooping suppression-time	ipv6 mld snooping suppression-time SECONDS no ipv6 mld snooping suppression-time
ipv6 mld snooping minimum-version	ipv6 mld snooping minimum-version 2 no ipv6 mld snooping minimum-version
ipv6 mld snooping unknown-data expiry-time	ipv6 mld snooping unknown-data expiry-time SECONDS no ipv6 mld snooping unknown-data expiry-time

コマンド	コマンドとパラメーター
ipv6 mld snooping unknown-data learn	ipv6 mld snooping unknown-data learn no ipv6 mld snooping unknown-data learn
ipv6 mld snooping unknown-data limit	ipv6 mld snooping unknown-data limit NUMBER no ipv6 mld snooping unknown-data limit

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。

コマンド	コマンドとパラメーター
show ipv6 mld snooping	show ipv6 mld snooping [vlan VLAN-ID [,|-]]
show ipv6 mld snooping groups	show ipv6 mld snooping groups [IPV6-ADDRESS | vlan VLAN-ID [,|-]]
show ipv6 mld snooping mrouter	show ipv6 mld snooping mrouter [vlan VLAN-ID [,|-]]
show ipv6 mld snooping statistics	show ipv6 mld snooping statistics {interface [INTERFACE-ID [,|-]] | vlan [VLAN-ID [,|-]]}
show ipv6 mld snooping static-group	show ipv6 mld snooping static-group [IPV6-ADDRESS | vlan VLAN-ID [,|-]]
clear ipv6 mld snooping groups	clear ipv6 mld snooping groups {all | IPV6-ADDRESS [vlan VLAN-ID]}
clear ipv6 mld snooping statistics	clear ipv6 mld snooping statistics {all | vlan VLAN-ID | interface INTERFACE-ID}
clear ipv6 mld snooping unknown-data	clear ipv6 mld snooping unknown-data {all | vlan VLAN-ID | group GROUP-ADDRESS}

5.10.1 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。
シンタックス	**ipv6 mld snooping** **no ipv6 mld snooping**
パラメーター	なし
デフォルト	装置全体の MLD スヌーピング機能は無効
コマンドモード	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	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。
制限事項	-
注意事項	MLD スヌーピングで学習したマルチキャストグループへの中継は、MAC アドレスベースで処理されます。例えば、ff1e:111::102:304 と ff1e:222::102:304 のマルチキャスト MAC アドレスは、どちらも 33:33:01:02:03:04 となるので、ff1e:111::102:304 宛てのマルチキャストデータを中継する際、ff1e:222::102:304 で学習したメンバーポートにも中継されます。
対象バージョン	1.01.01

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)#
```

5.10.2 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。
シンタックス	**ipv6 mld snooping** **no ipv6 mld snooping**
パラメーター	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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.10.3 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。
シンタックス	**ipv6 mld snooping fast-leave** [**group-list** *ACCESS-LIST-NAME*] **no ipv6 mld snooping fast-leave**
パラメーター	**group-list** *ACCESS-LIST-NAME*（省略可能）：MLD メンバーシップの即時脱退を有効にするアクセスリスト名を指定します。
デフォルト	無効
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01 1.06.01：**group-list** パラメーター追加

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)#
```

5.10.4 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が Group-Specific クエリーメッセージ、または Group-Source-Specific クエリーメッセージを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。
シンタックス	**ipv6 mld snooping last-listener-query-interval** *SECONDS* **no ipv6 mld snooping last-listener-query-interval**
パラメーター	*SECONDS*：Group-Specific クエリーメッセージの送信間隔を 1～25 秒の範囲で指定します。
デフォルト	1 秒
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	MLD Done メッセージを受信し、レスポンス時間後にレポートを受信していない場合、MLD スヌーピングクエリアは、インターフェース上にローカルメンバーが存在しないとみなします。ユーザーは、インターバル時間を小さくすることで、グループ最後のメンバーの離脱を装置が検知するまでの時間を短縮できます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、Group-Specific クエリーメッセージの送信間隔を 3 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ipv6 mld snooping last-listener-query-interval 3
(config-vlan)#
```

5.10.5 ipv6 mld snooping mrouter

ipv6 mld snooping mrouter	
目的	指定したインターフェースをマルチキャストルーターポートとして設定します。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設定もできます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**ipv6 mld snooping mrouter {interface** *INTERFACE-ID* **[,|-] | forbidden interface** *INTERFACE-ID* **[,|-] | learn pimv6}** **no ipv6 mld snooping mrouter {interface** *INTERFACE-ID* **[,|-] | forbidden interface** *INTERFACE-ID* **[,|-] | learn pimv6}**
パラメーター	**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ポートとして設定する場合に指定します。 **interface** *INTERFACE-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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。

ipv6 mld snooping mrouter	
	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	IPv6 MLD スヌーピングマルチキャストルーターポート：設定なし 自動学習：有効
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	マルチキャストルーターポートは、設定する VLAN に所属しているポートまたはポートチャネルを指定して設定します。 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。 マルチキャストルーターポートは、動的な学習、および MLD スヌーピングエントリーへのスタティックな設定ができます。動的な学習では、相手装置がルーターであることを識別するために、MLD スヌーピングエントリーは MLD と PIM IPv6 パケットを確認します。
制限事項	-
注意事項	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、WARNING メッセージが表示されます。
対象バージョン	1.01.01

使用例：VLAN 1 で、ポート 1/0/1 を MLD スヌーピングマルチキャストルーターポートにする方法、およびポート 1/0/2 を MLD スヌーピングマルチキャストルーターポートにしない方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping mrouter interface port 1/0/1
(config-vlan)# ipv6 mld snooping mrouter forbidden interface port 1/0/2
(config-vlan)#
```

使用例：VLAN 4 で、マルチキャストルーターポートの自動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)#
```

5.10.6 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て、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。
シンタックス	**ipv6 mld snooping ignore-topology-change-notification** **no ipv6 mld snooping ignore-topology-change-notification**
パラメーター	なし
デフォルト	無効
コマンドモード	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

ipv6 mld snooping ignore-topology-change-notification	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.10.7 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。
シンタックス	**ipv6 mld snooping proxy-reporting** [**source** *IPV6-ADDRESS*] **no ipv6 mld snooping proxy-reporting**
パラメーター	**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
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	**source** *IPV6-ADDRESS* で指定した IPv6 アドレスは、レポートの送信元 IP として使用されます。 プロキシレポーティングの送信元 IP を指定しない場合、IP アドレスはゼロアドレスが適用されます。インターフェース MAC は、レポートの送信元 MAC として使用されます。VLAN に IP アドレスが設定されていない場合、システム MAC が使用されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.10.8 ipv6 mld snooping querier

ipv6 mld snooping querier	
目的	MLD クエリア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

ipv6 mld snooping querier	
	します。
シンタックス	**ipv6 mld snooping querier** **no ipv6 mld snooping querier**
パラメーター	なし
デフォルト	無効
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	MLD クエリア機能を有効にすると、他の装置から送信された MLD クエリーメッセージを確認します。MLD クエリーメッセージを受信すると、より低い値の IPv6 アドレスが設定されている装置がクエリアになります。
制限事項	MLD クエリア機能を有効にするには、VLAN インターフェースが必要です。また、インターフェースに IPv6 アドレスが設定されている必要があります。
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 で、MLD クエリア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 querier
(config-vlan)#
```

5.10.9 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、一般クエリーメッセージ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。
シンタックス	**ipv6 mld snooping query-interval** *SECONDS* **no ipv6 mld snooping query-interval**
パラメーター	*SECONDS*：MLD スヌーピングのクエリアが一般クエリーメッセージを送信する間隔を 1～31,744 秒の範囲で指定します。
デフォルト	125 秒
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、一般クエリーメッセージの送信間隔を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ipv6 mld snooping query-interval 300
(config-vlan)#
```

5.10.10 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ー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。
シンタックス	**ipv6 mld snooping query-max-response-time** *SECONDS* **no ipv6 mld snooping query-max-response-time**
パラメーター	*SECONDS*：MLD スヌーピングのクエリーで通知される最大応答時間を 1～25 秒の範囲で指定します。
デフォルト	10 秒
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、クエリーで通知される最大応答時間を 20 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ipv6 mld snooping query-max-response-time 20
(config-vlan)#
```

5.10.11 ipv6 mld snooping query-version

ipv6 mld snooping query-version	
目的	MLD スヌーピングのクエリアによって送信される、一般クエリー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。
シンタックス	**ipv6 mld snooping query-version** {1 | 2} **no ipv6 mld snooping query-version**
パラメーター	1：MLD スヌーピングのクエリアによって送信される一般クエリーのバージョンを 1 にする場合に指定します。 2：MLD スヌーピングのクエリアによって送信される一般クエリーのバージョンを 2 にする場合に指定します。
デフォルト	2
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、一般クエリーのバージョンを 1 に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ipv6 mld snooping query-version 1
(config-vlan)#
```

5.10.12 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。
シンタックス	**ipv6 mld snooping report-suppression** **no ipv6 mld snooping report-suppression**
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.10.13 ipv6 mld snooping robustness-variable

ipv6 mld snooping robustness-variable	
目的	MLD スヌーピングで使用される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。
シンタックス	**ipv6 mld snooping robustness-variable** *VALUE* **no ipv6 mld snooping robustness-variable**
パラメーター	*VALUE*：ロバストネス変数の値を 1～7 の範囲で指定します。
デフォルト	2
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	ロバストネス変数の値は、以下の MLD メッセージ間隔の計算で使用されます。 • **Group member interval**：マルチキャストルーターが、現在のグループメンバー以外には、ネットワーク上にグループのメンバーが存在しないと判断するまでの時間です。 　• 計算式：(ロバストネス変数×クエリー間隔)＋(1×クエリー応答間隔) • **Other querier present interval**：マルチキャストルーターが、クエリアである別のマルチキャストルーターが存在しないと判断するまでの時間です。 　• 計算式：(ロバストネス変数×クエリー間隔)＋(0.5×クエリー応答間隔) • **Last listener query count**：ルーターが、グループのローカルリスナーが存在しないとみなすまでに送信される、Group-Specific Query の数です。デフォルトの数はロバストネス変数の値です。 パケットロスが高いネットワークでは、この値を大きくすることにより MLD の動作を安定させることができます。

ipv6 mld snooping robustness-variable	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、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 1000
(config-vlan)# ipv6 mld snooping robustness-variable 3
(config-vlan)#
```

5.10.14 ipv6 mld snooping static-group

ipv6 mld snooping static-group	
目的	MLD スヌーピングのスタティック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。
シンタックス	**ipv6 mld snooping static-group** *IPV6-ADDRESS* **interface** *INTERFACE-ID* [,|-] **no ipv6 mld snooping static-group** *IPV6-ADDRESS* [**interface** *INTERFACE-ID* [,|-]]
パラメーター	*IPV6-ADDRESS*：IPv6 マルチキャストグループアドレスを指定します。 **interface** *INTERFACE-ID*：MLD スヌーピングのスタティックグループに追加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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	スタティックグループの設定なし
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 で、MLD スヌーピングのスタティックグループを設定する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping static-group ff02::12:03 interface port 1/0/5
(config-vlan)#
```

5.10.15 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。
シンタックス	**ipv6 mld snooping suppression-time** *SECONDS* **no ipv6 mld snooping suppression-time**
パラメーター	*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

ipv6 mld snooping suppression-time	
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.10.16 ipv6 mld snooping minimum-version

ipv6 mld snooping minimum-version	
目的	インターフェース上で許容される MLD ホスト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。
シンタックス	**ipv6 mld snooping minimum-version 2** **no ipv6 mld snooping minimum-version**
パラメーター	なし
デフォルト	最小バージョンの制限なし
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	MLD リスナーレポートの除去だけに適用されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 で、すべての MLDv1 ホストの参加を制限する方法を示します。

```
# configure terminal
(config)# vlan 1
(config-vlan)# ipv6 mld snooping minimum-version 2
(config-vlan)#
```

5.10.17 ipv6 mld snooping unknown-data expiry-time

ipv6 mld snooping unknown-data expiry-time	
目的	リスナーが存在しないマルチキャストパケットを受信したときに MLD スヌーピングで学習したグループ情報の有効期限を指定します。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。
シンタックス	**ipv6 mld snooping unknown-data expiry-time** *SECONDS* **no ipv6 mld snooping unknown-data expiry-time**
パラメーター	*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
コマンドモード	VLAN 設定モード
特権レベル	レベル：12

ipv6 mld snooping unknown-data expiry-time	
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、リスナーが存在しないマルチキャストパケットを受信して学習したグループ情報の有効期限を 300 秒に設定する方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ipv6 mld snooping unknown-data expiry-time 300
(config-vlan)#
```

5.10.18 ipv6 mld snooping unknown-data learn

ipv6 mld snooping unknown-data learn	
目的	リスナーが存在しないマルチキャストパケットを受信したときにグループ情報を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。
シンタックス	**ipv6 mld snooping unknown-data learn** **no ipv6 mld snooping unknown-data learn**
パラメーター	なし
デフォルト	有効（**ipv6 mld snooping unknown-data learn**）
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	この機能が有効な場合、MLD スヌーピングは、受信したマルチキャストパケットのグループ情報を学習します。グループ情報の学習は、メンバーシップ情報に登録されたことによって行われるのではなく、マルチキャストパケットを受信したことによって行われます。リスナーが存在しないマルチキャストパケットは、記録され、転送されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1000 で、リスナーが存在しないマルチキャストパケットを受信したときにグループ情報を学習する機能を有効にする方法を示します。

```
# configure terminal
(config)# vlan 1000
(config-vlan)# ipv6 mld snooping unknown-data learn
(config-vlan)#
```

5.10.19 ipv6 mld snooping unknown-data limit

ipv6 mld snooping unknown-data limit	
目的	MLD スヌーピングによって、未知のマルチキャストパケットから学習するグループ情報の最大数を指定します。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。
シンタックス	**ipv6 mld snooping unknown-data limit** *NUMBER* **no ipv6 mld snooping unknown-data limit**

ipv6 mld snooping unknown-data limit	
パラメーター	*NUMBER*：学習するグループ情報の最大数を、1～128 の範囲で指定します。
デフォルト	128
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：未知のマルチキャストパケットから学習するグループ情報の最大数を 100 に設定する方法を示します。

```
# configure terminal
(config)# ipv6 mld snooping unknown-data limit 100
(config)#
```

5.10.20 show ipv6 mld snooping

show ipv6 mld snooping	
目的	MLD スヌーピングの設定情報を表示します。
シンタックス	**show ipv6 mld snooping** [**vlan** *VLAN-ID* [,|-]]
パラメーター	**vlan** *VLAN-ID*（省略可能）：MLD スヌーピングの設定情報を表示する VLAN を指定します。複数指定できます。
デフォルト	なし
コマンドモード	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情報を表示します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MLD スヌーピングの設定状態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)

VLAN #1 configuration
    MLD snooping state                 : Enabled ...(3)
    Minimum version                    : v2 ...(4)
    Fast leave                         : Enabled (host-based) ...(5)
    Report suppression                 : Enabled ...(6)
    Suppression time                   : 10 seconds ...(7)
    Proxy reporting                    : Disabled (Source ::) ...(8)
    Mrouter port learning              : Enabled ...(9)
    Querier state                      : Enabled (Non-active) ...(10)
    Query version                      : v2 ...(11)
    Query interval                     : 125 seconds ...(12)
    Max response time                  : 10 seconds ...(13)
    Robustness value                   : 2 ...(14)
    Last listener query interval       : 1 seconds ...(15)
```

```
    Unknown data learning              : Enabled ...(16)
    Unknown data expiry time           : Infinity ...(17)
    Ignore topology change             : Disabled ...(18)

 Total Entries: 1
```

項番	説明
(1)	グローバル設定モードの MLD スヌーピング機能の有効／無効を表示します。
(2)	未知のマルチキャストパケットから学習可能な最大グループ数を表示します。
(3)	VLAN 上の MLD スヌーピング機能の有効／無効を表示します。
(4)	インターフェース上で許容される MLD ホストの最小バージョンを表示します。
(5)	MLD スヌーピングの高速離脱機能の有効／無効を表示します。 Enabled (host-based)：高速離脱が有効 Disabled (host-based)：高速離脱が無効
(6)	MLD スヌーピングのレポート抑制機能の有効／無効を表示します。
(7)	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。
(8)	MLD スヌーピングのプロキシレポーティング機能の有効／無効を表示します。
(9)	マルチキャストルーターポートの自動学習の有効／無効を表示します。
(10)	MLD クエリア機能の有効／無効を表示します。
(11)	MLD スヌーピングのクエリアによって送信される一般クエリーパケットのバージョンを表示します。
(12)	MLD スヌーピングのクエリアが一般クエリーメッセージを定期的に送信する間隔を表示します。
(13)	MLD スヌーピングのクエリーで通知される最大応答時間を表示します。
(14)	MLD スヌーピングで使用するロバストネス変数の値を表示します。
(15)	脱退メッセージを受信したときに送信するクエリーの送信間隔を表示します。
(16)	リスナーが存在しないマルチキャストパケットを受信したときにグループ情報を学習する機能の有効／無効を表示します。
(17)	リスナーが存在しないマルチキャストパケットを受信したときに学習したグループ情報の有効期限を表示します。
(18)	スパニングツリープロトコルに起因するクエリーの送信禁止の設定を表示します。

5.10.21 show ipv6 mld snooping groups

show ipv6 mld snooping groups	
目的	学習した MLD スヌーピンググループ情報を表示します。
シンタックス	**show ipv6 mld snooping groups** [*IPV6-ADDRESS* | **vlan** *VLAN-ID* [,|-]]
パラメーター	*IPV6-ADDRESS*（省略可能）：MLD スヌーピンググループ情報を表示する IPv6 アドレスを指定します。 **vlan** *VLAN-ID*（省略可能）：MLD スヌーピンググループ情報を表示する VLAN を指定します。複数指定できます。
デフォルト	なし
コマンドモード	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 アドレスを指定しない場合、すべての MLD スヌーピンググループ情報が表示されます。 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

show ipv6 mld snooping groups	
	ピンググループ情報が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：MLD スヌーピンググループ情報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
------- --------------------- ---------------------- -- --------   ---------
1       ff1e::                            *           EX 258        1/0/7
1       ff1e::3                           *           EX 258        1/0/7
1       ff1e::4                3620:110:1::3a2b       IN 258        1/0/7

Total Entries: 3
```

項番	説明
(1)	VLAN ID を表示します。
(2)	グループ IPv6 アドレスを表示します。
(3)	送信元 IP アドレスを表示します。
(4)	FM グループフィルターモードを表示します。 EX：exclude IN：include
(5)	MLD スヌーピングでの学習を終了する時間を表示します。
(6)	ポート番号またはポートチャネル番号を表示します。

5.10.22 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。
シンタックス	**show ipv6 mld snooping mrouter** [**vlan** *VLAN-ID* [,|-]]
パラメーター	**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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
-----   ----------------------------
```

```
1       1/0/4,1/0/8 (static)
        1/0/10 (forbidden)
        1/0/12 (dynamic)
3       1/0/14 (static)
        1/0/15 (dynamic)

Total Entries: 2
```

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。

5.10.23 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。
シンタックス	**show ipv6 mld snooping statistics** {**interface** [*INTERFACE-ID* [,|-]] | **vlan** [*VLAN-ID* [,|-]]}
パラメーター	**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。 *INTERFACE-ID*（省略可能）：MLD スヌーピングの統計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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。 **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。
デフォルト	なし
コマンドモード	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、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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：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 1/0/1,1/0/3-4

Interface Port1/0/1 ...(1)
  Rx: v1Report 1, v2Report 2, Query 1, v1Done 2
  Tx: v1Report 1, v2Report 2, Query 1, v1Done 2

Interface Port1/0/3
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface Port1/0/4
```

```
  Rx: v1Report 3, v2Report 0, Query 3, v1Done 0
  Tx: v1Report 2, v2Report 2, Query 1, v1Done 2

Total Entries: 3

# show ipv6 mld snooping statistics vlan 1

VLAN 1 Statistics: ...(2)
Rx: v1Report 3, v2Report 0, Query 3, v1Done 0
Tx: v1Report 2, v2Report 2, Query 1, v1Done 2

Total Entries: 1
```

項番	説明
(1)	インターフェースの MLD スヌーピングの統計情報を表示します。
(2)	VLAN の MLD スヌーピングの統計情報を表示します。

5.10.24 show ipv6 mld snooping static-group

show ipv6 mld snooping static-group	
目的	スタティックに設定された MLD スヌーピンググループ情報を表示します。
シンタックス	**show ipv6 mld snooping static-group** [*IPV6-ADDRESS* | **vlan** *VLAN-ID* [,|-]]
パラメーター	*IPV6-ADDRESS*（省略可能）：MLD スヌーピンググループ情報を表示するグループ IPv6 アドレスを指定します。 **vlan** *VLAN-ID*（省略可能）：MLD スヌーピンググループ情報を表示する VLAN を指定します。複数指定できます。
デフォルト	なし
コマンドモード	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	グループ IPv6 アドレスまたは VLAN を指定しない場合、スタティックに設定されたすべての MLD スヌーピンググループ情報が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：スタティックに設定された MLD スヌーピンググループ情報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
-------  ---------------                      -------------------------
1        ff1e::1                              1/0/1,1/0/5

Total Entries: 1
```

項番	説明
(1)	VLAN ID を表示します。
(2)	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。

5.10.25 clear ipv6 mld snooping groups

clear ipv6 mld snooping groups	
目的	MLD スヌーピングで動的に登録したグループのメンバーシップ情報をクリアします。
シンタックス	**clear ipv6 mld snooping groups** {**all** | *IPV6-ADDRESS* [**vlan** *VLAN-ID*]}
パラメーター	**all**：すべての動的な MLD スヌーピンググループのメンバーシップ情報を削除する場合に指定します。 *IPV6-ADDRESS*：メンバーシップ情報を削除する動的な MLD スヌーピンググループのグループ IPv6 アドレスを指定します。 **vlan** *VLAN-ID*（省略可能）：メンバーシップ情報を削除する動的な MLD スヌーピンググループの VLAN ID を指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：すべての動的な MLD スヌーピンググループのメンバーシップ情報を削除する方法を示します。

```
# clear ipv6 mld snooping groups all
#
```

5.10.26 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。
シンタックス	**clear ipv6 mld snooping statistics** {**all** | **vlan** *VLAN-ID* | **interface** *INTERFACE-ID*}
パラメーター	**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** *INTERFACE-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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

5.10.27 clear ipv6 mld snooping unknown-data

clear ipv6 mld snooping unknown-data	
目的	リスナーが存在しないマルチキャストパケットを受信したときに MLD スヌーピングが学習したグループ情報を削除します。
シンタックス	**clear ipv6 mld snooping unknown-data** {**all** | **vlan** *VLAN-ID* | **group** *GROUP-ADDRESS*}
パラメーター	**all**：すべての VLAN の関連するグループ情報を削除する場合に指定します。 **vlan** *VLAN-ID*：特定の VLAN の関連するグループ情報を削除する場合に指定します。 **group** *GROUP-ADDRESS*：特定のマルチキャストグループアドレスのグループ情報を削除する場合に指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：すべての VLAN の関連するグループ情報を削除する方法を示します。

```
# clear ipv6 mld snooping unknown-data all
#
```

5.11 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)関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ethernet ring g8032 profile	ethernet ring g8032 profile PROFILE-NAME no ethernet ring g8032 profile PROFILE-NAME
revertive (ERPS)	revertive no revertive
tcn-propagation	tcn-propagation no tcn-propagation
timer (ERPS)	timer {guard MILLI-SECONDS | hold-off SECONDS | wtr MINUTES} no timer [guard | hold-off | wtr]
ethernet ring g8032	ethernet ring g8032 RING-NAME no ethernet ring g8032 RING-NAME
port0	port0 interface INTERFACE-ID no port0
port1	port1 {interface INTERFACE-ID | none} no port1
instance (ERPS)	instance INSTANCE-ID no instance INSTANCE-ID
sub-ring	sub-ring SUB-RING-NAME no sub-ring SUB-RING-NAME
description (ERPS)	description DESCRIPTION no description
level	level MEL-VALUE no level
profile (ERPS)	profile PROFILE-NAME no profile PROFILE-NAME
rpl	rpl {port0 | port1} [owner] no rpl
r-aps channel-vlan	r-aps channel-vlan VLAN-ID no r-aps channel-vlan
inclusion-list vlan-ids	inclusion-list vlan-ids VLAN-ID [,|-] no inclusion-list vlan-ids VLAN-ID [,|-]
activate	activate no activate
show ethernet ring g8032	show ethernet ring g8032 {status | brief} [RING-NAME]

5.11.1 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

ethernet ring g8032 profile	
	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。
シンタックス	**ethernet ring g8032 profile** *PROFILE-NAME* **no ethernet ring g8032 profile** *PROFILE-NAME*
パラメーター	*PROFILE-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
コマンドモード	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	-
制限事項	最大登録可能数は 8 個です。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.2 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。
シンタックス	**revertive** **no revertive**
パラメーター	なし
デフォルト	有効
コマンドモード	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。
制限事項	-
注意事項	運用中は設定を変更しないでください。
対象バージョン	1.01.01

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)#
```

5.11.3 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。
シンタックス	tcn-propagation no tcn-propagation
パラメーター	なし
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.4 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。
シンタックス	timer {guard *MILLI-SECONDS* | hold-off *SECONDS* | wtr *MINUTES*} no timer [guard | hold-off | wtr]
パラメーター	guard *MILLI-SECONDS*：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
コマンドモード	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

timer (ERPS)	
	イマーがリセットされます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.5 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。
シンタックス	**ethernet ring g8032** *RING-NAME* **no ethernet ring g8032** *RING-NAME*
パラメーター	*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
コマンドモード	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	-
制限事項	最大登録可能数は 14 個です。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.6 port0

port0	
目的	リングの第 1 リングポートを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**port0 interface** *INTERFACE-ID* **no port0**
パラメーター	**interface** *INTERFACE-ID*：第 1 リングポート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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。

port0	
デフォルト	なし
コマンドモード	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
制限事項	ERPS 機能は、スパニングツリー、RPVST+、MMRP-Plus 機能とは併用できません。また、同一インターフェースでポートリダンダント、ループ検知機能（loop-detection action notify-only コマンド設定時を除く）と併用することはできません。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.7 port1

port1	
目的	リングの第 2 リングポートを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	port1 {interface *INTERFACE-ID* | none} no port1
パラメーター	interface *INTERFACE-ID*：第 2 リングポート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：物理ポートを指定します。 • port-channel：ポートチャネルを指定します。 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
コマンドモード	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
制限事項	ERPS 機能は、スパニングツリー、RPVST+、MMRP-Plus 機能とは併用できません。また、同一インターフェースでポートリダンダント、ループ検知機能（loop-detection action notify-only コマンド設定時を除く）と併用することはできません。

port1	
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.8 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。
シンタックス	**instance** *INSTANCE-ID* **no instance** *INSTANCE-ID*
パラメーター	*INSTANCE-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
コマンドモード	ERPS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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.9 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。
シンタックス	**sub-ring** *SUB-RING-NAME* **no sub-ring** *SUB-RING-NAME*
パラメーター	*SUB-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
コマンドモード	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。

sub-ring	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.10 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。
シンタックス	**description** *DESCRIPTION* **no description**
パラメーター	*DESCRIPTION*：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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.11 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。
シンタックス	**level** *MEL-VALUE* **no level**
パラメーター	*MEL-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
コマンドモード	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。
制限事項	CFM（Connectivity Fault Management）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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.12 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。
シンタックス	**profile** *PROFILE-NAME* **no profile** *PROFILE-NAME*
パラメーター	*PROFILE-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
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.13 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。
シンタックス	rpl {port0 | port1} [owner] no rpl
パラメーター	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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.11.14 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。
シンタックス	r-aps channel-vlan *VLAN-ID* no r-aps channel-vlan
パラメーター	*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。

r-aps channel-vlan	
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

5.11.15 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。
シンタックス	**inclusion-list vlan-ids** *VLAN-ID* [,|-] **no inclusion-list vlan-ids** *VLAN-ID* [,|-]
パラメーター	*VLAN-ID*：対象の ERP インスタンスで保護される VLAN 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
コマンドモード	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	-
制限事項	-
注意事項	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)
対象バージョン	1.01.01

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)#
```

5.11.16 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。
シンタックス	activate no activate
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	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 プロファイルを設定してください。
対象バージョン	1.01.01

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)#
```

5.11.17 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。
シンタックス	show ethernet ring g8032 {status | brief} [*RING-NAME*]
パラメーター	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）：ERP インスタンスの情報を表示するリングを指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-

show ethernet ring g8032	
対象バージョン	1.01.01

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。 －：リングポート設定なし
(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。

項番	説明
	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／無効を表示します。 Revertive：有効 Non-revertive：無効
(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)	リングプロテクション(ERPS)におけるノードの役割を表示します。 Owner：RPL オーナー None：役割なし
(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 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）

項番	説明
	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

5.12 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。

コマンド	コマンドとパラメーター
mmrp-plus enable	mmrp-plus enable no mmrp-plus enable
mmrp-plus switch hello-interval	mmrp-plus switch hello-interval TIME no mmrp-plus switch hello-interval
mmrp-plus switch polling-rate	mmrp-plus switch polling-rate RATE no mmrp-plus switch polling-rate
mmrp-plus vlangroup slave-vid	mmrp-plus vlangroup GROUP slave-vid VLAN-ID [,|-] no mmrp-plus vlangroup GROUP [slave-vid VLAN-ID [,|-]]
no mmrp-plus ring	no mmrp-plus ring RINGID [,|-]
mmrp-plus ring name	mmrp-plus ring RINGID [,|-] name NAME no mmrp-plus ring RINGID [,|-] name
mmrp-plus ring vid	mmrp-plus ring RINGID [,|-] vid VID no mmrp-plus ring RINGID [,|-] vid
mmrp-plus ring vlangroup	mmrp-plus ring RINGID [,|-] vlangroup GROUP no mmrp-plus ring RINGID [,|-] vlangroup
mmrp-plus ring ring-master	mmrp-plus ring RINGID ring-master master INTERFACE-ID slave INTERFACE-ID no mmrp-plus ring RINGID ring-master
mmrp-plus ring divided-master	mmrp-plus ring RINGID divided-master INTERFACE-ID no mmrp-plus ring RINGID divided-master
mmrp-plus ring divided-slave	mmrp-plus ring RINGID divided-slave INTERFACE-ID no mmrp-plus ring RINGID divided-slave
mmrp-plus ring aware	mmrp-plus ring RINGID aware INTERFACE-ID INTERFACE-ID no mmrp-plus ring RINGID aware
mmrp-plus ring revertive	mmrp-plus ring RINGID [,|-] revertive {REVERT-TIMER | disable} no mmrp-plus ring RINGID [,|-] revertive
mmrp-plus ring transmit-fdb-flush port	mmrp-plus ring RINGID [,|-] transmit-fdb-flush port INTERFACE-ID [,|-] no mmrp-plus ring RINGID [,|-] transmit-fdb-flush port
mmrp-plus ring transmit-fdb-flush retransmit enable	mmrp-plus ring RINGID [,|-] transmit-fdb-flush retransmit enable no mmrp-plus ring RINGID [,|-] transmit-fdb-flush retransmit enable
mmrp-plus ring fdb-flush port	mmrp-plus ring RINGID [,|-] fdb-flush port INTERFACE-ID [,|-] no mmrp-plus ring RINGID [,|-] fdb-flush port
mmrp-plus ring fdb-flush timer	mmrp-plus ring RINGID [,|-] fdb-flush timer TIME no mmrp-plus ring RINGID [,|-] fdb-flush timer

コマンド	コマンドとパラメーター
mmrp-plus ring listening-timer	mmrp-plus ring RINGID [,|-] listening-timer TIME no mmrp-plus ring RINGID [,|-] listening-timer
mmrp-plus ring hello-timeout	mmrp-plus ring RINGID [,|-] hello-timeout TIME no mmrp-plus ring RINGID [,|-] hello-timeout
mmrp-plus ring port-restart enable	mmrp-plus ring RINGID [,|-] port-restart enable no mmrp-plus ring RINGID [,|-] port-restart enable
mmrp-plus ring port-restart forcedown-time	mmrp-plus ring RINGID [,|-] port-restart forcedown-time TIME no mmrp-plus ring RINGID [,|-] port-restart forcedown-time
mmrp-plus ring port-restart linkup-wait	mmrp-plus ring RINGID [,|-] port-restart linkup-wait TIME no mmrp-plus ring RINGID [,|-] port-restart linkup-wait
mmrp-plus ring uplink port	mmrp-plus ring RINGID [,|-] uplink port INTERFACE-ID [,|-] no mmrp-plus ring RINGID [,|-] uplink port

MMRP-Plus 関連の show／操作コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show mmrp-plus configuration	show mmrp-plus configuration
show mmrp-plus configuration ring	show mmrp-plus configuration ring RINGID [,|-]
show mmrp-plus vlangroup	show mmrp-plus vlangroup [GROUP]
show mmrp-plus status	show mmrp-plus status
show mmrp-plus status port	show mmrp-plus status INTERFACE-ID [,|-]
show mmrp-plus status ring	show mmrp-plus status ring RINGID [,|-]
clear mmrp-plus failure ring	clear mmrp-plus failure ring RINGID [,|-]
debug mmrp	debug mmrp [event | hello | cpu | fdbflush] no debug mmrp [event | hello | cpu | fdbflush]

5.12.1 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。
シンタックス	**mmrp-plus enable** **no mmrp-plus enable**
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。

mmrp-plus enable	
制限事項	MMRP-Plus 機能は、スパニングツリー、RPVST+、ERPS 機能とは併用できません。また、同一インターフェースでポートリダンダント、ループ検知機能（loop-detection action notify-only コマンド設定時を除く）と併用することはできません。
注意事項	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。
対象バージョン	1.03.01

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)#
```

5.12.2 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。
シンタックス	**mmrp-plus switch hello-interval** *TIME* **no mmrp-plus switch hello-interval**
パラメーター	*TIME*：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
コマンドモード	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	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。
制限事項	-
注意事項	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。
対象バージョン	1.03.01

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)#
```

5.12.3 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。
シンタックス	**mmrp-plus switch polling-rate** *RATE* **no mmrp-plus switch polling-rate**
パラメーター	*RATE*：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

mmrp-plus switch polling-rate	
コマンドモード	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	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。
制限事項	-
注意事項	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。
対象バージョン	1.03.01

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)#
```

5.12.4 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。
シンタックス	**mmrp-plus vlangroup** *GROUP* **slave-vid** *VLAN-ID* [,|-] **no mmrp-plus vlangroup** *GROUP* [**slave-vid** *VLAN-ID* [,|-]]
パラメーター	*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 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
コマンドモード	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	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。
制限事項	-
注意事項	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

mmrp-plus vlangroup slave-vid	
	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。
対象バージョン	1.03.01

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)#
```

5.12.5 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。
シンタックス	**no mmrp-plus ring** *RINGID* [,|-]
パラメーター	*RINGID*：MMRP-Plus 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	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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)#
```

5.12.6 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **name** *NAME* **no mmrp-plus ring** *RINGID* [,|-] **name**
パラメーター	*RINGID*：MMRP-Plus 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。 *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
コマンドモード	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	-

mmrp-plus ring name	
制限事項	-
注意事項	-
対象バージョン	1.03.01

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)#
```

5.12.7 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **vid** *VID* **no mmrp-plus ring** *RINGID* [,|-] **vid**
パラメーター	*RINGID*：MMRP-Plus 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。 *VID*：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
コマンドモード	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	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。
制限事項	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。
注意事項	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。
対象バージョン	1.03.01

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)#
```

5.12.8 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **vlangroup** *GROUP* **no mmrp-plus ring** *RINGID* [,|-] **vlangroup**
パラメーター	*RINGID*：MMRP-Plus 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。 *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
コマンドモード	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	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。
制限事項	-
注意事項	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 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。
対象バージョン	1.03.01

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)#
```

5.12.9 mmrp-plus ring ring-master

mmrp-plus ring ring-master	
目的	シングルマスター構成における、マスター装置の MMRP-Plus リングポート（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。
シンタックス	**mmrp-plus ring** *RINGID* **ring-master master** *INTERFACE-ID* **slave** *INTERFACE-ID* **no mmrp-plus ring** *RINGID* **ring-master**
パラメーター	*RINGID*：MMRP-Plus のリング ID を 1～1000 の範囲で指定します。

mmrp-plus ring ring-master	
	master *INTERFACE-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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。 **slave** *INTERFACE-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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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	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。
制限事項	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、以下の機能を有効にしないでください。 • ループ検知機能（**loop-detection action notify-only** コマンド設定時を除く） • CFM
注意事項	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 の制御フレームの送出、および中継を他のフレームよりも優先させるため、MMRP-Plus のリングポートには **mls qos scheduler sp** コマンドを設定し、絶対優先度スケジューリングで使用してください。 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。
対象バージョン	1.03.01

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)#
```

5.12.10 mmrp-plus ring divided-master

mmrp-plus ring divided-master	
目的	分散マスター構成における、分散マスター装置の MMRP-Plus リングポート（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。
シンタックス	**mmrp-plus ring** *RINGID* **divided-master** *INTERFACE-ID*

mmrp-plus ring divided-master	
	no mmrp-plus ring *RINGID* **divided-master**
パラメーター	*RINGID*：MMRP-Plus のリング ID を 1～1000 の範囲で指定します。 *INTERFACE-ID*：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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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	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。
制限事項	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、以下の機能を有効にしないでください。 • ループ検知機能（**loop-detection action notify-only** コマンド設定時を除く） • CFM
注意事項	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 の制御フレームの送出、および中継を他のフレームよりも優先させるため、MMRP-Plus のリングポートには **mls qos scheduler sp** コマンドを設定し、絶対優先度スケジューリングで使用してください。 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。
対象バージョン	1.03.01

使用例：リング ID 3 のリングの分散マスター装置のリングポート（分散マスターポート）をポート 1/0/24 に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 3 divided-master port 1/0/24
(config)#
```

5.12.11 mmrp-plus ring divided-slave

mmrp-plus ring divided-slave	
目的	分散マスター構成における、分散スレーブ装置の MMRP-Plus リングポート（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。
シンタックス	**mmrp-plus ring** *RINGID* **divided-slave** *INTERFACE-ID* **no mmrp-plus ring** *RINGID* **divided-slave**
パラメーター	*RINGID*：MMRP-Plus のリング ID を 1～1000 の範囲で指定します。

mmrp-plus ring divided-slave	
	INTERFACE-ID：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：物理ポートを指定します。 • port-channel：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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	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。
制限事項	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、以下の機能を有効にしないでください。 • ループ検知機能（loop-detection action notify-only コマンド設定時を除く） • CFM
注意事項	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 の制御フレームの送出、および中継を他のフレームよりも優先させるため、MMRP-Plus のリングポートには mls qos scheduler sp コマンドを設定し、絶対優先度スケジューリングで使用してください。 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。
対象バージョン	1.03.01

