

ApresiaNP4000 シリーズ

AEOS-NP4000 Ver. 1.02

コマンドリファレンス

**APRESIA Systems 株式会社**

制定・改訂履歴表

No.	年 月 日	内 容
-	2019 年 11 月 15 日	<ul style="list-style-type: none"> <li>• TD61-6769B AEOS-NP4000 Ver. 1.01 コマンドリファレンスより作成</li> <li>• 全章を対象に誤字・脱字・体裁を修正</li> <li>• 全章を対象にインターフェースパラメーターの説明、VLAN インターフェースのパラメーター表記を修正</li> <li>• 「1.1 本文中の表記について」に、インターフェースパラメーターの範囲指定の説明を追加</li> <li>• 「1.2 コマンドシンタックス」を修正</li> <li>• 「1.3 コンソールポートへの接続」を修正</li> <li>• 「1.8 インターフェースの表記法」を修正</li> <li>• 「1.9 VLAN インターフェース」を修正</li> <li>• 「2.1 インターフェースコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- interface を修正</li> <li>- interface range を修正</li> <li>- description の目的、使用例を修正</li> <li>- show interfaces を修正</li> <li>- show interfaces counters のパラメーター、ガイドラインを修正</li> <li>- show interfaces gbic を修正</li> <li>- show interfaces description のパラメーターを修正</li> <li>- show interfaces transceiver を修正</li> <li>- show counters の使用例を修正</li> </ul> </li> <li>• 「2.2 ポート設定コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- speed の注意事項を追加</li> <li>- duplex の注意事項を追加</li> <li>- speed_duplex (mgmt 0)の注意事項を追加</li> </ul> </li> <li>• 「2.4 省電力イーサネット(EEE)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show eee のパラメーターを修正</li> </ul> </li> <li>• 「2.5 スタックコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- stack preempt の制限事項を修正</li> <li>- show stack のガイドラインを追加</li> </ul> </li> <li>• 「3.1 基本 CLI コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show version の使用例を修正、対象バージョンを追加</li> <li>- show environment の使用例を修正</li> <li>- show unit を修正</li> </ul> </li> <li>• 「3.2 ファイルシステムコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show storage media-info を修正</li> </ul> </li> <li>• 「3.3 ターミナルコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- terminal speed を修正</li> </ul> </li> <li>• 「3.5 基本 IPv4 コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip address を修正</li> <li>- ip proxy-arp の目的、ガイドラインを修正</li> <li>- ip local-proxy-arp を修正</li> <li>- ip mtu を追加</li> <li>- arp の制限事項を修正</li> <li>- show ip interface のパラメーター、使用例を修正</li> <li>- show arp を修正</li> <li>- show arp timeout のパラメーター、使用例を修正</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- clear arp-cache のパラメーターを修正</li> <li>• 「3.6 基本 IPv6 コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ipv6 address の制限事項、使用例を修正</li> <li>- ipv6 address eui-64 の制限事項を修正</li> <li>- ipv6 address dhcp の制限事項を修正</li> <li>- ipv6 address autoconfig の制限事項を修正</li> <li>- ipv6 hop-limit を追加</li> <li>- ipv6 mtu を追加</li> <li>- ipv6 nd suppress-ra を追加</li> <li>- ipv6 nd managed-config-flag を追加</li> <li>- ipv6 nd other-config-flag を追加</li> <li>- ipv6 nd prefix を追加</li> <li>- ipv6 nd ra interval を追加</li> <li>- ipv6 nd ra lifetime を追加</li> <li>- ipv6 nd reachable-time を追加</li> <li>- ipv6 nd ns-interval を修正</li> <li>- ipv6 neighbor の制限事項を修正</li> <li>- show ipv6 interface のパラメーター、使用例を修正</li> <li>- show ipv6 neighbors の使用例を修正</li> <li>- clear ipv6 neighbors のパラメーターを修正</li> </ul> </li> <li>• 「3.9 システムファイル管理コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip tftp source-interface を修正</li> <li>- ip ftp source-interface を修正</li> <li>- show boot を修正</li> <li>- show running-config のパラメーターを修正</li> <li>- show config differences の追加</li> <li>- backup clone のガイドラインを修正</li> <li>- write の注意事項を修正</li> <li>- reboot のパラメーターを修正、ガイドラインを追加</li> <li>- copy のパラメーターを削除</li> <li>- backup のガイドラインを修正</li> <li>- restore のガイドライン、使用例を修正</li> </ul> </li> <li>• 「4.1 DHCP クライアントコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip dhcp client client-id を修正</li> </ul> </li> <li>• 「4.2 DHCP サーバーコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip dhcp pool の制限事項を修正</li> <li>- lease のシンタックスを修正</li> </ul> </li> <li>• 「4.3 DHCPv6 クライアントコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show ipv6 dhcp interface の目的、使用例を修正</li> </ul> </li> <li>• 「4.4 DHCPv6 サーバーコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- address prefix のパラメーターを修正</li> </ul> </li> <li>• 「4.8 TELNET コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip telnet source-interface の注意事項を追加</li> </ul> </li> <li>• 「4.9 SSH コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show ip ssh の使用例を修正</li> </ul> </li> <li>• 「4.12 SNMP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- snmp-server name を修正</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- snmp-server enable traps environment のシンタックスを修正</li> <li>- snmp-server source-interface traps の注意事項を追加</li> <li>- show snmp-server を修正</li> <li>- show snmp を削除</li> <li>- show snmp community を追加</li> <li>- show snmp host を追加</li> <li>- show snmp-server traps を追加</li> <li>- show snmp user の使用例を修正</li> <li>- show snmp group を追加</li> <li>- show snmp view を追加</li> <li>- show snmp engineID を追加</li> <li>• 「4.13 ミラーリングコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- monitor session destination interface を修正</li> <li>- monitor session destination remote vlan を修正</li> <li>- monitor session source interface を修正</li> <li>- monitor session source acl を修正</li> <li>- monitor session source remote vlan を修正</li> <li>- remote-span を修正</li> <li>- no monitor session のパラメーター、ガイドラインを修正</li> <li>- show monitor session を修正</li> </ul> </li> <li>• 「4.14 LLDP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- lldp dot1-tlv-select を修正</li> <li>- lldp dot3-tlv-select を修正</li> <li>- lldp fast-count を修正</li> <li>- lldp hold-multiplier を修正</li> <li>- lldp management-address を修正</li> <li>- lldp med-tlv-select を修正</li> <li>- lldp receive を修正</li> <li>- lldp reinit を修正</li> <li>- lldp run を修正</li> <li>- lldp forward を修正</li> <li>- lldp tlv-select を修正</li> <li>- lldp transmit を修正</li> <li>- lldp tx-delay を修正</li> <li>- lldp tx-interval を修正</li> <li>- lldp subtype port-id を修正</li> <li>- lldp err-disable の使用例を修正</li> <li>- lldp notification enable を修正</li> <li>- lldp med notification enable を追加</li> <li>- snmp-server enable traps lldp を修正</li> <li>- snmp-server enable traps lldp med を追加</li> <li>- show lldp の使用例を修正</li> <li>- show lldp interface の目的、使用例を修正</li> <li>- show lldp local interface を修正</li> <li>- show lldp management-address を修正</li> <li>- show lldp neighbors interface を修正</li> <li>- show lldp traffic の目的、使用例を修正</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- show lldp traffic interface を修正</li> <li>- clear lldp table を修正</li> <li>- clear lldp counters を修正</li> <li>• 「5.1 FDB コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- mac-address-table learning のパラメーターを修正</li> </ul> </li> <li>• 「5.2 ジャンボフレームコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- max-rcv-frame-size の注意事項を修正</li> </ul> </li> <li>• 「5.3 ポートチャンネルコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- channel-group のパラメーターを修正</li> </ul> </li> <li>• 「5.4 ポートリダンダントコマンド」を追加</li> <li>• 「5.6 ループ検知コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- loop-detection global enable の制限事項を修正</li> <li>- loop-detection enable (Interface) の制限事項を修正</li> <li>- loop-detection mode のガイドラインを修正、制限事項を追加</li> <li>- loop-detection vlan を修正</li> <li>- loop-detection action notify-only を追加</li> <li>- loop-detection no-check-src を追加</li> <li>- show loop-detection を修正</li> </ul> </li> <li>• 「5.7 ストームコントロールコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- storm-control の使用例を修正</li> <li>- show storm-control のパラメーター、使用例を修正</li> </ul> </li> <li>• 「5.9 IGMP スヌーピングコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip igmp snooping を修正</li> <li>- ip igmp snooping (VLAN) を追加</li> </ul> </li> <li>• 「5.10 MLD スヌーピングコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ipv6 mld snooping を修正</li> <li>- ipv6 mld snooping (VLAN) を追加</li> <li>- ipv6 mld snooping proxy-reporting のガイドラインを削除</li> <li>- show ipv6 mld snooping statistics の使用例を修正</li> </ul> </li> <li>• 「5.11 リングプロテクション(ERPS)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- port0 のパラメーター、制限事項を修正</li> <li>- port1 のパラメーター、制限事項を修正</li> <li>- rpl のシンタックス、パラメーターを修正</li> </ul> </li> <li>• 「5.12 MMRP-Plus コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- mmrp-plus enable の制限事項を修正</li> <li>- mmrp-plus ring ring-master の制限事項を修正</li> <li>- mmrp-plus ring divided-master の制限事項を修正</li> <li>- mmrp-plus ring divided-slave の制限事項を修正</li> <li>- mmrp-plus ring aware の制限事項を修正</li> <li>- show mmrp-plus configuration の使用例を修正</li> <li>- show mmrp-plus configuration ring の使用例を修正</li> <li>- debug mmrp のコマンドモードを修正</li> </ul> </li> <li>• 「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 <ul style="list-style-type: none"> <li>- spanning-tree global state の制限事項を修正</li> <li>- spanning-tree mode の制限事項を追加</li> <li>- spanning-tree state の制限事項を修正</li> <li>- spanning-tree link-type を修正</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- spanning-tree portfast のガイドラインを修正</li> <li>- show spanning-tree の使用例を修正</li> <li>- show spanning-tree configuration interface の使用例を修正</li> <li>- show spanning-tree mst の使用例を修正</li> <li>• 「5.14 RPVST+コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- spanning-tree vlan の制限事項を修正</li> <li>- show spanning-tree vlan の使用例を修正</li> <li>- show spanning-tree vlan interface の使用例を修正</li> </ul> </li> <li>• 「5.15 トラフィックセグメンテーションコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- traffic-segmentation forward のパラメーターを修正</li> </ul> </li> <li>• 「5.16 VLAN コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- switchport mode のガイドラインを修正</li> <li>- protocol-vlan profile (Interface) のシンタックスを修正</li> </ul> </li> <li>• 「5.18 VLAN トンネルコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- dot1q inner ethertype の目的、ガイドラインを修正</li> <li>- dot1q tunneling ethertype を修正</li> <li>- switchport vlan mapping を修正</li> <li>- vlan mapping profile を修正</li> <li>- vlan mapping rule を修正</li> <li>- switchport vlan mapping profile を修正</li> <li>- vlan mapping miss drop を修正</li> <li>- dot1q-tunnel trust inner-priority を修正</li> <li>- dot1q-tunnel insert dot1q-tag を修正</li> <li>- show dot1q ethertype を修正</li> <li>- show vlan mapping を修正</li> <li>- show dot1q-tunnel を修正</li> <li>- show vlan mapping profile を修正</li> </ul> </li> <li>• 「6.1 プロトコル非依存コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip route を修正</li> <li>- ipv6 route の制限事項、使用例を修正</li> </ul> </li> <li>• 「7.1 優先制御(QoS)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- priority-queue cos-map を修正</li> <li>- mls qos scheduler を修正</li> <li>- wrr-queue bandwidth を修正</li> <li>- wdrr-queue bandwidth を修正</li> <li>- mls qos trust を修正</li> <li>- mls qos cos を修正</li> <li>- mls qos map dscp-cos を修正</li> <li>- mls qos map cos-color を修正</li> <li>- mls qos map dscp-color を修正</li> <li>- mls qos dscp-mutation を修正</li> <li>- mls qos map dscp-mutation を修正</li> <li>- set を修正</li> <li>- show mls qos interface を修正</li> <li>- show mls qos queueing を修正</li> <li>- show mls qos map dscp-mutation の目的、使用例を修正</li> <li>- show policy-map のパラメーターを修正</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>• 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- access-list resequence を修正</li> <li>- expert access-group の制限事項を修正</li> <li>- permit   deny (expert access-list)を修正</li> <li>- ip access-group の制限事項を修正</li> <li>- permit   deny (ip access-list)を修正</li> <li>- ipv6 access-group の制限事項を修正</li> <li>- permit   deny (ipv6 access-list)を修正</li> <li>- mac access-group の制限事項を修正</li> <li>- permit   deny (mac access-list)を修正</li> <li>- vlan access-map のガイドラインを修正</li> <li>- action のパラメーターを修正</li> <li>- show access-group のパラメーターを修正</li> <li>- show access-list resource reserved-group を追加</li> <li>- show access-list resource reserved-priority を追加</li> </ul> </li> <li>• 「9.1 AccessDefender 共通コマンド」を追加</li> <li>• 「9.2 認証、許可、アカウントिंग(AAA)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- aaa accounting network を追加</li> <li>- aaa authentication control sufficient を修正</li> <li>- aaa authentication dot1x を追加</li> <li>- aaa authentication mac-auth を追加</li> <li>- aaa authentication web-auth を追加</li> <li>- aaa default class を追加</li> <li>- show radius statistics の使用例を修正</li> </ul> </li> <li>• 「9.3 MAC 認証コマンド」を追加</li> <li>• 「9.4 IEEE 802.1X 認証コマンド」を追加</li> <li>• 「9.5 SSL コマンド」を追加</li> <li>• 「9.6 Web 認証コマンド」を追加</li> <li>• 「9.7 DHCP スヌーピングコマンド」を追加</li> <li>• 「10.1 デバッグコマンド」の以下のコマンドを修正 <ul style="list-style-type: none"> <li>- debug show access-defender internal-resource を追加</li> <li>- debug show inetstat を追加</li> <li>- debug show memory-pool を追加</li> <li>- debug show tcpstat を追加</li> <li>- debug show udpstat を追加</li> <li>- show tech-support を修正</li> </ul> </li> <li>• 「10.2 エラー復旧コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- errdisable recovery を修正</li> <li>- show errdisable recovery の使用例を修正</li> </ul> </li> <li>• 「10.4 システムログコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- logging on の制限事項を修正</li> <li>- logging buffered を修正</li> <li>- logging source-interface の注意事項を追加</li> <li>- command logging enable のガイドラインを修正</li> <li>- show logging の目的を修正</li> <li>- show logging sram を追加</li> <li>- show attack-logging を削除</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- clear logging の注意事項、対象バージョンを追加</li> <li>- clear attack-logging を削除</li> <li>• 「10.5 CPU 使用率監視コマンド」を追加</li> <li>• 「11.1 システム復旧手順(パスワードのリセット)」を修正</li> </ul>
A	2020 年 4 月 28 日	<ul style="list-style-type: none"> <li>• 全章を対象に誤字・脱字・体裁を修正</li> <li>• 全章を対象にインターフェース設定モードの記載を見直し</li> <li>• 制定・改訂来歴表を修正</li> <li>• 「1.4 初めての CLI への接続」を修正</li> <li>• 「1.6 ユーザーアカウントの作成」を修正</li> <li>• 「1.7 コマンドモード」を修正</li> <li>• 「1.11 コマンド入力の補助機能」を追加</li> <li>• 「1.12 表示結果出力修飾子」を追加</li> <li>• 「2.1 インターフェースコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- shutdown のガイドラインを修正</li> </ul> </li> <li>• 「2.2 ポート設定コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- speed を修正</li> <li>- duplex を修正</li> </ul> </li> <li>• 「2.3 アラーム LED コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- alarm warn-led state enable のガイドラインを修正</li> </ul> </li> <li>• 「2.4 省電力イーサネット (EEE) コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- eee のガイドラインを削除、制限事項を追加</li> </ul> </li> <li>• 「2.5 スタックコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- stack bandwidth の制限事項を修正</li> </ul> </li> <li>• 「3.1 基本 CLI コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- login (EXEC) の目的、ガイドラインを修正</li> </ul> </li> <li>• 「3.4 アクセス管理コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- service user-account encryption を修正</li> <li>- session-timeout を修正</li> </ul> </li> <li>• 「3.5 基本 IPv4 コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip address のシンタックスを修正</li> </ul> </li> <li>• 「3.6 基本 IPv6 コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show ipv6 neighbors の使用例を修正</li> </ul> </li> <li>• 「3.8 Gratuitous ARP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- arp gratuitous-send の対象バージョンを追加</li> </ul> </li> <li>• 「3.9 システムファイル管理コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- backup clone のガイドラインを修正、注意事項を追加</li> <li>- configure replace のシンタックスを修正</li> </ul> </li> <li>• 「4.2 DHCP サーバーコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- class (DHCP Server) を修正</li> <li>- address range を修正</li> <li>- option のパラメーターを修正</li> <li>- ip dhcp class のガイドライン、使用例を修正</li> <li>- option hex を修正</li> <li>- ip dhcp use class を修正</li> <li>- ip dhcp ping packets を修正</li> <li>- ip dhcp ping timeout を修正</li> <li>- show ip dhcp binding のガイドライン、使用例を修正</li> </ul> </li> </ul>



No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- show ip dhcp conflict を修正</li> <li>- clear ip dhcp binding を修正</li> <li>- clear ip dhcp conflict を修正</li> <li>• 「4.8 TELNET コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show ip telnet server を追加</li> <li>- telnet の使用例を修正</li> </ul> </li> <li>• 「4.10 RMON コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- rmon collection stats の制限事項を追加</li> <li>- rmon collection history の制限事項を追加</li> </ul> </li> <li>• 「4.12 SNMP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- snmp-server host のガイドラインを修正</li> <li>- snmp-server user のシンタックスを修正</li> </ul> </li> <li>• 「4.14 LLDP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show lldp traffic の使用例を修正</li> </ul> </li> <li>• 「4.17 CFM コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- cfm mep の注意事項を追加</li> </ul> </li> <li>• 「5.3 ポートチャネルコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- channel-group の注意事項を削除</li> <li>- lacp timeout の注意事項を削除</li> </ul> </li> <li>• 「5.4 ポートリダンダントコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- redundant group-number のガイドラインを追加、制限事項を修正</li> <li>- redundant group-number preempt のガイドラインを修正</li> <li>- redundant mac-address-table-update を修正</li> <li>- redundant fdb-flush send enable の目的を修正</li> </ul> </li> <li>• 「5.6 ループ検知コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- loop-detection enable (Interface) のガイドラインを修正</li> <li>- loop-detection action notify-only のガイドラインを修正</li> <li>- loop-detection no-check-src のガイドラインを修正</li> </ul> </li> <li>• 「5.7 ストームコントロールコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- storm-control の制限事項を修正</li> </ul> </li> <li>• 「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 <ul style="list-style-type: none"> <li>- multicast filtering-mode の目的、パラメーターを修正</li> </ul> </li> <li>• 「5.9 IGMP スヌーピングコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip igmp snooping mrouter のガイドラインを修正、注意事項を追加</li> </ul> </li> <li>• 「5.10 MLD スヌーピングコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ipv6 mld snooping mrouter のガイドラインを修正、注意事項を追加</li> </ul> </li> <li>• 「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 <ul style="list-style-type: none"> <li>- spanning-tree state のガイドラインを追加</li> <li>- spanning-tree cost のガイドラインを追加</li> <li>- spanning-tree guard root のガイドラインを追加</li> <li>- spanning-tree link-type のガイドラインを追加</li> <li>- spanning-tree portfast のガイドラインを修正</li> <li>- spanning-tree port-priority のガイドラインを追加</li> <li>- spanning-tree tcnfilter のガイドラインを追加</li> <li>- spanning-tree forward-bpdu のガイドラインを追加</li> <li>- spanning-tree mst hello-time のガイドラインを追加</li> <li>- spanning-tree mst のガイドラインを修正</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- show spanning-tree mst の使用例を修正</li> <li>• 「5.14 RPVST+コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- spanning-tree vlan cost のガイドラインを修正</li> <li>- spanning-tree vlan port-priority のガイドラインを修正</li> </ul> </li> <li>• 「5.15 トラフィックセグメンテーションコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- traffic-segmentation forward を修正</li> <li>- show traffic-segmentation forward の目的、使用例を修正</li> </ul> </li> <li>• 「5.16 VLAN コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- switchport mode のガイドラインを追加</li> <li>- switchport access vlan のガイドラインを追加</li> <li>- switchport trunk allowed vlan を修正</li> <li>- switchport trunk native vlan のガイドラインを追加</li> <li>- switchport hybrid allowed vlan を修正</li> <li>- switchport hybrid native vlan のガイドラインを追加</li> <li>- protocol-vlan profile を修正</li> <li>- protocol-vlan profile (Interface) を修正</li> <li>- acceptable-frame のガイドラインを追加</li> <li>- ingress-checking のガイドラインを追加</li> <li>- show protocol-vlan を修正</li> </ul> </li> <li>• 「5.17 プライベート VLAN コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- switchport mode private-vlan のガイドラインを追加</li> <li>- switchport private-vlan host-association のガイドラインを追加</li> <li>- switchport private-vlan mapping のガイドラインを追加</li> </ul> </li> <li>• 「5.18 VLAN トンネルコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- dot1q tunneling ethertype のガイドラインを修正</li> <li>- switchport vlan mapping のガイドラインを追加</li> <li>- vlan mapping profile のシンタックスを修正</li> <li>- switchport vlan mapping profile のガイドラインを修正</li> <li>- vlan mapping miss drop のガイドラインを修正</li> <li>- dot1q-tunnel trust inner-priority のガイドラインを修正</li> <li>- dot1q-tunnel insert dot1q-tag のガイドラインを修正</li> </ul> </li> <li>• 「6.1 プロトコル非依存コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip route のシンタックスを修正</li> <li>- ipv6 route のシンタックスを修正</li> </ul> </li> <li>• 「7.1 優先制御(QoS) コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- packet-buffer mode を追加</li> <li>- mls qos trust のガイドラインを修正</li> <li>- mls qos cos のガイドラインを修正</li> </ul> </li> <li>• 「7.2 WRED コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- random-detect のシンタックス、パラメーターを修正</li> <li>- random-detect profile を修正</li> <li>- show random-detect profile を修正</li> </ul> </li> <li>• 「8.1 アクセスリスト(ACL) コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- acl-hardware-counter の制限事項を追加</li> <li>- action の注意事項を追加</li> </ul> </li> <li>• 「9.1 AccessDefender 共通コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- copy (AccessDefender) のガイドラインを修正、注意事項を追加</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- access-defender erase の注意事項を追加</li> <li>• 「10.4 システムログコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- logging buffered のガイドラインを修正</li> <li>- show logging sram の制限事項を追加</li> <li>- clear logging の目的、注意事項を修正</li> </ul> </li> </ul>
B	2020年9月30日	<ul style="list-style-type: none"> <li>• 全章を対象に no コマンドの記載を見直し</li> <li>• 全章を対象に誤字・脱字・体裁を修正</li> <li>• 「2.1 インターフェースコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show interfaces の制限事項を追加</li> <li>- show interfaces counters の制限事項を追加</li> <li>- show interfaces status の制限事項を追加</li> <li>- show interfaces utilization の制限事項を追加</li> <li>- show interfaces gbic の制限事項を追加</li> <li>- show interfaces description の制限事項を追加</li> <li>- show interfaces auto-negotiation の制限事項を追加</li> <li>- show interfaces transceiver の制限事項を追加</li> <li>- show counters の使用例を修正</li> </ul> </li> <li>• 「2.2 ポート設定コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- mdix を修正</li> </ul> </li> <li>• 「3.1 基本 CLI コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show environment の使用例を修正</li> </ul> </li> <li>• 「3.4 アクセス管理コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- access-class を修正</li> <li>- login (Line)のガイドラインを修正</li> </ul> </li> <li>• 「3.7 IP ユーティリティーコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ping access-class を修正</li> </ul> </li> <li>• 「3.9 システムファイル管理コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- copy のガイドライン、使用例を修正</li> <li>- restore のガイドラインを修正</li> </ul> </li> <li>• 「4.2 DHCP サーバーコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show ip dhcp pool を修正</li> <li>- show ip dhcp server を修正</li> <li>- show ip dhcp server statistics の使用例を修正</li> </ul> </li> <li>• 「4.4 DHCPv6 サーバーコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ipv6 dhcp pool の注意事項を追加</li> <li>- address prefix の注意事項を追加</li> <li>- address-assignment の注意事項を追加</li> <li>- domain-name (DHCPv6 Server)の注意事項を追加</li> <li>- dns-server (DHCPv6 Server)の注意事項を追加</li> <li>- prefix-delegation pool の注意事項を追加</li> <li>- prefix-delegation の注意事項を追加</li> <li>- ipv6 dhcp excluded-address の注意事項を追加</li> <li>- ipv6 local pool の注意事項を追加</li> <li>- ipv6 dhcp server の注意事項を追加</li> <li>- show ipv6 dhcp binding を修正</li> <li>- show ipv6 dhcp pool を修正</li> <li>- show ipv6 excluded-address の目的、使用例を修正</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- show ipv6 local pool を修正</li> <li>- show ipv6 dhcp operation の使用例を修正</li> <li>- clear ipv6 dhcp binding を修正</li> <li>• 「4.6 時刻および SNTP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- clock set を修正</li> <li>- clock summer-time を修正</li> <li>- clock timezone を修正</li> <li>- sntp server を修正</li> <li>- sntp interval を修正</li> <li>- sntp enable のガイドラインを追加</li> <li>- show clock のガイドライン、使用例を修正</li> <li>- show sntp の使用例を修正</li> </ul> </li> <li>• 「4.7 NTP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ntp server を修正</li> <li>- ntp peer を修正</li> <li>- ntp update-calendar を修正</li> <li>- ntp authenticate を修正</li> <li>- ntp authentication-key を修正</li> <li>- ntp trusted-key を修正</li> <li>- ntp control-key を修正</li> <li>- ntp request-key を修正</li> <li>- ntp disable を修正</li> <li>- ntp access-group を修正</li> <li>- ntp max-associations を修正</li> <li>- ntp master を修正</li> <li>- service ntp のガイドライン、制限事項を追加</li> <li>- show ntp associations を修正</li> <li>- show ntp status の使用例を修正</li> </ul> </li> <li>• 「4.9 SSH コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show crypto key mypubkey の使用例を修正</li> <li>- crypto key generate を修正</li> <li>- crypto key zeroize のガイドライン、使用例を修正</li> </ul> </li> <li>• 「4.12 SNMP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- snmp-server community を修正</li> <li>- snmp-server trap-sending disable を修正</li> <li>- snmp trap link-status を修正</li> <li>- snmp-server user を修正</li> <li>- snmp-server group のパラメーター、制限事項を修正</li> <li>- show snmp-server trap-sending を修正</li> <li>- show snmp trap link-status を修正</li> </ul> </li> <li>• 「4.13 ミラーリングコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- monitor session source interface の制限事項を追加</li> </ul> </li> <li>• 「4.16 単方向リンク検出(ULD)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- uld enable を修正</li> <li>- uld action を修正</li> <li>- uld discovery-time を修正</li> <li>- errdisable recovery cause uld を追加</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- show uld の使用例を修正</li> <li>• 「4.17 CFM コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- fault-alarm のデフォルトを修正</li> <li>- mip creation (MD) のデフォルトを修正</li> <li>- sender-id (MD) のデフォルトを修正</li> </ul> </li> <li>• 「5.9 IGMP スヌーピングコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip igmp snooping querier の制限事項を追加</li> </ul> </li> <li>• 「5.6 ループ検知コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- loop-detection mode のガイドラインを修正</li> <li>- errdisable recovery cause loop-detection を追加</li> </ul> </li> <li>• 「5.7 ストームコントロールコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- storm-control を修正</li> <li>- storm-control action を追加</li> <li>- storm-control polling を削除</li> <li>- storm-control polling interval を追加</li> <li>- storm-control polling retries を追加</li> <li>- errdisable recovery cause storm-control を追加</li> <li>- show storm-control を修正</li> </ul> </li> <li>• 「5.12 MMRP-Plus コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- mmrp-plus switch hello-interval の注意事項を追加</li> <li>- mmrp-plus switch polling-rate の制限事項を削除、注意事項を追加</li> <li>- mmrp-plus ring vid の注意事項を追加</li> <li>- mmrp-plus ring ring-master の制限事項を追加</li> <li>- mmrp-plus ring divided-master の制限事項を追加</li> <li>- mmrp-plus ring divided-slave の制限事項を追加</li> <li>- mmrp-plus ring fdb-flush timer の注意事項を追加</li> <li>- mmrp-plus ring listening-timer の注意事項を追加</li> <li>- mmrp-plus ring hello-timeout の注意事項を追加</li> </ul> </li> <li>• 「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 <ul style="list-style-type: none"> <li>- spanning-tree mode の注意事項を追加</li> </ul> </li> <li>• 「5.15 トラフィックセグメンテーションコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- traffic-segmentation forward の制限事項を追加</li> </ul> </li> <li>• 「7.1 優先制御(QoS)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- packet-buffer mode の対象バージョンを修正</li> <li>- rate-limit input を追加</li> <li>- rate-limit output を追加</li> <li>- match のガイドラインを修正</li> </ul> </li> <li>• 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- acl-hardware-counter のパラメーターを修正</li> <li>- permit   deny (expert access-list) の「拡張エキスパートアクセスリストの抽出条件」を修正</li> <li>- permit   deny (ip access-list) の「IP アクセスリストの抽出条件」を修正</li> <li>- permit   deny (ipv6 access-list) の「IPv6 アクセスリストの抽出条件」を修正</li> <li>- show access-list resource reserved-priority のガイドラインを追加</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- clear acl-hardware-counter のパラメーターを修正</li> <li>• 「9.1 AccessDefender 共通コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- access-defender の制限事項を追加</li> <li>- aaa-local-db user のパラメーターを修正</li> <li>- access-defender static mac を修正</li> <li>- authentication advanced-vlan-setting を修正</li> <li>- authentication interface を修正</li> <li>- logout aging-time を修正</li> <li>- logout clock を修正</li> <li>- logout linkdown disable interface を修正</li> <li>- logout linkdown time のガイドラインを修正</li> <li>- logout linkdown time enable interface のガイドラインを修正</li> <li>- logout ping dst-ip を修正</li> <li>- logout ping ttl を修正</li> <li>- logout timeout を修正</li> <li>- total-client を修正</li> <li>- vlan mode を修正</li> <li>- show access-defender client を修正</li> <li>- show access-defender deny の使用例を修正</li> <li>- show access-defender port-configuration の使用例を修正</li> <li>- show access-defender port-channel-configuration の使用例を修正</li> <li>- show access-defender rule-statistics の使用例を修正</li> <li>- copy (AccessDefender)を修正</li> <li>- access-defender deny を修正</li> <li>- access-defender logout を修正</li> </ul> </li> <li>• 「9.3 MAC 認証コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- mac-authentication enable を修正</li> <li>- mac-authentication discard-time のガイドラインを修正</li> <li>- mac-authentication password を修正</li> <li>- mac-authentication username mac-format のガイドラインを追加</li> </ul> </li> <li>• 「9.4 IEEE 802.1X 認証コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- dot1x enable を修正</li> <li>- dot1x ignore-eapol-start interface を修正</li> <li>- show access-defender dot1x を修正</li> <li>- show access-defender dot1x interface を追加</li> </ul> </li> <li>• 「9.6 Web 認証コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- web-authentication enable を修正</li> <li>- web-authentication http-port を修正</li> <li>- web-authentication https-port を修正</li> <li>- web-authentication redirect disable のデフォルトを修正</li> <li>- web-authentication redirect proxy-port を修正</li> <li>- web-authentication snooping proxy-port を修正</li> </ul> </li> <li>• 「9.7 DHCP スヌーピングコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- dhcp-snooping enable を修正</li> <li>- dhcp-snooping interface の制限事項を修正</li> <li>- dhcp-snooping mode deny のガイドラインを修正</li> <li>- dhcp-snooping mode timer のパラメーターを修正</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- dhcp-snooping mode mac-authentication のガイドラインを修正</li> <li>- dhcp-snooping static-entry の制限事項を修正、注意事項を追加</li> <li>- show access-defender dhcp-snooping configuration の使用例を修正</li> <li>- show access-defender dhcp-snooping status の使用例を修正</li> <li>• 「10.2 エラー復旧コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- errdisable recovery を修正</li> <li>- show errdisable recovery の目的、使用例を修正</li> </ul> </li> <li>• 「10.3 メモリーエラー自動復旧コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- memory-error auto-recovery mode disable のデフォルトを修正</li> <li>- memory-error auto-recovery notify disable のデフォルトを修正</li> <li>- memory-error fault-action shutdown-all のガイドラインを追加</li> </ul> </li> </ul>
C	2020 年 10 月 2 日	<ul style="list-style-type: none"> <li>• 「2.2 ポート設定コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- mdix のパラメーターを修正</li> </ul> </li> </ul>
D	2021 年 2 月 26 日	<ul style="list-style-type: none"> <li>• 全章を対象に誤字・脱字・体裁を修正</li> <li>• 制定・改訂来歴表を修正</li> <li>• 「1.2 コマンドシンタックス」を修正</li> <li>• 「2.1 インターフェースコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- interface を修正</li> <li>- interface range のパラメーターを修正</li> </ul> </li> <li>• 「2.2 ポート設定コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- speed を修正</li> <li>- duplex を修正</li> <li>- speed_duplex (mgmt 0)を修正</li> </ul> </li> <li>• 「3.3 ターミナルコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- terminal length default のガイドラインを修正</li> <li>- terminal width default のガイドラインと使用例を修正</li> <li>- terminal length を修正</li> <li>- terminal width の使用例を修正</li> </ul> </li> <li>• 「3.4 アクセス管理コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- login (Line)を修正</li> </ul> </li> <li>• 「3.5 基本 IPv4 コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip address の目的とパラメーターを修正</li> <li>- arp を修正</li> <li>- show arp を修正</li> </ul> </li> <li>• 「3.6 基本 IPv6 コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ipv6 address を修正</li> <li>- ipv6 address eui-64 を修正</li> <li>- ipv6 address dhcp を修正</li> <li>- ipv6 address autoconfig を修正</li> <li>- ipv6 neighbor を修正</li> <li>- show ipv6 general-prefix を修正</li> </ul> </li> <li>• 「3.7 IP ユーティリティーコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ping を修正</li> </ul> </li> <li>• 「3.9 ファイルシステムコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- dir の使用例を修正</li> <li>- show storage media-info の使用例を修正</li> </ul> </li> <li>• 「4.2 DHCP サーバーコマンド」の以下を修正</li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- host の使用例を修正</li> <li>- hardware-address を修正</li> <li>- client-identifier の使用例を修正</li> <li>- service dhcp を修正</li> <li>• 「4.3 DHCPv6 クライアントコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ipv6 dhcp client pd を修正</li> <li>- show ipv6 dhcp interface の使用例を修正</li> </ul> </li> <li>• 「4.7 NTP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ntp update-calendar を修正</li> </ul> </li> <li>• 「4.11 sFlow コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show sflow の使用例を修正</li> </ul> </li> <li>• 「4.14 LLDP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- lldp receive の使用例を修正</li> <li>- lldp transmit の使用例を修正</li> </ul> </li> <li>• 「4.17 CFM コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- cfm mp-ltr-all を修正</li> <li>- show cfm linktrace を修正</li> <li>- show cfm mp-ltr-all の目的と使用例を修正</li> <li>- cfm linktrace を修正</li> <li>- cfm loopback test を修正</li> <li>- clear cfm linktrace を修正</li> </ul> </li> <li>• 「5.1 FDB コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- mac-address-table static を修正</li> <li>- show mac-address-table を修正</li> <li>- clear mac-address-table を修正</li> </ul> </li> <li>• 「5.4 ポートリダンダントコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- redundant fdb-flush dst-mac のパラメーターを修正</li> </ul> </li> <li>• 「5.6 ループ検知コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- loop-detection no-check-src の注意事項を修正</li> </ul> </li> <li>• 「5.12 MMRP-Plus コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- mmrp-plus vlangroup slave-vid の注意事項を追加</li> </ul> </li> <li>• 「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 <ul style="list-style-type: none"> <li>- spanning-tree mode のガイドラインを追加</li> <li>- show spanning-tree の使用例を修正</li> <li>- show spanning-tree configuration interface の使用例を修正</li> <li>- show spanning-tree mst の使用例を修正</li> </ul> </li> <li>• 「5.16 VLAN コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- vlan を修正</li> <li>- name (VLAN) のデフォルトを修正</li> <li>- switchport mode を修正</li> <li>- show vlan の使用例を修正</li> </ul> </li> <li>• 「5.17 プライベート VLAN コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- switchport mode private-vlan の使用例を修正</li> </ul> </li> <li>• 「5.18 VLAN トンネルコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- vlan mapping rule のガイドラインを追加</li> </ul> </li> <li>• 「6.1 プロトコル非依存コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip route を修正</li> </ul> </li> </ul>



No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>- ipv6 route を修正</li> <li>- show ip route を修正</li> <li>- show ipv6 route を修正</li> <li>• 「7.1 優先制御(QoS) コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- match のガイドラインを修正</li> <li>- police のガイドラインを追加</li> <li>- police cir のガイドラインを追加</li> </ul> </li> <li>• 「8.1 アクセスリスト(ACL) コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- acl-hardware-counter の制限事項を修正</li> <li>- list-remark の使用例を修正</li> <li>- expert access-group を修正</li> <li>- expert access-list の使用例を修正</li> <li>- permit   deny (expert access-list)のガイドラインを追加</li> <li>- 「拡張エキスパートアクセスリストの抽出条件」を修正</li> <li>- ip access-group を修正</li> <li>- ip access-list のパラメーターと使用例を修正</li> <li>- 「IP アクセスリストの抽出条件」を修正</li> <li>- ipv6 access-group を修正</li> <li>- ipv6 access-list のパラメーターと使用例を修正</li> <li>- 「IPv6 アクセスリストの抽出条件」を修正</li> <li>- mac access-group を修正</li> <li>- mac access-list の使用例を修正</li> <li>- permit   deny (mac access-list)のガイドラインを追加</li> <li>- 「拡張 MAC アクセスリストの抽出条件」を修正</li> <li>- match ip address を修正</li> <li>- match ipv6 address を修正</li> <li>- match mac address を修正</li> <li>- action を修正</li> <li>- show access-list のパラメーターを修正</li> </ul> </li> <li>• 「9.1 AccessDefender 共通コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- access-defender static mac のパラメーターを修正</li> <li>- show access-defender rule-statistics の使用例を修正</li> <li>- copy (AccessDefender)のガイドラインを修正</li> <li>- access-defender deny のパラメーターを修正</li> <li>- access-defender logout のパラメーターを修正</li> </ul> </li> <li>• 「9.2 認証、許可、アカウントिंग(AAA) コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show tacacs statistics の制限事項を追加</li> </ul> </li> <li>• 「9.4 IEEE 802.1X 認証コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- dot1x initialize interface の注意事項を追加</li> <li>- dot1x re-authenticate interface の注意事項を追加</li> </ul> </li> <li>• 「10.1 デバッグコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show tech-support の使用例を修正</li> </ul> </li> <li>• 「10.4 システムログコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- command logging enable の制限事項を追加</li> </ul> </li> </ul>
E	2021年3月31日	<ul style="list-style-type: none"> <li>• 全章を対象に誤字・脱字・体裁を修正</li> <li>• 全章を対象にコマンドモード遷移に関する記載を修正</li> <li>• 5.1章の名称を「FDB コマンド」に修正</li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>• 「3.4 アクセス管理コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- banner login を修正</li> <li>- line の使用例を修正</li> <li>- clear line を修正</li> </ul> </li> <li>• 「4.11 sFlow コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- sflow receiver を修正</li> <li>- sflow sampler を修正</li> <li>- sflow poller を修正</li> <li>- show sflow の使用例を修正</li> </ul> </li> <li>• 「4.17 CFM コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- cfm enable のガイドラインを修正</li> <li>- cfm ma のガイドラインを修正</li> <li>- cfm mep のガイドラインを修正</li> <li>- show cfm mip ccm の使用例を修正</li> <li>- show cfm pkt-cnt interface の使用例を修正</li> </ul> </li> <li>• 「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</li> <li>• 「5.11 リングプロテクション(ERPS)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- instance (ERPS) を修正</li> <li>- sub-ring を修正</li> <li>- profile (ERPS) を修正</li> </ul> </li> <li>• 「5.18 VLAN トンネルコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- vlan mapping profile のガイドラインを修正</li> </ul> </li> <li>• 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- permit   deny (expert access-list) のパラメーターを修正、制限事項を追加</li> <li>- permit   deny (ip access-list) のパラメーターを修正、制限事項を追加</li> <li>- permit   deny (ipv6 access-list) のパラメーターを修正、制限事項を追加</li> </ul> </li> </ul>
F	2021年5月31日	<ul style="list-style-type: none"> <li>• 「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</li> <li>• 「Gratuitous ARP コマンド」の記載を、「3 基礎知識」配下に変更</li> <li>• 「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</li> <li>• 「FDB コマンド」の記載を、「5 レイヤー2」配下に変更</li> <li>• 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</li> <li>• 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</li> <li>• 全章を対象に各コマンドの見出しを追加</li> <li>• 全章を対象に誤字・脱字・体裁を修正</li> <li>• 「1 はじめに」に「適応機種と対応バージョン」を追加</li> <li>• 「2.1 インターフェースコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show interfaces の使用例を修正</li> </ul> </li> <li>• 「2.5 スタックコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- stack bandwidth の制限事項を修正</li> </ul> </li> <li>• 「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</li> <li>• 「3.8 Gratuitous ARP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- ip gratuitous-arps を修正</li> </ul> </li> </ul>

No.	年 月 日	内 容
		<ul style="list-style-type: none"> <li>• 「4.4 DHCPv6 サーバーコマンド」の以下を修正 <ul style="list-style-type: none"> <li>- address prefix の制限事項を追加</li> <li>- address-assignment の制限事項を追加</li> <li>- prefix-delegation pool の制限事項を追加</li> <li>- prefix-delegation の制限事項を追加</li> </ul> </li> <li>• 「4.7 NTP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show ntp associations の注意事項を追加、使用例を修正</li> </ul> </li> <li>• 「4.8 TELNET コマンド」を追加し、関連コマンドを配下に変更</li> <li>• 「4.9 SSH コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- crypto key generate の注意事項を追加</li> </ul> </li> <li>• 「4.12 SNMP コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- show snmp user の使用例を修正</li> </ul> </li> <li>• 「5.6 ループ検知コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- loop-detection action notify-only の注意事項を追加</li> <li>- loop-detection no-check-src の注意事項を追加</li> </ul> </li> <li>• 「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</li> <li>• 「5.12 MMRP-Plus コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- debug mmrp を修正</li> </ul> </li> <li>• 「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 <ul style="list-style-type: none"> <li>- spanning-tree priority を修正</li> <li>- spanning-tree (timers) を修正</li> <li>- spanning-tree cost を修正</li> <li>- spanning-tree port-priority を修正</li> <li>- spanning-tree mst configuration のガイドラインを追加</li> <li>- spanning-tree mst priority を修正</li> <li>- spanning-tree mst を、spanning-tree mst cost と spanning-tree mst port-priority の2つに分割</li> <li>- show spanning-tree を修正</li> <li>- show spanning-tree configuration interface を修正</li> <li>- show spanning-tree mst を修正</li> <li>- clear spanning-tree detected-protocols を修正</li> </ul> </li> <li>• 「5.14 RPVST+コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- spanning-tree vlan を修正</li> <li>- spanning-tree vlan priority を修正</li> <li>- spanning-tree vlan (timers) を修正</li> <li>- spanning-tree vlan cost を修正</li> <li>- spanning-tree vlan port-priority を修正</li> <li>- show spanning-tree vlan を修正</li> <li>- show spanning-tree vlan interface を修正</li> </ul> </li> <li>• 「8.1 アクセスリスト(ACL)コマンド」の以下を修正 <ul style="list-style-type: none"> <li>- vlan filter の注意事項を追加</li> </ul> </li> </ul>

# 目次

制定・改訂来歴表	1
1 はじめに	22
1.1 本文中の表記について	25
1.2 コマンドシンタックス	26
1.3 コンソールポートへの接続	28
1.4 初めての CLI への接続	29
1.5 ユーザーアカウント	30
1.6 ユーザーアカウントの作成	31
1.7 コマンドモード	32
1.8 インターフェースの表記法	34
1.9 VLAN インターフェース	35
1.10 エラーメッセージ	36
1.11 コマンド入力の補助機能	37
1.12 表示結果出力修飾子	38
1.13 本書でのコマンド説明の記載項目	39
2 インターフェースとハードウェア	40
2.1 インターフェースコマンド	40
2.2 ポート設定コマンド	60
2.3 アラーム LED コマンド	66
2.4 省電力イーサネット (EEE) コマンド	73
2.5 スタックコマンド	75
3 基礎知識	82
3.1 基本 CLI コマンド	82
3.2 ファイルシステムコマンド	94
3.3 ターミナルコマンド	101
3.4 アクセス管理コマンド	105
3.5 基本 IPv4 コマンド	116
3.6 基本 IPv6 コマンド	125
3.7 IP ユーティリティーコマンド	141
3.8 Gratuitous ARP コマンド	145
3.9 システムファイル管理コマンド	147
4 管理	171
4.1 DHCP クライアントコマンド	171
4.2 DHCP サーバーコマンド	174
4.3 DHCPv6 クライアントコマンド	200
4.4 DHCPv6 サーバーコマンド	204
4.5 DHCP Auto Configuration コマンド	221
4.6 時刻および SNTP コマンド	223
4.7 NTP コマンド	229
4.8 TELNET コマンド	242
4.9 SSH コマンド	245
4.10 RMON コマンド	253
4.11 sFlow コマンド	262

4.12	SNMP コマンド	270
4.13	ミラーリングコマンド	294
4.14	LLDP コマンド	303
4.15	EtherOAM コマンド	331
4.16	単方向リンク検出(ULD) コマンド	347
4.17	CFM コマンド	351
5	レイヤー2	384
5.1	FDB コマンド	384
5.2	ジャンボフレームコマンド	392
5.3	ポートチャネルコマンド	393
5.4	ポートリダundantコマンド	400
5.5	リンクダウン連携コマンド	406
5.6	ループ検知コマンド	409
5.7	ストームコントロールコマンド	418
5.8	マルチキャストフィルタリングモードコマンド	425
5.9	IGMP スヌーピングコマンド	427
5.10	MLD スヌーピングコマンド	444
5.11	リングプロテクション(ERPS) コマンド	461
5.12	MMRP-Plus コマンド	474
5.13	スパニングツリープロトコルコマンド	499
5.14	RPVST+コマンド	524
5.15	トラフィックセグメンテーションコマンド	532
5.16	VLAN コマンド	534
5.17	プライベート VLAN コマンド	548
5.18	VLAN トンネルコマンド	554
6	レイヤー3	568
6.1	プロトコル非依存コマンド	568
6.2	IPv4 マルチキャストコマンド	574
6.3	IPv6 マルチキャストコマンド	575
7	優先制御(QoS)	576
7.1	優先制御(QoS) コマンド	576
7.2	WRED コマンド	614
8	アクセスリスト(ACL)	621
8.1	アクセスリスト(ACL) コマンド	621
9	セキュリティ	658
9.1	AccessDefender 共通コマンド	658
9.2	認証、許可、アカウントティング(AAA) コマンド	692
9.3	MAC 認証コマンド	720
9.4	IEEE 802.1X 認証コマンド	724
9.5	SSL コマンド	737
9.6	Web 認証コマンド	741
9.7	DHCP スヌーピングコマンド	751
10	サポート	759
10.1	デバッグコマンド	759
10.2	エラー復旧コマンド	779

10.3	メモリーエラー自動復旧コマンド.....	782
10.4	システムログコマンド.....	785
10.5	CPU 使用率監視コマンド.....	797
11	付録.....	799
11.1	システム復旧手順(パスワードのリセット).....	799

# 1 はじめに

---

## ■本書の目的

ApresiaNP4000 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
ApresiaNP4000-20Xt4X	AEOS-NP4000 Ver. 1.01.01～

## ■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、ApresiaNP4000-20Xt4X 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。

ApresiaNP4000 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。

## 1 はじめに

### ■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。



## 1 はじめに

### ■ 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/イーサネットは、富士ゼロックス株式会社の登録商標です。

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、または登録商標です。

## 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	<code>command [parameter1]</code>
説明	<code>parameter1</code> 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	<code>command {parameter1   parameter2}</code>
説明	コマンドを実行するために必要なパラメーターが <code>parameter1</code> 、および <code>parameter2</code> 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	<code>command [parameter1   parameter2   parameter3]</code>
説明	以下の3つのコマンドを個別に実行できます。 <ul style="list-style-type: none"> <li>• <code>command parameter1</code></li> <li>• <code>command parameter2</code></li> <li>• <code>command parameter3</code></li> </ul>

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。

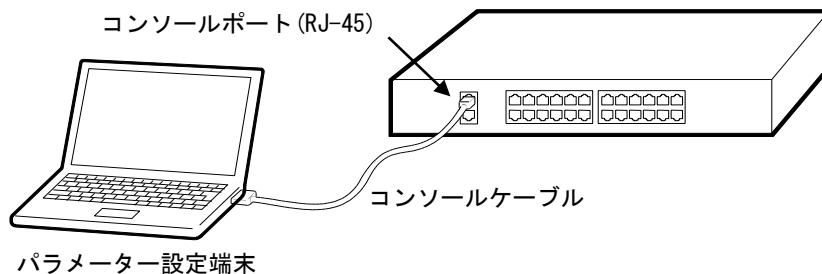
編集機能	
Enter キー	コマンドを実行します。
Delete キー	カーソル位置の文字を削除します。
Backspace キー	カーソル位置の1つ左の文字を削除します。
Ctrl+A キー	カーソルを行頭へ移動します。
Ctrl+E キー	カーソルを行末へ移動します。
Ctrl+K キー	カーソル位置の文字から行末までを削除します。
Ctrl+Z キー	グローバル設定モードまたはサブ設定モードの場合に、入力途中の文字列を破棄して特権実行モードに戻ります。
左矢印キー	カーソルを左へ移動します。
右矢印キー	カーソルを右へ移動します。
上矢印キーまたは Ctrl+P キー	コマンド履歴リスト ( <code>show history</code> 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 ( <code>show history</code> 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	
	<p>CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All</p> <p>この状態では以下の操作によるスクロールが可能です。</p> <ul style="list-style-type: none"><li>• 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。</li><li>• スペースキーまたは N キー：次のページを表示します。</li><li>• Enter キー：次の行を表示します。</li><li>• A キー：すべての情報を表示します。</li></ul> <p>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。</p>

## 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 コネクタで、もう一方がメス型 DB-9 コネクタ）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：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-CA-CE-00
  H/W Version: A

Power On Self Test: 100 %

Please Wait, Loading V1.02.01

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...
```

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。

## 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 ApresiaNP4000-20Xt4X

Firmware: Build 1.02.01

>
```

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 ApresiaNP4000-20Xt4X

Firmware: Build 1.02.01

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 <b>clear</b> 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。

コマンドモード	説明
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) (config-if-port-channel)#	ポートチャネル関連の設定を、指定したポートチャネルで実施する設定モードです。
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、 <b>description</b> 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。非スタックメンバーの装置の場合は 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 1/0/18
interface port 1/0/18
interface port 1/0/19
interface port 1/0/20
interface port 1/0/21
interface port 1/0/22
interface port 1/0/23
interface port 1/0/24

# SSH

ip ssh server
ssh user user1 authentication-method password

#-----
#                End of configuration file for ApresiaNP4000-20Xt4X
#-----
```

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
-----
Port1/0/13    disabled   trunk     auto    auto       10GBASE-T
Port1/0/14    disabled   trunk     auto    auto       10GBASE-T
Port1/0/21    connected  trunk     a-full  a-10G     10GBASE-R
Port1/0/22    connected  trunk     a-full  a-10G     10GBASE-R

Total Entries: 24
```

## 1.13 本書でのコマンド説明の記載項目

コマンドラインインターフェース (CLI) で使用できるすべてのコマンドは、論理的に整理され、機能別に区分されています。

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	コマンドの機能を説明します。
シンタックス	コマンド、およびコマンドに関連付けられているすべてのパラメーターを示します。
パラメーター	コマンドのすべてのパラメーターの詳細を説明します。パラメーター、変数、省略可能、必須など、パラメーターの情報を示します。また、パラメーターごとに、適用範囲、制限、使用法、デフォルト設定などを示しています。
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。コマンドを実行する前の設定値や管理状態を示しています。
コマンドモード	コマンドを実行できるモードを示します。 コマンドモードの説明については、「1.7 コマンドモード」を参照してください。
特権レベル	各コマンドのユーザー特権レベルを示します。
ガイドライン	必要に応じて、コマンドの詳細な説明、およびコマンドの利用シナリオを示します。
制限事項	各コマンドの制限事項を示します。
注意事項	各コマンドの注意事項を示します。
対象バージョン	各コマンドの対象バージョンを示します。

使用例：各コマンドの実行例を示します。例は、特権実行モードから示しています。



## 2 インターフェイスとハードウェア

### 2.1 インターフェイスコマンド

インターフェイ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

インターフェイス関連の 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   stack-port]
clear counters	clear counters {all   interface INTERFACE-ID [,  -]   cpu-port   stack-port}

#### 2.1.1 interface

interface	
目的	単一インターフェイスのインターフェイス設定モードに遷移します。また、VLAN インターフェイ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	<b>interface</b> INTERFACE-ID <b>no interface</b> INTERFACE-ID
パラメーター	INTERFACE-ID: インターフェイスを指定します。インターフェイスは、インターフェイスの種類とインターフェイス番号から構成されます。本コマンドでは、イ

interface	
	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 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。</li> <li>• <b>port-channel</b> &lt;1-48&gt; : ポートチャンネルを指定します。</li> <li>• <b>vlan</b> &lt;1-4094&gt; : 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。</li> <li>• <b>mgmt</b> &lt;0&gt; : マネージメントポートを指定します。</li> <li>• <b>l2vlan</b> &lt;1-4094&gt; : レイヤー2 VLAN インターフェースを指定します。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> 指定時 : (config-if-port)#</li> <li>• <b>port-channel</b> 指定時 : (config-if-port-channel)#</li> <li>• <b>vlan</b> 指定時 : (config-if-vlan)#</li> <li>• <b>mgmt</b> 指定時 : (config-if-mgmt)#</li> <li>• <b>l2vlan</b> 指定時 : (config-if-l2vlan)#</li> </ul>
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	<p>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。</p> <p>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、<b>interface port</b> 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、<b>interface mgmt</b> 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。</p> <p>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、<b>interface vlan</b> 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 <b>vlan</b> 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、<b>no interface vlan</b> コマンドを使用します。</p> <p>ポートチャンネルは、<b>channel-group</b> 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。ポートチャンネルのインターフェース設定モードに遷移するには、<b>interface port-channel</b> 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、<b>no interface port-channel</b> コマンドを使用してポートチャンネルを削除することもできます。</p> <p><b>vlan</b> 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、<b>description</b> 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、<b>description</b> コマンドを設定していない状態では構成情報で <b>interface l2vlan</b> 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、<b>interface l2vlan</b> コマンドを使用します。<b>no vlan</b> コマンドで VLAN を削除すると、対応するレイヤー2 VLAN インターフェースも自動的に削除されます。</p>
制限事項	-

interface	
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	<b>interface range</b> <i>INTERFACE-ID</i> [, [-]
パラメーター	<p><i>INTERFACE-ID</i>：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。</p> <ul style="list-style-type: none"> <li>• <b>port</b>：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。</li> <li>• <b>l2vlan</b> &lt;1-4094&gt;：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。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> 指定時：(config-if-port-range)#</li> <li>• <b>l2vlan</b> 指定時：(config-if-l2vlan-range)#</li> </ul>
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。
制限事項	-
注意事項	-

interface range	
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	<b>description</b> <i>STRING</i> <b>no description</b>
パラメーター	<i>STRING</i> ：インターフェースの説明を最大 64 文字で指定します。
デフォルト	なし
コマンドモード	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	<b>shutdown</b> <b>no shutdown</b>
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。  インターフェースが無効状態では、ポートはすべてのパケットを送受信できません。no shutdown コマンドを使用すると、ポートは有効状態になります。  ポートがシャットダウンされると、リンク状態もオフになります。

shutdown	
制限事項	-
注意事項	本コマンドを実行した場合、ひとつのポートを無効化するため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、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 show interfaces

show interfaces	
目的	インターフェイス情報を表示します。
シンタックス	<b>show interfaces</b> [ <i>INTERFACE-ID</i> [,  -]]
パラメーター	<i>INTERFACE-ID</i> (省略可能)：情報を表示するインターフェイスを、以下のパラメーターで指定します。 <ul style="list-style-type: none"> <li>• <b>port</b>：物理ポートを指定します。複数指定できます。</li> <li>• <b>vlan</b> &lt;1-4094&gt;：VLAN インターフェイスを指定します。</li> <li>• <b>mgmt</b> &lt;0&gt;：マネージメントポートを指定します。</li> </ul>
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	インターフェイ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 インターフェイ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 down ... (1)
Interface type: VLAN ... (2)
Interface description: ... (3)
MAC address: 00-40-66-AF-F0-48 ... (4)
```

項番	説明
(1)	VLAN インターフェイスの状態を表示します。
(2)	インターフェイスの種類を表示します。
(3)	インターフェイスの説明を表示します。
(4)	インターフェイスの MAC アドレスを表示します。

使用例：ポート 1/0/1 のインターフェイ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: 10GBASE-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: 293 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。
(2)	インターフェースの種類を表示します。
(3)	インターフェース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 の設定を表示します。
(6)	送信時および受信時のフロー制御の ON/OFF の設定を表示します。
(7)	送信時および受信時のフロー制御の ON/OFF の実動作を表示します。
(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。
(9)	MTU を表示します。
(10)	1 秒あたりの受信ビット数および送信ビット数を表示します。
(11)	受信したバイト数および送信した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送信パケット数を表示します。
(13)	受信したパケット数および送信したパケット数を表示します。
(14)	受信したマルチキャストパケット数およびブロードキャストパケット数を表示します。
(15)	受信 FCS エラーおよびアンダーパケットエラーのパケット数を表示します。
(16)	受信オーバーパケットエラーおよびフラグメントエラーのパケット数を表示します。
(17)	受信ジャバークエットエラーおよび受信パケットドロップエラーのパケット数を表示します。
(18)	転送先のポートやインターフェースの MTU よりもフレームサイズが大きいため破棄された受信フレーム数を表示します。
(19)	送信 FCS エラーのパケット数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コリジョン回数を表示します。

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。
(2)	インターフェイスの種類を表示します。
(3)	インターフェイスの説明を表示します。
(4)	デュプレックスモード、動作速度、および MDIX の設定を表示します。

### 2.1.6 show interfaces counters

show interfaces counters	
目的	指定したインターフェイスのカウンターを表示します。
シンタックス	<b>show interfaces</b> [ <i>INTERFACE-ID</i> [,  -]] <b>counters</b> [ <b>errors</b> ]
パラメーター	<p><i>INTERFACE-ID</i> (省略可能) : カウンターを表示するインターフェイスを、以下のパラメーターで指定します。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>mgmt</b> &lt;0&gt; : 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、<b>errors</b> パラメーターは省略できません。</li> </ul> <p><b>errors</b> (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。</p>
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	インターフェイスを指定しない場合は、すべての物理ポートのカウンターが表示されます。
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) Port	(2) Align-Err	(3) Fcs-Err	(4) Rcv-Err	(5) Undersize	(6) Xmit-Err	(7) OutDiscard
Port1/0/1		0	0	0	0	0
Port1/0/2		0	0	0	0	0

(8) Port	(9) Single-Col	(10) Multi-Col	(11) Late-Col	(12) Excess-Col	(13) Carri-Sen	(14) Runts
Port1/0/1	0	0	0	0	0	0
Port1/0/2	0	0	0	0	0	0

(15) Port	(16) Giants	(17) Symbol-Err	(18) SQETest-Err	(19) DeferredTx	(20) IntMacTx	(21) 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



項番	説明
	た、またはアサートされていなかった回数を表示します。
(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。

## 2.1.7 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	<b>show interfaces</b> [ <i>INTERFACE-ID</i> [,  -]] <b>status</b>
パラメーター	<i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのポートの接続状態が表示されます。
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)      (6)
Port      Status      VLAN      Duplex    Speed      Type
-----
Port1/0/1  connected   1          a-full    a-1000     10GBASE-T
Port1/0/2  not-connected 1          auto      auto       10GBASE-T
Port1/0/3  not-connected 1          auto      auto       10GBASE-T
Port1/0/4  not-connected 1          auto      auto       10GBASE-T
Port1/0/5  not-connected 1          auto      auto       10GBASE-T
Port1/0/6  not-connected 1          auto      auto       10GBASE-T
Port1/0/7  not-connected 1          auto      auto       10GBASE-T
Port1/0/8  not-connected 1          auto      auto       10GBASE-T

Total Entries: 8
```

項番	説明
(1)	ポート番号を表示します。
(2)	接続状態を表示します。
(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 と表示します。 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を表示します。
(5)	速度を表示します。
(6)	インターフェースタイプを表示します。

## 2.1.8 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	<b>show interfaces</b> [ <i>INTERFACE-ID</i> [,  -]] <b>utilization</b>
パラメーター	<i>INTERFACE-ID</i> (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。

show interfaces utilization	
	<ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのポートの使用率が表示されます。
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 1/0/10 のポート使用率を表示する方法を示します。

```
# show interfaces port 1/0/1-10 utilization
(1)          (2)          (3)          (4)
Port         TX packets/sec / TX bits/sec / Utilization
              (5)          (6)
              RX packets/sec  RX bits/sec
-----
Port1/0/1           0           0           0
                  0           0
Port1/0/2           0           0           0
                  0           0
Port1/0/3           0           0           0
                  0           0
Port1/0/4           0           0           0
                  0           0
Port1/0/5           0           0           0
                  0           0
Port1/0/6           0           0           0
                  0           0
Port1/0/7           0           0           0
                  0           0
Port1/0/8           0           0           0
                  0           0
Port1/0/9           0           0           0
                  0           0
Port1/0/10          0           0           0
                  0           0

Total Entries: 10
```

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を表示します。
(3)	1秒あたりの送信ビット数を表示します。
(4)	使用率を表示します。
(5)	1秒あたりの受信パケット数を表示します。
(6)	1秒あたりの受信ビット数を表示します。

### 2.1.9 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	<code>show interfaces [INTERFACE-ID [, -]] gbic</code>

show interfaces gbic	
パラメーター	<i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースのトランシーバー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 1/0/21 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 1/0/21 gbic

Port1/0/21 ... (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。

### 2.1.10 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	<b>show interfaces</b> [ <i>INTERFACE-ID</i> [,  -]] <b>description</b>
パラメーター	<i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>vlan</b> &lt;1-4094&gt; : VLAN インターフェースを指定します。</li> <li>• <b>mgmt</b> &lt;0&gt; : マネージメントポートを指定します。</li> <li>• <b>l2vlan</b> [&lt;1-4094&gt;] : 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。</li> </ul>
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、すべてのインターフェースの説明とリンク状態が表示されます。
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)
Interface          (2)      Status      (3)      Administrative      (4)      Description
-----
Port1/0/1          up        enabled     Connection to core.
Port1/0/2          down     enabled
Port1/0/3          down     enabled
Port1/0/4          down     enabled
Port1/0/5          down     enabled
Port1/0/6          down     enabled
Port1/0/7          down     enabled
Port1/0/8          down     enabled
Port1/0/9          down     enabled
Port1/0/10         down     enabled
Port1/0/11         down     enabled
Port1/0/12         down     enabled
Port1/0/13         down     enabled
Port1/0/14         down     enabled
Port1/0/15         down     enabled
Port1/0/16         down     enabled
Port1/0/17         down     enabled
Port1/0/18         down     enabled
Port1/0/19         down     enabled
Port1/0/20         down     enabled
Port1/0/21         down     enabled
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)	リンク状態を表示します。
(3)	ポートを意図的にシャットダウンしているかどうかを表示します。 enabled：ポートがアクティブな状態 disabled：ポートが意図的にシャットダウンされている状態
(4)	説明を表示します。

### 2.1.11 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	<b>show interfaces</b> [ <i>INTERFACE-ID</i> [, [-]] <b>auto-negotiation</b>
パラメーター	<i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li><b>port</b>：物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースのオートネゴシエーション情報の詳細が表示されます。
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: 100M_Full, 1000M_Full, 10G_Full ... (6)
  Capability Advertised Bits: 100M_Half, 100M_Full, 1000M_Full, 10G_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: 100M_Full, 1000M_Full, 10G_Full
  Capability Advertised Bits: 100M_Half, 100M_Full, 1000M_Full, 10G_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。

### 2.1.12 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	<b>show interfaces</b> [ <i>INTERFACE-ID</i> [, -]] <b>transceiver</b> [ <i>detail</i> ]
パラメーター	<i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li><b>port</b>：物理ポートを指定します。複数指定できます。</li> </ul> <b>detail</b> (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

show interfaces transceiver	
ガイドライン	インターフェースを指定しない場合、すべての光トランシーバーの動作状況が表示されます。
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	<b>detail</b> 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)
port      Voltage      Bias Current TX Power      RX Power
          (V)          (mA)          (mW/dbm)      (mW/dbm)
-----
Port1/0/21 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。

### 2.1.13 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	<b>show counters</b> [ <b>interface</b> <i>INTERFACE-ID</i> [, -]   <b>cpu-port</b>   <b>stack-port</b> ]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li><b>port</b>：物理ポートを指定します。複数指定できます。</li> </ul> <b>cpu-port</b> (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。 <b>stack-port</b> (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	インターフェースを指定しない場合、すべてのインターフェースのカウンターが表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：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)
rxHCPkt9217to16383Octets :              0 ... (21)
txHCPkt64Octets        :             41 ... (22)
txHCPkt65to127Octets  :             32 ... (23)
txHCPkt128to255Octets :              0 ... (24)
txHCPkt256to511Octets :              0 ... (25)
txHCPkt512to1023Octets :              0 ... (26)
txHCPkt1024to1518Octets :              0 ... (27)
txHCPkt1519to1522Octets :              0 ... (28)
txHCPkt1519to2047Octets :              0 ... (29)
txHCPkt2048to4095Octets :              0 ... (30)
txHCPkt4096to9216Octets :              0 ... (31)
txHCPkt9217to16383Octets :              0 ... (32)

rxCRCAAlignErrors      :              0 ... (33)
rxUndersizedPkts       :              0 ... (34)
rxOversizedPkts        :              0 ... (35)
rxFragmentPkts         :              0 ... (36)
rxJabbers               :              0 ... (37)
rxSymbolErrors         :              0 ... (38)
rxDropPkts              :           50256 ... (39)

txCollisions            :              0 ... (40)
ifInErrors              :              0 ... (41)
ifOutErrors             :              0 ... (42)
ifInDiscards            :           50256 ... (43)
ifInUnknownProtos      :              0 ... (44)
ifOutDiscards           :              0 ... (45)
txDelayExceededDiscards :              0 ... (46)
txCRC                   :              0 ... (47)
txCoS0DropPkts         :              0 ... (48)
txCoS1DropPkts         :              0 ... (49)
txCoS2DropPkts         :              0 ... (50)
txCoS3DropPkts         :              0 ... (51)
txCoS4DropPkts         :              0 ... (52)
txCoS5DropPkts         :              0 ... (53)
txCoS6DropPkts         :              0 ... (54)
txCoS7DropPkts         :              0 ... (55)
```



dot3StatsAlignmentErrors	:	0 ... (56)
dot3StatsFCSErrors	:	0 ... (57)
dot3StatsSingleColFrames	:	0 ... (58)
dot3StatsMultiColFrames	:	0 ... (59)
dot3StatsSQETestErrors	:	0 ... (60)
dot3StatsDeferredTransmissions	:	0 ... (61)
dot3StatsLateCollisions	:	0 ... (62)
dot3StatsExcessiveCollisions	:	0 ... (63)
dot3StatsInternalMacTransmitErrors	:	0 ... (64)
dot3StatsCarrierSenseErrors	:	0 ... (65)
dot3StatsFrameTooLongs	:	0 ... (66)
dot3StatsInternalMacReceiveErrors	:	0 ... (67)
linkChange	:	2 ... (68)

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)	受信 9,217~16,383 オクテットパケットカウンターを表示します。
(22)	送信 64 オクテットパケットカウンターを表示します。
(23)	送信 65~127 オクテットパケットカウンターを表示します。
(24)	送信 128~255 オクテットパケットカウンターを表示します。
(25)	送信 256~511 オクテットパケットカウンターを表示します。
(26)	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。
(27)	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。
(28)	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。
(29)	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。
(30)	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。
(31)	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。
(32)	送信 9,217~16,383 オクテットパケットカウンターを表示します。

項番	説明
(33)	受信 FCS エラーパケットカウンタを表示します。
(34)	受信アンダーサイズパケットカウンタを表示します。
(35)	受信オーバーサイズパケットカウンタを表示します。
(36)	受信フラグメントカウンタを表示します。
(37)	受信ジャバパケットカウンタを表示します。
(38)	受信コードエラーパケットカウンタを表示します。
(39)	受信パケットドロップカウンタを表示します。
(40)	送信コリジョンカウンタを表示します。
(41)	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。
(42)	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。
(43)	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。
(44)	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。
(45)	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。
(46)	送信マルチ遅延パケットカウンタを表示します。
(47)	送信 FCS エラーカウンタを表示します。
(48)	CoS キュー0 の送信パケットドロップカウンタを表示します。
(49)	CoS キュー1 の送信パケットドロップカウンタを表示します。
(50)	CoS キュー2 の送信パケットドロップカウンタを表示します。
(51)	CoS キュー3 の送信パケットドロップカウンタを表示します。
(52)	CoS キュー4 の送信パケットドロップカウンタを表示します。
(53)	CoS キュー5 の送信パケットドロップカウンタを表示します。
(54)	CoS キュー6 の送信パケットドロップカウンタを表示します。
(55)	CoS キュー7 の送信パケットドロップカウンタを表示します。
(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。
(57)	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 チェックに合格しないパケットの数を表示します。
(58)	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。
(59)	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。
(60)	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。
(61)	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。
(62)	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。
(63)	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。
(64)	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。

項番	説明
(65)	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。
(66)	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。
(67)	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。
(68)	ポートのステータスが変化した際にカウントされる数字を表示します。

使用例：スタックポートのカウンターを表示する方法を示します。

```
# show counters stack-port

Unit 1, Stack Port 23 counters
ifInErrors           :                0 ... (1)

Unit 1, Stack Port 24 counters
ifInErrors           :                0

Unit 2, Stack Port 23 counters
ifInErrors           :                0

Unit 2, Stack Port 24 counters
ifInErrors           :                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。

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
(1)      (2)      (3)
CoS      cpuRxPkts      cpuTxDropPkts
-----
0                0                0
1                0                0
2                0                0
3                0                0
4                0                0
5                0                0
6                0                0
7                0                0
```

項番	説明
(1)	CoS キューを表示します。
(2)	CoS ごとの受信パケットカウンターを表示します。
(3)	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。

### 2.1.14 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。

clear counters	
シンタックス	<code>clear counters {all   interface <i>INTERFACE-ID</i> [, -]   cpu-port   stack-port}</code>
パラメーター	<p><b>all</b> : すべてのインターフェイスのカウンターをクリアする場合に指定します。</p> <p><b>interface <i>INTERFACE-ID</i></b> : カウンターをクリアするインターフェイスを、以下のパラメーターで指定します。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>mgmt &lt;0&gt;</b> : マネージメントポートを指定します。</li> </ul> <p><b>cpu-port</b> : 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。</p> <p><b>stack-port</b> : 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。</p>
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	<b>stack-port</b> 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

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 {100   1000 [master   slave]   10giga   auto [SPEED-LIST]} no speed
duplex	duplex {full   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

### 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 {100   1000 [master   slave]   10giga   auto [SPEED-LIST]} no speed
パラメーター	<p>■ RJ-45 ポート (100BASE-TX/1000BASE-T/10GBASE-T) の場合</p> <p><b>100</b> : 通信速度を 100Mbps に設定する場合に指定します。</p> <p><b>1000</b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>master</b> (省略可能) : マスター装置として動作させる場合</li> <li>• <b>slave</b> (省略可能) : スレーブ装置として動作させる場合</li> </ul> <p><b>10giga</b> : 通信速度を 10Gbps に設定する場合に指定します。</p> <p><b>auto</b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>SPEED-LIST</b> (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。</li> <li>• <b>10</b> (省略可能) : 10Mbps をアドバタイズする場合</li> <li>• <b>100</b> (省略可能) : 100Mbps をアドバタイズする場合</li> <li>• <b>1000</b> (省略可能) : 1000Mbps をアドバタイズする場合</li> </ul> <p>■ SFP/SFP+ポートの場合</p> <p><b>1000</b> : 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。</p> <p><b>10giga</b> : 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。</p>

speed	
	<b>auto</b> : トランシーバーの自動認識を有効にする場合に指定します。1Gbps の場合はオートネゴシエーションが有効になります。
デフォルト	RJ-45 ポート (100BASE-TX/1000BASE-T/10GBASE-T) : <b>auto 100, 1000, 10giga</b> (オートネゴシエーション有効, 100/1000Mbps/10Gbps) SFP/SFP+ポート : <b>auto</b> (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	<p>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。</p> <ul style="list-style-type: none"> <li>• RJ-45 ポート (100BASE-TX/1000BASE-T/10GBASE-T) の使用方法と設定コマンド</li> <li>• SFP/SFP+ポートの使用方法と設定コマンド</li> </ul> <p>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 <b>auto</b> 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。</p> <p>1000BASE-T、10GBASE-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。</p> <p>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。</p>
制限事項	ApresiaNP4000 シリーズでは、 <b>auto-downgrade</b> パラメーターは未サポートです。 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	<p>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 (<b>auto</b>) のまま使用してください。</p> <p>本コマンドの <b>1000</b> 指定で、<b>master</b> または <b>slave</b> 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 (<b>duplex auto</b>) のまま使用してください。</p> <p>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、<b>master</b> または <b>slave</b> 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。</p>
対象バージョン	1.01.01

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

- ApresiaNP4000-20Xt4X の Port 1/0/1~1/0/20

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

オートネゴシエーションの有効/無効 ※()内は有効時のアダバタイズ内容	設定コマンド
	<ul style="list-style-type: none"> <li>• speed auto 100 / duplex full</li> <li>• speed 100 / duplex auto</li> </ul>
有効 (1000M/Full)	speed auto 1000 / duplex auto <その他の設定パターン> <ul style="list-style-type: none"> <li>• speed auto 1000 / duplex full</li> <li>• speed 1000 [master slave] / duplex auto</li> </ul>
有効 (10G/Full)	speed auto 10giga / duplex auto <その他の設定パターン> <ul style="list-style-type: none"> <li>• speed auto 10giga / duplex full</li> <li>• speed 10giga / duplex auto</li> </ul>
有効 (100M/Full, 1000M/Full)	speed auto 100,1000 / duplex auto <その他の設定パターン> <ul style="list-style-type: none"> <li>• speed auto 100,1000 / duplex full</li> </ul>
有効 (100M/Full, 10G/Full)	speed auto 100,10giga / duplex auto <その他の設定パターン> <ul style="list-style-type: none"> <li>• speed auto 100,10giga / duplex full</li> </ul>
有効 (1000M/Full, 10G/Full)	speed auto 1000,10giga / duplex auto <その他の設定パターン> <ul style="list-style-type: none"> <li>• speed auto 1000,10giga / duplex full</li> </ul>
オートネゴシエーション無効、 100Mbps/Full 固定	speed 100 / duplex full

#### ■ SFP/SFP+ポートの使用方法和設定コマンド

- ApresiaNP4000-20Xt4X の Port 1/0/21~1/0/24

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

### 2.2.2 duplex

duplex	
目的	ポートのデュプレックスモードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	duplex {full   auto} no duplex
パラメーター	■ RJ-45 ポート (100BASE-TX/1000BASE-T/10GBASE-T) の場合

duplex	
	<p><b>full</b> : 全二重モードに設定する場合に指定します。</p> <p><b>auto</b> : 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。</p> <p>■ SFP/SFP+ポートの場合</p> <p><b>full</b> : 全二重モードに設定する場合に指定します。</p> <p><b>auto</b> : 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。</p>
デフォルト	RJ-45 ポート、SFP/SFP+ポート : <b>auto</b>
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	<p>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。</p> <ul style="list-style-type: none"> <li>• RJ-45 ポート(100BASE-TX/1000BASE-T/10GBASE-T)の使用方法と設定コマンド</li> <li>• SFP/SFP+ポートの使用方法と設定コマンド</li> </ul> <p>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。</p> <p>1000BASE-T、10GBASE-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。</p> <p>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。</p>
制限事項	本装置では半二重モードをサポートしていないため、本コマンドはデュプレックスモードをオートネゴシエーションによりアダプタイズするか、または固定にするかの選択のみ可能です。
注意事項	<p>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(<b>auto</b>)のまま使用してください。</p> <p>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。</p>
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	<p><b>mdix</b> {auto   normal   cross}</p> <p><b>no mdix</b></p>
パラメーター	<b>auto</b> : Auto MDI/MDI-X モードに設定する場合に指定します。



mdix	
	<p><b>normal</b> : 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。</p> <p><b>cross</b> : 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。</p>
デフォルト	Auto MDI/MDI-X ( <b>auto</b> )
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	<b>flowcontrol {on   off}</b> <b>no flowcontrol</b>
パラメーター	<p><b>on</b> : PAUSE フレームの送受信を有効にする場合に指定します。</p> <p><b>off</b> : PAUSE フレームの送受信を無効にする場合に指定します。</p>
デフォルト	無効 ( <b>off</b> )
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 <b>flowcontrol on</b> コマンド、 <b>flowcontrol off</b> コマンド、または <b>no flowcontrol</b> 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。

speed_duplex (mgmt 0)	
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	ApresiaNP4000 シリーズでは、オートネゴシエーションが有効な場合のみ 1000BASE-T をサポートしています。
制限事項	-
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)#
```

## 2.3 アラーム LED コマンド

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 warn-led global enable	alarm warn-led global enable no alarm warn-led global enable
alarm warn-led duration	alarm warn-led duration {SECONDS   infinite} no alarm warn-led duration
alarm warn-led state enable	alarm warn-led state enable [cause {loop-detection   storm-control   all}] no alarm warn-led state enable
show alarm warn-led	show alarm warn-led [interface INTERFACE-ID [,  -]]
debug alarm warn-led test	debug alarm warn-led [interface INTERFACE-ID [,  -]] test

### 2.3.1 alarm warn-led global enable

alarm warn-led global enable	
目的	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 warn-led global enable no alarm warn-led 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	-
対象バージョン	1.01.01

使用例：アラーム LED を有効にする方法を示します。

```
# configure terminal
(config)# alarm warn-led global enable
(config)#
```

### 2.3.2 alarm warn-led duration

alarm warn-led duration	
目的	アラーム LED が「警告」ステータスに変化したときのアラーム LED の動作時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	alarm warn-led duration {SECONDS   infinite} no alarm warn-led duration
パラメーター	SECONDS : 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

alarm warn-led duration	
コマンドモード	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 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、アラーム LED が動作します。ループ検知の状態は <b>show loop-detection</b> 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 <b>show storm-control</b> 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: アラーム LED の動作時間を 30 秒に設定する方法を示します。

```
# configure terminal
(config)# alarm warn-led duration 30
(config)#
```

### 2.3.3 alarm warn-led state enable

alarm warn-led state enable	
目的	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	<b>alarm warn-led state enable [cause {loop-detection   storm-control   all}]</b> <b>no alarm warn-led state enable</b>
パラメーター	<b>cause</b> (省略可能): アラーム LED で通知する機能を設定する場合に指定します。 <b>loop-detection</b> (省略可能): ループ検知による警告が発生したときに、アラーム LED で通知する場合に指定します。 <b>storm-control</b> (省略可能): ストームコントロールによる警告が発生したときに、アラーム LED で通知する場合に指定します。 <b>all</b> (省略可能): ループ検知またはストームコントロールによる警告が発生したときに、アラーム LED で通知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, port-channel)
特権レベル	レベル: 12
ガイドライン	インターフェース上でアラーム LED を有効にする際、その原因を指定できます。ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> コマンド) で設定してください。 <b>cause</b> を指定しない場合、ループ検知による警告のみ通知するように設定されています。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例: ポート 1/0/1 でストームコントロールによる警告が発生したときに、アラーム LED 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 warn-led state enable cause storm-control
(config-if-port)#
```

使用例：ポートチャンネル2でループ検知による警告が発生したときに、アラーム LED 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-channel 2
(config-if-port-channel)# alarm warn-led state enable cause loop-detection
(config-if-port-channel)#
```

### 2.3.4 show alarm warn-led

show alarm warn-led	
目的	アラーム LED の設定と状態を表示します。
シンタックス	<b>show alarm warn-led</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (省略可能) : アラーム LED の設定と状態を表示するインターフェイスを、以下のパラメーターで指定します。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	インターフェイスを指定しない場合、すべてのインターフェイスのアラーム LED の設定と状態が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：アラーム LED の設定と状態を表示する方法を示します。

```
# show alarm warn-led

Alarm Warning LEDs:
-----
Global State      : 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
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)
Port1/0/5        Disabled -              Inactive 0 second(s)
Port1/0/6        Disabled -              Inactive 0 second(s)
Port1/0/7        Disabled -              Inactive 0 second(s)
Port1/0/8        Disabled -              Inactive 0 second(s)
Port1/0/9        Disabled -              Inactive 0 second(s)
Port1/0/10       Disabled -              Inactive 0 second(s)
Port1/0/11       Disabled -              Inactive 0 second(s)
Port1/0/12       Disabled -              Inactive 0 second(s)
Port1/0/13       Disabled -              Inactive 0 second(s)
Port1/0/14       Disabled -              Inactive 0 second(s)
Port1/0/15       Disabled -              Inactive 0 second(s)
```

Port1/0/16	Disabled	-	Inactive	0	second(s)
Port1/0/17	Disabled	-	Inactive	0	second(s)
Port1/0/18	Disabled	-	Inactive	0	second(s)
Port1/0/19	Disabled	-	Inactive	0	second(s)
Port1/0/20	Disabled	-	Inactive	0	second(s)
Port1/0/21	Disabled	-	Inactive	0	second(s)
Port1/0/22	Disabled	-	Inactive	0	second(s)

Alarm Events:

(3)	(8)
Interface	Reason
-----	
Port1/0/1	Storm(BC)
Port1/0/2	Loop

項番	説明
(1)	アラーム LED のグローバル状態の有効/無効を表示します。
(2)	アラーム LED の動作時間を表示します。
(3)	インターフェース ID を表示します。
(4)	アラーム LED の有効/無効を表示します。
(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。 Storm Control : 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 All : ループ検知またはストームコントロールによる警告
(6)	アラーム LED の現在の状態を表示します。 Inactive : 非アクティブ Ready : アクティブ Warning : 警告
(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)	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 Storm(MC) : マルチキャストストーム Storm(DLF) : 未知のユニキャストストーム 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 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 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 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

使用例：ポート 1/0/1 からポート 1/0/5 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 1/0/1-5
```

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	

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)
Port1/0/5	Disabled	-	Inactive	0 second(s)
Alarm Events:				
(3)	(8)			
Interface	Reason			
-----				
Port1/0/1	Storm(BC)			
Port1/0/2	Loop			

項番	説明
(1)	アラーム LED のグローバル状態の有効／無効を表示します。
(2)	アラーム LED の動作時間を表示します。
(3)	インターフェース ID を表示します。
(4)	アラーム LED の有効／無効を表示します。
(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。 Storm Control : 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 All : ループ検知またはストームコントロールによる警告
(6)	アラーム LED の現在の状態を表示します。 Inactive : 非アクティブ Ready : アクティブ Warning : 警告
(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)	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 Storm(MC) : マルチキャストストーム Storm(DLF) : 未知のユニキャストストーム 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 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 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 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

使用例：ポートチャンネル 2 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-channel 2
```

Alarm Warning LEDs:				
-----				
Global State	:	Enabled	...	(1)
Duration	:	30 second(s)	...	(2)
(3)	(4)	(5)	(6)	(7)
Interface	State	Cause Enabled	Current Status	Warning Time Left
-----				
Port-channel2	Enabled	Loop Detection	Ready	30 second(s)
Alarm Events:				
(3)	(8)			

Interface	Reason
-----	

項番	説明
(1)	アラーム LED のグローバル状態の有効/無効を表示します。
(2)	アラーム LED の動作時間を表示します。
(3)	インターフェース ID を表示します。
(4)	アラーム LED の有効/無効を表示します。
(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。 Storm Control : 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 All : ループ検知またはストームコントロールによる警告
(6)	アラーム LED の現在の状態を表示します。 Inactive : 非アクティブ Ready : アクティブ Warning : 警告
(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)	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 Storm(MC) : マルチキャストストーム Storm(DLF) : 未知のユニキャストストーム 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 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 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 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

### 2.3.5 debug alarm warn-led test

debug alarm warn-led test	
目的	テストする目的で、アラーム LED を手動でオン/オフします。
シンタックス	<code>debug alarm warn-led [interface <i>INTERFACE-ID</i> [, -]] test</code>
パラメーター	<code>interface <i>INTERFACE-ID</i></code> (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。 <ul style="list-style-type: none"> <li>• <code>port</code> : 物理ポートを指定します。複数指定できます。</li> <li>• <code>port-channel</code> : ポートチャンネルを指定します。</li> </ul>
デフォルト	アラーム LED がオフ
コマンドモード	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	ポートのアラーム LED が「Ready(アクティブ)」または「Inactive(非アクティブ)」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。  アラーム LED の状態が「Warning(警告)」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(アクティブ)」になります。



debug alarm warn-led test	
	インターフェースを指定しない場合、すべてのインターフェースのアラーム 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、再びアラーム LED が動作する条件を満たした場合は、各アラーム LED が動作します。
対象バージョン	1.01.01

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。

```
# configure terminal
(config)# debug alarm warn-led interface port 1/0/1 test
(config)#
```

## 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。物理ポートの消費電力は、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	1.01.01

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) の有効または無効を表示します。
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) の有効または無効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	インターフェースを指定しない場合、すべてのインターフェースの省電力イーサネット (EEE) の有効または無効が表示されます。
制限事項	-

show eee	
注意事項	-
対象バージョン	1.01.01

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
1/0/5        Enabled
1/0/6        Enabled
1/0/7        Enabled
1/0/8        Enabled
1/0/9        Enabled
1/0/10       Enabled
1/0/11       Enabled
1/0/12       Enabled
1/0/13       Enabled
1/0/14       Enabled
1/0/15       Enabled
1/0/16       Enabled
1/0/17       Enabled
1/0/18       Enabled
1/0/19       Enabled
1/0/20       Enabled
1/0/21       -
1/0/22       -
1/0/23       -
1/0/24       -
```

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 (EEE) の有効／無効を表示します。

## 2.5 スタックコマンド

スタック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
stack bandwidth	stack bandwidth 10G {2-port   4-port} 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
snmp-server enable traps stack	snmp-server enable traps stack no snmp-server enable traps stack
show stack	show stack

### 2.5.1 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、 <b>no stack</b> コマンドを使用します。								
シンタックス	<b>stack bandwidth 10G {2-port   4-port}</b> <b>no stack</b>								
パラメーター	<b>10G</b> : SFP+ポート (10GBASE-R) をスタックポートとして割り当てる場合に指定します。 <b>2-port</b> : スタックポートの帯域幅を 2 ports に設定する場合に指定します。 <b>4-port</b> : スタックポートの帯域幅を 4 ports 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	特権実行モード								
特権レベル	レベル : 12								
ガイドライン	<p>スタックポートとして使用可能なポートは、本コマンドの設定により、スタックポートまたは通常のポートのいずれかとして機能します。</p> <p>スタックを構成する場合は、他のスタックメンバー装置と接続する前に、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。</p> <p>スタックポートの帯域幅の設定により、スタックポート 1 およびスタックポート 2 として動作するポートは以下のように異なります。</p> <table border="1"> <thead> <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> </thead> <tbody> <tr> <td>ApresiaNP</td> <td>10G 2-port</td> <td>ポート 1/0/23</td> <td>ポート 1/0/24</td> </tr> </tbody> </table>	装置	帯域幅の設定	スタックポート 1	スタックポート 2	ApresiaNP	10G 2-port	ポート 1/0/23	ポート 1/0/24
装置	帯域幅の設定	スタックポート 1	スタックポート 2						
ApresiaNP	10G 2-port	ポート 1/0/23	ポート 1/0/24						

stack bandwidth				
	4000-20Xt4X	10G 4-port	ポート 1/0/21 および ポート 1/0/23	ポート 1/0/22 および ポート 1/0/24
	<p>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スタック内の同じ装置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。</p> <p>本コマンドは、構成情報を保存し、装置を再起動するまで有効になりません。</p>			
制限事項	<p>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。</p> <p>本コマンドは、他のスタックメンバー装置が接続されている状態では設定できません。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• login</li> <li>• logout</li> <li>• reboot</li> <li>• enable</li> <li>• copy running-config startup-config</li> <li>• [no] stack renumber</li> <li>• stack my_box_id</li> <li>• write memory</li> </ul>			
注意事項	<p>スタック機能を利用する際には、スタックポートを 2 ポート使用し、リングトポロジーで接続することを推奨します。</p> <p>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。</p> <p>プリエンプトモード無効時のスタック構成において、<b>stack preempt</b> 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。</p> <p><b>no stack</b> コマンド実行後は装置を再起動してください。</p>			
対象バージョン	1.01.01			

使用例：スタックポートの帯域幅を 4 ports 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.
```

## 2.5.2 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

stack renumber	
	のコマンドを使用します。
シンタックス	<b>stack</b> <i>CURRENT-UNIT-ID</i> <b>renumber</b> <i>NEW-UNIT-ID</i> <b>no stack</b> <i>CURRENT-UNIT-ID</i> <b>renumber</b>
パラメーター	<i>CURRENT-UNIT-ID</i> : ボックス ID を手動で設定する装置のボックス ID を 1~4 の範囲で指定します。 <i>NEW-UNIT-ID</i> : 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
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	スタックが有効な場合に、マスターからスタックメンバーのボックス ID を手動で変更するときに使用します。  スタックが無効な場合、装置にボックス ID が割り当てられていません。装置が新たにスタックに追加されると、マスターによってボックス ID が自動割り当てされます。ボックス ID を割り当てられた後、 <b>write memory</b> コマンドを実行することで、ボックス ID を構成情報に保存できます。割り当てられたボックス ID は、次の再起動後から使用されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例: 装置 2 のボックス ID を「3」に再割り当てする方法を示します。

```
# stack 2 renumber 3
```

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

### 2.5.3 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	<b>stack</b> <i>CURRENT-UNIT-ID</i> <b>priority</b> <i>NEW-PRIORITY-NUMBER</i> <b>no stack</b> <i>CURRENT-UNIT-ID</i> <b>priority</b>
パラメーター	<i>CURRENT-UNIT-ID</i> : 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。 <i>NEW-PRIORITY-NUMBER</i> : 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	スタックが有効な場合に、マスターからスタックメンバーの優先度を手動で変更するときに使用します。  設定を保存すると、新しい優先度設定が個々の装置に保存されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：装置 2 の優先度を 10 に設定する方法を示します。

```
# stack 2 priority 10
```

### 2.5.4 stack my\_box\_id

stack my_box_id	
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	<b>stack my_box_id</b> <i>NEW-UNIT-ID</i> <b>no stack my_box_id</b>
パラメーター	<i>NEW-UNIT-ID</i> ：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
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	スタックを有効にする前に、装置のボックス ID を手動で指定する場合に使用します。  スタックが無効な場合、装置にボックス ID が割り当てられていません。装置が新たにスタックに追加されると、マスターによってボックス ID が自動割り当てされます。ボックス ID を割り当てられた後、 <b>copy running-config startup-config</b> コマンドを実行することで、ボックス ID を構成情報に保存できます。割り当てられたボックス ID は、次の再起動後から使用されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：装置のボックス ID を「3」に割り当てる方法を示します。

```
# stack my_box_id 3
```

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

### 2.5.5 stack my\_box\_priority

stack my_box_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	<b>stack my_box_priority</b> <i>NEW-PRIORITY-NUMBER</i> <b>no stack my_box_priority</b>
パラメーター	<i>NEW-PRIORITY-NUMBER</i> ：優先度の値を 1~63 の範囲で指定します。値が小さいほど優先度が高くなります。
デフォルト	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	スタックを有効にする前に、装置のスタックの優先度を手動で指定する場合に使用します。  設定を保存すると、新しい優先度設定が装置に保存されます。  複数の装置の優先度が同じ場合は、MAC アドレスが小さい装置が優先されます。
制限事項	-

stack my_box_priority	
注意事項	-
対象バージョン	1.01.01

使用例：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
```

### 2.5.6 stack preempt

stack preempt	
目的	より高い優先度の装置がスタック構成に追加されたときに、マスターの役割を差し替える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	<b>stack preempt</b> <b>no stack preempt</b>
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	-
制限事項	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。  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	-
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
```

### 2.5.7 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	<b>snmp-server enable traps stack</b> <b>no snmp-server enable traps stack</b>
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、 <b>snmp-server enable traps</b> 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)#
```

## 2.5.8 show stack

show stack	
目的	スタック情報を表示します。
シンタックス	<b>show stack</b>
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-NP4000 Ver. 1.02.01以降では <b>show version</b> コマンドを使用してください。AEOS-NP4000 Ver. 1.01.02以前では <b>show mac-address-table</b> コマンドを使用してください。
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)

Topology                : Duplex_Ring ... (4)
My Box ID               : 1 ... (5)
Master ID               : 1 ... (6)
BK Master ID           : 2 ... (7)
Box Count               : 2 ... (8)
(9) (10) (11)           (12) (13) (14)           (15) (16) (17)
Box User Module         Prio-           Prom      Runtime  H/W
ID Set Name            Exist rity MAC          Version   Version  Version
-----
1  Auto ApresiaNP4000-20Xt4X Exist 0      00-40-66-AF-F0-48 1.00.00  1.01.01  A
2  Auto ApresiaNP4000-20Xt4X Exist 32     00-40-66-AF-F1-87 1.00.00  1.01.01  A
3  -   NOT_EXIST          No
4  -   NOT_EXIST          No

Stack Bandwidth:
(9) (18) (19) (20)
Box  User Set  SIO1 Active  SIO2 Active
ID   Bandwidth  Bandwidth    Bandwidth
----
1    2-port(10G) 1-port      1-port
2    2-port(10G) 1-port      1-port
3
4
```

項番	説明
(1)	スタックの有効/無効を表示します。
(2)	プリエンプトモードの有効/無効を表示します。
(3)	トラップの有効/無効を表示します。
(4)	スタックトポロジを表示します。 Duplex_Chain : チェーントポロジ Duplex_Ring : リングトポロジ
(5)	装置のボックス ID を表示します。
(6)	マスターのボックス ID を表示します。
(7)	バックアップマスターのボックス ID を表示します。
(8)	スタックを構成している装置の数を表示します。
(9)	ボックス ID を表示します。
(10)	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
(11)	装置の名称を表示します。
(12)	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。
(13)	優先度を表示します。
(14)	MAC アドレスを表示します。
(15)	ブートローダーバージョンを表示します。
(16)	ファームウェアバージョンを表示します。
(17)	ハードウェアリビジョンを表示します。
(18)	<b>stack bandwidth</b> コマンドで設定したポート構成を表示します。
(19)	スタックポート 1 の接続状態を表示します。
(20)	スタックポート 2 の接続状態を表示します。

## 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

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
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	<b>help</b>
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	<p>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。</p> <p>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。</p> <p>コマンドのパラメーターと引数のリストを表示する場合、コマンドラインで、パラメーターまたは引数の代わりにクエスチョンマーク (?) を入力します。すでに入力したコマンド、パラメーター、および引数に基づいて、該当するパラメーターや引数がリスト表示されます。コマンドシンタックスヘルプと呼ばれる機能です。</p>

help	
	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	<b>enable</b> [ <i>PRIVILEGE-LEVEL</i> ]
パラメーター	<i>PRIVILEGE-LEVEL</i> (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

enable	
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	<b>disable</b> [ <i>PRIVILEGE-LEVEL</i> ]
パラメーター	<i>PRIVILEGE-LEVEL</i> (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 <b>disable</b> 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	<b>login</b>
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	CLI で <b>login</b> コマンドを実施すると、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	-

login (EXEC)	
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	<b>logout</b>
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	<b>configure terminal</b>
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 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

show version	
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 1.02.01 : 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      ApresiaNP4000-20Xt4X    H/W:A
                               Bootloader:1.00.00
                               Runtime:1.01.01
                               CPLD:10
```

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-NP4000 Ver. 1.02.01 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-NP4000 Ver. 1.01.02 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。

### 3.1.10 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	<b>show environment [fan   memory   power   temperature   health]</b>
パラメーター	<b>fan</b> (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。 <b>memory</b> (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。 <b>power</b> (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。 <b>temperature</b> (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。 <b>health</b> (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	表示する情報の種類を指定しない場合、すべての環境情報が表示されます。
制限事項	-
注意事項	-



show environment

対象バージョン | 1.01.01

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      25C

Detail Fan Status: ... (4)
-----

Unit 1:
  Fan 1 (OK)      Fan 2 (OK)      Fan 3 (OK)
  Fan 4 (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。
(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。

項番	説明
(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：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      25C
2         Normal      24C

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

Detail Power Status:
```

3 基礎知識 | 3.1 基本 CLI コマンド

```

(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  0                 0

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

項番	説明
	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。

### 3.1.11 show unit

show unit	
目的	システムユニットの情報を表示します。

show unit	
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装置のボックス ID を指定しない場合、すべてのスタックメンバー装置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      ApresiaNP4000-20Xt4X
 2      ApresiaNP4000-20Xt4X
(1)          (3)          (4)          (5)
Unit          Serial-Number          Status          Up Time
-----
 1      400010000034          ok          ODT0H4M22S
 2      400010000040          ok          ODT0H4M21S
(1)  (6)  (7)  (8)  (9)
Unit  Memory  Total  Used  Free
-----
 1      DRAM  2097152 K  194512 K  1902640 K
 1      FLASH  523776 K  24906 K  498870 K
 2      DRAM  2097152 K  194397 K  1902755 K
 2      FLASH  523776 K  25258 K  498518 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)	連続稼働時間を表示します。
(6)	メモリー種別を表示します。
(7)	メモリー容量を表示します。
(8)	使用中のメモリー容量を表示します。
(9)	未使用のメモリー容量を表示します。

### 3.1.12 show cpu utilization

show cpu utilization	
目的	CPU 使用率の情報を表示します。

show cpu utilization	
シンタックス	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	ユーザー実行モード、特権実行モード、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：CPU 使用率の情報を表示する方法を示します。

```
# show cpu utilization

CPU Utilization
(1)                    (2)                    (3)
Five seconds - 4 %    One minute - 5 %    Five minutes - 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。

### 3.1.13 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 [ <i>DIRECTORY-URL</i> ]
パラメーター	<i>DIRECTORY-URL</i> (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	-
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 14:46:11  log
 2  -rw          1664 Dec 18 2020 14:45:36  primary.cfg
 3  -rw      8431260 Oct 02 2020 14:07:56  AEOS-NP4000_R10202.had
 4  -rw      8431260 Dec 18 2020 14:34:38  AEOS-NP4000_R10202_sec.had
 5  -rw          1384 Dec 18 2020 14:35:22  secondary.cfg
 6  d--          0 Dec 18 2020 05:43:48  system

536346624 bytes total (514832384 bytes free)

# cd log
# dir

Directory of /c:/log
No files in directory
536346624 bytes total (514832384 bytes free)
```

### 3 基礎知識 | 3.2 ファイルシステムコマンド

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	<b>delete</b> <i>FILE-URL</i>
パラメーター	<i>FILE-URL</i> : 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	<b>boot image</b> コマンドで指定したブートイメージファイル、および <b>boot config</b> 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。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：「test.txt」という名前のファイル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：スタック構成の装置において、ボックス ID 2 の装置の「test.txt」という名前のファイル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	<b>dir</b> [ <i>URL</i> ]
パラメーター	<i>URL</i> (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
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。 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、 <b>show storage media-info</b> コマンドを使用して表示できます。
制限事項	-
注意事項	-



dir	
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      8431260 Oct 02 2020 14:07:56 AEOS-NP4000_R10202.had
2  -rw      8431260 Dec 18 2020 14:34:38 AEOS-NP4000_R10202_sec.had
3  -rw           1384 Dec 18 2020 14:49:36 primary.cfg
4  -rw           1384 Dec 18 2020 14:49:37 secondary.cfg
5  d--              0 Dec 18 2020 05:53:44 system

536346624 bytes total (514824192 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：スタック構成の装置において、ボックス ID 2 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      8431260 Oct 02 2020 14:07:56 AEOS-NP4000_R10202.had
2  -rw      8431260 Dec 18 2020 14:34:38 AEOS-NP4000_R10202_sec.had
3  -rw           1384 Dec 18 2020 14:49:36 primary.cfg
4  -rw           1384 Dec 18 2020 14:49:37 secondary.cfg
5  d--              0 Dec 18 2020 05:53:44 system

536346624 bytes total (514824192 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。

項番	説明
	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	<b>mkdir</b> <i>DIRECTORY-NAME</i>
パラメーター	<i>DIRECTORY-NAME</i> : 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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例 : 「newdir」という名前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 : スタック構成の装置において、ボックス ID 2 の装置に「test\_dir」という名前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	<b>more</b> <i>FILE-URL</i>
パラメーター	<i>FILE-URL</i> : 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	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。

more	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ファイル「primary.cfg」の内容を表示する方法を示します。

```
# more primary.cfg

#-----
#                               ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch
#                               Configuration
#
#                               Firmware: Build 1.02.02
#                               Copyright(C) 2018 APRESIA Systems, Ltd. All rights reserved.
#-----

# Date: Fri Dec 18 14:35:21 2020

# STACK

no stack
no stack my_box_id
stack my_box_priority 32
no stack preempt

# PORT

interface port 1/0/1
interface port 1/0/2
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

使用例：スタック構成の装置において、ボックス ID 2 の装置のファイル「primary.cfg」の内容を表示する方法を示します。

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

#-----
#                               ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch
#                               Configuration
#
#                               Firmware: Build 1.02.02
#                               Copyright(C) 2018 APRESIA Systems, Ltd. All rights reserved.
#-----

# Date: Fri Dec 18 14:45:36 2020

# STACK

## stacking config information
## #Box          Prio-
## #ID   Type      Exist rity
## #---  -----  -----
## #  1 ApresiaNP4000-20Xt4X exist 10
## #  2 ApresiaNP4000-20Xt4X 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	<b>rename</b> <i>FILE-URL1</i> <i>FILE-URL2</i>
パラメーター	<i>FILE-URL1</i> : 名前を変更するファイルの URL を指定します。 <i>FILE-URL2</i> : 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	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: 「doc1.txt」というファイルの名前を「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: スタック構成の装置において、ボックス ID 2 の装置の「before.txt」というファイルの名前を「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	<b>rmdir</b> <i>DIRECTORY-NAME</i>
パラメーター	<i>DIRECTORY-NAME</i> : 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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例: 「newdir」という名前のディレクトリー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：スタック構成の装置において、ボックス ID 2 の装置の「test\_dir」という名前のディレクトリ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	<b>show storage media-info</b> [unit <i>UNIT-ID</i> ]
パラメーター	<b>unit</b> <i>UNIT-ID</i> (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	スタック構成で特定の装置のボックス ID を指定しない場合、すべてのスタックメンバー装置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 511 MB FFS
1 d: SD Card 944 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	<b>terminal length default</b> NUMBER <b>no terminal length default</b>
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	-
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	<b>terminal width default</b> <i>NUMBER</i> <b>no terminal width default</b>
パラメーター	<i>NUMBER</i> : 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	-
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	<b>terminal speed</b> <i>BPS</i> <b>no terminal speed</b>
パラメーター	<i>BPS</i> : 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	-
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	<b>show terminal</b>
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
  Width: 80 columns
  Default Length: 24 lines
  Default Width: 80 columns
  Baud Rate: 9600 bps
```

## 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、 <b>no terminal length</b> コマンドを使用します。
シンタックス	<b>terminal length</b> <i>NUMBER</i> <b>no terminal length</b>
パラメーター	<i>NUMBER</i> : 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。
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、 <b>no terminal width</b> コマンドを使用します。
シンタックス	<b>terminal width</b> <i>NUMBER</i> <b>no terminal width</b>
パラメーター	<i>NUMBER</i> : 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	username NAME [privilege LEVEL] [nopassword   password [0   7] PASSWORD] no username [NAME]
パラメーター	NAME: ユーザーアカウントのユーザー名を最大 32 文字で指定します。 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。 nopassword (省略可能): 作成するユーザーアカウントにパスワードを設定しな

username	
	<p>い場合に指定します。</p> <p><b>password</b> (省略可能) : ユーザーアカウントのパスワードを指定します。</p> <p><b>0</b> (省略可能) : パスワードを平文で入力する場合に指定します。パスワードのデフォルト設定です。</p> <p><b>7</b> (省略可能) : 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。</p> <p><i>PASSWORD</i> (省略可能) : 平文で入力する場合は、文字列を最大 32 文字で指定します。文字列には、スペースを含めることができます。暗号化した形式で入力する場合は、文字列を 35 文字で指定します。いずれの場合も、大文字と小文字が区別されます。</p>
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	<p>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、<b>enable</b> コマンドを実行してください。</p> <p>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。</p> <p>ユーザー名を指定せずに <b>no username</b> 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。</p> <p>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、<b>enable</b> コマンドを実行します。</p>
制限事項	-
注意事項	username 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である「ap_recovery」を使用することはできません。
対象バージョン	1.01.01

使用例 : ユーザー名が「admin」、パスワードが「mypassword」の管理用ユーザーアカウントを作成する方法を示します。

```
# configure terminal
(config)# username admin privilege 15 password 0 mypassword
(config)#
```

使用例 : ユーザー名が「admin」のユーザーアカウントを削除する方法を示します。

```
# configure terminal
(config)# no username admin
(config)#
```

### 3.4.2 enable password

enable password	
目的	異なる特権レベルに遷移する enable password を設定します。空の文字列にパスワードを戻す場合は、 <b>no enable password</b> コマンドを使用します。
シンタックス	<b>enable password</b> [level <i>PRIVILEGE-LEVEL</i> ] [0   7] <i>PASSWORD</i> <b>no enable password</b> [level <i>PRIVILEGE-LEVEL</i> ]

enable password	
パラメーター	<p><b>level</b> <i>PRIVILEGE-LEVEL</i> (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。<b>enable password</b> コマンド、または <b>no enable password</b> コマンドで引数を指定しない場合、特権レベルはデフォルトの 15 (従来の有効化特権) に設定されます。</p> <p><b>0</b> (省略可能) : パスワードを平文で入力する場合に指定します。パスワードのデフォルト設定です。</p> <p><b>7</b> (省略可能) : 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。</p> <p><b>PASSWORD</b> : 平文で入力する場合は、文字列を最大 32 文字で指定します。文字列には、スペースを含めることができます。暗号化した形式で入力する場合は、文字列を 35 文字で指定します。いずれの場合も、大文字と小文字が区別されません。</p>
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	<p><b>enable password</b> 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である「ap_recovery」を使用することはできません。</p> <p><b>enable password</b> 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。</p>
対象バージョン	1.01.01

使用例 : 特権レベル 15 で「MyEnablePassword」というパスワードで **enable password** 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	<p><b>service user-account encryption</b></p> <p><b>no service user-account encryption</b></p>
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

service user-account encryption	
	<p>たに設定した場合でも、暗号化されて設定されます。</p> <ul style="list-style-type: none"> <li>• <code>username</code> コマンド</li> <li>• <code>enable password</code> コマンド</li> <li>• <code>password</code> コマンド</li> <li>• <code>aaa-local-db user</code> コマンド</li> <li>• <code>mac-authentication password</code> コマンド</li> <li>• <code>snmp-server community</code> コマンド</li> <li>• <code>snmp-server host</code> コマンド</li> <li>• <code>snmp-server user</code> コマンド</li> <li>• <code>snmp-server group</code> コマンド</li> <li>• <code>radius-server host</code> コマンド</li> <li>• <code>tacacs-server host</code> コマンド</li> </ul> <p>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。</p>
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	<code>prompt STRING</code> <code>no prompt</code>
パラメーター	<p><i>STRING</i>：プロンプトを定義する文字列を最大 35 文字で指定します。最初の 15 文字のみ表示されます。指定した文字、または以下の制御文字に基づいたプロンプトになります。</p> <ul style="list-style-type: none"> <li>• <code>%h</code>：SNMP エージェント名</li> <li>• <code>%s</code>：スペース</li> <li>• <code>%%</code>：%記号</li> </ul>
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	<p>ユーザーが SNMP エージェント名を指定した場合、最初の 15 文字だけ表示されます。プロンプトの最大表示文字数は 15 文字です。特権レベルの文字は、プロンプトの最後の文字として表示されます。</p> <p>文字は、以下のように定義されます。</p> <ul style="list-style-type: none"> <li>• <code>'&gt;</code> ユーザーレベルを表します。</li> <li>• <code>'#</code> 特権ユーザーレベルを表します。</li> </ul>
制限事項	-

prompt	
注意事項	-
対象バージョン	1.01.01

使用例：Administrator 権限を使用するプロンプトを「BRANCH A」に変更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	<b>banner login</b> <i>cMESSAGEc</i> <b>no banner login</b>
パラメーター	<i>c</i> ：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。  <i>MESSAGE</i> ：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
```

### 3 基礎知識 | 3.4 アクセス管理コマンド

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。

login (Line)	
デフォルト	ラインセッション(コンソール) : <b>no login</b> (無効) ラインセッション(Telnet) : <b>login</b> (パスワードの入力が必要) ラインセッション(SSH) : <b>login</b> (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	<p>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。</p> <ul style="list-style-type: none"> <li>ログイン方法が無効 <b>no login</b> 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。</li> <li>ログイン方法が <b>login</b> 設定で <b>password</b> 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。</li> <li>ログイン方法が <b>login local</b> 設定の場合は、ローカルのユーザーアカウント (<b>username</b> 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。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>SSH 公開鍵</li> <li>ホストベース認証</li> <li>パスワード認証</li> </ul> <p>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 <b>username</b> 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。</p> <ul style="list-style-type: none"> <li>ログイン方法が <b>no login</b> 設定の場合、認証時にパスワードが無視されます。<b>username</b> 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。</li> <li>ログイン方法が <b>login</b> 設定の場合は <b>password</b> コマンドでパスワードの設定が必要です。<b>username</b> コマンドで設定したユーザー名と、<b>password</b> 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。</li> <li>ログイン方法が <b>login local</b> 設定の場合は、ローカルのユーザーアカウント (<b>username</b> 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。</li> </ul>
制限事項	本コマンドは、AAA が無効 ( <b>no aaa new-model</b> (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	<b>password</b> [0   7] <i>PASSWORD</i> <b>no password</b>
パラメーター	0 (省略可能) : パスワードを平文で入力する場合に指定します。パスワードのデフォルト設定です。  7 (省略可能) : 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。  <i>PASSWORD</i> : 平文で入力する場合は、文字列を最大 32 文字で指定します。文字列には、スペースを含めることができます。暗号化した形式で入力する場合は、文字列を 35 文字で指定します。いずれの場合も、大文字と小文字が区別されません。
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	password 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である「ap_recovery」を使用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	<b>session-timeout</b> <i>MINUTES</i> <b>no session-timeout</b>
パラメーター	<i>MINUTES</i> : 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

session-timeout	
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	<p>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 <b>login local</b> 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。</p> <ul style="list-style-type: none"> <li>• <b>session-timeout 0 or 1</b> 設定時 : リトライ回数は 1 回</li> <li>• <b>session-timeout 2</b> 設定時 : リトライ回数は 2 回</li> <li>• <b>session-timeout 3</b> 以上に設定時 : リトライ回数は 3 回</li> </ul> <p>ラインセッション (SSH) のログイン処理のリトライ回数は、<b>ip ssh authentication-retries</b> コマンドで設定します。</p>
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)経由のアクセスを制限する標準 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。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	<b>access-class</b> <i>IP-ACL-NAME</i> <b>no access-class</b> <i>IP-ACL-NAME</i>
パラメーター	<i>IP-ACL-NAME</i> : 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。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	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	<p>各ラインセッション(Telnet、SSH)ごとに最大 2 つのアクセスリストを適用できます。</p> <p>本機能は、装置宛てパケットの送信元 IPv4/IPv6 アドレスのみをチェックします。</p> <p>指定した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。</p> <p>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。</p>
制限事項	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	<b>show users</b>
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	<b>show privilege</b>
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	<b>clear line</b> <i>LINE-ID</i>
パラメーター	<i>LINE-ID</i> : 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、 <b>show users</b> 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
ip mtu	ip mtu BYTES no ip mtu
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 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IP アドレスを設定します。また、マネジメントポートの 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	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) : 設定する IPv4 アドレスをセカンダリーIP アドレスにす

ip address	
	<p>る場合に指定します。secondary を指定しない場合、設定する IPv4 アドレスはプライマリーIP アドレスになります。マネージメントポートには設定できません。</p> <p><b>dhcp</b> : DHCP で VLAN インターフェースの IP 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には設定できません。</p>
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	<p>手動割り当ての場合、ユーザーは VLAN に複数の IP アドレスを指定して、複数のネットワークを割り当てます。複数の IP アドレスのうち、いずれか 1 つをプライマリーIP アドレスにします。残りはセカンダリーIP アドレスです。プライマリーアドレスは、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 メッセージの送信元 IP アドレスとして使用されます。</p> <p>マネージメントポートにセカンダリーIP アドレスは割り当てられません。</p>
制限事項	<p>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。</p> <p>装置全体に設定可能な IPv4 アドレス数は、セカンダリーIP 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。</p>
注意事項	<b>ip address dhcp</b> コマンドを設定したインターフェースでセカンダリーIP アドレスを設定することは未サポートです。
対象バージョン	1.01.01