使用例：リング ID 3 のリングの分散スレーブ装置のリングポート（分散マスターポート）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)#
```

5.12.12 mmrp-plus ring aware

mmrp-plus ring aware	
目的	アウェア装置の MMRP-Plus リングポート（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。
シンタックス	mmrp-plus ring *RINGID* aware *INTERFACE-ID INTERFACE-ID* no mmrp-plus ring *RINGID* aware
パラメーター	*RINGID*：MMRP-Plus のリング ID を 1～1000 の範囲で指定します。 *INTERFACE-ID*：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。

mmrp-plus ring aware	
	• port：物理ポートを指定します。 • port-channel：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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	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。
制限事項	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、以下の機能を有効にしないでください。 • ループ検知機能（loop-detection action notify-only コマンド設定時を除く） • CFM
注意事項	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 の制御フレームの送出、および中継を他のフレームよりも優先させるため、MMRP-Plus のリングポートには mls qos scheduler sp コマンドを設定し、絶対優先度スケジューリングで使用してください。 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。
対象バージョン	1.03.01

使用例：リング ID 5 のリングのアウェア装置のリングポート（アウェアポート）を、ポートチャネル 1 およびポート 1/0/1 に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 5 aware port-channel 1 port 1/0/1
(config)#
```

5.12.13 mmrp-plus ring revertive

mmrp-plus ring revertive	
目的	リンクダウン障害復旧後の Failure 状態からの切り戻り方法を選択します。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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **revertive** {*REVERT-TIMER* | **disable**} **no mmrp-plus ring** *RINGID* [,|-] **revertive**
パラメーター	*RINGID*：MMRP-Plus 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。 *REVERT-TIMER*：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）
コマンドモード	グローバル設定モード
特権レベル	レベル：12

mmrp-plus ring revertive	
ガイドライン	切り戻りタイマー値が 0 の場合は、リンクダウン障害復旧直後に 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、Failure 状態に遷移しません。 切り戻りタイマー値が 0 以外に設定されている場合は、リンクダウン障害復旧後に Failure 状態に遷移し、次に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。
制限事項	-
注意事項	-
対象バージョン	1.03.01

使用例：リング ID 5 のリングのリンクダウン障害復旧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)#
```

5.12.14 mmrp-plus ring transmit-fdb-flush port

mmrp-plus ring transmit-fdb-flush port	
目的	リングの経路が変更されたときに、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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **transmit-fdb-flush port** *INTERFACE-ID* [,|-] **no mmrp-plus ring** *RINGID* [,|-] **transmit-fdb-flush port**
パラメーター	*RINGID*：障害発生元となるリングのリング ID を 1～1000 の範囲で指定します。複数指定できます。 *INTERFACE-ID*：FDB フラッシュフレームを送信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
コマンドモード	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	障害発生時に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は、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てください。 *INTERFACE-ID* には、障害発生元とは異なるリングのポートを指定します。
制限事項	-
注意事項	-
対象バージョン	1.03.01

使用例：リング ID 3 のリングのリンクダウン障害発生時に、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)#
```

5.12.15 mmrp-plus ring transmit-fdb-flush retransmit enable

mmrp-plus ring transmit-fdb-flush retransmit enable	
目的	別リングへ送出される FDB フラッシュフレームを、分散マスター装置および分散スレーブ装置が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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **transmit-fdb-flush retransmit enable** **no mmrp-plus ring** *RINGID* [,|-] **transmit-fdb-flush retransmit enable**
パラメーター	*RINGID*：障害発生元となるリングのリング 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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

使用例：別リングへ送出される FDB フラッシュフレームを、分散マスター装置および分散スレーブ装置が中継する機能を、リング ID 3 で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)#
```

5.12.16 mmrp-plus ring fdb-flush port

mmrp-plus ring fdb-flush port	
目的	MMRP-Plus リングで障害発生時に 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **fdb-flush port** *INTERFACE-ID* [,|-] **no mmrp-plus ring** *RINGID* [,|-] **fdb-flush port**
パラメーター	*RINGID*：障害発生元となるリングのリング ID を 1～1000 の範囲で指定します。複数指定できます。 *INTERFACE-ID*：障害発生時に FDB エントリーを消去するポートを指定します。複数指定できます。
デフォルト	すべてのポートで FDB エントリーを消去する
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.03.01

使用例：リング ID 1 で障害発生時に、ポート 1/0/21 からポート 1/0/23 で FDB フラッシュする方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1 fdb-flush port 1/0/21-23
(config)#
```

5.12.17 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **fdb-flush timer** *TIME* **no mmrp-plus ring** *RINGID* [,|-] **fdb-flush timer**
パラメーター	*RINGID*：MMRP-Plus 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。 *TIME*：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
コマンドモード	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	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。
制限事項	-
注意事項	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。
対象バージョン	1.03.01

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)#
```

5.12.18 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **listening-timer** *TIME* **no mmrp-plus ring** *RINGID* [,|-] **listening-timer**
パラメーター	*RINGID*：MMRP-Plus 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。 *TIME*：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
コマンドモード	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	リスニングタイマーは、MMRP-Plus が設定されているポートがリンクアップした直後に遷移する Listening 状態のタイムアウト時間です。
制限事項	-
注意事項	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。
対象バージョン	1.03.01

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)#
```

5.12.19 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **hello-timeout** *TIME* **no mmrp-plus ring** *RINGID* [,|-] **hello-timeout**
パラメーター	*RINGID*：MMRP-Plus 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。 *TIME*：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）
コマンドモード	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	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
制限事項	-
注意事項	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。 LLDP 疑似リンクダウン機能（**lldp err-disable** コマンド）と併用する場合、受信タイムアウト時間は、LLDP のネイバー装置の情報保持時間（LLDPDU 送信間隔）より短くしないでください。 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。
対象バージョン	1.03.01

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（実際の動作では 9 秒）に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1 hello-timeout 10
(config)#
```

5.12.20 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **port-restart enable** **no mmrp-plus ring** *RINGID* [,|-] **port-restart enable**
パラメーター	*RINGID*：MMRP-Plus 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
コマンドモード	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	本機能は、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 MMRP-Plus アウェア機能未対応スイッチを接続する場合に使用します。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。
制限事項	リングに、アウェアポート（**mmrp-plus ring aware** コマンド）が設定されている場合は使用できません。 アップリンクポート連携機能（**mmrp-plus ring uplink port** コマンド）とは併用できません。 LLDP 疑似リンクダウン機能（**lldp err-disable** コマンド）とは併用できません。
注意事項	本機能を使用した MMRP-Plus アウェアスイッチとの接続はしないでください。 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。
対象バージョン	1.07.01

使用例：リング ID 1 からリング ID 2 の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 1-2 port-restart enable
(config)#
```

5.12.21 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **port-restart forcedown-time** *TIME* **no mmrp-plus ring** *RINGID* [,|-] **port-restart forcedown-time**
パラメーター	*RINGID*：MMRP-Plus 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。 *TIME*：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）
コマンドモード	グローバル設定モード

mmrp-plus ring port-restart forcedown-time	
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	forcedown-time が短い場合、対向スイッチの FDB がクリアされない場合があります。
対象バージョン	1.07.01

使用例：リング ID 1 からリング ID 2 のポートリスタート機能によるリンク瞬断時間を 1000 ミリ秒に設定する方法を示します。

```
# configure terminal
(config)# mmrp-plus ring 1-2 port-restart forcedown-time 10
(config)#
```

5.12.22 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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **port-restart linkup-wait** *TIME* **no mmrp-plus ring** *RINGID* [,|-] **port-restart linkup-wait**
パラメーター	*RINGID*：MMRP-Plus 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。 *TIME*：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）
コマンドモード	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	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。
制限事項	-
注意事項	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。
対象バージョン	1.07.01

使用例：リング ID 2 のポートリスタート機能によるリンク保護時間を 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)#
```

5.12.23 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

mmrp-plus ring uplink port	
	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。
シンタックス	**mmrp-plus ring** *RINGID* [,|-] **uplink port** *INTERFACE-ID* [,|-] **no mmrp-plus ring** *RINGID* [,|-] **uplink port**
パラメーター	*RINGID*：MMRP-Plus 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。 *INTERFACE-ID*：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
コマンドモード	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	本機能は、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、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。 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。
制限事項	本機能は、シングルマスター構成（**mmrp-plus ring ring-master** コマンド）の場合、またはリングにアウェアポート（**mmrp-plus ring aware** コマンド）が設定されている場合は使用できません。 ポートリスタート機能（**mmrp-plus ring port-restart enable** コマンド）とは併用できません。
注意事項	-
対象バージョン	1.07.01

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 からポート 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)#
```

5.12.24 show mmrp-plus configuration

show mmrp-plus configuration	
目的	MMRP-Plus の構成情報を表示します。
シンタックス	**show mmrp-plus configuration**
パラメーター	なし
デフォルト	なし

show mmrp-plus configuration	
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

使用例：MMRP-Plus の構成情報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              1/0/24     | 4014  1    -  2  0        1     10
```

項番	説明
(1)	MMRP-Plus の有効／無効を表示します。
(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。
(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。
(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)」を表示します。 シングルマスター構成では、スレーブポートに「(S)」を表示します。
(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設定を表示します。

項番	説明
	0：有効 －：無効
(11)	MMRP-Plus のリングに対応づけられた 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。 0：リンクダウン障害復旧直後に自動的に Listening 状態へ遷移 disable：手動切り戻り
(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。

5.12.25 show mmrp-plus configuration ring

show mmrp-plus configuration ring	
目的	MMRP-Plus のリング単位での構成情報を表示します。
シンタックス	**show mmrp-plus configuration ring** *RINGID* [,|-]
パラメーター	*RINGID*：MMRP-Plus 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	なし
コマンドモード	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	－
制限事項	－
注意事項	－
対象バージョン	1.03.01

使用例：リング ID 4 の MMRP-Plus の構成情報を表示する方法を示します。

```
# show mmrp-plus configuration ring 4

================================================================================
Ring ID             : 4 ...(1)
Ring name           : Ring004 ...(2)
Type                : Divided Slave ...(3)
Slave Port          : 1/0/24 ...(4)
VLAN ID             : 4014 ...(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              : 1/0/1-1/0/2 ...(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)	MMRP-Plus のリングに対応づけられた VLAN グループ番号を表示します。未設定の場合は Default と表示されます。 本項目はアウェアでは表示されません。
(7)	マスターVLAN を表示します。 本項目はアウェアでは表示されません。
(8)	スレーブ VLAN を表示します。 本項目はアウェアでは表示されません。
(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。 0：リンクダウン障害復旧直後に自動的に Listening 状態へ遷移 Disable：手動切り戻り
(14)	ポートリスタート機能の有効／無効を表示します。 本項目はアウェアでは表示されません。
(15)	ポートリスタート機能によるリンク瞬断時間を表示します。 本項目はアウェアでは表示されません。
(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。 本項目はアウェアでは表示されません。
(17)	リングが切り替わる際に、追加で FDB フラッシュフレームを送信するポート番号を表示します。 本項目はアウェア、シングルマスターでは表示されません。
(18)	FDB フラッシュフレーム中継機能の有効／無効を表示します。 本項目はアウェア、シングルマスターでは表示されません。
(19)	アップリンクポートに指定したポート番号を表示します。 本項目はアウェア、シングルマスターでは表示されません。

5.12.26 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。
シンタックス	**show mmrp-plus vlangroup** [*GROUP*]
パラメーター	*GROUP*（省略可能）：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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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。

5.12.27 show mmrp-plus status

show mmrp-plus status	
目的	MMRP-Plus の動作状態を表示します。
シンタックス	**show mmrp-plus status**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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)            (7)            (8)
 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。
(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)	リングポートのマスターVLAN およびスレーブ VLAN の抑止状態を表示します。 Blocking：ユーザーフレームを抑止（マスターポートではマスターVLAN を中継、スレーブポートではスレーブ VLAN を中継） Forwarding：すべてのユーザーフレームを中継 Down：障害発生中（すべてのフレームを破棄） FailureUp：障害復旧後（手動切り戻り実行前。すべてのフレームを破棄） Listening：リング復旧中（マスターポートおよびスレーブポートはハローフレームのみ送受信可能。アウェアポートはハローフレームのみを中継）
(8)	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。

5.12.28 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。
シンタックス	**show mmrp-plus status** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：動作状態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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし

show mmrp-plus status port	
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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 ...(10)
  Connection       : Broken ...(11)
-----------------------------------------------------------------
  (12)             (13)                    (14)
  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：デフォルトのアウェアポート • MMRP-Plus 有効後の MMRP-Plus ハローフレーム未受信時、または正常時とは反対方向の MMRP-Plus ハローフレーム受信時 Ring Aware Master：スレーブ方向に接続されたアウェアポート • スレーブポートからの MMRP-Plus ハローフレーム（HelloB1/HelloF1）受信時 Ring Aware Slave：マスター方向に接続されたアウェアポート • マスターポートからの MMRP-Plus ハローフレーム（HelloB2/HelloF2）受信時 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。
(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。 Blocking：リング正常時（マスターポートではマスターVLAN を中継、スレーブポートではスレーブ VLAN を中継） Forwarding：リング障害時（すべてのユーザーフレームを中継） Down：リングポートの障害発生中（すべてのフレームを破棄） FailureUp：障害復旧後（手動切り戻り実行前。すべてのフレームを破棄） Listening：リング復旧中（マスターポートおよびスレーブポートはハローフレームのみ送受信可能。アウェアポートはハローフレームのみを中継）
(10)	リングポートのマスターVLAN およびスレーブ VLAN の中継抑止状態を表示します。 Blocking：マスターVLAN、またはスレーブ VLAN のユーザーフレーム中継を抑止（マスターポートではスレーブ VLAN の中継を抑止、スレーブポートではマスターVLAN の中継を抑止） Forwarding：すべてのユーザーフレームを中継 Down、FailureUp、Listening：（9）と同様
(11)	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）
(12)	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
(13)	受信フレーム数を表示します。
(14)	送信フレーム数を表示します。

5.12.29 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。
シンタックス	**show mmrp-plus status ring** *RINGID* [,|-]
パラメーター	*RINGID*：MMRP-Plus 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	なし
コマンドモード	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	-

show mmrp-plus status ring	
制限事項	-
注意事項	-
対象バージョン	1.03.01

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 ...(10)
  Connection       : Normal ...(11)
-------------------------------------------------------------------
  (12)             (13)                    (14)
  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：デフォルトのアウェアポート • MMRP-Plus 有効後の MMRP-Plus ハローフレーム未受信時、または正常時とは反対方向の MMRP-Plus ハローフレーム受信時 Ring Aware Master：スレーブ方向に接続されたアウェアポート • スレーブポートからの MMRP-Plus ハローフレーム（HelloB1/HelloF1）受信時 Ring Aware Slave：マスター方向に接続されたアウェアポート • マスターポートからの MMRP-Plus ハローフレーム（HelloB2/HelloF2）受信時 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。
(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。 Blocking：リング正常時（マスターポートではマスターVLAN を中継、スレーブポートではスレーブ VLAN を中継） Forwarding：リング障害時（すべてのユーザーフレームを中継） Down：リングポートの障害発生中（すべてのフレームを破棄） FailureUp：障害復旧後（手動切り戻り実行前。すべてのフレームを破棄） Listening：リング復旧中（マスターポートおよびスレーブポートはハローフレームのみ送受信可能。アウェアポートはハローフレームのみを中継）
(10)	リングポートのマスターVLAN およびスレーブ VLAN の中継抑止状態を表示します。 Blocking：マスターVLAN、またはスレーブ VLAN のユーザーフレーム中継を抑止（マスターポートではスレーブ VLAN の中継を抑止、スレーブポートではマスターVLAN の中継を抑止） Forwarding：すべてのユーザーフレームを中継 Down、FailureUp、Listening：（9）と同様
(11)	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）
(12)	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

項番	説明
	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
(13)	受信フレーム数を表示します。
(14)	送信フレーム数を表示します。

5.12.30 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。
シンタックス	**clear mmrp-plus failure ring** *RINGID* [,|-]
パラメーター	*RINGID*：MMRP-Plus 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	なし
コマンドモード	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、FailureUp 状態のリングポートは 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。
制限事項	-
注意事項	-
対象バージョン	1.03.01

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
#
```

5.12.31 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。
シンタックス	**debug mmrp** [event | hello | cpu | fdbflush] **no debug mmrp** [event | hello | cpu | fdbflush]
パラメーター	**event**（省略可能）：イベント関連のデバッグ情報を有効にする場合に指定します。 **hello**（省略可能）：ハローパケット関連のデバッグ情報を有効にする場合に指定します。 **cpu**（省略可能）：CPU パケット関連のデバッグ情報を有効にする場合に指定します。 **fdbflush**（省略可能）：FDB フラッシュ関連のデバッグ情報を有効にする場合に指定します。
デフォルト	無効
コマンドモード	特権実行モード
特権レベル	レベル：15

debug mmrp	
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。
制限事項	-
注意事項	本コマンドはデバッグ目的の機能のため、運用環境で有効にすることは推奨しません。
対象バージョン	1.03.01

使用例：MMRP-Plus のデバッグ機能、およびイベント関連のデバッグ情報を有効にする方法を示します。

```
# debug mmrp
# debug mmrp event
#
```

5.13 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。

コマンド	コマンドとパラメーター
forward-bpdu global enable	forward-bpdu global enable no forward-bpdu global enable
spanning-tree global state	spanning-tree global state {enable | disable} no spanning-tree global state
spanning-tree mode	spanning-tree mode {mstp | rstp | stp | rpvst+} no spanning-tree mode
spanning-tree priority	spanning-tree priority PRIORITY no spanning-tree priority
spanning-tree (timers)	spanning-tree {hello-time SECONDS | forward-time SECONDS | max-age SECONDS} no spanning-tree {hello-time | forward-time | max-age}
spanning-tree tx-hold-count	spanning-tree tx-hold-count VALUE no spanning-tree tx-hold-count
spanning-tree nni-bpdu-address	spanning-tree nni-bpdu-address {dot1d | dot1ad} no spanning-tree nni-bpdu-address
spanning-tree state	spanning-tree state {enable | disable} no spanning-tree state
spanning-tree cost	spanning-tree cost COST no spanning-tree cost
spanning-tree guard root	spanning-tree guard root no spanning-tree guard root
spanning-tree link-type	spanning-tree link-type {point-to-point | shared} no spanning-tree link-type
spanning-tree portfast	spanning-tree portfast {disable | edge | network} no spanning-tree portfast
spanning-tree port-priority	spanning-tree port-priority PRIORITY no spanning-tree port-priority
spanning-tree tcnfilter	spanning-tree tcnfilter no spanning-tree tcnfilter
spanning-tree forward-bpdu	spanning-tree forward-bpdu no spanning-tree forward-bpdu
spanning-tree mst configuration	spanning-tree mst configuration no spanning-tree mst configuration
instance (MSTP)	instance INSTANCE-ID vlans VLAN-ID [,|-] no instance INSTANCE-ID [vlans VLAN-ID [,|-]]
name (MSTP)	name NAME no name NAME

コマンド	コマンドとパラメーター
revision (MSTP)	revision VERSION no revision
spanning-tree mst priority	spanning-tree mst INSTANCE-ID priority PRIORITY no spanning-tree mst INSTANCE-ID priority
spanning-tree mst hello-time	spanning-tree mst hello-time SECONDS no spanning-tree mst hello-time
spanning-tree mst max-hops	spanning-tree mst max-hops HOP-COUNT no spanning-tree mst max-hops
spanning-tree mst cost	spanning-tree mst INSTANCE-ID cost COST no spanning-tree mst INSTANCE-ID cost
spanning-tree mst port-priority	spanning-tree mst INSTANCE-ID port-priority PRIORITY no spanning-tree mst INSTANCE-ID port-priority
snmp-server enable traps stp	snmp-server enable traps stp [new-root] [topology-chg] no snmp-server enable traps stp [new-root] [topology-chg]

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。

コマンド	コマンドとパラメーター
show spanning-tree	show spanning-tree [interface INTERFACE-ID [,|-]]
show spanning-tree configuration interface	show spanning-tree configuration interface [INTERFACE-ID [,|-]]
show spanning-tree mst	show spanning-tree mst [configuration [digest]] show spanning-tree mst [instance INSTANCE-ID [,|-]] [interface INTERFACE-ID [,|-]] [detail]
clear spanning-tree detected-protocols	clear spanning-tree detected-protocols {all | interface INTERFACE-ID}

5.13.1 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。
シンタックス	**forward-bpdu global enable** **no forward-bpdu global enable**
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。

forward-bpdu global enable	
制限事項	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。
注意事項	-
対象バージョン	1.09.01

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)#
```

5.13.2 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。
シンタックス	spanning-tree global state {enable | disable} no spanning-tree global state
パラメーター	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）
コマンドモード	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	-
制限事項	スパニングツリー、および RPVST+機能は、ERPS、MMRP-Plus 機能とは併用できません。また、同一インターフェースでポートリダンダント、ループ検知（loop-detection action notify-only コマンド設定時を除く）、VLAN タグ変換機能と併用することはできません。 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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.3 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。
シンタックス	spanning-tree mode {mstp | rstp | stp | rpvst+} no spanning-tree mode
パラメーター	mstp：マルチプルスパニングツリープロトコル（MSTP）を使用する場合に指定します。 rstp：ラピッドスパニングツリープロトコル（RSTP）を使用する場合に指定しま

spanning-tree mode	
	す。 stp：スパニングツリープロトコル（IEEE 802.1D 準拠）を使用する場合に指定します。 rpvst+：ラピッド Per-VLAN スパニングツリープロトコル（RPVST+）を使用する場合に指定します。
デフォルト	RSTP
コマンドモード	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	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。
制限事項	VLAN タグ変換機能と RPVST+を同一ポートで併用できません。
注意事項	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。
対象バージョン	1.01.01

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)#
```

5.13.4 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。
シンタックス	spanning-tree priority *PRIORITY* no spanning-tree priority
パラメーター	*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
コマンドモード	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	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
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.5 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。
シンタックス	**spanning-tree {hello-time** *SECONDS* **| forward-time** *SECONDS* **| max-age** *SECONDS***}** **no spanning-tree {hello-time | forward-time | max-age}**
パラメーター	**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
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

5.13.6 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。
シンタックス	**spanning-tree tx-hold-count** *VALUE* **no spanning-tree tx-hold-count**
パラメーター	*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
コマンドモード	グローバル設定モード

spanning-tree tx-hold-count	
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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.7 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。
シンタックス	**spanning-tree nni-bpdu-address {dot1d | dot1ad}** **no spanning-tree nni-bpdu-address**
パラメーター	**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
コマンドモード	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、BPDU の宛先アドレスとして Customer Bridge Group Address が使用されます。 すべてのスパニングツリープロトコルに有効です。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.8 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。

spanning-tree state	
シンタックス	spanning-tree state {enable | disable} no spanning-tree state
パラメーター	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）
コマンドモード	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。
制限事項	スパニングツリー、および RPVST+機能は、ERPS、MMRP-Plus 機能とは併用できません。また、同一インターフェースでポートリダンダント、ループ検知（loop-detection action notify-only コマンド設定時を除く）、VLAN タグ変換機能と併用することはできません。
注意事項	spanning-tree state は、ブリッジングループを防ぐために慎重に使用してください。
対象バージョン	1.01.01

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)#
```

5.13.9 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。
シンタックス	spanning-tree cost *COST* no spanning-tree cost
パラメーター	*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
コマンドモード	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
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.10 spanning-tree guard root

spanning-tree guard root	
目的	ルートガード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。
シンタックス	spanning-tree guard root no spanning-tree guard root
パラメーター	なし
デフォルト	無効
コマンドモード	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、ポートがルートポートになることを防ぎます。ネットワークのコア領域への外部ブリッジがスパニングツリーアクティブトポロジーへ影響を与えるのを防ぐため、インターネットサービスプロバイダーの役に立ちます。この理由は、外部ブリッジが管理者の完全な管理下に存在しないことです。 ルートポートになることからポートを防ぐと、ポートは指定ポートとしての役割だけを果たします。ポートが優先度の高いコンフィグレーション BPDU を受信すると、ポートは閉塞状態にある代替ポートに変わります。受信した上位ファクターは、スパニングツリープロトコルの計算に加わりません。ポートはリンク上の BPDU を確認します。ポートは、上位 BPDU の受信タイムアウトを検出すると、ポートは指定された役割に変更されます。 ポートは、ルートガードのために代替ポート状態へ変化すると、システムメッセージを表示します。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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 がルートポートになることを防ぐ方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# spanning-tree guard root
(config-if-port)#
```

5.13.11 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。
シンタックス	spanning-tree link-type {point-to-point | shared}

spanning-tree link-type	
	no spanning-tree link-type
パラメーター	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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.12 spanning-tree portfast

spanning-tree portfast	
目的	Port Fast モードを指定します。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。
シンタックス	spanning-tree portfast {disable | edge | network} no spanning-tree portfast
パラメーター	disable：Port Fast モードを無効に設定する場合に指定します。 edge：Port Fast モードをエッジポートに設定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設定する場合に指定します。
デフォルト	network
コマンドモード	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。 ポートは、以下の 3 つの Port Fast モードのいずれかになります。 • Edge mode：リンクアップ時に、転送遅延時間（フォワードタイム）を待つことなく、ポートはフォワーディング状態に遷移します。その後、BPDU を受信すると、ポートは Non-port-fast 状態に変更されます。 • Disable mode：ポートは常に、Non-port-fast 状態です。フォワーディング状態に遷移する前に、常に転送遅延時間（フォワードタイム）の経

spanning-tree portfast	
	過を待ちます。 • **Network mode**：3 秒間、ポートは Non-port-fast 状態にとどまります。BPDU をまったく受信しない場合、ポートは port-fast 状態に変更され、フォワーディング状態に遷移します。その後、BPDU を受信すると、ポートは Non-port-fast 状態に変更されます。 Non-port-fast 状態では、転送遅延時間（フォワードタイム）を待って、リスニングからラーニング状態へ、あるいはラーニングからフォワーディング状態へ遷移します。
制限事項	Network mode は、RSTP モードまたは MSTP モードの場合のみ、有効です。
注意事項	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。
対象バージョン	1.01.01

使用例：ポート 1/0/7 を Port-fast edge モード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)#
```

5.13.13 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。
シンタックス	**spanning-tree port-priority** *PRIORITY* **no spanning-tree port-priority**
パラメーター	*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
コマンドモード	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
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.14 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。
シンタックス	spanning-tree tcnfilter no spanning-tree tcnfilter
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.15 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。
シンタックス	spanning-tree forward-bpdu no spanning-tree forward-bpdu
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	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

spanning-tree forward-bpdu	
	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.16 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。
シンタックス	spanning-tree mst configuration no spanning-tree mst configuration
パラメーター	なし
デフォルト	なし
コマンドモード	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	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) • 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）
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.17 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。

instance (MSTP)	
シンタックス	**instance** *INSTANCE-ID* **vlans** *VLAN-ID* [,|-] **no instance** *INSTANCE-ID* [**vlans** *VLAN-ID* [,|-]]
パラメーター	*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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.18 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。
シンタックス	**name** *NAME* **no name** *NAME*
パラメーター	*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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.19 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。
シンタックス	**revision** *VERSION* **no revision**
パラメーター	*VERSION*：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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.20 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。
シンタックス	**spanning-tree mst** *INSTANCE-ID* **priority** *PRIORITY* **no spanning-tree mst** *INSTANCE-ID* **priority**
パラメーター	*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
コマンドモード	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	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.21 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。
シンタックス	**spanning-tree mst hello-time** *SECONDS* **no spanning-tree mst hello-time**
パラメーター	*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
コマンドモード	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。
制限事項	MSTP ハロータイムは、MSTP だけで有効です。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.22 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。
シンタックス	**spanning-tree mst max-hops** *HOP-COUNT* **no spanning-tree mst max-hops**
パラメーター	**max-hops** *HOP-COUNT*：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
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.23 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。
シンタックス	**spanning-tree mst** *INSTANCE-ID* **cost** *COST* **no spanning-tree mst** *INSTANCE-ID* **cost**
パラメーター	*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
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.24 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。
シンタックス	**spanning-tree mst** *INSTANCE-ID* **port-priority** *PRIORITY* **no spanning-tree mst** *INSTANCE-ID* **port-priority**
パラメーター	*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
コマンドモード	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。
制限事項	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。
注意事項	-

spanning-tree mst port-priority	
対象バージョン	1.01.01

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)#
```

5.13.25 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。
シンタックス	snmp-server enable traps stp [new-root] [topology-chg] no snmp-server enable traps stp [new-root] [topology-chg]
パラメーター	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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.13.26 show spanning-tree

show spanning-tree	
目的	STP または RSTP の動作状況を表示します。
シンタックス	show spanning-tree [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID*（省略可能）：STP または RSTP の詳細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：物理ポートを指定します。複数指定できます。 • port-channel：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	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

show spanning-tree	
	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。
注意事項	-
対象バージョン	1.01.01

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: 00-40-66-A8-CC-36 ...(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／無効を表示します。
(2)	スパニングツリープロトコルを表示します。
(3)	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

項番	説明
	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

5.13.27 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情報を表示します。
シンタックス	**show spanning-tree configuration interface** [*INTERFACE-ID* [,|-]]
パラメーター	*INTERFACE-ID*（省略可能）：スパニングツリープロトコルの設定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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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情報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／無効を表示します。
(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。 auto：自動判別（全二重のポートはポイントツーポイントリンク、半二重のポートはシェアードリンクと判別される） 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／無効を表示します。
(10)	トポロジー変更通知（TCN）のフィルタリング機能の有効／無効を表示します。
(11)	BPDU のソフトウェア転送の有効／無効を表示します。

5.13.28 show spanning-tree mst

show spanning-tree mst	
目的	MSTP の情報を表示します。
シンタックス	show spanning-tree mst [configuration [digest]] show spanning-tree mst [instance *INSTANCE-ID* [,|-]] [interface *INTERFACE-ID* [,|-]] [detail]
パラメーター	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 *INTERFACE-ID*（省略可能）：MSTP 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：物理ポートを指定します。複数指定できます。 • port-channel：ポートチャネルを指定します。 detail（省略可能）：詳細情報を表示する場合に指定します。
デフォルト	なし
コマンドモード	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。

show spanning-tree mst	
	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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: 00-40-66-A8-CC-36, 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: 00-40-66-A8-CC-36, 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／無効を表示します。
(2)	スパニングツリープロトコルを表示します。

項番	説明
(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 BPUD 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。
(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。 auto：自動判別（全二重のポートはポイントツーポイントリンク、半二重のポートはシェアードリンクと判別される） 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。 auto：自動判別（全二重のポートはポイントツーポイントリンク、半二重のポートはシェアードリンクと判別される） 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

項番	説明
	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
(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。

5.13.29 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。
シンタックス	**clear spanning-tree detected-protocols** {**all** | **interface** *INTERFACE-ID*}
パラメーター	**all**：すべてのポートに検知動作を行わせます。 **interface** *INTERFACE-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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	–
対象バージョン	1.01.01

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
#
```

5.14 RPVST+コマンド

RPVST+（ラピッド Per-VLAN スパニングツリープラス）関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
spanning-tree vlan	spanning-tree vlan VLAN-ID no spanning-tree vlan VLAN-ID
spanning-tree vlan priority	spanning-tree vlan VLAN-ID priority PRIORITY no spanning-tree vlan VLAN-ID priority
spanning-tree vlan (timers)	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}
spanning-tree vlan cost	spanning-tree vlan VLAN-ID cost COST no spanning-tree vlan VLAN-ID cost
spanning-tree vlan port-priority	spanning-tree vlan VLAN-ID port-priority PRIORITY no spanning-tree vlan VLAN-ID port-priority
show spanning-tree vlan	show spanning-tree vlan [VLAN-ID]
show spanning-tree vlan interface	show spanning-tree vlan VLAN-ID interface INTERFACE-ID [,|-]

5.14.1 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。
シンタックス	**spanning-tree vlan** *VLAN-ID* **no spanning-tree vlan** *VLAN-ID*
パラメーター	*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
コマンドモード	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	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**
制限事項	サポートする VLAN 数は、装置全体で最大 200 個です。 スパニングツリー、および RPVST+機能は、ERPS、MMRP-Plus 機能とは併用できません。また、同一インターフェースでポートリダンダント、ループ検知（**loop-detection action notify-only** コマンド設定時を除く）、VLAN タグ変換機能と併用することはできません。 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 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。

spanning-tree vlan	
	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。

VLAN 数	各ポートの役割(Role)	ポート数
200	Root Port, Alternate Port, Backup Port	3
	Designated Port	3
100	Root Port, Alternate Port, Backup Port	6
	Designated Port	6
50	Root Port, Alternate Port, Backup Port	12
	Designated Port	12

注意事項	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。
対象バージョン	1.03.01

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)#
```

5.14.2 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。
シンタックス	**spanning-tree vlan** *VLAN-ID* **priority** *PRIORITY* **no spanning-tree vlan** *VLAN-ID* **priority**
パラメーター	*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
コマンドモード	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	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。
制限事項	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。
注意事項	-
対象バージョン	1.03.01

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)#
```

5.14.3 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。
シンタックス	**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**}
パラメーター	*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
コマンドモード	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	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*
制限事項	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。
注意事項	-
対象バージョン	1.03.01

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)#
```

5.14.4 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。
シンタックス	**spanning-tree vlan** *VLAN-ID* **cost** *COST* **no spanning-tree vlan** *VLAN-ID* **cost**
パラメーター	*VLAN-ID*：VLAN ID を、1～4094 の範囲で指定します。

spanning-tree vlan cost	
	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
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.03.01

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)#
```

5.14.5 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。
シンタックス	**spanning-tree vlan** *VLAN-ID* **port-priority** *PRIORITY* **no spanning-tree vlan** *VLAN-ID* **port-priority**
パラメーター	*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
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.03.01

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)#
```

5.14.6 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。
シンタックス	**show spanning-tree vlan** [*VLAN-ID*]
パラメーター	*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。
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	–
対象バージョン	1.03.01

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: 00-40-66-01-02-03 ...(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: 00-40-66-01-02-03 ...(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。

項番	説明
(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

5.14.7 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。
シンタックス	**show spanning-tree vlan** *VLAN-ID* **interface** *INTERFACE-ID* [,|-]
パラメーター	*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、1～4094 の範囲で指定します。 *INTERFACE-ID*：RPVST+詳細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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	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

show spanning-tree vlan interface	
	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。
注意事項	-
対象バージョン	1.03.01

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: 00-40-66-01-02-03
 (10)                                 (11)
 Designated bridge priority: 32768, address: 00-40-66-01-02-03
 (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。
(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

項番	説明
	ます。
(14)	ポートのリンクタイプの設定を表示します。 auto：自動判別（全二重のポートはポイントツーポイントリンク、半二重のポートはシェアードリンクと判別される） 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。

5.15 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）関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
traffic-segmentation forward	traffic-segmentation forward interface INTERFACE-ID [,|-] no traffic-segmentation forward interface INTERFACE-ID [,|-]
show traffic-segmentation forward	show traffic-segmentation forward [interface INTERFACE-ID [,|-]]

5.15.1 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。
シンタックス	**traffic-segmentation forward interface** *INTERFACE-ID* [,|-] **no traffic-segmentation forward interface** *INTERFACE-ID* [,|-]
パラメーター	**interface** *INTERFACE-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**：物理ポートを指定します。 • **range port**：物理ポートを範囲で指定します。
デフォルト	なし（転送ドメインは未設定）
コマンドモード	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 つでも指定した設定した場合は、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。
制限事項	レイヤー3 中継するトラフィックは、トラフィックセグメンテーション（中継パス制限）による転送先インターフェース制限の対象外で、トラフィックセグメンテーション（中継パス制限）の設定にかかわらずレイヤー3 中継されます。
注意事項	-
対象バージョン	1.01.01

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 からポート 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)#
```

5.15.2 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。
シンタックス	show traffic-segmentation forward [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID*（省略可能）：転送ドメイン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：物理ポートを指定します。 • range port：物理ポートを範囲で指定します。 • port-channel：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

5.16 VLAN コマンド

VLAN 関連の設定コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
vlan	vlan VLAN-ID [,|-] no vlan VLAN-ID [,|-]
name (VLAN)	name VLAN-NAME no name
switchport mode	switchport mode {access | hybrid | trunk | dot1q-tunnel} no switchport mode
switchport access vlan	switchport access vlan VLAN-ID no switchport access vlan
switchport trunk allowed vlan	switchport trunk allowed vlan {all | [add | remove | except] VLAN-ID [,|-]} no switchport trunk allowed vlan
switchport trunk native vlan	switchport trunk native vlan {VLAN-ID | tag} no switchport trunk native vlan [tag]
switchport hybrid allowed vlan	switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} VLAN-ID [,|-] no switchport hybrid allowed vlan
switchport hybrid native vlan	switchport hybrid native vlan VLAN-ID no switchport hybrid native vlan
protocol-vlan profile	protocol-vlan profile PROFILE-ID frame-type {ethernet2 | snap | llc} ether-type TYPE-VALUE no protocol-vlan profile PROFILE-ID
protocol-vlan profile (Interface)	protocol-vlan profile PROFILE-ID vlan VLAN-ID [priority COS-VALUE] no protocol-vlan profile [PROFILE-ID]
acceptable-frame	acceptable-frame {tagged-only | untagged-only | admit-all} no acceptable-frame
ingress-checking	ingress-checking no ingress-checking

VLAN 関連の show コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show vlan	show vlan [VLAN-ID [,|-] | interface [INTERFACE-ID [,|-]] | detail]
show protocol-vlan	show protocol-vlan {profile [PROFILE-ID [,|-]] | interface [INTERFACE-ID [,|-]]}

5.16.1 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。
シンタックス	**vlan** *VLAN-ID* [,|-] **no vlan** *VLAN-ID* [,|-]
パラメーター	*VLAN-ID*：作成・変更する VLAN 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
コマンドモード	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	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.16.2 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。
シンタックス	**name** *VLAN-NAME* **no name**
パラメーター	*VLAN-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）
コマンドモード	VLAN 設定モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.16.3 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。
シンタックス	switchport mode {access | hybrid | trunk | dot1q-tunnel} no switchport mode
パラメーター	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
コマンドモード	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。 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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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)#
```

5.16.4 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。
シンタックス	**switchport access vlan** *VLAN-ID* **no switchport access vlan**
パラメーター	*VLAN-ID*：インターフェースのアクセス VLAN を指定します。指定した VLAN ID の VLAN が存在しない場合は、VLAN が自動的に作成されます。
デフォルト	VLAN 1
コマンドモード	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。 アクセスモード、またはトンネルモードに設定されているインターフェースに有効です。 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、前のコマンドが上書きされます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 を、アクセス VLAN 1000 でアクセス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 mode access
(config-if-port)# switchport access vlan 1000
(config-if-port)#
```