使用例 : VLAN 100 インターフェースで、10.108.1.27 をプライマリーアドレスに、192.31.7.17 と 192.31.8.17 をセカンダリー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 address 10.108.1.27/24
(config-if-vlan)# ip address 192.31.7.17/24 secondary
(config-if-vlan)# ip address 192.31.8.17/24 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 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	<b>ip default-gateway</b> <i>IP-ADDRESS</i> <b>no ip default-gateway</b> <i>IP-ADDRESS</i>
パラメーター	<i>IP-ADDRESS</i> : デフォルトゲートウェイの IP アドレスを指定します。
デフォルト	デフォルトゲートウェイの IP アドレスは 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	他の IP サブネット宛ての IP パケットは、デフォルトゲートウェイに送信されません。
制限事項	-

ip default-gateway (mgmt 0)	
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 IP アドレスを 10.20.30.40 に設定する方法を示します。

```
# configure terminal
(config)# interface mgmt 0
(config-if-mgmt)# ip default-gateway 10.20.30.40
(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	<b>ip proxy-arp</b> <b>no ip proxy-arp</b>
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	<p>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。</p> <ul style="list-style-type: none"> <li>装置に直接接続されている、プロキシ ARP を有効にした IP インターフェース以外のネットワーク宛での ARP リクエスト</li> <li>ルートテーブルに経路情報が登録されているネットワーク宛での ARP リクエスト</li> </ul>
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	<b>ip local-proxy-arp</b> <b>no ip local-proxy-arp</b>
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)

ip local-proxy-arp	
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、 <b>ip proxy-arp</b> 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-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 ip mtu

ip mtu	
目的	IPv4 の MTU 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	<b>ip mtu BYTES</b> <b>no ip mtu</b>
パラメーター	<i>BYTES</i> : IP MTU 値を 512~16,383 バイトの範囲で指定します。
デフォルト	1500 バイト
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	IPv4 の MTU 値は、ルーティング対象の IPv4 パケットの上限サイズ（イーサネットヘッダーと FCS を除いたサイズ）を決定します。MTU 値を超過したルーティング対象の IPv4 パケットは破棄されます。  ICMP などの装置の自発パケットが MTU 値を超過する場合は、フラグメントされて送信されます。
制限事項	IPv4 と IPv6 の併用環境で本コマンドを設定する場合は、 <b>ipv6 mtu</b> コマンドも同じ値に設定する必要があります。
注意事項	IPv4 パケットをルーティングする際に、ARP Request を送信して ARP 解決を行うトリガーとなる IPv4 パケットの上限サイズ（イーサネットヘッダーと FCS を除いたサイズ）は 2026 バイトです。それ以上のサイズの IPv4 パケットをトリガーとしては ARP 解決できないため、必要な場合はスタティック ARP エントリーを使用してください。
対象バージョン	1.01.01

使用例：VLAN 4 インターフェースの IPv4 MTU 値を 6000 バイトに設定する方法を示します。

```
# configure terminal
(config)# interface vlan 4
```



```
(config-if-vlan)# ip mtu 6000
(config-if-vlan)#
```

### 3.5.6 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	<b>arp</b> <i>IP-ADDRESS</i> <i>MAC-ADDRESS</i> <b>no arp</b> <i>IP-ADDRESS</i> <i>MAC-ADDRESS</i>
パラメーター	<i>IP-ADDRESS</i> : スタティックエントリーの IP アドレスを指定します。 <i>MAC-ADDRESS</i> : 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。 <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul>
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、 <b>mac-address-table static</b> 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。 ユニキャスト MAC アドレスのスタティック MAC アドレスエントリーが最大 256 個のため、スタティック ARP エントリーも最大 256 個以内で使用してください。
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)#
```

### 3.5.7 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	<b>arp timeout</b> <i>MINUTES</i> <b>no arp timeout</b>
パラメーター	<i>MINUTES</i> : 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。

arp timeout	
	ルートのネクストホップの ARP エントリは、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 エントリを消去するには、 <b>clear arp-cache</b> 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)#
```

### 3.5.8 show ip interface

show ip interface	
目的	IP インターフェース情報を表示します。
シンタックス	<b>show ip interface</b> [ <i>INTERFACE-ID</i> ] [ <b>brief</b> ]
パラメーター	<i>INTERFACE-ID</i> (省略可能)：情報を表示する IP インターフェースを、以下のパラメーターで指定します。 <ul style="list-style-type: none"> <li>• <b>mgmt</b>：マネージメントポートを指定します。</li> <li>• <b>vlan</b>：VLAN インターフェースを指定します。</li> </ul> <b>brief</b> (省略可能)：IP 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	パラメーターを指定しない場合、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：IP 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)	IP 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 IP 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 down
  IP address is 0.0.0.0/0 (Manual) ... (3)
  ARP timeout is 240 minutes ... (4)
  IP MTU is 1500 bytes ... (5)
  Proxy ARP is disabled ... (6)
  IP Local Proxy ARP is disabled ... (7)
  Gratuitous-send is disabled, interval is 0 seconds ... (8)
```

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)	IP 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)	IPv4 インターフェースの MTU を表示します。
(6)	プロキシ ARP の有効/無効を表示します。
(7)	ローカルプロキシ ARP の有効/無効を表示します。
(8)	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。

### 3.5.9 show arp

show arp	
目的	ARP テーブルのエントリを表示します。
シンタックス	<b>show arp</b> [ <i>ARP-TYPE</i>   <i>IP-ADDRESS</i> [ <i>MASK</i> ]   <b>interface</b> <i>INTERFACE-ID</i>   <i>MAC-ADDRESS</i> ]
パラメーター	<p><i>ARP-TYPE</i> (省略可能)：表示するエントリの種類を、以下のパラメーターで指定します。</p> <ul style="list-style-type: none"> <li><b>dynamic</b>：ダイナミックエントリを指定します。</li> <li><b>static</b>：スタティックエントリを指定します。</li> </ul> <p><i>IP-ADDRESS</i> [<i>MASK</i>] (省略可能)：表示するエントリの IP 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。</p> <p><b>interface</b> <i>INTERFACE-ID</i> (省略可能)：エントリ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。</p> <ul style="list-style-type: none"> <li><b>mgmt</b>：マネージメントポートを指定します。</li> <li><b>vlan</b>：VLAN インターフェースを指定します。</li> </ul> <p><i>MAC-ADDRESS</i> (省略可能)：表示するエントリの MAC アドレスを、以下のいずれかの形式で指定します。</p> <ul style="list-style-type: none"> <li>XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul>
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 arp	
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、ARP テーブルのすべてのエントリが表示されます。
制限事項	-
注意事項	ARP-TYPE に <b>static</b> を指定した場合、未使用のスタティックエントリも表示されます。未使用のスタティックエントリは、IP 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の種類を表示します。 S - Static Entry：スタティックエントリ
(2)	IP アドレスを表示します。
(3)	MAC アドレスを表示します。
(4)	エントリを学習した IP 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、またはスタティックエントリの場合は forever と表示されます。マネージメントポートで学習したダイナミックエントリの場合は 0 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	<b>show arp timeout [interface vlan VLAN-ID]</b>
パラメーター	<b>vlan VLAN-ID</b> (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	インターフェースを指定しない場合、すべての VLAN インターフェースの ARP エージングタイムが表示されます。
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	<b>clear arp-cache</b> { <b>all</b>   <b>interface</b> <i>INTERFACE-ID</i>   <i>IP-ADDRESS</i> }
パラメーター	<p><b>all</b> : 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。</p> <p><b>interface</b> <i>INTERFACE-ID</i> : ダイナミックエントリーをすべて消去する IP インターフェースを、以下のパラメーターで指定します。</p> <ul style="list-style-type: none"> <li>• <b>vlan</b> : VLAN インターフェースを指定します。</li> <li>• <b>mgmt</b> : マネージメントポートを指定します。</li> </ul> <p><i>IP-ADDRESS</i> : ダイナミックエントリーを消去する IP アドレスを指定します。</p>
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 hop-limit	ipv6 hop-limit VALUE no ipv6 hop-limit
ipv6 mtu	ipv6 mtu BYTES no ipv6 mtu
ipv6 nd suppress-ra	ipv6 nd suppress-ra no ipv6 nd suppress-ra
ipv6 nd managed-config-flag	ipv6 nd managed-config-flag no ipv6 nd managed-config-flag
ipv6 nd other-config-flag	ipv6 nd other-config-flag no ipv6 nd other-config-flag
ipv6 nd prefix	ipv6 nd prefix IPV6-PREFIX/PREFIX-LENGTH VALID-LIFETIME PREFERRED-LIFETIME [off-link] [no-autoconfig] no ipv6 nd prefix IPV6-PREFIX/PREFIX-LENGTH
ipv6 nd ra interval	ipv6 nd ra interval MAX-SECS [MIN-SECS] no ipv6 nd ra interval
ipv6 nd ra lifetime	ipv6 nd ra lifetime SECONDS no ipv6 nd ra lifetime
ipv6 nd reachable-time	ipv6 nd reachable-time MILLI-SECONDS no ipv6 nd reachable-time
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]
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	<b>ipv6 enable</b> <b>no ipv6 enable</b>
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	<b>ipv6 enable</b> 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。
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	<b>ipv6 address</b> { <i>IPV6-ADDRESS/PREFIX-LENGTH</i>   <i>PREFIX-NAME SUB-BITS/PREFIX-LENGTH</i>   <i>IPV6-ADDRESS link-local</i> } <b>no ipv6 address</b> { <i>IPV6-ADDRESS/PREFIX-LENGTH</i>   <i>PREFIX-NAME SUB-BITS/PREFIX-LENGTH</i>   <i>IPV6-ADDRESS link-local</i> }
パラメーター	<i>IPV6-ADDRESS/PREFIX-LENGTH</i> : IPv6 アドレスとプレフィックス長を指定します。  <i>PREFIX-NAME SUB-BITS/PREFIX-LENGTH</i> : 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。 <ul style="list-style-type: none"> <li>• <i>PREFIX-NAME</i> : プレフィックス名を指定します。</li> <li>• <i>SUB-BITS</i> : 委譲されたプレフィックス部以外の値を指定します。</li> <li>• <i>PREFIX-LENGTH</i> : プレフィックス長を指定します。</li> </ul> <i>IPV6-ADDRESS link-local</i> : リンクローカルアドレスを指定します。

ipv6 address	
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	<p>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。</p> <p>VLAN インターフェースで本設定を実施すると、<b>ipv6 enable</b> も自動的に設定されます。</p>
制限事項	<p>IPv6 アドレスは、マネージメントポートには設定できません。</p> <p>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。</p> <p>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。</p>
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



ipv6 address eui-64	
	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	<b>ipv6 address IPV6-PREFIX/PREFIX-LENGTH eui-64</b> <b>no ipv6 address IPV6-PREFIX/PREFIX-LENGTH eui-64</b>
パラメーター	<i>IPV6-PREFIX</i> : 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。 <i>PREFIX-LENGTH</i> : 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、 <b>ipv6 enable</b> 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。
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	<b>ipv6 address dhcp [rapid-commit]</b> <b>no ipv6 address dhcp</b>
パラメーター	<b>rapid-commit</b> (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	<b>rapid-commit</b> 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、 <b>ipv6 enable</b> 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 dhcp	
	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。
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。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ipv6 address autoconfig [default]</b> <b>no ipv6 address autoconfig</b>
パラメーター	<b>default</b> (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、他のルーターから受信した Router Advertisement メッセージ内のプレフィックス情報と、対象 VLAN インターフェースのインターフェース ID に基づいて、IPv6 アドレスが自動構成されます。  <b>default</b> を指定した場合、受信した Router Advertisement に基づいて、ルートタイプが SLAAC (Stateless address autoconfiguration) のデフォルトルートが IPv6 ルーティングテーブルに登録されます。  本設定を実施すると、 <b>ipv6 enable</b> 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。
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 hop-limit

ipv6 hop-limit	
目的	装置に IPv6 ホップリミットを設定します。デフォルト設定に戻すには、no 形式

ipv6 hop-limit	
	のコマンドを使用します。
シンタックス	<b>ipv6 hop-limit</b> <i>VALUE</i> <b>no ipv6 hop-limit</b>
パラメーター	<i>VALUE</i> : IPv6 ホップリミットを 0~255 の範囲で指定します。0 を指定した場合、デフォルトを使用してパケットを送信します。
デフォルト	64
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	指定したホップリミットは、本装置で発生した IPv6 パケットにも使用されません。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例: IPv6 ホップリミット値を設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 hop-limit 255
(config-if-vlan)#
```

### 3.6.7 ipv6 mtu

ipv6 mtu	
目的	IPv6 の MTU 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	<b>ipv6 mtu</b> <i>BYTES</i> <b>no ipv6 mtu</b>
パラメーター	<i>BYTES</i> : IPv6 MTU 値を 1,280~65,534 バイトの範囲で指定します。
デフォルト	1500 バイト
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 の MTU 値は、ルーティング対象の IPv6 パケットの上限サイズ（イーサネットヘッダーと FCS を除いたサイズ）を決定します。MTU 値を超過したルーティング対象の IPv6 パケットは破棄されます。  ICMPv6 などの装置の自発パケットが MTU 値を超過する場合は、フラグメントされて送信されます。  本コマンドは RA メッセージでアドバタイズされる MTU 値も変更します。
制限事項	本コマンドを設定する場合には <b>ip mtu</b> コマンドも同じ値に設定する必要があります。
注意事項	本コマンドは最大 1712 バイトまでサポートしています。
対象バージョン	1.01.01

使用例: VLAN 4 インターフェースの IPv6 MTU 値を 1712 バイトに設定する方法を示します。

```
# configure terminal
(config)# interface vlan 4
(config-if-vlan)# ipv6 mtu 1712
(config-if-vlan)# exit
```

```
(config)#
```

使用例：デフォルトの IPv6 MTU 値に戻す方法を示します。

```
# configure terminal
(config)# interface vlan 4
(config-if-vlan)# no ipv6 mtu
(config-if-vlan)#
```

### 3.6.8 ipv6 nd suppress-ra

ipv6 nd suppress-ra	
目的	RA メッセージの送信抑制を有効にします。送信抑制を無効にして RA メッセージを送信するには、 <b>no ipv6 nd suppress-ra</b> コマンドを使用します。
シンタックス	<b>ipv6 nd suppress-ra</b> <b>no ipv6 nd suppress-ra</b>
パラメーター	なし
デフォルト	RA メッセージの送信抑制が有効で、RA メッセージを送信しない ( <b>ipv6 nd suppress-ra</b> )
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	RA メッセージを送信する場合は <b>no ipv6 nd suppress-ra</b> コマンドで送信の抑制を無効にしてください。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 インターフェースで、RA メッセージを送信するために送信の抑制を無効にする方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# no ipv6 nd suppress-ra
(config-if-vlan)#
```

### 3.6.9 ipv6 nd managed-config-flag

ipv6 nd managed-config-flag	
目的	RA メッセージの M フラグ (Managed address configuration flag) を ON(1)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	<b>ipv6 nd managed-config-flag</b> <b>no ipv6 nd managed-config-flag</b>
パラメーター	なし
デフォルト	OFF (0)
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	RA メッセージの M フラグを ON(1)にすると、IPv6 アドレスをステートフルな方法で取得するようホストに指示することになります。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 インターフェースで送信する RA メッセージの M フラグを ON(1)に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 nd managed-config-flag
(config-if-vlan)#
```

### 3.6.10 ipv6 nd other-config-flag

ipv6 nd other-config-flag	
目的	RA メッセージの 0 フラグ (Other configuration flag) を ON(1)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	<b>ipv6 nd other-config-flag</b> <b>no ipv6 nd other-config-flag</b>
パラメーター	なし
デフォルト	OFF (0)
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	RA メッセージの 0 フラグを ON(1)にすると、IPv6 アドレス以外の情報をステートフルな方法で取得するようホストに指示することになります。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：VLAN 1 インターフェースで送信する RA メッセージの 0 フラグを ON(1)に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 nd other-config-flag
(config-if-vlan)#
```

### 3.6.11 ipv6 nd prefix

ipv6 nd prefix	
目的	RA メッセージでアドバタイズされる IPv6 プレフィックス情報の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	<b>ipv6 nd prefix</b> <i>IPV6-PREFIX/PREFIX-LENGTH VALID-LIFETIME PREFERRED-LIFETIME</i> [off-link] [no-autoconfig] <b>no ipv6 nd prefix</b> <i>IPV6-PREFIX/PREFIX-LENGTH</i>
パラメーター	<i>IPV6-PREFIX/PREFIX-LENGTH</i> ：アドバタイズされる IPv6 プレフィックスを指定します。 <i>VALID-LIFETIME</i> ：指定した IPv6 プレフィックス情報の有効期間 (Valid Lifetime) を 0~4,294,967,295 秒の範囲で指定します。 <i>PREFERRED-LIFETIME</i> ：指定した IPv6 プレフィックス情報の推奨期間 (Preferred Lifetime) を 0~4,294,967,295 秒の範囲で指定します。 <b>off-link</b> (省略可能)：指定した IPv6 プレフィックス情報の On-link フラグを OFF (0)にする場合に指定します。

ipv6 nd prefix	
	<b>no-autoconfig</b> (省略可能) : 指定した IPv6 プレフィックス情報の Autonomous address-configuration フラグを OFF(0) にする場合に指定します。
デフォルト	IPv6 プレフィックス情報が自動作成される場合のデフォルト値 <ul style="list-style-type: none"> <li>有効期間 (Valid Lifetime) : 2,592,000 秒 (30 日)</li> <li>推奨期間 (Preferred Lifetime) : 604,800 秒 (7 日)</li> <li>On-link フラグ : ON(1)</li> <li>Autonomous address-configuration フラグ : ON(1)</li> </ul>
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	<p><b>ipv6 address</b> コマンドで IPv6 アドレスを設定すると、それに対応した IPv6 プレフィックス情報がデフォルト値で自動的に設定されます。</p> <p>RA メッセージの送信はデフォルトでは抑制されているため、RA メッセージを送信する場合は <b>no ipv6 nd suppress-ra</b> コマンドで送信の抑制を無効にしてください。</p> <p>IPv6 プレフィックス情報の有効期間 (Valid Lifetime) は、推奨期間 (Preferred Lifetime) より長い期間を指定してください。有効期間と推奨期間は、Autonomous address-configuration フラグが ON(1) の IPv6 プレフィックス情報の場合に有効です。</p>
制限事項	-
注意事項	<p><b>ipv6 address</b> コマンドで設定した IPv6 アドレスに対応する IPv6 プレフィックス情報以外は設定できません。</p> <p><b>ipv6 address</b> コマンドで IPv6 アドレスを設定した際に自動的に設定された本設定は、パラメーターがすべてデフォルト値のため <b>show running-config</b> コマンドで表示される構成情報では表示されません。確認する場合は <b>show running-config all</b> コマンドで確認してください。</p> <p><b>ipv6 address PREFIX-NAME SUB-BITS/PREFIX-LENGTH</b> コマンドで設定した IPv6 アドレスに対応する IPv6 プレフィックスに関しては、本コマンドで IPv6 プレフィックス情報のパラメーターを変更できません。</p>
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 プレフィックス情報「3ffe:501:ffff:100::/64」の有効期間 (Valid Lifetime) を 30000 秒に、推奨期間 (Preferred Lifetime) を 20000 秒に変更する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 nd prefix 3ffe:501:ffff:100::/64 30000 20000
(config-if-vlan)#
```

### 3.6.12 ipv6 nd ra interval

ipv6 nd ra interval	
目的	RA メッセージ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	<b>ipv6 nd ra interval MAX-SECS [MIN-SECS]</b> <b>no ipv6 nd ra interval</b>
パラメーター	<b>MAX-SECS</b> : RA メッセージの最大送信間隔を、4~1800 秒の範囲で指定します。

ipv6 nd ra interval	
	<i>MIN-SECS</i> (省略可能) : RA メッセージの最小送信間隔を、3~1350 秒の範囲で指定します。最大送信間隔の 0.75 倍以下の値を指定してください。
デフォルト	最大送信間隔 : 200 秒、最小送信間隔 : 66 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	最小送信間隔を指定しない場合は、以下のルールに基づいて決定されます。 <ul style="list-style-type: none"> <li>最大送信間隔を 4~8 秒で指定した場合は、最小送信間隔は最大送信間隔と同じ値になります。</li> <li>最大送信間隔を 9 秒以上に指定した場合は、最小送信間隔は最大送信間隔のおよそ 3 分の 1 になります。</li> </ul>
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送信する RA メッセージの最大送信間隔を 1500 秒に、最小送信間隔を 1000 秒に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 nd ra interval 1500 1000
(config-if-vlan)#
```

### 3.6.13 ipv6 nd ra lifetime

ipv6 nd ra lifetime	
目的	RA メッセージでアドバタイズする Router Lifetime を設定します。デフ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	<b>ipv6 nd ra lifetime SECONDS</b> <b>no ipv6 nd ra lifetime</b>
パラメーター	<i>SECONDS</i> : Router Lifetime を 0~9000 秒の範囲で指定します。
デフォルト	1800 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	Router Lifetime は、RA メッセージを受信してデフォルトルートを設定したホストがそのデフォルトルートを保持する期間を指示します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例 : VLAN 1 インターフェースで送信する RA メッセージの Router Lifetime を 9000 秒に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 nd ra lifetime 9000
(config-if-vlan)#
```

## 3.6.14 ipv6 nd reachable-time

ipv6 nd reachable-time	
目的	NDP で使用される Reachable 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	<code>ipv6 nd reachable-time <i>MILLI-SECONDS</i></code> <code>no ipv6 nd reachable-time</code>
パラメーター	<i>MILLI-SECONDS</i> : Reachable タイムを 0~3,600,000 ミリ秒 (1000 ミリ秒単位) で指定します。
デフォルト	RA メッセージでアドバタイズされる値 : 1200000 (1200 秒) 自装置の IPv6 インターフェースの設定値 : 1200000 (1200 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	設定した Reachable タイムは自装置の IPv6 インターフェースで使用され、RA メッセージでもアドバタイズされます。0 を指定した場合、自装置の IPv6 インターフェースでは 30 秒で動作し、RA メッセージでは 0 をアドバタイズします。
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 Reachable タイムを 3600 秒に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ipv6 nd reachable-time 3600000
(config-if-vlan)#
```

## 3.6.15 ipv6 nd ns-interval

ipv6 nd ns-interval	
目的	NS メッセージを再送信する間隔 (Retransmit タイマー) 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	<code>ipv6 nd ns-interval <i>MILLI-SECONDS</i></code> <code>no ipv6 nd ns-interval</code>
パラメーター	<i>MILLI-SECONDS</i> : Retransmit タイマーを 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、実動作は以下 <ul style="list-style-type: none"> <li>RA メッセージでアドバタイズされる値 : 0</li> <li>自装置の IPv6 インターフェースの設定値 : 1000 ミリ秒 (1 秒)</li> </ul>
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	設定した Retransmit タイマーは自装置の IPv6 インターフェースで使用され、RA メッセージでもアドバタイズされます。デフォルト設定の 0 の場合は、自装置の IPv6 インターフェースでは 1 秒で動作し、RA メッセージでは 0 をアドバタイズします。
制限事項	-
注意事項	<code>ipv6 address</code> コマンドと <code>ipv6 nd ns-interval</code> 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：VLAN 1 インターフェースの Retransmit タイマーを 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)#
```

### 3.6.16 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	<b>ipv6 neighbor</b> <i>IPV6-ADDRESS INTERFACE-NAME MAC-ADDRESS</i> <b>no ipv6 neighbor</b> <i>IPV6-ADDRESS INTERFACE-NAME</i>
パラメーター	<i>IPV6-ADDRESS</i> ：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。  <i>INTERFACE-NAME</i> ：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 ( <b>vlan</b> と VLAN ID の間を空けない形式) を指定します。  <i>MAC-ADDRESS</i> ：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。 <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul>
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、 <b>show</b> 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、 <b>mac-address-table static</b> 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 256 個まで設定できません。
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)#
```

## 3.6.17 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	<b>show ipv6 interface</b> [ <i>INTERFACE-ID</i> ] [ <b>brief</b> ]
パラメーター	<i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>vlan</b> : VLAN インターフェースを指定します。</li> </ul> <b>brief</b> (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	-
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:feaa:521b
  Global unicast address: ... (5)
    2001:db8:1:1::1001/64 (Manual)
  IPv6 MTU is 1500 bytes ... (6)
  RA messages are sent between 66 to 200 seconds ... (7)
  RA advertised reachable time is 1200000 milliseconds ... (8)
  RA advertised retransmit interval is 0 milliseconds ... (9)
  RA advertised life time is 1800 seconds ... (10)
  RA advertised O flag is OFF, M flag is OFF ... (11)
  RA advertised prefixes ... (12)
    2001:db8:1:1::/64
      valid lifetime is 2592000, preferred lifetime is 604800

vlan20 is up, link status is up
  IPv6 is enabled,
  Link-local address:
    fe80::240:66ff:feaa:521b
  Global unicast address:
    2001:db8:2222:3333:240:66ff:feaa:521b/64 (SLAAC)
  IPv6 MTU is 1500 bytes
  RA messages are sent between 66 to 200 seconds
  RA advertised reachable time is 1200000 milliseconds
  RA advertised retransmit interval is 0 milliseconds
  RA advertised life time is 1800 seconds
  RA advertised O flag is OFF, M flag is OFF

Total Entries: 2
```

項番	説明
(1)	インターフェース ID を表示します。

項番	説明
(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。
(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 (SLAAC) 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 MTU を表示します。
(7)	RA メッセージの最小送信間隔と最大送信間隔を表示します。
(8)	RA メッセージでアドバタイズされる Reachable タイムを表示します。
(9)	RA メッセージでアドバタイズされる Retransmit タイマーを表示します。
(10)	RA メッセージでアドバタイズされる Router Lifetime を表示します。
(11)	RA メッセージでアドバタイズされる 0 フラグ (Other configuration flag) 、M フラグ (Managed address configuration flag) の OFF (0) / ON (1) を表示します。
(12)	RA メッセージでアドバタイズされるプレフィックス情報を表示します。

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:feaa:521b ... (3)
    2001:db8:1:1::1001

vlan20 is up, link status is up
    fe80::240:66ff:feaa:521b
    2001:db8:2222:3333:240:66ff:feaa:521b

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。

### 3.6.18 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	<b>show ipv6 general-prefix</b> [ <i>PREFIX-NAME</i> ]
パラメーター	<i>PREFIX-NAME</i> (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

show ipv6 general-prefix	
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。

### 3.6.19 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	<b>show ipv6 neighbors</b> [ <i>INTERFACE-NAME</i> ] [ <i>IPv6-ADDRESS</i> ]
パラメーター	<i>INTERFACE-NAME</i> (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 ( <b>vlan</b> と VLAN ID の間を空けない形式) を指定します。 <i>IPv6-ADDRESS</i> (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。
(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。 INCOMP (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

### 3.6.20 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	<code>clear ipv6 neighbors {all   interface <i>INTERFACE-ID</i>}</code>
パラメーター	<p><b>all</b> : 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。</p> <p><b>interface <i>INTERFACE-ID</i></b> : 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。</p> <ul style="list-style-type: none"> <li><b>vlan</b> : VLAN インターフェースを指定します。</li> </ul>
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]
tracert	tracert {[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	ping によるアクセスを制限する標準 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。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	<b>ping access-class</b> <i>IP-ACL-NAME</i> <b>no ping access-class</b> <i>IP-ACL-NAME</i>
パラメーター	<i>IP-ACL-NAME</i> : 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。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	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	<p>アクセスリストは2つ設定できます。1つはIPv4用、もう1つはIPv6用です。IPv4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。</p> <p>本機能は、装置宛て ICMP リクエストパケットの送信元 IPv4/IPv6 アドレスのみをチェックします。</p> <p>指定した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。</p> <p>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。</p>
制限事項	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、ping 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 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	<b>ping</b> {[ip] <i>IP-ADDRESS</i>   [ipv6] <i>IPV6-ADDRESS</i> } [count <i>TIMES</i> ] [timeout <i>SECONDS</i> ] [source { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> }] [size <i>LENGTH</i> ] [interval <i>SECONDS</i> ]
パラメーター	<p>[ip] <i>IP-ADDRESS</i> : 宛先 IPv4 アドレスを指定します。</p> <p>[ipv6] <i>IPV6-ADDRESS</i> : 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、「<i>IPV6-ADDRESS%INTERFACE-NAME</i>」のように VLAN インターフェース (<b>vlan</b> と VLAN ID の間を空けない形式) を付加して指定します。</p> <p><b>count</b> <i>TIMES</i> (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。</p> <p><b>timeout</b> <i>SECONDS</i> (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。</p> <p><b>source</b> {<i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i>} (省略可能) : ping パケットに使用される送信元 IPv4 アドレス、または送信元 IPv6 アドレスを指定します。装置に設定している IP アドレスの中から指定してください。また、宛先 IP アドレスと送信元 IP アドレスは、同じ種類の IP アドレス (IPv4 または IPv6) を指定してください。</p> <p><b>size</b> <i>LENGTH</i> (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。</p> <p><b>interval</b> <i>SECONDS</i> (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。</p>
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ことは、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

### 3 基礎知識 | 3.7 IP ユーティリティーコマンド

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	装置から IP ネットワークを経由して、特定の宛先ホストに到達するホップごとのパスを表示します。
シンタックス	<code>traceroute</code> <b>{</b> [ip] <i>IP-ADDRESS</i>   [ipv6] <i>IPV6-ADDRESS</i> <b>}</b> [ <b>probe</b> <i>NUMBER</i> ] [ <b>timeout</b> <i>SECONDS</i> ] [ <b>max-ttl</b> <i>TTL</i> ] [ <b>port</b> <i>DEST-PORT</i> ]
パラメーター	<b>[ip]</b> <i>IP-ADDRESS</i> : 対象ホストの IPv4 アドレスを指定します。 <b>[ipv6]</b> <i>IPV6-ADDRESS</i> : 対象ホストの IPv6 アドレスを指定します。 <b>probe</b> <i>NUMBER</i> (省略可能) : ホップごとの送信プローブ数を 1~1000 の範囲で指定します。 <b>timeout</b> <i>SECONDS</i> (省略可能) : 応答タイムアウト時間を 1~65535 秒の範囲で指定します。 <b>max-ttl</b> <i>TTL</i> (省略可能) : 送信 UDP データグラムの最大 TTL (Time To Live) 値を、1~255 の範囲で指定します。 <b>port</b> <i>DEST-PORT</i> (省略可能) : 送信データグラムで使用される UDP 宛先ベースポート番号を、1~65535 の範囲で指定します。UDP 宛先ベースポート番号は、データグラムが送信されるたびに加算されます。デフォルトの traceroute ポート範囲にあるポートを、宛先ホストがリスニングしている場合に指定してください。
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 宛先の UDP ベースポート番号 : 33434 各 TTL のクエリー数 : 3



traceroute	
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	<b>traceroute</b> の実行後に、コマンドの実行を中断する場合は、Ctrl+C キーを押します。 別のサービスによってルート変更が発生したかどうかを確認する場合は、TOS オプションを使用します。
制限事項	<b>traceroute</b> 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：ホスト 172.50.71.123 に traceroute を実行する方法を示します。

```
# traceroute 172.50.71.123

<10 ms 172.50.71.123

Trace complete.
```

使用例：ホスト 172.50.71.123 に traceroute を実行する方法を示します。以下の例は、ルーターが応答していないことを示しています。

```
# traceroute 172.50.71.123

*      Request timed out.
*      Request timed out.
*      Request timed out.
```

使用例：ホスト 172.50.71.123 に traceroute を実行する方法を示します。以下の例は、宛先に到達不能であるとルーターが応答していることを示しています。

```
# traceroute 172.50.71.123

<10 ms Network Unreachable
<10 ms Network Unreachable
<10 ms Network Unreachable
```

使用例：IPv6 アドレスが 2001:238:f8a:77:7c10:41c0:6ddd:ecab のホストに、traceroute を実行する方法を示します。

```
# traceroute 2001:238:f8a:77:7c10:41c0:6ddd:ecab

<10 ms 2001:238:f8a:77:7c10:41c0:6ddd:ecab

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-arp	ip gratuitous-arp [dad-reply] no ip gratuitous-arp [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	<b>ip arp gratuitous</b> <b>no ip arp gratuitous</b>
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-arp

ip gratuitous-arp	
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	<b>ip gratuitous-arp [dad-reply]</b> <b>no ip gratuitous-arp [dad-reply]</b>
パラメーター	<b>dad-reply</b> (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、 <b>ip gratuitous-arps</b> 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、 <b>ip gratuitous-arps dad-reply</b> コマンドを設定します。
制限事項	構成情報では、 <b>ip gratuitous-arps</b> と <b>ip gratuitous-arps dad-reply</b> は別に表示されます。設定を削除する場合は、それぞれの <b>no</b> 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、 <b>no</b> 形式のコマンドを使用します。
シンタックス	<b>arp gratuitous-send interval SECONDS</b> <b>no arp gratuitous-send</b>
パラメーター	<b>SECONDS</b> ：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 1.02.01：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 1
(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]
reboot	reboot [unit UNIT-ID] [force_agree]
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
restore	restore {tftp: [//LOCATION[/PATH]]   ftp: [//USER-NAME:PASSWORD@LOCATION:TCP-PORT[/PATH]]   memory-card: [/PATH]} prefix BASENAME
clear running-config	clear running-config
reset system	reset system [factory-default]

## 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	<code>boot image [check] URL [primary   secondary]</code>
パラメーター	<p><b>check</b> (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。</p> <p><b>URL</b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>c:/URL</b> : 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、<code>c:/switch-image.had</code> と入力します。</li> <li>• <b>d:/URL</b> : 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、<code>d:/switch-image.had</code> と入力します。</li> <li>• <b>UNIT-ID:/c:/URL</b> : 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、<code>unit2:/c:/switch-image.had</code> と入力します。</li> </ul> <p><b>primary</b> (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。</p> <p><b>secondary</b> (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。</p>
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	<p><b>primary</b> および <b>secondary</b> 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。</p> <p>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、ファイルが有効なブートイメージファイルであることが確認されます。</p> <p><b>check</b> 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。</p> <p><b>boot image</b> 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 <code>startup-config</code> とは別の領域です。</p> <p>装置が起動すると、最初にプライマリーブートイメージファイルが読み込まれます。プライマリーブートイメージファイルが読み込めない場合は、セカンダリーブートイメージファイルが読み込まれます。セカンダリーブートイメージファイルも読み込めない場合、ローカルフラッシュ内で有効なブートイメージファイルと判定されており、かつ最新の日時であるファイルが使用されます。</p>
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：スタック構成の装置において、ボックス ID 2 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: 1.02.02
Description: APRESIA Systems, Ltd TenGigabit 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	<b>boot config</b> <i>URL</i> [ <b>primary</b>   <b>secondary</b> ]
パラメーター	<p><i>URL</i> : 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。</p> <ul style="list-style-type: none"> <li>• <b>c:/URL</b> : 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。</li> <li>• <b>d:/URL</b> : 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。</li> <li>• <b>UNIT-ID:/c:/URL</b> : スタックメンバーのローカルフラッシュ上のファイル</li> </ul>

boot config	
	<p>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。</p> <p><b>primary</b> (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。</p> <p><b>secondary</b> (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。</p>
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	<p><b>primary</b> および <b>secondary</b> 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。</p> <p><b>boot config</b> 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。</p> <p>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。</p> <p>工場出荷状態では「primary.cfg」が設定されています。</p>
制限事項	-
注意事項	<p>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。</p> <p>ローカルフラッシュのブートスクリプトで、SD カード上の構成情報ファイルを指定する場合は、SD カードを取り外さないでください。この状態で SD カードを取り外すと、startup-config にはローカルフラッシュ内で有効な構成情報と判定されたファイルのうち、最新日時のファイルが適用されます。</p>
対象バージョン	1.01.01

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：スタック構成の装置において、ボックス ID 2 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	<b>ip tftp source-interface</b> <i>INTERFACE-ID</i> <b>no ip tftp source-interface</b>
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>vlan</b>: VLAN インターフェースを指定します。</li> <li>• <b>mgmt</b>: マネージメントポートを指定します。</li> </ul>
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、 <b>vlan</b> 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、 <b>mgmt</b> 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	<b>ip ftp source-interface</b> <i>INTERFACE-ID</i> <b>no ip ftp source-interface</b>
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>vlan</b>: VLAN インターフェースを指定します。</li> <li>• <b>mgmt</b>: マネージメントポートを指定します。</li> </ul>
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



ip ftp source-interface	
特権レベル	レベル : 12
ガイドライン	-
制限事項	-
注意事項	<p>マネージメントポート経由で管理する場合は、<b>vlan</b> 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。</p> <p>VLAN インターフェース経由で管理する場合は、<b>mgmt</b> 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。</p>
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	<b>show boot</b> [ <b>unit</b> <i>UNIT-ID</i> ]
パラメーター	<b>unit</b> <i>UNIT-ID</i> (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	<p>「apresia-loader.conf」が保存されている SD カードを挿入した場合は、SD カード内のファイルの情報も表示されます。</p> <p>スタック構成で特定の装置のボックス ID を指定しない場合、すべてのスタックメンバー装置の情報が表示されます。</p>
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 カード上の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、そのファイルのパスを表示します。
(7)	SD カード上のファイルをプライマリー構成情報として使用する場合、その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 ファイル内のコマンドを表示します。
シンタックス	<b>show running-config</b> [ <b>effective</b>   <b>all</b> ] [ <b>interface</b> <i>INTERFACE-ID</i>   <b>function</b> [ <i>MODULE-TITLE</i> ]]
パラメーター	<p><b>effective</b> (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。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設定については <code>disable stp</code> コマンドだけが表示されます。より下位のレイヤーの、スパニングツリープロトコルのその他の設定は、すべて表示されません。下位レイヤーの設定は、上位レイヤーの設定が有効な場合だけ表示されます。<b>effective</b> を指定しない場合、デフォルト設定から変更された設定だけが表示されます。</p> <p><b>all</b> (省略可能) : デフォルト設定から変更されていないコマンドを含め、すべてのコマンド設定を表示する場合に指定します。<b>all</b> を指定しない場合、デフォルト設定から変更された設定だけが表示されます。</p> <p><b>interface</b> <i>INTERFACE-ID</i> (省略可能) : コマンド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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> <li>• <b>vlan</b> : VLAN インターフェースを指定します。</li> <li>• <b>mgmt</b> : マネージメントポートを指定します。</li> </ul> <p><b>function</b> (省略可能) : すべての機能に関連する情報を表示します。</p> <p><i>MODULE-TITLE</i> (省略可能) : 機能に関連する情報を表示する場合に、完全な機能名を大文字で入力します。例えば、スタックの場合は <code>STACK</code> と入力します。</p>
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	インターフェースを指定しない場合、すべてのインターフェースのコマンド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：running-config ファイルの内容を表示する方法を示します。

```
# show running-config
Building configuration...

Current configuration : 1570 bytes ... (1)
(2)
#-----
#                               ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch
#                               Configuration
#
#                               Firmware: Build 1.01.01
#                               Copyright (C) 2017 APRESIA Systems, Ltd. All rights reserved.
#-----

# Date: Tue Oct 03 10:37:38 2017

# STACK

## stacking config information
## #Box          Prio-
## #ID   Type      Exist rity
## #---  -----  -----
## #  1 ApresiaNP4000-20Xt4X exist 32
## #  2 NOT_EXIST 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。
(2)	running-config の内容（コマンド設定）を表示します。

### 3.9.7 show startup-config

show startup-config	
目的	startup-config ファイルの内容を表示します。
シンタックス	<b>show startup-config</b>
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 ファイルの内容を表示する方法を示します。

```
# show startup-config
(1)
#-----
#                               ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch
#                               Configuration
#
#                               Firmware: Build 1.01.01
#                               Copyright (C) 2017 APRESIA Systems, Ltd. All rights reserved.
```

```
#-----
# Date: Tue Oct 03 10:28:44 2017

# STACK

stack bandwidth 10G 2-port
no stack my_box_id
stack my_box_priority 32
no stack preempt

# BASIC

terminal speed 115200

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

項番	説明
(1)	startup-config の内容 (コマンド設定) を表示します。

### 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	<code>show config differences {flash: URL1   running-config   startup-config} {flash: URL2   running-config   startup-config}</code>
パラメーター	<p><b>flash: URL1</b>: 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。</p> <ul style="list-style-type: none"> <li>• <b>c:/URL1</b>: 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。</li> <li>• <b>d:/URL1</b>: 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。</li> <li>• <b>UNIT-ID:/c:/URL1</b>: 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。</li> </ul> <p><b>running-config</b>: 比較対象として、本装置の running-config を指定します。</p> <p><b>startup-config</b>: 比較対象として、本装置の startup-config を指定します。</p> <p><b>flash: URL2</b>: 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。</p> <ul style="list-style-type: none"> <li>• <b>c:/URL2</b>: 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。</li> <li>• <b>d:/URL2</b>: 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。</li> <li>• <b>UNIT-ID:/c:/URL2</b>: 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。</li> </ul>
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

show config differences	
ガイドライン	-
制限事項	-
注意事項	-
対象バージョン	1.02.01

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。

<pre># show config differences flash: d:/config.cfg running-config  Config differences: (1) +vlan 10,20,500 +interface port 1/0/24 + switchport access vlan 500 -vlan 10,20 -logging server 10.249.234.112 severity debugging facility 23 port 514</pre>
--

項番	説明
(1)	<p>2つの構成情報の差分を表示します。</p> <p>show config differences A B と実行した場合に以下のように表示されます。</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• Aに含まれていなくて、Bに含まれている設定：先頭に“-”が付与されて表示</li> </ul>

### 3.9.9 backup clone

backup clone	
目的	装置が動作するため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	<b>backup clone</b>
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	<p>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。</p> <p>以下のファイルがバックアップされます。</p> <ul style="list-style-type: none"> <li>• ブートスクリプト：apresia-loader.conf <ul style="list-style-type: none"> <li>• ブートスクリプトは以下の内容で設定されています。</li> </ul> </li> <li>• プライマリーブートイメージファイル：/d:/apresia-software.had</li> <li>• プライマリー構成情報：/d:/apresia-startup-config.txt</li> <li>• ブートイメージファイル：apresia-software.had</li> <li>• startup-config：apresia-startup-config.txt</li> <li>• ランタイムバージョンテキストファイル：apresia-system-name.txt</li> <li>• SSHv2 RSA 鍵対ファイル：apresia-rsa-key</li> <li>• SSHv2 DSA 鍵対ファイル：apresia-dsa-key</li> <li>• 以下の Web 認証ページ <ul style="list-style-type: none"> <li>• ログイン認証ページ：apresia-login-page</li> <li>• 認証成功ページ：apresia-login-success-page</li> </ul> </li> </ul>

## backup clone

- 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
- 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
- 以下の Web ページ画像
  - Web ページ画像 01：apresia-webpage-image01
  - Web ページ画像 02：apresia-webpage-image02
  - Web ページ画像 03：apresia-webpage-image03
  - Web ページ画像 04：apresia-webpage-image04
  - Web ページ画像 05：apresia-webpage-image05
  - Web ページ画像 06：apresia-webpage-image06
  - Web ページ画像 07：apresia-webpage-image07
  - Web ページ画像 08：apresia-webpage-image08
  - Web ページ画像 09：apresia-webpage-image09
  - Web ページ画像 10：apresia-webpage-image10

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

backup clone	
制限事項	す。複製した「apresia-aaa-local-db」を直接参照することはありません。
注意事項	<p>-</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>write memory</b> 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。</li> <li>• <b>copy</b> コマンドでブートイメージファイルをコピーし、<b>boot image</b> コマンドでブートイメージファイルを指定できます。</li> </ul> <p>スタック構成の装置で <b>backup clone</b> を実施した場合、実行中に“DEBG(7) Unit &lt;unit-id&gt; fails to send a stacking message. (Type: &lt;msg-type&gt;[, Sub type: &lt;sub-type&gt;])”ログが出力されますが、<b>backup clone</b> 実行中の一時的なものであり動作に問題はありません。<b>backup clone</b> 終了後には出力されなくなります。</p>
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、動作に必要なファイルをバックアップする方法を示します。

```
# backup clone

Uploading boot information (apresia-loader.conf)..... Done.
Uploading firmware image file (apresia-software.had)..... Done.
Uploading start-up configuration file (apresia-startup-config.txt)..... Done.
Uploading system name file (apresia-system-name.txt)..... Done.
Uploading SSH RSA key file (apresia-rsa-key)..... Fail.
Uploading SSH DSA key file (apresia-dsa-key)..... Done.
Uploading web authentication login-page file (apresia-login-page)..... Done.
Uploading web authentication login-success-page file (apresia-login-success-page)..... Done.
Uploading web authentication login-failure-page file (apresia-login-failure-page)..... Done.
Uploading web authentication logout-success-page file (apresia-logout-success-page)..... Done.
Uploading web authentication logout-failure-page file (apresia-logout-failure-page)..... Done.
Uploading web authentication redirect-error-page file (apresia-redirect-error-page)..... Done.
Uploading access defender local database settings file (apresia-aaa-local-db)..... Done.
Uploading SSL server certificate file (apresia-https-certificate)..... Done.
Uploading SSL server private key file (apresia-https-private-key)..... Done.
Uploading web authentication webpage-image01 file (apresia-webpage-image01)..... Done.
Uploading web authentication webpage-image02 file (apresia-webpage-image02)..... Done.
Uploading web authentication webpage-image03 file (apresia-webpage-image03)..... Done.
Uploading web authentication webpage-image04 file (apresia-webpage-image04)..... Done.
Uploading web authentication webpage-image05 file (apresia-webpage-image05)..... Done.
Uploading web authentication webpage-image06 file (apresia-webpage-image06)..... Done.
Uploading web authentication webpage-image07 file (apresia-webpage-image07)..... Done.
Uploading web authentication webpage-image08 file (apresia-webpage-image08)..... Done.
```

```
Uploading web authentication webpage-image09 file (apresia-webpage-image09)..... Done.
Uploading web authentication webpage-image10 file (apresia-webpage-image10)..... Done.
```

### 3.9.10 write

write	
目的	現在の構成情報を startup-config ファイルに書き込みます。
シンタックス	<b>write [memory]</b>
パラメーター	<b>memory</b> (省略可能) : 現在の構成情報をフラッシュメモリー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、現在の構成情報を SD カードにも保存します。
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	<p><b>write [memory]</b> コマンドは、現在動作中の構成情報をプライマリーで指定した構成情報ファイルにのみ上書き保存します。</p> <p>セカンダリーで指定した構成情報ファイルに上書き保存する場合は、<b>copy running-config</b> コマンドを使用してください。ただし、スタック構成の場合に、スタックマスター以外のメンバー装置のセカンダリー構成情報ファイルをコピー先として指定して実施することはサポートしていません。</p> <p>一部のスタックメンバーに SD カードが未挿入の状態では <b>write memory</b> 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。</p> <ul style="list-style-type: none"> <li>“Saving all configurations to SD-Card”</li> </ul> <p>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。</p>
対象バージョン	1.01.01

使用例 : running-config をフラッシュメモリーに書き込み、フラッシュメモリーに書き込んだ設定を、次回起動時の構成情報として使用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 reboot

reboot	
目的	装置を再起動します。
シンタックス	<b>reboot [unit UNIT-ID] [force_agree]</b>
パラメーター	<p><b>unit UNIT-ID</b> (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。</p> <p><b>force_agree</b> (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。</p>
デフォルト	なし
コマンドモード	特権実行モード



reboot	
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装置のボックス ID を指定しない場合、スタック構成全体が再起動されます。
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

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：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...
```

### 3.9.12 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	<b>copy boot</b>
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。
制限事項	-
注意事項	-
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 カードにブート情報を保存する方法を示します。

```
# copy boot

Writing the boot information to SD card..... Done.
```

### 3.9.13 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	<b>erase boot</b>
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

erase boot	
特権レベル	レベル : 15
ガイドライン	装置のローカルフラッシュから構成情報とブートイメージファイルを消去します。
制限事項	-
注意事項	正しく使用できるブート情報ファイルが保存されている SD カードを挿入しない限り、 <b>erase boot</b> コマンドを実行した後に装置を起動すると、ブート情報ファイル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.

### 3.9.14 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	<b>configure replace</b> { <b>tftp:</b> //location/filename   <b>ftp:</b> //username:password@location:tcpport/filename   <b>flash:</b> FILENAME} [ <b>force</b> ]
パラメーター	<p><b>tftp:</b> : 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。 //location/filename : TFTP サーバー上の構成情報の URL を指定します。</p> <p><b>ftp:</b> : 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。</p> <p><b>flash:</b> : 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。</p> <p><b>force</b> (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。</p>
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	装置がネットワークに接続されていない場合は、ネットワークのループを避けるために、本コマンドを実行します。
制限事項	-
注意事項	<p>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。</p> <p>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。</p> <p>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。</p>
対象バージョン	1.01.01

### 3 基礎知識 | 3.9 システムファイル管理コマンド

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
```

#### 3.9.15 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	<pre>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</pre>
パラメーター	<p><i>SOURCE-URL</i> : 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。</p> <ul style="list-style-type: none"><li>• <b>startup-config</b> : startup-config をコピー（アップロード）する場合に指定します。</li><li>• <b>running-config</b> : running-config をコピー（アップロード）する場合に指定します。</li><li>• <b>flash</b> : [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。</li><li>• <b>log</b> : システムログをコピーする場合に指定します。</li></ul> <p><i>DESTINATION-URL</i> : 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</p>

copy	
	<p>メーターが使用できます。</p> <ul style="list-style-type: none"> <li>• <b>running-config</b> : running-config へ適用する場合に指定します。</li> <li>• <b>startup-config</b> : 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、<b>boot config</b> コマンドで指定されるファイル名と同じになります。</li> <li>• <b>flash</b>: [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。</li> </ul> <p><i>LOCATION</i>: 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。</p> <p><i>USER-NAME</i>: FTP サーバーのユーザー名を指定します。</p> <p><i>PASSWORD</i>: 上記ユーザーのパスワードを指定します。</p>
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	<p>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、<b>boot config</b> 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、<b>boot config</b> コマンドで設定したファイルの内容が上書きされます。</p> <p>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。</p> <p>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。</p> <p>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、<b>boot image</b> コマンドで指定します。</p>
制限事項	<b>copy tftp: startup-config</b> コマンドと <b>copy ftp: startup-config</b> 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	<p>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。</p> <p>コピー先として flash を指定して SD カードに構成情報をアップロードした場合は、先頭にバイナリの制御データが付与された形式の構成情報ファイルになります。</p> <p>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。</p>

copy	
	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。
<b>対象バージョン</b>	1.01.01

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.

```

### 3.9.16 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	<b>backup</b> { <b>tftp</b> : [// <i>LOCATION</i> [/ <i>PATH</i> ]]   <b>ftp</b> : [// <i>USER-NAME</i> : <i>PASSWORD</i> @ <i>LOCATION</i> : <i>TCP-PORT</i> [/ <i>PATH</i> ]]   <b>memory-card</b> : [/ <i>PATH</i> ]} <b>prefix</b> <i>BASENAME</i>
パラメーター	<p><b>tftp</b>: : 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。</p> <ul style="list-style-type: none"> <li>• <i>LOCATION</i> (省略可能) : TFTP サーバーの IPv4/IPv6 アドレスを指定します。</li> <li>• <i>PATH</i> (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。</li> </ul> <p><b>ftp</b>: : 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。</p> <ul style="list-style-type: none"> <li>• <i>USER-NAME</i> (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。</li> <li>• <i>PASSWORD</i> (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。</li> <li>• <i>LOCATION</i> (省略可能) : FTP サーバーの IPv4/IPv6 アドレスを指定します。</li> <li>• <i>TCP-PORT</i> (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。</li> <li>• <i>PATH</i> (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。</li> </ul> <p><b>memory-card</b>: : 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。</p> <ul style="list-style-type: none"> <li>• <i>PATH</i> (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。</li> </ul> <p><b>prefix</b> <i>BASENAME</i>: 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。¥ / : * ? " &lt; &gt;   およびスペースは使用できません。</p>
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	<p><b>backup</b> コマンドで動作に必要なファイルをバックアップし、<b>restore</b> 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。</p> <p>以下のファイルがバックアップされます。</p> <ul style="list-style-type: none"> <li>• ブートイメージファイル : <i>BASENAME</i>-software.had</li> <li>• startup-config : <i>BASENAME</i>-startup-config.txt</li> </ul>

backup	
	<ul style="list-style-type: none"> <li>• running-config : <i>BASENAME</i>-running-config.txt</li> <li>• ランタイムバージョンテキストファイル : <i>BASENAME</i>-system-name.txt</li> <li>• SSHv2 RSA 鍵対ファイル : <i>BASENAME</i>-rsa-key</li> <li>• SSHv2 DSA 鍵対ファイル : <i>BASENAME</i>-dsa-key</li> <li>• 以下の Web 認証ページ <ul style="list-style-type: none"> <li>• ログイン認証ページ : <i>BASENAME</i>-login-page</li> <li>• 認証成功ページ : <i>BASENAME</i>-login-success-page</li> <li>• 認証失敗ページ : <i>BASENAME</i>-login-failure-page</li> <li>• ログアウト成功ページ : <i>BASENAME</i>-logout-success-page</li> <li>• ログアウト失敗ページ : <i>BASENAME</i>-logout-failure-page</li> <li>• リダイレクト失敗ページ : <i>BASENAME</i>-redirect-error-page</li> </ul> </li> <li>• AccessDefender のローカルデータベース : <i>BASENAME</i>-aaa-local-db</li> <li>• SSL サーバー証明書 : <i>BASENAME</i>-https-certificate</li> <li>• SSL サーバーの秘密鍵 : <i>BASENAME</i>-https-private-key</li> <li>• 以下の Web ページ画像 <ul style="list-style-type: none"> <li>• Web ページ画像 01 : <i>BASENAME</i>-webpage-image01</li> <li>• Web ページ画像 02 : <i>BASENAME</i>-webpage-image02</li> <li>• Web ページ画像 03 : <i>BASENAME</i>-webpage-image03</li> <li>• Web ページ画像 04 : <i>BASENAME</i>-webpage-image04</li> <li>• Web ページ画像 05 : <i>BASENAME</i>-webpage-image05</li> <li>• Web ページ画像 06 : <i>BASENAME</i>-webpage-image06</li> <li>• Web ページ画像 07 : <i>BASENAME</i>-webpage-image07</li> <li>• Web ページ画像 08 : <i>BASENAME</i>-webpage-image08</li> <li>• Web ページ画像 09 : <i>BASENAME</i>-webpage-image09</li> <li>• Web ページ画像 10 : <i>BASENAME</i>-webpage-image10</li> </ul> </li> </ul> <p>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。</p>
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	<p>本コマンドでバックアップした構成情報ファイル「<i>BASENAME</i>-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。</p> <p>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。</p> <p>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。</p>
対象バージョン	1.01.01

使用例：プレフィックス文字列を「backup1」として、動作に必要なファイルを装置のローカルフラッシュから SD カードにバックアップする方法を示します。

```
# backup memory-card: prefix backup1
```

```

Uploading firmware image file (backup1-software.had)..... Done.
Uploading start-up configuration file (backup1-startup-config.txt)..... Done.
Uploading running configuration file (backup1-running-config.txt)..... Done.
Uploading system name file (backup1-system-name.txt)..... Done.
Uploading SSH RSA key file (backup1-rsa-key)..... Done.
Uploading SSH DSA key file (backup1-dsa-key)..... Done.
Uploading web authentication login-page file (backup1-login-page)..... Done.
Uploading web authentication login-success-page file (backup1-login-success-page)..... Done.
Uploading web authentication login-failure-page file (backup1-login-failure-page)..... Done.
Uploading web authentication logout-success-page file (backup1-logout-success-page)..... Done.
Uploading web authentication logout-failure-page file (backup1-logout-failure-page)..... Done.
Uploading web authentication redirect-error-page file (backup1-redirect-error-page)..... Done.
Uploading access defender local database settings file (backup1-aaa-local-db)..... Done.
Uploading SSL server certificate file (backup1-https-certificate)..... Done.
Uploading SSL server private key file (backup1-https-private-key)..... Done.
Uploading web authentication webpage-image01 file (backup1-webpage-image01)..... Done.
Uploading web authentication webpage-image02 file (backup1-webpage-image02)..... Done.
Uploading web authentication webpage-image03 file (backup1-webpage-image03)..... Done.
Uploading web authentication webpage-image04 file (backup1-webpage-image04)..... Done.
Uploading web authentication webpage-image05 file (backup1-webpage-image05)..... Done.
Uploading web authentication webpage-image06 file (backup1-webpage-image06)..... Done.
Uploading web authentication webpage-image07 file (backup1-webpage-image07)..... Done.
Uploading web authentication webpage-image08 file (backup1-webpage-image08)..... Done.
Uploading web authentication webpage-image09 file (backup1-webpage-image09)..... Done.
Uploading web authentication webpage-image10 file (backup1-webpage-image10)..... Done.

```

### 3.9.17 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	<b>restore</b> { <b>tftp</b> : [// <i>LOCATION</i> [/ <i>PATH</i> ]]   <b>ftp</b> : [// <i>USER-NAME</i> : <i>PASSWORD</i> @ <i>LOCATION</i> : <i>TCP-PORT</i> [/ <i>PATH</i> ]]   <b>memory-card</b> : [/ <i>PATH</i> ]} <b>prefix</b> <i>BASENAME</i>
パラメーター	<p><b>tftp</b>: : 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。</p> <ul style="list-style-type: none"> <li><i>LOCATION</i> (省略可能) : TFTP サーバーの IPv4/IPv6 アドレスを指定します。</li> <li><i>PATH</i> (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。</li> </ul> <p><b>ftp</b>: : 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。</p> <ul style="list-style-type: none"> <li><i>USER-NAME</i> (省略可能) : FTP サーバーの FTP アカунトのユーザー名を指定します。</li> <li><i>PASSWORD</i> (省略可能) : FTP サーバーの FTP アカунトのパスワードを指定します。</li> <li><i>LOCATION</i> (省略可能) : FTP サーバーの IPv4/IPv6 アドレスを指定します。</li> <li><i>TCP-PORT</i> (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。</li> <li><i>PATH</i> (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。</li> </ul> <p><b>memory-card</b>: : 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。</p> <ul style="list-style-type: none"> <li><i>PATH</i> (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。</li> </ul> <p><b>prefix</b> <i>BASENAME</i>: 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。¥ / : * ? " &lt; &gt;   およびスペースは使用できません。</p>



restore	
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	<p><b>backup</b> コマンドで動作に必要なファイルをバックアップし、<b>restore</b> 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。</p> <p><b>restore</b> コマンドを実施した後は、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。</p> <p>以下のファイルがリストアされます。</p> <ul style="list-style-type: none"> <li>• ブートイメージファイル : <i>BASENAME</i>-software.had</li> <li>• startup-config : <i>BASENAME</i>-startup-config.txt</li> <li>• ランタイムバージョンテキストファイル : <i>BASENAME</i>-system-name.txt</li> <li>• SSHv2 RSA 鍵対ファイル : <i>BASENAME</i>-rsa-key</li> <li>• SSHv2 DSA 鍵対ファイル : <i>BASENAME</i>-dsa-key</li> <li>• 以下の Web 認証ページ <ul style="list-style-type: none"> <li>• ログイン認証ページ : <i>BASENAME</i>-login-page</li> <li>• 認証成功ページ : <i>BASENAME</i>-login-success-page</li> <li>• 認証失敗ページ : <i>BASENAME</i>-login-failure-page</li> <li>• ログアウト成功ページ : <i>BASENAME</i>-logout-success-page</li> <li>• ログアウト失敗ページ : <i>BASENAME</i>-logout-failure-page</li> <li>• リダイレクト失敗ページ : <i>BASENAME</i>-redirect-error-page</li> </ul> </li> <li>• AccessDefender のローカルデータベース : <i>BASENAME</i>-aaa-local-db</li> <li>• SSL サーバー証明書 : <i>BASENAME</i>-https-certificate</li> <li>• SSL サーバーの秘密鍵 : <i>BASENAME</i>-https-private-key</li> <li>• 以下の Web ページ画像 <ul style="list-style-type: none"> <li>• Web ページ画像 01 : <i>BASENAME</i>-webpage-image01</li> <li>• Web ページ画像 02 : <i>BASENAME</i>-webpage-image02</li> <li>• Web ページ画像 03 : <i>BASENAME</i>-webpage-image03</li> <li>• Web ページ画像 04 : <i>BASENAME</i>-webpage-image04</li> <li>• Web ページ画像 05 : <i>BASENAME</i>-webpage-image05</li> <li>• Web ページ画像 06 : <i>BASENAME</i>-webpage-image06</li> <li>• Web ページ画像 07 : <i>BASENAME</i>-webpage-image07</li> <li>• Web ページ画像 08 : <i>BASENAME</i>-webpage-image08</li> <li>• Web ページ画像 09 : <i>BASENAME</i>-webpage-image09</li> <li>• Web ページ画像 10 : <i>BASENAME</i>-webpage-image10</li> </ul> </li> </ul> <p>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。</p> <p>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、<b>show crypto key mypubkey</b> コマンドで表示できます。</p> <p>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、<b>show ssl https-certificate</b> コマンド、<b>show ssl https-private-key</b> コマンド、および <b>show access-defender aaa-local-db</b> コマンドを使用します。</p>

restore	
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	-
対象バージョン	1.01.01

使用例：プレフィックス文字列を「backup1」としてバックアップした動作に必要なファイルを、SDカードから装置のローカルフラッシュにリストアする方法を示します。

```
# restore memory-card: prefix backup1

Downloading firmware image file (backup1-software.had)..... Done.
Downloading start-up configuration file (backup1-startup-config.txt)..... Done.
Downloading system name file (backup1-system-name.txt)..... Done.
Downloading SSH RSA key file (backup1-rsa-key)..... Done.
Downloading SSH DSA key file (backup1-dsa-key)..... Done.
Downloading web authentication login-page file (backup1-login-page)..... Done.
Downloading web authentication login-success-page file (backup1-login-success-page)..... Done.
Downloading web authentication login-failure-page file (backup1-login-failure-page)..... Done.
Downloading web authentication logout-success-page file (backup1-logout-success-page)..... Done.
Downloading web authentication logout-failure-page file (backup1-logout-failure-page)..... Done.
Downloading web authentication redirect-error-page file (backup1-redirect-error-page)..... Done.
Downloading access defender local database settings file (backup1-aaa-local-db)..... Done.
Downloading SSL server certificate file (backup1-https-certificate)..... Done.
Downloading SSL server private key file (backup1-https-private-key)..... Done.
Downloading web authentication webpage-image01 file (backup1-webpage-image01)..... Done.
Downloading web authentication webpage-image02 file (backup1-webpage-image02)..... Done.
Downloading web authentication webpage-image03 file (backup1-webpage-image03)..... Done.
Downloading web authentication webpage-image04 file (backup1-webpage-image04)..... Done.
Downloading web authentication webpage-image05 file (backup1-webpage-image05)..... Done.
Downloading web authentication webpage-image06 file (backup1-webpage-image06)..... Done.
Downloading web authentication webpage-image07 file (backup1-webpage-image07)..... Done.
Downloading web authentication webpage-image08 file (backup1-webpage-image08)..... Done.
Downloading web authentication webpage-image09 file (backup1-webpage-image09)..... Done.
Downloading web authentication webpage-image10 file (backup1-webpage-image10)..... Done.
```

### 3.9.18 clear running-config

clear running-config	
目的	running-config を消去します。
シンタックス	<b>clear running-config</b>
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構成情報が消去されます。また、接続済みのリモート接続は、すべて切断されます。
制限事項	-
注意事項	本コマンドを実行すると、装置に保存されているログメッセージも削除されます。
対象バージョン	1.01.01

使用例：running-config 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
```

## 3.9.19 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	<code>reset system [factory-default]</code>
パラメーター	<code>factory-default</code> (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。
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	<p>スタックに関する設定を含む構成情報を初期化します。</p> <p><code>factory-default</code> 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。</p> <ul style="list-style-type: none"> <li>• すべてのローカルフラッシュに保存されたファイル (セキュリティー認証ファイルを含む。) (ただし、<code>boot image</code> 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。)</li> <li>• すべてのログおよびエラーログエントリー</li> </ul>
制限事項	-
注意事項	-
対象バージョン	1.01.01

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 DISCOVER メッセージのオプション 60 の値として使用するベンダークラス識別子を指定します。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	<b>ip dhcp client class-id</b> { <i>STRING</i>   <b>hex</b> <i>HEX-STRING</i> } <b>no ip dhcp client class-id</b>
パラメーター	<i>STRING</i> : ベンダークラス識別子を最大 32 文字で指定します。 <i>HEX-STRING</i> : ベンダークラス識別子を最大 64 文字（16 進表記）で指定します。
デフォルト	装置タイプをクラス ID として使用
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	指定できるのは、DHCP DISCOVER メッセージの後の送信だけです。設定が有効になるのは、DHCP クライアントがインターフェース上で、DHCP サーバーからの IP アドレス取得が可能な場合だけです。ベンダークラス識別子には、IP アドレスを要求している装置のタイプを指定します。クラス識別子がインターフェースに対して設定されている場合だけ、オプション 60 は DISCOVER メッセージと共に送信されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例: VLAN 100 インターフェースで、DHCP クライアントを有効にして、ベンダークラス識別子の送信を有効にする方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# ip address dhcp
(config-if-vlan)# ip dhcp client class-id VOIP-Device
(config-if-vlan)#
```

## 4.1.2 ip dhcp client client-id

ip dhcp client client-id	
目的	DISCOVER メッセージのクライアント ID として使用する MAC アドレスを、VLAN インターフェースで指定します。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	<b>ip dhcp client client-id</b> <i>INTERFACE-ID</i> <b>no ip dhcp client client-id</b>
パラメーター	<i>INTERFACE-ID</i> : DISCOVER メッセージのクライアント 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。 <ul style="list-style-type: none"> <li>• <b>vlan</b>: VLAN インターフェースを指定します。</li> </ul>
デフォルト	対象 VLAN インターフェースの MAC アドレスをクライアント ID として使用
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 インターフェースで、クライアント ID として VLAN 200 インターフェースの MAC アドレスを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 DISCOVER メッセージと共に送信するホスト名オプションの値を指定します。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	<b>ip dhcp client hostname</b> <i>HOST-NAME</i> <b>no ip dhcp client hostname</b>
パラメーター	<i>HOST-NAME</i> : ホスト名を最大 64 文字で指定します。ホスト名には文字、数字、およびハイフンのみを使用できます。
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(vlan)
特権レベル	レベル: 12
ガイドライン	指定できるのは DHCP DISCOVER メッセージの後の送信だけです。設定が有効になるのは、DHCP クライアントがインターフェース上で DHCP サーバーからの IP アドレス取得が可能な場合だけです。設定しない場合、オプション 12 を設定していないメッセージが装置に送信されます。
制限事項	-
注意事項	ホスト名の先頭は文字に、末尾は文字または数字にしてください。
対象バージョン	1.01.01

使用例：ホスト名オプション値を 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	DHCP サーバーから要求する IP アドレスの優先リース期間を指定します。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	<b>ip dhcp client lease</b> <i>DAYS</i> [ <i>HOURS</i> [ <i>MINUTES</i> ]] <b>no ip dhcp client lease</b>
パラメーター	<i>DAYS</i> ：リース期間の日数を 0～10000 日の範囲で指定します。 <i>HOURS</i> (省略可能)：リース期間の時間数を 0～23 時間の範囲で指定します。 <i>MINUTES</i> (省略可能)：リース期間の分数を 0～59 分の範囲で指定します。
デフォルト	リースオプションは送信されない
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	設定が有効になるのは、DHCP クライアントがインターフェースの IP アドレスを要求できる場合だけです。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：IP アドレスのリースを 5 日に設定する方法を示します。

```
# configure terminal
(config)# interface vlan 100
(config-if-vlan)# ip address dhcp
(config-if-vlan)# ip dhcp client lease 5
(config-if-vlan)#
```

## 4.2 DHCP サーバーコマンド

DHCP サーバー関連の設定コマンドは以下のとおりです。

コマンド	コマンドとパラメーター
ip dhcp pool	ip dhcp pool POOL-NAME no ip dhcp pool POOL-NAME
network	network {NETWORK-ADDRESS MASK   NETWORK-ADDRESS/PREFIX-LENGTH} no network
class (DHCP 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	ip dhcp class CLASS-NAME no ip dhcp class CLASS-NAME
option hex	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	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

### 4.2.1 ip dhcp pool

ip dhcp pool	
目的	DHCP サーバーで DHCP アドレスプールを設定します。また、DHCP プール設定モードに遷移します。遷移後のプロンプトは (config-dhcp-pool)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	ip dhcp pool <i>POOL-NAME</i> no ip dhcp pool <i>POOL-NAME</i>
パラメーター	<i>POOL-NAME</i> : DHCP アドレスプール名を最大 32 文字で指定します。
デフォルト	なし
コマンドモード	グ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 <b>network</b> 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を指定する場合は、 <b>client-identifier</b> または <b>hardware-address</b> コマンドと <b>host</b> コマンドを実行してください。



ip dhcp pool	
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 32 個設定でき、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、 <b>no service dhcp</b> 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)#
```

## 4.2.2 network

network	
目的	DHCP アドレスプールに対して関連付けられたマスクを使用して、ネットワークを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>network</b> { <i>NETWORK-ADDRESS MASK</i>   <i>NETWORK-ADDRESS/PREFIX-LENGTH</i> } <b>no network</b>
パラメーター	<i>NETWORK-ADDRESS</i> ：DHCP アドレスプールのネットワークアドレスを指定します。 <i>MASK</i> ：ネットワークアドレスのネットワーク部分をマスクするビットを指定します。 <i>PREFIX-LENGTH</i> ：ネットワークのプレフィックス長を指定します。ネットワークマスクはこの方法でも指定できます。
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	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。 <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> 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。

network	
	DHCP アドレスプールに対して設定されたネットワークは、ナチュラルネットワークまたはサブネットワークです。設定された DHCP アドレスプールは、ツリーとして編成されます。ツリーのルートは、ナチュラルネットワークが含まれているアドレスプールです。サブネットワークが含まれているアドレスプールは、ルートの下にあるブランチです。手動バインディングエントリ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、 <b>no service dhcp</b> 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 <b>class</b> コマンドの設定と <b>option</b> コマンドの設定も削除されます。
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)#
```

### 4.2.3 class (DHCP Server)

class (DHCP Server)	
目的	DHCP アドレスプールで使用する DHCP クラスを設定します。また、DHCP プールクラス設定モードに遷移します。遷移後のプロンプトは (config-dhcp-pool-class)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>class</b> <i>CLASS-NAME</i> <b>no class</b> <i>CLASS-NAME</i>
パラメーター	<i>CLASS-NAME</i> : 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、 <b>ip dhcp use class</b> を有効に設定する必要があります。 <b>option hex</b> 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、 <b>address range</b> コマンドで DHCP クラスに関連付ける割り当てる IP アドレスの範囲を設定します。受信した DHCP パケットが複数の DHCP クラスに一致する場合、一致したすべての DHCP クラスに関連付けられた IP アドレスの範囲が割り当て候補になります。
制限事項	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。

class (DHCP Server)	
	本設定を反映するには、 <b>no service dhcp</b> 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)#
```

#### 4.2.4 address range

address range	
目的	DHCP クラスに関連付ける IP アドレスの範囲を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>address range</b> <i>START-IP-ADDRESS END-IP-ADDRESS</i> <b>no address range</b> <i>START-IP-ADDRESS END-IP-ADDRESS</i>
パラメーター	<i>START-IP-ADDRESS</i> : IP アドレス範囲の最初の IP アドレスを指定します。 <i>END-IP-ADDRESS</i> : 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、 <b>ip dhcp use class</b> を有効に設定する必要があります。 <b>option hex</b> 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、 <b>address range</b> 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 <b>address range</b> が設定されている DHCP クラスで <b>address range</b> を再設定した場合は、上書き設定されます。 <b>address range</b> 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、 <b>no service dhcp</b> 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)#
```

#### 4.2.5 host

host	
目的	DHCP アドレスプール内にある手動バインディングエントリーの IP アドレスを指定します。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	<b>host</b> { <i>IP-ADDRESS MASK</i>   <i>IP-ADDRESS/PREFIX-LENGTH</i> } <b>no host</b>
パラメーター	<i>IP-ADDRESS</i> : 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。 <i>MASK</i> : ホストアドレスのネットワーク部分をマスクするビットを指定します。 <i>PREFIX-LENGTH</i> : ネットワークのプレフィックス長を指定します。ネットワークマスクはこの方法でも指定できます。
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	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、 <b>no service dhcp</b> 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)#
```

#### 4.2.6 hardware-address

hardware-address	
目的	DHCP アドレスプール内にある手動バインディングエントリーの MAC アドレスを指定します。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	<b>hardware-address</b> <i>MAC-ADDRESS</i> <b>no hardware-address</b>
パラメーター	<i>MAC-ADDRESS</i> : 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。 <ul style="list-style-type: none"> <li>XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> </ul>

hardware-address	
	<ul style="list-style-type: none"> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン":"で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット"."で区切る形式)</li> <li>• XXXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul>
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	<p>バインディングエントリは、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。</p> <p>バインディングエントリを使用して、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。</p> <p>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を指定する場合は、<b>client-identifier</b> コマンドと <b>host</b> 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を指定する場合は、<b>hardware-address</b> コマンドと <b>host</b> コマンドを実行してください。</p>
制限事項	手動バインディングエントリは、DHCP アドレスプールで 1 つだけ指定できません。
注意事項	<p>DHCP サーバーが有効状態では、設定内容が反映されません。</p> <p>本設定を反映するには、<b>no service dhcp</b> 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。</p>
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「pool1」を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# hardware-address 00:00:5E:00:53:A1
(config-dhcp-pool)# host 192.0.2.201/24
(config-dhcp-pool)#
```

#### 4.2.7 client-identifier

client-identifier	
目的	DHCP アドレスプール内の手動バインディングエントリで、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	<b>client-identifier IDENTIFIER</b> <b>no client-identifier</b>
パラメーター	<i>IDENTIFIER</i> : DHCP クライアント ID を 16 進文字列 (最大 14 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 アドレスプール内の手動バインディングエントリ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を 1 つだけ指定できます。手動バインディングエントリを使用して、IP アドレスを、クライアン

client-identifier	
	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を指定する場合は、 <b>client-identifier</b> コマンドと <b>host</b> 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、 <b>no service dhcp</b> 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「pool12」を設定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool12
(config-dhcp-pool)# client-identifier 01524153203124
(config-dhcp-pool)# host 192.0.2.202/24
(config-dhcp-pool)#
```

#### 4.2.8 lease

lease	
目的	アドレスプールから割り当てられた IP アドレスのリース期間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>lease</b> { <i>DAYS</i> [ <i>HOURS</i> [ <i>MINUTES</i> [ <i>SECONDS</i> ]]]   <b>infinite</b> } <b>no lease</b>
パラメーター	<i>DAYS</i> ：リース期間の日数を、0～365 日の範囲で指定します。 <i>HOURS</i> (省略可能)：リース期間の時間数を、0～23 時間の範囲で指定します。 <i>MINUTES</i> (省略可能)：リース期間の分数を、0～59 分の範囲で指定します。 <i>SECONDS</i> (省略可能)：リース期間の秒数を、0～59 秒の範囲で指定します。 <b>infinite</b> ：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、 <b>no service dhcp</b> 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」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
```

#### 4.2.9 default-router

default-router	
目的	DHCP クライアントのデフォルトルーターを指定します。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	<b>default-router</b> <i>IP-ADDRESS</i> [ <i>IP-ADDRESS2</i> ... <i>IP-ADDRESS8</i> ] <b>no default-router</b> <i>IP-ADDRESS</i> [ <i>IP-ADDRESS2</i> ... <i>IP-ADDRESS8</i> ]
パラメーター	<i>IP-ADDRESS</i> : 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。  <i>IP-ADDRESS2</i> ... <i>IP-ADDRESS8</i> : 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、 <b>no service dhcp</b> 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
```

#### 4.2.10 domain-name (DHCP Server)

domain-name (DHCP Server)	
目的	DHCP クライアントのドメイン名を指定します。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	<b>domain-name</b> <i>NAME</i> <b>no domain-name</b>
パラメーター	<i>NAME</i> : ドメイン名を最大 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	-
制限事項	指定できるドメイン名は1つだけです。

domain-name (DHCP Server)	
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、 <b>no service dhcp</b> 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
```

#### 4.2.11 dns-server (DHCP Server)

dns-server (DHCP Server)	
目的	DHCP クライアントの DNS サーバーを指定します。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	<b>dns-server</b> <i>IP-ADDRESS</i> [ <i>IP-ADDRESS2</i> ... <i>IP-ADDRESS8</i> ] <b>no dns-server</b> <i>IP-ADDRESS</i> [ <i>IP-ADDRESS2</i> ... <i>IP-ADDRESS8</i> ]
パラメーター	<i>IP-ADDRESS</i> : 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。 <i>IP-ADDRESS2</i> ... <i>IP-ADDRESS8</i> : 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。
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、 <b>no service dhcp</b> 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
```

#### 4.2.12 netbios-node-type

netbios-node-type	
目的	Microsoft DHCP クライアントの NetBIOS ノードタイプを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>netbios-node-type</b> { <i>b-node</i>   <i>h-node</i>   <i>m-node</i>   <i>p-node</i> } <b>no netbios-node-type</b>
パラメーター	<b>b-node</b> : 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。



netbios-node-type	
	<p><b>p-node</b> : NetBIOS ノードタイプがピアツーピアの場合に指定します。</p> <p><b>m-node</b> : NetBIOS ノードタイプが混合の場合に指定します。</p> <p><b>h-node</b> : NetBIOS ノードタイプがハイブリッドの場合に指定します。</p>
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	<p>DHCP サーバーが有効状態では、設定内容が反映されません。</p> <p>本設定を反映するには、<b>no service dhcp</b> 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。</p>
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)#
```

#### 4.2.13 netbios-name-server

netbios-name-server	
目的	Microsoft DHCP クライアントに WINS サーバーを指定します。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	<p><b>netbios-name-server</b> <i>IP-ADDRESS</i> [<i>IP-ADDRESS2</i> .. <i>IP-ADDRESS8</i>]</p> <p><b>no netbios-name-server</b> <i>IP-ADDRESS</i> [<i>IP-ADDRESS2</i> .. <i>IP-ADDRESS8</i>]</p>
パラメーター	<p><i>IP-ADDRESS</i> : 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。</p> <p><i>IP-ADDRESS2</i> .. <i>IP-ADDRESS8</i> : 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。</p>
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	<p>DHCP サーバーが有効状態では、設定内容が反映されません。</p> <p>本設定を反映するには、<b>no service dhcp</b> コマンドにて DHCP サーバー機能を</p>

netbios-name-server	
	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)#
```

#### 4.2.14 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	<b>next-server</b> <i>IP-ADDRESS</i> <b>no next-server</b>
パラメーター	<i>IP-ADDRESS</i> : 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、 <b>no service dhcp</b> 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：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
```

#### 4.2.15 bootfile

bootfile	
目的	装置をブートするための DHCP クライアントの構成情報、またはブートイメージファイルを指定します。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	<b>bootfile</b> <i>URL</i> <b>no bootfile</b>
パラメーター	<i>URL</i> : 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

bootfile	
ガイドライン	<b>next-server</b> 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、 <b>no service dhcp</b> 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)#
```

#### 4.2.16 option

option	
目的	DHCP サーバーオプションを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>option</b> <i>CODE</i> { <b>ascii</b> <i>STRING</i>   <b>hex</b> { <i>HEX-STRING</i>   <b>none</b> }   <b>ip</b> <i>IP-ADDRESS</i> [ <i>IP-ADDRESS2</i> ... <i>IP-ADDRESS8</i> ]} <b>no option</b> <i>CODE</i>
パラメーター	<i>CODE</i> : オプション番号を 10 進数で指定します。 <b>ascii</b> <i>STRING</i> : オプションの値を、ASCII 文字列（最大 255 バイト）で指定します。 <b>hex</b> <i>HEX-STRING</i> : オプションの値を、16 進文字列（最大 254 文字）で指定します。 <b>hex none</b> : オプションの値を、長さが 0 の 16 進文字列に設定する場合に指定します。 <b>ip</b> <i>IP-ADDRESS</i> : オプションの値を、IP アドレスで指定します。
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 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、 <b>default-router</b> 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、 <b>option</b> コマンドでは設定できません。 <ul style="list-style-type: none"> <li>• オプション 1（ネットワークによって設定される Subnet Mask）</li> <li>• 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）</li> <li>• オプション 6（DNS サーバーによって設定される Domain Name Server）</li> <li>• オプション 15（ドメイン名によって設定される Domain Name）</li> <li>• オプション 44（NetBIOS ネームサーバーによって設定される NetBIOS</li> </ul>

option	
	<p>Name Server)</p> <ul style="list-style-type: none"> <li>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)</li> <li>オプション 51 (リースによって設定される IP Address Lease Time)</li> <li>オプション 58 (リースによって設定される Renewal (T1) Time Value)</li> <li>オプション 59 (リースによって設定される Rebinding (T2) Time Value)</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>オプション 12 (Host Name、デフォルトオプション)</li> <li>オプション 50 (Requested Address、デフォルトオプション)</li> <li>オプション 53 (DHCP Message Type、デフォルトオプション)</li> <li>オプション 54 (Server Identifier、デフォルトオプション)</li> <li>オプション 55 (Parameter Request List、デフォルトオプション)</li> <li>オプション 61 (Client Identifier、デフォルトオプション)</li> <li>オプション 82 (Relay Agent Information Option、デフォルトオプション)</li> </ul>
制限事項	<p>IP アドレスは、最大 8 個指定できます。</p> <p>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。</p> <p>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。</p>
注意事項	<p>DHCP サーバーが有効状態では、設定内容が反映されません。</p> <p>本設定を反映するには、<b>no service dhcp</b> 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。</p>
対象バージョン	1.01.01

使用例: DHCP サーバーオプション 69 (SMTP Server オプション) を、16 進形式で指定する方法を示します。16 進文字列は c0a800fe (192.168.0.254) としています。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# option 69 hex c0a800fe
```

使用例: DHCP サーバーオプション 40 (クライアントの NIS ドメインの名前) を、ASCII 文字列形式で指定する方法を示します。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# option 40 ascii net.market
```

使用例: DHCP サーバーオプション 72 (WWW Server オプション) を、IP 形式で指定する方法を示します。2 つの WWW サーバー 172.19.10.1 と 172.19.10.100 を設定しています。

```
# configure terminal
(config)# ip dhcp pool pool1
(config-dhcp-pool)# option 72 ip 172.19.10.1 172.19.10.100
```

## 4.2.17 ip dhcp class

ip dhcp class	
目的	DHCP クラスを設定します。また、DHCP クラス設定モードに遷移します。遷移後のプロンプトは (config-dhcp-class)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ip dhcp class</b> CLASS-NAME <b>no ip dhcp class</b> 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	グ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、 <b>ip dhcp use class</b> を有効に設定する必要があります。 <b>option hex</b> 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、 <b>no service dhcp</b> 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)#
```

## 4.2.18 option hex

option hex	
目的	DHCP クラスの DHCP オプション一致条件を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>option</b> CODE hex PATTERN [*] [bitmask MASK] <b>no option</b> 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

option hex	
ガイドライン	<p>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、<b>ip dhcp use class</b> を有効に設定する必要があります。</p> <p><b>option hex</b> 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。</p> <p>1 つの DHCP クラスに複数の一致条件を設定できます。</p> <p>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。</p> <p>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。</p> <p>一般的に使用される DHCP オプションは以下のとおりです。</p> <ul style="list-style-type: none"> <li>• オプション 60 (Vendor Class Identifier)</li> <li>• オプション 61 (Client Identifier)</li> <li>• オプション 77 (User Class)</li> <li>• オプション 82 (Relay Agent Information Option) (DHCP サーバーのみ)</li> <li>• オプション 124 (Vendor-identifying Vendor Class)</li> <li>• オプション 125 (Vendor-identifying Vendor-specific Information)</li> </ul>
制限事項	-
注意事項	<p>DHCP サーバーが有効状態では、設定内容が反映されません。</p> <p>本設定を反映するには、<b>no service dhcp</b> 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。</p>
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)#
```

#### 4.2.19 ip dhcp use class

ip dhcp use class	
目的	DHCP サーバー機能において、DHCP クラスによるアドレス割り当てを有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>ip dhcp use class</b> <b>no ip dhcp use class</b>
パラメーター	なし
デフォルト	無効

ip dhcp use class	
コマンドモード	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	<p>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、<b>ip dhcp use class</b> を有効に設定する必要があります。</p> <p><b>option hex</b> 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。</p> <p>DHCP クラスによるアドレス割り当てを有効にした場合は、<b>network</b> コマンド以外に <b>address range</b> コマンドで割り当てる IP アドレスの範囲を設定します。<b>address range</b> 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。</p> <p>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。</p>
制限事項	-
注意事項	<p>DHCP サーバーが有効状態では、設定内容が反映されません。</p> <p>本設定を反映するには、<b>no service dhcp</b> 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。</p>
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)#
```

#### 4.2.20 ip dhcp excluded-address

ip dhcp excluded-address	
目的	IP アドレスの範囲をクライアントへの割り当てから除外します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ip dhcp excluded-address</b> <i>START-IP-ADDRESS</i> <i>END-IP-ADDRESS</i> <b>no ip dhcp excluded-address</b> <i>START-IP-ADDRESS</i> <i>END-IP-ADDRESS</i>
パラメーター	<p><i>START-IP-ADDRESS</i> : 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。</p> <p><i>END-IP-ADDRESS</i> : 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。</p>
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、 <b>ip dhcp excluded-address</b> 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。

ip dhcp excluded-address	
	本設定を反映するには、 <b>no service dhcp</b> 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。

<pre># 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</pre>
---

#### 4.2.21 ip dhcp ping packets

ip dhcp ping packets	
目的	割り当て候補の IP アドレスに対して、DHCP サーバーが ping による事前確認で送信する ping パケットの数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>ip dhcp ping packets</b> <i>COUNT</i> <b>no ip dhcp ping packets</b>
パラメーター	<i>COUNT</i> : 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、 <b>no service dhcp</b> 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。

<pre># configure terminal (config)# ip dhcp ping packets 3 (config)#</pre>
--

#### 4.2.22 ip dhcp ping timeout

ip dhcp ping timeout	
目的	ping による事前確認の応答タイムアウト時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>ip dhcp ping timeout</b> <i>MILLI-SECONDS</i> <b>no ip dhcp ping timeout</b>



ip dhcp ping timeout	
パラメーター	<i>MILLI-SECONDS</i> : 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、 <b>no service dhcp</b> 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)#
```

#### 4.2.23 service dhcp

service dhcp	
目的	DHCP サーバー機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>service dhcp</b> <b>no service dhcp</b>
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、 <b>no service dhcp</b> 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 サーバー機能を有効にする方法を示します。

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

## 4.2.24 show ip dhcp binding

show ip dhcp binding	
目的	DHCP サーバーでアドレスバインディングエントリーを表示します。
シンタックス	<b>show ip dhcp binding</b> [ <i>IP-ADDRESS</i> ]
パラメーター	<i>IP-ADDRESS</i> (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 2017 09:12 AM Automatic
10.1.9.1       0100B7443DC224  Mar 10 2017 10:12 AM Automatic
10.1.11.10     0100B22291226D  Infinite              Manual
```

項番	説明
(1)	DHCP クライアントに割り当てた IP アドレスを表示します。
(2)	DHCP クライアント ID または MAC アドレスを表示します。
(3)	リース満了日時を表示します。
(4)	IP アドレスの割り当て方法を表示します。 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 2017 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

## 4.2.25 show ip dhcp conflict

show ip dhcp conflict	
目的	DHCP サーバーの割り当て候補から除外された IP アドレス (DHCP 競合エントリー) を表示します。
シンタックス	<b>show ip dhcp conflict</b> [ <i>IP-ADDRESS</i> ]
パラメーター	<i>IP-ADDRESS</i> (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、 <b>clear ip dhcp conflict</b> 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。

## 4.2.26 show ip dhcp pool

show ip dhcp pool	
目的	DHCP アドレスプールに関する設定情報を表示します。
シンタックス	<b>show ip dhcp pool</b> [ <i>POOL-NAME</i> ]
パラメーター	<i>POOL-NAME</i> (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。

show ip dhcp pool	
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 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 cl ... (11)
  address-range 192.0.2.101 192.0.2.130 ... (12)
Remaining unallocated address number: 252 ... (13)
Number of leased addresses: 2 ... (14)
```

項番	説明
(1)	DHCP アドレスプール名を表示します。
(2)	サブネットを表示します。
(3)	ブートイメージファイルのパスを表示します。
(4)	デフォルトゲートウェイの IP アドレスを表示します。
(5)	DNS サーバーの IP アドレスを表示します。
(6)	WINS サーバーの IP アドレスを表示します。
(7)	ドメイン名を表示します。
(8)	IP アドレスのリース期間を表示します。
(9)	NetBIOS ノードタイプを表示します。
(10)	ブートイメージファイルを取得するためのブートサーバーの IP アドレスを表示します。
(11)	関連付けられた DHCP クラスを表示します。
(12)	DHCP クラスに関連付ける IP アドレスの範囲を表示します。
(13)	リースされていない IP アドレスの個数を表示します。
(14)	リースされた IP アドレスの個数を表示します。

#### 4.2.27 show ip dhcp server

show ip dhcp server	
目的	DHCP サーバーの設定情報を表示します。
シンタックス	<b>show ip dhcp server</b>
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 ip dhcp server	
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のための DHCP アドレスプール）を表示します。

#### 4.2.28 show ip dhcp server statistics

show ip dhcp server statistics	
目的	DHCP サーバーの統計情報を表示します。
シンタックス	<b>show ip dhcp server statistics</b>
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）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。

#### 4.2.29 clear ip dhcp binding

clear ip dhcp binding	
目的	DHCP サーバーデータベースから、アドレスバインディングエントリーを削除します。
シンタックス	<code>clear ip dhcp {all   pool POOL-NAME} binding [*   IP-ADDRESS]</code>
パラメーター	<p><b>all</b> : 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。</p> <p><b>pool POOL-NAME</b> : 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。</p> <p><b>*</b> : 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。</p> <p><b>IP-ADDRESS</b> : 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。</p>
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	<p>DHCP アドレスプールに <b>all</b> を指定して、IP アドレスに <b>*</b> 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。</p> <p>DHCP アドレスプールに <b>all</b> 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。</p> <p>特定の DHCP アドレスプールを指定して、IP アドレスに <b>*</b> 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。</p> <p>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。</p>
制限事項	-

clear ip dhcp binding	
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
#
```

#### 4.2.30 clear ip dhcp conflict

clear ip dhcp conflict	
目的	DHCP サーバーデータベースから、DHCP 競合エントリーを削除します。
シンタックス	<b>clear ip dhcp {all   pool POOL-NAME} conflict {*   IP-ADDRESS}</b>
パラメーター	<p><b>all</b>：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。</p> <p><b>pool POOL-NAME</b>：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。</p> <p><b>*</b>：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。</p> <p><b>IP-ADDRESS</b>：削除する DHCP 競合エントリーの IP アドレスを指定します。</p>
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	<p>DHCP アドレスプールに <b>all</b> を指定して、IP アドレスに <b>*</b> 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。</p> <p>DHCP アドレスプールに <b>all</b> 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。</p> <p>特定の DHCP アドレスプールを指定して、IP アドレスに <b>*</b> 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。</p> <p>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。</p>
制限事項	-
注意事項	-

clear ip dhcp conflict	
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
#
```

### 4.2.31 clear ip dhcp server statistics

clear ip dhcp server statistics	
目的	すべての DHCP サーバーカウンターをリセットします。
シンタックス	<b>clear ip dhcp server statistics</b>
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：すべての DHCP カウンターを 0 にリセットする方法を示します。

```
# clear ip dhcp server statistics
#
```



## 4.3 DHCPv6 クライアントコマンド

DHCPv6 クライアント関連の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

### 4.3.1 ipv6 dhcp client pd

ipv6 dhcp client pd	
目的	DHCPv6-PD によるプレフィックス委譲を要求する DHCPv6 クライアント機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>ipv6 dhcp client pd</b> {PREFIX-NAME [rapid-commit]   hint IPV6-PREFIX} <b>no ipv6 dhcp client pd</b>
パラメーター	<b>PREFIX-NAME</b> : プレフィックス名を最大 12 文字で指定します。 <b>rapid-commit</b> (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。 <b>hint IPV6-PREFIX</b> : 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。 <b>hint</b> 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。 <b>rapid-commit</b> 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)#
```

### 4.3.2 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	<b>show ipv6 dhcp</b>
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。

### 4.3.3 show ipv6 dhcp interface

show ipv6 dhcp interface	
目的	インターフェースの DHCPv6 関連の設定を表示します。
シンタックス	<b>show ipv6 dhcp interface</b> [ <i>INTERFACE-NAME</i> ]
パラメーター	<i>INTERFACE-NAME</i> (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 ( <b>vlan</b> 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。

#### 4.3.4 clear ipv6 dhcp client

clear ipv6 dhcp client	
目的	VLAN インターフェースの DHCPv6 クライアントを再起動します。
シンタックス	<b>clear ipv6 dhcp client</b> <i>INTERFACE-NAME</i>
パラメーター	<i>INTERFACE-NAME</i> : DHCPv6 クライアントを再起動する VLAN インターフェース ( <b>vlan</b> 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
#
```

## 4.4 DHCPv6 サーバーコマンド

DHCPv6 サーバー関連の設定コマンドは以下のとおりです。

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}

#### 4.4.1 ipv6 dhcp pool

ipv6 dhcp pool	
目的	DHCPv6 サーバーで DHCPv6 プレフィックスプールを設定します。また、DHCPv6 プール設定モードに遷移します。遷移後のプロンプトは (config-dhcp)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ipv6 dhcp pool</b> <i>POOL-NAME</i> <b>no ipv6 dhcp pool</b> <i>POOL-NAME</i>
パラメーター	<i>POOL-NAME</i> : DHCPv6 プレフィックスプール名を最大 12 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	<b>ipv6 dhcp server</b> コマンドで DHCP IPv6 サーバーサービスを有効にしたインターフェースで、受信する DHCP 要求に応じるための IPv6 DHCP プールを指定します。
制限事項	IPv6 DHCP プールは最大 16 個設定できます。DHCP クライアントの手動バインディングエントリは最大 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、 <b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、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)#
```

#### 4.4.2 address prefix

address prefix	
目的	アドレス割り当てのアドレスプレフィックスを指定します。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	<b>address prefix</b> <i>IPV6-PREFIX/PREFIX-LENGTH</i> [ <b>lifetime</b> <i>VALID-LIFETIME</i> <i>PREFERRED-LIFETIME</i> ] <b>no address prefix</b>
パラメーター	<i>IPV6-PREFIX</i> : 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を指定します。  <i>PREFIX-LENGTH</i> : IPv6 アドレスプレフィックスの長さを指定します。  <b>lifetime</b> <i>VALID-LIFETIME</i> (省略可能): IPv6 アドレスプレフィックスの有効期間を、60~4294967295 秒の範囲または <b>infinite</b> (無期限) で指定します。有効期間は、推奨期間よりも長くしてください。期間を指定しない場合、デフォルトの有効期間は 2592000 秒 (30 日) です。  <i>PREFERRED-LIFETIME</i> (省略可能): IPv6 アドレスプレフィックスの推奨期間を、

address prefix	
	60～4294967295 秒の範囲または <b>infinite</b> (無期限) で指定します。推奨期間を指定しない場合、デフォルトの推奨期間は 604800 秒 (7 日) 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
特権レベル	レベル : 12
ガイドライン	後から実行したコマンドにより、前のコマンドは上書きされます。  サーバーがクライアントから要求を受信すると、サーバーは受信したインターフェースと関連付けられた IPv6 DHCP プールをチェックします。要求元クライアントのアドレスを割り当てるように静的バインディングアドレスエントリーが定義されている場合、静的バインディングアドレスが割り当てられます。静的バインディングアドレスエントリーが定義されていない場合、サーバーは、IPv6 DHCP プールに対して指定したアドレスプレフィックスからアドレスを割り当てます。
制限事項	1 つの DHCPv6 プールに対して構成できる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 <b>address-assignment</b> 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、 <b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、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 DHCP プール「pool1」にアドレスプレフィックス 2001:0db8::0/64 を構成する方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool1
(config-dhcp)# address prefix 2001:0db8::0/64 lifetime 200 100
(config-dhcp)#
```

#### 4.4.3 address-assignment

address-assignment	
目的	指定したクライアントに割り当てる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	<b>address-assignment</b> <i>IPV6-ADDRESS CLIENT-DUID</i> [ <b>iaid</b> <i>IAID</i> ] [ <b>lifetime</b> <i>VALID-LIFETIME PREFERRED-LIFETIME</i> ] <b>no address-assignment</b> <i>IPV6-ADDRESS CLIENT-DUID</i> [ <b>iaid</b> <i>IAID</i> ]
パラメーター	<i>IPV6-ADDRESS</i> : 特定の DHCPv6 クライアントに割り当てる IPv6 アドレスを指定します。  <i>CLIENT-DUID</i> : IPv6 アドレスを取得する DHCPv6 クライアントの DHCP 固有識別子 (DUID) を指定します。  <b>iaid</b> <i>IAID</i> (省略可能) : DHCPv6 クライアントのインターフェースのアイデンティティアソシエーション識別子 (IAID) を指定します。IAID は、1～8 文字の 16 進文字列です。IAID は、クライアントに割り当てられた恒久アドレス (IANA) の集合を一意に識別します。

address-assignment	
	<p><b>lifetime</b> <i>VALID-LIFETIME</i> (省略可能) : IPv6 アドレスの有効期間を、60～4294967295 秒の範囲で指定します。最大値を指定すると、有効期間は無期限になります。有効期間は、推奨期間より長くしてください。</p> <p><i>PREFERRED-LIFETIME</i> (省略可能) : IPv6 アドレスの推奨期間を、60～4294967295 秒の範囲で指定します。最大値を指定すると、推奨期間は無期限になります。</p>
デフォルト	有効期間 : 2592000 秒 (30 日)、推奨期間 : 604800 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	<p>サーバーがクライアントから要求を受信すると、サーバーは、受信したインターフェースと関連付けられた IPv6 DHCP プールをチェックします。</p> <p>以下のすべての条件が成立する場合、一致したエントリーが割り当てられます。</p> <ul style="list-style-type: none"> <li>• 要求メッセージに IANA オプションが含まれている</li> <li>• IAID を使用して構成された空きの静的エントリーがある</li> <li>• エントリーがメッセージの DUID と IAID の両方と一致する</li> </ul> <p>以下のすべての条件が成立する場合、DUID と一致したエントリーが応答で返されます。</p> <ul style="list-style-type: none"> <li>• 一致するエントリーがない</li> <li>• IAID の指定がない空きの静的エントリーがある</li> <li>• エントリーがメッセージの DUID と一致する</li> </ul> <p>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)。一致するエントリーがない場合、クライアントには IPv6 DHCP プールで指定されたアドレスプレフィックスのアドレスが割り当てられません。</p>
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 <b>address prefix</b> 設定を削除すると、 <b>address-assignment</b> 設定も削除されます。
注意事項	<p>DHCPv6 サーバーが有効状態では、設定内容が反映されません。</p> <p>本設定を反映するには、<b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、再度 DHCPv6 サーバー機能を有効にしてください。</p> <p>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。</p>
対象バージョン	1.01.01

使用例 : 「pool1」という名前の IPv6 DHCP プールにある静的バインディングアドレスエントリーを構成して、IPv6 DHCP プールを VLAN 100 インターフェースと関連付ける方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool1
(config-dhcp)# address prefix 2001:0db8::0/64 lifetime 200 100
(config-dhcp)# address-assignment 2001:0db8::1:2 000300010506bbccdde
(config-dhcp)# exit
(config)# interface vlan 100
(config-if-vlan)# ipv6 dhcp server pool1
(config-if-vlan)#
```



使用例：「pool2」という名前の IPv6 DHCP プールにある静的バインディングアドレスエントリーを、IAID オプションを使用して構成して、IPv6 DHCP プールを VLAN 200 インターフェースと関連付ける方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool2
(config-dhcp)# address prefix 2001:aab8::0/64 lifetime 200 100
(config-dhcp)# address-assignment 2001:aab8::2:2 00030001050611223344 iaid 1234
(config-dhcp)# exit
(config)# interface vlan 200
(config-if-vlan)# ipv6 dhcp server pool2
(config-if-vlan)#
```

#### 4.4.4 domain-name (DHCPv6 Server)

domain-name (DHCPv6 Server)	
目的	要求元の DHCPv6 クライアントに割り当てられるドメイン名を構成します。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	<b>domain-name</b> <i>DOMAIN-NAME</i> <b>no domain-name</b>
パラメーター	<i>DOMAIN-NAME</i> : ドメイン名を最大 253 文字で指定します。
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	ドメイン名は 1 つだけ指定できます。
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、 <b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、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：「pool1」という名前の DHCPv6 サーバープール内のドメイン名を構成する方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool1
(config-dhcp)# domain-name v6domain
(config-dhcp)#
```

#### 4.4.5 dns-server (DHCPv6 Server)

dns-server (DHCPv6 Server)	
目的	要求元の IPv6 クライアントに割り当てられる DNS IPv6 サーバーリストを構成します。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	<b>dns-server</b> <i>IPV6-ADDRESS</i> <b>no dns-server</b> <i>IPV6-ADDRESS</i>
パラメーター	<i>IPV6-ADDRESS</i> : DHCPv6 クライアントが DNS サーバーとして使用する 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	DHCPv6 プール設定モード
特権レベル	レベル : 12
ガイドライン	複数のサーバーアドレスを構成する場合、構成するサーバーアドレスの数だけ、

dns-server (DHCPv6 Server)	
	コマンドの実行を繰り返してください。
制限事項	-
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、 <b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、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：「pool1」という名前の DHCPv6 サーバープール内の DNS IPv6 サーバーを構成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)#
```

#### 4.4.6 prefix-delegation pool

prefix-delegation pool	
目的	プールからプレフィックスを委譲できるローカル IPv6 プレフィックスプールを指定します。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	<b>prefix-delegation pool LOCAL-POOL-NAME [lifetime VALID-LIFETIME PREFERRED-LIFETIME]</b> <b>no prefix-delegation pool LOCAL-POOL-NAME</b>
パラメーター	<b>LOCAL-POOL-NAME</b> ：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。  <b>lifetime VALID-LIFETIME</b> (省略可能)：IPv6 アドレスプレフィックスの有効期間を、60～4294967295 秒の範囲または <b>infinite</b> (無期限) で指定します。有効期間は、推奨期間より長くしてください。有効期間を指定しない場合、デフォルトの有効期間は 2592000 秒 (30 日) です。  <b>lifetime PREFERRED-LIFETIME</b> (省略可能)：IPv6 アドレスプレフィックスの推奨期間を、60～4294967295 秒の範囲または <b>infinite</b> (無期限) で指定します。推奨期間を指定しない場合、デフォルトの推奨期間は 604800 秒 (7 日) 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
特権レベル	レベル：12
ガイドライン	DHCP プールのサービスを受けるクライアントにプレフィックスを委譲するために、IPv6 DHCP プールにあるローカル IPv6 プレフィックスプールを指定するコマンドです。  サーバーがクライアントから要求を受信すると、サーバーは受信したインターフェースと関連付けられた IPv6 DHCP プールをチェックします。  プレフィックスを要求元クライアントに委譲するように静的バインディングプレフィックスエントリが定義されている場合、静的バインディングプレフィックスが委譲されます。  静的バインディングプレフィックスエントリがプレフィックスを要求元クライアントに委譲するように定義されていない場合、サーバーは、IPv6 DHCP プールで指定されたローカル IPv6 プレフィックスプールのプレフィックスを委譲しま

prefix-delegation pool	
	す。
制限事項	1 つの IPv6 DHCP プールでは、ローカル IPv6 プレフィックスプールを 1 つだけ指定できます。  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 <b>prefix-delegation</b> 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、 <b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、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：「clientprefix」という名前のローカル IPv6 プレフィックスプールを構成し、「pool1」という名前の IPv6 DHCP プール内のプールを指定して、IPv6 DHCP プールを VLAN 100 インターフェースと関連付ける方法を示します。

```
# configure terminal
(config)# ipv6 local pool clientprefix 3004:db8::/48 64
(config)# ipv6 dhcp pool pool1
(config-dhcp)# prefix-delegation pool clientprefix lifetime 300 200
(config-dhcp)# exit
(config)# interface vlan 100
(config-if-vlan)# ipv6 dhcp server pool1
(config-if-vlan)#
```

#### 4.4.7 prefix-delegation

prefix-delegation	
目的	指定したクライアントに委譲するプレフィックスを指定します。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	<b>prefix-delegation</b> <i>IPV6-PREFIX/PREFIX-LENGTH CLIENT-DUID</i> [ <b>iaid</b> <i>IAID</i> ] [ <b>lifetime</b> <i>VALID-LIFETIME PREFERRED-LIFETIME</i> ] <b>no prefix-delegation</b> <i>IPV6-PREFIX/PREFIX-LENGTH CLIENT-DUID</i> [ <b>iaid</b> <i>IAID</i> ]
パラメーター	<i>IPV6-PREFIX</i> : 指定した DHCPv6 クライアントに割り当て権限を委譲する IPv6 アドレスプレフィックスを指定します。  <i>PREFIX-LENGTH</i> : 割り当て権限を委譲する IPv6 アドレスプレフィックスの長さを指定します。  <i>CLIENT-DUID</i> : DHCPv6 プレフィックス委譲機能対応機器（移譲先機器）の DHCP 固有識別子（DUID）を指定します。  <b>iaid</b> <i>IAID</i> (省略可能): DHCPv6 プレフィックス委譲機能対応機器（移譲先機器）のインターフェースのアイデンティティアソシエーション識別子（IAID）を指定します。IAID は、1~8 文字の 16 進文字列です。IAID は、要求元のルーターに割り当てられたプレフィックスの集合を一意に識別します。  <b>lifetime</b> <i>VALID-LIFETIME</i> (省略可能): IPv6 アドレスプレフィックスの有効期間を、60~4294967295 秒の範囲または <b>infinite</b> （無期限）で指定します。有効期間は、推奨期間より長くしてください。有効期間を指定しない場合、デフォルトの有効期間は 2592000 秒（30 日）です。  <i>PREFERRED-LIFETIME</i> (省略可能): IPv6 アドレスプレフィックスの推奨期間を、60~4294967295 秒の範囲または <b>infinite</b> （無期限）で指定します。推奨期間を

prefix-delegation	
	指定しない場合、デフォルトの推奨期間は 604800 秒（7 日）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
特権レベル	レベル : 12
ガイドライン	<p>1 つのクライアント、または 1 つのクライアントの IAPD に対して、複数の静的バインディングプレフィックスエントリを定義できます。</p> <p>サーバーがクライアントから要求を受信すると、サーバーは受信したインターフェースと関連付けられた IPv6 DHCP プールをチェックします。</p> <p>以下のすべての条件が成立する場合、すべての一致したエントリが委譲されます。</p> <ul style="list-style-type: none"> <li>• 要求メッセージに IAPD オプションが含まれている</li> <li>• IAID を使用して構成された空きの静的エントリがある</li> <li>• エントリがメッセージの DUID と IAID の両方と一致する</li> </ul> <p>以下のすべての条件が成立する場合、DUID と一致したエントリが応答で返されます。</p> <ul style="list-style-type: none"> <li>• 一致するエントリがない</li> <li>• IAID の指定がない空きの静的エントリがある</li> <li>• エントリがメッセージの DUID と一致する</li> </ul> <p>また、以下のすべての条件が成立する場合も、DUID と一致したエントリが応答で返されます。</p> <ul style="list-style-type: none"> <li>• 要求メッセージに IAID オプションがない</li> <li>• IAID の指定がない空きの静的エントリがある</li> <li>• エントリがメッセージの DUID と一致する</li> </ul> <p>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）。一致するエントリがない場合、IPv6 DHCP プールで指定されたローカル IPv6 プレフィックスプールのプレフィックスが、クライアントに委譲されます。</p>
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 <b>prefix-delegation pool</b> 設定を削除すると、 <b>prefix-delegation</b> 設定も削除されます。
注意事項	<p>DHCPv6 サーバーが有効状態では、設定内容が反映されません。</p> <p>本設定を反映するには、<b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、再度 DHCPv6 サーバー機能を有効にしてください。</p> <p>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。</p>
対象バージョン	1.01.01

使用例 : 「pool1」という名前の IPv6 DHCP プールにある静的バインディングプレフィックスエントリを構成して、IPv6 DHCP プールを VLAN 100 インターフェースと関連付ける方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool1
(config-dhcp)# prefix-delegation 3004:db8::889/64 000300010506bbccdde
(config-dhcp)# exit
(config)# interface vlan 100
(config-if-vlan)# ipv6 dhcp server pool1
```

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

#### 4.4.8 ipv6 dhcp excluded-address

ipv6 dhcp excluded-address	
目的	DHCPv6 サーバーが DHCP クライアントに割り当てる IPv6 アドレスのうち、割り当てから除外する IPv6 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	<b>ipv6 dhcp excluded-address</b> <i>LOW-ADDRESS</i> [ <i>HIGH-ADDRESS</i> ] <b>no ipv6 dhcp excluded-address</b> <i>LOW-ADDRESS</i> [ <i>HIGH-ADDRESS</i> ]
パラメーター	<i>LOW-ADDRESS</i> : 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。  <i>HIGH-ADDRESS</i> (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	DHCPv6 サーバーは、装置の IPv6 アドレスを除くすべてのアドレスをクライアントに割り当てます。除外対象のアドレスは、アドレス割り当て用のプールにだけ、適用されます。
制限事項	除外対象の IPv6 アドレスは、1 つのプールにつき最大 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、 <b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、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 3004:db8::1:10 を除外対象アドレスに構成する方法を示します。

```
# configure terminal
(config)# ipv6 dhcp excluded-address 3004:db8::1:10
(config)#
```

#### 4.4.9 ipv6 local pool

ipv6 local pool	
目的	ローカル IPv6 プレフィックスプールを構成します。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	<b>ipv6 local pool</b> <i>LOCAL-POOL-NAME</i> <i>IPv6-PREFIX/PREFIX-LENGTH</i> <i>ASSIGNED-LENGTH</i> <b>no ipv6 local pool</b> <i>LOCAL-POOL-NAME</i>
パラメーター	<i>LOCAL-POOL-NAME</i> : 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。  <i>IPv6-PREFIX</i> : 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を指定します。  <i>PREFIX-LENGTH</i> : 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の長さを指定します。

ipv6 local pool	
	<i>ASSIGNED-LENGTH</i> : ローカル IPv6 プレフィックスプールに割り当て権限が委譲されるプレフィックス長を指定します。割り当てられる長さの値は、プレフィックスの長さより大きくしてください。
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、 <b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、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: 「clientprefix」という名前のローカル IPv6 プレフィックスプールを作成して、作成したローカルプールを DHCP プール「pool1」で使用する方法を示します。

```
# configure terminal
(config)# ipv6 local pool clientprefix 3004:db8::/48 64
(config)# ipv6 dhcp pool pool1
(config-dhcp)# prefix-delegation pool clientprefix lifetime 300 200
(config-dhcp)#
```

#### 4.4.10 ipv6 dhcp server

ipv6 dhcp server	
目的	インターフェースの DHCP IPv6 サーバー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	<b>ipv6 dhcp server</b> <i>POOL-NAME</i> [ <b>rapid-commit</b> ] [ <b>preference</b> <i>VALUE</i> ] [ <b>allow-hint</b> ] <b>no ipv6 dhcp server</b>
パラメーター	<i>POOL-NAME</i> : インターフェースで受信する要求に応じるための、DHCPv6 プレフィックスプール名を指定します。  <b>rapid-commit</b> (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。  <b>preference</b> <i>VALUE</i> (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。  <b>allow-hint</b> (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

ipv6 dhcp server	
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	<p>IPv6 DHCP プールは、複数のインターフェースと関連付けられます。1 つのインターフェースには、IPv6 DHCP プールを 1 つだけ関連付けられます。DHCP (IPv6) のクライアント、サーバーの各機能は、1 つのインターフェース上では相互に排他的です。</p> <p>コマンド実行時に <b>rapid-commit</b> 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。</p> <p><b>preference</b> 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。</p> <p><b>allow-hint</b> 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。</p>
制限事項	IPv6 DHCP プールは、関連付けを行う前に構成してください。
注意事項	<p>DHCPv6 サーバーが有効状態では、設定内容が反映されません。</p> <p>本設定を反映するには、<b>no service ipv6 dhcp</b> コマンドにて DHCPv6 サーバー機能をいったん無効状態にした後、再度 DHCPv6 サーバー機能を有効にしてください。</p>
対象バージョン	1.01.01

使用例 : DHCP プール「pool1」を作成し、VLAN 100 インターフェースの DHCP IPv6 サーバーサービスが DHCP プール「pool1」を使用して、プレフィックスを委譲可能にする方法を示します。