5.16.5 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。
シンタックス	**switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] *VLAN-ID* [,|-]} **no switchport trunk allowed vlan**
パラメーター	**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、VLAN を追加する場合に指定します。

switchport trunk allowed vlan	
	remove（省略可能）：許可する VLAN のリストから、VLAN を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、指定した VLAN 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 を指定します。複数指定できます。**add** 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）
コマンドモード	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。 トランクモードのインターフェースで設定できます。 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。
制限事項	-
注意事項	**add** 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 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。
対象バージョン	1.01.01

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)#
```

5.16.6 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。
シンタックス	**switchport trunk native vlan** {*VLAN-ID* | **tag**} **no switchport trunk native vlan** [**tag**]
パラメーター	*VLAN-ID*：トランクポートのネイティブ VLAN を指定します。指定した VLAN ID の VLAN が存在しない場合でも設定はできますが、VLAN は自動的に作成されません。 **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。

switchport trunk native vlan	
デフォルト	ネイティブ VLAN は 1 で、タグなしモード
コマンドモード	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。 トランクモードのインターフェースで設定できます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 をトランクモードに設定し、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)#
```

5.16.7 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。
シンタックス	**switchport hybrid allowed vlan {[add] {tagged | untagged} | remove}** *VLAN-ID* [,|-] **no switchport hybrid allowed vlan**
パラメーター	**add**（省略可能）：許可する VLAN のリストに、VLAN を追加する場合に指定します。 **remove**：許可する VLAN のリストから、VLAN を削除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。 *VLAN-ID*：VLAN ID を指定します。複数指定できます。**add** 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）
コマンドモード	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。 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。

switchport hybrid allowed vlan	
	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。
制限事項	-
注意事項	**add** 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 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。
対象バージョン	1.01.01

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)#
```

5.16.8 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。
シンタックス	**switchport hybrid native vlan** *VLAN-ID* **no switchport hybrid native vlan**
パラメーター	*VLAN-ID*：ハイブリッドポートのネイティブ VLAN を指定します。指定した VLAN ID の VLAN が存在しない場合でも設定はできますが、VLAN は自動的に作成されません。
デフォルト	VLAN 1
コマンドモード	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。 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。 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

switchport hybrid native vlan	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 をハイブリッドモードに設定し、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)#
```

5.16.9 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。
シンタックス	protocol-vlan profile *PROFILE-ID* frame-type {ethernet2 | snap | llc} ether-type *TYPE-VALUE* no protocol-vlan profile *PROFILE-ID*
パラメーター	*PROFILE-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 *TYPE-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
コマンドモード	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	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。
制限事項	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。 プロトコルグループを削除すると、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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.16.10 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。
シンタックス	**protocol-vlan profile** *PROFILE-ID* **vlan** *VLAN-ID* [**priority** *COS-VALUE*] **no protocol-vlan profile** [*PROFILE-ID*]
パラメーター	*PROFILE-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
コマンドモード	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。 ハイブリッドモード、またはトンネルモードのインターフェースで設定できます。 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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

5.16.11 acceptable-frame

acceptable-frame	
目的	受け付け可能なフレー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。
シンタックス	**acceptable-frame** {**tagged-only** | **untagged-only** | **admit-all**} **no acceptable-frame**
パラメーター	**tagged-only**：タグ付きフレームのみを受け入れる場合に指定します。 **untagged-only**：タグなしフレームのみを受け入れる場合に指定します。 **admit-all**：すべてのフレームを受け入れる場合に指定します。
デフォルト	アクセス VLAN モード：untagged-only 他の VLAN モード：admit-all
コマンドモード	インターフェース設定モード(port, range, port-channel)

acceptable-frame	
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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 で受け付け可能なフレームタイプとして、tagged-only を指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)#
```

5.16.12 ingress-checking

ingress-checking	
目的	受信したフレームの受け入れ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。
シンタックス	ingress-checking no ingress-checking
パラメーター	なし
デフォルト	有効（ingress-checking）
コマンドモード	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。 受け入れチェックが有効で、受信したインターフェースが受信パケットの所定の VLAN に所属するインターフェースではない場合、パケットは廃棄されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の受け入れチェックを有効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)#
```

5.16.13 show vlan

show vlan	
目的	装置上のすべての VLAN のパラメーター、または指定した 1 つの VLAN のパラメーターを表示します。
シンタックス	show vlan [*VLAN-ID* [,|-] | interface [*INTERFACE-ID* [,|-]] | detail]
パラメーター	*VLAN-ID*（省略可能）：メンバーポート情報を表示する VLAN を 1～4094 の範囲で指定します。複数指定できます。

show vlan	
	interface：インターフェースの VLAN 関連の設定を表示する場合に指定します。 *INTERFACE-ID*（省略可能）：VLAN 関連の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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。 **detail**（省略可能）：VLAN の詳細情報を表示する場合に指定します。
デフォルト	なし
コマンドモード	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。 **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 VLAN 関連の設定情報が表示されます。
制限事項	–
注意事項	–
対象バージョン	1.01.01 1.03.01：**detail** パラメーター追加

使用例：現在のすべての VLAN エントリー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 : 1/0/21-1/0/28 ...(5)
 VLAN 100
   Name : VLAN0100
   Description :
   Tagged Member Ports   : 1/0/25-1/0/26
   Untagged Member Ports : 1/0/1-1/0/10
 VLAN 200
   Name : VLAN0200
   Description :
   Tagged Member Ports   : 1/0/25-1/0/26
   Untagged Member Ports : 1/0/11-1/0/20
 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：ポート 1/0/1 からポート 1/0/6 について、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 ...(8)
    Acceptable frame type  : Untagged-Only ...(9)

  Port1/0/2
    VLAN mode              : Trunk
    Native VLAN            : 1 (Untagged) ...(4)
    Trunk allowed VLAN     : 1-4094 ...(5)
    Ingress checking       : Enabled
    Acceptable frame type  : Admit-All

  Port1/0/3
    VLAN mode              : Hybrid
    Native VLAN            : 1
    Hybrid untagged VLAN   : 1,50,60 ...(6)
    Hybrid tagged VLAN     : 10,20 ...(7)
    Ingress checking       : Enabled
    Acceptable frame type  : Admit-All

  Port1/0/4
    VLAN mode              : Dot1q-Tunnel
    Access VLAN            : 10
    Hybrid untagged VLAN   : 50,60
    Ingress checking       : Enabled
    Acceptable frame type  : Admit-All

  Port1/0/5
    VLAN mode              : Promiscuous
    Native VLAN            : 100
    Ingress checking       : Enabled
    Acceptable frame type  : Admit-All

  Port1/0/6
    VLAN mode              : Host
    Native VLAN            : 101
    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 VLAN の VLAN ID を表示します。
(4)	ネイティブ VLAN の VLAN ID を表示します。
(5)	トランクポートで送受信できる VLAN ID を表示します。
(6)	タグなしフレームとして送受信できる VLAN ID を表示します。
(7)	タグ付きフレームとして送受信できる VLAN ID を表示します。
(8)	受け入れチェックの有効／無効を表示します。
(9)	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

項番	説明
	Untagged-Only：タグなしフレームのみ Admit-All：すべてのフレーム

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     16 17    24 25
                  +------+ +------+ +------+ +---
 Port Mode      1 aaaaaaaa aaaaaaaa aaaaaaaa ttaa

--- vlan mapping information --- ...(2)
                u = untag  t = tag
                C Port
                  1      8 9     16 17    24 25
 Name       VID  +------+ +------+ +------+ +---
default       1 1 ........ ........ ....uuuu uuuu
VLAN0100    100 1 uuuuuuuu uu...... ........ tt..
VLAN0200    200 1 ........ ..uuuuuu uuuu.... 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。

5.16.14 show protocol-vlan

show protocol-vlan	
目的	プロトコル VLAN の設定情報を表示します。
シンタックス	**show protocol-vlan** {**profile** [*PROFILE-ID* [,|-]] | **interface** [*INTERFACE-ID* [,|-]]}
パラメーター	**profile**：プロトコルグループの設定情報を表示する場合に指定します。 *PROFILE-ID*（省略可能）：設定情報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。 *INTERFACE-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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。

show protocol-vlan	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：すべてのプロトコルグループの設定情報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。
(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 からポート 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。

5.17 プライベート VLAN コマンド

プライベート VLAN 関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
private-vlan	private-vlan {community | isolated | primary} no private-vlan {community | isolated | primary}
private-vlan association	private-vlan association {add SECONDARY-VLAN-ID [,|-] | remove SECONDARY-VLAN-ID [,|-]} no private-vlan association
switchport mode private-vlan	switchport mode private-vlan {host | promiscuous} no switchport mode
switchport private-vlan host-association	switchport private-vlan host-association PRIMARY-VLAN-ID SECONDARY-VLAN-ID no switchport private-vlan host-association
switchport private-vlan mapping	switchport private-vlan mapping PRIMARY-VLAN-ID {add SECONDARY-VLAN-ID [,|-] | remove SECONDARY-VLAN-ID [,|-]} no switchport private-vlan mapping
show vlan private-vlan	show vlan private-vlan
private-vlan synchronize	private-vlan synchronize

5.17.1 private-vlan

private-vlan	
目的	プライベート VLAN として 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。
シンタックス	private-vlan {community | isolated | primary} no private-vlan {community | isolated | primary}
パラメーター	community：VLAN を、プライベート VLAN ドメインの中のコミュニティーVLAN として設定する場合に指定します。コミュニティーVLAN 内のメンバーポート同士のやりとりが可能です。レイヤー2 での他のコミュニティーのメンバーポートとは、やりとりできません。 isolated：VLAN を、プライベート VLAN ドメインの中の独立 VLAN として設定する場合に指定します。独立 VLAN のメンバーポート同士のやりとりはできません。レイヤー2 でのコミュニティーVLAN のメンバーポートとは、やりとりできません。 primary：VLAN を、プライベート VLAN ドメインの中のプライマリーVLAN として設定する場合に指定します。
デフォルト	なし
コマンドモード	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 ドメインは、1 つのプライマリーVLAN、1 つの独立 VLAN、および複数のコミュニティーVLAN で定義されます。他のプライベート VLAN 設定コマンドで参照されることを前提として、プライベート VLAN の役割を指定するコマンドです。
制限事項	-

private-vlan	
注意事項	-
対象バージョン	1.01.01

使用例：VLAN をプライベート VLAN として設定する方法を示します。以下の例では、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)#
```

5.17.2 private-vlan association

private-vlan association	
目的	セカンダリーVLAN をプライマリーVLAN に関連付けます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	private-vlan association {add *SECONDARY-VLAN-ID* [,|-] | remove *SECONDARY-VLAN-ID* [,|-]} no private-vlan association
パラメーター	add *SECONDARY-VLAN-ID*：プライマリーVLAN へセカンダリーVLAN を関連付ける場合に、セカンダリーVLAN の VLAN ID を、2～4094 の範囲で指定します。複数指定できます。 remove *SECONDARY-VLAN-ID*：プライマリーVLAN とセカンダリーVLAN の関連付けを削除する場合に、セカンダリーVLAN の VLAN ID 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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.17.3 switchport mode private-vlan

switchport mode private-vlan	
目的	プライベート VLAN ホストポート、またはプロミスキャスポートとして、ポートを指定します。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。

switchport mode private-vlan	
シンタックス	**switchport mode private-vlan {host | promiscuous}** **no switchport mode**
パラメーター	**host**：セカンダリーVLAN 用のポート（独立ポートまたはコミュニティーポート）として、ポートを設定する場合に指定します。 **promiscuous**：プライマリーVLAN 用のポート（プロミスキャスポート）として、ポートを設定する場合に指定します。
デフォルト	アクセス VLAN モードとして設定済み
コマンドモード	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。 独立ポートまたはコミュニティーポートは、**switchport mode private-vlan host** コマンドでポートモードを設定し、**switchport private-vlan host-association** コマンドでセカンダリーVLAN を割り当てます。 プロミスキャスポートは、**switchport mode private-vlan promiscuous** コマンドでポートモードを設定し、**switchport private-vlan mapping** コマンドでプライマリーVLAN とセカンダリーVLAN を割り当てます。 スイッチ間を接続するトランクポートは、**switchport mode trunk** コマンドでポートモードを設定し、**switchport trunk allowed vlan** コマンドでプライマリーVLAN とセカンダリーVLAN を割り当てます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 をプライベート VLAN ホストポートに、ポート 1/0/2 をプライベート VLAN 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)#
```

5.17.4 switchport private-vlan host-association

switchport private-vlan host-association	
目的	独立ポートまたはコミュニティーポートに、プライベート VLAN を関連付けます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**switchport private-vlan host-association** *PRIMARY-VLAN-ID SECONDARY-VLAN-ID* **no switchport private-vlan host-association**
パラメーター	*PRIMARY-VLAN-ID*：関連付けるプライマリーVLAN の VLAN ID を、2～4094 の範囲で指定します。 *SECONDARY-VLAN-ID*：関連付けるセカンダリーVLAN の VLAN ID を、2～4094 の範囲で指定します。

switchport private-vlan host-association	
デフォルト	なし
コマンドモード	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。 コマンドで指定したセカンダリーVLAN が独立 VLAN の場合、ポートは独立ポートになります。コマンドで指定したセカンダリーVLAN がコミュニティーVLAN の場合、ポートはコミュニティーポートになります。また、指定したセカンダリーVLAN とプライマリーVLAN の、タグなしメンバーとしてポートを設定します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 を、プライマリーVLAN 1000 とセカンダリーVLAN 1001 に関連付ける方法を示します。

```
# 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)#
```

5.17.5 switchport private-vlan mapping

switchport private-vlan mapping	
目的	プライベート VLAN メンバーシップを、プロミスキャスポートに関連付けます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**switchport private-vlan mapping** *PRIMARY-VLAN-ID* {**add** *SECONDARY-VLAN-ID* [,|-] | **remove** *SECONDARY-VLAN-ID* [,|-]} **no switchport private-vlan mapping**
パラメーター	*PRIMARY-VLAN-ID*：マッピングするプライマリーVLAN の VLAN ID を、2～4094 の範囲で指定します。 **add** *SECONDARY-VLAN-ID*：VLAN をメンバーシップとして加える場合に、セカンダリーVLAN の VLAN ID を、2～4094 の範囲で指定します。複数指定できます。 **remove** *SECONDARY-VLAN-ID*：セカンダリーVLAN をメンバーシップから外す場合に、セカンダリーVLAN の VLAN ID を指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/2 を、プライベート VLAN プロミスキャスポートとして設定する方法を示します。また、プライベート VLAN プロミスキャスポートとして設定したインターフェースを、以下の VLAN にマッピングする方法を示します。

- プライマリーVLAN 1000
- セカンダリーVLAN 1001
- セカンダリーVLAN 1002

```
# 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)#
```

5.17.6 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。
シンタックス	**show vlan private-vlan**
パラメーター	なし
デフォルト	なし
コマンドモード	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	プライベート VLAN ドメインに含まれるプライベート VLAN の一覧、セカンダリー VLAN のプライマリーVLAN への関連付け、および各プライベート VLAN のメンバーポートを表示するコマンドです。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
-----------------------------------------------------
300             200              Isolated     1/0/9-1/0/16,1/0/24
300             100              Community    1/0/1-1/0/8,1/0/24

Total Entries: 2
```

項番	説明
(1)	プライマリーVLAN ID を表示します。
(2)	セカンダリー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。

5.17.7 private-vlan synchronize

private-vlan synchronize	
目的	プライマリーVLAN と同じマッピング MSTP ID を持つように、セカンダリーVLAN を同期させます。
シンタックス	private-vlan synchronize
パラメーター	なし
デフォルト	なし
コマンドモード	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 を設定している場合、セカンダリーVLAN はプライマリーVLAN と同じ MSTP ID へマッピングされる必要があります。private-vlan synchronize は、MSTP コンフィグレーションモードから遷移する前に MSTP ID マッピングを同期するコマンドです。running configuration には保存されません。
制限事項	-
注意事項	マッピングが同期されていない場合には、show spanning-tree mst configuration コマンドで警告メッセージが表示されます。
対象バージョン	1.01.01

使用例：MSTP コンフィグレーションモードから遷移する前に、MSTP マッピングを同期する方法を示します。

```
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)# instance 1 vlans 1-100
(config-mst)# instance 2 vlans 101-200
(config-mst)# private-vlan synchronize
(config-mst)#
```

5.18 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。

コマンド	コマンドとパラメーター
dot1q inner ethertype	dot1q inner ethertype VALUE no dot1q inner ethertype
dot1q tunneling ethertype	dot1q tunneling ethertype VALUE no dot1q tunneling ethertype
switchport vlan mapping	switchport vlan mapping original-vlan ORIGINAL-VLAN [ORIGINAL-INNER-VLAN] resultant-vlan RESULTANT-VLAN [RESULTANT-INNER-VLAN] [priority COS-VALUE] switchport vlan mapping original-vlan ORIGINAL-VLAN [,|-] dot1q-tunnel DOT1Q-TUNNEL-VLAN [priority COS-VALUE] no switchport vlan mapping original-vlan ORIGINAL-VLAN [,|-] [ORIGINAL-INNER-VLAN]
vlan mapping profile	vlan mapping profile PROFILE-ID [type PROFILE-TYPE] no vlan mapping profile PROFILE-ID
vlan mapping rule	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-VALUE] no rule SEQ [,|-]
switchport vlan mapping profile	switchport vlan mapping profile PROFILE-ID no switchport vlan mapping profile PROFILE-ID
vlan mapping miss drop	vlan mapping miss drop no vlan mapping miss drop
dot1q-tunnel trust inner-priority	dot1q-tunnel trust inner-priority no dot1q-tunnel trust inner-priority
dot1q-tunnel insert dot1q-tag	dot1q-tunnel insert dot1q-tag DOT1Q-VLAN no 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。

コマンド	コマンドとパラメーター
show dot1q ethertype	show dot1q ethertype [interface INTERFACE-ID [,|-]]
show vlan mapping	show vlan mapping [interface INTERFACE-ID [,|-]]
show dot1q-tunnel	show dot1q-tunnel [interface INTERFACE-ID [,|-]]
show vlan mapping profile	show vlan mapping profile [PROFILE-ID]

5.18.1 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。

dot1q inner ethertype	
シンタックス	**dot1q inner ethertype** *VALUE* **no dot1q inner ethertype**
パラメーター	*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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.18.2 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。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	**dot1q tunneling ethertype** *VALUE* **no dot1q tunneling ethertype**
パラメーター	*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
コマンドモード	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。 トランクモードのインターフェースで設定できます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.18.3 switchport vlan mapping

switchport vlan mapping	
目的	主にトランクポートで使用する VLAN 変換エントリーを指定します。または、トンネルポートのためのサービス VLAN マッピングエントリーを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**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*] **no switchport vlan mapping original-vlan** *ORIGINAL-VLAN* [,|-] [*ORIGINAL-INNER-VLAN*]
パラメーター	*ORIGINAL-VLAN*：VLAN 変換エントリーまたはサービス VLAN マッピングエントリーと照合される受信フレームの VLAN ID を、1～4094 の範囲で指定します。複数指定できます。 *ORIGINAL-INNER-VLAN*（省略可能）：トランクポートにおいて、VLAN 変換エントリーと照合される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*：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。VLAN 変換エントリーにマッチしたフレームは双方向で変換されます。 *RESULTANT-INNER-VLAN*（省略可能）：トランクポートにおいて、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。 **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設定する優先度を指定します。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
コマンドモード	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* 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。 トランクポートにおいて **switchport vlan mapping original-vlan** *ORIGINAL-VLAN ORIGINAL-INNER-VLAN* **resultant-vlan** *RESULTANT-VLAN RESULTANT-INNER-*

switchport vlan mapping	
	VLAN コマンドを設定した場合には、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、**switchport vlan mapping original-vlan** *ORIGINAL-VLAN* **resultant-vlan** *RESULTANT-VLAN* コマンドを使用します。*ORIGINAL-INNER-VLAN* と *RESULTANT-INNER-VLAN* 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。 **<サービス VLAN マッピングエントリー>** **dot1q-tunnel** *DOT1Q-TUNNEL-VLAN* 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。 トンネルポートにおいて、受信したカスタマーVLAN タグ付きフレームと一致するサービス VLAN マッピングエントリーが存在せず、受信ポートで **vlan mapping miss drop** コマンドが有効な場合には、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には、**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。
制限事項	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 タグ変換機能と RPVST+を同一ポートで併用できません。
注意事項	*RESULTANT-INNER-VLAN* を指定しない形式（**switchport vlan mapping original-vlan** *ORIGINAL-VLAN ORIGINAL-INNER-VLAN* **resultant-vlan** *RESULTANT-VLAN*）で設定した場合は、*RESULTANT-INNER-VLAN* を *ORIGINAL-INNER-VLAN* の値で設定した場合と同じ動作になります。（例：″switchport vlan mapping original-vlan 10 1234 resultant-vlan 50″ と設定した場合は、″switchport vlan mapping original-vlan 10 1234 resultant-vlan 50 1234″ と設定した場合と同じ動作）
対象バージョン	1.01.01

使用例：トランクモードに設定したポート 1/0/1 で、VLAN 変換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 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、サービス VLAN マッピングエントリーを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)#
```

5.18.4 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。
シンタックス	**vlan mapping profile** *PROFILE-ID* [**type** *PROFILE-TYPE*] **no vlan mapping profile** *PROFILE-ID*
パラメーター	*PROFILE-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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN マッピングプロファイル 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)#
```

5.18.5 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。
シンタックス	**rule** [*SEQ*] **match** *CONDITION* **dot1q-tunnel outer-vid** *VLAN-ID* [**priority**

vlan mapping rule	
	COS-VALUE] [inner-vid *VLAN-ID*] rule [*SEQ*] match *CONDITION* translate outer-vid *VLAN-ID* [priority *COS-VALUE*] no rule *SEQ* [,|-]
パラメーター	*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
コマンドモード	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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式） 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

■ 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

タイプ	使用できる抽出条件
	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
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/SUBNET-MASK*：送信元 IPv4 アドレスを指定
宛先 IP アドレス	**dst-ip** *DST-IP-ADDR/SUBNET-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** *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/PREFIX-LENGTH*：送信元 IPv6 アドレスを指定
宛先 IPv6 アドレス	**dst-ipv6** *DST-IPV6-ADDR/PREFIX-LENGTH*：宛先 IPv6 アドレスを指定

使用例：プロファイルタイプが ip の VLAN マッピングプロファイル 1 を作成し、VLAN マッピングルールを設定する方法を示します。

```
# 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)#
```

5.18.6 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。
シンタックス	**switchport vlan mapping profile** *PROFILE-ID* **no switchport vlan mapping profile** *PROFILE-ID*
パラメーター	*PROFILE-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
コマンドモード	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。

switchport vlan mapping profile	
	トンネルモードのインターフェースで設定できます。 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。 VLAN マッピングプロファイルを適用したポートの動作モードをトンネルモード以外に変更すると、本設定は削除されます。
制限事項	ApresiaNP2000 シリーズでは、適用できるプロファイルタイプ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］のプロファイルを適用することはできません。 　• ［ethernet タイプ］［ip タイプ］［ipv6 タイプ］が適用済み 　• ［ethernet タイプ］［ipv6 タイプ］が適用済み 　• ［ip タイプ］［ipv6 タイプ］が適用済み • 以下の状況では、新たに［ipv6 タイプ］のプロファイルを適用することはできません。 　• ［ethernet タイプ］［ip タイプ］［ethernet ip タイプ］が適用済み 　• ［ethernet タイプ］［ethernet ip タイプ］が適用済み 　• ［ip タイプ］［ethernet ip タイプ］が適用済み • 以下の状況では、新たに［ethernet タイプ］のプロファイル、または［ip タイプ］のプロファイルを適用することはできません。 　• ［ipv6 タイプ］［ethernet ip タイプ］が適用済み
注意事項	-
対象バージョン	1.01.01

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 1 を適用する方法を示します。

```
# 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)# exit
(config)# interface port 1/0/1
(config-if-port)# switchport mode dot1q-tunnel
(config-if-port)# switchport vlan mapping profile 1
(config-if-port)#
```

5.18.7 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。
シンタックス	**vlan mapping miss drop** **no vlan mapping miss drop**
パラメーター	なし

vlan mapping miss drop	
デフォルト	無効
コマンドモード	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。 トンネルモードのインターフェースで設定できます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.18.8 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。
シンタックス	dot1q-tunnel trust inner-priority no dot1q-tunnel trust inner-priority
パラメーター	なし
デフォルト	無効
コマンドモード	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。 トンネルモードのインターフェースで設定できます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.18.9 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。
シンタックス	**dot1q-tunnel insert dot1q-tag** *DOT1Q-VLAN* **no dot1q-tunnel insert dot1q-tag**
パラメーター	*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
コマンドモード	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。 トンネルモードのインターフェースで設定できます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

5.18.10 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。
シンタックス	show dot1q ethertype [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID*（省略可能）：TPID 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：物理ポートを指定します。複数指定できます。 • port-channel：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

5.18.11 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。
シンタックス	show vlan mapping [interface *INTERFACE-ID* [,|-]]
パラメーター	interface *INTERFACE-ID*（省略可能）：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：物理ポートを指定します。複数指定できます。 • port-channel：ポートチャネルを指定します。

show vlan mapping	
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

5.18.12 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。
シンタックス	**show dot1q-tunnel [interface** *INTERFACE-ID* **[,|-]]**
パラメーター	**interface** *INTERFACE-ID*（省略可能）：トンネルポート関連の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。

show dot1q-tunnel	
	• port：物理ポートを指定します。複数指定できます。 • port-channel：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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、すべてのトンネルポートの情報が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 タグの優先度の反映オプションの有効／無効を表示します。
(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／無効を表示します。
(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。

5.18.13 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。
シンタックス	**show vlan mapping profile** [*PROFILE-ID*]
パラメーター	*PROFILE-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。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

5.19 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。

コマンド	コマンドとパラメーター
voice vlan	voice vlan VLAN-ID no voice vlan
voice vlan qos	voice vlan qos COS-VALUE no voice vlan qos
voice vlan dscp	voice vlan dscp VALUE no voice vlan dscp
voice vlan aging	voice vlan aging MINUTES no voice vlan aging
voice vlan mac-address	voice vlan mac-address MAC-ADDRESS MASK [description STRING] no voice vlan mac-address MAC-ADDRESS MASK
voice vlan mode	voice vlan mode {auto untag | auto tag | manual} no voice vlan mode
voice vlan enable	voice vlan enable no voice vlan enable

Voice VLAN 関連の show コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show voice vlan	show voice vlan [interface [INTERFACE-ID [,|-]]]
show voice vlan device	show voice vlan device [interface INTERFACE-ID [,|-]]
show voice vlan lldp-med device	show voice vlan lldp-med device [interface INTERFACE-ID [,|-]]

5.19.1 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。
シンタックス	**voice vlan** *VLAN-ID* **no voice vlan**
パラメーター	*VLAN-ID*：Voice VLAN として使用する VLAN ID を、2～4094 の範囲で指定します。
デフォルト	無効
コマンドモード	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	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	
	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。
制限事項	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。 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。
注意事項	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。
対象バージョン	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)#
```

5.19.2 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。
シンタックス	**voice vlan qos** *COS-VALUE* **no voice vlan qos**
パラメーター	*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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	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)#
```

5.19.3 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。
シンタックス	**voice vlan dscp** *VALUE* **no voice vlan dscp**
パラメーター	*VALUE*：DSCP を 0～63 の範囲で指定します。
デフォルト	なし
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	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)#
```

5.19.4 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。
シンタックス	**voice vlan aging** *MINUTES* **no voice vlan aging**
パラメーター	*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
コマンドモード	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	Voice VLAN 端末からの音声パケットが停止し、その Voice VLAN 端末の MAC アドレスが FDB からエージアウトされると、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。

voice vlan aging	
制限事項	-
注意事項	-
対象バージョン	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)#
```

5.19.5 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は、no 形式のコマンドを使用します。
シンタックス	**voice vlan mac-address** *MAC-ADDRESS MASK* [**description** *STRING*] **no voice vlan mac-address** *MAC-ADDRESS MASK*
パラメーター	*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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式） **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	以下に示す 8 つのベンダーの OUI（MAC アドレスの上位 24 ビット）が登録されています。 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
コマンドモード	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	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。
制限事項	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。
注意事項	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。
対象バージョン	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)#
```

5.19.6 voice vlan mode

voice vlan mode	
目的	Voice VLAN の動作モードを指定します。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。
シンタックス	**voice vlan mode {auto untag | auto tag | manual}** **no voice vlan mode**
パラメーター	**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)
コマンドモード	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、またはプライオリティタグ形式(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。
制限事項	-
注意事項	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。
対象バージョン	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)#
```

5.19.7 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。
シンタックス	**voice vlan enable** **no voice vlan enable**
パラメーター	-
デフォルト	無効
コマンドモード	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。 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。
制限事項	-
注意事項	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。
対象バージョン	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)#
```

5.19.8 show voice vlan

show voice vlan	
目的	Voice VLAN の設定を表示します。
シンタックス	**show voice vlan** [**interface** [*INTERFACE-ID* [,|-]]]
パラメーター	**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。 *INTERFACE-ID*（省略可能）：Voice VLAN 関連の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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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

show voice vlan	
	は、すべてのインターフェースの Voice VLAN 関連の設定情報が表示されます。
制限事項	-
注意事項	-
対象バージョン	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         : 1/0/1-1/0/2,1/0/5-1/0/6,1/0/49 ...(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設定を表示します。
(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／無効を表示します。
(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

5.19.9 show voice vlan device

show voice vlan device	
目的	Voice VLAN 端末を表示します。
シンタックス	**show voice vlan device** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：Voice VLAN 端末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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	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 FDB に登録されている状態 Aging：Voice VLAN 端末の MAC アドレスが FDB からエージアウトされ、Voice VLAN 端末のエージングタイマーが開始している状態

5.19.10 show voice vlan lldp-med device

show voice vlan lldp-med device	
目的	LLDP-MED 端末を表示します。
シンタックス	**show voice vlan lldp-med device** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：LLDP-MED 端末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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	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)	LLDP-MED 端末が登録された日時を表示します。
(8)	LLDP-MED 端末がエージアウトされるまでの残り時間を表示します。

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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ip forwarding	ip forwarding no ip forwarding
ipv6 forwarding	ipv6 forwarding no ipv6 forwarding
ip route	ip route {DST-NETWORK-PREFIX PREFIX-MASK | NETWORK-ADDRESS/MASK-LENGTH} IP-ADDRESS [primary | backup] no ip route {DST-NETWORK-PREFIX PREFIX-MASK | NETWORK-ADDRESS/MASK-LENGTH} IP-ADDRESS
ipv6 route	ipv6 route {default | NETWORK-PREFIX/PREFIX-LENGTH} [INTERFACE-NAME] NEXT-HOP-ADDRESS [primary | backup] no ipv6 route {default | NETWORK-PREFIX/PREFIX-LENGTH} [INTERFACE-NAME] NEXT-HOP-ADDRESS
show ip forwarding	show ip forwarding
show ipv6 forwarding	show ipv6 forwarding
show ip route	show ip route [IP-ADDRESS [MASK] | PROTOCOL | hardware]
show ip route summary	show ip route summary
show ipv6 route	show ipv6 route [[IPV6-ADDRESS | NETWORK-PREFIX/PREFIX-LENGTH [longer-prefixes] | interface INTERFACE-NAME | PROTOCOL] [database] | hardware]
show ipv6 route summary	show ipv6 route summary

6.1.1 ip forwarding

ip forwarding	
目的	IPv4 Forwarding 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。
シンタックス	**ip forwarding** **no ip forwarding**
パラメーター	なし
デフォルト	有効（**ip forwarding**）
コマンドモード	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	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。 AEOS-NP2000 Ver. 1.09.05 で IPv4 Forwarding 機能を無効にしたスタック構成を使用する場合は、注意事項の動作を回避するために以下の手順を推奨します。 • IPv4 Forwarding 機能を無効にしたスタック構成に新たにスタックメンバーを追加する場合は、新たに追加する装置でスタックの設定を実施して設定保存した後、「電源 OFF の状態でスタック構成に接続してから起

ip forwarding	
	動する手順」で追加する。 • IPv4 Forwarding 機能を無効にしたスタック構成で故障などによりスタックメンバーを交換する場合は、代替装置でスタックの設定を実施して設定保存した後、「電源 OFF の状態でスタック構成に接続してから起動する手順」で追加する。
制限事項	-
注意事項	AEOS-NP2000 Ver. 1.09.05 の場合、IPv4 Forwarding 機能を無効にしたスタック構成に、デフォルトの IPv4 Forwarding 有効設定の装置を起動した状態でスタック構成に接続して取り込むと、その追加した装置では IPv4 Forwarding 機能が有効設定の動作になってしまうことに注意してください。この場合は、設定を保存してから追加した装置を再起動してください。なお、AEOS-NP2000 Ver. 1.09.06 以降では、この注意事項の動作は仕様改善されています。
対象バージョン	1.09.05

使用例：IPv4 Forwarding 機能を有効にする方法を示します。

```
# configure terminal
(config)# ip forwarding

 WARNING: The command does not take effect until the next reboot.
(config)#
```

6.1.2 ipv6 forwarding

ipv6 forwarding	
目的	IPv6 Forwarding 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。
シンタックス	**ipv6 forwarding** **no ipv6 forwarding**
パラメーター	なし
デフォルト	有効（**ipv6 forwarding**）
コマンドモード	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	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。 AEOS-NP2000 Ver. 1.09.05 で IPv6 Forwarding 機能を無効にしたスタック構成を使用する場合は、注意事項の動作を回避するために以下の手順を推奨します。 • IPv6 Forwarding 機能を無効にしたスタック構成に新たにスタックメンバーを追加する場合は、新たに追加する装置でスタックの設定を実施して設定保存した後、「電源 OFF の状態でスタック構成に接続してから起動する手順」で追加する。 • IPv6 Forwarding 機能を無効にしたスタック構成で故障などによりスタックメンバーを交換する場合は、代替装置でスタックの設定を実施して設定保存した後、「電源 OFF の状態でスタック構成に接続してから起動する手順」で追加する。
制限事項	-
注意事項	AEOS-NP2000 Ver. 1.09.05 の場合、IPv6 Forwarding 機能を無効にしたスタック構成に、デフォルトの IPv6 Forwarding 有効設定の装置を起動した状態でスタック構成に接続して取り込むと、その追加した装置では IPv6 Forwarding 機能が有効設定の動作になってしまうことに注意してください。この場合は、設定を保存

ipv6 forwarding	
	してから追加した装置を再起動してください。なお、AEOS-NP2000 Ver. 1.09.06 以降では、この注意事項の動作は仕様改善されています。
対象バージョン	1.09.05

使用例：IPv6 Forwarding 機能を有効にする方法を示します。

```
# configure terminal
(config)# ipv6 forwarding

 WARNING: The command does not take effect until the next reboot.
(config)#
```

6.1.3 ip route

ip route	
目的	IPv4 スタティックルートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**ip route** {*DST-NETWORK-PREFIX PREFIX-MASK* ｜ *NETWORK-ADDRESS/MASK-LENGTH*} *IP-ADDRESS* [**primary** ｜ **backup**] **no ip route** {*DST-NETWORK-PREFIX PREFIX-MASK* ｜ *NETWORK-ADDRESS/MASK-LENGTH*} *IP-ADDRESS*
パラメーター	*DST-NETWORK-PREFIX PREFIX-MASK*：宛先ネットワークの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-ADDRESS/MASK-LENGTH*：宛先ネットワークの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。デフォルトルートを指定する場合は 0.0.0.0/0 を指定します。（例：192.0.2.0/24） *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
コマンドモード	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	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。
制限事項	スタティックルートのリソースは IPv4 スタティックルートと IPv6 スタティックルートで共用されていて、最大 256 個分のリソースの範囲内で設定可能です。IPv4 スタティックルートを 1 つ設定すると 1 個分のリソースを消費します。そのため、IPv4 スタティックルートだけを設定した場合は最大 256 エントリーとなります。IPv6 スタティックルートを 1 つ設定すると 2 個分のリソースを消費します。そのため、IPv6 スタティックルートだけを設定した場合は最大 128 エ

ip route	
	ントリーとなります。
注意事項	宛先ネットワークを「ネットワークアドレスとサブネットマスク」形式で指定しても、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」形式で表示されます。
対象バージョン	1.01.01

使用例：「宛先ネットワーク：192.0.2.0/24、ネクストホップ：10.1.1.254」の IPv4 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 192.0.2.0/24 10.1.1.254
(config)#
```

6.1.4 ipv6 route

ipv6 route	
目的	IPv6 スタティックルートを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**ipv6 route** {**default** ｜ *NETWORK-PREFIX/PREFIX-LENGTH*} [*INTERFACE-NAME*] *NEXT-HOP-ADDRESS* [**primary** ｜ **backup**] **no ipv6 route** {**default** ｜ *NETWORK-PREFIX/PREFIX-LENGTH*} [*INTERFACE-NAME*] *NEXT-HOP-ADDRESS*
パラメーター	**default**：デフォルトルートを設定する場合に指定します。 *NETWORK-PREFIX/PREFIX-LENGTH*：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。指定できるプレフィックス長は最大 64 です。 *INTERFACE-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。 *NEXT-HOP-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
コマンドモード	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	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。
制限事項	スタティックルートのリソースは IPv4 スタティックルートと IPv6 スタティックルートで共用されていて、最大 256 個分のリソースの範囲内で設定可能です。

ipv6 route	
	IPv4 スタティックルートを 1 つ設定すると 1 個分のリソースを消費します。そのため、IPv4 スタティックルートだけを設定した場合は最大 256 エントリーとなります。IPv6 スタティックルートを 1 つ設定すると 2 個分のリソースを消費します。そのため、IPv6 スタティックルートだけを設定した場合は最大 128 エントリーとなります。
注意事項	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。
対象バージョン	1.01.01

使用例：「宛先ネットワーク：2001:db8:1:2::/64、ネクストホップ：vlan1 fe80::0000:00ff:1111:2233」の IPv6 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 2001:db8:1:2::/64 vlan1 fe80::0000:00ff:1111:2233
(config)#
```