```
# configure terminal
(config)# ipv6 dhcp pool pool1
(config-dhcp)# exit
(config)# interface vlan 100
(config-if-vlan)# ipv6 dhcp server pool1
(config-if-vlan)#
```

#### 4.4.11 service ipv6 dhcp

service ipv6 dhcp	
目的	装置で IPv6 DHCP サーバーを有効にします。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	<b>service ipv6 dhcp</b> <b>no service ipv6 dhcp</b>
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	-

service ipv6 dhcp	
対象バージョン	1.01.01

使用例：IPv6 DHCP サーバーを有効にする方法を示します。

```
# configure terminal
(config)# service ipv6 dhcp
(config)#
```

#### 4.4.12 show ipv6 dhcp binding

show ipv6 dhcp binding	
目的	DHCPv6 サーバーでアドレスバインディングエントリを表示します。
シンタックス	<b>show ipv6 dhcp binding</b> [ <i>IPV6-ADDRESS</i> ]
パラメーター	<i>IPV6-ADDRESS</i> (省略可能) : 表示するアドレスバインディングエントリの 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の総数を表示します。

#### 4.4.13 show ipv6 dhcp pool

show ipv6 dhcp pool	
目的	DHCPv6 プレフィックスプールに関する設定情報を表示します。



show ipv6 dhcp pool	
シンタックス	show ipv6 dhcp pool [ <i>POOL-NAME</i> ]
パラメーター	<i>POOL-NAME</i> (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ックスを表示します。
(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)	プレフィッ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)	委譲するプレフィックスの推奨期間を表示します。
(9)	委譲するプレフィックスの有効期間を表示します。

#### 4.4.14 show ipv6 excluded-address

show ipv6 excluded-address	
目的	リースする範囲から除外する IPv6 アドレスを表示します。
シンタックス	<b>show ipv6 excluded-address</b>
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。

#### 4.4.15 show ipv6 local pool

show ipv6 local pool	
目的	ローカル IPv6 プレフィックスプールの情報を表示します。
シンタックス	<b>show ipv6 local pool</b> [ <i>LOCAL-POOL-NAME</i> ]
パラメーター	<i>LOCAL-POOL-NAME</i> (省略可能) : 表示するローカル IPv6 プレフィックスプールを指定します。
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。



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。

#### 4.4.16 show ipv6 dhcp operation

show ipv6 dhcp operation	
目的	DHCPv6 サーバーの設定を表示します。
シンタックス	<b>show ipv6 dhcp operation</b>
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 ipv6 dhcp operation	
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。

項番	説明
(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)	手動プレフィクス委譲エントリーの有効期間を表示します。
(19)	委譲するプレフィクスの推奨期間を表示します。
(20)	委譲するプレフィクスの有効期間を表示します。

#### 4.4.17 clear ipv6 dhcp binding

clear ipv6 dhcp binding	
目的	DHCPv6 サーバーに登録されたバインディングエントリーを削除します。
シンタックス	<code>clear ipv6 dhcp binding {all   IPV6-ADDRESS}</code>
パラメーター	<code>all</code> : 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。 <code>IPV6-ADDRESS</code> : 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
#
```

## 4.5 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

### 4.5.1 autoconfig enable

autoconfig enable	
目的	DHCP Auto Configuration を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>autoconfig enable</b> <b>no autoconfig enable</b>
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	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul> <p>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。</p> <p>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。</p>
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)#
```

### 4.5.2 show autoconfig

show autoconfig	
目的	DHCP Auto Configuration の設定を表示します。
シンタックス	<b>show autoconfig</b>
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

## 4.6 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

### 4.6.1 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	<b>clock set</b> 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 <b>clock timezone</b> 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
#
```

#### 4.6.2 clock summer-time

clock summer-time	
目的	システムが自動的にサマータイムに切り替わることを有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<p><b>clock summer-time recurring</b> WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM [OFFSET]</p> <p><b>clock summer-time date</b> DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM [OFFSET]</p> <p><b>no clock summer-time</b></p>
パラメーター	<p><b>recurring</b>：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。</p> <ul style="list-style-type: none"> <li>• <i>WEEK</i>：週を 1~4, last で指定します</li> <li>• <i>DAY</i>：曜日を sun, mon, tue, wed, thu, fri, sat で指定します。</li> <li>• <i>MONTH</i>：月を jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec で指定します。</li> <li>• <i>HH:MM</i>：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。</li> </ul> <p><b>date</b>：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。</p> <ul style="list-style-type: none"> <li>• <i>DATE</i>：日を指定します。</li> <li>• <i>MONTH</i>：月を jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec で指定します。</li> <li>• <i>YEAR</i>：西暦年を指定します。</li> <li>• <i>HH:MM</i>：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。</li> </ul> <p><i>OFFSET</i> (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。</p>
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)#
```

### 4.6.3 clock timezone

clock timezone	
目的	タイムゾーン (UTC (協定世界時) からのオフセット) を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>clock timezone</b> {+   -} <i>HOURS-OFFSET</i> [ <i>MINUTES-OFFSET</i> ] <b>no clock timezone</b>
パラメーター	+ : UTC からのオフセットが正值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。 <i>HOURS-OFFSET</i> : UTC からのオフセットを 0~13 時間の範囲で指定します。 <i>MINUTES-OFFSET</i> (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)#
```

### 4.6.4 sntp server

sntp server	
目的	Sntp で時刻を問い合わせる NTP/Sntp サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>sntp server</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> } <b>no sntp server</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> }
パラメーター	<i>IP-ADDRESS</i> : NTP/Sntp サーバーの IPv4 アドレスを指定します。 <i>IPV6-ADDRESS</i> : 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 ( <b>show sntp</b> での表示順)

sntp server	
	<p>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。</p> <p>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。</p> <p>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。</p>
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)#
```

#### 4.6.5 sntp interval

sntp interval	
目的	SNTP での時刻の問い合わせ間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>sntp interval SECONDS</b> <b>no sntp interval</b>
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)#
```

#### 4.6.6 sntp enable

sntp enable	
目的	SNTP クライアント機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>sntp enable</b> <b>no sntp enable</b>
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)#
```

#### 4.6.7 show clock

show clock	
目的	日時情報を表示します。
シンタックス	<b>show clock</b>
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, 2017-03-01 ... (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 <b>recurring</b> 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 <b>date</b> パラメーターを指定して有効にした場合

#### 4.6.8 show sntp

show sntp	
目的	SNTP の情報を表示します。
シンタックス	<b>show sntp</b>
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
-----
10.0.0.11             8        4        00:02:02
10.0.0.11             7        4        00:01:02 Synced
10::2                 -----
fe80::1111 vlan1     -----
-----
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。

## 4.7 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

### 4.7.1 ntp server

ntp server	
目的	クライアントモードで時刻を問い合わせる NTP サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp server</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> } [ <b>version</b> <i>NUMBER</i> ] [ <b>key</b> <i>KEY-ID</i> ]

ntp server	
	<code>[prefer] [min-poll INTERVAL] [max-poll INTERVAL]</code> <code>no ntp server {IP-ADDRESS   IPV6-ADDRESS}</code>
パラメーター	<p><i>IP-ADDRESS</i> : NTP サーバーの IPv4 アドレスを指定します。</p> <p><i>IPV6-ADDRESS</i> : NTP サーバーの IPv6 アドレスを指定します。</p> <p><b>version</b> <i>NUMBER</i> (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。</p> <p><b>key</b> <i>KEY-ID</i> (省略可能) : 認証キーの ID を 1~255 の範囲で指定します。</p> <p><b>prefer</b> (省略可能) : 優先する NTP サーバーの場合に指定します。</p> <p><b>min-poll</b> <i>INTERVAL</i> (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 <i>n</i> とすると、2 の <i>n</i> 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 <i>n</i>=6 (64 秒) です。</p> <p><b>max-poll</b> <i>INTERVAL</i> (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 <i>n</i> とすると、2 の <i>n</i> 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 <i>n</i>=10 (1024 秒) です。</p>
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、 <b>prefer</b> 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)#
```

#### 4.7.2 ntp peer

ntp peer	
目的	Symmetric Active モードで関係付ける NTP サーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<code>ntp peer {IP-ADDRESS   IPV6-ADDRESS} [version NUMBER] [key KEY-ID]</code> <code>[prefer] [min-poll INTERVAL] [max-poll INTERVAL]</code> <code>no ntp peer {IP-ADDRESS   IPV6-ADDRESS}</code>
パラメーター	<p><i>IP-ADDRESS</i> : NTP サーバーの IPv4 アドレスを指定します。</p> <p><i>IPV6-ADDRESS</i> : NTP サーバーの IPv6 アドレスを指定します。</p> <p><b>version</b> <i>NUMBER</i> (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。</p> <p><b>key</b> <i>KEY-ID</i> (省略可能) : 認証キーの ID を 1~255 の範囲で指定します。</p>

ntp peer	
	<p><b>prefer</b> (省略可能) : 優先する NTP サーバーの場合に指定します。</p> <p><b>min-poll INTERVAL</b> (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。</p> <p><b>max-poll INTERVAL</b> (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。</p>
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)#
```

### 4.7.3 ntp update-calendar

ntp update-calendar	
目的	NTP で取得した時刻のハードウェアクロックへの更新を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp update-calendar</b> <b>no ntp update-calendar</b>
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)#
```



## 4.7.4 ntp authenticate

ntp authenticate	
目的	NTP 認証を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp authenticate</b> <b>no ntp authenticate</b>
パラメーター	なし
デフォルト	NTP 認証は有効 ( <b>ntp authenticate</b> )
コマンドモード	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。 <ul style="list-style-type: none"> <li>• NTP 認証を <b>ntp authenticate</b> コマンドで有効にする</li> <li>• NTP 認証キーを <b>ntp authentication-key</b> コマンドで定義</li> <li>• 使用する NTP 認証キーID を <b>ntp trusted-key</b> コマンドで指定</li> </ul> また、NTP 認証を使用して同期する NTP サーバーに対しては、 <b>ntp server</b> コマンド、または <b>ntp peer</b> コマンドにおいて、 <b>key</b> 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、 <b>ntp access-group</b> コマンドで <b>notrust</b> 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)#
```

## 4.7.5 ntp authentication-key

ntp authentication-key	
目的	NTP の認証キーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp authentication-key KEY-ID md5 VALUE</b> <b>no ntp authentication-key KEY-ID</b>
パラメーター	<b>KEY-ID</b> : 認証キーID を 1~255 の範囲で指定します。 <b>md5 VALUE</b> : 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	
	<ul style="list-style-type: none"> <li>• NTP 認証を <b>ntp authenticate</b> コマンドで有効にする</li> <li>• NTP 認証キーを <b>ntp authentication-key</b> コマンドで定義</li> <li>• 使用する NTP 認証キーID を <b>ntp trusted-key</b> コマンドで指定</li> </ul> <p>また、NTP 認証を使用して同期する NTP サーバーに対しては、<b>ntp server</b> コマンド、または <b>ntp peer</b> コマンドにおいて、<b>key</b> パラメーターで NTP 認証キーID を指定してください。</p>
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)#
```

#### 4.7.6 ntp trusted-key

ntp trusted-key	
目的	NTP 認証で使用する認証キーとして有効にする認証キーID を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp trusted-key</b> <i>KEY-ID</i> <b>no ntp trusted-key</b> <i>KEY-ID</i>
パラメーター	<i>KEY-ID</i> : 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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• NTP 認証を <b>ntp authenticate</b> コマンドで有効にする</li> <li>• NTP 認証キーを <b>ntp authentication-key</b> コマンドで定義</li> <li>• 使用する NTP 認証キーID を <b>ntp trusted-key</b> コマンドで指定</li> </ul> <p>また、NTP 認証を使用して同期する NTP サーバーに対しては、<b>ntp server</b> コマンド、または <b>ntp peer</b> コマンドにおいて、<b>key</b> パラメーターで NTP 認証キーID を指定してください。</p>
制限事項	<b>ntp authentication-key</b> 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)#
```

## 4.7.7 ntp control-key

ntp control-key	
目的	NTP control message (Mode=6) の認証キーID を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp control-key</b> <i>KEY-ID</i> <b>no ntp control-key</b>
パラメーター	<i>KEY-ID</i> : 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	<b>ntp authentication-key</b> 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)#
```

## 4.7.8 ntp request-key

ntp request-key	
目的	モード 7 の NTP パケットの認証キーID を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp request-key</b> <i>KEY-ID</i> <b>no ntp request-key</b>
パラメーター	<i>KEY-ID</i> : 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	<b>ntp authentication-key</b> 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)#
```

## 4.7.9 ntp disable

ntp disable	
目的	対象 VLAN インターフェースの NTP サービスを無効にします。有効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp disable</b> <b>no ntp disable</b>
パラメーター	なし
デフォルト	NTP サービスは有効 ( <b>no ntp disable</b> )
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)#
```

## 4.7.10 ntp access-group

ntp access-group	
目的	NTP サービスへのアクセス制御を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp access-group {default   <i>IP-ADDRESS</i> [<i>IP-MASK</i>]   <i>IPV6-ADDRESS</i>   <i>IPV6-ADDRESS/PREFIX-LENGTH</i>} [ignore] [nomodify] [noquery] [nopeer] [noserve] [notrust] [version]</b> <b>no ntp access-group {default   <i>IP-ADDRESS</i> [<i>IP-MASK</i>]   <i>IPV6-ADDRESS</i>   <i>IPV6-ADDRESS/PREFIX-LENGTH</i>}</b>
パラメーター	<b>default</b> : 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。  <i>IP-ADDRESS</i> : 特定の IPv4 アドレスを対象にする場合に指定します。  <i>IP-ADDRESS IP-MASK</i> : 特定の IPv4 ネットワークを対象にする場合に指定します。  <i>IPV6-ADDRESS</i> : 特定の IPv6 アドレスを対象にする場合に指定します。  <i>IPV6-ADDRESS/PREFIX-LENGTH</i> : 特定の IPv6 ネットワークを対象にする場合に指定します。  <b>ignore</b> (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。  <b>nomodify</b> (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。  <b>noquery</b> (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	
	<p><b>nopeer</b> (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。</p> <p><b>noserve</b> (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。</p> <p><b>notrust</b> (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。</p> <p><b>version</b> (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。</p>
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、 <b>default</b> 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	<p>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。</p> <p>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。</p>
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)#
```

#### 4.7.11 ntp max-associations

ntp max-associations	
目的	アソシエーション (NTP ピア、NTP クライアント) の最大数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<p><b>ntp max-associations</b> <i>NUMBER</i></p> <p><b>no ntp max-associations</b></p>
パラメーター	<i>NUMBER</i> : 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)#
```

#### 4.7.12 ntp master

ntp master	
目的	自装置のハードウェアクロック (RTC) を信頼できる情報源として利用することを有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>ntp master</b> <i>STRATUM</i> <b>no ntp master</b>
パラメーター	<i>STRATUM</i> : 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)#
```

#### 4.7.13 service ntp

service ntp	
目的	NTP サービスを有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>service ntp</b> <b>no service ntp</b>
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)#
```

#### 4.7.14 show ntp associations

show ntp associations	
目的	NTP アソシエーションの状態を表示します。
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 192.168.10.101, Local 192.168.10.102
(3)                               (4)                               (5)                               (6)
Our mode client, Peer mode server, Stratum 6, Precision -22
(7)                               (8)                               (9)                               (10)
Leap 00, RefID [192.168.10.254], RootDistance 0.00009, RootDispersion 0.04179
(11)                               (12)                               (13)                               (14)                               (15)
PPoll 10, HPoll 10, KeyID 0, Version 4, Association 8360
(16)                               (17)                               (18)                               (19)                               (20)
Reach 377, Unreach 0, Flash 0x0000, Timer 948s, flags System_Peer, Config
Reference Timestamp : e29fbe49.00842c93 Fri, Jun 26 2020 9:22:33.002 ... (21)
Originate Timestamp : e29fbf51.2b8d07f8 Fri, Jun 26 2020 9:26:57.170 ... (22)
Receive Timestamp   : e29fbf51.313ffd51 Fri, Jun 26 2020 9:26:57.192 ... (23)
Transmit Timestamp  : e29fbf51.31401179 Fri, Jun 26 2020 9:26:57.192 ... (24)
Filter Delay:      0.00000 0.00000 0.00000 0.00000 ... (25)
                   0.00000 0.00000 0.00000 0.00000
Filter Offset:    0.022263 0.023537 0.025275 0.016526 ... (26)
                   0.017822 0.019188 0.020576 0.021219
Filter Order:     0         1         2         3         ... (27)
                   4         5         6         7
(28)                               (29)                               (30)                               (31)
Offset 0.022263, Delay 0.00000, Error Bound 0.12512, Filter Error 0.05753
```

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。

#### 4.7.15 show ntp status

show ntp status	
目的	NTP の状態を表示します。
シンタックス	<b>show ntp status</b>
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 2017 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。

## 4.8 TELNET コマンド

TELNET 関連の設定コマンドは以下のとおりです。

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]

### 4.8.1 ip telnet server

ip telnet server	
目的	Telnet サーバーを有効にします。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	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 サーバーを有効にする方法を示します。

```
# configure terminal
(config)# ip telnet server
(config)#
```

### 4.8.2 ip telnet service-port

ip telnet service-port	
目的	Telnet 用のサービス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。
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

ip telnet service-port	
	のウェルノウン TCP ポート番号は、23 です。
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 サービスポート番号を、3000 に変更する方法を示します。

```
# configure terminal
(config)# ip telnet service-port 3000
(config)#
```

### 4.8.3 ip telnet source-interface

ip telnet source-interface	
目的	Telnet 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	<b>ip telnet source-interface</b> <i>INTERFACE-ID</i> <b>no ip telnet source-interface</b>
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>vlan</b> : VLAN インターフェースを指定します。</li> <li>• <b>mgmt</b> : マネージメントポートを指定します。</li> </ul>
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、 <b>vlan</b> 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、 <b>mgmt</b> 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)#
```

### 4.8.4 show ip telnet server

show ip telnet server	
目的	Telnet サーバーの有効/無効を表示します。

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。

#### 4.8.5 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:
```

## 4.9 SSH コマンド

SSH (Secure Shell) 関連の設定コマンドは以下のとおりです。

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}

### 4.9.1 ip ssh server

ip ssh server	
目的	SSH サーバー機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
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	-
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例 : SSH サーバー機能を有効にする方法を示します。

```
# configure terminal
(config)# ip ssh server
```

```
(config)#
```

### 4.9.2 ip ssh service-port

ip ssh service-port	
目的	SSH のサービス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。
シンタックス	<b>ip ssh service-port</b> <i>TCP-PORT</i> <b>no ip ssh service-port</b>
パラメーター	<i>TCP-PORT</i> : SSH プロトコル用のサービスポートとして使用する 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 ポートは 22 です。
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: サービスポート番号を 3000 に変更する方法を示します。

```
# configure terminal
(config)# ip ssh service-port 3000
(config)#
```

### 4.9.3 ip ssh timeout

ip ssh timeout	
目的	SSH 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	<b>ip ssh timeout</b> <i>SECONDS</i> <b>no ip ssh timeout</b>
パラメーター	<i>SECONDS</i> : 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
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)#
```

## 4.9.4 ip ssh authentication-retries

ip ssh authentication-retries	
目的	SSH 認証の再試行回数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>ip ssh authentication-retries</b> <i>NUMBER</i> <b>no ip ssh authentication-retries</b>
パラメーター	<i>NUMBER</i> : SSH 認証の再試行回数を 1~32 の範囲で指定します。すべての試みが失敗した場合はセッションが閉じます。
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	-
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。2 回の再試行に失敗すると、接続は失敗します。

```
# configure terminal
(config)# ip ssh authentication-retries 2
(config)#
```

## 4.9.5 ssh user authentication-method

ssh user authentication-method	
目的	ユーザーアカウントの SSH 認証方式を構成します。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	<b>ssh user</b> <i>NAME</i> <b>authentication-method</b> { <b>password</b>   <b>publickey</b> <i>URL</i>   <b>hostbased</b> <i>URL</i> <b>host-name</b> <i>HOSTNAME</i> [ <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> ]} <b>no ssh user</b> <i>NAME</i> <b>authentication-method</b>
パラメーター	<b>user</b> <i>NAME</i> : 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。 <b>password</b> : 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。 <b>publickey</b> <i>URL</i> : 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。 <b>hostbased</b> <i>URL</i> : 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。 <b>host-name</b> <i>HOSTNAME</i> : 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。 <i>IP-ADDRESS</i> (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。 <i>IPV6-ADDRESS</i> (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



ssh user authentication-method	
	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	<p>管理者がユーザーの認証方法を指定するコマンドです。</p> <p>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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
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 の認証方法を公開鍵に構成する方法を示します。

```
# configure terminal
(config)# ssh user user1 authentication-method publickey c:/user1.pub
(config)#
```

#### 4.9.6 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	<b>show ip ssh</b>
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 構成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。

#### 4.9.7 show ssh

show ssh	
目的	SSH サーバー接続の状態を表示します。
シンタックス	<b>show ssh</b>
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)	セッションの SSH バージョンを表示します。
(3)	SSH クライアントが使用している暗号化アルゴリズムまたは Hashed Message Authentication Code (HMAC) アルゴリズムを表示します。
(4)	セッションのログインユーザー名を表示します。
(5)	確立された SSH セッションのクライアントの IP アドレスを表示します。

#### 4.9.8 show crypto key mypubkey

show crypto key mypubkey	
目的	RSA 公開鍵対、または DSA 公開鍵対を表示します。
シンタックス	<b>show crypto key mypubkey {rsa   dsa}</b>
パラメーター	<b>rsa</b> : RSA 公開鍵を表示する場合に指定します。 <b>dsa</b> : 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

show crypto key mypubkey	
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: 15:16:45, 2017-10-19 ... (1)
Key Size: 768 bits ... (2)
Key Data: ... (3)
AAAAB3Nz aClyc2EA AAADAQAB AAAAYQCW gpe00f18 X6GFLhv2 r5WiBgFV P8xJLmrG
Pf/fuc7i 8CsPlywF 6C+e5AH7 1EZp5QSV o/iqJmY5 emQQe5AV vYE5M3wp jwwBzO+V
qXuloFxA H5yUp4oS lnm+E/iG 4B8ic6E=
```

項番	説明
(1)	RSA 公開鍵が生成された日時を表示します。 <b>restore</b> コマンドを実施して装置を起動しなおした後は、 <b>restore</b> 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 Hn72kln/ D6ftT324 kHfVymGg 4GQ/ICwP
AAAAFQDM cz4dZV/Q Tv/QbTj8 oZTLiRpb FwAAAIEA gSlwH5Jf 8FngnWdg 2lQfXRGW
40MoIO4H h+g6E1MF NdFxruOf QG3++sj0 rcEMsqpw T2lqu5zF K4n5J6tj YD1Ep7fn
2Q+vidj7 A9PFI5KQ xlaASrQA 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。 <b>restore</b> コマンドを実施して装置を起動しなおした後は、 <b>restore</b> 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。

## 4.9.9 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	<code>crypto key generate {rsa [modulus MODULUS-SIZE]   dsa}</code>
パラメーター	<p><code>rsa</code> : RSA 鍵対を生成する場合に指定します。</p> <p><code>modulus MODULUS-SIZE</code> (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。</p> <p><code>dsa</code> : 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。</p>
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	<p>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。</p> <p>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。</p>
制限事項	-
注意事項	<p>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。</p> <p>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。</p>
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.
```

## 4.9.10 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	<code>crypto key zeroize {rsa   dsa}</code>
パラメーター	<p><code>rsa</code> : RSA 鍵対を削除する場合に指定します。</p> <p><code>dsa</code> : DSA 鍵対を削除する場合に指定します。</p>

crypto key zeroize	
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	<p>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。</p> <p>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。</p> <p>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。</p>
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
```

## 4.10 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 INDEX [owner NAME] no rmon collection stats INDEX
rmon collection history	rmon collection history INDEX [owner NAME] [buckets NUM] [interval SECONDS] no rmon collection history INDEX
rmon alarm	rmon alarm INDEX VARIABLE INTERVAL {delta   absolute} rising- threshold VALUE [RISING-EVENT-NUMBER] falling-threshold VALUE [FALLING-EVENT-NUMBER] [owner STRING] no rmon alarm INDEX
rmon event	rmon event INDEX [log] [trap COMMUNITY] [owner NAME] [description TEXT] no rmon event INDEX
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 alarm	show rmon alarm
show rmon events	show rmon events
show rmon history	show rmon history
show rmon statistics	show rmon statistics

### 4.10.1 rmon collection stats

rmon collection stats	
目的	構成対象のインターフェースで、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	<b>rmon collection stats</b> INDEX [owner NAME] <b>no rmon collection stats</b> INDEX
パラメーター	INDEX: 遠隔ネットワーク監視テーブル (RMON 情報) のインデックスを 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。
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 統計情報のエントリー番号は動的です。RMON 統計情報が有効なインターフェースだけ、対応するエントリーがテーブルに存在します。
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、インデックス 65、所有者名「guest」を使用して、RMON 統計情報を設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/2
(config-if-port)# rmon collection stats 65 owner guest
(config-if-port)#
```

#### 4.10.2 rmon collection history

rmon collection history	
目的	構成対象のインターフェースで、RMON 履歴の収集を有効にします。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	<b>rmon collection history</b> <i>INDEX</i> [ <i>owner NAME</i> ] [ <i>buckets NUM</i> ] [ <i>interval SECONDS</i> ] <b>no rmon collection history</b> <i>INDEX</i>
パラメーター	<i>INDEX</i> : RMON 履歴のインデックスを 1～65535 の範囲で指定します。 <i>owner NAME</i> (省略可能) : 所有者名を最大 127 文字で指定します。 <i>buckets NUM</i> (省略可能) : RMON 履歴のパケット数を、1～65535 の範囲で指定します。指定しない場合、デフォルトは 50 です。 <i>interval SECONDS</i> (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。デフォルトは 1800 秒です。
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 履歴のエントリー番号は動的です。RMON 履歴収集が有効なインターフェースだけ、対応するエントリーがテーブルに存在します。構成対象のインターフェースは、作成されるエントリーのデータソースになります。
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 it@domain.com interval 2000
(config-if-port)#
```

#### 4.10.3 rmon alarm

rmon alarm	
目的	インターフェースを監視するためのアラームエントリーを構成します。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	<b>rmon alarm</b> <i>INDEX VARIABLE INTERVAL</i> { <i>delta</i>   <i>absolute</i> } <b>rising-threshold</b> <i>VALUE</i> [ <i>RISING-EVENT-NUMBER</i> ] <b>falling-threshold</b> <i>VALUE</i> [ <i>FALLING-EVENT-NUMBER</i> ] [ <i>owner STRING</i> ] <b>no rmon alarm</b> <i>INDEX</i>
パラメーター	<i>INDEX</i> : アラームエントリーのインデックスを 1～65535 の範囲で指定します。

rmon alarm	
	<p><i>VARIABLE</i>: サンプルングする変数のオブジェクト識別子 (OID) を指定します。</p> <p><i>INTERVAL</i>: 変数をサンプルングし、上限値および下限値に対してチェックを行う間隔 (サンプルング間隔) を 1~2147483647 の範囲で指定します。</p> <p><b>delta</b>: 前回のサンプルング値からの差分値を比較対象にする場合に指定します。</p> <p><b>absolute</b>: サンプルング値をそのまま比較対象にする場合に指定します。</p> <p><b>rising-threshold VALUE</b>: 上限値を 0~2147483647 の範囲で指定します。</p> <p><i>RISING-EVENT-NUMBER</i> (省略可能): 上限値超過時に使用するイベントエントリーのインデックスを、1~65535 の範囲で指定します。指定しない場合、上限値を超えてもアクションは行いません。</p> <p><b>falling-threshold VALUE</b>: 下限値を 0~2147483647 の範囲で指定します。</p> <p><i>FALLING-EVENT-NUMBER</i> (省略可能): 下限値超過時に使用するイベントエントリーのインデックスを、1~65535 の範囲で指定します。指定しない場合、下限値を超えてもアクションは行いません。</p> <p><b>owner STRING</b> (省略可能): 所有者名を最大 127 文字で指定します。</p>
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: インターフェースを監視するアラームエントリーを構成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 1 owner Name
(config)#
```

#### 4.10.4 rmon event

rmon event	
目的	イベントエントリーを構成します。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	<b>rmon event INDEX [log] [trap COMMUNITY] [owner NAME] [description TEXT]</b> <b>no rmon event INDEX</b>
パラメーター	<p><i>INDEX</i>: イベントエントリーのインデックスを 1~65535 の範囲で指定します。</p> <p><b>log</b> (省略可能): 通知のログメッセージを出力する場合に指定します。</p> <p><b>trap COMMUNITY</b> (省略可能): SNMP トラップを送信する場合に、SNMP コミュニティーを最大 127 文字で指定します。</p> <p><b>owner NAME</b> (省略可能): 所有者名を最大 127 文字で指定します。</p> <p><b>description STRING</b> (省略可能): RMON イベントエントリーの説明を、最大 127 文字のテキスト文字列で指定します。</p>



rmon event	
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	<p><b>log</b> を指定して、<b>trap</b> を指定しない場合、イベント発生時に作成されたエントリーから、ログエントリーが出力されます。<b>log</b> を指定せず、<b>trap</b> を指定した場合、イベント発生時に作成されたエントリーから、SNMP トラップが出力されます。</p> <p><b>log</b> と <b>trap</b> の両方のパラメーターを指定した場合、イベント発生時に作成されたエントリーから、ログエントリーと SNMP トラップが出力されます。</p>
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例: インデックス 13 で、イベント発生時にログを出力するようにイベントを構成する方法を示します。

```
# configure terminal
(config)# rmon event 13 log owner it@domain.com description ifInNUcastPkts is too much
(config)#
```

#### 4.10.5 snmp-server enable traps rmon

snmp-server enable traps rmon	
目的	RMON 機能の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<pre>snmp-server enable traps rmon [rising-alarm   falling-alarm] no snmp-server enable traps rmon [rising-alarm   falling-alarm]</pre>
パラメーター	<p><b>rising-alarm</b> (省略可能): 上限値超過通知 (SNMP トラップ) の送信を制御する場合に指定します。</p> <p><b>falling-alarm</b> (省略可能): 下限値超過通知 (SNMP トラップ) の送信を制御する場合に指定します。</p>
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	<p>パラメーターを指定しない場合、両方のパラメーターに対して設定が反映されません。</p> <p>本コマンドを有効にする場合は、<b>snmp-server enable traps</b> コマンドでグローバル設定も有効にしてください。</p>
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)#
```

## 4.10.6 show rmon alarm

show rmon alarm	
目的	アラームエントリーを表示します。
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)	サンプリングする OID を表示します。
(4)	サンプリング間隔を表示します。
(5)	上限値および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)	上限値を表示します。
(8)	上限値超過時に使用するイベントエントリーのインデックスを表示します。
(9)	下限値を表示します。
(10)	下限値超過時に使用するイベントエントリーのインデックスを表示します。
(11)	初めてのサンプリング値により送信される可能性があるアラームを表示します。 On startup enable rising or falling alarm : サンプリング値が上限値または下限値を超過している場合に送信される可能性がある On startup enable rising alarm : 初めてのサンプリング値が上限値を超過している場合に送信される可能性がある On startup enable falling alarm : 初めてのサンプリング値が下限値を超過している場合に送信される可能性がある

## 4.10.7 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
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 1, owned by manager1
  Description is Errors ... (3)
  Event trigger action: log & trap send to community manager ... (4)
  Last triggered time: 21:45:25, 0 ... (5)
  Log: 1 ... (6)
    Log Time: 0d, 21h:45m:25s ... (7)
    Log Description: Errors ... (8)

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap send to community manager
  Last triggered time: 0:0:0, 0
```

項番	説明
(1)	イベントエントリ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)	イベントエントリーの説明を表示します。
(4)	上限値超過時または下限値超過時の動作を表示します。
(5)	最後にイベントが発生した日時を表示します。
(6)	ログのインデックスを表示します。
(7)	イベントが発生した日時を表示します。
(8)	イベントエントリーのメッセージを表示します。

## 4.10.8 show rmon history

show rmon history	
目的	RMON 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	-

show rmon history	
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：RMON 履歴を表示する方法を示します。

```
# show rmon history
(1)      (2)      (3)
Index 1, owned by test, Data source is Port1/0/2
Interval: 30 seconds ... (4)
(5)      (6)
Requested buckets: 50, Granted buckets: 50
Sample 1 ... (7)
(8)      (9)
Received octets: 303595962, Received packets: 357568
(10)     (11)
Broadcast packets: 3289, Multicast packets: 7287
Estimated utilization: 19 ... (12)
(13)     (14)
Undersized packets: 213, Oversized packets: 24
(15)     (16)
Fragments: 2, Jabbers: 1
(17)     (18)
CRC alignment errors: 0, Collisions: 0
Drop events: 0 ... (19)
Sample 2
Received octets: 303596354, Received packets: 357898
Broadcast packets: 3329, Multicast packets: 7337
Estimated utilization: 19
Undersized packets: 213, Oversized packets: 24
Fragments: 2, Jabbers: 2
CRC alignment errors: 0, Collisions: 0
Drop events: 0
```

項番	説明
(1)	RMON 履歴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)	RMON 履歴を蓄積するインターフェース ID を表示します。
(4)	サンプリング間隔を表示します。
(5)	要求されたパケット数を表示します。
(6)	提供されたパケット数を表示します。
(7)	パケット番号を表示します。
(8)	受信したオクテット数を表示します。
(9)	受信したパケット数を表示します。
(10)	ブロードキャストパケット数を表示します。
(11)	マルチキャストパケット数を表示します。
(12)	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。
(13)	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。
(14)	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。
(15)	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。
(16)	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)

項番	説明
	エラーを伴うパケット数を表示します。
(17)	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。
(18)	コリジョンの推定値を表示します。
(19)	リソース不足のために廃棄されたイベントの数 (イベントの廃棄が検出された回数) を表示します。

#### 4.10.9 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	<b>show rmon statistics</b>
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 , Data source is Port1/0/1
(4)      (5)
Received octets: 0, Received packets: 0
(6)      (7)
Broadcast packets: 0, Multicast packets: 0
(8)      (9)
Undersized packets: 0, Oversized packets: 0
(10)     (11)
Fragments: 0, Jabbers: 0
(12)     (13)
CRC alignment errors: 0, Collisions: 0
Drop events: 0 ... (14)
(15)
Packets in 64 octets: 0, Packets in 65-127 octets: 0
Packets in 128-255 octets: 0, Packets in 256-511 octets: 0
Packets in 512-1023 octets: 0, Packets in 1024-1518 octets: 0

```

項番	説明
(1)	RMON 統計情報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)	RMON 統計情報を蓄積するインターフェース ID を表示します。
(4)	受信したオクテット数を表示します。
(5)	受信した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。

項番	説明
(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数 (イベントの廃棄が検出された回数) 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 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]

### 4.11.1 sflow receiver

sflow receiver	
目的	sFlow エージェントのレシーバーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
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	<p>INDEX: レシーバーID を 1~4 の範囲で指定します。</p> <p>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。ユーザーは所有者名に空の文字列を指定できません。</p> <p>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 <b>infinite</b> が設定されます。</p> <ul style="list-style-type: none"> <li>SECONDS: 有効期限を 1~2,000,000 秒の範囲で指定します。</li> <li>infinite: 有効期限を無期限にする場合に指定します。</li> </ul> <p>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。</p> <p>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。</p> <p>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。</p>
デフォルト	<p>レシーバーは未設定</p> <p>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:</p> <ul style="list-style-type: none"> <li>所有者名: 空の文字列</li> <li>有効期限: <b>infinite</b></li> <li>sFlow データグラムの最大サイズ: 1400 バイト</li> <li>sFlow コレクターの IPv4 アドレス: 0.0.0.0</li> <li>UDP ポート番号: 6343</li> </ul>

sflow receiver	
コマンドモード	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	<p>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。</p> <p>有効期限を <b>infinite</b> 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。</p> <p>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。</p> <p>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。</p>
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 86400 秒、sFlow コレクターの IP アドレスを 10.1.1.2 でレシーバーを設定する方法を示します。

```
# configure terminal
(config)# sflow receiver 1 owner collector1 expiry 86400 host 10.1.1.2
(config)#
```

#### 4.11.2 sflow sampler

sflow sampler	
目的	sFlow エージェントのサンプラーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<pre>sflow sampler INSTANCE [receiver RECEIVER] [inbound   outbound] [sampling-rate RATE] [max-header-size SIZE] no sflow sampler INSTANCE</pre>
パラメーター	<p><b>INSTANCE</b> : 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。</p> <p><b>receiver RECEIVER</b> (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。</p> <p>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 <b>inbound</b> が設定されます。</p> <ul style="list-style-type: none"> <li><b>inbound</b> : 受信パケットをサンプリング対象にする。</li> <li><b>outbound</b> : 送信パケットをサンプリング対象にする。</li> </ul> <p><b>sampling-rate RATE</b> (省略可能) : パケットのサンプリングレートを 0~65536 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)</p> <p><b>max-header-size SIZE</b> (省略可能) : サンプリングしたパケットからコピーする</p>



sflow sampler	
	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	<p>サンプラーは未設定</p> <p>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：</p> <ul style="list-style-type: none"> <li>• レシーバーID : 0</li> <li>• サンプリング対象 : <b>inbound</b></li> <li>• サンプリングレート : 0</li> <li>• コピーするデータの最大バイト数 : 128</li> </ul>
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	<p>実際のサンプリングレートは「設定値×256」で動作します。</p> <p>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)</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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, …)</p>
制限事項	<p>未設定のレシーバーID を指定して設定できません。</p> <p>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。</p>
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)#
```

## 4.11.3 sflow poller

sflow poller	
目的	sFlow エージェントのポーラーを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>sflow poller</b> <i>INSTANCE</i> [ <b>receiver</b> <i>RECEIVER</i> ] [ <b>interval</b> <i>SECONDS</i> ] <b>no sflow poller</b> <i>INSTANCE</i>
パラメーター	<i>INSTANCE</i> : ポーラーのインスタンス ID を 1~65535 の範囲で指定します。  <b>receiver</b> <i>RECEIVER</i> (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。  <b>interval</b> <i>SECONDS</i> (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 : <ul style="list-style-type: none"> <li>レシーバーID : 0</li> <li>ポーリング間隔 : 0 秒</li> </ul>
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)#
```

## 4.11.4 show sflow

show sflow	
目的	sFlow 情報を表示します。
シンタックス	<b>show sflow</b> [ <b>agent</b>   <b>receiver</b>   <b>sampler</b>   <b>poller</b> ]
パラメーター	<b>agent</b> (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。  <b>receiver</b> (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	
	<b>sampler</b> (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。 <b>poller</b> (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中の最小 VLAN ID の VLAN インターフェースの IPv4 アドレスが sFlow Agent Address として設定されます。  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 として設定されます。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) Interface	(2) Instance	(3) Receiver	(4) Interval
Port1/0/1	1	1	60
Port1/0/5	105	1	60

項番	説明
(1)	ポーラーを設定したポート番号を表示します。
(2)	ポーラーのインデックスを表示します。
(3)	ポーラー用のレシーバーのインデックスを表示します。
(4)	ポーリング間隔を表示します。

## 4.12 SNMP コマンド

SNMP (Simple Network Management Protocol) 関連の設定コマンドは以下のとおりです。

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 NAME no snmp-server name
snmp-server location	snmp-server location TEXT no snmp-server location
snmp-server contact	snmp-server contact TEXT 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] no snmp-server enable traps environment [fan   power   temperature]
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

#### 4.12.1 snmp-server

snmp-server	
目的	SNMP エージェントを有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>snmp-server</b> <b>no snmp-server</b>
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 要求を SNMP エージェントに送信して、SNMP エージェントから SNMP 応答と通知を受信することで、SNMP エージェントを管理します。SNMP エージェントが管理可能になる前に、SNMP エージェント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：SNMP エージェントを有効にする方法を示します。

```
# configure terminal
(config)# snmp-server
(config)#
```

#### 4.12.2 snmp-server name

snmp-server name	
目的	システム名情報を構成します。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	<b>snmp-server name</b> <i>NAME</i> <b>no snmp-server name</b>
パラメーター	<i>NAME</i> ：SNMP エージェント名情報（装置名など）を記述した文字列を、最大 64 文字で指定します。エージェント名には、文字、数字、およびハイフンを使用できます。ただし、エージェント名の先頭と末尾は文字、または数字にしてください。
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	<i>NAME</i> の文字列は、コマンド "prompt %h" のプロンプト結果に影響します。15 文字を超えた場合、プロンプトの最大表示範囲を超えますのでコマンド "prompt %h" と一緒に使用する場合は、 <i>NAME</i> の文字列を 15 文字以下にしてください。
制限事項	-
注意事項	エージェント名の先頭に数字を指定できるのは AEOS-NP4000 Ver. 1.02.01 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 1.02.01：設定可能文字列の仕様変更

使用例：システム名を「SiteA-switch」に構成する方法を示します。

```
# configure terminal
(config)# snmp-server name SiteA-switch
(config)#
```

#### 4.12.3 snmp-server location

snmp-server location	
目的	システムロケーション情報を構成します。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	<b>snmp-server location</b> <i>TEXT</i> <b>no snmp-server location</b>
パラメーター	<b>location</b> <i>TEXT</i> ：システムロケーション情報（設置場所など）を記述した文字列を、最大 255 文字で指定します。シンタックスは一般的な文字列です。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	-

snmp-server location	
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情報を文字列「HQ 15F」で構成する方法を示します。

```
# configure terminal
(config)# snmp-server location HQ 15F
(config)#
```

#### 4.12.4 snmp-server contact

snmp-server contact	
目的	装置のシステムコンタクト情報を構成します。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	<b>snmp-server contact</b> <i>TEXT</i> <b>no snmp-server contact</b>
パラメーター	<b>contact</b> <i>TEXT</i> ：システムコンタクト情報（連絡先など）を記述する文字列を、最大 255 文字で指定します。シンタックスは一般的な文字列です。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情報を文字列「MIS Department II」で構成する方法を示します。

```
# configure terminal
(config)# snmp-server contact MIS Department II
(config)#
```

#### 4.12.5 snmp-server service-port

snmp-server service-port	
目的	SNMP UDP ポート番号を構成します。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	<b>snmp-server service-port</b> <i>PORT-NUMBER</i> <b>no snmp-server service-port</b>
パラメーター	<i>PORT-NUMBER</i> ：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	エージェントは、構成されたサービス UDP ポート番号の SNMP 要求パケットをリッスンします。
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 UDP ポート番号を構成する方法を示します。

```
# configure terminal
(config)# snmp-server service-port 50000
(config)#
```

#### 4.12.6 snmp-server response broadcast-request

snmp-server response broadcast-request	
目的	ブロードキャスト SNMP GetRequest パケットに対するサーバーの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	<b>snmp-server response broadcast-request</b> <b>no snmp-server response broadcast-request</b>
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、ネットワーク装置を検知するためにブロードキャスト SNMP GetRequest パケットを送信します。NMS ツールがネットワーク装置を検知するためにブロードキャスト SNMP GetRequest パケットを送信する機能をサポートするには、ブロードキャスト GetRequest パケットへの応答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：ブロードキャスト SNMP GetRequest パケットに対するサーバーの応答を有効にする方法を示します。

```
# configure terminal
(config)# snmp-server response broadcast-request
(config)#
```

#### 4.12.7 snmp-server community

snmp-server community	
目的	SNMP にアクセスするためのコミュニティ名を設定します。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	<b>snmp-server community</b> [0   7] <i>COMMUNITY-STRING</i> [ <b>view</b> <i>VIEW-NAME</i> ] [ <b>ro</b>   <b>rw</b> ] [ <b>access</b> <i>IP-ACL-NAME</i> ] <b>no snmp-server community</b> [0   7] <i>COMMUNITY-STRING</i>
パラメーター	0 (省略可能)：SNMP コミュニティ名を平文で入力する場合に指定します。SNMP コミュニティ名のデフォルト設定です。  7 (省略可能)：SNMP コミュニティ名を暗号化した形式で入力する場合に指定します。  <i>COMMUNITY-STRING</i> ：平文で入力する場合は、文字列を最大 32 文字で指定します。文字列には、スペースを含めることができます。暗号化した形式で入力する場合は、文字列を 67 文字で指定します。いずれの場合も、大文字と小文字が区別されます。

snmp-server community	
	<p><b>view</b> <i>VIEW-NAME</i> (省略可能) : SNMP コミュニティーからアクセス可能な SNMP ビュー名を指定します。</p> <p><b>ro</b> (省略可能) : MIB へのアクセス権を read-only に設定する場合に指定します。</p> <p><b>rw</b> (省略可能) : MIB へのアクセス権を read-write に設定する場合に指定します。</p> <p><b>access</b> <i>IP-ACL-NAME</i> (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。</p>
デフォルト	<p>private (CommunityView, Read/Write)</p> <p>public (CommunityView, Read Only)</p> <p>※コミュニティー名 (SNMP ビュー名, アクセス権)</p>
コマンドモード	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	<p>SNMPv1 または SNMPv2c の管理に必要なコミュニティー名を設定する簡単な方法を提供します。</p> <p>本コマンドでコミュニティー名を設定すると、2 つの <b>snmp-server group</b> 設定が自動的に作成されます。それぞれ SNMPv1 と SNMPv2c に対応し、コミュニティー名がグループ名になります。</p> <p><b>view</b> パラメーターを指定しない場合、デフォルトで設定されている CommunityView が適用されます。</p> <p><b>ro</b> もしくは <b>rw</b> パラメーターを指定しない場合、<b>ro</b> パラメーターが適用されます。<b>ro</b> パラメーターを指定した場合、指定した <b>view</b> パラメーター (未指定時は CommunityView) が、自動的に作成される <b>snmp-server group</b> 設定の read-view, notify-view に反映されます。<b>rw</b> パラメーターを指定した場合、指定した <b>view</b> パラメーター (未指定時は CommunityView) が、自動的に作成される <b>snmp-server group</b> 設定の read-view, write-view, notify-view に反映されます。</p> <p><b>access</b> 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。</p> <p><b>access</b> パラメーターを指定した場合、対応する 2 つの <b>snmp-server group</b> 設定にも反映されます。</p> <p><b>no snmp-server community</b> コマンドで設定を削除すると、対応する 2 つの <b>snmp-server group</b> 設定も削除されます。</p> <p>SNMP コミュニティー名は、暗号化形式または平文で指定します。平文で指定した場合、サービスパスワード暗号化機能を有効化すると、SNMP コミュニティー名が暗号化されます。</p>
制限事項	<b>snmp-server community</b> コマンドを設定した場合に自動的に作成される 2 つの <b>snmp-server group</b> 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	<b>snmp-server community</b> コマンドを設定した場合には SNMPv1 と SNMPv2c の両方の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。

snmp-server community	
	本設定の <b>access</b> 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」を作成して、interfacesMibView に read-write アクセスができるコミュニティ名「comaccess」を作成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)#
```

#### 4.12.8 snmp-server host

snmp-server host	
目的	SNMP トラップの受信者を指定します。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	<b>snmp-server host</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> } [ <b>version</b> { <b>1</b>   <b>2c</b>   <b>3</b> { <b>auth</b>   <b>noauth</b>   <b>priv</b> }}] [ <b>0</b>   <b>7</b> ] <i>COMMUNITY-STRING</i> [ <b>port</b> <i>PORT-NUMBER</i> ] <b>no snmp-server host</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> }
パラメーター	<p><i>IP-ADDRESS</i> : SNMP トラップの宛先ホストの IPv4 アドレスを指定します。</p> <p><i>IPV6-ADDRESS</i> : SNMP トラップの宛先ホストの IPv6 アドレスを指定します。</p> <p><b>version</b> (省略可能) : SNMP トラップの送信に使用する SNMP のバージョンを指定します。指定しない場合のデフォルトは、SNMPv1 です。</p> <ul style="list-style-type: none"> <li>• <b>1</b> : SNMP のバージョンを SNMPv1 に設定する場合に指定します。</li> <li>• <b>2c</b> : SNMP のバージョンを SNMPv2c に設定する場合に指定します。</li> <li>• <b>3</b> : SNMP のバージョンを SNMPv3 に設定する場合に指定します。</li> </ul> <p><b>auth</b> : パケットを認証し、暗号化しない場合に指定します。</p> <p><b>noauth</b> : パケットを認証せず、暗号化しない場合に指定します。</p> <p><b>priv</b> : パケットを認証し、暗号化する場合に指定します。</p> <p><b>0</b> (省略可能) : SNMP コミュニティ名を平文で入力する場合に指定します。SNMP コミュニティ名のデフォルト設定です。</p> <p><b>7</b> (省略可能) : SNMP コミュニティ名を暗号化した形式で入力する場合に指定します。</p> <p><i>COMMUNITY-STRING</i> : 通知パケットで送信する SNMP コミュニティ名を指定します。SNMP のバージョンが SNMPv3 の場合、コミュニティ名は <b>snmp-server user</b> コマンドで定義されたユーザー名として使用されます。平文で入力する場合は、文字列を最大 32 文字で指定します。文字列には、スペースを含めることができます。暗号化した形式で入力する場合は、文字列を 67 文字で指定します。いずれの場合も、大文字と小文字が区別されます。</p> <p><b>port</b> <i>PORT-NUMBER</i> (省略可能) : UDP ポート番号を 1~65535 の範囲で指定します。デフォルトの SNMP トラップ UDP ポート番号は、162 です。指定するポート番号によっては、他のプロトコルと競合する場合があります。</p>
デフォルト	ホストエントリー : なし、SNMP のバージョン : 1
コマンドモード	グローバル設定モード

snmp-server host	
特権レベル	レベル : 12
ガイドライン	<p>SNMP トラップは、SNMP トラップパケットとして送信されます。ユーザーは、装置が SNMP トラップを送信できるように、<b>snmp-server host</b> コマンドを使用して SNMP トラップの受信者を 1 件以上作成してください。</p> <p>作成したユーザーへの通知パケットのバージョンを指定します。SNMPv1 および SNMPv2c の場合、通知は SNMP トラップフレームで送信されます。SNMPv3 の場合、通知は SNMPv3 ヘッダー付きの SNMPv2 トラップフレームで送信されます。</p> <p>SNMPv1 および SNMPv2c で特定のホストに SNMP トラップパケットを送信するように指定する場合、指定したコミュニティ名は、SNMP トラップパケットでコミュニティ名として機能します。</p> <p>SNMPv3 で特定のホストに SNMP トラップパケットを送信するように指定する場合、パケットの送信で認証と暗号化を行うかどうかを指定します。指定したコミュニティ名は、SNMPv3 パケットのユーザー名として機能します。<b>snmp-server user v3</b> を使用して、最初にユーザーを作成してください。</p> <p>SNMP トラップパケットの送信では、指定したユーザー、またはコミュニティ名と関連付けられた notify-view をシステムがチェックします。</p>
制限事項	SNMP トラップパケットと共に送信されるバインディング変数が notify-view に存在しない場合、通知は指定したホストに送信されません。
注意事項	-
対象バージョン	1.01.01

使用例：SNMP トラップ受信者 163.10.50.126 を、SNMPv1 認証セキュリティレベルで、コミュニティ名を「comaccess」にして設定する方法を示します。

```
# configure terminal
(config)# snmp-server community comaccess rw
(config)# snmp-server host 163.10.50.126 version 1 comaccess
(config)#
```

使用例：SNMP トラップ受信者 163.10.50.126 を、SNMPv3 認証セキュリティレベルで、ユーザー名を「useraccess」にして設定する方法を示します。また、UDP ポート番号を 50001 に構成します。

```
# configure terminal
(config)# snmp-server group groupaccess v3 auth read CommunityView write CommunityView
(config)# snmp-server user useraccess groupaccess v3 auth md5 12345678
(config)# snmp-server host 163.10.50.126 version 3 auth useraccess port 50001
(config)#
```

#### 4.12.9 snmp-server enable traps

snmp-server enable traps	
目的	SNMP トラップパケットの送信をグローバルに有効にします。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	<b>snmp-server enable traps</b> <b>no snmp-server enable traps</b>
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

snmp-server enable traps	
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送信状態を有効にする方法を示します。

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

#### 4.12.10 snmp-server enable traps snmp

snmp-server enable traps snmp	
目的	SNMP 標準トラップの送信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>snmp-server enable traps snmp</b> [authentication   linkup   linkdown   coldstart   warmstart] <b>no snmp-server enable traps snmp</b> [authentication   linkup   linkdown   coldstart   warmstart]
パラメーター	<p><b>authentication</b> (省略可能)：SNMP 認証失敗通知の送信を制御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コミュニティ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。</p> <p><b>linkup</b> (省略可能)：リンクアップ通知の送信を制御する場合に指定します。いずれかの通信リンクが確立したことを装置が認識すると、リンクアップ通知が出力されます。</p> <p><b>linkdown</b> (省略可能)：リンクダウン通知の送信を制御する場合に指定します。いずれかの通信リンクが失敗したことを装置が認識すると、リンクダウン通知が出力されます。</p> <p><b>coldstart</b> (省略可能)：コールドスタート通知の送信を制御する場合に指定します。</p> <p><b>warmstart</b> (省略可能)：ウォームスタート通知の送信を制御する場合に指定します。</p>
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	<p>パラメーターを指定しない場合、すべてのパラメーターに対して設定が反映されます。</p> <p>本コマンドを有効にする場合は、<b>snmp-server enable traps</b> コマンドでグローバル設定も有効にしてください。</p>
制限事項	-
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し、コミュニティ名「public」で 10.9.18.100 宛てに送信するように設定する方法を示します。

```
# configure terminal
(config)# snmp-server enable traps
(config)# snmp-server enable traps snmp
(config)# snmp-server host 10.9.18.100 version 2c public
(config)#
```

使用例：SNMP 認証失敗通知を有効にする方法を示します。

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

#### 4.12.11 snmp-server enable traps environment

snmp-server enable traps environment	
目的	環境モニタリング通知の SNMP トラップを有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>snmp-server enable traps environment [fan] [power] [temperature]</b> <b>no snmp-server enable traps environment [fan   power   temperature]</b>
パラメーター	<b>fan</b> (省略可能)：ファン関連の通知 (SNMP トラップ) の送信を制御する場合に指定します。 <b>power</b> (省略可能)：電源関連の通知 (SNMP トラップ) の送信を制御する場合に指定します。 <b>temperature</b> (省略可能)：温度関連の通知 (SNMP トラップ) の送信を制御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	<b>fan</b> パラメーター、 <b>power</b> パラメーター、 <b>temperature</b> パラメーターのいずれも指定しない場合は、すべての環境モニタリング通知の SNMP トラップが制御されます。 本コマンドを有効にする場合は、 <b>snmp-server enable traps</b> 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：環境モニタリング通知の SNMP トラップを有効にする方法を示します。

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

#### 4.12.12 snmp-server source-interface traps

snmp-server source-interface traps	
目的	SNMP トラップパケットの送信元アドレスとして使用される IP アドレスが指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。



snmp-server source-interface traps	
シンタックス	<b>snmp-server source-interface traps</b> <i>INTERFACE-ID</i> <b>no snmp-server source-interface traps</b>
パラメーター	<i>INTERFACE-ID</i> : SNMP トラップパケットの送信元アドレスとして使用される IP アドレスが指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。 <ul style="list-style-type: none"> <li>• <b>vlan</b>: VLAN インターフェースを指定します。</li> <li>• <b>mgmt</b>: マネージメントポートを指定します。</li> </ul>
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、 <b>vlan</b> 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、 <b>mgmt</b> 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: VLAN 100 インターフェースを SNMP トラップパケットの送信元インターフェースとして構成する方法を示します。

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

#### 4.12.13 snmp-server trap-sending disable

snmp-server trap-sending disable	
目的	設定したポートからの自装置の SNMP トラップ送信を禁止します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>snmp-server trap-sending disable</b> <b>no snmp-server trap-sending disable</b>
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 ( <b>no snmp-server trap-sending disable</b> )
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	-
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)#
```

## 4.12.14 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	<b>snmp trap link-status</b> <b>no snmp trap link-status</b>
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 ( <b>snmp trap link-status</b> )
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したい場合に、 <b>no snmp trap link-status</b> コマンドを実施してください。
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、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)#
```