6.1.5 show ip forwarding

show ip forwarding	
目的	IPv4 Forwarding 機能の有効／無効を表示します。
シンタックス	**show ip forwarding**
パラメーター	なし
デフォルト	なし
コマンドモード	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	–
制限事項	**ip forwarding** コマンドで設定を変更した後、装置を再起動して実際の動作に反映する前の状態でも、本コマンドでは変更後の設定で表示されます。
注意事項	–
対象バージョン	1.09.05

使用例：IPv4 Forwarding 機能の有効／無効を表示する方法を示します。

```
# show ip forwarding

IP forwarding is on ...(1)
```

項番	説明
(1)	IPv4 Forwarding 機能の有効／無効を表示します。 IP forwarding is on：有効 IP forwarding is off：無効

6.1.6 show ipv6 forwarding

show ipv6 forwarding	
目的	IPv6 Forwarding 機能の有効／無効を表示します。
シンタックス	**show ipv6 forwarding**
パラメーター	なし
デフォルト	なし

show ipv6 forwarding	
コマンドモード	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	-
制限事項	**ipv6 forwarding** コマンドで設定を変更した後、装置を再起動して実際の動作に反映する前の状態でも、本コマンドでは変更後の設定で表示されます。
注意事項	-
対象バージョン	1.09.05

使用例：IPv6 Forwarding 機能の有効／無効を表示する方法を示します。

```
# show ipv6 forwarding

IPV6 forwarding is on ...(1)
```

項番	説明
(1)	IPv6 Forwarding 機能の有効／無効を表示します。 IPV6 forwarding is on：有効 IPV6 forwarding is off：無効

6.1.7 show ip route

show ip route	
目的	ルーティングテーブルを表示します。
シンタックス	**show ip route** [*IP-ADDRESS* [*MASK*] | *PROTOCOL* | **hardware**]
パラメーター	*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。 **hardware**（省略可能）：スイッチ LSI に登録されたルート情報を表示する場合に指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：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 10.1.1.2 to network 0.0.0.0 ...(1)
(2)  (3)        (4)    (5)            (6)
S*   0.0.0.0/0 [1/1] via 10.1.1.2, vlan20
S    192.168.100.0/24 [60/1] via 192.168.10.2, vlan10
S    192.168.200.0/24 [60/1] via 192.168.10.2, vlan10
C    10.1.1.0/24 is directly connected, vlan20
C    192.168.10.0/24 is directly connected, vlan10

Total Entries: 5
```

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。

6.1.8 show ip route summary

show ip route summary	
目的	ルーティングテーブルの概要情報を表示します。
シンタックス	show ip route summary
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：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           3
Total            5
```

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。

6.1.9 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。
シンタックス	**show ipv6 route** [[*IPV6-ADDRESS* | *NETWORK-PREFIX/PREFIX-LENGTH* [**longer-prefixes**] | **interface** *INTERFACE-NAME* | *PROTOCOL*] [**database**] | **hardware**]
パラメーター	*IPV6-ADDRESS*（省略可能）：ルート情報を表示する IPv6 アドレスを指定します。指定した IPv6 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。 *NETWORK-PREFIX/PREFIX-LENGTH*（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プレフィックス長を指定します。 **longer-prefixes**（省略可能）：*PREFIX-LENGTH* で指定したプレフィックス長よりも長いプレフィックス長のルート情報を表示する場合に指定します。 **interface** *INTERFACE-NAME*（省略可能）：表示するルート情報の送信インターフェース ID（**vlan** と VLAN ID の間を空けない形式）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。 **database**（省略可能）：ルーティングデータベース内のすべての関連エントリーを表示する場合に指定します。 **hardware**（省略可能）：スイッチ LSI に登録されたルート情報を表示する場合に指定します。
デフォルト	なし
コマンドモード	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	–
制限事項	–
注意事項	–
対象バージョン	1.01.01

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::2, vlan20
C     2001:db8::/64 [0/1] is directly connected, vlan20
C     2001:db8:300::/64 [0/1] is directly connected, vlan10
S     2001:db8:300:aaaa::/64 [1/1] via 2001:db8:300::2, vlan10
S     2001:db8:300:bbbb::/64 [1/1] via 2001:db8:300::2, vlan10

Total Entries: 5 entries, 5 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。

6.1.10 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。
シンタックス	**show ipv6 route summary**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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          2
Static             3
SLAAC              0
Total              5
```

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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show ip mroute forwarding-cache	show ip mroute forwarding-cache [group-addr GROUP-ADDRESS [source-addr SOURCE-ADDRESS]]

6.2.1 show ip mroute forwarding-cache

show ip mroute forwarding-cache	
目的	IP マルチキャスト転送キャッシュデータベースの内容を表示します。
シンタックス	**show ip mroute forwarding-cache** [**group-addr** *GROUP-ADDRESS* [**source-addr** *SOURCE-ADDRESS*]]
パラメーター	**group-addr** *GROUP-ADDRESS*（省略可能）：マルチキャスト転送キャッシュデータベースの内容を表示するマルチキャストグループのアドレスを指定します。 **source-addr** *SOURCE-ADDRESS*（省略可能）：マルチキャスト転送キャッシュデータベースの内容を表示するマルチキャスト送信元 IP アドレスを指定します。
デフォルト	なし
コマンドモード	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 マルチキャスト転送キャッシュデータベースとは、IGMP スヌーピンググループメンバーテーブル、およびマルチキャストルーターポートを要約したテーブルです。
制限事項	–
注意事項	マルチキャストをハードウェア転送するためのフォワーディングキャッシュの最大数は 1,024 です。 なお、フォワーディングキャッシュは IPv6 マルチキャストと共有します。デュアルスタックでご使用の場合は、**show ipv6 mroute forwarding-cache** コマンドも合わせてご確認ください。
対象バージョン	1.01.01

使用例：IP マルチキャスト転送キャッシュデータベース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)

(*, 232.1.1.2) VLAN0010
  Outgoing interface list:

(*, 232.1.1.3) VLAN0010
  Outgoing interface list: 1/0/2, port-channel5

Total Entries: 3
```

項番	説明
(1)	マルチキャストエントリーを表示します。
(2)	送信先のインターフェース ID 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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show ipv6 mroute forwarding-cache	show ipv6 mroute forwarding-cache [group-addr GROUP-ADDRESS [source-addr SOURCE-ADDRESS]]

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データベースの内容を表示します。
シンタックス	**show ipv6 mroute forwarding-cache** [**group-addr** *GROUP-ADDRESS* [**source-addr** *SOURCE-ADDRESS*]]
パラメーター	**group-addr** *GROUP-ADDRESS*（省略可能）：マルチキャスト転送キャッシュデータベースの内容を表示するマルチキャストグループの IPv6 アドレスを指定します。 **source-addr** *SOURCE-ADDRESS*（省略可能）：マルチキャスト転送キャッシュデータベースの内容を表示するマルチキャスト送信元 IPv6 アドレスを指定します。
デフォルト	なし
コマンドモード	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データベースとは、MLD スヌーピンググループメンバーテーブル、およびマルチキャストルーターポートを要約したテーブルです。
制限事項	-
注意事項	IPv6 マルチキャストをハードウェア転送するためのフォワーディングキャッシュの最大数は 1,024 です。 なお、フォワーディングキャッシュは IPv4 マルチキャストと共有します。デュアルスタックでご使用の場合は、**show ip mroute forwarding-cache** コマンドも合わせてご確認ください。
対象バージョン	1.01.01

使用例：IPv6 マルチキャスト転送キャッシュデータベース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::1:1:1:2) VLAN0010
  Outgoing interface list:

(*, ff0e::1:1:1:3) VLAN0010
  Outgoing interface list: 1/0/2, port-channel5

Total Entries: 3
```

項番	説明
(1)	マルチキャストエントリーを表示します。
(2)	送信先のインターフェース ID を表示します。

7 優先制御(QoS)

7.1 優先制御(QoS)コマンド

優先制御(QoS)関連の設定コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
priority-queue cos-map	priority-queue cos-map QUEUE-ID COS-LIST no priority-queue cos-map
mls qos scheduler	mls qos scheduler {sp | rr | wrr | wdrr} no mls qos scheduler
wrr-queue bandwidth	wrr-queue bandwidth WEIGHT0...WEIGHT7 no wrr-queue bandwidth
wdrr-queue bandwidth	wdrr-queue bandwidth QUANTUM0...QUANTUM7 no wdrr-queue bandwidth
mls qos trust	mls qos trust {cos | dscp} no mls qos trust
mls qos cos	mls qos cos {COS-VALUE | override} no mls qos cos
mls qos map dscp-cos	mls qos map dscp-cos DSCP-LIST to COS-VALUE no mls qos map dscp-cos DSCP-LIST
mls qos map cos-color	mls qos map cos-color COS-LIST to {green | yellow | red} no mls qos map cos-color
mls qos map dscp-color	mls qos map dscp-color DSCP-LIST to {green | yellow | red} no mls qos map dscp-color DSCP-LIST
mls qos dscp-mutation	mls qos dscp-mutation DSCP-MAP-NAME no mls qos dscp-mutation
mls qos map dscp-mutation	mls qos map dscp-mutation DSCP-MAP-NAME DSCP-LIST to OUTPUT-DSCP no mls qos map dscp-mutation DSCP-MAP-NAME
queue rate-limit	queue QUEUE-ID rate-limit {MIN-BANDWIDTH-KBPS | percent MIN-PERCENTAGE} {MAX-BANDWIDTH-KBPS | percent MAX-PERCENTAGE} no queue QUEUE-ID rate-limit
rate-limit input	rate-limit input {KBPS | percent PERCENTAGE} [BURST-SIZE] no rate-limit input
rate-limit output	rate-limit output {KBPS | percent PERCENTAGE} [BURST-SIZE] no rate-limit output
class-map	class-map [match-all | match-any] CLASS-MAP-NAME no class-map CLASS-MAP-NAME

コマンド	コマンドとパラメーター
match	match {access-group name ACCESS-LIST-NAME | cos [inner] COS-LIST | [ip] dscp DSCP-LIST | [ip] precedence IP-PRECEDENCE-LIST | protocol PROTOCOL-NAME | vlan [inner] VLAN-LIST} no match {access-group name ACCESS-LIST-NAME | cos [inner] COS-LIST | [ip] dscp DSCP-LIST | [ip] precedence IP-PRECEDENCE-LIST | protocol PROTOCOL-NAME | vlan [inner] VLAN-ID-LIST}
policy-map	policy-map POLICY-MAP-NAME no policy-map POLICY-MAP-NAME
class (QoS)	class CLASS-MAP-NAME no class CLASS-MAP-NAME
set	set {[ip] precedence PRECEDENCE | [ip] dscp DSCP | cos COS | cos-queue COS-QUEUE} no set {[ip] precedence PRECEDENCE | [ip] dscp DSCP | cos COS | cos-queue COS-QUEUE}
police	police KBPS [BURST-NORMAL [BURST-MAX]] [conform-action ACTION] exceed-action ACTION [violate-action ACTION] [color-aware] no police
police cir	police cir CIR [bc CONFORM-BURST] pir PIR [be PEAK-BURST] [conform-action ACTION] [exceed-action ACTION [violate-action ACTION]] [color-aware] no police
police aggregate	police aggregate AG-POLICER-NAME no police
mls qos aggregate-policer	mls qos aggregate-policer AG-POLICER-NAME KBPS [BURST-NORMAL [BURST-MAX]] [conform-action ACTION] exceed-action ACTION [violate-action ACTION] [color-aware] mls qos aggregate-policer AG-POLICER-NAME cir CIR [bc CONFORM-BURST] pir PIR [be PEAK-BURST] [conform-action ACTION] [exceed-action ACTION [violate-action ACTION]] [color-aware] no mls qos aggregate-policer AG-POLICER-NAME
service-policy	service-policy {input | output} POLICY-MAP-NAME no service-policy {input | output}
cpu rate-limit	cpu rate-limit {cos0 RATE0 | cos1 RATE1 | cos2 RATE2 | cos3 RATE3} no cpu rate-limit {cos0 | cos1 | cos2 | cos3}

優先制御(QoS)関連の show コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show mls qos queueing	show mls qos queueing [interface INTERFACE-ID [,|-]]
show mls qos interface scheduler	show mls qos interface [INTERFACE-ID [,|-]] scheduler

コマンド	コマンドとパラメーター
show mls qos interface trust	show mls qos interface [INTERFACE-ID [,|-]] trust
show mls qos interface cos	show mls qos interface [INTERFACE-ID [,|-]] cos
show mls qos interface map dscp-cos	show mls qos interface [INTERFACE-ID [,|-]] map dscp-cos
show mls qos interface map cos-color	show mls qos interface [INTERFACE-ID [,|-]] map cos-color
show mls qos interface map dscp-color	show mls qos interface [INTERFACE-ID [,|-]] map dscp-color
show mls qos map dscp-mutation	show mls qos map dscp-mutation [DSCP-MAP-NAME]
show mls qos interface dscp-mutation	show mls qos interface [INTERFACE-ID [,|-]] dscp-mutation
show mls qos interface queue-rate-limit	show mls qos interface [INTERFACE-ID [,|-]] queue-rate-limit
show mls qos interface rate-limit	show mls qos interface [INTERFACE-ID [,|-]] rate-limit
show class-map	show class-map [CLASS-MAP-NAME]
show policy-map	show policy-map [POLICY-MAP-NAME | interface INTERFACE-ID]
show mls qos aggregate-policer	show mls qos aggregate-policer [AG-POLICER-NAME]

7.1.1 priority-queue cos-map

priority-queue cos-map	
目的	Class of Service (CoS) 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。
シンタックス	**priority-queue cos-map** *QUEUE-ID COS-LIST* **no priority-queue cos-map**
パラメーター	*QUEUE-ID*：送信キューを 0～7 の範囲で指定します。 *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、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 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
コマンドモード	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	-

priority-queue cos-map	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：CoS 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。
シンタックス	**mls qos scheduler {sp | rr | wrr | wdrr}** **no mls qos scheduler**
パラメーター	**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 に設定されている送信キューは 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 に設定されている送信キューは Strict Priority Queuing で動作します。
デフォルト	WRR (Weighted Round Robin)
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**wrr-queue bandwidth** *WEIGHT0...WEIGHT7* **no wrr-queue bandwidth**
パラメーター	*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

wrr-queue bandwidth	
	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
コマンドモード	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	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 に設定されている送信キューは Strict Priority Queuing で動作します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**wdrr-queue bandwidth** *QUANTUM0...QUANTUM7* **no wdrr-queue bandwidth**
パラメーター	*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
コマンドモード	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	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 に設定されている送信キューは Strict Priority Queuing で動作します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**mls qos trust {cos ｜ dscp}** **no mls qos trust**
パラメーター	**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）
コマンドモード	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 へのマッピング」で反映された CoS 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 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

mls qos trust	
	のマッピング」が反映されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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	インターフェースのデフォルトの Class of Service (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。
シンタックス	**mls qos cos** {*COS-VALUE* | **override**} **no mls qos cos**
パラメーター	*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
コマンドモード	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	**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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 Class of Service (CoS) 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。
シンタックス	**mls qos map dscp-cos** *DSCP-LIST* **to** *COS-VALUE* **no mls qos map dscp-cos** *DSCP-LIST*
パラメーター	*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 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
コマンドモード	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	DSCP から CoS へのマッピングを使用する場合は、**mls qos trust** コマンドで対象ポートを「受信トラフィックの DSCP を信頼するモード」に設定します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**mls qos map cos-color** *COS-LIST* **to** {**green** | **yellow** | **red**} **no mls qos map cos-color**
パラメーター	*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。 **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。

mls qos map cos-color	
	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**
コマンドモード	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	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** コマンドで対象ポートを「受信トラフィックの CoS を信頼するモード」に設定します。
制限事項	「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。
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**mls qos map dscp-color** *DSCP-LIST* **to** {**green** | **yellow** | **red**} **no mls qos map dscp-color** *DSCP-LIST*
パラメーター	*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**
コマンドモード	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	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** コマンドで対象ポートを「受信トラフィックの DSCP を信頼するモード」に設定します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**mls qos dscp-mutation** *DSCP-MAP-NAME* **no mls qos dscp-mutation**
パラメーター	*DSCP-MAP-NAME*：DSCP 変換マップ名を指定します。
デフォルト	なし
コマンドモード	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	受信時の DSCP 変換マップを使用する場合は、**mls qos trust** コマンドで対象ポートを「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
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**mls qos map dscp-mutation** *DSCP-MAP-NAME DSCP-LIST* **to** *OUTPUT-DSCP* **no mls qos map dscp-mutation** *DSCP-MAP-NAME*
パラメーター	*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

mls qos map dscp-mutation	
	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。 *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
コマンドモード	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	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。
制限事項	定義できる DSCP 変換マップは最大 255 個です。
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**queue** *QUEUE-ID* **rate-limit** {*MIN-BANDWIDTH-KBPS* | **percent** *MIN-PERCENTAGE*} {*MAX-BANDWIDTH-KBPS* | **percent** *MAX-PERCENTAGE*} **no queue** *QUEUE-ID* **rate-limit**
パラメーター	*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-BANDWIDTH-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-BANDWIDTH-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
コマンドモード	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	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制限されます。 *MIN-BANDWIDTH-KBPS* パラメーターと *MAX-BANDWIDTH-KBPS* パラメーターの設定値

queue rate-limit	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**rate-limit input** {*KBPS* | **percent** *PERCENTAGE*} [*BURST-SIZE*] **no rate-limit input**
パラメーター	*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-SIZE*（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
コマンドモード	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	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-SIZE* 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。 受信ポートごと、送信ポートごとの帯域制限では、IFG(Inter Frame Gap)と Preamble/SFD を含めないで帯域計測します。
制限事項	*BURST-SIZE* パラメーターに 0 を指定した場合には帯域制限は動作しません。*BURST-SIZE* パラメーターには 0 を設定しないでください。
注意事項	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 input** コマンドで削除してから、再度設定してください。

rate-limit input	
対象バージョン	1.01.01

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。
シンタックス	**rate-limit output** {*KBPS* ｜ **percent** *PERCENTAGE*} [*BURST-SIZE*] **no rate-limit output**
パラメーター	*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-SIZE*（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
コマンドモード	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	*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-SIZE* 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。 受信ポートごと、送信ポートごとの帯域制限では、IFG(Inter Frame Gap)と Preamble/SFD を含めないで帯域計測します。
制限事項	*BURST-SIZE* パラメーターに 0 を指定した場合には帯域制限は動作しません。*BURST-SIZE* パラメーターには 0 を設定しないでください。
注意事項	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。
対象バージョン	1.01.01

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 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。
シンタックス	**class-map** [**match-all** | **match-any**] *CLASS-MAP-NAME* **no class-map** *CLASS-MAP-NAME*
パラメーター	**match-all** (省略可能):複数の一致条件を評価する方法を指定します。クラスマップ内の複数の match ステートメントを論理 AND に基づいて評価する場合に指定します。 **match-any** (省略可能):複数の一致条件を評価する方法を指定します。クラスマップ内の複数の match ステートメントを論理 OR に基づいて評価する場合に指定します。 *CLASS-MAP-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	class-default (デフォルトクラス) のみ作成済み
コマンドモード	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	実行すると、クラスマップ設定モードに遷移して、クラスの一致条件を定義する **match** コマンドが実行できます。no match ステートメントがクラスに定義された場合、トラフィックはクラスに分類されません。 複数の **match** コマンドがクラスに定義されている場合、複数の一致条件を論理 AND または論理 OR のどちらで評価するかを、**match-all** または **match-any** パラメーターで指定してください。 **match-all** も **match-any** も指定しない場合は、**match-any** が暗黙で指定されます。 class-default は、デフォルトクラスの予約名です。
制限事項	最大クラスマップ数は 255 です。
注意事項	-
対象バージョン	1.01.01

使用例:クラスマップの設定方法を示します。名前を「class_home_user」としています。クラスマップ「class_home_user」に含まれるトラフィックの条件として、アクセスリスト「acl_home_user」と IPv6 プロトコルを、match ステートメントで指定しています。

```
# configure terminal
(config)# class-map match-all class_home_user
(config-cmap)# match access-group name acl_home_user
(config-cmap)# match protocol ipv6
(config-cmap)#
```

7.1.16 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。
シンタックス	**match** {**access-group name** *ACCESS-LIST-NAME* | **cos** [**inner**] *COS-LIST* | [**ip**] **dscp** *DSCP-LIST* | [**ip**] **precedence** *IP-PRECEDENCE-LIST* | **protocol**

match	
	PROTOCOL-NAME | vlan [inner] *VLAN-LIST*} no match {access-group name *ACCESS-LIST-NAME* | cos [inner] *COS-LIST* | [ip] dscp *DSCP-LIST* | [ip] precedence *IP-PRECEDENCE-LIST* | protocol *PROTOCOL-NAME* | vlan [inner] *VLAN-ID-LIST*}
パラメーター	access-group name *ACCESS-LIST-NAME*：一致条件とするアクセスリスト名を指定します。アクセスリストで許可されるトラフィックが分類されます。 cos *COS-LIST*：一致条件とする IEEE 802.1Q 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コンマで区切ります。または、ハイフンを使用して範囲として指定します。 inner（省略可能）：レイヤー2 Class of Service（CoS）のマーキングで QinQ パケットの最も内側の CoS 値を一致条件とする場合に指定します。 ip（省略可能）：IPv4 パケットのみ DSCP を確認する場合に指定します。指定しない場合、IPv4 パケットと IPv6 パケットの両方でマッチングさせます。 dscp *DSCP-LIST*：一致条件とする Differentiated Service Code Point（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ります。または、ハイフンを使用して範囲として指定します。 ip（省略可能）：IPv4 パケットのみ優先度を確認する場合に指定します。指定しない場合、IP パケットと IPv6 パケットの両方でマッチングさせます。IPv6 パケットの場合、優先度は、IPv6 ヘッダーのクラスマップの最上位 3 ビットです。 precedence *IP-PRECEDENCE-LIST*：一致条件とする優先度を、0～7 の範囲で指定します。複数の優先度値を指定する場合はコンマで区切ります。または、ハイフンを使用して範囲として指定します。 protocol *PROTOCOL-NAME*：一致条件とするプロトコル名を指定します。 vlan *VLAN-ID-LIST*：一致条件とする VLAN ID を 1～4094 の範囲で指定します。有効な VLAN ID を指定してください。複数の VLAN ID を指定する場合はコンマで区切ります。または、ハイフンを使用して範囲として指定します。 inner（省略可能）：IEEE 802.1Q 二重タグフレームの最も内側の VLAN ID を一致条件とする場合に指定します。
デフォルト	なし
コマンドモード	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 protocol コマンドでサポートされるプロトコルの参照は、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

match	
	• **ntp** - 時刻プロトコル • **ospf** - Open Shortest Path First • **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** 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]**、または **match vlan [inner]**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**、または **match precedence** 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**、または **match ip precedence** 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** 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。
制限事項	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 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** で拡張エキスパートアクセスリスト、IP アクセスリスト、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)

match	
注意事項	-
対象バージョン	1.01.01

使用例：「class-home-user」というクラスマップを指定して、クラスの一致条件に「acl-home-user」という名前のアクセスリスト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：「cos」というクラスマップを指定して、一致条件に CoS 値 1、2、3 を指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)#
```

使用例：voice と video-n-data というクラスを作成して、CoS 値に基づいてトラフィックを分類する方法を示します。分類後は、cos-based-treatment ポリシーマップ内で適切なパケットが QoS 処理されます（この例では、QoS は、クラス voice には 1 レートポリサー、クラス video-n-data には 2 レートポリサーとしています)。この例ではサービスポリシーの対象をポート 1/0/1 としています。

```
# configure terminal
(config)# class-map voice
(config-cmap)# match cos 7
(config-cmap)# exit
(config)# class-map video-n-data
(config-cmap)# match cos 5
(config-cmap)# exit
(config)# policy-map cos-based-treatment
(config-pmap)# class voice
(config-pmap-c)# police 8000 1000 exceed-action drop
(config-pmap-c)# exit
(config-pmap)# class video-n-data
(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 exceed-action set-
dscp-transmit 2 violate-action drop
(config-pmap-c)# exit
(config-pmap)# exit
(config)# interface port 1/0/1
(config-if-port)# service-policy input cos-based-treatment
(config-if-port)#
```

7.1.17 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。
シンタックス	**policy-map** *POLICY-MAP-NAME* **no policy-map** *POLICY-MAP-NAME*
パラメーター	*POLICY-MAP-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
コマンドモード	グローバル設定モード

policy-map	
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。
制限事項	作成できるポリシーマップは最大 255 個です。
注意事項	-
対象バージョン	1.01.01

使用例：policy というポリシーマップを作成する方法を示します。ポリシーマップ内には、2 つのクラスポリシーを設定しています。class1 というクラスポリシーは、アクセスリスト「acl_rd」と一致するトラフィックのポリシーを指定します。2 番目のクラスは、class-default という名前のデフォルトのクラスです。定義済みのクラスと一致しないパケットを含んでいます。

```
# configure terminal
(config)# class-map class1
(config-cmap)# match access-group name acl_rd
(config-cmap)# exit
(config)# policy-map policy
(config-pmap)# class class1
(config-pmap-c)# set ip dscp 46
(config-pmap-c)# exit
(config-pmap)# class class-default
(config-pmap-c)# set ip dscp 00
(config-pmap-c)#
```

7.1.18 class (QoS)

class (QoS)	
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。
シンタックス	**class** *CLASS-MAP-NAME* **no class** *CLASS-MAP-NAME*
パラメーター	*CLASS-MAP-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）
コマンドモード	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。
制限事項	最大クラス数は 255 です。
注意事項	-
対象バージョン	1.01.01

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)#
```

7.1.19 set

set	
目的	送信パケットについて、優先度値フィールド、DSCP フィールド、および CoS フィールドを新たに設定します。パケットの CoS キューを指定することもできます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	set {[ip] precedence *PRECEDENCE* ｜ [ip] dscp *DSCP* ｜ cos *COS* ｜ cos-queue *COS-QUEUE*} no set {[ip] precedence *PRECEDENCE* ｜ [ip] dscp *DSCP* ｜ cos *COS* ｜ cos-queue *COS-QUEUE*}
パラメーター	ip（省略可能）：IPv4 パケットのみ優先度値を設定する場合に指定します。指定しない場合、IPv4 と IPv6 の両方の優先度値がマークされます。IPv6 パケットの場合、優先度値は IPv6 ヘッダーのトラフィッククラスの最も重要な 3 ビットです。優先度値を設定しても、CoS キューの選択には影響を与えません。 precedence *PRECEDENCE*：パケットの新しい優先度値を、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（省略可能）：IPv4 パケットのみ DSCP を設定する場合に指定します。指定しない場合、IPv4 と IPv6 の両方の DSCP がマークされます。DSCP を設定しても、CoS キューの選択には影響を与えません。 dscp *DSCP*：パケットの新しい DSCP を、0～63 の範囲で指定します。 cos *COS*：パケットに割り当てる新しい CoS 値を、0～7 の範囲で指定します。 cos-queue *COS-QUEUE*：パケットに割り当てる CoS キューを直接指定します。CoS キューを指定すると、既存の CoS キューの選択が上書きされます。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
コマンドモード	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、1 つのクラスに対して複数の set コマンドを設定できます。 条件一致したパケットに直接 CoS キューを割り当てるには、set cos-queue コマンドを実行してください。 set dscp コマンドは、CoS キューの選択には影響を与えません。 set cos-queue コマンドは、送信パケットの CoS 値を変更しません。

set	
	police コマンドと **set** コマンドは、同じクラスに対して実行できます。 **set [ip] precedence** コマンドは、グリーントラフィックのみに適用されます。その他のコマンドは、パケットのすべてのトラフィック初期カラーに適用されます。
制限事項	スタック構成において、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、**set cos-queue** コマンドによる送信キューの変更は動作しません。 ApresiaNP2000-48T4X、および ApresiaNP2000-48T4X-PoE において、以下のトラフィックに対しては、**set cos-queue** コマンドによる送信キューの変更は動作しません。 • ポート 1～24、49～50 で受信して、ポート 25～48、51～52 から送信するトラフィック • ポート 25～48、51～52 で受信して、ポート 1～24、49～50 から送信するトラフィック
注意事項	-
対象バージョン	1.01.01

使用例：class1 クラスのポリシーを使用して、ポリシーマップ policy1 を設定する方法を示します。class1 クラスに含まれているパケットは、DSCP が 10、認定速度が 1Mbps で、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)# policy-map policy1
(config-pmap)# class class1
(config-pmap-c)# set ip dscp 10
(config-pmap-c)# police 1000000 16384 exceed-action set-dscp-transmit 10
(config-pmap-c)# exit
(config-pmap)#
```

7.1.20 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。
シンタックス	**police** *KBPS* [*BURST-NORMAL* [*BURST-MAX*]] [**conform-action** *ACTION*] **exceed-action** *ACTION* [**violate-action** *ACTION*] [**color-aware**] **no police**
パラメーター	*KBPS*：平均レートを 0～10,000,000(Kbps)の範囲で指定します。 *BURST-NORMAL*（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。 **confirm-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。

police	
	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
コマンドモード	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	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 confirm-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。

police	
	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。
制限事項	**set-lp-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。
注意事項	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。
対象バージョン	1.01.01

使用例：[平均レート=5000Kbps，標準バーストサイズ=16KByte，**confirm-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)#
```

7.1.21 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。
シンタックス	**police cir** *CIR* [**bc** *CONFORM-BURST*] **pir** *PIR* [**be** *PEAK-BURST*] [**conform-action** *ACTION*] [**exceed-action** *ACTION* [**violate-action** *ACTION*]] [**color-aware**] **no police**
パラメーター	*CIR*：保証帯域を 0～10,000,000(Kbps)の範囲で指定します。

police cir	
	bc *CONFORM-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** *PEAK-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。 **confirm-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。 • **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-lp-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
コマンドモード	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	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 **confirm-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

police cir	
	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。
制限事項	set-lp-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。
注意事項	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。
対象バージョン	1.01.01

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，confirm-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)#
```

7.1.22 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。

police aggregate	
シンタックス	police aggregate *AG-POLICER-NAME* no police
パラメーター	*AG-POLICER-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
コマンドモード	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	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 コマンドは、種類が異なるクラスマップに適用することはできません。 • 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 *ACCESS-LIST-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 *ACCESS-LIST-NAME*（IP アクセスリスト） 　• match [ip] dscp *DSCP-LIST* 　• match ip precedence *IP-PRECEDENCE-LIST* 　• match ip 　• match 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 *ACCESS-LIST-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 *ACCESS-LIST-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

police aggregate	
	• 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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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)#
```

7.1.23 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。
シンタックス	**mls qos aggregate-policer** *AG-POLICER-NAME KBPS* [*BURST-NORMAL* [*BURST-MAX*]] [**conform-action** *ACTION*] **exceed-action** *ACTION* [**violate-action** *ACTION*] [**color-aware**] **mls qos aggregate-policer** *AG-POLICER-NAME* **cir** *CIR* [**bc** *CONFORM-BURST*] **pir** *PIR* [**be** *PEAK-BURST*] [**conform-action** *ACTION*] [**exceed-action** *ACTION* [**violate-action** *ACTION*]] [**color-aware**] **no mls qos aggregate-policer** *AG-POLICER-NAME*
パラメーター	*AG-POLICER-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-NORMAL*（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

mls qos aggregate-policer	
	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。 **confirm-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-lp-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** *CONFORM-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** *PEAK-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
コマンドモード	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	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：!#$%&()+,.=@[]^_`{}~/:<>*-'¥"

mls qos aggregate-policer	
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

使用例：1 レート 2 カラーポリサーとして使用する「agg-policer5」という名前の集約ポリサーを、[平均レート=8000Kbps, 標準バーストサイズ=32KByte, confirm-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)#
```

7.1.24 service-policy

service-policy	
目的	ポリシーマップをインターフェースに設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	service-policy {input | output} *POLICY-MAP-NAME* no service-policy {input | output}
パラメーター	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。 *POLICY-MAP-NAME*：ポリシーマップ名を指定します。
デフォルト	なし
コマンドモード	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	1 つのインターフェースには、受信方向に 1 個、送信方向に 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。
制限事項	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)
注意事項	-
対象バージョン	1.01.01

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)#
```

7.1.25 cpu rate-limit

cpu rate-limit	
目的	CPU 宛てパケットの最大受信レートを変更します。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。
シンタックス	**cpu rate-limit** {**cos0** *RATE0* ｜ **cos1** *RATE1* ｜ **cos2** *RATE2* ｜ **cos3** *RATE3*} **no cpu rate-limit** {**cos0** ｜ **cos1** ｜ **cos2** ｜ **cos3**}
パラメーター	**cos0** *RATE0*：CPU 宛て CoS 0 の最大受信レートを、50～1000pps の範囲で指定します。 **cos1** *RATE1*：CPU 宛て CoS 1 の最大受信レートを、50～1000pps の範囲で指定します。 **cos2** *RATE2*：CPU 宛て CoS 2 の最大受信レートを、50～1000pps の範囲で指定します。 **cos3** *RATE3*：CPU 宛て CoS 3 の最大受信レートを、50～2000pps の範囲で指定します。
デフォルト	CPU 宛て CoS 0 = 150pps CPU 宛て CoS 1 = 150pps CPU 宛て CoS 2 = 500pps CPU 宛て CoS 3 = 2,000pps
コマンドモード	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	スイッチ LSI から CPU 宛てに転送するパケットは、用途ごとにクラス分け(CoS)し、クラスごとに最大受信レートを設けて制御を行っています。CPU 使用率が高い環境であれば、不要なパケットを扱うクラス(CoS)の最大受信レートを下げることで、CPU 使用率を下げることが可能です。また、CPU 使用率が低い環境であれば、処理量を上げたいパケットを扱うクラス(CoS)の最大受信レートを上げることで、該当パケットを扱う処理量を上げることが可能です。クラスごとのパケットの種類を下記に示します。 • CPU 宛て CoS 0：未使用 • CPU 宛て CoS 1：Unknown Unicast IPv4/IPv6 パケット、Unknown Multicast IPv4/IPv6 パケット • CPU 宛て CoS 2：ARP Request パケット(※1)、Broadcast IP パケット(※1)、MAC 認証対象パケット、IEEE 802.1X 認証対象パケット、Web 認証対象パケット • CPU 宛て CoS 3：LLDPDU、IPv6 の All Router/Host 宛てパケット、DHCP IPv4/IPv6 Message、IGMP/MLD Message (※1)は設定に関係なく常に CPU 宛てに転送されます。(※1)で示す以外のパケットは、各機能の設定が有効時のみ CPU 宛に転送されます。 上記で示した以外のパケットは、CoS 0～3 より優先度の高いクラスに割り当てられています。 パケットによってはクラスごとの最大受信レートとは異なる受信制限を設けているものがあります。 スタックポートを経由して転送される一部のパケットは異なるクラスで扱われるものがあります。
制限事項	CPU 宛て CoS 0～3 以外のクラスの最大受信レートの変更はできません。

cpu rate-limit	
注意事項	CPU 使用率が 100%になることで CPU リソースを使用する機能に影響を与えます。 最大受信レートは CPU 使用率が常に 100%未満になる値を設定してください。
対象バージョン	1.09.01

使用例：CPU 宛て CoS 0 の最大受信レートを 300pps に変更する方法を示します。

```
# configure terminal
(config)# cpu rate-limit cos0 300
(config)#
```

7.1.26 show mls qos queueing

show mls qos queueing	
目的	CoS から送信キューへのマッピング設定を表示します。また、指定したインターフェースの 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。
シンタックス	**show mls qos queueing** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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 から送信キューへのマッピング設定が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：CoS 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。

7.1.27 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。
シンタックス	**show mls qos interface** [*INTERFACE-ID* [,|-]] **scheduler**
パラメーター	*INTERFACE-ID*（省略可能）：QoS 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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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

7.1.28 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。
シンタックス	**show mls qos interface** [*INTERFACE-ID* [,|-]] **trust**
パラメーター	*INTERFACE-ID*（省略可能）：QoS 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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/2 からポート 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

7.1.29 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。
シンタックス	**show mls qos interface** [*INTERFACE-ID* [,|-]] **cos**
パラメーター	*INTERFACE-ID*（省略可能）：QoS 設定を表示するインターフェースを、以下のパ

show mls qos interface cos	
	ラメーターで指定します。 • port：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/2 からポート 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

7.1.30 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。
シンタックス	**show mls qos interface** [*INTERFACE-ID* [,|-]] **map dscp-cos**
パラメーター	*INTERFACE-ID*（省略可能）：QoS 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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 の、DSCP から CoS 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 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。

7.1.31 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。
シンタックス	**show mls qos interface** [*INTERFACE-ID* [,|-]] **map cos-color**
パラメーター	*INTERFACE-ID*（省略可能）：QoS 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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/3 からポート 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 値を表示します。
(3)	イエロートラフィックに分類される CoS 値を表示します。
(4)	レッドトラフィックに分類される CoS 値を表示します。

7.1.32 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。
シンタックス	**show mls qos interface** [*INTERFACE-ID* [,|-]] **map dscp-color**
パラメーター	*INTERFACE-ID*（省略可能）：QoS 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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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。

7.1.33 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。
シンタックス	**show mls qos map dscp-mutation** [*DSCP-MAP-NAME*]
パラメーター	*DSCP-MAP-NAME*（省略可能）：DSCP 変換マップ名を指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

7.1.34 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。
シンタックス	**show mls qos interface** [*INTERFACE-ID* [,|-]] **dscp-mutation**
パラメーター	*INTERFACE-ID*（省略可能）：QoS 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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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。

7.1.35 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。
シンタックス	**show mls qos interface** [*INTERFACE-ID* [,|-]] **queue-rate-limit**
パラメーター	*INTERFACE-ID*（省略可能）：QoS 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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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

項番	説明
	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。

7.1.36 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。
シンタックス	**show mls qos interface** [*INTERFACE-ID* [,|-]] **rate-limit**
パラメーター	*INTERFACE-ID*（省略可能）：QoS 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**：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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** 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** 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。

7.1.37 show class-map

show class-map	
目的	クラスマップを表示します。
シンタックス	**show class-map** [*CLASS-MAP-NAME*]
パラメーター	*CLASS-MAP-NAME*（省略可能）：クラスマップ名を指定します。

show class-map	
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

7.1.38 show policy-map

show policy-map	
目的	ポリシーマップを表示します。
シンタックス	**show policy-map** [*POLICY-MAP-NAME* | **interface** *INTERFACE-ID*]
パラメーター	*POLICY-MAP-NAME*（省略可能）：ポリシーマップ名を指定します。指定しない場合、すべてのポリシーマップが表示されます。 **interface** *INTERFACE-ID*（省略可能）：ポリシーマップ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**：物理ポートを指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

7.1.39 show mls qos aggregate-policer

show mls qos aggregate-policer	
目的	集約ポリサーを表示します。
シンタックス	**show mls qos aggregate-policer** [*AG-POLICER-NAME*]
パラメーター	*AG-POLICER-NAME*（省略可能）：集約ポリサー名を指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)関連の設定コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
access-list resequence	access-list resequence {ACL-NAME | ACL-NUMBER} STARTING-SEQUENCE-NUMBER INCREMENT no access-list resequence
acl-hardware-counter	acl-hardware-counter {access-group {ACL-NAME | ACL-NUMBER} | vlan-filter MAP-NAME} no acl-hardware-counter {access-group {ACL-NAME | ACL-NUMBER} | vlan-filter MAP-NAME}
list-remark	list-remark TEXT no list-remark
expert access-group	expert access-group {NAME | NUMBER} [in | out] no expert access-group [NAME | NUMBER] [in | out]
expert access-list	expert access-list extended NAME [NUMBER] no expert access-list extended {NAME | NUMBER}
permit | deny (expert access-list)	[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
ip access-group	ip access-group {NAME | NUMBER} [in | out] no ip access-group [NAME | NUMBER] [in | out]
ip access-list	ip access-list [extended] NAME [NUMBER] no ip access-list [extended] {NAME | NUMBER}
permit | deny (ip access-list)	[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 PROTOCOL-ID] CONDITION [SEQ] {permit [authentication-bypass] | deny} CONDITION no SEQ
arp access-group	arp access-group {NAME | NUMBER} [in] no arp access-group [NAME | NUMBER] [in]
arp access-list	arp access-list NAME [NUMBER] no arp access-list {NAME | NUMBER}
permit | deny (arp access-list)	[SEQ] {permit [authentication-bypass] | deny} ip SENDER-IP-ADDRESS mac SRC-MAC-ADDRESS no SEQ

コマンド	コマンドとパラメーター
ipv6 access-group	ipv6 access-group {NAME | NUMBER} [in | out] no ipv6 access-group [NAME | NUMBER] [in | out]
ipv6 access-list	ipv6 access-list [extended] NAME [NUMBER] no ipv6 access-list [extended] {NAME | NUMBER}
permit | deny (ipv6 access-list)	[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 PROTOCOL-ID] CONDITION [SEQ] {permit [authentication-bypass] | deny} CONDITION no SEQ
mac access-list enable ip-packets	mac access-list enable ip-packets no mac access-list enable ip-packets
mac access-group	mac access-group {NAME | NUMBER} [in | out] no mac access-group [NAME | NUMBER] [in | out]
mac access-list	mac access-list extended NAME [NUMBER] no mac access-list extended {NAME | NUMBER}
permit | deny (mac access-list)	[SEQ] {permit [authentication-bypass] | deny} CONDITION no SEQ
vlan access-map	vlan access-map MAP-NAME [SEQUENCE-NUM] no vlan access-map MAP-NAME [SEQUENCE-NUM]
match ip address	match ip address {ACL-NAME | ACL-NUMBER} no match ip address {ACL-NAME | ACL-NUMBER}
match arp address	match arp address {ACL-NAME | ACL-NUMBER} no match arp address {ACL-NAME | ACL-NUMBER}
match ipv6 address	match ipv6 address {ACL-NAME | ACL-NUMBER} no match ipv6 address {ACL-NAME | ACL-NUMBER}
match mac address	match mac address {ACL-NAME | ACL-NUMBER} no match mac address {ACL-NAME | ACL-NUMBER}
action	action {forward | drop | redirect INTERFACE-ID} no action
vlan filter	vlan filter MAP-NAME vlan-list VLAN-ID-LIST no vlan filter MAP-NAME vlan-list VLAN-ID-LIST

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。

コマンド	コマンドとパラメーター
show access-group	show access-group [interface INTERFACE-ID]
show access-list	show access-list [ip [NAME | NUMBER] | arp [NAME | NUMBER] | mac [NAME | NUMBER] | ipv6 [NAME | NUMBER] | expert [NAME | NUMBER]]

コマンド	コマンドとパラメーター
show access-list resource reserved-group	show access-list resource reserved-group
show access-list resource reserved-priority	show access-list resource reserved-priority
show vlan access-map	show vlan access-map [MAP-NAME]
show vlan filter	show vlan filter [access-map MAP-NAME | vlan VLAN-ID]
clear acl-hardware-counter	clear acl-hardware-counter {access-group [ACL-NAME | ACL-NUMBER] | vlan-filter [MAP-NAME]}

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、設定済みエントリーのシーケンス番号を一括変更します。
シンタックス	access-list resequence {*ACL-NAME* | *ACL-NUMBER*} *STARTING-SEQUENCE-NUMBER INCREMENT* no access-list resequence
パラメーター	*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-NUMBER*：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。 *STARTING-SEQUENCE-NUMBER*：変更するエントリーのシーケンス番号の開始値を、1～65535 の範囲で指定します。デフォルトは 10 です。 *INCREMENT*：シーケンス番号の増分値（ステップ値）を 1～32 の範囲で指定します。デフォルトは 10 です。
デフォルト	開始値：10、増分値：10
コマンドモード	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	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エントリー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、設定済みエントリー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エントリーのシーケンス番号が一括変更されます。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

使用例：R&D という名称の IP アクセスリストのシーケンス番号を変更する方法を示します。

```
# configure terminal
(config)# show access-list ip R&D

Extended IP access list R&D(ID: 3552)
    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

(config)# ip access-list extended R&D
(config-ip-ext-acl)# 5 permit tcp any 10.30.0.0 0.0.255.255
(config-ip-ext-acl)# exit
(config)# show access-list ip R&D

Extended IP access list R&D(ID: 3552)
    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

(config)# access-list resequence R&D 1 2
(config)# show access-list ip R&D

Extended IP access list R&D(ID: 3552)
    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指定したアクセスリスト名の、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。
シンタックス	acl-hardware-counter {access-group {*ACL-NAME* | *ACL-NUMBER*} | vlan-filter *MAP-NAME*} no acl-hardware-counter {access-group {*ACL-NAME* | *ACL-NUMBER*} | vlan-filter *MAP-NAME*}
パラメーター	access-group *ACL-NAME*：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を指定します。 access-group *ACL-NUMBER*：ハードウェアカウンターを有効にする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
コマンドモード	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	access-group パラメーターを指定すると、指定したアクセスリストに適用されるすべてのインターフェースのアクセスリストハードウェアカウンターが有効になります。各ルールに一致するパケットの数がカウントされます。 vlan-filter パラメーターを指定すると、指定した VLAN アクセスマップに適用されるすべての VLAN のアクセスリストハードウェアカウンターが有効になります。各 VLAN アクセスマップによって許可されるパケットの数がカウントされま

acl-hardware-counter	
	す。
制限事項	以下の機能で使用している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。 • 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
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**list-remark** *TEXT* **no list-remark**
パラメーター	*TEXT*：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
コマンドモード	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	拡張 MAC 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、および拡張エキスパートアクセスリストのアクセスリスト設定モードで使用するコマンドです。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	expert access-group {*NAME* | *NUMBER*} [in | out] no expert access-group [*NAME* | *NUMBER*] [in | out]
パラメーター	*NAME*：適用する拡張エキスパートアクセスリスト名を指定します。 *NUMBER*：適用する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
コマンドモード	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。ApresiaNP2000 シリーズでは、装置全体で Ingress グループ用に 1792 個、Egress グループ用に 512 個のリソースが用意されていますが、消費量はアクセスリスト種別により異なります。 ApresiaNP2000 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のみで使用する場合、拡張エキスパートアクセスリストを Ingress グループに最大 896 個、Egress グループに最大 256 個設定できます。 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）を使用したルール設定は、装置全体で最大 32 個まで設定できます。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**expert access-list extended** *NAME* [*NUMBER*] **no expert access-list extended** {*NAME* | *NUMBER*}
パラメーター	*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。 *NUMBER*（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
コマンドモード	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	すべてのアクセスリスト内で、名前を一意にしてください。名前に使用する文字は、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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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において、permit（許可）エントリー、または deny（拒否）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。
シンタックス	[*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*

permit | deny (expert access-list)	
	no *SEQ*
パラメーター	*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：許可エントリーを設定する場合に指定します。 authentication-bypass（省略可能）：AccessDefender 認証のための CPU コピーを行わない許可エントリーを設定する場合に指定します。 deny：拒否エントリーを設定する場合に指定します。 tcp：TCP プロトコルに対するエントリーとする場合に指定します。 udp：UDP プロトコルに対するエントリーとする場合に指定します。 icmp：ICMP プロトコルに対するエントリーとする場合に指定します。 *PROTOCOL*（省略可能）：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
コマンドモード	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エントリーを作成した場合、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エントリー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 認証ポートでの、permit エントリーと permit authentication-bypass エントリーの違いは以下のとおりです。 • permit エントリーに一致したパケットは、認証のために CPU にコピーされます。なお、許可エントリーのため、未認証状態でも中継は許可されます。 • permit authentication-bypass エントリーに一致したパケットは、認証のための CPU コピーは行われません。なお、許可エントリーのため、未認証状態でも中継は許可されます。 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値を 0 で指定したビットがチェック対象になり、ワイルドカードビット値を 1 で指定したビットはチェック対象外になります。（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） • 送信元 IP アドレス（*SRC-IP-ADDR SRC-IP-WILDCARD*）

permit | deny (expert access-list)	
	• 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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式）
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

■ 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

抽出条件	概要
	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) mask-request(17,0) mobile-redirect(32,-) net-

抽出条件	概要
	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 値を 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 値も 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「exp_acl」を作成し、「送信元 IP アドレスが 192.0.2.100 で、送信元 MAC アドレスが 00:00:5E:00:53:00 の TCP パケットを拒否するエントリー」を設定する方法を示します。

```
# configure terminal
(config)# expert access-list extended exp_acl
(config-exp-nacl)# 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 アクセスリストを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	ip access-group {*NAME* | *NUMBER*} [in | out] no ip access-group [*NAME* | *NUMBER*] [in | out]
パラメーター	*NAME*：適用する IP アクセスリスト名を指定します。 *NUMBER*：適用する IP アクセスリスト番号を、1～3999 の範囲で指定します。

ip access-group	
	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
コマンドモード	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。ApresiaNP2000 シリーズでは、装置全体で Ingress グループ用に 1792 個、Egress グループ用に 512 個のリソースが用意されていますが、消費量はアクセスリスト種別により異なります。 ApresiaNP2000 シリーズですべてのリソースを IP アクセスリストのみで使用する場合、IP アクセスリストを Ingress グループに最大 896 個、Egress グループに最大 512 個設定できます。 コマンドが正しく適用された場合、残りの使用可能エントリー数が表示されます。 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）を使用したルール設定は、装置全体で最大 32 個まで設定できます。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	ip access-list [extended] *NAME* [*NUMBER*] no ip access-list [extended] {*NAME* | *NUMBER*}
パラメーター	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。 *NUMBER* (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
コマンドモード	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	すべてのアクセスリスト内で、名前を一意にしてください。名前に使用する文字は、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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 アクセスリストにおいて、permit (許可) エントリー、または deny (拒否) 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。
シンタックス	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 *PROTOCOL-ID*] *CONDITION* 標準 IP アクセスリスト： [*SEQ*] {permit [authentication-bypass] | deny} *CONDITION*

permit | deny (ip access-list)	
	no *SEQ*
パラメーター	*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：許可エントリーを設定する場合に指定します。 authentication-bypass（省略可能）：AccessDefender 認証のための CPU コピーを行わない許可エントリーを設定する場合に指定します。 deny：拒否エントリーを設定する場合に指定します。 tcp：TCP プロトコルに対するエントリーとする場合に指定します。 udp：UDP プロトコルに対するエントリーとする場合に指定します。 icmp：ICMP プロトコルに対するエントリーとする場合に指定します。 *PROTOCOL*（省略可能）：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 *PROTOCOL-ID*（省略可能）：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
コマンドモード	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エントリーを作成した場合、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エントリー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 認証ポートでの、permit エントリーと permit authentication-bypass エントリーの違いは以下のとおりです。 • permit エントリーに一致したパケットは、認証のために CPU にコピーされます。なお、許可エントリーのため、未認証状態でも中継は許可されます。 • permit authentication-bypass エントリーに一致したパケットは、認証のための CPU コピーは行われません。なお、許可エントリーのため、未認証状態でも中継は許可されます。 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値を 0 で指定したビットがチェック対象になり、ワイルドカードビット値を 1 で指定したビットはチェック対象外になります。（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） • 送信元 IP アドレス（*SRC-IP-ADDR SRC-IP-WILDCARD*）

permit | deny (ip access-list)	
	• 宛先 IP アドレス (*DST-IP-ADDR DST-IP-WILDCARD*)
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

■ 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	○	○	○	○	○	−	−	○	○
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

抽出条件	概要
	• **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：「Strict-Control」という名前の拡張 IP アクセスリストに、以下の 4 つのエントリーを設定する方法を示します。

- 宛先 IP アドレスが 10.20.0.0/16 の TCP パケットを許可するエントリー
- 宛先 IP アドレスが 10.100.1.2 の TCP パケットを許可するエントリー
- 宛先 L4 ポート番号が 80 の TCP パケットを許可するエントリー
- すべての ICMP パケットを許可するエントリー

```
# configure terminal
(config)# ip access-list extended Strict-Control
(config-ip-ext-acl)# permit tcp any 10.20.0.0 0.0.255.255
(config-ip-ext-acl)# permit tcp any host 10.100.1.2
(config-ip-ext-acl)# permit tcp any any eq 80
(config-ip-ext-acl)# permit icmp any any
(config-ip-ext-acl)#
```

使用例：「std-acl」という名前の標準 IP アクセスリストに、以下の 2 つのエントリーを設定する方法を示します。

- 宛先 IP アドレスが 10.20.0.0/16 の IP パケットを許可するエントリー
- 宛先 IP アドレスが 10.100.1.2 の IP パケットを許可するエントリー

```
# configure terminal
(config)# ip access-list std-acl
(config-ip-acl)# permit any 10.20.0.0 0.0.255.255
(config-ip-acl)# permit any host 10.100.1.2
(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 アクセスリストを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	arp access-group {*NAME* | *NUMBER*} [in] no arp access-group [*NAME* | *NUMBER*] [in]
パラメーター	*NAME*：適用する ARP アクセスリスト名を指定します。 *NUMBER*：適用する 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
コマンドモード	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	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。 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。ApresiaNP2000 シリーズでは、装置全体で Ingress グループ用に 1792 個、Egress グループ用に 512 個のリソースが用意されていますが、消費量はアクセスリスト種別により異なります。 ApresiaNP2000 シリーズですべてのリソースを ARP アクセスリストのみで使用する場合、ARP アクセスリストを Ingress グループに最大 896 個設定できます。 コマンドが正しく適用された場合、残りの使用可能エントリー数が表示されます。
制限事項	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。
注意事項	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。
対象バージョン	1.09.05

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。
シンタックス	**arp access-list** *NAME* [*NUMBER*] **no arp access-list** {*NAME* | *NUMBER*}
パラメーター	*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。 *NUMBER*（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
コマンドモード	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	すべてのアクセスリスト内で、名前を一意にしてください。名前に使用する文字は、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。
制限事項	-
注意事項	-
対象バージョン	1.09.05

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 アクセスリストにおいて、permit（許可）エントリー、または deny（拒否）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。
シンタックス	[*SEQ*] {**permit** [**authentication-bypass**] | **deny**} **ip** *SENDER-IP-ADDRESS* **mac** *SRC-MAC-ADDRESS* **no** *SEQ*
パラメーター	*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**：許可エントリーを設定する場合に指定します。 **authentication-bypass**（省略可能）：AccessDefender 認証のための CPU コピーを行わない許可エントリーを設定する場合に指定します。 **deny**：拒否エントリーを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。

permit | deny (arp access-list)	
	• **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
コマンドモード	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エントリーを作成した場合、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エントリー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 認証ポートでの、**permit** エントリーと **permit authentication-bypass** エントリーの違いは以下のとおりです。 • **permit** エントリーに一致したパケットは、認証のために CPU にコピーされます。なお、許可エントリーのため、未認証状態でも中継は許可されます。 • **permit authentication-bypass** エントリーに一致したパケットは、認証のための CPU コピーは行われません。なお、許可エントリーのため、未認証状態でも中継は許可されます。 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値を 0 で指定したビットがチェック対象になり、ワイルドカードビット値を 1 で指定したビットはチェック対象外になります。（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） • 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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式）
制限事項	-
注意事項	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。
対象バージョン	1.09.05

使用例：「ARP-ACL」という名前の ARP アクセスリストに、以下の 2 つのエントリーを設定する方法を示します。

- Sender IP address フィールドが 192.0.2.0/24 の ARP パケットを許可するエントリー
- 送信元 MAC アドレスが 00:00:5E:00:53:00～00:00:5E:00:53:FF の ARP パケットを許可するエントリー

```
# configure terminal
(config)# arp access-list ARP-ACL
(config-arp-nacl)# permit ip 192.0.2.0 0.0.0.255 mac any
(config-arp-nacl)# permit ip any mac 00:00:5e:00:53:00 00:00:00:00:00:ff
(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 アクセスリストを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**ipv6 access-group** {*NAME* | *NUMBER*} [**in** | **out**] **no ipv6 access-group** [*NAME* | *NUMBER*] [**in** | **out**]
パラメーター	*NAME*：適用する IPv6 アクセスリスト名を指定します。 *NUMBER*：適用する 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
コマンドモード	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。ApresiaNP2000 シリーズでは、装置全体で Ingress グループ用に 1792 個、Egress グループ用に 512 個のリソースが用意されていますが、消費量はアクセスリスト種別により異なります。 ApresiaNP2000 シリーズですべてのリソースを IPv6 アクセスリストのみで使用する場合、IPv6 アクセスリストを Ingress グループに最大 384 個、Egress グループに最大 256 個設定できます。 コマンドが正しく適用された場合、残りの使用可能エントリー数が表示されます。 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**）を使用したルール設定は、装置全体で最大 32 個まで設定できます。

ipv6 access-group	
	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**ipv6 access-list** [extended] *NAME* [*NUMBER*] **no ipv6 access-list** [extended] {*NAME* | *NUMBER*}
パラメーター	**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。 *NUMBER* (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
コマンドモード	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	すべてのアクセスリスト内で、名前を一意にしてください。名前に使用する文字は、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。
制限事項	-

ipv6 access-list	
注意事項	-
対象バージョン	1.01.01

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 アクセスリストにおいて、permit（許可）エントリー、または deny（拒否）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。
シンタックス	**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 *PROTOCOL-ID*] *CONDITION* **標準 IPv6 アクセスリスト：** [*SEQ*] {permit [authentication-bypass] | deny} *CONDITION* no *SEQ*
パラメーター	*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：許可エントリーを設定する場合に指定します。 authentication-bypass（省略可能）：AccessDefender 認証のための CPU コピーを行わない許可エントリーを設定する場合に指定します。 deny：拒否エントリーを設定する場合に指定します。 tcp：TCP プロトコルに対するエントリーとする場合に指定します。 udp：UDP プロトコルに対するエントリーとする場合に指定します。 icmp：ICMP プロトコルに対するエントリーとする場合に指定します。 *PROTOCOL*（省略可能）：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 *PROTOCOL-ID*（省略可能）：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
コマンドモード	IPv6 アクセスリスト設定モード

permit | deny (ipv6 access-list)	
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エントリーを作成した場合、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エントリー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 認証ポートでの、**permit** エントリーと **permit authentication-bypass** エントリーの違いは以下のとおりです。 • **permit** エントリーに一致したパケットは、認証のために CPU にコピーされます。なお、許可エントリーのため、未認証状態でも中継は許可されます。 • **permit authentication-bypass** エントリーに一致したパケットは、認証のための CPU コピーは行われません。なお、許可エントリーのため、未認証状態でも中継は許可されます。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01 1.09.05：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

抽出条件	概要
	SRC-IPV6-ADDR/PREFIX-LENGTH：送信元 IPv6 アドレスのプレフィックス指定
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 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/PREFIX-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：「ipv6-control」という名前の拡張 IPv6 アクセスリストに、以下の 4 つのエントリーを設定する方法を示します。

- 宛先 IPv6 アドレスが 2001:db8:100:200::/64 の TCP パケットを許可するエントリー
- 宛先 IPv6 アドレスが 2001:db8::aaaa の TCP パケットを許可するエントリー
- 宛先 L4 ポート番号が 80 の TCP パケットを許可するエントリー
- すべての ICMP パケットを許可するエントリー

```
# configure terminal
(config)# ipv6 access-list extended ipv6-control
(config-ipv6-ext-acl)# permit tcp any 2001:db8:100:200::/64
(config-ipv6-ext-acl)# permit tcp any host 2001:db8::aaaa
(config-ipv6-ext-acl)# permit tcp any any eq 80
(config-ipv6-ext-acl)# permit icmp any any
(config-ipv6-ext-acl)#
```

使用例：「ipv6-std-control」という名前の標準 IPv6 アクセスリストに、以下の 2 つのエントリーを設定する方法を示します。

- 宛先 IPv6 アドレスが 2001:db8:100:200::/64 の TCP パケットを許可するエントリー
- 宛先 IPv6 アドレスが 2001:db8::aaaa の TCP パケットを許可するエントリー

```
# configure terminal
(config)# ipv6 access-list ipv6-std-control
(config-ipv6-acl)# permit any 2001:db8:100:200::/64
(config-ipv6-acl)# permit any host 2001:db8::aaaa
(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。
シンタックス	**mac access-list enable ip-packets** **no mac access-list enable ip-packets**
パラメーター	なし
デフォルト	無効
コマンドモード	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、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

mac access-list enable ip-packets	
	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、1 つのパケットが異なる種別の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、その場合は以下の優先度で適用されるアクセスリストが選択されます。アクセスリストの優先度は **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、「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。 • 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。
制限事項	-
注意事項	-
対象バージョン	1.09.01

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設定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 アクセスリストを指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**mac access-group** {*NAME* | *NUMBER*} [**in** | **out**] **no mac access-group** [*NAME* | *NUMBER*] [**in** | **out**]
パラメーター	*NAME*：適用する拡張 MAC アクセスリスト名を指定します。 *NUMBER*：適用する拡張 MAC アクセスリスト番号を、6000～7999 の範囲で指定します。 **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
コマンドモード	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

mac access-group	
	す。ApresiaNP2000 シリーズでは、装置全体で Ingress グループ用に 1792 個、Egress グループ用に 512 個のリソースが用意されていますが、消費量はアクセスリスト種別により異なります。 ApresiaNP2000 シリーズですべてのリソースを拡張 MAC アクセスリストのみで使用する場合、拡張 MAC アクセスリストを Ingress グループに最大 1792 個、Egress グループに最大 512 個設定できます。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**mac access-list extended** *NAME* [*NUMBER*] **no mac access-list extended** {*NAME* | *NUMBER*}
パラメーター	*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。 *NUMBER*（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
コマンドモード	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	すべてのアクセスリスト内で、名前を一意にしてください。名前に使用する文字は、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。
制限事項	-
注意事項	-

mac access-list	
対象バージョン	1.01.01

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 アクセスリストにおいて、permit（許可）エントリー、または deny（拒否）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。
シンタックス	[*SEQ*] {permit [authentication-bypass] | deny} *CONDITION* no *SEQ*
パラメーター	*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：許可エントリーを設定する場合に指定します。 authentication-bypass（省略可能）：AccessDefender 認証のための CPU コピーを行わない許可エントリーを設定する場合に指定します。 deny：拒否エントリーを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 アクセスリストの抽出条件」を参照。
デフォルト	なし
コマンドモード	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エントリーを作成した場合、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エントリー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 認証ポートでの、permit エントリーと permit authentication-bypass エントリーの違いは以下のとおりです。 • permit エントリーに一致したパケットは、認証のために CPU にコピーされます。なお、許可エントリーのため、未認証状態でも中継は許可されます。 • permit authentication-bypass エントリーに一致したパケットは、認証のための CPU コピーは行われません。なお、許可エントリーのため、未認証状態でも中継は許可されます。 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値を 0 で指定したビットがチェック対象になり、ワイ

permit | deny (mac access-list)	
	ルドカードビット値を 1 で指定したビットはチェック対象外になります。(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) • 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*） • イーサタイプ（ethernet-type *TYPE MASK*） 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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式）
制限事項	-
注意事項	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。
対象バージョン	1.01.01

■ 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 値を 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 値も 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「daily-profile」を作成し、「送信元MACアドレスが00:00:5E:00:53:00～00:00:5E:00:53:FFの非IPフレームを許可するエントリー」を設定する方法を示します。

```
# configure terminal
(config)# mac access-list extended daily-profile
(config-mac-ext-acl)# permit 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。
シンタックス	**vlan access-map** *MAP-NAME* [*SEQUENCE-NUM*] **no vlan access-map** *MAP-NAME* [*SEQUENCE-NUM*]
パラメーター	*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。 *SEQUENCE-NUM*（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
コマンドモード	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	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**match ip address** {*ACL-NAME* | *ACL-NUMBER*} **no match ip address** {*ACL-NAME* | *ACL-NUMBER*}
パラメーター	*ACL-NAME*：関連付ける IP アクセスリスト名を指定します。 *ACL-NUMBER*：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
コマンドモード	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。 IP アクセスリストを関連付けた IPv4 サブマップは、IPv4 パケットだけが対象になります。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**match arp address** {*ACL-NAME* | *ACL-NUMBER*} **no match arp address** {*ACL-NAME* | *ACL-NUMBER*}
パラメーター	*ACL-NAME*：関連付ける ARP アクセスリスト名を指定します。

match arp address	
	ACL-NUMBER：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
コマンドモード	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 パケットだけが対象になります。 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 | 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。
制限事項	-
注意事項	-
対象バージョン	1.09.05

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。
シンタックス	**match ipv6 address** {*ACL-NAME* | *ACL-NUMBER*} **no match ipv6 address** {*ACL-NAME* | *ACL-NUMBER*}
パラメーター	*ACL-NAME*：関連付ける IPv6 アクセスリスト名を指定します。 *ACL-NUMBER*：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
コマンドモード	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

match ipv6 address	
	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 パケットだけが対象になります。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**match mac address** {*ACL-NAME* | *ACL-NUMBER*} **no match mac address** {*ACL-NAME* | *ACL-NUMBER*}
パラメーター	*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-NUMBER*：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
コマンドモード	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 パケットだけが対象になります。なお、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

match mac address	
	パケットも対象になります。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**action {forward | drop | redirect** *INTERFACE-ID*} **no action**
パラメーター	**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** *INTERFACE-ID*：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**：物理ポートを指定します。
デフォルト	**forward**
コマンドモード	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。
制限事項	-

action	
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	vlan filter *MAP-NAME* vlan-list *VLAN-ID-LIST* no vlan filter *MAP-NAME* vlan-list *VLAN-ID-LIST*
パラメーター	*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
コマンドモード	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	-
制限事項	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。
注意事項	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) ApresiaNP2000-24T4X が 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、最大で約 275 秒程度かかることがあります。 • (例) ApresiaNP2000-48T4X が 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、最大で約 540 秒程度かかることがあります。 AEOS-NP2000 Ver. 1.09.01 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。
対象バージョン	1.01.01

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	ポートに適用されたアクセスリスト情報を表示します。

show access-group	
シンタックス	show access-group [interface *INTERFACE-ID*]
パラメーター	interface *INTERFACE-ID*（省略可能）：アクセスリス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：物理ポートを指定します。複数指定できます。
デフォルト	なし
コマンドモード	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、アクセスリストが適用されたすべてのポートの情報が表示されます。
制限事項	interface パラメーターを使用してアクセスリストを適用していないポートを指定しても、何も表示されません。
注意事項	-
対象バージョン	1.01.01

使用例：すべてのポート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。
(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情報を表示します。
シンタックス	show access-list [ip [*NAME* | *NUMBER*] | arp [*NAME* | *NUMBER*] | mac [*NAME* | *NUMBER*] | ipv6 [*NAME* | *NUMBER*] | expert [*NAME* | *NUMBER*]]
パラメーター	ip（省略可能）：標準 IP アクセスリストまたは拡張 IP アクセスリストを表示する場合に指定します。以下のパラメーターで、表示する IP アクセスリストを指定できます。 • *NAME*（省略可能）：IP アクセスリスト名 • *NUMBER*（省略可能）：IP アクセスリスト番号(1～3999) arp（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。以下のパラメーターで、表示する ARP アクセスリストを指定できます。 • *NAME*（省略可能）：ARP アクセスリスト名 • *NUMBER*（省略可能）：ARP アクセスリスト番号(4000～5999) mac（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。以下のパラメーターで、表示する拡張 MAC アクセスリストを指定できます。 • *NAME*（省略可能）：拡張 MAC アクセスリスト名 • *NUMBER*（省略可能）：拡張 MAC アクセスリスト番号(6000～7999)

show access-list	
	ipv6（省略可能）：標準 IPv6 アクセスリストまたは拡張 IPv6 アクセスリストを表示する場合に指定します。以下のパラメーターで、表示する IPv6 アクセスリストを指定できます。 • *NAME*（省略可能）：IPv6 アクセスリスト名 • *NUMBER*（省略可能）：IPv6 アクセスリスト番号(11000～14999) **expert**（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。以下のパラメーターで、表示する拡張エキスパートアクセスリストを指定できます。 • *NAME*（省略可能）：拡張エキスパートアクセスリスト名 • *NUMBER*（省略可能）：拡張エキスパートアクセスリスト番号(8000～9999)
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01 1.09.05：arp パラメーターを追加

使用例：すべてのアクセスリスト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：「R&D」という名前の IP アクセスリストの設定情報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)	エントリーを表示します。

使用例：ハードウェアカウンターが有効に設定されているアクセスリストの設定情報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)	エントリーを表示します。
(3)	アクセスリストハードウェアカウンターによってカウントされた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によってカウントされた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。

使用例：拡張 MAC アクセスリストの設定情報を表示する方法を示します。

```
# show access-list mac

Extended MAC access list macAcl2(ID: 7998) ...(1)
    (2)                       (3)              (4)
    1 deny any any vlan 1  (Ing: 0 packets  Egr: 0 packets)
    65535 permit any any  (Ing: 0 packets  Egr: 0 packets)

    Counter enable on following port(s): ...(5)

Extended MAC access list macAcl1(ID: 7999)
    1 permit any any vlan 1  (Ing: 0 packets  Egr: 0 packets)
    65535 deny any any  (Ing: 0 packets  Egr: 0 packets)

    Counter enable on following port(s):
```

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)	エントリーを表示します。
(3)	アクセスリストハードウェアカウンターによってカウントされた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によってカウントされた送信パケット数を表示しま

項番	説明
	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。
シンタックス	show access-list resource reserved-group
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.04.01

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)：Pv6 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)

項番	説明
	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
(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)：Pv6 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。
シンタックス	show access-list resource reserved-priority
パラメーター	なし
デフォルト	なし
コマンドモード	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	アクセスリスト機能では、各アクセスリストが以下の優先度順で動作します。 **優先度** / **アクセスリスト種別** **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
制限事項	-
注意事項	-
対象バージョン	1.04.01

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) : Pv6 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
(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) : Pv6 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情報を表示します。
シンタックス	**show vlan access-map** [*MAP-NAME*]
パラメーター	*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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN アクセスマップを表示する方法を示します。

```
# show vlan access-map

VLAN access-map vlan-map 10 ...(1)
  (2)                       (3)
  match ip access list: stp_ip1(ID: 1888)
  action: forward ...(4)
  Counter enable on VLAN(s): 1-2 ...(5)
  match count: 8541 packets ...(6)
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の種類を表示します。
(3)	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。
(4)	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。
(5)	アクセスリストハードウェアカウンターが有効になっている VLAN を表示します。
(6)	アクセスリストハードウェアカウンターによってカウントされたパケット数を表示します。

8.1.32 show vlan filter

show vlan filter	
目的	VLAN フィルターの設定情報を表示します。
シンタックス	**show vlan filter** [**access-map** *MAP-NAME* | **vlan** *VLAN-ID*]
パラメーター	**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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN フィルターの設定情報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。
シンタックス	**clear acl-hardware-counter {access-group [*ACL-NAME* | *ACL-NUMBER*] | vlan-filter [*MAP-NAME*]}**
パラメーター	*ACL-NAME*（省略可能）：ハードウェアカウンターをクリアするアクセスリスト名を指定します。 *ACL-NUMBER*（省略可能）：ハードウェアカウンターをクリアするアクセスリスト番号を指定します。 *MAP-NAME*（省略可能）：ハードウェアカウンターをクリアする VLAN アクセスマップ名を指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	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 アクセスマップ名を指定しない場合、すべての VLAN フィルターのハードウェアカウンターがクリアされます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：アクセスリスト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。

コマンド	コマンドとパラメーター
access-defender	access-defender
total-client	total-client NUMBER1 [deny-client NUMBER2] no total-client
authentication interface	authentication interface INTERFACE-ID [,|-] {dot1x | mac | web | gateway | static | web-mac | web-dot1x | dot1x-mac | web-dot1x-mac} no authentication interface INTERFACE-ID [, | -] {dot1x | mac | web | gateway | static | web-mac | web-dot1x | dot1x-mac | web-dot1x-mac}
aaa-local-db user	aaa-local-db user USER-ID [password [0 | 7] PASSWORD] [vlan VLAN-ID] [class CLASS-ID] no aaa-local-db [user USER-ID]
access-defender static mac	access-defender static mac MAC-ADDRESS [vlan VLAN-ID] [class CLASS-ID] interface INTERFACE-ID no access-defender static mac MAC-ADDRESS
logout aging-time	logout aging-time SECONDS [MINUTES [HOURS [DAYS]]] {web | gateway | mac | dot1x} no logout aging-time [web | gateway | mac | dot1x]
logout timeout	logout timeout SECONDS [MINUTES [HOURS [DAYS]]] {web | gateway | mac | dot1x} no logout timeout [web | gateway | mac | dot1x]
logout clock	logout clock HH:MM {web | gateway | mac | dot1x} no logout clock [web | gateway | mac | dot1x]
logout ping dst-ip	logout ping dst-ip {IP-ADDRESS | IPV6-ADDRESS} no logout ping dst-ip
logout ping ttl	logout ping ttl VALUE no logout ping ttl
logout linkdown disable interface	logout linkdown disable interface INTERFACE-ID [,|-] no logout linkdown disable interface INTERFACE-ID [,|-]
logout linkdown time	logout linkdown time SECONDS no logout linkdown time
logout linkdown time enable interface	logout linkdown time enable interface INTERFACE-ID [,|-] no logout linkdown time enable interface INTERFACE-ID [,|-]
roaming enable interface	roaming enable interface INTERFACE-ID [,|-] no roaming enable interface INTERFACE-ID [,|-]

コマンド	コマンドとパラメーター
authentication prefer-attribute	authentication {web-mac | dot1x-mac | web-dot1x | web-dot1x-mac} prefer-attribute {web | dot1x | mac} no authentication {web-mac | dot1x-mac | web-dot1x | web-dot1x-mac} prefer-attribute
authentication advanced-vlan-setting	authentication {web-mac | web-dot1x} advanced-vlan-setting no authentication {web-mac | web-dot1x} advanced-vlan-setting
authentication web-mac abort-if-failure	authentication web-mac abort-if-failure no authentication web-mac abort-if-failure
max-client interface	max-client NUMBER interface INTERFACE-ID [,|-] no max-client interface INTERFACE-ID [,|-]
max-discard	max-discard NUMBER no max-discard
vlan mode	vlan mode {dynamic port-base | static} no vlan mode
radius-server attribute mac-format	radius-server attribute mac-format case {lowercase | uppercase} delimiter {{hyphen | colon | dot} number {1 | 2 | 5} | none} no 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。

コマンド	コマンドとパラメーター
show access-defender aaa-local-db	show access-defender aaa-local-db
show access-defender client	show access-defender client [interface INTERFACE-ID [,|-]] [type {dhcp-snooping | disc | dot1x | gateway | mac | static | web}]
show access-defender deny	show access-defender deny
show access-defender port-configuration	show access-defender port-configuration
show access-defender port-channel-configuration	show access-defender port-channel-configuration
show access-defender rule-statistics	show access-defender rule-statistics
copy (AccessDefender)	copy {flash: [URL] | tftp: [URL]} {SYSTEM-FILE1 | webpages WEBPAGES-ID SYSTEM-FILE2} copy {SYSTEM-FILE1 | webpages WEBPAGES-ID SYSTEM-FILE2} {flash: [URL] | tftp: [URL]}
access-defender deny	access-defender deny {ip {IP-ADDRESS | IPV6-ADDRESS} | mac MAC-ADDRESS} timer MINUTES no access-defender deny {ip {IP-ADDRESS | IPV6-ADDRESS} | mac MAC-ADDRESS}
access-defender erase	access-defender erase [SYSTEM-FILE | webpages WEBPAGES-ID]

コマンド	コマンドとパラメーター
access-defender logout	access-defender logout {ip {IP-ADDRESS │ IPV6-ADDRESS} │ mac MAC-ADDRESS │ user USER-ID}

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。
シンタックス	**access-defender**
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**total-client** *NUMBER1* [**deny-client** *NUMBER2*] **no total-client**
パラメーター	*NUMBER1*：認証クライアントの最大数を、1～768 の範囲で指定します。 **deny-client** *NUMBER2*（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。
デフォルト	**total-client**：なし、**deny-client**：なし
コマンドモード	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。 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

total-client	
	ライ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。
制限事項	-
注意事項	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。 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。
対象バージョン	1.01.01

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。
シンタックス	**authentication interface** *INTERFACE-ID* [,|-] {dot1x | mac | web | gateway | static | web-mac | web-dot1x | dot1x-mac | web-dot1x-mac} **no authentication interface** *INTERFACE-ID* [, | -] {dot1x | mac | web | gateway | static | web-mac | web-dot1x | dot1x-mac | web-dot1x-mac}
パラメーター	*INTERFACE-ID*：認証を有効に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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。 **dot1x**：IEEE 802.1X 認証の有効／無効を設定する場合に指定します。 **mac**：MAC 認証の有効／無効を設定する場合に指定します。 **web**：Web 認証の有効／無効を設定する場合に指定します。 **gateway**：ゲートウェイ認証の有効／無効を設定する場合に指定します。 **static**：スタティック認証の有効／無効を設定する場合に指定します。 **web-mac**：Web/MAC 認証(AND)の有効／無効を設定する場合に指定します。 **web-dot1x**：Web/IEEE 802.1X 認証(AND)の有効／無効を設定する場合に指定します。 **dot1x-mac**：IEEE 802.1X/MAC 認証(AND)の有効／無効を設定する場合に指定します。 **web-dot1x-mac**：Web/IEEE 802.1X/MAC 認証(AND)の有効／無効を設定する場合に指定します。
デフォルト	なし

authentication interface	
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
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。
制限事項	ゲートウェイ認証を有効にしたインターフェースでは、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、ポートチャネルを指定して設定しま