## 4.12.15 snmp-server user

snmp-server user	
目的	SNMP ユーザーを作成します。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	<b>snmp-server user USER-NAME [0   7] GROUP-NAME v3 [encrypted] [auth {md5   sha} AUTH-PASSWORD [priv PRIV-PASSWORD]] [access IP-ACL-NAME]</b> <b>no snmp-server user USER-NAME [0   7] GROUP-NAME v3</b>
パラメーター	<p><b>USER-NAME</b> : ユーザー名を最大 32 文字で指定します。シンタックスは一般的な文字列です。スペースは使用できません。</p> <p><b>0</b> (省略可能) : ユーザーが所属するグループ名を平文で入力する場合に指定します。</p> <p><b>7</b> (省略可能) : ユーザーが所属するグループ名を暗号化した形式で入力する場合に指定します。</p> <p><b>GROUP-NAME</b> : ユーザーが所属するグループ名を指定します。シンタックスは一般的な文字列です。スペースは使用できません。平文で入力する場合は、文字列を最大 32 文字で指定します。文字列には、スペースを含めることができます。暗号化した形式で入力する場合は、文字列を 67 文字で指定します。いずれの場合も、大文字と小文字が区別されます。</p> <p><b>v3</b> : SNMPv3 セキュリティモードを使用するユーザーを作成する場合に指定します。</p> <p><b>encrypted</b> (省略可能) : パスワードを暗号化形式で入力する場合に指定します。</p> <p><b>auth md5</b> (省略可能) : HMAC-MD5-96 認証を使用する場合に指定します。</p>

snmp-server user	
	<p><b>auth sha</b> (省略可能) : HMAC-SHA-96 認証を使用する場合に指定します。</p> <p><i>AUTH-PASSWORD</i> : 認証に使用するパスワードを指定します。HMAC-MD5-96 認証を使用する場合のパスワードは、8~16 文字の範囲の平文で指定します。HMAC-SHA-96 認証を使用する場合のパスワードは、8~20 文字の範囲の平文で指定します。シンタックスは一般的な文字列です。スペースは使用できません。指定したアルゴリズムに基づいて認証鍵が出力されます。<b>encrypted</b> パラメーターを指定した場合、MD5 パスワードを 16 オクテット、または SHA パスワードを 20 オクテットで指定します。形式は 16 進値です。</p> <p><b>priv PRIV-PASSWORD</b> (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。シンタックスは一般的な文字列です。スペースは使用できません。パスワードに基づいて秘密鍵が出力されます。<b>encrypted</b> パラメーターを指定した場合、秘密鍵を 16 オクテットで指定します。形式は 16 進値です。パケット暗号化方式は DES (Data Encryption Standard) のみ使用可能です。</p> <p><b>access IP-ACL-NAME</b> (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。</p>
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	<p>パスワードは平文、ローカライズした MD5 形式、または SHA 形式のいずれかで指定できます。</p> <p>16 進値として以下の英数字を指定できます。</p> <ul style="list-style-type: none"> <li>• 数字 (0~9) 、大文字 (A~F) 、小文字 (a~f)</li> </ul> <p><b>access</b> 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。</p>
制限事項	<p>SNMP エージェントのホストに関連付けられている SNMP ユーザーは、削除できません。</p> <p><b>snmp-server user</b> 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。</p>
注意事項	<p>パスワードを紛失した場合、紛失したパスワードはユーザーを再設定しても復旧できません。</p> <p>本設定の <b>access</b> 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。</p>
対象バージョン	1.01.01

使用例 : SNMPv3 グループ public のユーザー「user1」に対して、平文パスワードを構成する方法を示します。

```
# configure terminal
(config)# snmp-server user user1 public v3 auth md5 authpassword priv privpassword
(config)#
```

使用例：平文パスワードの代わりに、MD5 ダイジェスト文字列を使用する方法を示します。

```
# configure terminal
(config)# snmp-server user user1 public v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
(config)#
```

#### 4.12.16 snmp-server group

snmp-server group	
目的	SNMP グループを構成します。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	<pre>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}}</pre>
パラメーター	<p><b>0</b> (省略可能)：グループ名を平文で入力する場合に指定します。グループ名のデフォルト設定です。</p> <p><b>7</b> (省略可能)：グループ名を暗号化した形式で入力する場合に指定します。</p> <p><i>GROUP-NAME</i>：平文で入力する場合は、文字列を最大 32 文字で指定します。文字列には、スペースを含めることができます。暗号化した形式で入力する場合は、文字列を 67 文字で指定します。いずれの場合も、大文字と小文字が区別されません。</p> <p><b>v1</b>：SNMPv1 セキュリティーモデルを使用する場合に指定します。</p> <p><b>v2c</b>：SNMPv2c セキュリティーモデルを使用する場合に指定します。</p> <p><b>v3</b>：SNMPv3 セキュリティーモデルを使用する場合に指定します。</p> <p><b>auth</b>：パケットを認証し、暗号化しない場合に指定します。</p> <p><b>noauth</b>：パケットを認証せず、暗号化もしない場合に指定します。</p> <p><b>priv</b>：パケットを認証し、暗号化する場合に指定します。</p> <p><b>read READ-VIEW</b> (省略可能)：グループのユーザーに読み取りを許可する read-view を指定します。</p> <p><b>write WRITE-VIEW</b> (省略可能)：グループのユーザーに書き込みを許可する write-view を指定します。</p> <p><b>notify NOTIFY-VIEW</b> (省略可能)：グループのユーザーに SNMP トラップの送信を許可する notify-view を指定します。</p> <p><b>access IP-ACL-NAME</b> (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。</p>
デフォルト	<pre>initial (SNMPv3/noauth/restricted/None/restricted) public (SNMPv1/noauth/CommunityView/None/CommunityView) public (SNMPv2c/noauth/CommunityView/None/CommunityView) private (SNMPv1/noauth/CommunityView/CommunityView/CommunityView) private (SNMPv2c/noauth/CommunityView/CommunityView/CommunityView) ※グループ名 (バージョン/セキュリティーレベル/Read View 名/Write View 名 /Notify View 名)</pre>
コマンドモード	グローバル設定モード

snmp-server group	
特権レベル	レベル : 12
ガイドライン	<p>SNMP グループは、許可されたセキュリティーモデル、read-view、write-view、notify-view を指定することで、ユーザーグループを定義します。</p> <p>セキュリティーモデルは、指定されたバージョンの SNMP を使用した SNMP エージェントへのアクセスに関する、グループユーザーへの許可の内容を定義します。</p> <p>セキュリティーモデル SNMPv1、SNMPv2c、SNMPv3 に対して、同じセキュリティーグループ名を同時に作成できます。SNMPv3 の場合、SNMPv3 Auth と SNMPv3 Priv に対して、同じグループ名を同時に作成できます。</p> <p>特定のセキュリティーモデルでアクセスしないようにグループを削除する場合は、<b>no snmp-server group</b> コマンドを使用します。</p> <p>特定のセキュリティーモードに対してグループの SNMP ビュープロファイルを更新する場合は、グループを削除して、新しい SNMP ビュープロファイルを持つグループを作成します。</p> <p>read-view は、グループユーザーが読み取りを許可される MIB オブジェクトを定義します。</p> <p>write-view は、グループユーザーが書き込みを許可される MIB オブジェクトを定義します。write-view を指定しない場合、すべての MIB オブジェクトに書き込みができません。</p> <p>notify-view は、システムが SNMP トラップマネージャーへの通知パケットの状態を報告できる、MIB オブジェクトを定義します。SNMP トラップマネージャーは、指定されたグループユーザー（コミュニティ名として機能）によって識別されます。notify-view を定義しない場合、すべての MIB オブジェクトを報告できません。</p>
制限事項	<b>snmp-server community</b> 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 グループエントリ設定を、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 <b>access</b> 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 : SNMPv3 アクセス、および SNMPv2c に対して、SNMP エージェントグループ「guestgroup」を作成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 group guestgroup v3 auth read interfacesMibView
(config)# snmp-server group guestgroup v2c read CommunityView write CommunityView
(config)#
```

#### 4.12.17 snmp-server view

snmp-server view	
目的	SNMP ビューを作成または変更します。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	<b>snmp-server view</b> <i>VIEW-NAME</i> <i>OID-TREE</i> {included   excluded} <b>no snmp-server view</b> <i>VIEW-NAME</i>

snmp-server view	
パラメーター	<p><b>VIEW-NAME</b>: 変更または作成する SNMP ビュー名を、1~32 文字の範囲で指定します。シンタックスは一般的な文字列です。スペースは使用できません。</p> <p><b>OID-TREE</b>: 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。OID ツリーを識別するために、「1.3.6.2.4」といった数字を指定します。</p> <p><b>included</b>: 指定した OID ツリーを SNMP ビューに含める場合に指定します。</p> <p><b>excluded</b>: 指定した OID ツリーを SNMP ビューから除外する場合に指定します。</p>
デフォルト	<p>restricted (1.3.6.1.2.1.1/included)</p> <p>restricted (1.3.6.1.2.1.11/included)</p> <p>restricted (1.3.6.1.6.3.10.2.1/included)</p> <p>restricted (1.3.6.1.6.3.11.2.1/included)</p> <p>restricted (1.3.6.1.6.3.15.1.1/included)</p> <p>CommunityView (1/included)</p> <p>CommunityView (1.3.6.1.6.3/excluded)</p> <p>CommunityView (1.3.6.1.6.3.1/included)</p> <p>※VIEW-NAME (OID-TREE/SNMP ビュータイプ)</p>
コマンドモード	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	MIB オブジェクトの SNMP ビューを作成するコマンドです。作成した SNMP ビューは、 <b>snmp-server group</b> と <b>snmp-server community</b> 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: 「interfacesMibView」という SNMP ビューを作成して、interfacesMibView を read view として含む SNMP グループ「guestgroup」を定義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 group guestgroup v3 auth read interfacesMibView
(config)#
```

#### 4.12.18 snmp-server engineID local

snmp-server engineID local	
目的	ローカル装置上の SNMP エンジン ID 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	<p><b>snmp-server engineID local ENGINEID-STRING</b></p> <p><b>no snmp-server engineID local</b></p>
パラメーター	<b>ENGINEID-STRING</b> : 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	SNMP エンジン ID は、装置を識別する一意の 16 進数です。16 進数はデフォルトで出力されます。24 文字より少ない 16 進数を指定すると、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	-
対象バージョン	1.01.01

使用例：SNMP エンジン ID を 800001160501020304050607 に構成する方法を示します。

```
# configure terminal
(config)# snmp-server engineID local 800001160501020304050607
(config)#
```

#### 4.12.19 show snmp-server

show snmp-server	
目的	SNMP エージェントの設定を表示します。
シンタックス	<b>show snmp-server</b>
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)	装置名などを表示します。
(3)	装置の設置場所情報などを表示します。
(4)	装置障害発生時の連絡先情報などを表示します。
(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での SNMP GetRequest に対する応答設定を表示します。

#### 4.12.20 show snmp community

show snmp community	
目的	SNMP コミュニティ名を表示します。
シンタックス	<b>show snmp community</b>
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

show snmp community	
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 コミュニティーからアクセス可能な SNMP ビュー名を表示します。

#### 4.12.21 show snmp host

show snmp host	
目的	SNMP トラップの宛先ホストを表示します。
シンタックス	<b>show snmp host</b>
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 : 10.20.30.40 ... (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: 1:12:123::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 IP 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。

#### 4.12.22 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	<b>show snmp-server traps</b>
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 トラップ関連設定を表示する方法を示します。

# show snmp-server traps
Global Trap State : Disabled ... (1)
Individual Trap State:
Authentication : Disabled ... (2)
Linkup : Disabled ... (3)
Linkdown : Disabled ... (4)
Coldstart : Disabled ... (5)
Warmstart : Disabled ... (6)

項番	説明
(1)	装置からの SNMP トラップの送信設定を表示します。
(2)	SNMP 認証失敗通知の送信設定を表示します。
(3)	リンクアップ通知の送信設定を表示します。

項番	説明
(4)	リンクダウン通知の送信設定を表示します。
(5)	コールドスタート通知の送信設定を表示します。
(6)	ウォームスタート通知の送信設定を表示します。

### 4.12.23 show snmp-server trap-sending

show snmp-server trap-sending	
目的	自装置の SNMP トラップの送信可能ポートまたは送信禁止ポートを表示します。
シンタックス	<b>show snmp-server trap-sending</b> [ <b>interface</b> <i>INTERFACE-ID</i> [, -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースの SNMP トラップの送信可否が表示されます。
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

### 4.12.24 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	<b>show snmp trap link-status</b> [ <b>interface</b> <i>INTERFACE-ID</i> [, -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (省略可能) : ポートのリンクアップ通知およびリンク

show snmp trap link-status	
	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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェース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 : 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)

#### 4.12.25 show snmp user

show snmp user	
目的	構成済みの SNMP ユーザーに関する情報を表示します。
シンタックス	<b>show snmp user</b> [ <i>USER-NAME</i> ]
パラメーター	<i>USER-NAME</i> (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	<b>snmp-server community</b> コマンドで作成したコミュニティ名は、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。

#### 4.12.26 show snmp group

show snmp group	
目的	SNMP グループ設定を表示します。
シンタックス	<b>show snmp group</b>
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 グループ設定を表示する方法を示します。

```
# show snmp group

GroupName: public ... (1)
SecurityModel: v1 ... (2)
(3) ReadView : CommunityView WriteView : (4)
NotifyView : CommunityView ... (5)
```

```

IP access control list: ... (6)

GroupName: public
SecurityModel: v2c
  ReadView      : CommunityView          WriteView      :
  NotifyView    : CommunityView
  IP access control list:

GroupName: initial
SecurityModel: v3/noauth
  ReadView      : restricted              WriteView      :
  NotifyView    : restricted
  IP access control list:

GroupName: private
SecurityModel: v1
  ReadView      : CommunityView          WriteView      : CommunityView
  NotifyView    : CommunityView
  IP access control list:

GroupName: private
SecurityModel: v2c
  ReadView      : CommunityView          WriteView      : CommunityView
  NotifyView    : CommunityView
  IP access control list:

Total Entries: 5

```

項番	説明
(1)	SNMP グループ名を表示します。
(2)	セキュリティーモデルを表示します。 v1 : SNMPv1 v2c : SNMPv2c v3/noauth : SNMPv3 (認証なし、暗号化なし) v3/auth : SNMPv3 (認証あり、暗号化なし) v3/priv : SNMPv3 (認証あり、暗号化あり)
(3)	グループのユーザーに読み取りを許可する SNMP ビュー (read-view) を表示します。
(4)	グループのユーザーに書き込みを許可する SNMP ビュー (write-view) を表示します。
(5)	グループのユーザーに SNMP トラップの送信を許可する SNMP ビュー (notify-view) を表示します。
(6)	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。

#### 4.12.27 show snmp view

show snmp view	
目的	SNMP ビュー設定を表示します。
シンタックス	<b>show snmp view</b>
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 snmp view	
注意事項	-
対象バージョン	1.01.01

使用例：SNMP ビュー設定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。

#### 4.12.28 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	<b>show snmp engineID</b>
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。

## 4.13 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]

### 4.13.1 monitor session destination interface

monitor session destination interface	
目的	ローカルモニターセッション、もしくはリモートモニターセッション（モニター先装置）において、ミラーリング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	<b>monitor session</b> SESSION-NUMBER destination interface INTERFACE-ID <b>no monitor session</b> 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。 <ul style="list-style-type: none"> <li>• port: 物理ポートを指定します。</li> <li>• port-channel: ポートチャネルを指定します。</li> </ul>
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	<p>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。</p> <p>すでに <b>monitor session destination remote vlan</b> 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。</p> <p>モニターセッションは、以下の数え方で装置全体で最大 4 リソースまで設定できます。</p> <ul style="list-style-type: none"> <li>送信元インターフェース設定に <b>rx</b> 指定（送信元アクセスリスト含む）と <b>tx</b> 指定の両方を含むモニターセッションの場合：2 リソース</li> <li>送信元インターフェース設定が <b>rx</b> 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の場合：1 リソース</li> <li>送信元インターフェース設定が <b>tx</b> 指定のみのモニターセッションの場合：1 リソース</li> </ul>
注意事項	<p>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 <b>monitor session destination interface</b> 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 <b>switchport access vlan</b> 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。</p>
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)#
```

#### 4.13.2 monitor session destination remote vlan

monitor session destination remote vlan	
目的	<p>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。</p>
シンタックス	<pre><b>monitor session</b> <i>SESSION-NUMBER</i> <b>destination remote vlan</b> <i>VLAN-ID</i> <b>interface</b> <i>INTERFACE-ID</i> <b>no monitor session</b> <i>SESSION-NUMBER</i> <b>destination remote vlan</b></pre>
パラメーター	<p><b>SESSION-NUMBER</b>：セッション番号を、1～4 の範囲で指定します。</p> <p><b>VLAN-ID</b>：リモートモニターVLAN を、2～4094 の範囲で指定します。</p> <p><b>interface INTERFACE-ID</b>：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。</p> <ul style="list-style-type: none"> <li><b>port</b>：物理ポートを指定します。</li> <li><b>port-channel</b>：ポートチャネルを指定します。</li> </ul>
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



monitor session destination remote vlan	
	<p>フェースのみ設定できます。</p> <p>本コマンドでリモートモニターセッション（モニター元装置）を設定する場合、宛先インターフェースに指定したリモートモニターVLAN が割り当てられていなくても、ミラーリング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。</p>
制限事項	<p>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。</p> <p>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。</p> <p>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。</p> <p>モニターセッションは、以下の数え方で装置全体で最大 4 リソースまで設定できます。</p> <ul style="list-style-type: none"> <li>送信元インターフェース設定に <b>rx</b> 指定（送信元アクセスリスト含む）と <b>tx</b> 指定の両方を含むモニターセッションの場合：2 リソース</li> <li>送信元インターフェース設定が <b>rx</b> 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の場合：1 リソース</li> <li>送信元インターフェース設定が <b>tx</b> 指定のみのモニターセッションの場合：1 リソース</li> </ul>
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)#
```

### 4.13.3 monitor session source interface

monitor session source interface	
目的	ローカルモニターセッション、もしくはリモートモニターセッション（モニター元装置）において、ミラーリングする送信元インターフェースを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<pre>monitor session SESSION-NUMBER source interface {INTERFACE-ID [, -] [both   rx   tx]   cpu rx} no monitor session SESSION-NUMBER source interface {INTERFACE-ID [, -]   cpu rx}</pre>
パラメーター	<p><b>SESSION-NUMBER</b>：セッション番号を、1~4 の範囲で指定します。</p> <p><b>INTERFACE-ID</b>：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。</p> <ul style="list-style-type: none"> <li><b>port</b>：物理ポートを指定します。複数指定できます。</li> <li><b>port-channel</b>：ポートチャンネルを指定します。</li> </ul>

monitor session source interface	
	<p><b>both</b> (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。</p> <p><b>rx</b> (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。</p> <p><b>tx</b> (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。</p> <p><b>cpu rx</b> : 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。</p>
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	<p>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せん。</p> <p><b>both</b>, <b>rx</b>, <b>tx</b> パラメーターを指定しない場合は、<b>both</b> 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、<b>both</b> パラメーターを指定して設定した場合は、構成情報では <b>rx</b> パラメーターと <b>tx</b> パラメーターの設定として表示されません。</p>
制限事項	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>モニターセッションは、以下の数え方で装置全体で最大 4 リソースまで設定できます。</p> <ul style="list-style-type: none"> <li>• 送信元インターフェース設定に <b>rx</b> 指定 (送信元アクセスリスト含む) と <b>tx</b> 指定の両方を含むモニターセッションの場合 : 2 リソース</li> <li>• 送信元インターフェース設定が <b>rx</b> 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の場合 : 1 リソース</li> <li>• 送信元インターフェース設定が <b>tx</b> 指定のみのモニターセッションの場合 : 1 リソース</li> </ul>
注意事項	<p>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 <b>rx</b>、<b>tx</b> 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。</p>
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)#
```

## 4.13.4 monitor session source acl

monitor session source acl	
目的	ローカルモニターセッション、もしくはリモートモニターセッション（モニター元装置）において、フローベースのモニターを行うための送信元アクセスリストを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>monitor session</b> <i>SESSION-NUMBER</i> <b>source acl</b> <i>ACCESS-LIST-NAME</i> <b>no monitor session</b> <i>SESSION-NUMBER</i> <b>source acl</b> <i>ACCESS-LIST-NAME</i>
パラメーター	<i>SESSION-NUMBER</i> : セッション番号を、1~4 の範囲で指定します。 <i>ACCESS-LIST-NAME</i> : 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。モニター用のアクセスリストとして、拡張 MAC アクセスリスト、IP アクセスリスト、および IPv6 アクセスリストのみ使用できます。
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	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せん。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、 <b>mac access-group</b> コマンド、 <b>ip access-group</b> コマンド、または <b>ipv6 access-group</b> 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。 モニターセッションは、以下の数え方で装置全体で最大 4 リソースまで設定できます。 <ul style="list-style-type: none"> <li>送信元インターフェース設定に <b>rx</b> 指定（送信元アクセスリスト含む）と <b>tx</b> 指定の両方を含むモニターセッションの場合 : 2 リソース</li> <li>送信元インターフェース設定が <b>rx</b> 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の場合 : 1 リソース</li> <li>送信元インターフェース設定が <b>tx</b> 指定のみのモニターセッションの場合 : 1 リソース</li> </ul>
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)#

## 4.13.5 monitor session source remote vlan

monitor session source remote vlan	
目的	リモートモニターセッション（モニター先装置）において、ミラーリング元のリモートモニターVLAN を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>monitor session</b> <i>SESSION-NUMBER</i> <b>source remote vlan</b> <i>VLAN-ID</i> <b>no monitor session</b> <i>SESSION-NUMBER</i> <b>source remote vlan</b>
パラメーター	<i>SESSION-NUMBER</i> : セッション番号を、1~4 の範囲で指定します。 <i>VLAN-ID</i> : 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
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 のみ設定できません。 リモートモニターセッション（モニター先装置）では、 <b>monitor session source remote vlan</b> 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、 <b>monitor session destination interface</b> 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 <b>switchport trunk allowed vlan</b> 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 packets はポート 1/0/1 で受信して、ポート 1/0/4 から送信されます。

```
# configure terminal
(config)# vlan 100
(config-vlan)# remote-span
(config-vlan)# exit
(config)# interface port 1/0/1
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk allowed vlan 100
(config-if-port)# exit
(config)# interface port 1/0/4
(config-if-port)# switchport mode access
(config-if-port)# switchport access vlan 100
(config-if-port)# exit
(config)# monitor session 2 source remote vlan 100
```

```
(config)# monitor session 2 destination interface port 1/0/4
(config)#
```

#### 4.13.6 remote-span

remote-span	
目的	VLAN をリモートモニターVLAN として設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>remote-span</b> <b>no remote-span</b>
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。  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)#
```

#### 4.13.7 no monitor session

no monitor session	
目的	モニターセッションを削除します。
シンタックス	<b>no monitor session</b> <i>SESSION-NUMBER</i>
パラメーター	<i>SESSION-NUMBER</i> : 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

no monitor session	
	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)#
```

#### 4.13.8 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	<b>show monitor session</b> [ <i>SESSION-NUMBER</i>   <b>remote</b>   <b>local</b> ]
パラメーター	<i>SESSION-NUMBER</i> (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。  <b>remote</b> (省略可能)：リモートモニターセッションを表示します。  <b>local</b> (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	セッション番号を指定しない場合、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

項番	説明
	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 ID 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 ID 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 ID 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 ID を表示します。 Both : ミラーリング対象が受信フレームおよび送信フレームの送信元インターフェース RX : ミラーリング対象が受信フレームのみの送信元インターフェース TX : ミラーリング対象が送信フレームのみの送信元インターフェース
(6)	リモートモニターセッション (モニター先装置) で設定した、ミラーリング元のリモートモニターVLAN を表示します。

## 4.14 LLDP コマンド

LLDP (Link Layer Discovery Protocol) 関連の設定コマンドは以下のとおりです。

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   max- frame-size] no lldp dot3-tlv-select [mac-phy-cfg   link-aggregation   max- frame-size]
lldp med-tlv-select	lldp med-tlv-select [capabilities   inventory-management] no lldp med-tlv-select [capabilities   inventory-management]
lldp err-disable	lldp err-disable no lldp err-disable



コマンド	コマンドとパラメーター
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 [,  -]]

#### 4.14.1 lldp run

lldp run	
目的	LLDP 機能のグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
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 <b>lldp transmit</b> コマンドを、物理ポートごとの LLDPDU 受信の有効/無効は <b>lldp receive</b> 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 機能をグローバルに有効にする方法を示します。

```
# configure terminal
(config)# lldp run
(config)#
```

#### 4.14.2 lldp transmit

lldp transmit	
目的	LLDPDU の送信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>lldp transmit</b> <b>no lldp transmit</b>
パラメーター	なし
デフォルト	有効 ( <b>lldp transmit</b> )
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、 <b>lldp run</b> 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)#
```

#### 4.14.3 lldp receive

lldp receive	
目的	LLDPDU の受信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>lldp receive</b> <b>no lldp receive</b>
パラメーター	なし
デフォルト	有効 ( <b>lldp receive</b> )
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、 <b>lldp run</b> 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)#
```

#### 4.14.4 lldp forward

lldp forward	
目的	LLDP 転送機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>lldp forward</b> <b>no lldp forward</b>
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、 <b>no lldp run</b> コマンドで LLDP 機能をグローバルに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)#
```

#### 4.14.5 lldp tx-delay

lldp tx-delay	
目的	LLDPDU の送信遅延間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>lldp tx-delay SECONDS</b> <b>no lldp tx-delay</b>
パラメーター	<i>SECONDS</i> : 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、 <b>lldp tx-interval</b> 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)#
```

## 4.14.6 lldp tx-interval

lldp tx-interval	
目的	LLDPDU の送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>lldp tx-interval</b> <i>SECONDS</i> <b>no lldp tx-interval</b>
パラメーター	<i>SECONDS</i> : LLDPDU を連続送信する場合の送信間隔を、5~32768 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、 <b>lldp tx-delay</b> 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)#
```

## 4.14.7 lldp hold-multiplier

lldp hold-multiplier	
目的	送信する LLDPDU の TTL 値を決定するための、LLDPDU 送信間隔の乗数 (Message TX Hold Multiplier) を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>lldp hold-multiplier</b> <i>VALUE</i> <b>no hold-multiplier</b>
パラメーター	<i>VALUE</i> : 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 ( <b>lldp tx-interval</b> ) × 乗数 ( <b>lldp hold-multiplier</b> ) 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)#
```

## 4.14.8 lldp reinit

lldp reinit	
目的	LLDP 再初期化の遅延時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>lldp reinit</b> <i>SECONDS</i> <b>no lldp reinit</b>
パラメーター	<i>SECONDS</i> : 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)#
```

## 4.14.9 lldp fast-count

lldp fast-count	
目的	LLDP-MED fast start 処理の実行回数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>lldp fast-count</b> <i>VALUE</i> <b>no lldp fast-count</b>
パラメーター	<i>VALUE</i> : 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)#
```

## 4.14.10 lldp subtype port-id

lldp subtype port-id	
目的	Port ID TLV のサブタイプを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>lldp subtype port-id</b> { <i>mac-address</i>   <i>local</i> }

lldp subtype port-id	
パラメーター	<p><b>mac-address</b> : 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。</p> <p><b>local</b> : 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。</p>
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)#
```

#### 4.14.11 lldp tlv-select

lldp tlv-select	
目的	IEEE 802.1AB basic management set のオプション TLV のうち、LLDPDU に付加して隣接装置に通知する TLV を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<pre>lldp tlv-select [port-description   system-capabilities   system-description   system-name] no lldp tlv-select [port-description   system-capabilities   system-description   system-name]</pre>
パラメーター	<p><b>port-description</b> (省略可能) : Port Description TLV を通知する場合に指定します。</p> <p><b>system-capabilities</b> (省略可能) : System Capabilities TLV を通知する場合に指定します。</p> <p><b>system-description</b> (省略可能) : System Description TLV を通知する場合に指定します。</p> <p><b>system-name</b> (省略可能) : System Name TLV を通知する場合に指定します。</p>
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	<p>System Name TLV で通知する System Name は、<b>snmp-server name</b> コマンドで設定できます。</p> <p>パラメーターを指定しないで <b>lldp tlv-select</b> を実行した場合は、すべての <b>lldp tlv-select</b> 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 <b>no lldp tlv-select</b> を実行した場合は、すべての <b>lldp tlv-select</b> 設定が削除されます。</p>
制限事項	-

lldp tlv-select	
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)#
```

#### 4.14.12 lldp management-address

lldp management-address	
目的	Management Address TLV で通知する管理用 IP アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>lldp management-address</b> [ <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> ] <b>no lldp management-address</b> [ <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> ]
パラメーター	<i>IP-ADDRESS</i> (省略可能)：管理用 IPv4 アドレスを指定します。 <i>IPV6-ADDRESS</i> (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	<b>lldp management-address</b> 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 <b>lldp management-address</b> 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 <b>lldp management-address</b> 設定も削除されます。  管理用 IP アドレスを指定しないで <b>no lldp management-address</b> を実行した場合は、すべての <b>lldp management-address</b> 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 <b>lldp management-address</b> 設定」と「管理用 IP アドレスを指定しない <b>lldp management-address</b> 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 <b>lldp management-address</b> 設定」のみ動作します。
対象バージョン	1.01.01

使用例：ポート 1/0/1 からポート 1/0/2 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)#
```

#### 4.14.13 lldp dot1-tlv-select

lldp dot1-tlv-select	
目的	IEEE 802.1 Organizationally Specific TLVs のうち、LLDPDU (LLDP data unit) に付加して隣接装置に通知する TLV を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<pre>lldp dot1-tlv-select {port-vlan   protocol-vlan <i>VLAN-ID</i> [,  -]   vlan-name [<i>VLAN-ID</i> [,  -]]   protocol-identity [<i>PROTOCOL-NAME</i>]}</pre> <pre>no lldp dot1-tlv-select {port-vlan   protocol-vlan [<i>VLAN-ID</i> [,  -]]   vlan-name [<i>VLAN-ID</i> [,  -]]   protocol-identity [<i>PROTOCOL-NAME</i>]}</pre>
パラメーター	<p><b>port-vlan</b> : Port VLAN ID TLV を通知する場合に指定します。</p> <p><b>protocol-vlan <i>VLAN-ID</i></b> : 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。</p> <p><b>vlan-name [<i>VLAN-ID</i>]</b> : 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。</p> <p><b>protocol-identity [<i>PROTOCOL-NAME</i>]</b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>eapol</b> : Extensible Authentication Protocol (EAP) over LAN</li> <li>• <b>lacp</b> : Link Aggregation Control Protocol</li> <li>• <b>stp</b> : スパニングツリープロトコル</li> </ul>
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
ガイドライン	<p>PPVID TLV は、<b>protocol-vlan</b> 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。</p> <p>VLAN Name TLV は、<b>vlan-name</b> パラメーターで指定した VLAN が、対象ポートに設</p>



lldp dot1-tlv-select	
	定されている場合に通知されます。 Protocol Identity TLV は、 <b>protocol-identity</b> 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	<b>lldp dot1-tlv-select protocol-vlan</b> 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。 <b>lldp dot1-tlv-select vlan-name</b> 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)#
```

#### 4.14.14 lldp dot3-tlv-select

lldp dot3-tlv-select	
目的	IEEE 802.3 Organizationally Specific TLVs のうち、LLDPDU に付加して隣接装置に通知する TLV を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>lldp dot3-tlv-select</b> [ <b>mac-phy-cfg</b>   <b>link-aggregation</b>   <b>max-frame-size</b> ] <b>no lldp dot3-tlv-select</b> [ <b>mac-phy-cfg</b>   <b>link-aggregation</b>   <b>max-frame-size</b> ]
パラメーター	<b>mac-phy-cfg</b> (省略可能) : MAC/PHY Configuration/Status TLV を通知する場合に指定します。 <b>link-aggregation</b> (省略可能) : Link Aggregation TLV を通知する場合に指定します。 <b>max-frame-size</b> (省略可能) : Maximum Frame Size TLV を通知する場合に指定し

lldp dot3-tlv-select	
	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 <code>lldp dot3-tlv-select</code> を実行した場合は、すべての <code>lldp dot3-tlv-select</code> 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 <code>no lldp dot3-tlv-select</code> を実行した場合は、すべての <code>lldp dot3-tlv-select</code> 設定が削除されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 で、MAC/PHY Configuration/Status TLV の通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp dot3-tlv-select mac-phy-cfg
(config-if-port)#
```

#### 4.14.15 lldp med-tlv-select

lldp med-tlv-select	
目的	LLDP-MED TLV のうち、LLDPDU に付加して隣接装置に通知する TLV を設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<code>lldp med-tlv-select [capabilities   inventory-management]</code> <code>no lldp med-tlv-select [capabilities   inventory-management]</code>
パラメーター	<b>capabilities</b> (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。  <b>inventory-management</b> (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。
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)
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。  パラメーターを指定しないで <code>lldp med-tlv-select</code> を実行した場合は、すべての <code>lldp med-tlv-select</code> 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 <code>no lldp med-tlv-select</code> を実行した場合は、すべての <code>lldp med-tlv-select</code> 設定が削除されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/1 で、LLDP-MED Capabilities TLV の通知を有効にする方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# lldp med-tlv-select capabilities
(config-if-port)#
```

#### 4.14.16 lldp err-disable

lldp err-disable	
目的	物理ポートで LLDP 疑似リンクダウン機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>lldp err-disable</b> <b>no lldp err-disable</b>
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	<p>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。</p> <p>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、<b>show channel-group</b> 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。</p> <p>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、<b>show mmrp-plus status ring</b> コマンドや <b>show mmrp-plus status port</b> 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。</p> <p>LLDP 疑似リンクダウン状態の物理ポートでは、<b>show interfaces status</b> コマンドのステータスは connected と表示され、<b>show interfaces port</b> コマンド、もしくは <b>show interfaces description</b> コマンドのステータスは errDis と表示されます。</p>
制限事項	-
注意事項	<p>物理ポートの設定用のコマンドです。</p> <p>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。</p> <p>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。</p> <p>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。</p>
対象バージョン	1.01.01

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)#
```

## 4.14.17 lldp notification enable

lldp notification enable	
目的	LLDP 関連の SNMP トラップ送信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>lldp notification enable</b> <b>no lldp notification enable</b>
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 関連の SNMP トラップ送信を有効にする場合は、 <b>snmp-server enable traps lldp</b> 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)#
```

## 4.14.18 lldp med notification enable

lldp med notification enable	
目的	LLDP-MED 関連の SNMP トラップ送信を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>lldp med notification enable</b> <b>no lldp med notification enable</b>
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、 <b>snmp-server enable traps lldp med</b> 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)#
```

## 4.14.19 snmp-server enable traps lldp

snmp-server enable traps lldp	
目的	LLDP 関連の SNMP トラップ送信をグローバルに有効にします。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	<b>snmp-server enable traps lldp</b> <b>no snmp-server enable traps lldp</b>
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、 <b>snmp-server enable traps</b> コマンドでグローバル設定も有効にしてください。  物理ポートごとの LLDP 関連の SNMP トラップ送信の有効/無効は <b>lldp notification enable</b> 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 トラップ送信をグローバルに有効にする方法を示します。

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

## 4.14.20 snmp-server enable traps lldp med

snmp-server enable traps lldp med	
目的	LLDP-MED 関連の SNMP トラップ送信をグローバルに有効にします。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	<b>snmp-server enable traps lldp med</b> <b>no snmp-server enable traps lldp med</b>
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、 <b>snmp-server enable traps</b> 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 <b>lldp med notification enable</b> 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 トラップ送信をグローバルに有効にする方法を示します。

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

## 4.14.21 show lldp

show lldp	
目的	装置の一般的な LLDP 設定を表示します。
シンタックス	<b>show lldp</b>
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：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-AF-F0-48 ... (2)
  System Name             : Switch ... (3)
  System Description      : ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch
                          Ver.1.02.01 ... (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      : 1.02.01 ... (10)
  Serial Number          : 400010000034 ... (11)
  Manufacturer Name     : APRESIA Systems, Ltd ... (12)
  Model Name             : ApresiaNP4000-20Xt4X TenGigabit ... (13)
  Asset ID               : ... (14)

LLDP Configurations
  LLDP State             : Disabled ... (15)
  LLDP Forward State     : Disabled ... (16)
  Message TX Interval    : 30 ... (17)
  Message TX Hold Multiplier: 4 ... (18)
  ReInit Delay           : 2 ... (19)
  TX Delay               : 2 ... (20)

LLDP-MED Configuration:
  Fast Start Repeat Count : 4 ... (21)

```

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。

項番	説明
(7)	LLDP-MED 対応機器として動作する際に通知するデバイスクラスを表示します。
(8)	LLDP-MED 対応機器として動作する際に通知するハードウェアリビジョンを表示します。
(9)	LLDP-MED 対応機器として動作する際に通知するファームウェアリビジョンを表示します。
(10)	LLDP-MED 対応機器として動作する際に通知するソフトウェアリビジョンを表示します。
(11)	LLDP-MED 対応機器として動作する際に通知するシリアル番号を表示します。
(12)	LLDP-MED 対応機器として動作する際に通知するメーカー名を表示します。
(13)	LLDP-MED 対応機器として動作する際に通知するモデル名を表示します。
(14)	LLDP-MED 対応機器として動作する際に通知するアセット ID を表示します。
(15)	装置全体の LLDP 設定の有効/無効を表示します。
(16)	LLDP 転送の有効/無効を表示します。
(17)	LLDPDU の送信間隔を表示します。
(18)	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。
(19)	LLDP 再初期化の遅延時間を表示します。
(20)	LLDPDU の送信遅延間隔を設定します。
(21)	LLDP-MED fast start 処理の実行回数を表示します。

#### 4.14.22 show lldp interface

show lldp interface	
目的	物理ポートの LLDP 設定を表示します。
シンタックス	<b>show lldp interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li><b>port</b>: 物理ポートを指定します。複数指定できます。</li> </ul>
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)
Link Aggregation	:Disabled ... (16)
Maximum Frame Size	:Disabled ... (17)
Organizationally Specific TLVs:	
Link Fault TLV	:Disabled ... (18)
LLDP-MED Organizationally Specific TLVs:	
LLDP-MED Capabilities TLV	:Disabled ... (19)
LLDP-MED Inventory TLV	:Disabled ... (20)

項番	説明
(1)	インターフェース ID を表示します。
(2)	インターフェース ID 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)	Link Aggregation TLV 付加の有効/無効を表示します。



項番	説明
(17)	Maximum Frame Size TLV 付加の有効/無効を表示します。
(18)	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。
(19)	LLDP-MED Capabilities TLV 付加の有効/無効を表示します。
(20)	LLDP-MED Inventory Management TLV 付加の有効/無効を表示します。

### 4.14.23 show lldp local interface

show lldp local interface	
目的	各 TLV の通知が有効になっている場合に、LLDP TLV に含めて隣接装置に通知される物理ポート情報を表示します。
シンタックス	<b>show lldp local interface</b> <i>INTERFACE-ID</i> [, -] [ <b>brief</b>   <b>detail</b> ]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。複数指定できます。</li> </ul> <b>brief</b> (省略可能): 情報を要約モードで表示します。 <b>detail</b> (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 1/0/15 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 1/0/15

Port ID: Port1/0/15 ... (1)
-----
Port ID Subtype           : Local ... (2)
Port ID                   : Port1/0/15 ... (3)
Port Description          : APRESIA Systems, Ltd
                          ApresiaNP4000-20Xt4X HW A firmware
                          1.02.01 Port 15 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)
Link Aggregation          : (See Detail) ... (11)
Maximum Frame Size        : 1536 ... (12)
Link Fault                 : - ... (13)
LLDP-MED capabilities     : (See Detail) ... (14)
```

項番	説明
(1)	インターフェース ID 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)	Link Aggregation TLV で通知される情報は、詳細モードで確認します。
(12)	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。
(13)	LLDP 疑似リンクダウンに関する情報を表示します。
(14)	LLDP-MED Capabilities 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 1/0/15 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 1/0/15 brief

Port ID: Port1/0/15 ... (1)
-----
Port ID Subtype           : Local ... (2)
Port ID                   : Port1/0/15 ... (3)
Port Description          : APRESIA Systems, Ltd
                          ApresiaNP4000-20Xt4X HW A firmware
                          1.02.01 Port 15 on Unit 1 ... (4)
```

項番	説明
(1)	インターフェース ID 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 1/0/15 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 1/0/15 detail

Port ID: Port1/0/15 ... (1)
-----
Port ID Subtype           : Local ... (2)
Port ID                   : Port1/0/15 ... (3)
Port Description          : APRESIA Systems, Ltd
                          ApresiaNP4000-20Xt4X HW A firmware
                          1.02.01 Port 15 on Unit 1 ... (4)
Port PVID                 : 1 ... (5)
Management Address Count  : 1 ... (6)
```

```

Address 1 : (default)
  Subtype                : IPv4
  Address                 : 192.168.10.100
  IF Type                 : IfIndex
  OID                    : 1.3.6.1.4.1.1.278.1.42.6

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 : 8000 (hex)
  Auto-Negotiation Operational MAU Type : 0000 (hex)

Link Aggregation          : ... (11)
  Aggregation Capability    : Aggregated
  Aggregation Status        : Not Currently in Aggregation
  Aggregation Port ID       : 0

Maximum Frame Size        : 1536 ... (12)

Link Fault                 : - ... (13)

LLDP-MED Capabilities Support: ... (14)
  Capabilities              :Support
  Network Policy            :Not Support
  Location Identification    :Not Support
  Extended Power Via MDI PSE :Not Support
  Extended Power Via MDI PD  :Not Support
  Inventory                  :Support

```

項番	説明
(1)	インターフェース ID 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。

項番	説明
(11)	Link Aggregation TLV で通知される情報を表示します。
(12)	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。
(13)	LLDP 疑似リンクダウンに関する情報を表示します。
(14)	LLDP-MED Capabilities TLV で通知される情報を表示します。

#### 4.14.24 show lldp management-address

show lldp management-address	
目的	Management Address TLV で通知する管理用アドレス情報を表示します。
シンタックス	<b>show lldp management-address</b> [ <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> ]
パラメーター	<i>IP-ADDRESS</i> (省略可能) : 表示する管理用 IPv4 アドレスを指定します。 <i>IPV6-ADDRESS</i> (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               : 1.3.6.1.4.1.278.1.42.6 ... (4)
Advertising Ports : - ... (5)

Address 2 :
-----
Subtype           : IPv4
Address           : 192.0.2.100
IF Type          : IfIndex
OID               : 1.3.6.1.4.1.278.1.42.6
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。

## 4.14.25 show lldp neighbors interface

show lldp neighbors interface	
目的	隣接装置の LLDP 情報を表示します。
シンタックス	<b>show lldp neighbors interface</b> <i>INTERFACE-ID</i> [, -] [ <b>brief</b>   <b>detail</b> ]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li><b>port</b>: 物理ポートを指定します。複数指定できます。</li> </ul> <b>brief</b> (省略可能): 情報を要約モードで表示します。 <b>detail</b> (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)	自装置のインターフェース ID 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。
(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)	自装置のインターフェース ID 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 (None)	: 0 ... (22)
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)	自装置のインターフェース ID を表示します。
(2)	登録された隣接装置の数を表示します。
(3)	登録番号を表示します。
(4)	隣接装置から通知された、Chassis ID TLV のサブタイプを表示します。
(5)	隣接装置から Chassis ID TLV で通知された、Chassis ID 情報を表示します。
(6)	隣接装置から通知された、Port ID TLV のサブタイプを表示します。
(7)	隣接装置から Port ID TLV で通知された、Port ID 情報を表示します。
(8)	隣接装置から Port Description TLV で通知された、ポートの説明を表示します。
(9)	隣接装置から System Name TLV で通知された、システム名を表示します。
(10)	隣接装置から System Description TLV で通知された、システムの説明を表示します。
(11)	隣接装置から System Capabilities TLV で通知された、システムの利用可能な能力を表示します。
(12)	隣接装置から Management Address TLV で通知された、管理用 IP アドレスの数と IP アドレス情報を表示します。0 個の場合は、IP アドレス情報は (None) と表示されます。
(13)	隣接装置から Port VLAN ID TLV で通知された、ポートの VLAN ID を表示します。
(14)	隣接装置から Port and Protocol VLAN ID (PPVID) TLV で通知された、プロトコル VLAN の数と VLAN 情報を表示します。0 個の場合は、VLAN 情報は (None) と表示されます。
(15)	隣接装置から VLAN Name TLV で通知された、VLAN の数と VLAN 情報を表示します。0 個の場合は、VLAN 情報は (None) と表示されます。
(16)	隣接装置から Protocol Identity TLV で通知された、プロトコルの数とプロトコル情報を表示します。0 個の場合は、プロトコル情報は (None) と表示されます。
(17)	隣接装置から MAC/PHY Configuration/Status TLV で通知された情報を表示します。
(18)	隣接装置から Power Via MDI TLV で通知された情報を表示します。
(19)	隣接装置から Link Aggregation TLV で通知された情報を表示します。
(20)	隣接装置から Maximum Frame Size TLV で通知された、最大フレームサイズを表示します。
(21)	隣接装置からベンダー独自の Link Fault TLV で通知された、LLDP 疑似リンクダウンに関する情報を表示します。
(22)	隣接装置から通知された、未知の TLV の数と TLV 情報を表示します。
(23)	隣接装置から LLDP-MED Capabilities TLV で通知された情報を表示します。
(24)	隣接装置から LLDP-MED Inventory Management TLV で通知された情報を表示します。

#### 4.14.26 show lldp traffic

show lldp traffic	
目的	グローバルな LLDP 統計情報を表示します。



show lldp traffic	
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。
(2)	LLDP テーブルに登録した回数を表示します。
(3)	クリアコマンドや、TTL 値が 0 秒の LLDPDU を受信して LLDP テーブルから削除した回数を表示します。
(4)	リソース不足のため、LLDP テーブルに登録されなかった回数を表示します。
(5)	TTL expired により LLDP テーブルから削除された回数を表示します。

#### 4.14.27 show lldp traffic interface

show lldp traffic interface	
目的	物理ポートの LLDP 統計情報を表示します。
シンタックス	show lldp traffic interface <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>port : 物理ポートを指定します。複数指定できます。</li> </ul>
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 1/0/20 の LLDP 統計情報を表示する方法を示します。

```
# show lldp traffic interface port 1/0/20

Port ID : Port1/0/20 ... (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)	インターフェース ID を表示します。
(2)	送信した LLDPDU の数を表示します。
(3)	廃棄した LLDPDU の数を表示します。
(4)	受信した無効な LLDPDU の数を表示します。
(5)	受信した LLDPDU の数を表示します。
(6)	廃棄した情報 (TLV) の数を表示します。
(7)	受信した未知の情報 (TLV) の数を表示します。
(8)	TTL expired により LLDP テーブルから削除された回数を表示します。

#### 4.14.28 clear lldp table

clear lldp table	
目的	LLDP テーブルに登録された隣接装置の LLDP 情報を削除します。
シンタックス	<code>clear lldp table {all   interface <i>INTERFACE-ID</i> [,  -]}</code>
パラメーター	<p><b>all</b> : すべてのインターフェースの隣接装置の LLDP 情報を削除する場合に指定します。</p> <p><b>interface <i>INTERFACE-ID</i></b> : 隣接装置の 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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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 : すべてのインターフェースの隣接装置の LLDP 情報を削除する方法を示します。

```

# clear lldp table all
#

```

#### 4.14.29 clear lldp counters

clear lldp counters	
目的	LLDP 統計情報を消去します。
シンタックス	<code>clear lldp counters [all   interface <i>INTERFACE-ID</i> [,  -]]</code>
パラメーター	<b>all</b> (省略可能) : すべてのインターフェースの 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。

clear lldp counters	
	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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 : すべてのインターフェースの LLDP 統計情報、およびグローバルな LLDP 統計情報を消去する方法を示します。

```
# clear lldp counters all
#
```

## 4.15 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}

## 4.15.1 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	<b>ethernet oam</b> <b>no ethernet oam</b>
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)#
```

## 4.15.2 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	<b>ethernet oam mode {active   passive}</b> <b>no ethernet oam mode</b>
パラメーター	<b>active</b> : 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。 <b>passive</b> : 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。 <ul style="list-style-type: none"> <li>• EtherOAM ディスカバリーの開始</li> <li>• リモートループバックの開始または停止</li> </ul>
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)#
```

### 4.15.3 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	<b>ethernet oam link-monitor error-symbol</b> [threshold <i>NUMBER</i> ] [window <i>DECISECONDS</i> ] <b>no ethernet oam link-monitor error-symbol</b> [threshold   window]
パラメーター	<b>threshold</b> <i>NUMBER</i> (省略可能)：シンボルエラー回数を 0～4294967295 の範囲で指定します。 <b>window</b> 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。 <b>window</b> <i>DECISECONDS</i> (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)#
```

#### 4.15.4 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	<b>ethernet oam link-monitor error-frame</b> [ <b>threshold</b> <i>NUMBER</i> ] [ <b>window</b> <i>DECISECONDS</i> ] <b>no ethernet oam link-monitor error-frame</b> [ <b>threshold</b>   <b>window</b> ]
パラメーター	<b>threshold</b> <i>NUMBER</i> (省略可能)：フレームエラー回数を 0～4294967295 の範囲で指定します。 <b>window</b> 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。 <b>window</b> <i>DECISECONDS</i> (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)#
```

#### 4.15.5 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	<b>ethernet oam link-monitor error-frame-seconds</b> [ <b>threshold</b> <i>NUMBER</i> ] [ <b>window</b> <i>DECISECONDS</i> ] <b>no ethernet oam link-monitor error-frame-seconds</b> [ <b>threshold</b>   <b>window</b> ]
パラメーター	<b>threshold</b> <i>NUMBER</i> (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。 <b>window</b> 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。  <b>window</b> <i>DECISECONDS</i> (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)#
```

#### 4.15.6 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	<b>ethernet oam link-monitor error-frame-period</b> [threshold <i>NUMBER</i> ] [window <i>NUMBER</i> ] <b>no ethernet oam link-monitor error-frame-period</b> [threshold   window]
パラメーター	<b>threshold</b> <i>NUMBER</i> (省略可能)：フレームエラー回数を、0～4294967295 の範囲で指定します。 <b>window</b> 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。 <b>window</b> <i>NUMBER</i> (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)#
```

#### 4.15.7 ethernet oam remote-failure critical-event

ethernet oam remote-failure critical-event	
目的	指定したインターフェースでクリティカルイベントの通知を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>ethernet oam remote-failure critical-event</b> <b>no ethernet oam remote-failure critical-event</b>
パラメーター	なし
デフォルト	有効 ( <b>ethernet oam remote-failure critical-event</b> )
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)#
```

#### 4.15.8 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	<b>show ethernet oam configuration</b> [ <b>interface</b> <i>INTERFACE-ID</i> [, [-]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースの構成が表示されます。
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)	インターフェース ID 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。

#### 4.15.9 show ethernet oam status

show ethernet oam status	
目的	EtherOAM のプライマリ制御と状態の情報を表示します。
シンタックス	<b>show ethernet oam status</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースの EtherOAM のプライマリ制御と状態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)	インターフェース ID 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

項番	説明
	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。

#### 4.15.10 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	<b>show ethernet oam statistics</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースの統計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)	インターフェース ID を表示します。
(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。

#### 4.15.11 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	<b>show ethernet oam event-log</b> [interface <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースのイベントログが表示されます。
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)
 1 Errored Frame records ... (9)
   Event index          : 1 ... (10)
   Time stamp           : 2024-01-16 10:30 ... (11)
   Error frame/symbol   : 1 ... (12)
   Window                : 1000 (millisecond) ... (13)
   Threshold             : 1 ... (14)
   Accumulated errors   : 1 ... (15)

 0 Errored Frame Period records ... (16)
 1 Errored Frame Second records ... (17)
   Event index          : 2
   Time stamp           : 2024-01-16 10:30
   Error frame/symbol   : 1
   Window                : 60000 (millisecond)
   Threshold             : 1
   Accumulated errors   : 1

Remote event logs: ... (18)
-----
 0 Errored Symbol records
 0 Errored Frame records
 0 Errored Frame Period records
 0 Errored Frame Second records
    
```

項番	説明
(1)	インターフェース ID 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)	イベント番号を表示します。
(11)	ログが記録された日時を表示します。
(12)	検知されたエラーフレーム数を表示します。
(13)	エラーフレーム数を監視する単位時間（単位：ミリ秒）を表示します。
(14)	イベントが発生する際のエラーフレーム数の上限値を表示します。
(15)	EtherOAM のリセット後の累計イベント数を表示します。
(16)	エラーフレーム期間イベントログの数を表示します。
(17)	エラーフレーム秒イベントログの数を表示します。
(18)	隣接装置におけるイベントログの数を表示します。



## 4.15.12 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	<b>clear ethernet oam statistics</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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	インターフェースを指定しない場合、すべてのインターフェースの統計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
#
```

## 4.15.13 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	<b>clear ethernet oam event-log</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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	インターフェースを指定しない場合、すべてのインターフェースのイベントログが消去されます。
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
#
```

## 4.15.14 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	<b>ethernet oam remote-loopback</b> { <b>start</b>   <b>stop</b> } <b>interface</b> <i>INTERFACE-ID</i> [,  -]

ethernet oam remote-loopback	
パラメーター	<p><b>start</b> : 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。</p> <p><b>stop</b> : 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。</p> <p><b>interface</b> <i>INTERFACE-ID</i> : 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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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	<p>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、<b>ethernet oam remote-loopback start</b> コマンドを使用します。</p> <p>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、<b>ethernet oam remote-loopback stop</b> コマンドを使用します。</p> <p>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。</p>
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。
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
```

#### 4.15.15 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	<b>ethernet oam received-remote-loopback {process   ignore}</b>
パラメーター	<p><b>process</b> : 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。</p> <p><b>ignore</b> : 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。</p>
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	<p><b>ethernet oam remote-loopback</b> 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。</p> <p>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。<b>ethernet oam remote-loopback</b> 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。</p>
制限事項	-

ethernet oam received-remote-loopback	
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)#
```

## 4.16 単方向リンク検出(ULD) コマンド

単方向リンク検出(ULD)関連の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 [,  -]]

### 4.16.1 uld enable

uld enable	
目的	単方向リンク検出機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>uld enable</b> <b>no uld enable</b>
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	<p>本コマンドを設定する前に、<b>ethernet oam</b> コマンドで対象ポートの EtherOAM 機能を有効にしてください。</p> <p>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。</p> <p>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。</p>
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)#
```

## 4.16.2 uld action

uld action	
目的	単方向リンク検出機能のアクションを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>uld action shutdown</b> <b>no uld action</b>
パラメーター	<b>shutdown</b> : 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 ( <b>no uld action</b> )
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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>errdisable recovery cause uld</b> 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。</li> <li>• ポートに対して <b>shutdown</b> コマンドを実行した後、<b>no shutdown</b> 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。</li> </ul>
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)#
```

## 4.16.3 uld discovery-time

uld discovery-time	
目的	単方向リンク検出機能の Discovery プロセスの完了待機時間を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>uld discovery-time SECONDS</b> <b>no uld discovery-time</b>
パラメーター	<b>SECONDS</b> : Discovery プロセスの完了待機時間を、5~65535 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	<p>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。</p> <p>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</p>

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)#
```

#### 4.16.4 errdisable recovery cause uld

errdisable recovery cause uld	
目的	単方向リンク検出機能によって err-disabled 状態に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	<b>errdisable recovery cause uld [interval SECONDS]</b> <b>no errdisable recovery cause uld [interval]</b>
パラメーター	<b>interval SECONDS</b> (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、5~86400 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	<p>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。</p> <p>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。</p> <p>err-disabled 状態にされたポートのリンク状態は、<b>show interfaces</b> コマンドでは "link status is down (error disabled: OAM Unidirectional Link)" と表示されます。また、<b>show interfaces status</b> コマンドの Status 項目では "err-disabled" と表示されます。</p> <p>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 <b>shutdown</b> コマンドを実行した後、<b>no shutdown</b> 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。</p>
制限事項	本コマンドの設定は、構成情報ではエラー復旧コマンド関連で表示されます。(ラベル : # ERRDISABLE)
注意事項	<b>interval</b> 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 <b>interval</b> 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	1.02.01

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)#
```

## 4.16.5 show uld

show uld	
目的	単方向リンク検出機能の情報を表示します。
シンタックス	<b>show uld</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースの単方向リンク検出機能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。

## 4.17 CFM コマンド

CFM (Connectivity Fault Management) 関連の設定コマンドは以下のとおりです。

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}

#### 4.17.1 cfm global enable

cfm global enable	
目的	CFM 機能のグローバル設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。

cfm global enable	
シンタックス	<b>cfm global enable</b> <b>no cfm global enable</b>
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：CFM をグローバルに有効にする方法を示します。

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

#### 4.17.2 cfm enable

cfm enable	
目的	CFM 機能のインターフェースごとの設定を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>cfm enable</b> <b>no cfm enable</b>
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 機能はトランクポート ( <b>switchport mode trunk</b> ) で使用してください。アクセスポート ( <b>switchport mode access</b> ) での使用は未サポートです。
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)#
```