<table>
<tr><th colspan="2">authentication interface</th></tr>
<tr><td></td><td>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。

トランクポートで認証に成功してダイナミックに VLAN が割り当てられた場合には、その VLAN はアクセスポートとして動作します（タグなしフレームを送受信）。ダイナミックに割り当てられた VLAN が switchport trunk allowed vlan コマンドで割り当てられていると当該ポートから送信するフレームがタグ付きフレームになってしまうため、そのポートでは switchport trunk allowed vlan コマンドで対象の VLAN を割り当てないで使用してください。</td></tr>
<tr><td>注意事項</td><td>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。以下に各認証機能の併用に関して示します。
<table>
<tr><th>認証機能</th><th>スタティック認証との併用（OR）</th><th>DHCP スヌーピングとの併用（AND）</th></tr>
<tr><td>web</td><td>可</td><td>可</td></tr>
<tr><td>dot1x</td><td>可</td><td>可</td></tr>
<tr><td>mac</td><td>可</td><td>可</td></tr>
<tr><td>web, mac（OR）</td><td>可</td><td>可</td></tr>
<tr><td>web, dot1x（OR）</td><td>可</td><td>可</td></tr>
<tr><td>dot1x, mac（OR）</td><td>可</td><td>可</td></tr>
<tr><td>web, dot1x, mac（OR）</td><td>可</td><td>可</td></tr>
<tr><td>gateway</td><td>不可</td><td>不可</td></tr>
<tr><td>web-mac（AND）</td><td>可</td><td>不可</td></tr>
<tr><td>web-dot1x（AND）</td><td>可</td><td>不可</td></tr>
<tr><td>dot1x-mac（AND）</td><td>可</td><td>不可</td></tr>
<tr><td>web-dot1x-mac（AND）</td><td>可</td><td>不可</td></tr>
</table>
AEOS-NP2000 Ver. 1.04 以降では、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。</td></tr>
<tr><td>対象バージョン</td><td>1.01.01</td></tr>
</table>

使用例：ポート 1/0/1 からポート 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。
シンタックス	**aaa-local-db user** *USER-ID* [**password** [0 | 7] *PASSWORD*] [**vlan** *VLAN-ID*] [**class** *CLASS-ID*] **no aaa-local-db** [**user** *USER-ID*]
パラメーター	*USER-ID*：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] *PASSWORD*（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。 • *PASSWORD*：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
コマンドモード	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。
制限事項	エントリーは、最大 3000 件まで登録できます。
注意事項	-
対象バージョン	1.01.01

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	スタティック認証で許可するエントリーを登録します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**access-defender static mac** *MAC-ADDRESS* [**vlan** *VLAN-ID*] [**class** *CLASS-ID*] **interface** *INTERFACE-ID* **no access-defender static mac** *MAC-ADDRESS*
パラメーター	*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

access-defender static mac	
	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 XX-XX-XX-XX-XX-XX 形式で表示されます。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式） **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** *INTERFACE-ID*：スタティック認証エントリーが接続され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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。
デフォルト	スタティックエントリーの設定なし
コマンドモード	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 1 つ登録するたびに、**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 つ消費します。 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。 本コマンドの設定は、**vlan mode** コマンドの設定に影響されません。
制限事項	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登録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登録した場合でも、内部のリソースは消費されます。
注意事項	スタティック認証エントリーを登録する場合は、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設定してください。
対象バージョン	1.01.01

使用例：スタティック認証エントリー「MAC アドレス=00:01:00:00:00:01、VLAN ID=10、クラス ID=1、ポート 1/0/1 に接続」を登録する方法を示します。

```
# configure terminal
(config)# access-defender static mac 00:01:00:00:00:01 vlan 10 class 1 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。

logout aging-time	
シンタックス	**logout aging-time** *SECONDS* [*MINUTES* [*HOURS* [*DAYS*]]] {**web** | **gateway** | **mac** | **dot1x**} **no logout aging-time** [**web** | **gateway** | **mac** | **dot1x**]
パラメーター	*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 秒の範囲で指定します。 • *MINUTES*（省略可能）：0～59 分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。 • *DAYS*（省略可能）：0～31 日の範囲で指定します。 **web**：Web 認証のクライアントを対象にする場合に指定します。 **gateway**：ゲートウェイ認証のクライアントを対象にする場合に指定します。 **mac**：MAC 認証のクライアントを対象にする場合に指定します。 **dot1x**：IEEE 802.1X 認証のクライアントを対象にする場合に指定します。
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）
コマンドモード	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されます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：Web 認証の認証済みクライアント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。
シンタックス	**logout timeout** *SECONDS* [*MINUTES* [*HOURS* [*DAYS*]]] {**web** | **gateway** | **mac** | **dot1x**} **no logout timeout** [**web** | **gateway** | **mac** | **dot1x**]

logout timeout	
パラメーター	*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 秒の範囲で指定します。 • *MINUTES*（省略可能）：0～59 分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。 • *DAYS*（省略可能）：0～31 日の範囲で指定します。 **web**：Web 認証のクライアントを対象にする場合に指定します。 **gateway**：ゲートウェイ認証のクライアントを対象にする場合に指定します。 **mac**：MAC 認証のクライアントを対象にする場合に指定します。 **dot1x**：IEEE 802.1X 認証のクライアントを対象にする場合に指定します。
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）
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	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されます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：Web 認証の認証済みクライアント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。
シンタックス	**logout clock** *HH:MM* {**web** | **gateway** | **mac** | **dot1x**} **no logout clock** [**web** | **gateway** | **mac** | **dot1x**]
パラメーター	*HH:MM*：ログアウト時刻を 時:分 形式で指定します。「時」は 24 時間表記で指定します。 **web**：Web 認証のクライアントを対象にする場合に指定します。 **gateway**：ゲートウェイ認証のクライアントを対象にする場合に指定します。 **mac**：MAC 認証のクライアントを対象にする場合に指定します。

logout clock	
	dot1x：IEEE 802.1X 認証のクライアントを対象にする場合に指定します。
デフォルト	無効
コマンドモード	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されます。 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：Web 認証の認証済みクライアントの指定時刻ログアウトを、18:00 に設定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。
シンタックス	**logout ping dst-ip** {*IP-ADDRESS* | *IPV6-ADDRESS*} **no logout ping dst-ip**
パラメーター	*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
コマンドモード	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 パケットを受信すると、その認証済みクライアントはログアウトされます。
制限事項	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、IPv4 アドレスと IPv6 アドレスを 1 個ずつ指定できます。
注意事項	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されます。
対象バージョン	1.01.03

使用例：宛先 IPv4 アドレスが 192.168.1.254 の 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 192.168.1.254
```

```
(config-a-def)#
```

使用例：宛先 IPv6 アドレスが 2001::2001 の 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::2001
(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。
シンタックス	**logout ping ttl** *VALUE* **no logout ping ttl**
パラメーター	*VALUE*：TTL 値を 1～255 の範囲で指定します。
デフォルト	無効
コマンドモード	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 パケットを受信すると、その認証済みクライアントはログアウトされます。
制限事項	Web 認証、ゲートウェイ認証でのみ有効です。 TTL 値は、1 件だけ指定できます。
注意事項	本コマンドと **logout ping dst-ip** コマンドを併用した場合は、IPv4 ping パケットが 2 つの条件を満たしたときのみ、認証済みクライアントがログアウトされます。
対象バージョン	1.01.03

使用例：TTL 値=1 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。
シンタックス	**logout linkdown disable interface** *INTERFACE-ID* [,|-] **no logout linkdown disable interface** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：認証ポートのリンクダウンによるログアウトを無効に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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
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**）
コマンドモード	AccessDefender 設定モード

logout linkdown disable interface	
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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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)#
```

使用例：ポートチャネル 1 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-channel 1
(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。
シンタックス	**logout linkdown time** *SECONDS* **no logout linkdown time**
パラメーター	*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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**logout linkdown time enable interface** *INTERFACE-ID* [,|-] **no logout linkdown time enable interface** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：リンクダウン監視時間を有効に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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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)#
```

使用例：ポートチャネル 1 のリンクダウンを監視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)# logout linkdown time enable interface port-channel 1
(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。
シンタックス	**roaming enable interface** *INTERFACE-ID* [,|-] **no roaming enable interface** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：ローミング機能を有効に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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。

roaming enable interface	
デフォルト	無効
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 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)#
```

使用例：ポートチャネル 1 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-channel 1
(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。
シンタックス	**authentication {web-mac ｜ dot1x-mac ｜ web-dot1x ｜ web-dot1x-mac} prefer-attribute {web ｜ dot1x ｜ mac}** **no authentication {web-mac ｜ dot1x-mac ｜ web-dot1x ｜ web-dot1x-mac} prefer-attribute**
パラメーター	**web-mac**：Web/MAC 認証(AND)を設定する場合に指定します。 **dot1x-mac**：IEEE 802.1X/MAC 認証(AND)を設定する場合に指定します。 **web-dot1x**：Web/IEEE 802.1X 認証(AND)を設定する場合に指定します。 **web-dot1x-mac**：Web/IEEE 802.1X/MAC 認証(AND)を設定する場合に指定します。 **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。 • **web**：Web 認証で取得した認証属性を適用します。 • **dot1x**：IEEE 802.1X 認証で取得した認証属性を適用します。 • **mac**：MAC 認証で取得した認証属性を適用します。
デフォルト	なし
コマンドモード	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/ログアウト成功時に出力されるアカウンティング情報のユーザー名
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	authentication {web-mac | web-dot1x} advanced-vlan-setting no authentication {web-mac | web-dot1x} advanced-vlan-setting
パラメーター	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
コマンドモード	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。 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。
制限事項	-
注意事項	-
対象バージョン	1.04.01

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 authentication web-mac abort-if-failure

authentication web-mac abort-if-failure	
目的	Web/MAC 認証(AND)において、MAC 認証処理で認証に失敗したクライアントに対して、Web 認証ページを応答しないよう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。
シンタックス	authentication web-mac abort-if-failure no authentication web-mac abort-if-failure
パラメーター	なし
デフォルト	Web 認証ページを応答しないようにする機能は無効（no authentication web-mac abort-if-failure）
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	本機能は、Web/MAC 認証(AND)と MAC 認証の併用ポートでは動作しません。

authentication web-mac abort-if-failure	
注意事項	-
対象バージョン	1.09.01

使用例：Web/MAC 認証(AND)において、MAC 認証処理で認証に失敗したクライアントに対して、Web 認証ページを応答しないように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)# authentication web-mac abort-if-failure
(config-a-def)#
```

9.1.18 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。
シンタックス	**max-client** *NUMBER* **interface** *INTERFACE-ID* [,|-] **no max-client interface** *INTERFACE-ID* [,|-]
パラメーター	*NUMBER*：認証可能なクライアントの最大数を、1～768 の範囲で指定します。 *INTERFACE-ID*：認証可能なクライアントの最大数を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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

使用例：ポートチャネル 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-channel 1
(config-a-def)#
```

9.1.19 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。
シンタックス	**max-discard** *NUMBER*

max-discard	
	no max-discard
パラメーター	*NUMBER*：Discard 登録されるクライアントの最大数を、100～200 の範囲で指定します。
デフォルト	200
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.03.01

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)#
```

9.1.20 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。
シンタックス	**vlan mode {dynamic port-base | static}** **no vlan mode**
パラメーター	**dynamic port-base**：AccessDefender の VLAN モードを dynamic port-base モードに設定する場合に指定します。 **static**：AccessDefender の VLAN モードを static モードに設定する場合に指定します。
デフォルト	無効
コマンドモード	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。dynamic port-base モードの場合の動作を以下に示します。

ログイン中の端末	後から認証を行う端末	ログイン可否
装置に設定済みの VLAN	VLAN 指定なし	可
	VLAN 指定あり（ログイン中の端末と同じ VLAN）	可
	VLAN 指定あり（ログイン中の端末と異なる VLAN）	不可
装置に設定済みの VLAN と異なる VLAN	VLAN 指定なし	不可
	VLAN 指定あり（ログイン中の端末と同じ VLAN）	可
	VLAN 指定あり（ログイン中の	不可

vlan mode	
	端末と異なる VLAN)
	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。 本コマンドの設定は、**access-defender static mac** コマンドの設定に影響しません。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

9.1.21 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。
シンタックス	**radius-server attribute mac-format case {lowercase | uppercase} delimiter {{hyphen | colon | dot} number {1 | 2 | 5} | none}** **no radius-server attribute mac-format**
パラメーター	**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） • **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）
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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)#
```

9.1.22 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。
シンタックス	show access-defender aaa-local-db
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

9.1.23 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。
シンタックス	show access-defender client [interface *INTERFACE-ID* [,|-]] [type {dhcp-snooping | disc | dot1x | gateway | mac | static | web}]
パラメーター	interface *INTERFACE-ID*（省略可能）：クライアントの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。

show access-defender client	
	• **port**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。 **type**（省略可能）：限定して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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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           :    4 ...(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

G   N/A               2000:adb8:85a3:85a2:aba3:8a2e:a370:7334  1/0/5*4094   10
webuser02                                                            5d1hr 0:00:24

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。

項番	説明
(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 時間より短い場合には、(時):(分):(秒) という形式で表示され、10 時間以上の場合には、(日)d(時)hr という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 時間より短い場合には、(時):(分):(秒) という形式で表示され、10 時間以上の場合には、(日)d(時)hr という形式で表示されます。

9.1.24 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。
シンタックス	show access-defender deny
パラメーター	なし
デフォルト	なし
コマンドモード	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	－
制限事項	－
注意事項	－
対象バージョン	1.01.01

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    :   3 ...(1)
(2)                 (3)                                    (4)
MAC address         IP                                     Timer
-----------------------------------------------------------------------
```

```
00-00-11-11-22-22 -                                      0:29:04
-                 100.100.100.100                        0:29:04
-                 1111:2222:3333:4444:5555:6666:7777:8888 0:29:05
```

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。

9.1.25 show access-defender port-configuration

show access-defender port-configuration	
目的	ポートの AccessDefender の設定を表示します。
シンタックス	**show access-defender port-configuration**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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     16 17    24 25
           +------+ +------+ +------+ +---
mac      1 ........ oooo.... oooooooo ....
802.1X   1 ........ ........ oooooooo ....
web      1 oooooooo ........ oooooooo ....
gateway  1 ........ ........ ........ oo..
web/mac  1 ........ ......oo ........ ....
web/.1X  1 ........ ....oo.. ........ ....
.1X/mac  1 ........ ........ ........ ....
w/.1X/m  1 ........ ........ ........ ....
DHCPSNP  1 ........ ........ ........ ....
roaming  1 ........ oooooooo ........ ....
static   1 ........ ........ ........ ....
linkdown 1 xxxxxxxx xxxxxxxx ........ ....
ld time  1 ........ ........ oooooooo ....
```

```
TTL       1 oooooooo ........ ........ ....
```

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。

9.1.26 show access-defender port-channel-configuration

show access-defender port-channel-configuration	
目的	ポートチャネルの AccessDefender の設定を表示します。
シンタックス	show access-defender port-channel-configuration
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 xxxxxxx.. ........ ........ ........ ........ ........
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。

9.1.27 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。
シンタックス	show access-defender rule-statistics
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
(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。

9.1.28 copy (AccessDefender)

copy (AccessDefender)	
目的	TFTP 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。
シンタックス	**copy** {**flash:** [*URL*] | **tftp:** [*URL*]} {*SYSTEM-FILE1* | **webpages** *WEBPAGES-ID SYSTEM-FILE2*} **copy** {*SYSTEM-FILE1* | **webpages** *WEBPAGES-ID SYSTEM-FILE2*} {**flash:** [*URL*] | **tftp:** [*URL*]}
パラメーター	**flash:**：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。 **tftp:**：TFTP を使用する場合に指定します。

copy (AccessDefender)	
	URL：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の URL を指定します。以下のいずれかの書式を使用します。 • **flash: c:/***URL*：装置のローカルフラッシュ上のファイルを指定します。例えば、c:/custom_login-page.html と入力します。 • **flash: d:/***URL*：SD カード上のファイルを指定します。例えば、d:/custom_login-page.html と入力します。 • **tftp:** [//*IP-ADDRESS*/[*DIRECTORY*/]*FILE-NAME*]：TFTP サーバー上のファイルを指定します。 　• *IP-ADDRESS*：TFTP サーバーの IP アドレスを指定します。 　• *DIRECTORY*（省略可能）：ディレクトリー名を指定します。 　• *FILE-NAME*：ダウンロード元ファイル名、またはアップロード先ファイル名を指定します。 *SYSTEM-FILE1*：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**：Web ページの画像 01 • **webpage-image02**：Web ページの画像 02 • **webpage-image03**：Web ページの画像 03 • **webpage-image04**：Web ページの画像 04 • **webpage-image05**：Web ページの画像 05 • **webpage-image06**：Web ページの画像 06 • **webpage-image07**：Web ページの画像 07 • **webpage-image08**：Web ページの画像 08 • **webpage-image09**：Web ページの画像 09 • **webpage-image10**：Web ページの画像 10 **webpages** *WEBPAGES-ID SYSTEM-FILE2*：個別 Web 認証ページ ID を 1～30 の範囲で指定します。また、個別 Web 認証ページで使用する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
デフォルト	なし
コマンドモード	特権実行モード

<table>
<tr><th colspan="2">copy (AccessDefender)</th></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。

ログイン認証ページ、認証成功ページ、認証失敗ページ、ログアウト成功ページ、ログアウト失敗ページ、およびリダイレクト失敗ページは、以下のとおりカスタマイズできます。
<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</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。
• 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

ユーザー名、パスワード、VLAN ID、クラス ID を指定する方法を示します。
<pre>temp01,temp01,10
temp02,temp02
temp03,temp03,,30
00096b82c51e,1q2w3d,100,10
01010102,*@&foe2zgl6pwJiXjVe0+amVwAAAAC+RzmF,1002,1002,*</pre>
ダウンロードした SSL サーバー証明書と秘密鍵は直ちに反映されます。

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。

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 行目のようにカンマ（,）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カンマおよびアスタリスク（,*）が追加されます。
</td></tr>
</table>

copy (AccessDefender)	
	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、**csr-certificate** パラメーターおよび **csr-privatekey** パラメーターを指定した場合のみ 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。 個別 Web 認証ページ： • 個別 Web 認証ページは、インターフェースごとに認証ページをカスタマイズする場合に使用します。適用する個別 Web 認証ページ ID は **web-authentication interface** コマンドで指定します。 • デフォルトでは個別 Web 認証ページは装置に保存されていません。 • 装置にダウンロードした個別 Web 認証ページは、先頭に個別 Web 認証ページ ID が付与されたファイル名で保存されます。（例：01-login-page, 01-login-success-page） • 装置に保存した個別 Web 認証ページは、**access-defender erase** コマンドで削除できます。 • すでに個別 Web 認証ページが存在する状態で再度ダウンロードした場合は、上書きされます。
制限事項	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。
注意事項	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

copy (AccessDefender)	
	せん。 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。
対象バージョン	1.01.03 1.03.01 : **webpage-image01** ～ **webpage-image10**, **csr-certificate**, **csr-private-key** パラメーター追加 1.09.01 : **webpages** 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「login-success-page.html」ファイルを認証成功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/login-success-page.html login-success-page

Address of remote host [192.168.1.110]?
Source filename [login-success-page.html]?
Destination filename login-success-page? [y/n]:  y

 Accessing tftp://192.168.1.110/login-success-page.html...
 Transmission start...
 Transmission finished, file length 1,336 bytes.
 Please wait, programming flash............. Done.
```

使用例：SD カードから「login-success-page.html」ファイルを認証成功ページとしてダウンロードする方法を示します。

```
# copy flash: d:/login-success-page.html login-success-page

Source filename [d:/login-success-page.html]?
Destination filename login-success-page? [y/n]:  y

 Copy in progress........................... 100 %
```

使用例：IP アドレス 192.168.1.110 の TFTP サーバーから「local-db.txt」ファイルを AccessDefender のローカルデータベースファイルとしてダウンロードする方法を示します。

```
# copy tftp: //192.168.1.110/local-db.txt aaa-local-db

Address of remote host [192.168.1.110]?
Source filename [local-db.txt]?
Destination filename aaa-local-db? [y/n]:  y

 Accessing tftp://192.168.1.110/local-db.txt...
 Transmission start...
 Transmission finished, file length 259,973 bytes.
 Set aaa DB success.
```

使用例：SD カードから「local-db.txt」ファイルを AccessDefender のローカルデータベースファイルとしてダウンロードする方法を示します。

```
# copy flash: d:/local-db.txt 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：IP アドレス 192.168.1.110 の TFTP サーバーから「key.prv」という名前の秘密鍵ファイルをダウンロードする方法を示します。

```
# copy tftp: //192.168.1.110/key.prv https-private-key

Address of remote host [192.168.1.110]?
Source filename [key.prv]?
Destination filename https-privatekey? [y/n]:  y

% Importing private key PEM file...
Reading file from tftp://192.168.1.110/key.prv
Loading key.prv from 192.168.1.110 (via Port1/0/24):!
[OK - 1675 bytes]
```

使用例：IP アドレス 192.168.1.110 の TFTP サーバーから「cert.crt」という名前の SSL サーバー証明書をダウンロードする方法を示します。

```
# copy tftp: //192.168.1.110/cert.crt https-certificate

Address of remote host [192.168.1.110]?
Source filename [cert.crt]?
Destination filename https-certificate? [y/n]:  y

% Importing certificate PEM file...
Reading file from tftp://192.168.1.110/cert.crt
Loading cert.crt from 192.168.1.110 (via Port1/0/24):!
[OK - 1403 bytes]
```

使用例：IP アドレス 192.168.1.110 の TFTP サーバーに「aaa-local-db」ファイルをアップロードして、ファイル名を「local-db.txt」に変更する方法を示します。

```
# copy aaa-local-db tftp: //192.168.1.110/local-db.txt

Address of remote host [192.168.1.110]?
Destination filename [local-db.txt]?

 Uploading aaa-local-db to tftp://192.168.1.110/local-db.txt...
 Transmission start...
 Transmission finished, file length 259,973 bytes.
```

9.1.29 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。
シンタックス	**access-defender deny** {**ip** {*IP-ADDRESS* | *IPV6-ADDRESS*} | **mac** *MAC-ADDRESS*} **timer** *MINUTES* **no access-defender deny** {**ip** {*IP-ADDRESS* | *IPV6-ADDRESS*} | **mac** *MAC-ADDRESS*}
パラメーター	**ip**：認証を一時的に拒否するクライアントの IP アドレスを指定します。 • *IP-ADDRESS*：IPv4 アドレスを指定します。 • *IPV6-ADDRESS*：IPv6 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。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式）

access-defender deny	
	• XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式） 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。
デフォルト	なし
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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
```

使用例：IPv6 アドレスが 2001::2001 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 2001::2001 timer 10
```

9.1.30 access-defender erase

access-defender erase	
目的	AccessDefender のシステムファイルを削除します。
シンタックス	access-defender erase [*SYSTEM-FILE* | webpages *WEBPAGES-ID*]
パラメーター	*SYSTEM-FILE*（省略可能）：削除するシステムファイルを指定します。以下のいずれかを指定してください。 • login-page：ログイン認証ページを削除します。 • login-success-page：認証成功ページを削除します。 • login-failure-page：認証失敗ページを削除します。 • logout-success-page：ログアウト成功ページを削除します。 • logout-failure-page：ログアウト失敗ページを削除します。 • redirect-error-page：リダイレクト失敗ページを削除します。 • aaa-local-db：AccessDefender のローカルデータベースを削除します。 • 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を削除します。 • webpage-image01：Web ページの画像 01 を削除します。 • webpage-image02：Web ページの画像 02 を削除します。 • webpage-image03：Web ページの画像 03 を削除します。 • webpage-image04：Web ページの画像 04 を削除します。 • webpage-image05：Web ページの画像 05 を削除します。 • webpage-image06：Web ページの画像 06 を削除します。 • webpage-image07：Web ページの画像 07 を削除します。 • webpage-image08：Web ページの画像 08 を削除します。 • webpage-image09：Web ページの画像 09 を削除します。

access-defender erase	
	• **webpage-image10**：Web ページの画像 10 を削除します。 **webpages** *WEBPAGES-ID*（省略可能）：削除する個別 Web 認証ページ ID を 1～30 の範囲で指定します。
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.03 1.03.01：**webpage-image01**～**webpage-image10** パラメーター追加 1.09.01：**webpages** パラメーター追加

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.
Erasing Web authentication webpages 1 in FLASH.......... Done.
Erasing Web authentication webpages 2 in FLASH.......... Done.
Erasing Web authentication webpages 3 in FLASH.......... Done.
Erasing Web authentication webpages 4 in FLASH.......... Done.
Erasing Web authentication webpages 5 in FLASH.......... Done.
～～省略～～
```

9.1.31 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

access-defender logout	
	録されたクライアントを手動で削除します。
シンタックス	**access-defender logout** {**ip** {*IP-ADDRESS* | *IPV6-ADDRESS*} | **mac** *MAC-ADDRESS* | **user** *USER-ID*}
パラメーター	**ip**：強制的にログアウトする認証済みクライアントの IP アドレスを指定します。 • *IP-ADDRESS*：IPv4 アドレスを指定します。 • *IPV6-ADDRESS*：IPv6 アドレスを指定します。 **mac** *MAC-ADDRESS*：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。 • XX-XX-XX-XX-XX-XX（1 バイトごとにハイフン"-"で区切る形式） • XX:XX:XX:XX:XX:XX（1 バイトごとにコロン":"で区切る形式） • XXXX.XXXX.XXXX（2 バイトごとにドット"."で区切る形式） • XXXXXXXXXXXX（区切り文字を使用しない形式） **user** *USER-ID*：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。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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：IPv6 アドレスが 2001::2001 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 2001::2001
```

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
```

9.2 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。

コマンド	コマンドとパラメーター
aaa new-model	aaa new-model no aaa new-model
radius-server host	radius-server host {IP-ADDRESS | IPV6-ADDRESS} [auth-port UDP-PORT] [acct-port UDP-PORT] [timeout SECONDS] [retransmit COUNT] key [0 | 7] KEY-STRING no radius-server host {IP-ADDRESS | IPV6-ADDRESS}
radius-server deadtime	radius-server deadtime MINUTES no radius-server deadtime
tacacs-server host	tacacs-server host IP-ADDRESS [port TCP-PORT] [timeout SECONDS] key [0 | 7] KEY-STRING no tacacs-server host IP-ADDRESS
ip radius source-interface	ip radius source-interface INTERFACE-ID no ip radius source-interface
ip tacacs source-interface	ip tacacs source-interface INTERFACE-ID no ip tacacs source-interface
ipv6 radius source-interface	ipv6 radius source-interface INTERFACE-ID no ipv6 radius source-interface
aaa group server radius	aaa group server radius GROUP-NAME no aaa group server radius GROUP-NAME
server (RADIUS)	server {IP-ADDRESS | IPV6-ADDRESS} no server {IP-ADDRESS| IPV6-ADDRESS}
aaa group server tacacs+	aaa group server tacacs+ GROUP-NAME no aaa group server tacacs+ GROUP-NAME
server (TACACS+)	server IP-ADDRESS no server IP-ADDRESS
aaa authentication login	aaa authentication login {default | LIST-NAME} METHOD1 [METHOD2...] no aaa authentication login {default | LIST-NAME}
login authentication	login authentication {default | METHOD-LIST} no login authentication
aaa authentication enable	aaa authentication enable default METHOD1 [METHOD2...] no aaa authentication enable default
aaa authentication mac-auth	aaa authentication mac-auth default METHOD1 [METHOD2...] [interface INTERFACE-ID [,|-]] no aaa authentication mac-auth default [interface INTERFACE-ID [,|-]]
aaa authentication dot1x	aaa authentication dot1x default METHOD1 [METHOD2...] no aaa authentication dot1x default

コマンド	コマンドとパラメーター
aaa authentication web-auth	aaa authentication web-auth ID default METHOD1 [METHOD2...] [interface INTERFACE-ID [,|-]] no aaa authentication web-auth ID default [interface INTERFACE-ID [,|-]]
aaa authentication control sufficient	aaa authentication control sufficient {web ID | mac | login} no aaa authentication control sufficient {web ID | mac | login}
aaa default class	aaa default class CLASS-ID no aaa default class
aaa accounting system	aaa accounting system default {none | start-stop METHOD1 [METHOD2...]} no aaa accounting system default
aaa accounting network	aaa accounting network default {none | start-stop METHOD1 [METHOD2...]} no aaa accounting network default
aaa accounting commands	aaa accounting commands LEVEL {default | LIST-NAME} {none | start-stop METHOD1 [METHOD2...]} no aaa accounting commands LEVEL {default | LIST-NAME}
accounting commands	accounting commands LEVEL {default | METHOD-LIST} no accounting commands LEVEL
aaa accounting exec	aaa accounting exec {default | LIST-NAME} {none | start-stop METHOD1 [METHOD2...]} no aaa accounting exec {default | LIST-NAME}
accounting exec	accounting exec {default | METHOD-LIST} no 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。

コマンド	コマンドとパラメーター
show aaa	show aaa
show radius statistics	show radius statistics
show tacacs statistics	show tacacs statistics
clear aaa counters servers	clear aaa counters servers {all | radius {IP-ADDRESS | IPV6-ADDRESS | all} | tacacs {IP-ADDRESS | all} | sg NAME}

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。
シンタックス	aaa new-model no aaa new-model
パラメーター	なし
デフォルト	無効

aaa new-model	
コマンドモード	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	認証の前に AAA を有効化し、アカウンティングで使用する AAA 認証方式リストを有効にするコマンドです。AAA が無効になっている場合、ログインユーザーは、**username** コマンドで作成したローカルユーザーアカウントテーブルによって認証されます。有効化された password は、**enable password** コマンドを実行して定義されたローカルテーブルによって認証されます。
制限事項	-
注意事項	本コマンドを設定するとコンソールポートを除く、すべてのラインセッションでログイン認証が有効となります。そのため、コンソールポート以外を利用して装置にログインする場合は、本コマンドを設定する前に **username** コマンドでユーザー名とパスワードを設定してください。
対象バージョン	1.01.01

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。
シンタックス	**radius-server host** {*IP-ADDRESS* | *IPV6-ADDRESS*} [**auth-port** *UDP-PORT*] [**acct-port** *UDP-PORT*] [**timeout** *SECONDS*] [**retransmit** *COUNT*] **key** [0 | 7] *KEY-STRING* **no radius-server host** {*IP-ADDRESS* | *IPV6-ADDRESS*}
パラメーター	*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。 **retransmit** *COUNT*（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**：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。

radius-server host	
デフォルト	RADIUS サーバーの設定なし
コマンドモード	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。 • Longest prefix match 規則に従ってデフォルトルート情報(0.0.0.0/0)よりも優先されるような、RADIUS サーバー(IPv4)への、よりプレフィックス長の長いルート情報（スタティックルート） • **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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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	RADIUS サーバーから応答がない場合に RADIUS サーバーをオフラインとみなすまでの期間（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。

radius-server deadtime	
シンタックス	**radius-server deadtime** *MINUTES* **no radius-server deadtime**
パラメーター	*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。0 を指定した場合、応答のない RADIUS サーバーに dead マークは設定されません。
デフォルト	0
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**tacacs-server host** *IP-ADDRESS* [**port** *TCP-PORT*] [**timeout** *SECONDS*] **key** [**0** | **7**] *KEY-STRING* **no tacacs-server host** *IP-ADDRESS*
パラメーター	*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**：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** *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

tacacs-server host	
コマンドモード	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。 • Longest prefix match 規則に従ってデフォルトルート情報(0.0.0.0/0)よりも優先されるような、TACACS+サーバーへの、よりプレフィックス長の長いルート情報（スタティックルート） • 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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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 アドレスに使用するインターフェースを指定します。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。
シンタックス	ip radius source-interface *INTERFACE-ID* no ip radius source-interface
パラメーター	*INTERFACE-ID*：RADIUS パケットの送信元 IPv4 アドレスに使用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。 • vlan：VLAN インターフェースを指定します。
デフォルト	RADIUS サーバーに最も近い IPv4 アドレスを使用
コマンドモード	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

ip radius source-interface	
	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.03

使用例：グローバル設定モードで、RADIUS パケットの送信元 IPv4 アドレスに VLAN 100 インターフェースの IPv4 アドレスを指定する方法を示します。

```
# configure terminal
(config)# ip radius source-interface vlan 100
(config)#
```

9.2.6 ip tacacs source-interface

ip tacacs source-interface	
目的	TACACS+パケットの送信元 IPv4 アドレスに使用するインターフェースを指定します。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。
シンタックス	**ip tacacs source-interface** *INTERFACE-ID* **no ip tacacs source-interface**
パラメーター	*INTERFACE-ID*：TACACS+パケットの送信元 IPv4 アドレスに使用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。 • **vlan**：VLAN インターフェースを指定します。
デフォルト	TACACS+サーバーに最も近い IPv4 アドレスを使用
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：グローバル設定モードで、TACACS+パケットの送信元 IPv4 アドレスに VLAN 100 インターフェースの IPv4 アドレスを指定する方法を示します。

```
# configure terminal
(config)# ip tacacs source-interface vlan 100
(config)#
```

9.2.7 ipv6 radius source-interface

ipv6 radius source-interface	
目的	RADIUS パケットの送信元 IPv6 アドレスに使用するインターフェースを指定します。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。
シンタックス	**ipv6 radius source-interface** *INTERFACE-ID* **no ipv6 radius source-interface**
パラメーター	*INTERFACE-ID*：RADIUS パケットの送信元 IPv6 アドレスに使用するインター

ipv6 radius source-interface	
	フェースを、以下のパラメーターで指定します。 • **vlan**：VLAN インターフェースを指定します。
デフォルト	RADIUS サーバーに最も近い IPv6 アドレスを使用
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.03