#### 4.17.3 cfm domain

cfm domain	
目的	メンテナンスドメイン (MD) を設定します。また、CFM MD 設定モードに遷移します。遷移後のプロンプトは (config-cfm-md)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>cfm domain DOMAIN-NAME level LEVEL</b> <b>no cfm domain DOMAIN-NAME</b>

cfm domain	
パラメーター	<p><b>domain</b> <i>DOMAIN-NAME</i> : MD 名を指定します。最大 22 文字で指定します。スペースは使用できません。</p> <p><b>level</b> <i>LEVEL</i> : ドメインレベルを 0~7 の範囲で指定します。</p>
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	<p>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。</p> <p>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。</p> <p>MD は装置全体で最大 8 個まで設定できます。</p>
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)#
```

#### 4.17.4 mip creation (MD)

mip creation (MD)	
目的	CFM MD 設定モードにおける、メンテナンス中間ポイント(MIP)作成ルールを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<p><b>mip creation {none   auto   explicit}</b></p> <p><b>no mip creation</b></p>
パラメーター	<p><b>none</b> : 対象 MA において MIP を作成しない場合に指定します。</p> <p><b>auto</b> : 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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>対象 MA のポートに MEP が設定されていない。</li> <li>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。</li> </ul> <p><b>explicit</b> : 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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>対象 MA のポートに MEP が設定されていない。</li> </ul>

mip creation (MD)	
	<ul style="list-style-type: none"> <li>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。</li> </ul>
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	<p>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。</p> <p>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 <b>mip creation</b> コマンドで設定します。</p>
制限事項	<p>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。</p> <p>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。</p>
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)#
```

#### 4.17.5 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	<b>sender-id {none   chassis   manage   chassis-manage}</b> <b>no sender-id</b>
パラメーター	<p><b>none</b> : CFM パケットに Sender ID TLV を付加しない場合に指定します。</p> <p><b>chassis</b> : 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。</p> <p><b>manage</b> : 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。</p> <p><b>chassis-manage</b> : 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。</p>
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 <b>sender-id</b> コマンドで設定します。
制限事項	-
注意事項	-

sender-id (MD)	
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)#
```

#### 4.17.6 cfm ma

cfm ma	
目的	メンテナンスアソシエーション(MA)を設定します。また、CFM MA 設定モードに遷移します。遷移後のプロンプトは (config-cfm-ma)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>cfm ma name</b> <i>MA-NAME</i> [ <b>vlan</b> <i>VLAN-ID</i> ] <b>no cfm ma name</b> <i>MA-NAME</i>
パラメーター	<b>name</b> <i>MA-NAME</i> : MA 名を指定します。最大 22 文字で指定します。スペースは使用できません。 <b>vlan</b> <i>VLAN-ID</i> (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 <b>vlan</b> 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)#
```

#### 4.17.7 mepid-list

mepid-list	
目的	MA の MEP ID リストを設定します。MEP ID をリストに追加する場合は、 <b>mepid-list add</b> 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、 <b>mepid-list delete</b> コマンドを使用します。
シンタックス	<b>mepid-list</b> { <b>add</b>   <b>delete</b> } <i>MEPID-LIST</i>

mepid-list	
パラメーター	<b>add</b> : MEP ID を MA の MEP ID リストに追加する場合に指定します。 <b>delete</b> : MEP ID を MA の MEP ID リストから削除する場合に指定します。 <i>MEPID-LIST</i> : 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	<b>cfm mep</b> 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)#
```

#### 4.17.8 ccm interval

ccm interval	
目的	メンテナンスアソシエーション(MA)の CCM 送信間隔を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>ccm interval</b> <i>INTERVAL</i> <b>no ccm interval</b>
パラメーター	<i>INTERVAL</i> : 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。 <ul style="list-style-type: none"> <li>• <b>100ms</b> : 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。</li> <li>• <b>1sec</b> : 1 秒</li> <li>• <b>10sec</b> : 10 秒</li> <li>• <b>1min</b> : 1 分</li> <li>• <b>10min</b> : 10 分</li> </ul>
デフォルト	CCM の送信間隔 : <b>10sec</b>
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)#

## 4.17.9 mip creation (MA)

mip creation (MA)	
目的	CFM MA 設定モードにおける、メンテナンス中間ポイント(MIP)作成ルールを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>mip creation {none   auto   explicit   defer}</b> <b>no mip creation</b>
パラメーター	<p><b>none</b> : 対象 MA において MIP を作成しない場合に指定します。</p> <p><b>auto</b> : 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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>対象 MA のポートに MEP が設定されていない。</li> <li>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。</li> </ul> <p><b>explicit</b> : 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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>対象 MA のポートに MEP が設定されていない。</li> <li>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。</li> </ul> <p><b>defer</b> : CFM MD 設定モードの <b>mip creation</b> 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。</p>
デフォルト	<b>defer</b>
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	<p>MA 内の中間装置では、装置上で MIP が作成できるように <b>auto</b> を指定してください。</p> <p>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。</p>
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-mal vlan 2
(config-cfm-ma)# mip creation auto
(config-cfm-ma)#
```

## 4.17.10 sender-id (MA)

sender-id (MA)	
目的	CFM MA 設定モードにおける、CFM 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	<b>sender-id</b> {none   chassis   manage   chassis-manage   defer} <b>no sender-id</b>
パラメーター	<b>none</b> : CFM パケットに Sender ID TLV を付加しない場合に指定します。 <b>chassis</b> : 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。 <b>manage</b> : 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。 <b>chassis-manage</b> : 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。 <b>defer</b> : CFM MD 設定モードの <b>sender-id</b> 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	<b>defer</b>
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 <b>sender-id</b> 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-mal 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-mal vlan 2
(config-cfm-ma)# sender-id chassis
(config-cfm-ma)#
```

## 4.17.11 cfm mep

cfm mep	
目的	メンテナンスエンドポイント (MEP) を設定します。また、CFM MEP 設定モードに遷移します。遷移後のプロンプトは (config-cfm-mep)# に変更されます。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>cfm mep mepid</b> <i>MEP-ID</i> <b>ma name</b> <i>MA-NAME</i> <b>domain</b> <i>DOMAIN-NAME</i> [ <b>direction</b> {up   down}] <b>no cfm mep mepid</b> <i>MEP-ID</i> <b>ma name</b> <i>MA-NAME</i> <b>domain</b> <i>DOMAIN-NAME</i>
パラメーター	<b>mepid</b> <i>MEP-ID</i> : MEP ID を 1~8191 の範囲で指定します。 <b>name</b> <i>MA-NAME</i> : MA 名を指定します。 <b>domain</b> <i>DOMAIN-NAME</i> : MD 名を指定します。 <b>direction</b> (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



cfm mep	
	<p>ていた MEP の CFM MEP 設定モードに遷移します。</p> <ul style="list-style-type: none"> <li>• <b>up</b> : 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。</li> <li>• <b>down</b> : 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。</li> </ul>
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	<p>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 <b>direction</b> パラメーターの指定は不要です。</p> <p>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。</p> <p>本コマンドで MEP を作成する前に、<b>mepid-list</b> コマンドで MEP ID を MA の MEP ID リストに追加してください。</p> <p>MEP は装置全体で最大 32 個まで設定できます。</p>
制限事項	<p>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。</p> <p>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。</p>
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)#
```

#### 4.17.12 mep enable

mep enable	
目的	MEP を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>mep enable</b> <b>no mep enable</b>
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	-

mep enable	
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)#
```

#### 4.17.13 ccm enable

ccm enable	
目的	MEP の Continuity Check Message (CCM) 機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>ccm enable</b> <b>no ccm enable</b>
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)#
```

#### 4.17.14 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	<b>pdu-priority</b> <i>COS-VALUE</i> <b>no pdu-priority</b>
パラメーター	<i>COS-VALUE</i> ：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	-
制限事項	-

pdu-priority	
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)#
```

#### 4.17.15 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	<b>fault-alarm</b> {none   all   mac-status   remote-ccm   error-ccm   xcon-ccm} <b>no fault-alarm</b>
パラメーター	<b>none</b> ：障害アラームを送信しない場合に指定します。 <b>all</b> ：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。 <b>mac-status</b> ：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。 <b>remote-ccm</b> ：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。 <b>error-ccm</b> ：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。 <b>xcon-ccm</b> ：「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。 <ul style="list-style-type: none"> <li>• (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。</li> <li>• 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。</li> <li>• 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。</li> <li>• DefErrorCCM：この MEP は無効な CCM を受信しています。</li> <li>• (最高) DefXconCCM：この MEP は他の MA からの CCM を受信しています。</li> </ul>
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)#
```

#### 4.17.16 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	<b>alarm-time</b> {delay <i>CENTISECOND</i>   reset <i>CENTISECOND</i> } <b>no alarm-time</b> {delay   reset}
パラメーター	<b>delay</b> <i>CENTISECOND</i> : 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。 <b>reset</b> <i>CENTISECOND</i> : 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)#
```

## 4.17.17 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	<b>ais</b> [period <i>PERIOD</i> ] [level <i>LEVEL</i> ] <b>no ais</b> [period   level]
パラメーター	<b>period</b> <i>PERIOD</i> (省略可能) : AIS Protocol Data Unit (AIS アラーム) の送信間隔を、 <b>1sec</b> (1 秒) または <b>1min</b> (1 分) で指定します。  <b>level</b> <i>LEVEL</i> (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 : <b>1sec</b> 、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)#
```

## 4.17.18 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	<b>lck</b> [period <i>PERIOD</i> ] [level <i>LEVEL</i> ] <b>no lck</b> [period   level]
パラメーター	<b>period</b> <i>PERIOD</i> (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。 <b>level</b> <i>LEVEL</i> (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)#
```

## 4.17.19 cfm mp-ltr-all

cfm mp-ltr-all	
目的	すべてのメンテナンスポイントが LTR (Link Trace Reply) を応答する機能を有効にします。無効にする場合は、no 形式のコマンドを使用します。
シンタックス	<b>cfm mp-ltr-all</b> <b>no cfm mp-ltr-all</b>
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)#
```

#### 4.17.20 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	<b>show cfm</b>
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。

#### 4.17.21 show cfm interface

show cfm interface	
目的	指定したポートの CFM 情報を表示します。
シンタックス	<b>show cfm interface</b> [ <i>INTERFACE-ID</i> [, -]]
パラメーター	<i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b>：物理ポートを指定します。複数指定できます。</li> </ul>
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	インターフェースを指定しない場合、すべてのインターフェースの CFM 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 情報を表示する方法を示します。

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

Port1/0/1 ... (1)
CFM is enabled ... (2)
MAC Address: 00-09-5A-B9-AC-1B ... (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)	インターフェース ID 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。

#### 4.17.22 show cfm domain

show cfm domain	
目的	MD 情報を表示します。
シンタックス	<code>show cfm domain DOMAIN-NAME</code>
パラメーター	<code>DOMAIN-NAME</code> : 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	-



show cfm domain	
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: opl ... (5)
MA Name: op-mal
```

項番	説明
(1)	MD 名を表示します。
(2)	ドメインレベルを表示します。
(3)	MIP の作成方法を表示します。 Auto : 自動作成 Explicit : 既存の下位の MEP が設定されているポートで MIP を作成 None : MIP を作成しない
(4)	Sender ID TLV の付加ルールを表示します。 Chassis : Chassis ID 情報を含む Sender ID TLV を付加 Chassis_manage : Chassis ID 情報と Management Address 情報を含む Sender ID TLV を付加 Manage : Management Address 情報を含む Sender ID TLV を付加 None : Sender ID TLV を付加しない
(5)	MD 内に存在する MA を表示します。

#### 4.17.23 show cfm ma

show cfm ma	
目的	MA 情報を表示します。
シンタックス	<code>show cfm ma name MA-NAME domain DOMAIN-NAME</code>
パラメーター	<code>ma name MA-NAME domain DOMAIN-NAME</code> : 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)	インターフェース ID を表示します。
(9)	サービス方向を表示します。

#### 4.17.24 show cfm mepid

show cfm mepid	
目的	MEP 情報を表示します。
シンタックス	<code>show cfm mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME</code>
パラメーター	<code>mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME</code> : 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: None ... (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)	インターフェース ID 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)	MEP の障害アラームの送信設定を表示します。 All : すべて送信する 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 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 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 Xcon CCM : 「DefXconCCM」の障害アラームだけを送信する None : 障害アラームを送信しない
(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

項番	説明
	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
(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。

#### 4.17.25 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	<b>show cfm mep fault</b>
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

show cfm mep fault	
特権レベル	レベル : 1
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

#### 4.17.26 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	<b>show cfm counter ccm</b>
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

show cfm counter ccm	
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 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)	インターフェース ID 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。

#### 4.17.27 show cfm remote-mep

show cfm remote-mep	
目的	リモート MEP 情報を表示します。
シンタックス	<code>show cfm remote-mep mepid LOCAL-MEP-ID ma name MA-NAME domain DOMAIN-NAME [remote-mepid REMOTE-MEPID]</code>
パラメーター	<code>mepid LOCAL-MEP-ID ma name MA-NAME domain DOMAIN-NAME</code> : 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。  <code>remote-mepid REMOTE-MEPID</code> (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	-

show cfm remote-mep	
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 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: 2017-07-06 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: 2017-07-06 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 (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する

項番	説明
	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。

#### 4.17.28 show cfm mip ccm

show cfm mip ccm	
目的	MIP CCM データベースエントリを表示します。
シンタックス	<b>show cfm mip ccm</b>
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数を表示します。



## 4.17.29 show cfm pkt-cnt interface

show cfm pkt-cnt interface	
目的	指定したポートのCFMパケットのRX/TXカウンターを表示します。
シンタックス	<b>show cfm pkt-cnt interface</b> [ <i>INTERFACE-ID</i> [,  -]] [ <b>rx</b> ] [ <b>tx</b> ]
パラメーター	<p><i>INTERFACE-ID</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul> <p><b>rx</b> (省略可能) : 指定したポートの受信パケット数 (RX カウンター) を表示する場合に指定します。</p> <p><b>tx</b> (省略可能) : 指定したポートの送信パケット数 (TX カウンター) を表示する場合に指定します。</p>
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、すべてのインターフェースのカウンターが表示されます。RX/TX タイプを指定した場合、すべてのポートまたは指定したポートのRXパケットカウンターまたはTXパケットカウンターが表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例 : ポート 1/0/1 の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)
    (3) (4)
    AllPkt:0          CCM:0
    (5) (6)
    LBR:0             LBM:0
    (7) (8)
    LTR:0             LTM:0
    (9) (10)
    VidDrop:0         OpcoDrop:0
  CFM TX Statistics ... (11)
    AllPkt:0          CCM:0
    LBR:0             LBM:0
    LTR:0             LTM:0
```

項番	説明
(1)	インターフェース ID 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。

項番	説明
(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 RX 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 rx

Port1/0/1 ... (1)
  CFM RX Statistics ... (2)
    (3)                (4)
    AllPkt:0          CCM:0
    (5)                (6)
    LBR:0             LBM:0
    (7)                (8)
    LTR:0             LTM:0
    (9)                (10)
    VidDrop:0         OpcoDrop:0
```

項番	説明
(1)	インターフェース ID 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 TX 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 tx

Port1/0/1 ... (1)
  CFM TX Statistics ... (2)
    (3)                (4)
    AllPkt:0          CCM:0
    (5)                (6)
    LBR:0             LBM:0
    (7)                (8)
    LTR:0             LTM:0
```

項番	説明
(1)	インターフェース ID 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。

項番	説明
(8)	LTM のパケット数を表示します。

### 4.17.30 show cfm mp-ltr-all

show cfm mp-ltr-all	
目的	すべてのメンテナンスポイントが LTR (Link Trace Reply) を応答する機能の有効/無効を表示します。
シンタックス	<b>show cfm mp-ltr-all</b>
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

### 4.17.31 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、 <b>cfm lck stop</b> コマンドを使用します。
シンタックス	<b>cfm lck start mepid</b> <i>MEP-ID</i> <b>ma name</b> <i>MA-NAME</i> <b>domain</b> <i>DOMAIN-NAME</i> <b>cfm lck stop mepid</b> <i>MEP-ID</i> <b>ma name</b> <i>MA-NAME</i> <b>domain</b> <i>DOMAIN-NAME</i>
パラメーター	<b>mepid</b> <i>MEP-ID</i> <b>ma name</b> <i>MA-NAME</i> <b>domain</b> <i>DOMAIN-NAME</i> : 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
--

#

## 4.17.32 clear cfm counter ccm

clear cfm counter ccm	
目的	すべての MEP の CCM パケットカウンタをクリアします。
シンタックス	<b>clear cfm counter ccm</b>
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：すべての MEP の CCM パケットカウンタをクリアする方法を示します。

```
# clear cfm counter ccm
#
```

## 4.17.33 clear cfm pkt-cnt interface

clear cfm pkt-cnt interface	
目的	指定したポートの CFM パケットの RX/TX カウンタをクリアします。
シンタックス	<b>clear cfm pkt-cnt interface</b> { <i>INTERFACE-ID</i> [,  -]   <b>all</b> } [ <b>rx</b> ] [ <b>tx</b> ]
パラメーター	<p><i>INTERFACE-ID</i> : カウンタ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。</p> <ul style="list-style-type: none"> <li><b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul> <p><b>all</b> : すべてのインターフェースの CFM カウンタをクリアする場合に指定します。</p> <p><b>rx</b> (省略可能) : 指定したポートの受信パケット数 (RX カウンタ) をクリアする場合に指定します。</p> <p><b>tx</b> (省略可能) : 指定したポートの送信パケット数 (TX カウンタ) をクリアする場合に指定します。</p>
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	ポートだけを指定した場合、指定したポートの RX パケットカウンタと TX パケットカウンタの両方がクリアされます。ポートと RX/TX タイプの両方を指定した場合、指定したポートの RX パケットカウンタまたは TX パケットカウンタがクリアされます。
制限事項	-
注意事項	-

## 4.17.34 cfm loopback test

cfm loopback test	
目的	CFM ループバックテストを実施します。

cfm loopback test	
シンタックス	<code>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]</code>
パラメーター	<p><b>MAC-ADDRESS</b> : 宛先 MAC アドレスを、以下のいずれかの形式で指定します。</p> <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul> <p><b>remote-mepid REMOTE-MEPID</b> : 宛先 MEP ID を指定します。</p> <p><b>mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME</b> : LBM (Loop Back Message) を送信する MEP ID を 1~8191 の範囲で指定し、所属する MA 名と MD 名を指定します。</p> <p><b>num NUMBER</b> (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。</p> <p><b>length LENGTH</b> (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。</p> <p><b>pattern STRING</b> (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。</p> <p><b>pdu-priority COS-VALUE</b> (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。</p>
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	<p>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。</p> <p>マルチキャストループバック機能を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。</p> <p>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。</p>
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).
```

### 4.17.35 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	<b>cfm linktrace</b> <i>MAC-ADDRESS</i> <b>mepid</b> <i>MEP-ID</i> <b>ma name</b> <i>MA-NAME</i> <b>domain</b> <i>DOMAIN-NAME</i> [ <b>ttl</b> <i>TTL</i> ] [ <b>pdu-priority</b> <i>COS-VALUE</i> ]
パラメーター	<p><i>MAC-ADDRESS</i> : 宛先 MAC アドレスを、以下のいずれかの形式で指定します。</p> <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul> <p><b>mepid</b> <i>MEP-ID</i> <b>ma name</b> <i>MA-NAME</i> <b>domain</b> <i>DOMAIN-NAME</i> : 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。</p> <p><b>ttl</b> <i>TTL</i> (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。</p> <p><b>pdu-priority</b> <i>COS-VALUE</i> (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。</p>
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 <b>show cfm linktrace</b> 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
```

## 4.17.36 show cfm linktrace

show cfm linktrace	
目的	CFM リンクトレース結果を表示します。
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
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	MEP ID を指定しない場合、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 (Link Trace Message) の送信元 MEP ID と、宛先 MAC アドレスを表示します。
(3)	CFM リンクトレースを実施日時を表示します。
(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 : フィルタリングデータベースによって、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

項番	説明
	Hit : LTM の宛先と一致するメンテナンスポイントに到達
(9)	宛先の MEP ID を表示します。

### 4.17.37 clear cfm linktrace

clear cfm linktrace	
目的	CFM リンクトレースの実施結果を削除します。
シンタックス	<code>clear cfm linktrace {mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME   all}</code>
パラメーター	<code>mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME</code> : CFM リンクトレース結果を削除する MEP ID を 1~8191 の範囲で指定し、所属する MA 名と MD 名を指定します。 <code>all</code> : 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
#
```

対象バージョン	1.01.01
---------	---------

使用例 : ポート 1/0/1 の TX パケット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
#
```



## 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イ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	<b>mac-address-table aging-time SECONDS</b> <b>no mac-address-table aging-time</b>
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 秒に設定するとエイ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。

<pre># configure terminal (config)# mac-address-table aging-time 200 (config)#</pre>
--

### 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	<b>mac-address-table aging destination-hit</b> <b>no mac-address-table aging destination-hit</b>
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。

<pre># configure terminal (config)# mac-address-table aging destination-hit (config)#</pre>
---

### 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	<b>mac-address-table learning interface <i>INTERFACE-ID</i> [,  -]</b> <b>no mac-address-table learning interface <i>INTERFACE-ID</i> [,  -]</b>
パラメーター	<b>interface <i>INTERFACE-ID</i></b> ：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。 <ul style="list-style-type: none"> <li>• <b>port</b>：物理ポートを指定します。複数指定できます。</li> </ul>
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	<pre>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] [, -]}</pre>
パラメーター	<p><b>MAC-ADDRESS</b>：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。</p> <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul> <p><b>vlan VLAN-ID</b>：追加するエントリーの VLAN ID を 1～4094 の範囲で指定します。</p> <p><b>interface INTERFACE-ID</b>：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。</p> <ul style="list-style-type: none"> <li>• <b>port</b>：物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b>：ポートチャネルを指定します。</li> </ul> <p><b>drop</b>：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。</p> <p><b>all</b>：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。</p>
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	<p>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。</p> <p>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。</p> <p>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。</p>

mac-address-table static	
	<p>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。</p> <p>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。</p>
制限事項	<p>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。</p> <ul style="list-style-type: none"> <li>ユニキャスト MAC アドレス : 256 エントリー</li> <li><b>drop</b> パラメーターを指定した MAC アドレス : 256 エントリー</li> <li>マルチキャスト MAC アドレス : 128 エントリー</li> </ul> <p>レイヤー3 中継後のトラフィックは、<b>drop</b> 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。</p>
注意事項	<p>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。</p>
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ンネル 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	<b>show mac-address-table</b> [dynamic   static] [address <i>MAC-ADDRESS</i>   interface <i>INTERFACE-ID</i>   vlan <i>VLAN-ID</i> ]
パラメーター	<p><b>dynamic</b> (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。</p> <p><b>static</b> (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。</p> <p><b>address</b> <i>MAC-ADDRESS</i> (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。</p>

show mac-address-table	
	<ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul> <p><b>interface</b> <i>INTERFACE-ID</i> (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イスを、以下のパラメーターで指定します。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul> <p><b>vlan</b> <i>VLAN-ID</i> (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。</p>
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、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イ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イ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イ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	<b>show mac-address-table learning</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースの MAC アドレス学習状態が表示されます。
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 アドレスエントリを消去します。
シンタックス	<b>clear mac-address-table dynamic</b> { <b>all</b>   <b>address</b> <i>MAC-ADDRESS</i>   <b>interface</b> <i>INTERFACE-ID</i>   <b>vlan</b> <i>VLAN-ID</i> }
パラメーター	<b>all</b> : すべてのダイナミック MAC アドレスエントリを消去する場合に指定します。 <b>address</b> <i>MAC-ADDRESS</i> : 消去するダイナミック MAC アドレスエントリを、以下のいずれかの形式で指定します。 <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> </ul>

clear mac-address-table	
	<ul style="list-style-type: none"> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul> <p><b>interface</b> <i>INTERFACE-ID</i>: 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。</p> <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。</li> <li>• <b>port-channel</b>: ポートチャネルを指定します。</li> </ul> <p><b>vlan</b> <i>VLAN-ID</i>: 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。</p>
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	<b>max-rcv-frame-size</b> BYTES <b>no max-rcv-frame-size</b>
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	ApresiaNP4000 シリーズでは最大 9216 バイトまでサポートしています。
注意事項	フレームの形式 (タグなし/タグ付き) にかかわらず、宛先 MAC アドレス~FCS が「設定値+4 バイト」のサイズまで送受信できます。
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 {dst-ip   dst-mac   src-dst-ip   src-dst-mac   src-ip   src-mac   dst-l4-port   src-dst-l4-port   src-l4-port} no port-channel load-balance
show channel-group	show channel-group [channel [CHANNEL-NO] {detail   neighbor}   load-balance   sys-id]

### 5.3.1 channel-group

channel-group	
目的	インターフェースをチャンネル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	<b>channel-group</b> CHANNEL-NO mode {on   active   passive} <b>no channel-group</b>
パラメーター	<p><b>CHANNEL-NO</b>: チャンネルグループ ID を 1~48 の範囲で指定します。ただし、LACP が使用できるチャンネルグループ ID は、1~48 の任意な ID を指定できますが、LACP として割り当て可能なチャンネルグループ数は 32 個までです。例えば、LACP で 32 個割り当てた場合、残りの 16 個はスタティックなチャンネルグループとして使用可能です。</p> <p><b>on</b>: インターフェースがチャンネルグループのスタティックなメンバーの場合に指定します。</p> <p><b>active</b>: インターフェースを LACP アクティブモードで動作させる場合に指定します。</p> <p><b>passive</b>: インターフェースを LACP パッシブモードで動作させる場合に指定します。</p>
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	<p>インターフェースが参加できるチャンネルグループは 1 つだけです。</p> <p>チャンネルグループに割り当て可能なメンバーポートの最大数は 8 ポートです。</p> <p>on モードを指定すると、チャンネルグループタイプはスタティックとなります。アクティブモードまたはパッシブモードを指定すると、チャンネルグループタイプ</p>

channel-group	
	<p>は LACP となります。チャンネルグループは、スタティックメンバーと LACP メンバーのどちらかだけで構成されます。チャンネルグループのタイプが一度決定されると、チャンネルタイプには、他のタイプのインターフェースは参加できません。</p> <p>チャンネルグループからインターフェースを削除する場合は、<b>no</b> 形式のコマンドを実行します。ポートの削除後、チャンネルグループにメンバーポートが存在しなくなると、チャンネルグループは自動的に削除されます。ポートチャネルは、<b>no interface port-channel</b> コマンドで削除することもできます。</p>
制限事項	-
注意事項	<p>ERPS のリングポートとして使用中のチャンネルグループは削除しないでください。</p> <p>チャンネルグループへの割り当てを行う場合は、インターフェース指定時に <b>interface range port</b> コマンドを使用せずに <b>interface port</b> コマンドを使用してください。</p> <p>LACP と LLDP 疑似リンクダウン機能をポートで併用することはできません。</p>
対象バージョン	1.01.01

使用例：ポート 1/0/4 を ID 3 として新しい LACP チャンネルグループに割り当て、LACP モードをアクティブに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	ポート優先度を設定します。デフォルト設定に戻すには、 <b>no</b> 形式のコマンドを使用します。
シンタックス	<b>lacp port-priority PRIORITY</b> <b>no lacp port-priority</b>
パラメーター	<i>PRIORITY</i> ：ポート優先度を 1～65,535 の範囲で指定します。
デフォルト	32768
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	どのポートをポートチャネルに参加させて、どのポートをスタンドアロンモードにするかを決定するコマンドです。値が小さいほど優先度は高くなります。複数のポートで優先度が同じ場合は、ポート番号で優先度を決定します。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ポート 1/0/4 からポート 1/0/5 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 range port 1/0/4-1/0/5
(config-if-port-range)# lacp port-priority 20000
(config-if-port-range)#
```

## 5.3.3 lacp timeout

lacp timeout	
目的	LACP のロングタイマーまたはショート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	<b>lacp timeout {short   long}</b> <b>no lacp timeout</b>
パラメーター	<b>short</b> : 受信した LACPDU 情報を 3 秒後に無効にする場合に指定します。short を指定すると、LACPDU の定期送信の間隔は 1 秒になります。 <b>long</b> : 受信した LACPDU 情報を 90 秒後に無効にする場合に指定します。long を指定すると、LACPDU の定期送信の間隔は 30 秒になります。
デフォルト	long
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、ポートの LACP タイムアウトをショート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)# lacp timeout short
(config-if-port)#
```

## 5.3.4 lacp system-priority

lacp system-priority	
目的	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	<b>lacp system-priority PRIORITY</b> <b>no lacp system-priority</b>
パラメーター	<b>PRIORITY</b> : 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	32768
コマンドモード	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 ネゴシエーションの間、ローカルパートナーのシステム優先度とポート優先度が、リモートパートナーとの間で交換されます。値が小さいほど優先度は高くなります。2 つの装置のシステム優先度が同じ場合は、LACP システム ID (MAC) によって優先度が決定されます。 <b>lacp system-priority</b> コマンドは、装置上のすべての LACP ポートチャネルに適用されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例 : LACP システム優先度を 30000 に設定する方法を示します。

```
# configure terminal
(config)# lacp system-priority 30000
(config)#
```

## 5.3.5 port-channel load-balance

port-channel load-balance	
目的	同じチャネルの複数のポートにパケットを分散させるために、装置が使用する負荷バランスの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 {dst-ip   dst-mac   src-dst-ip   src-dst-mac   src-ip   src-mac   dst-l4-port   src-dst-l4-port   src-l4-port} no port-channel load-balance
パラメーター	dst-ip : 宛先 IP アドレスによる負荷分散を行う場合に指定します。 dst-mac : 宛先 MAC アドレスによる負荷分散を行う場合指定します。 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を行う場合に指定します。 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を行う場合に指定します。 src-ip : 送信元 IP アドレスによる負荷分散を行う場合に指定します。 src-mac : 送信元 MAC アドレスによる負荷分散を行う場合に指定します。 dst-l4-port : 宛先レイヤー4 TCP/UDP ポートによる負荷分散を行う場合に指定します。 src-dst-l4-port : 送信元レイヤー4 TCP/UDP ポートと宛先レイヤー4 TCP/UDP ポートによる負荷分散を行う場合に指定します。 src-l4-port : 送信元レイヤー4 TCP/UDP ポートによる負荷分散を行う場合に指定します。
デフォルト	src-dst-mac
コマンドモード	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	選択できるアルゴリズムは1つだけです。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：負荷バランスアルゴリズムに src-ip を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	チャネルグループ情報を表示します。
シンタックス	show channel-group [channel [CHANNEL-NO]] {detail   neighbor}   load-balance   sys-id]
パラメーター	channel (省略可能) : ポートチャネルのチャネルグループ情報を表示する場合に指定します。

show channel-group	
	<p><i>CHANNEL-NO</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>detail</b> : チャネルグループ情報の詳細を表示する場合に指定します。</li> <li>• <b>neighbor</b> : ネイバー情報を表示する場合に指定します。</li> </ul> <p><b>load-balance</b> (省略可能) : 負荷分散情報を表示する場合に指定します。</p> <p><b>sys-id</b> (省略可能) : LACP で使用されるシステム識別子を表示する場合に指定します。</p>
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	ポートチャネル番号を指定しない場合、すべてのポートチャネルが表示されず。 <b>channel</b> 、 <b>load-balance</b> 、 <b>sys-id</b> パラメーターを指定しない場合、チャネルグループのサマリー情報だけが表示されます。
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)
Port         Flags      State      Priority    Port
-----
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、最大ポート数、およびプロトコルを表示します。
(5)	メンバーポートを表示します。
(6)	フラグを表示します。
(7)	LACP の状態を表示します。
(8)	ポート優先度を表示します。
(9)	ポート番号を表示します。

## 5 レイヤー2 | 5.3 ポートチャネルコマンド

使用例：ポートチャネル3に関するネイバー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)
  Port         Partner      Partner    Partner    Partner
             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)	チャンネルグループ ID を表示します。
(3)	装置のメンバーポートを表示します。
(4)	ネイバーのシステム識別子を表示します。
(5)	ネイバーのポート番号を表示します。
(6)	ネイバーのフラグを表示します。
(7)	ネイバーのポート優先度を表示します。

使用例：すべてのチャンネルグループに関する負荷バランス情報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)	装置が使用する負荷バランスのアルゴリズムを表示します。

使用例：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)	システム識別子を表示します。

使用例：すべてのポートチャネルに関するサマリー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)	装置が使用する負荷分散のアルゴリズムを表示します。

## 5 レイヤー2 | 5.3 ポートチャネルコマンド

項番	説明
(2)	システム識別子を表示します。
(3)	チャンネルグループ ID を表示します。
(4)	プロトコルを表示します。



## 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	<b>redundant group-number REDUNDANT-NO {primary   secondary}</b> <b>no redundant group-number</b>
パラメーター	<b>REDUNDANT-NO</b> : リダンダントグループ ID を 1～32 の範囲で指定します。 <b>primary</b> : Primary ポートに指定します。 <b>secondary</b> : 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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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 ( <b>loop-detection action notify-only</b> 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	1.02.01

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	<b>redundant group-number REDUNDANT-NO preempt {disable   delay SECONDS}</b> <b>no redundant group-number REDUNDANT-NO preempt</b>
パラメーター	<i>REDUNDANT-NO</i> ：リダンダントグループ ID を 1～32 の範囲で指定します。 <i>SECONDS</i> ：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。 <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
制限事項	-
注意事項	-
対象バージョン	1.02.01

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時に、MAC アドレス再学習フレームを送信する機能を設定します。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。

redundant mac-address-table-update	
シンタックス	<b>redundant mac-address-table-update count</b> <i>COUNT</i> <b>no redundant mac-address-table-update</b>
パラメーター	<i>COUNT</i> : 送信回数を 1~3 の範囲で指定します。
デフォルト	0 (再学習フレームの送信をしない)
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	-
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	1.02.01

使用例: Active 状態のポートが切り替わる時に、MAC アドレス再学習フレームを送信する回数を 3 回に設定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時に、FDB フラッシュフレームを送信する機能を設定します。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	<b>redundant fdb-flush send enable count</b> <i>COUNT</i> <b>no redundant fdb-flush send enable</b>
パラメーター	<i>COUNT</i> : 送信回数を 1~3 の範囲で指定します。
デフォルト	0 (FDB フラッシュフレームの送信をしない)
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	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、 <b>redundant fdb-flush receive enable</b> 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、本装置の MAC アドレスであり、EtherType は 0x8820 です。  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	-
対象バージョン	1.02.01

使用例: FDB フラッシュフレームの送信を有効にして、送信回数を 3 回に設定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設定します。デフ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	<b>redundant fdb-flush receive enable</b> <b>no redundant fdb-flush receive enable</b>
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 <b>redundant fdb-flush dst-mac</b> 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	-
対象バージョン	1.02.01

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	<b>redundant fdb-flush vid <i>VLAN-ID</i></b> <b>no redundant fdb-flush vid</b>
パラメーター	<i>VLAN-ID</i> : FDB フラッシュフレームの VLAN タグの VLAN ID
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	1.02.01

使用例：FDB フラッシュフレームの VLAN タグの 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	<b>redundant fdb-flush dst-mac</b> <i>MAC-ADDRESS</i> <b>no redundant fdb-flush dst-mac</b>
パラメーター	<i>MAC-ADDRESS</i> : 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。 <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul>
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	1.02.01

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	<b>show redundant</b> [ <i>portbase</i> ]
パラメーター	<b>portbase</b> (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	1.02.01

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)
(6) C Pre Port
      1      8 9      16 17      24
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、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"はスタックのボックス ID (シャーシ ID) を示します。スタックを構成していない場合は 1 が表示されます。 "Pre"はプリエンプトモードの設定を表示します。- (プリエンプトモード有効でディレイ時間 0 秒設定)、1~300(プリエンプトモード有効で設定したディレイ時間を表示)、Dis (プリエンプトモード無効)が表示されます。

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  Down    1      Primary
Port1/0/2  Down    1      Secondary
    
```

項番	説明
(1)	ポートリダンダントを設定したインターフェース ID 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 <i>INSTANCE-ID</i> track-port interface <i>INTERFACE-ID</i> [,  -] relay-port interface <i>INTERFACE-ID</i> [,  -] no link-relay id <i>INSTANCE-ID</i>
パラメーター	id <i>INSTANCE-ID</i> : 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 <i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>port: 物理ポートを指定します。複数指定できます。</li> </ul> relay-port interface <i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>port: 物理ポートを指定します。複数指定できます。</li> </ul>
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	<p>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。</p> <p>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。</p> <p>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</p>

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	1.01.01

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	<b>show link-relay</b>
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
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"はスタックのボックス ID (シャーン ID) を示します。スタックを構成していない場合は 1 が表示されます。



## 5.5.3 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	1.01.01

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	<p>ループ検知機能 (<b>loop-detection action notify-only</b> 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。</p> <p>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 <b>loop-detection action notify-only</b> コマンドを設定してください。</p> <p>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、<b>loop-detection mode</b> 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 <b>loop-detection action notify-only</b> コマンドを設定してください。</p>

loop-detection global enable	
注意事項	-
対象バージョン	1.01.01

使用例：ポートベースのループ検知機能をグローバルに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	<b>loop-detection enable</b> <b>no loop-detection enable</b>
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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> コマンド) で設定してください。
制限事項	ループ検知機能 ( <b>loop-detection action notify-only</b> 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、ポートチャンネル) 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 <b>loop-detection action notify-only</b> 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、ポートチャンネル) 上で MMRP-Plus、ERPS、MSTP、RPVST+機能と併用する場合は、 <b>loop-detection mode</b> 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 <b>loop-detection action notify-only</b> コマンド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 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	ループ検知のタイマー間隔を設定します。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	<b>loop-detection interval SECONDS</b> <b>no loop-detection interval</b>
パラメーター	<b>interval SECONDS</b> : ループ検知フレームの送信間隔を 1~32767 秒の範囲で指定

loop-detection interval	
	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	<code>loop-detection mode {port-based   vlan-based}</code> <code>no loop-detection mode</code>
パラメーター	<b>port-based</b> : ポートベースモードにする場合に指定します。 <b>vlan-based</b> : 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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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) がシャットダウン (err-disabled 状態に変更) されます。</li> </ul> <p>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。</p>

loop-detection mode	
	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li><b>errdisable recovery cause loop-detection</b> 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。</li> <li>ポートに対して <b>shutdown</b> コマンドを実行した後、<b>no shutdown</b> 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。</li> </ul>
制限事項	<p>ループ検知可能な VLAN 数は、装置全体で最大 100 個です。</p> <p>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。</p>
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	<pre>loop-detection vlan VLAN-LIST [, -] no loop-detection vlan VLAN-LIST [, -]</pre>
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

loop-detection vlan	
	から特定の VLAN ID を削除したい場合は、 <b>no loop-detection vlan</b> 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 <b>no loop-detection vlan</b> コマンドを実行するか、もしくは <b>loop-detection vlan 1-4094</b> 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	<b>loop-detection action notify-only</b> <b>no loop-detection action notify-only</b>
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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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 <b>loop-detection interval</b> 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ンネルで設定する場合は、先にポートチャン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ン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	1.02.01

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	<code>loop-detection no-check-src</code> <code>no loop-detection no-check-src</code>
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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <code>interface port-channel</code> 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ンネルで設定する場合は、先にポートチャン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ン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	1.02.01

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	<code>errdisable recovery cause loop-detection [interval SECONDS]</code> <code>no errdisable recovery cause loop-detection [interval]</code>
パラメーター	<code>interval SECONDS</code> (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、5~86400 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。

errdisable recovery cause loop-detection	
	<p>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。</p> <p>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、<b>show interfaces</b> コマンドでは “link status is down (error disabled: Loop Detection)” と表示されます。また、<b>show interfaces status</b> コマンドの Status 項目では “err-disabled” と表示されません。</p> <p>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 <b>shutdown</b> コマンドを実行した後、<b>no shutdown</b> 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。</p>
制限事項	本コマンドの設定は、構成情報ではエラー復旧コマンド関連で表示されます。(ラベル: # ERRDISABLE)
注意事項	<b>interval</b> 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 <b>interval</b> 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	<b>show loop-detection</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<p><b>interface</b> <i>INTERFACE-ID</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。</li> <li>• <b>range port</b>: 物理ポートを範囲で指定します。</li> <li>• <b>port-channel</b>: ポートチャンネルを指定します。</li> </ul>
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、すべてのインターフェースのループ検知機能の設定が表示されます。
制限事項	-
注意事項	noChkSrc 項目と Action 項目は AEOS-NP4000 Ver. 1.02.01 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 1.02.01: 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)	インターフェース ID 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)	インターフェース ID 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。

項番	説明
(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)	インターフェース ID 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]
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	<p><b>broadcast</b> : ブロードキャストを対象にする場合に指定します。</p> <p><b>multicast</b> : マルチキャストを対象にする場合に指定します。</p> <p><b>unicast</b> : 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。</p> <p><b>level pps PPS-RISE [PPS-LOW]</b> : しきい値を 1 秒あたりの受信フレーム数で指定します。</p> <ul style="list-style-type: none"> <li>• PPS-RISE : 上限値を 0~2147483647 の範囲で指定します。</li> <li>• PPS-LOW (省略可能) : 下限値を 0~2147483647 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。</li> </ul> <p><b>level kbps KBPS-RISE [KBPS-LOW]</b> : 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/解消を示すログは出力されません。</p> <ul style="list-style-type: none"> <li>• KBPS-RISE : 上限値を 0~2147483647 の範囲で 64Kbps 単位で指定します。</li> <li>• KBPS-LOW (省略可能) : 下限値を 0~2147483647 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。</li> </ul> <p><b>level LEVEL-RISE [LEVEL-LOW]</b> : しきい値をポートの総帯域幅に対するパーセン</p>

storm-control	
	<p>ページで指定します。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／解消を示すログは出力されません。</p> <ul style="list-style-type: none"> <li>• <i>LEVEL-RISE</i> : 上限値を 0~100 の範囲で指定します。</li> <li>• <i>LEVEL-LOW</i> (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 <i>LEVEL-RISE</i> の 80%の値となります。</li> </ul>
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	<p>アクションが <b>drop</b> 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。</p> <p>アクションが <b>shutdown</b> 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。</p> <p>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。</p>
制限事項	<p>ApresiaNP4000 シリーズでは、ポートチャンネルでストームコントロールを設定できません。また、ポートチャンネルのメンバーポートでも設定できません。</p> <p>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。</p> <p>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 <b>shutdown</b> は設定できません。</p> <p>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／解消を示すログは出力されません。</p> <p>アクションに <b>drop</b> もしくは <b>none</b> を指定した場合は、Unicast に関するストームの検知／解消を示すログは出力されません。</p>
注意事項	-
対象バージョン	1.01.01

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)#
```

### 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	<b>storm-control action {shutdown   drop   none}</b> <b>no storm-control action</b>
パラメーター	<b>shutdown</b> : 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) する場合に指定します。

storm-control action	
	<p><b>drop</b> : 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する場合に指定します。</p> <p><b>none</b> : 上限値を超えると、ログのみ出力する場合に指定します。</p>
デフォルト	帯域制限動作 ( <b>drop</b> )
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	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>errdisable recovery cause storm-control</b> 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。</li> <li>• ポートに対して <b>shutdown</b> コマンドを実行した後、<b>no shutdown</b> 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。</li> </ul>
制限事項	<p>ApresiaNP4000 シリーズでは、ポートチャネルでストームコントロールを設定できません。また、ポートチャネルのメンバーポートでも設定できません。</p> <p>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 <b>shutdown</b> は設定できません。</p> <p>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/解消を示すログは出力されません。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• アクションが <b>drop</b> 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、<b>show storm-control</b> コマンドやログ出力では multicast パラメーターの対象として扱いますが、帯域制限動作だけは broadcast パラメーターの対象として扱われる仕様制限があります。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• アクションが <b>drop</b> または <b>none</b> 設定の場合、ストームの検知/解消を示すログは出力されません。</li> <li>• アクションが <b>shutdown</b> 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。</li> </ul>
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)#
```

## 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 <i>SECONDS</i> no storm-control polling interval
パラメーター	<i>SECONDS</i> : 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 { <i>NUMBER</i>   infinite} no storm-control polling retries
パラメーター	<i>NUMBER</i> : 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。  <i>infinite</i> : 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、5~86400 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	<p>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。</p> <p>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。</p> <p>err-disabled 状態にされたポートのリンク状態は、<b>show interfaces</b> コマンドでは "link status is down (error disabled: Storm Control)" と表示されます。また、<b>show interfaces status</b> コマンドの Status 項目では "err-disabled" と表示されます</p> <p>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 <b>shutdown</b> コマンドを実行した後、<b>no shutdown</b> 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。</p>
制限事項	本コマンドの設定は、構成情報ではエラー復旧コマンド関連で表示されます。(ラベル : # ERRDISABLE)
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 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	<p>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。</p> <ul style="list-style-type: none"> <li>port : 物理ポートを指定します。</li> <li>range port : 物理ポートを範囲で指定します。</li> </ul> <p>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。</p>

show storm-control	
	<p><b>multicast</b> (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。</p> <p><b>unicast</b> (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。</p>
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 <b>drop</b> 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

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)	インターフェース ID 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。 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)



項番	説明
	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)	インターフェース ID 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	<b>forward-all</b> : 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。 <b>forward-unregistered</b> : 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。 <b>filter-unregistered</b> : 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する forward-unregistered: マルチキャスト転送テーブルに基づいて、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する filter-unregistered: マルチキャスト転送テーブルに基づいて、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する

## 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 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

コマンド	コマンドとパラメーター
ip igmp snooping minimum-version	ip igmp snooping minimum-version {2   3} no ip igmp snooping minimum-version

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}

### 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	<b>ip igmp snooping</b> <b>no ip igmp snooping</b>
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 <b>ip igmp snooping</b> 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 <b>ip igmp snooping</b> 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：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	<b>ip igmp snooping</b> <b>no ip igmp snooping</b>
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 <b>ip igmp snooping</b> 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 <b>ip igmp snooping</b> 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	<b>ip igmp snooping dyn-mr-aging-time SECONDS</b> <b>no ip igmp snooping dyn-mr-aging-time</b>
パラメーター	<i>SECONDS</i> : 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	<b>ip igmp snooping fast-leave</b> <b>no ip igmp snooping fast-leave</b>
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	-
制限事項	-
注意事項	<p>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。</p> <ul style="list-style-type: none"> <li>装置が代表クエリアの場合の計算式 : Last member query interval × Robustness value</li> <li>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</li> </ul> <p>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。</p>
対象バージョン	1.01.01

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	<b>ip igmp snooping ignore-topology-change-notification</b> <b>no ip igmp snooping ignore-topology-change-notification</b>
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。

ip igmp snooping ignore-topology-change-notification	
	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、スパン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	<b>ip igmp snooping last-member-query-interval</b> <i>SECONDS</i> <b>no ip igmp snooping last-member-query-interval</b>
パラメーター	<i>SECONDS</i> : 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	<b>ip igmp snooping mrouter</b> [ <b>forbidden</b> ] <b>interface</b> <i>INTERFACE-ID</i> [,   -]



ip igmp snooping mrouter	
	<b>no ip igmp snooping mrouter [forbidden] interface <i>INTERFACE-ID</i> [, -]</b>
パラメーター	<p><b>forbidden</b> (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。</p> <p><b>interface <i>INTERFACE-ID</i></b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	<p>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ンネルを指定して設定します。</p> <p>マルチキャストルーターポートとしてポートチャンネルを指定する場合は、<b>interface port-channel</b> パラメーターで指定してください。ポートチャン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。</p> <p>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。</p>
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ン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。
シンタックス	<b>ip igmp snooping proxy-reporting [source <i>IP-ADDRESS</i>]</b> <b>no ip igmp snooping proxy-reporting</b>
パラメーター	<b>source <i>IP-ADDRESS</i></b> (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	<b>source <i>IP-ADDRESS</i></b> 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

ip igmp snooping proxy-reporting	
	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ター機能を有効にして、プロキシレポーター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	<b>ip igmp snooping querier</b> <b>no ip igmp snooping querier</b>
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	<b>ip igmp snooping query-interval SECONDS</b> <b>no ip igmp snooping query-interval</b>
パラメーター	<i>SECONDS</i> ：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

ip igmp snooping query-interval	
	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	<b>ip igmp snooping query-max-response-time SECONDS</b> <b>no ip igmp snooping query-max-response-time</b>
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	<b>ip igmp snooping query-version {1   2   3}</b> <b>no ip igmp snooping query-version</b>
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。

ip igmp snooping query-version	
	<p>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。</p> <p>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。</p>
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	<p><b>ip igmp snooping report-suppression</b></p> <p><b>no ip igmp snooping report-suppression</b></p>
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	-
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	<code>ip igmp snooping robustness-variable VALUE</code> <code>no ip igmp snooping robustness-variable</code>
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	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>Group member interval</b>: 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。 <ul style="list-style-type: none"> <li>• 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)</li> </ul> </li> <li>• <b>Other querier present interval</b>: 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。 <ul style="list-style-type: none"> <li>• 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)</li> </ul> </li> <li>• <b>Last member query count</b>: 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。</li> </ul> <p>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。</p>
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は、no 形式のコマンドを使用します。
シンタックス	<code>ip igmp snooping static-group GROUP-ADDRESS interface INTERFACE-ID [,  -]</code> <code>no ip igmp snooping static-group GROUP-ADDRESS [interface INTERFACE-ID [,  -]]</code>
パラメーター	<p>GROUP-ADDRESS: IP マルチキャストグループアドレスを指定します。</p> <p>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。</p>

ip igmp snooping static-group	
	<ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャネルを指定します。</li> </ul>
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	<b>ip igmp snooping suppression-time SECONDS</b> <b>no ip igmp snooping suppression-time</b>
パラメーター	<i>SECONDS</i> : 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	<b>ip igmp snooping minimum-version {2   3}</b> <b>no ip igmp snooping minimum-version</b>
パラメーター	<b>2</b> : IGMPv1 メッセージを除去する場合に指定します。

ip igmp snooping minimum-version	
	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 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	<b>show ip igmp snooping</b> [vlan <i>VLAN-ID</i> [,  -]]
パラメーター	<b>vlan</b> <i>VLAN-ID</i> (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)
```

VLAN #1 configuration	
IGMP snooping state	: Enabled ... (3)
Minimum version	: v3 ... (4)
Fast leave	: Enabled (host-based) ... (5)
Report suppression	: Enabled ... (6)
Suppression time	: 10 seconds ... (7)
Querier state	: Enabled (Non-active) ... (8)
Query version	: v3 ... (9)
Query interval	: 125 seconds ... (10)
Max response time	: 10 seconds ... (11)
Robustness value	: 2 ... (12)
Last member query interval	: 1 seconds ... (13)
Proxy reporting	: Enabled (Source 1.2.3.4) ... (14)
Ignore topology change	: Disabled ... (15)
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)	VLAN 上の IGMP 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 IGMP ホストの最小バージョンを表示します。
(5)	IGMP スヌーピングの高速離脱機能の有効/無効設定を表示します。 Enabled (host-based) : 高速離脱が有効 Disabled (host-based) : 高速離脱が無効
(6)	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。
(7)	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。
(8)	IGMP クエリア機能の有効/無効を表示します。
(9)	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。
(10)	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。
(11)	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。
(12)	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。
(13)	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。
(14)	IGMP スヌーピングのプロキシレポート機能の有効/無効を表示します。
(15)	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。

### 5.9.19 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	<b>show ip igmp snooping groups</b> [vlan <i>VLAN-ID</i> [,  -]   <i>GROUP-ADDRESS</i> ]
パラメーター	<b>vlan</b> <i>VLAN-ID</i> (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。  <i>GROUP-ADDRESS</i> (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



show ip igmp snooping groups	
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	-
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)	インターフェース ID を表示します。

### 5.9.20 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	<b>show ip igmp snooping mrouter</b> [vlan <i>VLAN-ID</i> [,  -]]
パラメーター	<b>vlan</b> <i>VLAN-ID</i> (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)	ポート番号を表示します。

### 5.9.21 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	<b>show ip igmp snooping statistics</b> { <b>interface</b> [ <i>INTERFACE-ID</i> [, -]]   <b>vlan</b> [ <i>VLAN-ID</i> [, -]]}
パラメーター	<p><b>interface</b> : 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。</p> <p><i>INTERFACE-ID</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul> <p><b>vlan</b> : VLAN の IGMP スヌーピング統計情報を表示する場合に指定します。</p> <p><i>VLAN-ID</i> (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。</p>
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	<p>インターフェースを指定しない場合、すべてのインターフェースの IGMP スヌーピングの統計情報が表示されます。</p> <p>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 スヌーピングの統計情報が表示されます。</p>
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。

<pre># show ip igmp snooping statistics vlan 1  VLAN 1 Statistics: ... (1)   IGMPv1 Rx: Report 0, Query 0   IGMPv2 Rx: Report 0, Query 0, Leave 1   IGMPv3 Rx: Report 1, Query 0   IGMPv1 Tx: Report 0, Query 0</pre>
---

IGMPv2 Tx: Report 0, Query 0, Leave 0 IGMPv3 Tx: Report 0, Query 0
Total Entries: 1

項番	説明
(1)	VLAN の IGMP スヌーピングの統計情報を表示します。

### 5.9.22 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	<b>show ip igmp snooping static-group</b> [ <i>GROUP-ADDRESS</i>   <b>vlan</b> <i>VLAN-ID</i> [, -]]
パラメーター	<i>GROUP-ADDRESS</i> (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。  <b>vlan</b> <i>VLAN-ID</i> (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)	インターフェース ID を表示します。

### 5.9.23 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。
シンタックス	<b>clear ip igmp snooping groups</b> {all   <i>GROUP-ADDRESS</i> [ <b>vlan</b> <i>VLAN-ID</i> ]}
パラメーター	<b>all</b> : 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。  <i>GROUP-ADDRESS</i> : 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

clear ip igmp snooping groups	
	<p>プのグループ IP アドレスを指定します。</p> <p><b>vlan</b> <i>VLAN-ID</i> (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。</p>
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
#
```

### 5.9.24 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クリアします。
シンタックス	<code>clear ip igmp snooping statistics {all   vlan <i>VLAN-ID</i>   interface <i>INTERFACE-ID</i>}</code>
パラメーター	<p><b>all</b> : すべての VLAN とすべてのポートの IGMP スヌーピングの統計情報をクリアする場合に指定します。</p> <p><b>vlan</b> <i>VLAN-ID</i> : IGMP スヌーピングの統計情報をクリアする VLAN を指定します。</p> <p><b>interface</b> <i>INTERFACE-ID</i> : IGMP スヌーピングの統計情報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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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クリアする方法を示します。

```
# clear ip igmp snooping statistics 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 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

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}

### 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	<b>ipv6 mld snooping</b> <b>no ipv6 mld snooping</b>
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 <b>ipv6 mld snooping</b> 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 <b>ipv6 mld snooping</b> 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：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)#
```

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)#
```

### 5.10.2 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	<b>ipv6 mld snooping</b> <b>no ipv6 mld snooping</b>
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 <b>ipv6 mld snooping</b> 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 <b>ipv6 mld snooping</b> 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	<b>ipv6 mld snooping fast-leave</b> <b>no ipv6 mld snooping fast-leave</b>
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	-
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

ipv6 mld snooping last-listener-query-interval	
	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	<b>ipv6 mld snooping last-listener-query-interval SECONDS</b> <b>no ipv6 mld snooping last-listener-query-interval</b>
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	<b>ipv6 mld snooping mrouter {interface INTERFACE-ID [, -]   forbidden interface INTERFACE-ID [, -]   learn pimv6}</b> <b>no ipv6 mld snooping mrouter {interface INTERFACE-ID [, -]   forbidden interface INTERFACE-ID [, -]   learn pimv6}</b>
パラメーター	<b>forbidden</b> (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。  <b>interface INTERFACE-ID</b> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b>: ポートチャンネルを指定します。</li> </ul> <b>learn pimv6</b> : 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



ipv6 mld snooping mrouter	
ガイドライン	<p>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ンネルを指定して設定します。</p> <p>マルチキャストルーターポートとしてポートチャンネルを指定する場合は、<b>interface port-channel</b> パラメーターで指定してください。ポートチャン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。</p> <p>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。</p>
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ン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	<b>ipv6 mld snooping ignore-topology-change-notification</b> <b>no ipv6 mld snooping ignore-topology-change-notification</b>
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	<p>MLD スヌーピングを有効にした装置では、スパニングツリー動作によって生じたリンクレイヤ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。</p> <p>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。</p>
制限事項	-
注意事項	-