使用例：グローバル設定モードで、RADIUS パケットの送信元 IPv6 アドレスに VLAN 100 インターフェースの IPv6 アドレスを指定する方法を示します。

```
# configure terminal
(config)# ipv6 radius source-interface vlan 100
(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。
シンタックス	**aaa group server radius** *GROUP-NAME* **no aaa group server radius** *GROUP-NAME*
パラメーター	*GROUP-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
コマンドモード	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。 「radius」というグループ名はデフォルトの 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

aaa group server radius	
	れている 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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**server** {*IP-ADDRESS* | *IPV6-ADDRESS*} **no server** {*IP-ADDRESS*| *IPV6-ADDRESS*}
パラメーター	*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
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**aaa group server tacacs+** *GROUP-NAME* **no aaa group server tacacs+** *GROUP-NAME*
パラメーター	*GROUP-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
コマンドモード	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。 「tacacs+」というグループ名はデフォルトの 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。
制限事項	-

aaa group server tacacs+	
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**server** *IP-ADDRESS* **no server** *IP-ADDRESS*
パラメーター	*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
コマンドモード	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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	aaa authentication login {default | *LIST-NAME*} *METHOD1* [*METHOD2...*] no aaa authentication login {default | *LIST-NAME*}
パラメーター	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認証アルゴリズムを試行する認証方式のリストを指定します。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。認証方式には、以下のパラメーターを指定できます。 • local：username コマンドで作成したユーザーアカウントで認証する場合に指定します。 • group radius：radius-server host コマンドで設定した RADIUS サーバーを対象にする場合に、デフォルトの RADIUS サーバーグループ「radius」を指定します。 • group tacacs+：tacacs-server host コマンドで設定した TACACS+サーバーを対象にする場合に、デフォルトの TACACS+サーバーグループ「tacacs+」を指定します。 • group *GROUP-NAME*：aaa group server コマンドで設定したサーバーグループを使用する場合に指定します。 • none：認証なしで許可する場合に指定します。
デフォルト	local
コマンドモード	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。

aaa authentication login	
	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**login authentication** {**default** | *METHOD-LIST*} **no login authentication**
パラメーター	**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。 *METHOD-LIST*：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
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：ローカルコンソールのラインで「CONSOLE-LINE-METHOD」という認証方式リストをログイン認証に使用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。
シンタックス	**aaa authentication enable default** *METHOD1* [*METHOD2...*]

aaa authentication enable	
	no aaa authentication enable default
パラメーター	*METHOD1* [*METHOD2...*]：ここで指定した順序で認証アルゴリズムを試行する認証方式のリストを指定します。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。認証方式には、以下のパラメーターを指定できます。 • enable：enable password コマンドで設定したパスワードで認証する場合に指定します。 • group radius：radius-server host コマンドで設定した RADIUS サーバーを対象にする場合に、デフォルトの RADIUS サーバーグループ「radius」を指定します。 • group tacacs+：tacacs-server host コマンドで設定した TACACS+サーバーを対象にする場合に、デフォルトの TACACS+サーバーグループ「tacacs+」を指定します。 • group *GROUP-NAME*：aaa group server コマンドで設定したサーバーグループを使用する場合に指定します。 • none：認証なしで許可する場合に指定します。
デフォルト	enable
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	aaa authentication mac-auth default *METHOD1* [*METHOD2...*] [interface *INTERFACE-ID* [,|-]] no aaa authentication mac-auth default [interface *INTERFACE-ID* [,|-]]
パラメーター	*METHOD1* [*METHOD2...*]：ここで指定した順序で認証アルゴリズムを試行する認証方式のリストを指定します。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。認証方式には、以下のパラメーターを指定できます。 • local：AccessDefender のローカルデータベースで認証する場合に指定します。 • group radius：radius-server host コマンドで設定した RADIUS サーバーを対象にする場合に、デフォルトの RADIUS サーバーグループ「radius」を指定します。 • group *GROUP-NAME*：aaa group server コマンドで設定したサーバーグループを使用する場合に指定します。 • force [vlan *VLAN-ID*]：強制的に認証する場合に指定します。認証後に変更する VLAN ID も指定できます。VLAN ID は 1～4094 の範囲で指定します。 interface *INTERFACE-ID*（省略可能）：対象の認証方式を適用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：物理ポートを指定します。複数指定できます。 • port-channel：ポートチャネルを指定します。
デフォルト	local
コマンドモード	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	interface パラメーターを省略した設定は装置全体で有効です。また、認証方式をインターフェースごとに設定する場合は interface パラメーターを指定します。両方を設定していて両方にマッチする場合は、interface パラメーターを指定した設定が優先されます。 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 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 認証でサポートしている RADIUS 属性は以下です。

aaa authentication mac-auth	
	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。
制限事項	認証方式として、TACACS+サーバーグループは指定できません。
注意事項	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。
対象バージョン	1.01.01 1.09.01：**interface** パラメーター追加

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。
シンタックス	**aaa authentication dot1x default** *METHOD1* [*METHOD2...*] **no aaa authentication dot1x default**
パラメーター	*METHOD1* [*METHOD2...*]：ここで指定した順序で認証アルゴリズムを試行する認証方式のリストを指定します。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。認証方式には、以下のパラメーターを指定できます。 • **local**：AccessDefender のローカルデータベースで認証する場合に指定します。 • **group radius**：**radius-server host** コマンドで設定した RADIUS サーバーを対象にする場合に、デフォルトの RADIUS サーバーグループ「radius」を指定します。 • **group** *GROUP-NAME*：**aaa group server** コマンドで設定したサーバーグループを使用する場合に指定します。 • **force** [**vlan** *VLAN-ID*]：強制的に認証する場合に指定します。認証後に変更する VLAN ID も指定できます。VLAN ID は 1～4094 の範囲で指定します。

<table>
<tr><th colspan="2">aaa authentication dot1x</th></tr>
<tr><td>デフォルト</td><td>local</td></tr>
<tr><td>コマンドモード</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。

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 認証でサポートしている 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>NAS-IP-Address</td><td>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)</td></tr>
<tr><td>Framed-MTU</td><td>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)</td></tr>
<tr><td>NAS-Port</td><td>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</td></tr>
<tr><td>NAS-Port-Type</td><td>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)</td></tr>
<tr><td>Service-Type</td><td>提供するサービスタイプ(Framed(2)固定)</td></tr>
<tr><td>Calling-Station-Id</td><td>サプリカントの MAC アドレス</td></tr>
<tr><td>EAP-Message</td><td>EAP メッセージの送受信に使用</td></tr>
<tr><td>Message-Authenticator</td><td>RADIUS パケットの内容を保証するために使用</td></tr>
<tr><td>State</td><td>オーセンティケーターと RADIUS サーバー間の State 情報の保持</td></tr>
<tr><td>Tunnel-Type</td><td>動的 VLAN 割り当て用応答属性(VLAN(13)に設定)</td></tr>
<tr><td>Tunnel-Medium-Type</td><td>動的 VLAN 割り当て用応答属性(IEEE 802(6)に設定)</td></tr>
<tr><td>Tunnel-Private-Group-Id</td><td>動的 VLAN 割り当て用応答属性(割り当てる VLAN ID、または VLAN 名称)</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>制限事項</td><td>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。</td></tr>
<tr><td>注意事項</td><td>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。</td></tr>
<tr><td>対象バージョン</td><td>1.01.03</td></tr>
</table>

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。
シンタックス	**aaa authentication web-auth** *ID* **default** *METHOD1* [*METHOD2...*] [**interface** *INTERFACE-ID* [,|-]] **no aaa authentication web-auth** *ID* **default** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	*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認証アルゴリズムを試行する認証方式のリストを指定します。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。認証方式には、以下のパラメーターを指定できます。 • **local**：AccessDefender のローカルデータベースで認証する場合に指定します。 • **group radius**：**radius-server host** コマンドで設定した RADIUS サーバーを対象にする場合に、デフォルトの RADIUS サーバーグループ「radius」を指定します。 • **group** *GROUP-NAME*：**aaa group server** コマンドで設定したサーバーグループを使用する場合に指定します。 • **force** [**vlan** *VLAN-ID*]：強制的に認証する場合に指定します。認証後に変更する VLAN ID も指定できます。VLAN ID は 1～4094 の範囲で指定します。 **interface** *INTERFACE-ID*（省略可能）：対象の認証方式を適用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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	local
コマンドモード	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	**interface** パラメーターを省略した設定は装置全体で有効です。また、認証方式をインターフェースごとに設定する場合は **interface** パラメーターを指定します。両方を設定していて両方にマッチする場合は、**interface** パラメーターを指定した設定が優先されます。 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 web** コマンドが有効に設定されている場合

aaa authentication web-auth	
	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 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 認証でサポートしている 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。
制限事項	認証方式として、TACACS+サーバーグループは指定できません。
注意事項	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。
対象バージョン	1.01.03 1.09.01 : interface パラメーター追加

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	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。
シンタックス	aaa authentication control sufficient {web *ID* | mac | login} no aaa authentication control sufficient {web *ID* | mac | login}
パラメーター	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
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：Web 認証 ID 1 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。
シンタックス	aaa default class *CLASS-ID* no aaa default class
パラメーター	*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。
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**aaa accounting system default** {**none** | **start-stop** *METHOD1* [*METHOD2...*]} **no aaa accounting system default**
パラメーター	**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アカウンティングアルゴリズムを試行する方式のリストを指定します。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。アカウンティング方式には、以下のパラメーターを指定できます。 • **group radius**：**radius-server host** コマンドで設定した RADIUS サーバーを対象にする場合に、デフォルトの RADIUS サーバーグループ「radius」を指定します。 • **group tacacs+**：**tacacs-server host** コマンドで設定した TACACS+サーバーを対象にする場合に、デフォルトの TACACS+サーバーグループ「tacacs+」を指定します。 • **group** *GROUP-NAME*：**aaa group server** コマンドで設定したサーバーグループを使用する場合に指定します。
デフォルト	アカウンティング方式リストの設定なし
コマンドモード	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。
制限事項	–
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**aaa accounting network default** {**none** | **start-stop** *METHOD1* [*METHOD2...*]}

aaa accounting network	
	no aaa accounting network default
パラメーター	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アカウンティングアルゴリズムを試行する方式のリストを指定します。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。アカウンティング方式には、以下のパラメーターを指定できます。 • group radius：radius-server host コマンドで設定した RADIUS サーバーを対象にする場合に、デフォルトの RADIUS サーバーグループ「radius」を指定します。 • group tacacs+：tacacs-server host コマンドで設定した TACACS+サーバーを対象にする場合に、デフォルトの TACACS+サーバーグループ「tacacs+」を指定します。 • group *GROUP-NAME*：aaa group server コマンドで設定したサーバーグループを使用する場合に指定します。
デフォルト	アカウンティング方式リストの設定なし
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	aaa accounting commands *LEVEL* {default | *LIST-NAME*} {none | start-stop *METHOD1* [*METHOD2...*]} no aaa accounting commands *LEVEL* {default | *LIST-NAME*}
パラメーター	*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。

aaa accounting commands	
	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アカウンティングアルゴリズムを試行する方式のリストを指定します。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。アカウンティング方式には、以下のパラメーターを指定できます。 • **group tacacs+**：**tacacs-server host** コマンドで設定した TACACS+サーバーを対象にする場合に、デフォルトの TACACS+サーバーグループ「tacacs+」を指定します。 • **group** *GROUP-NAME*：**aaa group server tacacs+** コマンドで設定した TACACS+サーバーグループを使用する場合に指定します。
デフォルト	アカウンティング方式リストの設定なし
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**accounting commands** *LEVEL* {**default** | *METHOD-LIST*} **no accounting commands** *LEVEL*
パラメーター	*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

accounting commands	
	す。 *METHOD-LIST*：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
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	**aaa accounting exec** {**default** | *LIST-NAME*} {**none** | **start-stop** *METHOD1* [*METHOD2...*]} **no aaa accounting exec** {**default** | *LIST-NAME*}
パラメーター	**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アカウンティングアルゴリズムを試行する方式のリストを指定します。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。アカウンティング方式には、以下のパラメーターを指定できます。 • **group radius**：**radius-server host** コマンドで設定した RADIUS サーバーを対象にする場合に、デフォルトの RADIUS サーバーグループ「radius」を指定します。 • **group tacacs+**：**tacacs-server host** コマンドで設定した TACACS+サーバーを対象にする場合に、デフォルトの TACACS+サーバーグループ「tacacs+」を指定します。

aaa accounting exec	
	• group *GROUP-NAME*：aaa group server コマンドで設定したサーバーグループを使用する場合に指定します。
デフォルト	アカウンティング方式リストの設定なし
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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。
シンタックス	accounting exec {default | *METHOD-LIST*} no accounting exec
パラメーター	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。 *METHOD-LIST*：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
コマンドモード	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。
制限事項	-
注意事項	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。
対象バージョン	1.01.01

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 機能のグローバル状態を表示します。
シンタックス	show aaa
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：AAA 機能のグローバル状態を表示する方法を示します。

```
# show aaa

 AAA is enabled. ...(1)
```

項番	説明
(1)	AAA サーバーの有効／無効を表示します。

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。
シンタックス	show radius statistics
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：サーバー関連の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。
(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。
(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有効または無効な 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有効または無効な 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有効または無効な 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。

項番	説明
(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。
シンタックス	**show tacacs statistics**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	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。
注意事項	TACACS+サーバーによる認証時のみ、本コマンドのカウントはカウントアップします。
対象バージョン	1.01.01

使用例：サーバー関連の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。
シンタックス	**clear aaa counters servers** {**all** ｜ **radius** {*IP-ADDRESS* ｜ *IPV6-ADDRESS* ｜ **all**} ｜ **tacacs** {*IP-ADDRESS* ｜ **all**} ｜ **sg** *NAME*}
パラメーター	**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 アドレスを指定します。

clear aaa counters servers	
	• *IPV6-ADDRESS*：RADIUS サーバーの IPv6 アドレスを指定します。 • all：すべての RADIUS サーバを対象にする場合に指定します。 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 アドレスを指定します。 • all：すべての TACACS+サーバを対象にする場合に指定します。 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。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：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 認証関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
mac-authentication enable	mac-authentication enable no mac-authentication enable
mac-authentication discard-time	mac-authentication discard-time SECONDS no mac-authentication discard-time
mac-authentication ignore-dhcp	mac-authentication ignore-dhcp no mac-authentication ignore-dhcp
mac-authentication password	mac-authentication password [0 | 7] PASSWORD {mac | web-mac | dot1x-mac | web-dot1x-mac} no mac-authentication password {mac | web-mac | dot1x-mac | web-dot1x-mac}
mac-authentication username mac-format	mac-authentication username mac-format case {lowercase | uppercase} delimiter {{hyphen | colon | dot} number {1 | 2 | 5} | none} no 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。
シンタックス	mac-authentication enable no mac-authentication enable
パラメーター	なし
デフォルト	無効
コマンドモード	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。 アクセスリスト機能の permit コマンドの authentication-bypass パラメーターを使用すると、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

mac-authentication enable	
	除します。
制限事項	-
注意事項	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。 認証バイパスを使用する際、対象フレームが自局 IP アドレスなどの CPU 宛ての場合、またはソフトウェア中継される場合は、認証が動作します。
対象バージョン	1.01.01

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。
シンタックス	**mac-authentication discard-time** *SECONDS* **no mac-authentication discard-time**
パラメーター	*SECONDS*：MAC 認証の認証破棄時間を 300～86,400 秒の範囲で指定します。
デフォルト	300 秒
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**mac-authentication ignore-dhcp** **no mac-authentication ignore-dhcp**

mac-authentication ignore-dhcp	
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**mac-authentication password** [0 | 7] *PASSWORD* {**mac** | **web-mac** | **dot1x-mac** | **web-dot1x-mac**} **no mac-authentication password** {**mac** | **web-mac** | **dot1x-mac** | **web-dot1x-mac**}
パラメーター	[0 | 7] *PASSWORD*：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。 • *PASSWORD*：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。 **mac**：MAC 認証で使用する場合に指定します。 **web-mac**：Web/MAC 認証(AND)で使用する場合に指定します。 **dot1x-mac**：IEEE 802.1X/MAC 認証(AND)で使用する場合に指定します。 **web-dot1x-mac**：Web/IEEE 802.1X/MAC 認証(AND)で使用する場合に指定します。
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。
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-

mac-authentication password	
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	mac-authentication username mac-format case {lowercase | uppercase} delimiter {{hyphen | colon | dot} number {1 | 2 | 5} | none} no mac-authentication username mac-format
パラメーター	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）
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。

コマンド	コマンドとパラメーター
dot1x enable	dot1x enable no dot1x enable
dot1x ignore-eapol-start interface	dot1x ignore-eapol-start interface INTERFACE-ID [,|-] no dot1x ignore-eapol-start interface INTERFACE-ID [,|-]
dot1x mode mac-authentication-fail	dot1x mode mac-authentication-fail no dot1x mode mac-authentication-fail
dot1x reauthentication interface	dot1x reauthentication interface INTERFACE-ID [,|-] no dot1x reauthentication interface INTERFACE-ID [,|-]
dot1x timeout quiet-period	dot1x timeout quiet-period SECONDS interface INTERFACE-ID [,|-] no dot1x timeout quiet-period interface INTERFACE-ID [,|-]
dot1x timeout re-authperiod	dot1x timeout re-authperiod SECONDS interface INTERFACE-ID [,|-] no dot1x timeout re-authperiod interface INTERFACE-ID [,|-]
dot1x timeout supp-timeout	dot1x timeout supp-timeout SECONDS interface INTERFACE-ID [,|-] no dot1x timeout supp-timeout interface INTERFACE-ID [,|-]
dot1x timeout server-timeout	dot1x timeout server-timeout SECONDS interface INTERFACE-ID [,|-] no dot1x timeout server-timeout interface INTERFACE-ID [,|-]
dot1x timeout tx-period	dot1x timeout tx-period SECONDS interface INTERFACE-ID [,|-] no dot1x timeout tx-period interface INTERFACE-ID [,|-]
fwd-eapol enable	fwd-eapol enable no 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。

コマンド	コマンドとパラメーター
show access-defender dot1x	show access-defender dot1x
show access-defender dot1x interface	show access-defender dot1x interface INTERFACE-ID [,|-]
show access-defender dot1x statistics	show access-defender dot1x statistics [interface INTERFACE-ID [,|-]]
dot1x initialize interface	dot1x initialize interface INTERFACE-ID [,|-]
dot1x re-authenticate interface	dot1x re-authenticate interface INTERFACE-ID [,|-]

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。
シンタックス	dot1x enable no dot1x enable
パラメーター	なし
デフォルト	無効
コマンドモード	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。 アクセスリスト機能の permit コマンドの authentication-bypass パラメーターを使用すると、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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.03

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。
シンタックス	dot1x ignore-eapol-start interface *INTERFACE-ID* [,|-] no dot1x ignore-eapol-start interface *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：EAPOL-Start 受信による認証の抑止機能を有効に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：物理ポートを指定します。複数指定できます。 • port-channel：ポートチャネルを指定します。
デフォルト	無効
コマンドモード	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

dot1x ignore-eapol-start interface	
	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。
制限事項	-
注意事項	-
対象バージョン	1.01.03

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)#
```

使用例：ポートチャネル 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-channel 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 認証を開始するモードを有効にします。MAC 認証が成功した場合は IEEE 802.1X 認証は行いません。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	**dot1x mode mac-authentication-fail** **no dot1x mode mac-authentication-fail**
パラメーター	なし
デフォルト	無効
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.04.01

使用例：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。
シンタックス	**dot1x reauthentication interface** *INTERFACE-ID* [,|-]

dot1x reauthentication interface	
	no dot1x reauthentication interface *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：IEEE 802.1X 認証の再認証を有効に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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	無効
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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)#
```

使用例：ポートチャネル 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-channel 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。
シンタックス	**dot1x timeout quiet-period** *SECONDS* **interface** *INTERFACE-ID* [,|-] **no dot1x timeout quiet-period interface** *INTERFACE-ID* [,|-]
パラメーター	*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 を指定した場合は、認証が失敗したときにステータスは保持されません。 **interface** *INTERFACE-ID*：ステータスの保持時間を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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	60 秒
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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)#
```

使用例：ポートチャネル 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-channel 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。
シンタックス	**dot1x timeout re-authperiod** *SECONDS* **interface** *INTERFACE-ID* [,|-] **no dot1x timeout re-authperiod interface** *INTERFACE-ID* [,|-]
パラメーター	*SECONDS*：再認証の間隔を、5～2,147,483,647 秒の範囲で指定します。 **interface** *INTERFACE-ID*：再認証の間隔を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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	3600 秒
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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)#
```

使用例：ポートチャネル 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-channel 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

dot1x timeout supp-timeout	
	は、no 形式のコマンドを使用します。
シンタックス	**dot1x timeout supp-timeout** *SECONDS* **interface** *INTERFACE-ID* [,|-] **no dot1x timeout supp-timeout interface** *INTERFACE-ID* [,|-]
パラメーター	*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** *INTERFACE-ID*：EAP-Request を再送信する間隔を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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	30 秒
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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)#
```

使用例：ポートチャネル 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-channel 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。
シンタックス	**dot1x timeout server-timeout** *SECONDS* **interface** *INTERFACE-ID* [,|-] **no dot1x timeout server-timeout interface** *INTERFACE-ID* [,|-]
パラメーター	*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** *INTERFACE-ID*：RADIUS サーバーからの応答待ち時間を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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	30 秒
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-

dot1x timeout server-timeout	
注意事項	-
対象バージョン	1.09.01

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)#
```

使用例：ポートチャネル 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-channel 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。
シンタックス	**dot1x timeout tx-period** *SECONDS* **interface** *INTERFACE-ID* [,|-] **no dot1x timeout tx-period interface** *INTERFACE-ID* [,|-]
パラメーター	*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。0 を指定した場合は、EAP-Request/EAP-Identity がサプリカントに送信されません。 **interface** *INTERFACE-ID*：EAP-Request/EAP-Identity をサプリカントに送信する間隔を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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	30 秒
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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)#
```

使用例：ポートチャネル 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-channel 1
```

```
(config-a-def)#
```

9.4.10 fwd-eapol enable

fwd-eapol enable	
目的	IEEE 802.1X 認証が無効の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。
シンタックス	fwd-eapol enable no fwd-eapol enable
パラメーター	なし
デフォルト	無効
コマンドモード	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	本設定が無効の場合は、IEEE 802.1X 認証が無効の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。
制限事項	-
注意事項	-
対象バージョン	1.03.01

使用例：IEEE 802.1X 認証が無効の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。
シンタックス	show access-defender dot1x
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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)
  (5)                    (6)
  portEnabled: true - portControl: Auto
  portStatus: authorized - currentId: 1 ...(7)
  protocol version: 2 ...(8)
```

```
reAuthenticate: Disabled ...(9)
reAuthPeriod: 3600 ...(10)
     (11)                    (12)
PAE: state:Authenticated - portMode: Auto
PAE: reAuthCount: 0 ...(13)
     (14)              (15)           (16)
PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
BE: state: Idle ...(17)
    (18)              (19)
BE: suppTimeout: 30 - serverTimeout: 30
    (20)                            (21)
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／無効を表示します。
(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)	サプリカントのリンクステータスを表示します。 常に「true」が表示されます。
(6)	サプリカントの認証モードを表示します。 常に「Auto」が表示されます。
(7)	サプリカントの現在の認証セッション ID を表示します。
(8)	IEEE 802.1X 認証/EAPOL プロトコルバージョンを表示します。
(9)	サプリカントの再認証状態設定の有効／無効を表示します。
(10)	サプリカントの再認証期間設定を表示します。
(11)	サプリカントの Port Access Entity (PAE) の現在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
(12)	サプリカントの PAE のポートモードを表示します。 常に「Auto」が表示されます。
(13)	サプリカントへの request-ID の再送信試行回数を表示します。
(14)	サプリカントの休止期間の設定を表示します。
(15)	サプリカントに許可されている再認証試行回数を表示します。 常に「2」が表示されます。
(16)	サプリカントの送信期間設定を表示します。
(17)	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

項番	説明
	Timeout：応答タイムアウト Idle：待機中 Initialize：初期化
(18)	サプリカントのタイムアウト設定を表示します。
(19)	RADIUS サーバーの応答待ち時間を表示します。
(20)	非認証サプリカントのパケット廃棄方向の設定を表示します。 常に「In」が表示されます。
(21)	非認証サプリカントの使用可能なパケット廃棄方向を表示します。 常に「In」が表示されます。

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。
シンタックス	**show access-defender dot1x interface** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：IEEE 802.1X 認証の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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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を表示します。
(4)	EAPOL-Start を受信したときの認証を抑止する機能の有効／無効を表示します。
(5)	認証が失敗したときのステータスの保持時間を表示します。

項番	説明
(6)	EAP-Request/EAP-Identity をサプリカントに送信する間隔を表示します。
(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 を再送信する間隔を表示します。
(8)	RADIUS サーバーからの応答待ち時間を表示します。
(9)	EAP-Request/EAP-Identity をサプリカントに再送信する回数を表示します。
(10)	IEEE 802.1X 認証の再認証の有効／無効を表示します。
(11)	再認証の間隔を表示します。

使用例：ポートチャネル 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-channel 1

Interface          : Port-channel1 ...(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    : Disabled ...(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を表示します。
(4)	EAPOL-Start を受信したときの認証を抑止する機能の有効／無効を表示します。
(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 を再送信する間隔を表示します。
(8)	RADIUS サーバーからの応答待ち時間を表示します。
(9)	EAP-Request/EAP-Identity をサプリカントに再送信する回数を表示します。
(10)	IEEE 802.1X 認証の再認証の有効／無効を表示します。
(11)	再認証の間隔を表示します。

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。
シンタックス	**show access-defender dot1x statistics** [**interface** *INTERFACE-ID* [,|-]]
パラメーター	**interface** *INTERFACE-ID*（省略可能）：IEEE 802.1X 認証に関する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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	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 access-defender dot1x statistics	
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。
制限事項	-
注意事項	-
対象バージョン	1.01.03

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。

使用例：ポートチャネル 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-channel 1

Port-channel1 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。
シンタックス	**dot1x initialize interface** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：IEEE 802.1X 認証を初期化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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	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。
対象バージョン	1.01.03

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)#
```

使用例：ポートチャネル 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-channel 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。
シンタックス	**dot1x re-authenticate interface** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：IEEE 802.1X 認証の再認証を実行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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	なし
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	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。
対象バージョン	1.01.03

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)#
```

使用例：ポートチャネル 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-channel 1
(config-a-def)#
```

9.5 SSL コマンド

SSL (SECURE SOCKETS LAYER) 関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
show ssl https-certificate	show ssl https-certificate
show ssl https-private-key	show ssl https-private-key
show ssl csr	show ssl csr
ssl gencsr rsakey	ssl gencsr rsakey [RSA-KEY-LENGTH]

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。
シンタックス	**show ssl https-certificate**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.03

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。

項番	説明
(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。
(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。
シンタックス	**show ssl https-private-key**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.03

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。
シンタックス	**show ssl csr**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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。
シンタックス	**ssl gencsr rsakey** [*RSA-KEY-LENGTH*]
パラメーター	RSA-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
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限事項	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。
注意事項	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。
対象バージョン	1.03.01

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 認証関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
web-authentication enable	web-authentication enable no web-authentication enable
web-authentication http-ip	web-authentication http-ip {ipv4 IP-ADDRESS | ipv6 IPV6-ADDRESS} no web-authentication http-ip {ipv4 | ipv6}
web-authentication http-port	web-authentication http-port {TCP-PORT | disable} no web-authentication http-port
web-authentication https-port	web-authentication https-port {TCP-PORT | disable} no web-authentication https-port
web-authentication redirect disable	web-authentication redirect disable [http | https] no web-authentication redirect disable
web-authentication redirect url	web-authentication redirect url URL no web-authentication redirect url
web-authentication http-session-timeout	web-authentication http-session-timeout SECONDS no web-authentication http-session-timeout
web-authentication overwrite enable	web-authentication overwrite enable no web-authentication overwrite enable
web-authentication ttl	web-authentication ttl VALUE interface INTERFACE-ID [,|-] no web-authentication ttl [VALUE] [interface INTERFACE-ID [,|-]]
web-authentication interface	web-authentication interface INTERFACE-ID [, | -] webpages WEBPAGES-ID no web-authentication interface INTERFACE-ID [, | -] webpages
web-authentication redirect proxy-port	web-authentication redirect proxy-port PROXY-PORT no web-authentication redirect proxy-port
web-authentication snooping proxy-port	web-authentication snooping proxy-port PROXY-PORT no web-authentication snooping proxy-port
web-authentication logging web-access on	web-authentication logging web-access on no web-authentication logging web-access on
show access-defender webpages	show access-defender webpages

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。
シンタックス	web-authentication enable no web-authentication enable
パラメーター	なし

web-authentication enable	
デフォルト	無効
コマンドモード	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。 アクセスリスト機能の permit コマンドの authentication-bypass パラメーターを使用すると、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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.03

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／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。
シンタックス	**web-authentication http-ip** {**ipv4** *IP-ADDRESS* | **ipv6** *IPV6-ADDRESS*} **no web-authentication http-ip** {**ipv4** | **ipv6**}
パラメーター	**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。 **ipv6** *IPV6-ADDRESS*：Web 認証用の Web サーバーの IPv6 アドレスを設定する場合に指定します。
デフォルト	なし
コマンドモード	AccessDefender 設定モード

web-authentication http-ip	
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。
制限事項	-
注意事項	-
対象バージョン	1.01.03

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)#
```

使用例：Web 認証用の Web サーバーの IPv6 アドレスを 2016::2016 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication http-ip ipv6 2016::2016
(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 プロトコルの有効／無効、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。
シンタックス	**web-authentication http-port** {*TCP-PORT* | **disable**} **no web-authentication http-port**
パラメーター	*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。 **disable**：HTTP プロトコルのアクセスを無効にする場合に指定します。
デフォルト	HTTP プロトコル：有効、TCP ポート番号：80
コマンドモード	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(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。
制限事項	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 ポート番号は指定できません。 • 21 (FTP protocol) • 22 (SSH protocol) • 23 (Telnet protocol) • 443 (HTTPS protocol) • **ip telnet service-port** コマンドで指定したポート番号 • **ip ssh service-port** コマンドで指定したポート番号 • **web-authentication https-port** コマンドで指定したポート番号 • **web-authentication snooping proxy-port** コマンドで指定したポート番号 • **web-authentication redirect proxy-port** コマンドで指定したポート番

web-authentication http-port	
	号 • web-deny-notify http-port コマンドで指定したポート番号 • web-deny-notify https-port コマンドで指定したポート番号
注意事項	本コマンドで disable パラメーターを指定して HTTP プロトコルのアクセスを無効にした場合は、HTTP（TCP ポート番号 80）パケットのリダイレクトも無効になります。
対象バージョン	1.01.03 1.09.01：disable パラメーター追加

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)#
```

使用例：Web 認証用の Web サーバーで、HTTP プロトコルのアクセスを無効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication http-port disable
(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 プロトコルの有効／無効、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。
シンタックス	web-authentication https-port {*TCP-PORT* | disable} no web-authentication https-port
パラメーター	*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。 disable：HTTPS プロトコルのアクセスを無効にする場合に指定します。
デフォルト	HTTPS プロトコル：有効、TCP ポート番号：443
コマンドモード	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。
制限事項	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 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 ポート番号は指定できません。 • 21（FTP protocol） • 22（SSH protocol） • 23（Telnet protocol） • 80（HTTP protocol） • ip telnet service-port コマンドで指定したポート番号 • ip ssh service-port コマンドで指定したポート番号 • web-authentication http-port コマンドで指定したポート番号 • web-authentication snooping proxy-port コマンドで指定したポート番

web-authentication https-port	
	号 • web-authentication redirect proxy-port コマンドで指定したポート番号 • web-deny-notify http-port コマンドで指定したポート番号 • web-deny-notify https-port コマンドで指定したポート番号
注意事項	本コマンドで disable パラメーターを指定して HTTPS プロトコルのアクセスを無効にした場合は、HTTPS（TCP ポート番号 443）パケットのリダイレクトも無効になります。
対象バージョン	1.01.03 1.09.01：disable パラメーター追加

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)#
```

使用例：Web 認証用の Web サーバーで、HTTPS プロトコルのアクセスを無効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication https-port disable
(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。
シンタックス	web-authentication redirect disable [http | https] no web-authentication redirect disable
パラメーター	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）
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.03.06

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。
シンタックス	**web-authentication redirect url** *URL* **no web-authentication redirect url**
パラメーター	*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。
コマンドモード	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)のプロトコルを使用して任意の URL を参照したときと、**web-authentication redirect proxy-port** コマンドで指定したプロキシを参照したときに、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 IPv4 アドレス／IPv6 アドレスは **web-authentication http-ip** コマンドで設定します。
制限事項	一度に指定できる URL は 1 つだけです。
注意事項	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。
対象バージョン	1.01.03

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。
シンタックス	**web-authentication http-session-timeout** *SECONDS* **no web-authentication http-session-timeout**
パラメーター	*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
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	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。
注意事項	-
対象バージョン	1.03.01

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。
シンタックス	**web-authentication overwrite enable** **no web-authentication overwrite enable**
パラメーター	なし
デフォルト	無効
コマンドモード	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

web-authentication overwrite enable	
	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。
制限事項	-
注意事項	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。
対象バージョン	1.04.01

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。
シンタックス	web-authentication ttl *VALUE* interface *INTERFACE-ID* [,|-] no web-authentication ttl [*VALUE*] [interface *INTERFACE-ID* [,|-]]
パラメーター	*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 *INTERFACE-ID*：TTL フィルター機能を有効に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：物理ポートを指定します。複数指定できます。 • port-channel：ポートチャネルを指定します。
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	インターフェースごとに最大 8 個設定できるのは AEOS-NP2000 Ver. 1.03.06 以降です。それより前のバージョンでは設定可能数はインターフェースごとに最大 1 個です。
対象バージョン	1.01.03 1.03.06：設定可能数の仕様変更

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 interface

web-authentication interface	
目的	インターフェースごとに適用する個別 Web 認証ページを設定します。 削除する場合は、no 形式のコマンドを使用します。
シンタックス	**web-authentication interface** *INTERFACE-ID* [, | -] **webpages** *WEBPAGES-ID* **no web-authentication interface** *INTERFACE-ID* [, | -] **webpages**
パラメーター	**interface** *INTERFACE-ID*：個別 Web 認証ページを適用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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。 *WEBPAGES-ID*：個別 Web 認証ページ ID を 1～30 の範囲で指定します。
デフォルト	なし
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	個別 Web 認証ページを使用する場合は、事前に個別 Web 認証ページを装置にダウンロードしてください。 指定した ID の個別 Web 認証ページが存在しない場合は、「デフォルト Web 認証ページ」が適用されます。デフォルト Web 認証ページがユーザーによってカスタマイズされて装置にダウンロードされている場合は、「カスタマイズされたデフォルト Web 認証ページ」が適用されます。
制限事項	個別 Web 認証ページを使用する装置で SD カードブートを併用する場合、カスタム認証ページの数によっては、SD カードの仕様制限ですべてのファイルを SD カードに保存できないことがあります。そのため、併用する場合は以下の目安例を参考に、使用する個別 Web 認証ページの数を検討してください。なお、以下の目安例は SD カードに余計なファイルが無い状態を想定しています。 • 個別 Web 認証ページごとに 6 種類すべての認証ページを準備する場合は、個別 Web 認証ページは 15 個(ID=1～15)を目安に使用してください。 • 個別 Web 認証ページごとに「ログイン認証ページ」「認証成功ページ」「認証失敗ページ」の 3 種類のみを準備し、他は「デフォルト Web 認証ページ」を使用する場合は、個別 Web 認証ページは 30 個まで使用できます。 同様に、**backup memory-card: prefix** コマンドを併用する場合も、この目安を参考に使用する個別 Web 認証ページの数を検討してください。
注意事項	-
対象バージョン	1.09.01

使用例：ポート 1/0/1 に適用する個別 Web 認証ページ ID を 5 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication interface port 1/0/1 webpages 5
(config-a-def)#
```

9.6.11 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。
シンタックス	**web-authentication redirect proxy-port** *PROXY-PORT* **no web-authentication redirect proxy-port**
パラメーター	*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
コマンドモード	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。
制限事項	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 ポート番号は、*PROXY-PORT* に指定できません。 • 21（FTP protocol） • 22（SSH protocol） • 23（Telnet protocol） • 80（HTTP protocol） • 443（HTTPS protocol） • **ip telnet service-port** コマンドで指定したポート番号 • **ip ssh service-port** コマンドで指定したポート番号 • **web-authentication http-port** コマンドで指定したポート番号 • **web-authentication https-port** コマンドで指定したポート番号 • **web-authentication snooping proxy-port** コマンドで指定したポート番号 • **web-deny-notify http-port** コマンドで指定したポート番号 • **web-deny-notify https-port** コマンドで指定したポート番号
注意事項	-
対象バージョン	1.01.03

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)#
```

9.6.12 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。

web-authentication snooping proxy-port	
シンタックス	**web-authentication snooping proxy-port** *PROXY-PORT* **no web-authentication snooping proxy-port**
パラメーター	*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
コマンドモード	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。
制限事項	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 ポート番号は、*PROXY-PORT* に指定できません。 • 21（FTP protocol） • 22（SSH protocol） • 23（Telnet protocol） • 80（HTTP protocol） • 443（HTTPS protocol） • **ip telnet service-port** コマンドで指定したポート番号 • **ip ssh service-port** コマンドで指定したポート番号 • **web-authentication http-port** コマンドで指定したポート番号 • **web-authentication https-port** コマンドで指定したポート番号 • **web-authentication redirect proxy-port** コマンドで指定したポート番号 • **web-deny-notify http-port** コマンドで指定したポート番号 • **web-deny-notify https-port** コマンドで指定したポート番号
注意事項	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。
対象バージョン	1.02.01

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)#
```

9.6.13 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。

web-authentication logging web-access on	
シンタックス	web-authentication logging web-access on no web-authentication logging web-access on
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	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。
注意事項	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。
対象バージョン	1.01.03

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)#
```

9.6.14 show access-defender webpages

show access-defender webpages	
目的	装置にダウンロードした Web 認証ページの情報を表示します。
シンタックス	show access-defender webpages
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	装置に最初から保存されている「デフォルト Web 認証ページ」の情報は表示されません。
注意事項	-
対象バージョン	1.09.01

使用例：装置にダウンロードした Web 認証ページの情報を表示する方法を示します。

```
# show access-defender webpages

WEBPAGES-ID:Default ...(1)
(2)                          (3)                 (4)
Filename                    Size                Date
-----------------------------------------------------------
login-failure-page           300 Jan 21 2017 09:00:00
login-page                  1000 Jan 21 2017 09:00:00
login-success-page          1000 Jan 21 2017 09:00:00
logout-failure-page          500 Jan 21 2017 09:00:00
logout-success-page          500 Jan 21 2017 09:00:00
redirect-error-page          500 Jan 21 2017 09:00:00

WEBPAGES-ID:1 ...(1)
(2)                          (3)                 (4)
```

```
Filename                        Size                 Date
-------------------------------------------------------------
01-login-failure-page            500 Dec 12 2019 11:14:17
01-login-page                   2000 Dec 12 2019 11:15:20
01-login-success-page           1000 Dec 12 2019 11:17:26
01-logout-failure-page           500 Dec 12 2019 11:19:40
01-logout-success-page           500 Dec 12 2019 11:20:21
01-redirect-error-page           500 Dec 12 2019 11:22:37

WEBPAGES-ID:5 ...(1)
(2)                             (3)                  (4)
Filename                        Size                 Date
-------------------------------------------------------------
05-login-page                   2000 Dec 12 2019 12:22:37
05-login-success-page           1000 Dec 12 2019 12:24:10
05-logout-success-page           500 Dec 12 2019 12:27:21
```

項番	説明
(1)	個別 Web 認証ページ ID を表示します。 「カスタマイズされたデフォルト Web 認証ページ」の場合は Default と表示されます。なお、カスタマイズされていない「デフォルト Web 認証ページ」は表示されません。
(2)	ファイル名を表示します。
(3)	ファイルサイズを表示します。
(4)	ファイルの更新日時を表示します。

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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
web-deny-notify (expert access-list)	[SEQ] web-deny-notify tcp CONDITION
web-deny-notify http-port	web-deny-notify http-port TCP-PORT no web-deny-notify http-port
web-deny-notify https-port	web-deny-notify https-port TCP-PORT no web-deny-notify https-port
web-deny-notify redirect url	web-deny-notify redirect url URL no web-deny-notify redirect url
copy (web-deny-notify)	copy {flash: [URL] ｜ tftp: [URL]} web-access-deny-page copy web-access-deny-page {flash: [URL] ｜ tftp: [URL]}
access-defender erase web-access-deny-page	access-defender erase web-access-deny-page

9.7.1 web-deny-notify (expert access-list)

web-deny-notify (expert access-list)	
目的	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。
シンタックス	[*SEQ*] **web-deny-notify tcp** *CONDITION*
パラメーター	*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 プロトコルに対するエントリーと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。
デフォルト	なし
コマンドモード	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	本エントリーにマッチした 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。

送信元		サポート可否
IP	MAC	
指定なし(any)	指定なし(any)	未サポート
指定なし(any)	特定端末指定	host 指定の場合のみサポート、マスク指定は未サポート

web-deny-notify (expert access-list)	
	特定端末指定 | 指定なし(any) | host 指定の場合のみサポート、マスク指定は未サポート 特定端末指定 | 特定端末指定 | host 指定の場合のみサポート、マスク指定は未サポート 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。 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エントリーを作成した場合、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エントリー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。
制限事項	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、各エントリー毎に最大 256Kbps に制限されています。 本コマンドは、構成情報ではアクセスリストコマンド（ラベル# ACL）で表示されます。
注意事項	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。
対象バージョン	1.09.01

■ 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」を作成し、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エントリー」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エントリー」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。
シンタックス	**web-deny-notify http-port** *TCP-PORT* **no web-deny-notify http-port**
パラメーター	*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
コマンドモード	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。
制限事項	以下に示す TCP ポート番号は指定できません。 • 21 (FTP protocol) • 22 (SSH protocol) • 23 (Telnet protocol) • 443 (HTTPS protocol) • **ip telnet service-port** コマンドで指定したポート番号 • **ip ssh service-port** コマンドで指定したポート番号 • **web-authentication http-port** コマンドで指定したポート番号 • **web-authentication https-port** コマンドで指定したポート番号 • **web-authentication snooping proxy-port** コマンドで指定したポート番号 • **web-authentication redirect proxy-port** コマンドで指定したポート番号 • **web-deny-notify https-port** コマンドで指定したポート番号 本コマンドは、構成情報では Web 認証コマンド（ラベル# WEB-AUTHENTICATION）で表示されます。
注意事項	-
対象バージョン	1.09.01

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。
シンタックス	**web-deny-notify https-port** *TCP-PORT* **no web-deny-notify https-port**
パラメーター	*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
コマンドモード	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。
制限事項	以下に示す TCP ポート番号は指定できません。 • 21 (FTP protocol) • 22 (SSH protocol) • 23 (Telnet protocol) • 80 (HTTP protocol) • **ip telnet service-port** コマンドで指定したポート番号 • **ip ssh service-port** コマンドで指定したポート番号 • **web-authentication http-port** コマンドで指定したポート番号 • **web-authentication https-port** コマンドで指定したポート番号 • **web-authentication snooping proxy-port** コマンドで指定したポート番号 • **web-authentication redirect proxy-port** コマンドで指定したポート番号 • **web-deny-notify http-port** コマンドで指定したポート番号 本コマンドは、構成情報では Web 認証コマンド（ラベル# WEB-AUTHENTICATION）で表示されます。
注意事項	-
対象バージョン	1.09.01

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。
シンタックス	**web-deny-notify redirect url** *URL* **no web-deny-notify redirect url**
パラメーター	*URL*：リダイレクト先 URL を、最大 255 文字で指定します。

web-deny-notify redirect url	
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。
コマンドモード	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エントリーに対して応答する、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。
制限事項	一度に指定できる URL は 1 つだけです。 本コマンドは、構成情報では Web 認証コマンド（ラベル# WEB-AUTHENTICATION）で表示されます。
注意事項	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
対象バージョン	1.09.01

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 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ロードまたはアップロードします。
シンタックス	**copy** {**flash**: [*URL*] | **tftp**: [*URL*]} **web-access-deny-page** **copy web-access-deny-page** {**flash**: [*URL*] | **tftp**: [*URL*]}

copy (web-deny-notify)	
パラメーター	**flash:**：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。 **tftp:**：TFTP を使用する場合に指定します。 *URL*：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の URL を指定します。以下のいずれかの書式を使用します。 • **flash: c:/***URL*：装置のローカルフラッシュ上のファイルを指定します。例えば、c:/custom_web-deny-notify.html と入力します。 • **flash: d:/***URL*：SD カード上のファイルを指定します。例えば、d:/custom_web-deny-notify.html と入力します。 • **tftp:** [//*IP-ADDRESS*/[*DIRECTORY*/]*FILE-NAME*]：TFTP サーバー上のファイルを指定します。 　• *IP-ADDRESS*：TFTP サーバーの IP アドレスを指定します。 　• *DIRECTORY*（省略可能）：ディレクトリー名を指定します。 　• *FILE-NAME*：ダウンロード元ファイル名、またはアップロード先ファイル名を指定します。
デフォルト	なし
コマンドモード	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。
制限事項	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。 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。
注意事項	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。
対象バージョン	1.09.01

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。
シンタックス	access-defender erase web-access-deny-page
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.09.01

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コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
dhcp-snooping enable	dhcp-snooping enable no dhcp-snooping enable
dhcp-snooping interface	dhcp-snooping interface INTERFACE-ID [,|-] no dhcp-snooping interface INTERFACE-ID [,|-]
dhcp-snooping mode deny	dhcp-snooping mode deny no dhcp-snooping mode deny
dhcp-snooping mode timer	dhcp-snooping mode timer SECONDS no dhcp-snooping mode timer
dhcp-snooping mode mac-authentication	dhcp-snooping mode mac-authentication no dhcp-snooping mode mac-authentication
dhcp-snooping static-entry	dhcp-snooping static-entry interface INTERFACE-ID IP-ADDRESS no dhcp-snooping static-entry [interface INTERFACE-ID] [IP-ADDRESS]
show access-defender dhcp-snooping configuration	show access-defender dhcp-snooping configuration
show access-defender dhcp-snooping mode-status	show access-defender dhcp-snooping mode-status
show access-defender dhcp-snooping 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。
シンタックス	dhcp-snooping enable no dhcp-snooping enable
パラメーター	なし
デフォルト	無効
コマンドモード	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

dhcp-snooping enable	
	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。
制限事項	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。
注意事項	DHCPv6 スヌーピングは未サポートです。
対象バージョン	1.01.03

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。
シンタックス	**dhcp-snooping interface** *INTERFACE-ID* [,|-] **no dhcp-snooping interface** *INTERFACE-ID* [,|-]
パラメーター	*INTERFACE-ID*：DHCP スヌーピングを有効に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**：物理ポートを指定します。複数指定できます。 • **port-channel**：ポートチャネルを指定します。
デフォルト	無効
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	-
制限事項	DHCP スヌーピングとゲートウェイ認証は併用できません。
注意事項	ポートチャネルのメンバーポートは、DHCP スヌーピングを有効にしないでください。
対象バージョン	1.01.03

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)#
```

使用例：ポートチャネル 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-channel 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。

dhcp-snooping mode deny	
シンタックス	**dhcp-snooping mode deny** **no dhcp-snooping mode deny**
パラメーター	なし
デフォルト	無効 (PERMIT モードに設定)
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.03

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。
シンタックス	**dhcp-snooping mode timer** *SECONDS* **no dhcp-snooping mode timer**
パラメーター	*SECONDS*：DHCP スヌーピングの動作モード自動切り替えタイマーの値を、0 または 30～604,800 秒の範囲で指定します。0 を指定すると、PERMIT モード固定になります。
デフォルト	1800 秒
コマンドモード	AccessDefender 設定モード
特権レベル	レベル：15
ガイドライン	DHCP スヌーピングの動作モード自動切り替えタイマーで指定した時間が経過すると、PERMIT モードから DENY モードに自動的に切り替わります。
制限事項	-
注意事項	PERMIT モードのときにタイマーの値が設定されると、タイマーがリセットされます。
対象バージョン	1.01.03

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 3,600 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 3600
(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。
シンタックス	**dhcp-snooping mode mac-authentication** **no dhcp-snooping mode mac-authentication**
パラメーター	なし
デフォルト	無効
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.03

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登録します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	**dhcp-snooping static-entry interface** *INTERFACE-ID IP-ADDRESS* **no dhcp-snooping static-entry** [**interface** *INTERFACE-ID*] [*IP-ADDRESS*]
パラメーター	**interface** *INTERFACE-ID*：DHCP スヌーピングのスタティックエントリーを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**：物理ポートを指定します。 • **port-channel**：ポートチャネルを指定します。 *IP-ADDRESS*：DHCP スヌーピングの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
コマンドモード	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、

dhcp-snooping static-entry	
	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。
制限事項	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。 本コマンドで DHCP スヌーピングのスタティックエントリーを登録している状態では、**total-client** コマンドによる認証クライアントの最大数を変更することはできません。
注意事項	DHCPv6 スヌーピングは未サポートです。
対象バージョン	1.01.03

使用例：ポート 1/0/1 の IP アドレス 192.168.1.10 のスタティックエントリーを登録する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping static-entry interface port 1/0/1 192.168.1.10
(config-a-def)#
```

使用例：ポートチャネル 1 の IP アドレス 192.168.1.10 のスタティックエントリーを登録する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping static-entry interface port-channel 1 192.168.1.10
(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。
シンタックス	**show access-defender dhcp-snooping configuration**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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     16 17    24 25
           +------+ +------+ +------+ +---
         1 oooooooo ........ ........ ....
```

```
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／無効を表示します。
(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）の設定を表示します。 DENY：コマンド設定時 PERMIT：コマンド未設定時
(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。
(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。
シンタックス	**show access-defender dhcp-snooping mode-status**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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。
シンタックス	**show access-defender dhcp-snooping status**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.03

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／無効を表示します。
(2)	DHCP スヌーピングの動作モードを表示します。
(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

項番	説明
	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。

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。

コマンド	コマンドとパラメーター
debug enable	debug enable no debug enable
debug clear buffer	debug clear buffer
debug clear cpu port	debug clear cpu port
debug clear error-log	debug clear error-log
debug copy	debug copy SOURCE-URL DESTINATION-URL debug copy SOURCE-URL {tftp: //LOCATION/DESTINATION-URL ｜ ftp: //USER-NAME:PASSWORD@LOCATION:TCP-PORT/DESTINATION-URL ｜ c:/DESTINATION-URL ｜ d:/DESTINATION-URL}
debug output	debug output {module MODULE-LIST ｜ all} {buffer ｜ console} no debug output {module MODULE-LIST ｜ all}
debug reboot on-error	debug reboot on-error no debug reboot on-error
debug reboot on-tscmoddown	debug reboot on-tscmoddown no debug reboot on-tscmoddown
debug show access-defender internal-resource	debug show access-defender internal-resource
debug show buffer	debug show buffer [utilization]
debug show cpu port	debug show cpu port [l2 ｜ l3 [unicast ｜ multicast] ｜ protocol NAME ｜ security]
debug show cpu utilization	debug show cpu utilization
debug show error-log	debug show error-log
debug show inetstat	debug show inetstat
debug show memory-pool	debug show memory-pool {summary ｜ MEMORY}
debug show netstat	debug show netstat
debug show output	debug show output
debug show ps	debug show ps
debug show tcpstat	debug show tcpstat
debug show udpstat	debug show udpstat
debug show wd-error-log	debug show wd-error-log
debug stack restart	debug stack restart unit UNIT-ID stack-port PORTNO
show switching resource status	show switching resource status

コマンド	コマンドとパラメーター
show tech-support	show tech-support [MODULE ｜ system-dump ｜ unit UNIT-ID ｜ interface {INTERFACE-ID [,｜-] ｜ stack-port} system-dump]

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。
シンタックス	debug enable no debug enable
パラメーター	なし
デフォルト	無効
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	debug clear buffer
パラメーター	なし
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 にトラップされたレイヤー2、レイヤー3、セキュリティー関連の制御パケットの統計情報を消去します。
シンタックス	**debug clear cpu port**
パラメーター	なし
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：レイヤー2、レイヤー3、セキュリティー関連の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。
シンタックス	**debug clear error-log**
パラメーター	なし
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	**debug copy** *SOURCE-URL DESTINATION-URL* **debug copy** *SOURCE-URL* {**tftp:** *//LOCATION/DESTINATION-URL* | **ftp:** *//USER-NAME:PASSWORD@LOCATION:TCP-PORT/DESTINATION-URL* | **c:***/DESTINATION-URL* | **d:***/DESTINATION-URL*}
パラメーター	*SOURCE-URL*：コピー元ファイルの送信元 URL を指定します。以下のいずれかのパラメーターを使用できます。

debug copy	
	• **buffer**：デバッグバッファーの情報をコピーします。 • **error-log**：エラーログの情報をコピーします。 • **tech-support**：技術サポート情報をコピーします。技術サポート情報は、FTP ではコピーできません。 **tftp:**：TFTP サーバーにコピーする場合に指定します。 • *LOCATION*：TFTP/FTP サーバーの、IPv4 または IPv6 アドレスを指定します。 • *DESTINATION-URL*：送信先 URL を指定します。 **ftp:**：FTP サーバーにコピーする場合に指定します。 • *USER-NAME*：FTP サーバーのユーザー名を指定します。 • *PASSWORD*：ユーザーのパスワードを指定します。 • *LOCATION*：TFTP/FTP サーバーの、IPv4 または IPv6 アドレスを指定します。 • *TCP-PORT*：TCP ポート番号を指定します。 • *DESTINATION-URL*：送信先 URL を指定します。 **c:**：ローカルフラッシュにコピーする場合に指定します。 • *DESTINATION-URL*：送信先 URL を指定します。 **d:**：SD カードにコピーする場合に指定します。 • *DESTINATION-URL*：送信先 URL を指定します。
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	なし
制限事項	–
注意事項	–
対象バージョン	1.01.01

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指定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	debug output {module *MODULE-LIST* | all} {buffer | console} no debug output {module *MODULE-LIST* | all}
パラメーター	*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
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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。
シンタックス	debug reboot on-error no debug reboot on-error

debug reboot on-error	
パラメーター	なし
デフォルト	有効（debug reboot on-error）
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：重大なエラーが発生したときに装置を再起動する方法を示します。

```
# configure terminal
(config)# debug reboot on-error
(config)#
```

10.1.8 debug reboot on-tscmoddown

debug reboot on-tscmoddown	
目的	スイッチ LSI の異常状態が継続した場合に、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。
シンタックス	debug reboot on-tscmoddown no debug reboot on-tscmoddown
パラメーター	なし
デフォルト	有効（debug reboot on-tscmoddown）
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.09.03

使用例：スイッチ LSI の異常状態が継続した場合に装置を再起動する方法を示します。

```
# configure terminal
(config)# debug reboot on-tscmoddown
(config)#
```

10.1.9 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。
シンタックス	debug show access-defender internal-resource
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	-

debug show access-defender internal-resource	
注意事項	-
対象バージョン	1.03.03

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。

```
# 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                       25/   256      0
Author-DB                    25/ 12400      0
WebAuth-HostDB                0/  4000      0
WebAuth-ConnectionDB          0/  1024      0
WebAuth-TcpPortDB             0/  1024      0
Web-Connection                0/    10   1558  2019-9-17 09:18:28
Web-ConnectionV6              0/    10      0
Security-client-DB           18/  4096      0
Security-client-cache         0/    64      0
Security-client-p-cache       6/  4096      0
```

10.1.10 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。
シンタックス	**debug show buffer [utilization]**
パラメーター	**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。
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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%
```

10.1.11 debug show cpu port

debug show cpu port	
目的	CPU にトラップされたレイヤー2、レイヤー3、セキュリティー関連の制御パケットの統計情報を表示します。
シンタックス	**debug show cpu port** [**l2** ｜ **l3** [**unicast** ｜ **multicast**] ｜ **protocol** *NAME* ｜ **security**]
パラメーター	**l2**（省略可能）：レイヤー2 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。 **l3**（省略可能）：レイヤー3 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。 • **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制御パケットの統計情報を表示する場合に指定します。
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	–
対象バージョン	1.01.01 1.03.03：**security** パラメーター追加

使用例：レイヤー2、レイヤー3、セキュリティー機能関連の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：レイヤー2 関連の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：セキュリティー関連の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
```

10.1.12 debug show cpu utilization

debug show cpu utilization	
目的	総 CPU 使用率、およびプロセスごとの CPU 使用率を表示します。
シンタックス	**debug show cpu utilization**
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：プロセスごとの CPU 使用率の表示方法を示します。

```
# 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。

10.1.13 debug show error-log

debug show error-log	
目的	エラーログの情報を表示します。
シンタックス	**debug show error-log**
パラメーター	なし
デフォルト	なし
コマンドモード	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	–
制限事項	–
注意事項	–
対象バージョン	1.01.01

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
# Persistent memory area
```

```
# Error level: DEBUG (2)
# Firmware version: 1.03.01
# Clock: 29860 ms
# Characters lost: 0
#

====================== SOFTWARE FATAL ERROR =======================
file=./Src/lac_db.c,line=456,Invalid semaphore handle : 00000000

Current TASK : Root
------------------------- TASK STACKTRACE ------------------------
-> 114989C
->  A9D394
->  ADC880
->  ADF940
-> 10A43B4
->  A053E4
->FFFFFFFC
->  A053E4
->FFFFFFFC
->  BAE6C8
->  A053E4
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

10.1.14 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。
シンタックス	debug show inetstat
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	–
対象バージョン	1.03.03

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)
```

10.1.15 debug show memory-pool

debug show memory-pool	
目的	メモリーバッファーの情報を表示します。
シンタックス	**debug show memory-pool** {**summary** | *MEMORY*}
パラメーター	**summary**：概略情報を表示する場合に指定します。 *MEMORY*：詳細情報を表示する場合にキーワードを入力します。
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	出力される情報量が多い場合、自装置宛パケットの送受信に遅延が発生することがあります。**summary** パラメーターに対応しているバージョン以降では、**summary** パラメーターを指定して実施することを推奨します。
対象バージョン	1.03.03 1.09.03：**summary** パラメーター追加

使用例：メモリーバッファーの概略情報を表示する方法を示します。

```
# debug show memory-pool summary

NIC_DMA Detail:

MEMORY   NAME        BASE      SIZE MAX_REQ   ALLOC  BLKS    FREE N_FRE MAX_BLK
01E57500 NIC_DMA   0FF519C8   13254   12FDC   12FDC     7     244    1     244
--------------------------------------------------------------------------------
        <=32  <=64 <=128 <=256 <=512 <=1024 <=1536 <=2048 <=5120 <=10240 >10240
Alloc:     0     1     0     1     0     0      0      4      0      0       1
Free:      0     0     0     0     0     1      0      0      0      0       0

Alloc fail times 0.

ssl_lib Detail:

MEMORY   NAME        BASE      SIZE MAX_REQ   ALLOC  BLKS    FREE N_FRE MAX_BLK
01E57020 ssl_lib   0E94FA7C   4B000       0       0     0   4AFE4    1   4AFE4
--------------------------------------------------------------------------------
        <=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.

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

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
```

10.1.16 debug show netstat

debug show netstat	
目的	OS のメモリー使用量を表示します。
シンタックス	debug show netstat
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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。

項番	説明
(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。

10.1.17 debug show output

debug show output	
目的	モジュールのデバッグ状態と出力情報を表示します。
シンタックス	**debug show output**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
```

10.1.18 debug show ps

debug show ps	
目的	OS のプロセスを表示します。
シンタックス	**debug show ps**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.01

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。

10.1.19 debug show tcpstat

debug show tcpstat	
目的	TCP 接続の詳細情報を表示します。
シンタックス	**debug show tcpstat**
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	–
対象バージョン	1.03.03

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
```

10.1.20 debug show udpstat

debug show udpstat	
目的	UDP 接続の詳細情報を表示します。
シンタックス	**debug show udpstat**
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.03.03

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
```

10.1.21 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。
シンタックス	debug show wd-error-log
パラメーター	なし
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.04.01

使用例：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。

```
# 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
```

10.1.22 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。
シンタックス	**debug stack restart unit** *UNIT-ID* **stack-port** *PORTNO*
パラメーター	*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。 • ApresiaNP2000-24T4X, ApresiaNP2000-24T4X-PoE：25～28 • ApresiaNP2000-48T4X, ApresiaNP2000-48T4X-PoE：49～52
デフォルト	なし
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.07.01

使用例：ボックス ID 1 のスタックポート（ポート 27）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 27
#
```

10.1.23 show switching resource status

show switching resource status	
目的	ARP キャッシュ、ネイバーキャッシュ、IP/IPv6 マルチキャストを制御するスイッチ LSI リソースの使用状況を表示します。
シンタックス	**show switching resource status**
パラメーター	なし
デフォルト	なし
コマンドモード	特権実行モード、任意の設定モード

show switching resource status	
特権レベル	レベル：15
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.07.01

使用例：スイッチ LSI リソースの使用状況を表示する方法を示します。

```
# show switching resource status

hardware switching resource status:
                  (1)              (2)
                 required         used
  arp                   4            4
  ipv6 neighbor         0            0

  total                 4            4
  free                             4092
  -------------- -------- -----------
  ip multicast          0            0
  ipv6 multicast        0            0

  total                 0            0
  free                             1024
```

項番	説明
(1)	各機能で必要とされるリソースの数を表示します。
(2)	各機能で実際に割り当てられるリソースの数を表示します。

10.1.24 show tech-support

show tech-support	
目的	技術サポート情報を表示します。
シンタックス	**show tech-support** [*MODULE* | **system-dump** | **unit** *UNIT-ID* | **interface** {*INTERFACE-ID* [,|-] | **stack-port**} **system-dump**]
パラメーター	*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 • **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**：EthernetOAM 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 • **port-channel**：ポートチャネル機能 • **rmon**：RMON 機能

show tech-support	
	• **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 • **ztp**：ZTP 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** *INTERFACE-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**：物理ポートを指定します。複数指定できます。 • **stack-port**：スタックポートを指定します。
デフォルト	なし
コマンドモード	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。
制限事項	–
注意事項	**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。
対象バージョン	1.02.01 1.03.06：**stack** パラメーター、**interface** パラメーター追加 1.04.01：**unit** パラメーター追加 1.05.01：**poe** パラメーター追加 1.06.01：**system-dump** パラメーター追加 1.09.01：**ztp** 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

#-------------------------------------------------------------------------------
#                  ApresiaNP2000-48T4X Gigabit Ethernet Switch
#                         Technical Support Information
#
#                            Firmware: Build 1.09.01
#   Copyright(C) 2016  APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------


********************   Basic System Information   ********************

[SYS 2021-1-8 15:33:30]

Boot Time           : 8 Jan 2021  13:17:30
RTC Time            : 2021/01/08 06:33:30
Boot PROM Version   : Build 1.00.00
Firmware Version    : Build 1.09.01
```

```
Hardware Version    : A
Serial number       : 188780000003
MAC Address         : 00-40-66-B4-96-B5
MAC Address Number  : 53

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

#-------------------------------------------------------------------------------
#                  ApresiaNP2000-48T4X Gigabit Ethernet Switch
#                         Technical Support Information
#
#                            Firmware: Build 1.09.01
#   Copyright(C) 2016  APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------

[MMRP 2021-1-8 15:34:11]

##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

#-------------------------------------------------------------------------------
#                  ApresiaNP2000-48T4X Gigabit Ethernet Switch
#                         Technical Support Information
#
#                            Firmware: Build 1.09.01
#   Copyright(C) 2016  APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------

[ACCESS_DEFENDER 2021-1-8 15:34:26]


#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

#-------------------------------------------------------------------------------
#                  ApresiaNP2000-48T4X Gigabit Ethernet Switch
#                         Technical Support Information
#
#                            Firmware: Build 1.09.01
#   Copyright(C) 2016  APRESIA Systems, Ltd. All rights reserved.
#-------------------------------------------------------------------------------

[MEAR 2021-1-8 15:34:42]

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
```

10.2 エラー復旧コマンド

エラー復旧関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
errdisable recovery	errdisable recovery cause {all ｜ loop-detection ｜ storm-control ｜ uld} [interval SECONDS] no errdisable recovery cause {all ｜ loop-detection ｜ storm-control ｜ uld} [interval]
show errdisable recovery	show errdisable recovery

10.2.1 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。
シンタックス	**errdisable recovery cause {all ｜ loop-detection ｜ storm-control ｜ uld}** [interval *SECONDS*] **no errdisable recovery cause {all ｜ loop-detection ｜ storm-control ｜ uld}** [interval]
パラメーター	**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によって err-disabled 状態に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）：err-disabled 状態になってから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
コマンドモード	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	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によって err-disabled 状態にされたポートを、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)

errdisable recovery	
	また、いずれの機能の場合でも、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。
制限事項	-
注意事項	**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。
対象バージョン	1.01.01 1.07.01：**uld** 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のすべての機能によって err-disabled 状態に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)#
```

10.2.2 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。
シンタックス	**show errdisable recovery**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
---------------------------------------  -----------  -------------
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)	ポートを err-disabled 状態にする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
(2)	自動復旧設定の有効／無効を表示します。 enabled：有効 disabled：無効
(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 状態になっているポート番号を表示します。
(5)	err-disabled 状態になっているポートが復旧されるまでの残り時間を表示します。

10.3 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。

コマンド	コマンドとパラメーター
memory-error auto-recovery mode disable	memory-error auto-recovery mode disable no memory-error auto-recovery mode disable
memory-error auto-recovery notify disable	memory-error auto-recovery notify disable no memory-error auto-recovery notify disable
memory-error fault-action shutdown-all	memory-error fault-action shutdown-all no memory-error fault-action shutdown-all
clear memory-error	clear memory-error

10.3.1 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。
シンタックス	memory-error auto-recovery mode disable no memory-error auto-recovery mode disable
パラメーター	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）
コマンドモード	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になっている場合は、スイッチの大規模集積（LSI）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「異常」になります。 • 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 メモリーエラー自動復旧機能が無効になっている場合は、SW-LSI メモリーの状態、すべてのカウンター、およびメモリー領域の監視はリセットされます。
制限事項	-
注意事項	-
対象バージョン	1.03.01

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)#
```

10.3.2 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。
シンタックス	memory-error auto-recovery notify disable no memory-error auto-recovery notify disable
パラメーター	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）
コマンドモード	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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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)#
```

10.3.3 memory-error fault-action shutdown-all

memory-error fault-action shutdown-all	
目的	SW-LSI メモリーの状態が「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。
シンタックス	memory-error fault-action shutdown-all no memory-error fault-action shutdown-all
パラメーター	なし
デフォルト	無効
コマンドモード	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	memory-error fault-action shutdown-all コマンドを設定しない場合、SW-LSI メモリーの状態が「異常」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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：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を有効にする方法を示します。

```
# configure terminal
(config)# memory-error fault-action shutdown-all
(config)#
```

10.3.4 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。
シンタックス	clear memory-error
パラメーター	なし
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：15
ガイドライン	SW-LSI メモリーの状態が「正常」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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

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
#
```

10.4 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。

コマンド	コマンドとパラメーター
logging on	logging on no logging on
logging buffered	logging buffered [severity SEVERITY] [discriminator NAME] [write-delay {SECONDS ｜ infinite}] no logging buffered default logging buffered
logging console	logging console [severity SEVERITY] [discriminator NAME] no logging console
logging discriminator	logging discriminator NAME [facility {drops STRING ｜ includes STRING}] [severity {drops SEVERITY-LIST ｜ includes SEVERITY-LIST}] no logging discriminator NAME
logging server	logging server {IP-ADDRESS ｜ IPV6-ADDRESS} [severity SEVERITY] [facility FACILITY] [discriminator NAME] [port UDP-PORT] no logging server {IP-ADDRESS ｜ IPV6-ADDRESS}
logging source-interface	logging source-interface INTERFACE-ID no logging source-interface
command logging enable	command logging enable no 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。

コマンド	コマンドとパラメーター
show logging	show logging [all ｜ [REF-SEQ] [+ NN ｜ - NN]]
show logging sram	show logging sram
clear logging	clear logging

10.4.1 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。
シンタックス	logging on no logging on
パラメーター	なし
デフォルト	有効（logging on）
コマンドモード	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	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。

logging on	
	• 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。
制限事項	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。
注意事項	-
対象バージョン	1.01.01

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)#
```

10.4.2 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。
シンタックス	logging buffered [severity *SEVERITY*] [discriminator *NAME*] [write-delay {*SECONDS* | infinite}] no logging buffered default logging buffered
パラメーター	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 の範囲で指定します。0 が最も重要度が高いレベル(emergencies)で、7 が最も重要度が低いレベル(debugging)です。 • 名称指定の場合は emergencies(0)，alerts(1)，critical(2)，errors(3)，warnings(4)，notifications(5)，informational(6)，debugging(7) のいずれかを指定します。(数値)は対応するレベルで、名称指定の場合は入力不要です。 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周期的書き込み間隔を指定します。AEOS-NP2000 Ver. 1.06.01 以降では SRAM に、AEOS-NP2000 Ver. 1.05.01 以前ではフラッシュメモリーに保存されます。 *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。

logging buffered	
デフォルト	重要度：informational(6) 周期的書き込み間隔：0 秒（1.06.01 以降），300 秒（1.05.01 以前）
コマンドモード	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	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、AEOS-NP2000 Ver. 1.06.01 以降は SRAM に、AEOS-NP2000 Ver. 1.05.01 以前はフラッシュメモリーに保存されます。 以下の操作時には、AEOS-NP2000 Ver. 1.06.01 以降では SRAM とフラッシュメモリーの両方に、AEOS-NP2000 Ver. 1.05.01 以前はフラッシュメモリーに、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** コマンドによる設定保存 • **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。 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。
制限事項	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。
注意事項	コマンドシンタックスのパラメーター指定は順不同ではありません。パラメーターの指定は、シンタックス欄の記載順に指定してください。パラメーター省略時は、省略したパラメーター以降が指定できます。 重要度をレベル数値で指定して設定した場合でも、構成情報では名称で表示されます。
対象バージョン	1.01.01 1.06.01：動作対象とデフォルトの仕様変更

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)#
```

10.4.3 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。
シンタックス	**logging console** [**severity** *SEVERITY*] [**discriminator** *NAME*] **no logging console**
パラメーター	**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 の範囲で指定します。0 が最も重要度が高いレベル(emergencies)で、7 が最も重要度が低いレベル(debugging)です。 • 名称指定の場合は **emergencies**(0)，**alerts**(1)，**critical**(2)，**errors**(3)，**warnings**(4)，**notifications**(5)，**informational**(6)，**debugging**(7) のいずれかを指定します。(数値)は対応するレベルで、名称指定の場合は入力不要です。 **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
コマンドモード	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	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。
制限事項	–
注意事項	コマンドシンタックスのパラメーター指定は順不同ではありません。パラメーターの指定は、シンタックス欄の記載順に指定してください。パラメーター省略時は、省略したパラメーター以降が指定できます。

logging console	
	重要度をレベル数値で指定して設定した場合でも、構成情報では名称で表示されます。
対象バージョン	1.01.01

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)#
```

10.4.4 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。
シンタックス	**logging discriminator** *NAME* [**facility** {**drops** *STRING* ｜ **includes** *STRING*}] [**severity** {**drops** *SEVERITY-LIST* ｜ **includes** *SEVERITY-LIST*}] **no logging discriminator** *NAME*
パラメーター	*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, 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
コマンドモード	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	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。

logging discriminator	
	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。
制限事項	-
注意事項	コマンドシンタックスのパラメーター指定は順不同ではありません。パラメーターの指定は、シンタックス欄の記載順に指定してください。パラメーター省略時は、省略したパラメーター以降が指定できます。
対象バージョン	1.01.01

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)#
```

10.4.5 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。
シンタックス	**logging server** {*IP-ADDRESS* ｜ *IPV6-ADDRESS*} [**severity** *SEVERITY*] [**facility** *FACILITY*] [**discriminator** *NAME*] [**port** *UDP-PORT*] **no logging server** {*IP-ADDRESS* ｜ *IPV6-ADDRESS*}
パラメーター	*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。 **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 の範囲で指定します。0 が最も重要度が高いレベル(emergencies)で、7 が最も重要度が低いレベル(debugging)です。 • 名称指定の場合は **emergencies**(0)，**alerts**(1)，**critical**(2)，**errors**(3)，**warnings**(4)，**notifications**(5)，**informational**(6)，**debugging**(7) のいずれかを指定します。(数値)は対応するレベルで、名称指定の場合は入力不要です。 **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。指定しない場合は重要度は 23(local7) になります。 • 数字コード指定の場合は 0～23 の範囲で指定します。 • 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) のいずれかを指定します。(数値)は対応する数字コードで、名称指定の場合は入力不要です。 **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

logging server	
	ります。
デフォルト	なし
コマンドモード	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	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。
制限事項	SYSLOG サーバーは 4 個まで設定できます。
注意事項	コマンドシンタックスのパラメーター指定は順不同ではありません。パラメーターの指定は、シンタックス欄の記載順に指定してください。パラメーター省略時は、省略したパラメーター以降が指定できます。 重要度をレベル数値で指定して設定した場合でも、構成情報では名称で表示されます。 ファシリティを名称で指定して設定した場合でも、構成情報では数字コードで表示されます。
対象バージョン	1.01.01

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)#
```

10.4.6 logging source-interface

logging source-interface	
目的	SYSLOG パケットの送信元アドレスとして使用される IP アドレスが設定されたインターフェースを指定します。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。
シンタックス	**logging source-interface** *INTERFACE-ID* **no logging source-interface**
パラメーター	*INTERFACE-ID*：SYSLOG パケットの送信元アドレスとして使用される IP アドレスが設定されたインターフェースを、以下のパラメーターで指定します。

logging source-interface	
	• vlan：VLAN インターフェースを指定します。 • mgmt：マネージメントポートを指定します。
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
コマンドモード	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	-
制限事項	-
注意事項	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。
対象バージョン	1.01.01

使用例：SYSLOG パケットの送信元インターフェースに VLAN 100 インターフェースを設定する方法を示します。

```
# configure terminal
(config)# logging source-interface vlan 100
(config)#
```

10.4.7 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。
シンタックス	command logging enable no command logging enable
パラメーター	なし
デフォルト	有効（command logging enable）
コマンドモード	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	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。
制限事項	本コマンドは、構成情報では CLI コマンド（ラベル# CLI）で表示されます。
注意事項	-
対象バージョン	1.01.01

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)#
```

10.4.8 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。
シンタックス	show logging [all ｜ [*REF-SEQ*] [+ *NN* ｜ - *NN*]]
パラメーター	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。シーケンス番号を省略して、メッセージの数を指定した場合は、シーケンス番号 1 から表示されます。「+」の後にスペースを入力せずにメッセージの数を入力した場合は、無視されます。 + *NN*（省略可能）：*REF-SEQ* で指定したシーケンス番号の後に発生したメッセージの数を指定します。インデックスが指定されていない場合、バッファー内で最も古いメッセージから表示します。「+」と数字の間にスペースを入力する必要があります。 - *NN*（省略可能）：*REF-SEQ* で指定したシーケンス番号の前に発生したメッセージの数を指定します。インデックスが指定されていない場合、最後にバッファーに書き込まれたメッセージから表示します。「-」と数字の間にスペースを入力する必要があります。
デフォルト	なし
コマンドモード	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	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。 シーケンス番号に続く一定数のメッセージを表示するように指定した場合、最も古いメッセージが、より新しいメッセージの前に表示されます。シーケンス番号の前に、ある一定数のメッセージを表示するように指定した場合、より新しいメッセージが、より古いメッセージの前に表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：最新のシステムメッセージから最大 200 個の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)	システムメッセージを新しい順に表示します。

使用例：*REF-SEQ* パラメーターを指定してシステムメッセージを確認する場合の表示例を以下に示します。シーケンス番号 3 から開始して、最新のシステムメッセージまで表示されます。シーケンス番号 3 よりも古いシステムメッセージは表示されません。

```
# 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)	システムメッセージを新しい順に表示します。

使用例：*REF-SEQ* パラメーターおよび+ *NN* パラメーターを指定してシステムメッセージを確認する場合の表示例を以下に示します。シーケンス番号 2 から、4 個のシステムメッセージが表示されます。シーケンス番号 2 よりも古いシステムメッセージ、およびシーケンス番号 5 よりも新しいシステムメッセージは表示されません。

```
# 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)	システムメッセージを古い順に表示します。

使用例：*REF-SEQ* パラメーターおよび- *NN* パラメーターを指定してシステムメッセージを確認する場合の表示例を以下に示します。シーケンス番号 4 から逆順に、3 個のシステムメッセージが表示されます。シーケンス番号 2 よりも古いシステムメッセージ、およびシーケンス番号 4 よりも新しいシステムメッセージは表示されません。

```
# 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)	システムメッセージを新しい順に表示します。

10.4.9 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。
シンタックス	**show logging sram**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	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。AEOS-NP2000 Ver. 1.06.01 以降では、**logging buffered** コマンドによるローカルメッセージバッファーの周期的な保存先はフラッシュメモリーから SRAM に変更されているため、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。
注意事項	-
対象バージョン	1.06.01

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。

10.4.10 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のログメッセージを削除します。AEOS-NP2000 Ver. 1.06.01 以降では、SRAM に保存されたログメッセージも削除されます。
シンタックス	**clear logging**
パラメーター	なし

clear logging	
デフォルト	なし
コマンドモード	特権実行モード
特権レベル	レベル：12
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.01.01 1.06.01：動作対象の仕様変更

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
#
```

10.5 CPU 使用率監視コマンド

CPU 使用率監視関連のコマンドは以下のとおりです。

コマンド	コマンドとパラメーター
cpu-protect system-memory limit-check fault-action reboot	cpu-protect system-memory limit-check fault-action reboot no cpu-protect system-memory limit-check fault-action reboot
cpu-protect system-memory limit-check threshold	cpu-protect system-memory limit-check threshold [VALUE] no cpu-protect system-memory limit-check
cpu-protect trace trigger	cpu-protect trace trigger THRESHOLD [polling SECONDS] no cpu-protect trace trigger
snmp-server enable traps environment memory	snmp-server enable traps environment memory no snmp-server enable traps environment memory
snmp-server enable traps cpu-protect	snmp-server enable traps cpu-protect no snmp-server enable traps cpu-protect
show cpu-protect trace	show cpu-protect trace

10.5.1 cpu-protect system-memory limit-check fault-action reboot

cpu-protect system-memory limit-check fault-action reboot	
目的	AEOS-NP2000 Ver. 1.09.05 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-NP2000 Ver. 1.09.05 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。
シンタックス	**cpu-protect system-memory limit-check fault-action reboot** **no cpu-protect system-memory limit-check fault-action reboot**
パラメーター	なし
デフォルト	AEOS-NP2000 Ver. 1.09.05 より前のバージョン：無効
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.05.01 1.09.05：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-NP2000 Ver. 1.09.05 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)#
```

10.5.2 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。
シンタックス	**cpu-protect system-memory limit-check threshold** [*VALUE*] **no cpu-protect system-memory limit-check**
パラメーター	*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%
コマンドモード	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	AEOS-NP2000 Ver. 1.09.01 以降では、トラップを出力する場合には、**snmp-server enable traps environment memory** コマンドを有効（デフォルト設定）にする必要があります。
制限事項	-
注意事項	-
対象バージョン	1.05.01 1.09.05：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)#
```

10.5.3 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）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。
シンタックス	**cpu-protect trace trigger** *THRESHOLD* [**polling** *SECONDS*] **no cpu-protect trace trigger**
パラメーター	*THRESHOLD*：CPU 使用率のしきい値を、50～100(%)の範囲で指定します。 **polling** *SECONDS*（省略可能）：CPU 使用率の監視間隔を、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
コマンドモード	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	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-protect trace trigger	
制限事項	-
注意事項	ログおよびトラップの出力は、AEOS-NP2000 Ver. 1.08.01 以降でサポートしています。
対象バージョン	1.03.03 1.08.01：polling パラメーター追加

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)#
```

10.5.4 snmp-server enable traps environment memory

snmp-server enable traps environment memory	
目的	システムメモリー使用率監視機能の 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。
シンタックス	snmp-server enable traps environment memory no snmp-server enable traps environment memory
パラメーター	なし
デフォルト	有効（snmp-server enable traps environment memory）
コマンドモード	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	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。
制限事項	本コマンドは、構成情報ではデバイス関連（ラベル# DEVICE）で表示されます。
注意事項	-
対象バージョン	1.09.01

使用例：システムメモリー使用率監視機能の 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 environment memory
(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。
シンタックス	snmp-server enable traps cpu-protect no snmp-server enable traps cpu-protect
パラメーター	なし
デフォルト	無効
コマンドモード	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	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。
制限事項	-

snmp-server enable traps cpu-protect	
注意事項	-
対象バージョン	1.08.01

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。
シンタックス	**show cpu-protect trace**
パラメーター	なし
デフォルト	なし
コマンドモード	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	-
制限事項	-
注意事項	-
対象バージョン	1.03.03 1.08.01：表示項目の仕様変更

使用例：CPU 使用率監視のトレース状態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)
```

項番	説明
(1)	CPU 使用率監視機能の有効／無効を表示します。
(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 使用率の監視間隔を表示します。

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、RSA 鍵/DSA 鍵も削除されます。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 ApresiaNP2000-24T4X

Firmware: Build 1.07.01


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 ApresiaNP2000-24T4X

Firmware: Build 1.07.01

> 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-NP2000 Ver. 1.09 コマンドリファレンス

Copyright(c) 2020 APRESIA Systems, Ltd.

2020年11月 初版
2022年2月 第6版

APRESIA Systems株式会社
東京都中央区築地二丁目3番4号
築地第一長岡ビル
https://www.apresiasystems.co.jp/