## ipv6 mld snooping ignore-topology-change-notification

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	<b>ipv6 mld snooping proxy-reporting</b> [ <i>source IPV6-ADDRESS</i> ] <b>no ipv6 mld snooping proxy-reporting</b>
パラメーター	<b>source</b> <i>IPV6-ADDRESS</i> (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	<b>source</b> <i>IPV6-ADDRESS</i> 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します。
シンタックス	<b>ipv6 mld snooping querier</b> <b>no ipv6 mld snooping querier</b>
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

ipv6 mld snooping querier	
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	<b>ipv6 mld snooping query-interval SECONDS</b> <b>no ipv6 mld snooping query-interval</b>
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	<b>ipv6 mld snooping query-max-response-time SECONDS</b> <b>no ipv6 mld snooping query-max-response-time</b>
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

ipv6 mld snooping query-max-response-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	-
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	<code>ipv6 mld snooping query-version {1   2}</code> <code>no ipv6 mld snooping query-version</code>
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	<code>ipv6 mld snooping report-suppression</code> <code>no ipv6 mld snooping report-suppression</code>
パラメーター	なし
デフォルト	無効

ipv6 mld snooping report-suppression	
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	<b>ipv6 mld snooping robustness-variable</b> <i>VALUE</i> <b>no ipv6 mld snooping robustness-variable</b>
パラメーター	<i>VALUE</i> : 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	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>Group member interval</b> : 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。 <ul style="list-style-type: none"> <li>• 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)</li> </ul> </li> <li>• <b>Other querier present interval</b> : 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。 <ul style="list-style-type: none"> <li>• 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)</li> </ul> </li> <li>• <b>Last listener query count</b> : 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。</li> </ul> <p>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。</p>
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	<b>ipv6 mld snooping static-group</b> <i>IPV6-ADDRESS</i> <b>interface</b> <i>INTERFACE-ID</i> [,   -] <b>no ipv6 mld snooping static-group</b> <i>IPV6-ADDRESS</i> [ <b>interface</b> <i>INTERFACE-ID</i> [,   -]]
パラメーター	<i>IPV6-ADDRESS</i> : IPv6 マルチキャストグループアドレスを指定します。 <b>interface</b> <i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b>: ポートチャンネルを指定します。</li> </ul>
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	<b>ipv6 mld snooping suppression-time</b> <i>SECONDS</i> <b>no ipv6 mld snooping suppression-time</b>
パラメーター	<i>SECONDS</i> : 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
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	<b>ipv6 mld snooping minimum-version 2</b> <b>no ipv6 mld snooping minimum-version</b>
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 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	<b>show ipv6 mld snooping [vlan VLAN-ID [,  -]]</b>
パラメーター	<b>vlan VLAN-ID</b> (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)

VLAN #1 configuration
```

MLD snooping state	: Enabled ... (2)
Minimum version	: v2 ... (3)
Fast leave	: Enabled (host-based) ... (4)
Report suppression	: Enabled ... (5)
Suppression time	: 10 seconds ... (6)
Proxy reporting	: Disabled (Source ::) ... (7)
Mrouter port learning	: Enabled ... (8)
Querier state	: Enabled (Non-active) ... (9)
Query version	: v2 ... (10)
Query interval	: 125 seconds ... (11)
Max response time	: 10 seconds ... (12)
Robustness value	: 2 ... (13)
Last listener query interval	: 1 seconds ... (14)
Ignore topology change	: Disabled ... (15)
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)	VLAN 上の MLD スヌーピング機能の有効/無効を表示します。
(3)	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。
(4)	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
(5)	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。
(6)	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。
(7)	MLD スヌーピングのプロキシレポート機能の有効/無効を表示します。
(8)	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。
(9)	MLD クエリア機能の有効/無効を表示します。
(10)	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。
(11)	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を送信する間隔を表示します。
(12)	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。
(13)	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。
(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)	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。

### 5.10.18 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	<b>show ipv6 mld snooping groups</b> [ <i>IPV6-ADDRESS</i>   <b>vlan</b> <i>VLAN-ID</i> [,  -]]
パラメーター	<i>IPV6-ADDRESS</i> (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。  <b>vlan</b> <i>VLAN-ID</i> (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



show ipv6 mld snooping groups	
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        ffle::                *                   EX 258       1/0/7
1        ffle::3              *                   EX 258       1/0/7
1        ffle::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)	インターフェース ID を表示します。

### 5.10.19 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	<b>show ipv6 mld snooping mrouter</b> [vlan <i>VLAN-ID</i> [, -]]
パラメーター	<b>vlan</b> <i>VLAN-ID</i> (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)	ポート番号を表示します。

### 5.10.20 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	<code>show ipv6 mld snooping statistics {interface [INTERFACE-ID [, -]]   vlan [VLAN-ID [, -]]}</code>
パラメーター	<p><b>interface</b> : 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。</p> <p><i>INTERFACE-ID</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul> <p><b>vlan</b> : 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。</p> <p><i>VLAN-ID</i> (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。</p>
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	<p>インターフェースを指定しない場合、すべてのインターフェースの MLD スヌーピングの統計情報が表示されます。</p> <p>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 スヌーピングの統計情報が表示されます。</p>
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。

### 5.10.21 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	<b>show ipv6 mld snooping static-group</b> [ <i>IPV6-ADDRESS</i>   <b>vlan</b> <i>VLAN-ID</i> [,  -]]
パラメーター	<i>IPV6-ADDRESS</i> (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。  <b>vlan</b> <i>VLAN-ID</i> (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        ffile::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。

項番	説明
(3)	インターフェース ID を表示します。

### 5.10.22 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	<code>clear ipv6 mld snooping groups {all   IPV6-ADDRESS [vlan VLAN-ID]}</code>
パラメーター	<p><b>all</b> : 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。</p> <p><b>IPV6-ADDRESS</b> : 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。</p> <p><b>vlan VLAN-ID</b> (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。</p>
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。

<pre># clear ipv6 mld snooping groups all #</pre>
---

### 5.10.23 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クリアします。
シンタックス	<code>clear ipv6 mld snooping statistics {all   vlan VLAN-ID   interface INTERFACE-ID}</code>
パラメーター	<p><b>all</b> : すべての VLAN とすべてのポートの MLD スヌーピングの統計情報をクリアする場合に指定します。</p> <p><b>vlan VLAN-ID</b> : MLD スヌーピングの統計情報をクリアする VLAN を指定します。</p> <p><b>interface INTERFACE-ID</b> : MLD スヌーピングの統計情報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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。</li> <li>• <b>port-channel</b> : ポートチャネルを指定します。</li> </ul>
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	-

```
clear ipv6 mld snooping statistics
```

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クリアする方法を示します。

```
# clear ipv6 mld snooping statistics 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	<b>ethernet ring g8032 profile</b> <i>PROFILE-NAME</i> <b>no ethernet ring g8032 profile</b> <i>PROFILE-NAME</i>
パラメーター	<i>PROFILE-NAME</i> : G. 8032 プロファイル名を最大 32 文字で指定します。
デフォルト	なし
コマンドモード	グ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、 <b>no revertive</b> コマンドを実行して使用を継続します。
シンタックス	<b>revertive</b> <b>no revertive</b>
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	<p>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。</p> <p>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に戻ることが推奨されます。</p> <p>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に直ちに直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。</p>
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	<b>tcn-propagation</b> <b>no tcn-propagation</b>
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	<b>timer {guard <i>MILLI-SECONDS</i>   hold-off <i>SECONDS</i>   wtr <i>MINUTES</i>}</b> <b>no timer [guard   hold-off   wtr]</b>
パラメーター	<b>guard <i>MILLI-SECONDS</i></b> ：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。 <b>hold-off <i>SECONDS</i></b> ：ホールドオフタイマー値を 0～10 秒の範囲で指定します。 <b>wtr <i>MINUTES</i></b> ：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、すべてのタイマーがリセットされます。



timer (ERPS)	
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	<b>ethernet ring g8032</b> <i>RING-NAME</i> <b>no ethernet ring g8032</b> <i>RING-NAME</i>
パラメーター	<i>RING-NAME</i> ：リング名を最大 32 文字で指定します。
デフォルト	なし
コマンドモード	グ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	<b>port0 interface</b> <i>INTERFACE-ID</i> <b>no port0</b>
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> ：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。 <ul style="list-style-type: none"> <li>• <b>port</b>：物理ポートを指定します。</li> <li>• <b>port-channel</b>：ポートチャンネルを指定します。</li> </ul>
デフォルト	なし
コマンドモード	ERPS 設定モード

port0	
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、リングトポロジは正常に動作せず、ループを生成します。 <ul style="list-style-type: none"> <li>指定したインターフェースがポートチャネルである</li> <li>ERPS インスタンスが有効化されている</li> <li>ポートチャネルメンバーが変更または削除されている</li> </ul>
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 ( <b>loop-detection action notify-only</b> 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	<b>port1</b> { <b>interface</b> <i>INTERFACE-ID</i>   <b>none</b> } <b>no port1</b>
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li><b>port</b> : 物理ポートを指定します。</li> <li><b>port-channel</b> : ポートチャネルを指定します。</li> </ul> <b>none</b> : 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、 <b>port1 none</b> 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、リングトポロジは正常に動作せず、ループを生成します。 <ul style="list-style-type: none"> <li>指定したインターフェースがポートチャネルである</li> <li>ERPS インスタンスが有効化されている</li> <li>ポートチャネルメンバーが変更または削除されている</li> </ul>
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 ( <b>loop-detection action notify-only</b> 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	<b>instance</b> <i>INSTANCE-ID</i> <b>no instance</b> <i>INSTANCE-ID</i>
パラメーター	<i>INSTANCE-ID</i> : 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 <b>port0</b> コマンドと <b>port1</b> 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	<b>sub-ring</b> <i>SUB-RING-NAME</i> <b>no sub-ring</b> <i>SUB-RING-NAME</i>
パラメーター	<i>SUB-RING-NAME</i> : 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。  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	-

sub-ring	
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	<b>description</b> <i>DESCRIPTION</i> <b>no description</b>
パラメーター	<i>DESCRIPTION</i> : ERP インスタンスの説明を最大 64 文字で指定します。
デフォルト	なし
コマンドモード	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

level	
	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	<b>level</b> <i>MEL-VALUE</i> <b>no level</b>
パラメーター	<i>MEL-VALUE</i> : 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	<b>profile</b> <i>PROFILE-NAME</i> <b>no profile</b> <i>PROFILE-NAME</i>
パラメーター	<i>PROFILE-NAME</i> : 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 プロファイルに関連付けることができます。一般的に、同じ G. 8032 プロファイルに関連付けた 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	<b>rpl {port0   port1} [owner]</b> <b>no rpl</b>
パラメーター	<b>port0</b> : 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。 <b>port1</b> : 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。 <b>owner</b> (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	<b>r-aps channel-vlan VLAN-ID</b> <b>no r-aps channel-vlan</b>
パラメーター	<b>VLAN-ID</b> : ERP インスタンスに使用する APS チャネル VLAN を 1~4094 の範囲で指定します。
デフォルト	なし
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

r-aps channel-vlan	
	<p>スは無効の状態になり、操作できなくなります。</p> <p>各 ERP インスタンスには、一意の APS チャンネル VLAN が必要です。</p> <p>サブリング ERP インスタンスの APS チャンネル VLAN は、サブリングの仮想チャンネルでもあります。</p>
制限事項	ERP インスタンスを動作状態にする場合は、APS チャンネル 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 チャンネル 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 チャンネル 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	<b>inclusion-list vlan-ids</b> <i>VLAN-ID</i> [,  -] <b>no inclusion-list vlan-ids</b> <i>VLAN-ID</i> [,  -]
パラメーター	<i>VLAN-ID</i> : 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	-
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。

activate	
シンタックス	<b>activate</b> <b>no activate</b>
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。 <ul style="list-style-type: none"> <li>設定した APS チャンネル VLAN が存在しない。</li> <li>設定したリングポートが、APS チャンネル VLAN のタグ付きメンバーポートでない。</li> </ul> <p>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。</p>
制限事項	-
注意事項	アクティブ化の前に、リングポート、APS チャンネル 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	<b>show ethernet ring g8032 {status   brief} [RING-NAME]</b>
パラメーター	<b>status</b> : 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。  <b>brief</b> : ERP インスタンスの概要を表示する場合に指定します。  <i>RING-NAME</i> (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	-
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) として使用するインターフェース ID 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。 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 チャンネル 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) として使用するインターフェース ID およびリングポート (port0、port1) の状態を表示します。

項番	説明
	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)
Ring          (3)      (4)      (5)
InstID      Status    Port-State
-----
ring1       1         Idle     p0:Port1/0/1,Blocking (RPL)
            2         Idle     p1:Port1/0/2,Forwarding
ring2       2         Idle     p0:Port1/0/3,Forwarding
            3         Idle     p1:-,Forwarding

Total Entries: 2
```

項番	説明
(1)	リングプロテクション(ERPS)の対応バージョンを表示します。
(2)	リング名を表示します。
(3)	ERP インスタンスのインスタンス ID を表示します。
(4)	ERP インスタンスの現在の状態を表示します。 Deactivated : ERP インスタンスが非アクティブ Idle : ERP インスタンスは標準状態 (RPL ポートが閉塞状態) Protection : いずれかのリングポートで障害を検出 (RPL ポートが開放状態)
(5)	現在の RPL ポート (port0、port1) のインターフェース ID 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 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	<b>mmrp-plus enable</b> <b>no mmrp-plus enable</b>
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。
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 ( <b>loop-detection action notify-only</b> 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：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	<b>mmrp-plus switch hello-interval</b> <i>TIME</i> <b>no mmrp-plus switch hello-interval</b>
パラメーター	<i>TIME</i> : 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、 <b>no mmrp-plus enable</b> 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	1.01.01

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	<b>mmrp-plus switch polling-rate</b> <i>RATE</i> <b>no mmrp-plus switch polling-rate</b>
パラメーター	<i>RATE</i> : 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
コマンドモード	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

mmrp-plus switch polling-rate	
	は、 <b>no mmrp-plus enable</b> 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	1.01.01

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	<b>mmrp-plus vlangroup</b> <i>GROUP</i> <b>slave-vid</b> <i>VLAN-ID</i> [, -] <b>no mmrp-plus vlangroup</b> <i>GROUP</i> [ <b>slave-vid</b> <i>VLAN-ID</i> [, -]]
パラメーター	<i>GROUP</i> : VLAN グループの番号を 1~8 の範囲で指定します。 <i>VLAN-ID</i> : 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、 <b>mmrp-plus ring vlangroup</b> 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、 <b>no mmrp-plus vlangroup slave-vid</b> 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	1.01.01

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	<b>no mmrp-plus ring</b> <i>RINGID</i> [,  -]
パラメーター	<i>RINGID</i> : 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	1.01.01

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	<b>mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>name</b> <i>NAME</i> <b>no mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>name</b>
パラメーター	<i>RINGID</i> : 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。 <i>NAME</i> : MMRP-Plus のリング名を最大 32 文字で指定します。
デフォルト	なし
コマンドモード	グ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。

mmrp-plus ring vid	
シンタックス	<b>mmrp-plus ring</b> <i>RINGID</i> [, -] vid <i>VID</i> <b>no mmrp-plus ring</b> <i>RINGID</i> [, -] vid
パラメーター	<i>RINGID</i> : MMRP-Plus のリング ID を 1~1000 の範囲で指定します。複数指定できません。 <i>VID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>mmrp-plus ring ring-master</b> コマンド</li> <li>• <b>mmrp-plus ring divided-master</b> コマンド</li> <li>• <b>mmrp-plus ring divided-slave</b> コマンド</li> <li>• <b>mmrp-plus ring aware</b> コマンド</li> </ul> <p>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。</p>
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、 <b>no vlan</b> コマンドを実行しても削除できません。
対象バージョン	1.01.01

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	<b>mmrp-plus ring</b> <i>RINGID</i> [, -] vlangroup <i>GROUP</i> <b>no mmrp-plus ring</b> <i>RINGID</i> [, -] vlangroup
パラメーター	<i>RINGID</i> : MMRP-Plus のリング ID を 1~1000 の範囲で指定します。複数指定できません。



mmrp-plus ring vlangroup	
	<i>GROUP</i> : 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	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>mmrp-plus ring ring-master</b> コマンド</li> <li>• <b>mmrp-plus ring divided-master</b> コマンド</li> <li>• <b>mmrp-plus ring divided-slave</b> コマンド</li> <li>• <b>mmrp-plus ring aware</b> コマンド</li> </ul> <p>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。</p>
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、 <b>no mmrp-plus enable</b> 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	1.01.01

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	<b>mmrp-plus ring</b> <i>RINGID</i> <b>ring-master</b> <b>master</b> <i>INTERFACE-ID</i> <b>slave</b> <i>INTERFACE-ID</i> <b>no mmrp-plus ring</b> <i>RINGID</i> <b>ring-master</b>
パラメーター	<p><i>RINGID</i>: MMRP-Plus のリング ID を 1~1000 の範囲で指定します。</p> <p><b>master</b> <i>INTERFACE-ID</i>: 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。</p> <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。</li> <li>• <b>port-channel</b>: ポートチャンネルを指定します。</li> </ul> <p><b>slave</b> <i>INTERFACE-ID</i>: 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。</p> <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。</li> <li>• <b>port-channel</b>: ポートチャンネルを指定します。</li> </ul>
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

mmrp-plus ring ring-master	
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。
制限事項	リングポートは、装置ごとに最大 24 個まで設定できます。スタック構成を組んでも、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。 <ul style="list-style-type: none"> <li>ループ検知機能 (<b>loop-detection action notify-only</b> コマンド設定時を除く)</li> <li>CFM</li> </ul>
注意事項	MMRP-Plus のリングポートに設定したポートチャネルには、メンバーポートの追加または削除はできません。  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 <b>mls qos scheduler sp</b> 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。
対象バージョン	1.01.01

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	<b>mmrp-plus ring RINGID divided-master INTERFACE-ID</b> <b>no mmrp-plus ring RINGID divided-master</b>
パラメーター	<b>RINGID</b> ：MMRP-Plus のリング ID を 1～1000 の範囲で指定します。 <b>INTERFACE-ID</b> ：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。 <ul style="list-style-type: none"> <li><b>port</b>：物理ポートを指定します。</li> <li><b>port-channel</b>：ポートチャネルを指定します。</li> </ul>
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。
制限事項	リングポートは、装置ごとに最大 24 個まで設定できます。スタック構成を組んでも、リングポート数は装置 1 台分の値となります。

mmrp-plus ring divided-master	
	MMRP-Plus のリングポートでは、以下の機能を有効にしないでください。 <ul style="list-style-type: none"> <li>ループ検知機能 (<b>loop-detection action notify-only</b> コマンド設定時を除く)</li> <li>CFM</li> </ul>
注意事項	MMRP-Plus のリングポートに設定したポートチャンネルには、メンバーポートの追加または削除はできません。  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 <b>mls qos scheduler sp</b> 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。
対象バージョン	1.01.01

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	<b>mmrp-plus ring</b> <i>RINGID</i> <b>divided-slave</b> <i>INTERFACE-ID</i> <b>no mmrp-plus ring</b> <i>RINGID</i> <b>divided-slave</b>
パラメーター	<i>RINGID</i> ：MMRP-Plus のリング ID を 1～1000 の範囲で指定します。 <i>INTERFACE-ID</i> ：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。 <ul style="list-style-type: none"> <li><b>port</b>：物理ポートを指定します。</li> <li><b>port-channel</b>：ポートチャンネルを指定します。</li> </ul>
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ンネルを、分散スレーブポートとして使用することはできません。  ポートチャン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。
制限事項	リングポートは、装置ごとに最大 24 個まで設定できます。スタック構成を組んでも、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。 <ul style="list-style-type: none"> <li>ループ検知機能 (<b>loop-detection action notify-only</b> コマンド設定時を除く)</li> <li>CFM</li> </ul>
注意事項	MMRP-Plus のリングポートに設定したポートチャンネルには、メンバーポートの追加または削除はできません。

mmrp-plus ring divided-slave	
	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 <b>mls qos scheduler sp</b> 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。
対象バージョン	1.01.01

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）をポートチャンネル 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	<b>mmrp-plus ring</b> <i>RINGID</i> <b>aware</b> <i>INTERFACE-ID</i> <i>INTERFACE-ID</i> <b>no mmrp-plus ring</b> <i>RINGID</i> <b>aware</b>
パラメーター	<i>RINGID</i> ：MMRP-Plus のリング ID を 1～1000 の範囲で指定します。 <i>INTERFACE-ID</i> ：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。 <ul style="list-style-type: none"> <li>• <b>port</b>：物理ポートを指定します。</li> <li>• <b>port-channel</b>：ポートチャンネルを指定します。</li> </ul>
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	ポートチャン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。
制限事項	リングポートは、装置ごとに最大 24 個まで設定できます。スタック構成を組んでも、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。 <ul style="list-style-type: none"> <li>• ループ検知機能（<b>loop-detection action notify-only</b> コマンド設定時を除く）</li> <li>• CFM</li> </ul>
注意事項	MMRP-Plus のリングポートに設定したポートチャンネルには、メンバーポートの追加または削除はできません。 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 <b>mls qos scheduler sp</b> 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。
対象バージョン	1.01.01

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、ポートチャンネル 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	<b>mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>revertive</b> { <i>REVERT-TIMER</i>   <b>disable</b> } <b>no mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>revertive</b>
パラメーター	<i>RINGID</i> : 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。 <i>REVERT-TIMER</i> : 自動切り戻りタイマー値を 0~86400 の範囲で指定します。 <b>disable</b> : 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)
コマンドモード	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	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。 <b>disable</b> パラメーターを指定した場合は、 <b>clear mmrp-plus failure ring</b> 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	1.01.01

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	<b>mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>transmit-fdb-flush port</b> <i>INTERFACE-ID</i> [,  -] <b>no mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>transmit-fdb-flush port</b>
パラメーター	<i>RINGID</i> : 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。 <i>INTERFACE-ID</i> : 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

mmrp-plus ring transmit-fdb-flush port	
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。  <i>INTERFACE-ID</i> 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	1.01.01

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	<b>mmrp-plus ring <i>RINGID</i> [,  -] transmit-fdb-flush retransmit enable</b> <b>no mmrp-plus ring <i>RINGID</i> [,  -] transmit-fdb-flush retransmit enable</b>
パラメーター	<i>RINGID</i> : 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	1.01.01

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	<b>mmrp-plus ring <i>RINGID</i> [,  -] fdb-flush port <i>INTERFACE-ID</i> [,  -]</b> <b>no mmrp-plus ring <i>RINGID</i> [,  -] fdb-flush port</b>
パラメーター	<i>RINGID</i> : 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。

mmrp-plus ring fdb-flush port	
	複数指定できます。 <i>INTERFACE-ID</i> : 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	1.01.01

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	<b>mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>fdb-flush timer</b> <i>TIME</i> <b>no mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>fdb-flush timer</b>
パラメーター	<i>RINGID</i> : 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。 <i>TIME</i> : 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	1.01.01

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。

mmrp-plus ring listening-timer	
シンタックス	<b>mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>listening-timer</b> <i>TIME</i> <b>no mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>listening-timer</b>
パラメーター	<i>RINGID</i> : 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。 <i>TIME</i> : リスニングタイマーを 1~86400 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	1.01.01

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	<b>mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>hello-timeout</b> <i>TIME</i> <b>no mmrp-plus ring</b> <i>RINGID</i> [,  -] <b>hello-timeout</b>
パラメーター	<i>RINGID</i> : 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。 <i>TIME</i> : MMRP-Plus ハローフレームの受信タイムアウト時間を 1~86400 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。 <ul style="list-style-type: none"> <li>• <b>mmrp-plus switch polling-rate</b> コマンド</li> <li>• <b>mmrp-plus switch hello-interval</b> コマンド</li> </ul>
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 ( <b>lldp err-disable</b> 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)



mmrp-plus ring hello-timeout	
	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	1.01.01

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 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	<b>show mmrp-plus configuration</b>
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：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 (0: enable -: disable)
  Vg  : VLAN Group
  Re  : Revertive setting
  Ht  : Hello Timeout Timer
  Lis : Listening Timer
  P   : Port-Channel
  (11)
  (4) (5) (6) (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    0  -  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ン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、ポートチャンネル番号です。 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)	※ApresiaNP4000 シリーズでは未サポートです。 ポートリスタート機能の設定を表示します。 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。

### 5.12.21 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	<b>show mmrp-plus configuration ring</b> <i>RINGID</i> [,  -]
パラメーター	<i>RINGID</i> : 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	1.01.01

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 エントリを消去するポートを表示します。

項番	説明
(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)	※ApresiaNP4000 シリーズでは未サポートです。 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)	※ApresiaNP4000 シリーズでは未サポートです。 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)	※ApresiaNP4000 シリーズでは未サポートです。 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)	※ApresiaNP4000 シリーズでは未サポートです。 アップリンクポートを表示します。 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。

### 5.12.22 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	<b>show mmrp-plus vlangroup</b> [ <i>GROUP</i> ]
パラメーター	<i>GROUP</i> (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	1.01.01

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。

<pre># show mmrp-plus vlangroup 8  VLAN Group Configuration: Group 8 ... (1)   Master VID   : 1-4094 ... (2)   Slave VID    : - ... (3)</pre>
---

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。

## 5.12.23 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	<b>show mmrp-plus status</b>
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：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
Pl       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

項番	説明
	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。

### 5.12.24 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	<b>show mmrp-plus status</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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 : MMRP-Plus のポートチャンネル 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)	インターフェース ID を表示します。
(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 <ul style="list-style-type: none"> <li>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</li> </ul> Ring Aware Master : スレーブ方向に接続されたアウェアポート <ul style="list-style-type: none"> <li>スレーブポートからの MMRP-Plus ハローフレーム (HelloB1/HelloF1) 受信時</li> </ul> Ring Aware Slave : マスター方向に接続されたアウェアポート <ul style="list-style-type: none"> <li>マスターポートからの MMRP-Plus ハローフレーム (HelloB2/HelloF2) 受信時</li> </ul> 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) 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

項番	説明
	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。

### 5.12.25 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	<b>show mmrp-plus status ring</b> <i>RINGID</i> [,  -]
パラメーター	<i>RINGID</i> : 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	1.01.01

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) Frame Type	(13) Receive Frame Count	(14) 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)	インターフェース ID を表示します。
(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 <ul style="list-style-type: none"> <li>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</li> </ul> Ring Aware Master : スレーブ方向に接続されたアウェアポート <ul style="list-style-type: none"> <li>スレーブポートからの MMRP-Plus ハローフレーム (HelloB1/HelloF1) 受信時</li> </ul> Ring Aware Slave : マスター方向に接続されたアウェアポート <ul style="list-style-type: none"> <li>マスターポートからの MMRP-Plus ハローフレーム (HelloB2/HelloF2) 受信時</li> </ul> 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

項番	説明
	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) 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。

### 5.12.26 clear mmrp-plus failure ring

clear mmrp-plus failure ring	
目的	Failure 状態を解除し、リング復旧処理を開始します (Listening 状態へ遷移します)。
シンタックス	<b>clear mmrp-plus failure ring</b> <i>RINGID</i> [, -]
パラメーター	<i>RINGID</i> : 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	<b>mmrp-plus ring revertive</b> 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 Failure 状態を解除し、リング復旧処理を開始できます (Listening 状態へ遷移します)。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例 : リング ID 1 の Failure 状態を解除し、リング復旧処理を開始する方法を示します。

```
# clear mmrp-plus failure ring 1
#
```

## 5.12.27 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	<code>debug mmrp [event   hello   cpu   fdbflush]</code> <code>no debug mmrp [event   hello   cpu   fdbflush]</code>
パラメーター	<b>event</b> (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。 <b>hello</b> (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。 <b>cpu</b> (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。 <b>fdbflush</b> (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
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	1.01.01

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
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
revision (MSTP)	revision VERSION no revision

コマンド	コマンドとパラメーター
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 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	<b>spanning-tree global state {enable   disable}</b> <b>no spanning-tree global state</b>
パラメーター	<b>enable</b> : グローバル設定を有効にする場合に指定します。 <b>disable</b> : 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 ( <b>spanning-tree global state disable</b> )
コマンドモード	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 ( <b>loop-detection action notify-only</b> 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	-
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)#
```

### 5.13.2 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	<b>spanning-tree mode {mstp   rstp   stp   rpvst+}</b> <b>no spanning-tree mode</b>
パラメーター	<b>mstp</b> ：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。 <b>rstp</b> ：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す。 <b>stp</b> ：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。 <b>rpvst+</b> ：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 <b>rpvst+</b> 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「 <b>stp</b> 、 <b>rstp</b> 、 <b>mstp</b> 」から「 <b>rpvst+</b> 」に変更する場合、または「 <b>rpvst+</b> 」から「 <b>stp</b> 、 <b>rstp</b> 、 <b>mstp</b> 」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)#
```

### 5.13.3 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	<b>spanning-tree priority PRIORITY</b> <b>no spanning-tree priority</b>
パラメーター	<b>PRIORITY</b> ：ブリッジ優先度を、0～61440 の範囲から 4096 の倍数で指定します。

spanning-tree priority	
デフォルト	32768
コマンドモード	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。 <ul style="list-style-type: none"> <li>• STP のブリッジ優先度</li> <li>• RSTP のブリッジ優先度</li> <li>• MSTP インスタンス 0 のブリッジ優先度</li> <li>• VLAN 1 のRPVST+ブリッジ優先度</li> </ul>
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：ブリッジの優先度を 4096 に設定する方法を示します。

```
# configure terminal
(config)# spanning-tree priority 4096
(config)#
```

#### 5.13.4 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	<b>spanning-tree {hello-time SECONDS   forward-time SECONDS   max-age SECONDS}</b> <b>no spanning-tree {hello-time   forward-time   max-age}</b>
パラメーター	<b>hello-time SECONDS</b> ：ハロータイムを、1～2 秒の範囲で指定します。 <b>forward-time SECONDS</b> ：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。 <b>max-age SECONDS</b> ：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、 <b>spanning-tree mst hello-time</b> 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)#
```

### 5.13.5 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	<b>spanning-tree tx-hold-count</b> <i>VALUE</i> <b>no spanning-tree tx-hold-count</b>
パラメーター	<i>VALUE</i> : 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
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)#
```

### 5.13.6 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	<b>spanning-tree nni-bpdu-address</b> {dot1d   dot1ad} <b>no spanning-tree nni-bpdu-address</b>
パラメーター	<b>dot1d</b> : 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。 <b>dot1ad</b> : 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。



spanning-tree nni-bpdu-address	
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)#
```

### 5.13.7 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。
シンタックス	<b>spanning-tree state {enable   disable}</b> <b>no spanning-tree state</b>
パラメーター	<b>enable</b> : 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。 <b>disable</b> : 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 ( <b>spanning-tree state enable</b> )
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 ( <b>interface port-channel</b> 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 ( <b>loop-detection action notify-only</b> 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	<b>spanning-tree state</b> 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)#
```

### 5.13.8 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	<b>spanning-tree cost COST</b> <b>no spanning-tree cost</b>
パラメーター	<b>COST</b> : パスコストを、1~200000000 の範囲で指定します。

spanning-tree cost	
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	<p>ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• STP 使用時のパスコスト</li> <li>• RSTP 使用時のパスコスト</li> <li>• VLAN 1 の RPVST+使用時のパスコスト</li> </ul>
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)#
```

### 5.13.9 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	<b>spanning-tree guard root</b> <b>no spanning-tree guard root</b>
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	<p>ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>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。</p> <p>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ギュレーション 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。</p> <p>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。</p>
制限事項	-

spanning-tree guard root	
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)#
```

### 5.13.10 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	<code>spanning-tree link-type {point-to-point   shared}</code> <code>no spanning-tree link-type</code>
パラメーター	<b>point-to-point</b> : 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。 <b>shared</b> : 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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <code>interface port-channel</code> 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)#
```

### 5.13.11 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	<code>spanning-tree portfast {disable   edge   network}</code> <code>no spanning-tree portfast</code>
パラメーター	<b>disable</b> : Port Fast モードを無効に設定する場合に指定します。 <b>edge</b> : 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。

spanning-tree portfast	
	<b>network</b> : 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	<p>ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>Edge mode</b> : 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。</li> <li>• <b>Disable mode</b> : 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) の経過を待ちます。</li> <li>• <b>Network mode</b> : 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。</li> </ul> <p>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。</p>
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、 <b>spanning-tree portfast</b> 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)#
```

### 5.13.12 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	<b>spanning-tree port-priority PRIORITY</b> <b>no spanning-tree port-priority</b>
パラメーター	<b>PRIORITY</b> : 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	<p>ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>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。</p>

spanning-tree port-priority	
	<ul style="list-style-type: none"> <li>• STP のポート優先度</li> <li>• RSTP のポート優先度</li> <li>• MSTP インスタンス 0 のポート優先度</li> <li>• VLAN 1 の RPVST+のポート優先度</li> </ul>
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)#
```

### 5.13.13 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	<b>spanning-tree tcnfilter</b> <b>no spanning-tree tcnfilter</b>
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	<p>ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>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。</p> <p>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。</p>
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)#
```

### 5.13.14 spanning-tree forward-bpdu

spanning-tree forward-bpdu	
目的	BPDU の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	<b>spanning-tree forward-bpdu</b> <b>no spanning-tree forward-bpdu</b>

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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> コマンド) で設定してください。  有効にした場合、受信した BPDU はタグのない形で、すべてのメンバーポートに転送されます。
制限事項	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)#
```

### 5.13.15 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	<b>spanning-tree mst configuration</b> <b>no spanning-tree mst configuration</b>
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。 <ul style="list-style-type: none"> <li>• <b>instance (MSTP)</b></li> <li>• <b>name (MSTP)</b></li> <li>• <b>revision (MSTP)</b></li> <li>• <b>spanning-tree mst priority</b> (MSTP インスタンス 0 の設定は除く)</li> <li>• <b>spanning-tree mst cost</b> (MSTP インスタンス 0 の設定は除く)</li> <li>• <b>spanning-tree mst port-priority</b> (MSTP インスタンス 0 の設定は除く)</li> </ul>
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)#
```

## 5.13.16 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 <b>no instance</b> 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 <b>no instance</b> コマンドを使用します。
シンタックス	<b>instance</b> <i>INSTANCE-ID</i> <b>vlangs</b> <i>VLAN-ID</i> [,  -] <b>no instance</b> <i>INSTANCE-ID</i> [ <b>vlangs</b> <i>VLAN-ID</i> [,  -]]
パラメーター	<i>INSTANCE-ID</i> : 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。  <b>vlangs</b> <i>VLAN-ID</i> : 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)#
```

## 5.13.17 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	<b>name</b> <i>NAME</i> <b>no name</b> <i>NAME</i>
パラメーター	<i>NAME</i> : リージョン名を、最大 32 文字で指定します。一般的な文字列とスペースを使用できます。
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)#
```

### 5.13.18 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	<b>revision</b> <i>VERSION</i> <b>no revision</b>
パラメーター	<i>VERSION</i> : MSTP コンフィグレーションのリビジョン番号を指定します。
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)#
```

### 5.13.19 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	<b>spanning-tree mst</b> <i>INSTANCE-ID</i> <b>priority</b> <i>PRIORITY</i> <b>no spanning-tree mst</b> <i>INSTANCE-ID</i> <b>priority</b>
パラメーター	<i>INSTANCE-ID</i> : MSTP インスタンス番号を、0～16 の範囲で指定します。 <i>PRIORITY</i> : ブリッジ優先度を、0～61440 の範囲から 4096 の倍数で指定します。
デフォルト	32768
コマンドモード	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( <b>spanning-tree priority</b> <i>PRIORITY</i> )で表示されます。
制限事項	本コマンドを実施する前に、 <b>instance (MSTP)</b> コマンドで対象の MSTP インスタンスを設定してください。



spanning-tree mst priority	
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)#
```

### 5.13.20 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	<b>spanning-tree mst hello-time SECONDS</b> <b>no spanning-tree mst hello-time</b>
パラメーター	<b>SECONDS</b> ：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（ <b>interface port-channel</b> 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)#
```

### 5.13.21 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	<b>spanning-tree mst max-hops HOP-COUNT</b> <b>no spanning-tree mst max-hops</b>
パラメーター	<b>max-hops HOP-COUNT</b> ：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	-

spanning-tree mst max-hops	
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)#
```

### 5.13.22 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	<b>spanning-tree mst</b> <i>INSTANCE-ID</i> <b>cost</b> <i>COST</i> <b>no spanning-tree mst</b> <i>INSTANCE-ID</i> <b>cost</b>
パラメーター	<i>INSTANCE-ID</i> ：MSTP インスタンス番号を、0～16 の範囲で指定します。 <i>COST</i> ：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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> コマンド) で設定してください。
制限事項	本コマンドを実施する前に、 <b>instance (MSTP)</b> 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)#
```

### 5.13.23 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	<b>spanning-tree mst</b> <i>INSTANCE-ID</i> <b>port-priority</b> <i>PRIORITY</i> <b>no spanning-tree mst</b> <i>INSTANCE-ID</i> <b>port-priority</b>
パラメーター	<i>INSTANCE-ID</i> ：MSTP インスタンス番号を、0～16 の範囲で指定します。 <i>PRIORITY</i> ：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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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

spanning-tree mst port-priority	
	MSTP インスタンス指定の無いコマンド形式 ( <b>spanning-tree port-priority PRIORITY</b> ) で表示されます。
制限事項	本コマンドを実施する前に、 <b>instance (MSTP)</b> 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)#
```

### 5.13.24 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	<b>snmp-server enable traps stp [new-root] [topology-chg]</b> <b>no snmp-server enable traps stp [new-root] [topology-chg]</b>
パラメーター	<b>new-root</b> (省略可能)：スパニングツリープロトコルの新ルートブリッジ通知 (SNMP トラップ) の送信を制御する場合に指定します。 <b>topology-chg</b> (省略可能)：トポロジー変更通知 (SNMP トラップ) の送信を制御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、両方のパラメーターに対して設定が反映されます。 本コマンドを有効にする場合は、 <b>snmp-server enable traps</b> 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 トラップを有効にし、コミュニティ名「public」で 10.9.18.100 宛てに送信するように設定する方法を示します。

```
# configure terminal
(config)# snmp-server enable traps
(config)# snmp-server enable traps stp
(config)# snmp-server host 10.9.18.100 version 2c public
(config)#
```

### 5.13.25 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	<b>show spanning-tree [interface INTERFACE-ID [,  -]]</b>

show spanning-tree	
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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 : 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)
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。

項番	説明
(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ンネル番号を表示します。
(17)	ポートの役割を表示します。 root : ルートポート designated : 指定ポート alternate : 代替ポート backup : バックアップポート disabled : 無効ポート
(18)	ポートのステータスを表示します。 forwarding : フォワーディング状態 blocking : ブロッキング状態 (ディスカード状態) 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

### 5.13.26 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	<b>show spanning-tree configuration interface</b> [ <i>INTERFACE-ID</i> [, [-]]
パラメーター	<i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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、すべてのインターフェースのインターフェース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

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ン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。

### 5.13.27 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	<pre> show spanning-tree mst [configuration [digest]] show spanning-tree mst [instance INSTANCE-ID [, -]] [interface INTERFACE-ID [, -]] [detail] </pre>
パラメーター	<p><b>configuration</b> (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。</p> <p><b>digest</b> (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。</p> <p><b>instance</b> <i>INSTANCE-ID</i> (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。</p> <p><b>interface</b> <i>INTERFACE-ID</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul> <p><b>detail</b> (省略可能) : 詳細情報を表示する場合に指定します。</p>

show spanning-tree mst	
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	MSTP インスタンスを指定しない場合、すべての MSTP インスタンスの MSTP 情報が表示されます。  インターフェースを指定しない場合、すべてのインターフェースの MSTP 情報が表示されます。  MSTP とプライベート VLAN を併用していて、プライマリーVLAN とセカンダリーVLAN が異なる MSTP インスタンスにマッピングされている場合には、 <b>show spanning-tree mst configuration</b> コマンドで警告メッセージが表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例：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)
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

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。
(3)	BPDU の宛先 MAC アドレスを表示します。
(4)	MSTP インスタンス数を表示します。
(5)	MSTP インスタンス番号を表示します。
(6)	MSTP インスタンスに割り当てられている VLAN を表示します。
(7)	自装置の MAC アドレスを表示します。
(8)	自装置の優先度 (ブリッジ優先度、sysid : MSTP インスタンス番号) を表示します。
(9)	CIST ルートの MAC アドレスを表示します。
(10)	CIST ルートの優先度 (ブリッジ優先度、sysid : MSTP インスタンス番号) を表示します。
(11)	CIST 外部ルートパスコストを表示します。
(12)	CIST リージョナルルートの MAC アドレスを表示します。
(13)	CIST リージョナルルートの優先度 (ブリッジ優先度、sysid : MSTP インスタンス番号) を表示します。
(14)	CIST 内部ルートパスコストを表示します。
(15)	ルートポートで受信した BPDU の送信元装置の MAC アドレスを表示します。自装置がルートブリッジの場合は自装置の MAC アドレスを表示します。
(16)	ルートポートで受信した BPDU の送信元装置の優先度 (ブリッジ優先度、sysid : MSTP インスタンス番号) を表示します。自装置がルートブリッジの場合は自装置の優先度を表示します。
(17)	スパニングツリープロトコルのトポロジーが変更された回数を表示します。
(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 (ディスカード状態) 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。



項番	説明
(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)
Instance Role      State      Cost      Priority
-----
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ン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

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

項番	説明
	non-edge : 無効ポート
(6)	BPDU の送受信数を表示します。
(7)	MSTP インスタンス番号を表示します。
(8)	MSTP インスタンスに割り当てられている VLAN を表示します。
(9)	ポートのステータスを表示します。 forwarding : フォワーディング状態 blocking : ブロッキング状態 (ディスカーディング状態) learning : ラーニング状態 disabled : 無効状態
(10)	ポートの役割を表示します。 root : ルートポート designated : 指定ポート alternate : 代替ポート backup : バックアップポート disabled : 無効ポート master : MSTI マスターポート
(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。

### 5.13.28 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	<b>clear spanning-tree detected-protocols</b> {all   interface <i>INTERFACE-ID</i> }
パラメーター	<p><b>all</b> : すべてのポートに検知動作を行わせます。</p> <p><b>interface <i>INTERFACE-ID</i></b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	<b>spanning-tree vlan</b> <i>VLAN-ID</i> <b>no spanning-tree vlan</b> <i>VLAN-ID</i>
パラメーター	<i>VLAN-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>spanning-tree vlan priority</b></li> <li>• <b>spanning-tree vlan (timers)</b></li> <li>• <b>spanning-tree vlan cost</b></li> <li>• <b>spanning-tree vlan port-priority</b></li> </ul>
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 ( <b>loop-detection action notify-only</b> 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 <b>spanning-tree state disable</b> コマンドにて無効に変更してください。																		
	<table border="1"> <thead> <tr> <th>VLAN 数</th> <th>各ポートの役割(Role)</th> <th>ポート数</th> </tr> </thead> <tbody> <tr> <td rowspan="2">200</td> <td>Root Port, Alternate Port, Backup Port</td> <td>3</td> </tr> <tr> <td>Designated Port</td> <td>3</td> </tr> <tr> <td rowspan="2">100</td> <td>Root Port, Alternate Port, Backup Port</td> <td>6</td> </tr> <tr> <td>Designated Port</td> <td>6</td> </tr> <tr> <td rowspan="2">50</td> <td>Root Port, Alternate Port, Backup Port</td> <td>12</td> </tr> <tr> <td>Designated Port</td> <td>12</td> </tr> </tbody> </table>	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
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	1.01.01																		

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	<b>spanning-tree vlan <i>VLAN-ID</i> priority <i>PRIORITY</i></b> <b>no spanning-tree vlan <i>VLAN-ID</i> priority</b>
パラメーター	<i>VLAN-ID</i> : VLAN ID を、1~4094 の範囲で指定します。 <i>PRIORITY</i> : ブリッジ優先度を、0~61440 の範囲から 4096 の倍数で指定します。
デフォルト	32768
コマンドモード	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( <b>spanning-tree priority <i>PRIORITY</i></b> )で表示されます。
制限事項	本コマンドを実施する前に、 <b>spanning-tree vlan</b> 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	1.01.01

使用例：VLAN 10 の RPVST+のブリッジの優先度を 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	<b>spanning-tree vlan</b> <i>VLAN-ID</i> { <b>hello-time</b> <i>SECONDS</i>   <b>forward-time</b> <i>SECONDS</i>   <b>max-age</b> <i>SECONDS</i> } <b>no spanning-tree vlan</b> <i>VLAN-ID</i> { <b>hello-time</b>   <b>forward-time</b>   <b>max-age</b> }
パラメーター	<i>VLAN-ID</i> : VLAN ID を、1~4094 の範囲で指定します。 <b>hello-time</b> <i>SECONDS</i> : ハロータイムを、1~2 秒の範囲で指定します。 <b>forward-time</b> <i>SECONDS</i> : 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。 <b>max-age</b> <i>SECONDS</i> : 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。 <ul style="list-style-type: none"> <li>ハロータイム設定: <b>spanning-tree hello-time</b> <i>SECONDS</i></li> <li>フォワードディレイタイム設定: <b>spanning-tree forward-time</b> <i>SECONDS</i></li> <li>最大エージタイム設定: <b>spanning-tree max-age</b> <i>SECONDS</i></li> </ul>
制限事項	本コマンドを実施する前に、 <b>spanning-tree vlan</b> 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	1.01.01

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	<b>spanning-tree vlan</b> <i>VLAN-ID</i> <b>cost</b> <i>COST</i> <b>no spanning-tree vlan</b> <i>VLAN-ID</i> <b>cost</b>
パラメーター	<i>VLAN-ID</i> : VLAN ID を、1~4094 の範囲で指定します。

spanning-tree vlan cost	
	<i>COST</i> : 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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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( <b>spanning-tree cost <i>COST</i></b> )で表示されます。
制限事項	本コマンドを実施する前に、 <b>spanning-tree vlan</b> 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ンネルで設定する場合は、先にポートチャン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ン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	1.01.01

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	<b>spanning-tree vlan <i>VLAN-ID</i> port-priority <i>PRIORITY</i></b> <b>no spanning-tree vlan <i>VLAN-ID</i> port-priority</b>
パラメーター	<i>VLAN-ID</i> : VLAN ID を、1~4094 の範囲で指定します。 <i>PRIORITY</i> : 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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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( <b>spanning-tree port-priority <i>PRIORITY</i></b> )で表示されます。
制限事項	本コマンドを実施する前に、 <b>spanning-tree vlan</b> 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ンネルで設定する場合は、先にポートチャン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ン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	1.01.01



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	<b>show spanning-tree vlan</b> [ <i>VLAN-ID</i> ]
パラメーター	<i>VLAN-ID</i> (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	VLAN ID を指定しない場合、RPVST+を有効にしたすべての 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：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)
Interface          Role          State          Cost          .Port#        Priority Link
-----          -----          -----          -----          -----          -----
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ンニングツリープロトコルを表示します。
(3)	ルートブリッジの優先度を表示します。
(4)	ルートブリッジの MAC アドレスを表示します。
(5)	自装置がルートブリッジの場合に表示されます。
(6)	ルートブリッジのハロータイムを表示します。
(7)	ルートブリッジの最大エージタイムを表示します。

項番	説明
(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ン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 (ディスカードイング状態) 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	<b>show spanning-tree vlan</b> <i>VLAN-ID</i> <b>interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>VLAN-ID</i> : 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。 <i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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、対象 VLAN の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	-

show spanning-tree vlan interface	
注意事項	-
対象バージョン	1.01.01

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ン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

項番	説明
	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。 <ul style="list-style-type: none"> <li>• port: 物理ポートを指定します。</li> <li>• range port: 物理ポートを範囲で指定します。</li> </ul>
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	<p>ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード（<b>interface port-channel</b> コマンド）で設定してください。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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ンネルを指定する場合は、そのポートチャン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ン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ン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。</p>
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	<b>show traffic-segmentation forward</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b>：物理ポートを指定します。</li> <li>• <b>range port</b>：物理ポートを範囲で指定します。</li> <li>• <b>port-channel</b>：ポートチャンネルを指定します。</li> </ul>
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、すべてのインターフェースの転送ドメインが表示されます。
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)	インターフェース ID 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	<b>vlan</b> <i>VLAN-ID</i> [,  -] <b>no vlan</b> <i>VLAN-ID</i> [,  -]
パラメーター	<i>VLAN-ID</i> : 作成・変更する VLAN を 1~4094 の範囲で指定します。複数指定できません。
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 <b>switchport access vlan</b> 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 <b>remote-span</b> 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	<b>name</b> <i>VLAN-NAME</i> <b>no name</b>
パラメーター	<i>VLAN-NAME</i> : VLAN 名を最大 32 文字で指定します。VLAN ごとに一意の名称を設定してください。
デフォルト	VLAN 1 は default ( <b>name default</b> 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	<b>switchport mode {access   hybrid   trunk   dot1q-tunnel}</b> <b>no switchport mode</b>
パラメーター	<b>access</b> : アクセスポートとして設定する場合に指定します。 <b>hybrid</b> : ハイブリッドポートとして設定する場合に指定します。 <b>trunk</b> : トランクポートとして設定する場合に指定します。 <b>dot1q-tunnel</b> : 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	<p>ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>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。</p> <p>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。</p> <p>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。<b>switchport trunk native vlan tag</b> 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。</p> <p>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。</p> <p>本コマンドで VLAN モードが変更された場合、以前の VLAN モードに関する VLAN 関連の設定も削除されます。</p>
制限事項	-
注意事項	<p>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 <b>switchport trunk allowed vlan all</b> 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。</p> <p>本コマンドで物理ポートをトランクポートとして設定する場合、およびトランクポートとして設定した物理ポートを他の VLAN モードに変更する場合は、複数インターフェースの範囲設定モード (<b>interface range port</b> コマンド) は使用せず、単一インターフェースのインターフェース設定モード (<b>interface port</b> コマンド) を使用してください。</p>
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	<b>switchport access vlan</b> <i>VLAN-ID</i> <b>no switchport access vlan</b>
パラメーター	<i>VLAN-ID</i> ：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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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	<b>switchport trunk allowed vlan</b> {all   [add   remove   except] <i>VLAN-ID</i> [,  -]} <b>no switchport trunk allowed vlan</b>
パラメーター	<b>all</b> ：すべての VLAN を許可する場合に指定します。 <b>add</b> (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	
	<p><b>remove</b> (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。</p> <p><b>except</b> (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。</p> <p><i>VLAN-ID</i> : VLAN ID を指定します。複数指定できます。<b>add</b> 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。</p>
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	<p>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 (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>トランクモードのインターフェースで設定できます。</p> <p>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。</p> <p><b>switchport trunk native vlan tag</b> 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。</p>
制限事項	-
注意事項	<p><b>add</b> 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 <b>add</b> 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、<b>remove</b> パラメーターを指定して設定してください。</p> <p>VLAN の設定を行う場合は、インターフェース指定時に <b>interface range port</b> コマンドを使用せずに <b>interface port</b> コマンドを使用してください。</p>
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	<b>switchport trunk native vlan {VLAN-ID   tag}</b> <b>no switchport trunk native vlan [tag]</b>
パラメーター	<p><i>VLAN-ID</i> : 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。</p> <p><b>tag</b> : 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。</p>
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)

switchport trunk native vlan	
特権レベル	レベル : 12
ガイドライン	<p>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 (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>トランクモードのインターフェースで設定できます。</p> <p>ネイティブ VLAN を使用する場合は、ネイティブ VLAN も <b>switchport trunk allowed vlan</b> コマンドで許可 VLAN として追加する必要があります。</p> <p>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、<b>acceptable-frame</b> コマンドで設定します。</p>
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	<b>switchport hybrid allowed vlan</b> {[add] {tagged   untagged}   remove} <b>VLAN-ID</b> [,  -] <b>no switchport hybrid allowed vlan</b>
パラメーター	<p><b>add</b> (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。</p> <p><b>remove</b> : 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。</p> <p><b>tagged</b> : 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。</p> <p><b>untagged</b> : 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。</p> <p><b>VLAN-ID</b> : VLAN ID を指定します。複数指定できます。<b>add</b> 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。</p>
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	<p>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 (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>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。</p> <p>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 <b>add tagged</b> 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。</p>

switchport hybrid allowed vlan	
	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 <b>add untagged</b> 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	<b>add</b> 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 <b>add</b> 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、 <b>remove</b> パラメーターを指定して設定してください。  VLAN の設定を行う場合は、インターフェース指定時に <b>interface range port</b> コマンドを使用せずに <b>interface port</b> 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	<b>switchport hybrid native vlan</b> <i>VLAN-ID</i> <b>no switchport hybrid native vlan</b>
パラメーター	<i>VLAN-ID</i> : 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 ( <b>interface port-channel</b> 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 <b>switchport hybrid allowed vlan</b> コマンドで許可 VLAN として追加する必要があります。  <b>switchport hybrid allowed vlan untagged</b> 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。 <b>switchport hybrid allowed vlan tagged</b> で追加した場合は、ネイティブ VLAN からタグ付きフレームとして送信します。なお、受信時の受け入れ可能なフレームタイプは、 <b>acceptable-frame</b> 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	<code>protocol-vlan profile PROFILE-ID frame-type {ethernet2   snap   llc} ether-type TYPE-VALUE</code> <code>no protocol-vlan profile PROFILE-ID</code>
パラメーター	<i>PROFILE-ID</i> ：プロトコルグループ ID を 1～16 の範囲で指定します。 <i>frame-type</i> ：フレームタイプを以下の中から指定します。 <ul style="list-style-type: none"> <li>• <b>ethernet2</b>：イーサネット II フレーム</li> <li>• <b>snap</b>：IEEE 802.2 SNAP フレーム</li> <li>• <b>llc</b>：IEEE 802.2 LLC フレーム</li> </ul> <i>TYPE-VALUE</i> ：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。 <ul style="list-style-type: none"> <li>• <b>ethernet2</b> を指定した場合は、イーサタイプと比較します。</li> <li>• <b>snap</b> を指定した場合は、SNAP ヘッダーのタイプと比較します。</li> <li>• <b>llc</b> を指定した場合は、LLC ヘッダーの DSAP/SSAP と比較します。</li> </ul>
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 <b>protocol-vlan profile (Interface)</b> 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	<code>protocol-vlan profile PROFILE-ID vlan VLAN-ID [priority COS-VALUE]</code>

protocol-vlan profile (Interface)	
	<b>no protocol-vlan profile</b> [ <i>PROFILE-ID</i> ]
パラメーター	<i>PROFILE-ID</i> : プロトコルグループ ID を 1~16 の範囲で指定します。 <i>VLAN-ID</i> : 受信 VLAN を 1~4094 の範囲で指定します。 <b>priority</b> <i>COS-VALUE</i> (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 ( <b>interface port-channel</b> 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せん。 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	<b>acceptable-frame</b> {tagged-only   untagged-only   admit-all} <b>no acceptable-frame</b>
パラメーター	<b>tagged-only</b> : タグ付きフレームのみを受け入れる場合に指定します。 <b>untagged-only</b> : タグなしフレームのみを受け入れる場合に指定します。 <b>admit-all</b> : 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)
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 ( <b>interface port-channel</b> 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	<b>ingress-checking</b> <b>no ingress-checking</b>
パラメーター	なし
デフォルト	有効 ( <b>ingress-checking</b> )
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 ( <b>interface port-channel</b> 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	<b>show vlan</b> [ <i>VLAN-ID</i> [, -]   <b>interface</b> [ <i>INTERFACE-ID</i> [, -]]   <b>detail</b> ]
パラメーター	<i>VLAN-ID</i> (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。  <b>interface</b> ：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。 <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b>：物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b>：ポートチャネルを指定します。</li> </ul> <b>detail</b> (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



show vlan	
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、すべての VLAN のメンバーポート情報が表示されます。 インターフェースを指定しない場合、すべてのインターフェースの VLAN 関連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：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 : 1/0/1-1/0/2,1/0/17-1/0/22 ... (5)
VLAN 100
  Name : VLAN0100
  Description :
  Tagged Member Ports : 1/0/2,1/0/21-1/0/23
  Untagged Member Ports : 1/0/3-1/0/8
VLAN 200
  Name : VLAN0200
  Description :
  Tagged Member Ports : 1/0/2,1/0/21-1/0/23
  Untagged Member Ports : 1/0/9-1/0/16
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)	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 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 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

```

```

+-----+ +-----+ +-----+
Port Mode 1 aaaaaaaaa aaaaaaaaa aaaaaaxx
Port Mode 2 aaaaaaaaa aaaaaaaaa aaaaaaxx

--- vlan mapping information --- ... (2)
      u = untag  t = tag
      C Port
      1      8 9      16 17      24
Name      VID  +-----+ +-----+ +-----+
default   1 1 uuuuuuuu uuuuuuuu uuuuuuux
default   1 2 uuuuuuuu uuuuuuuu uuuuuuux

```

項番	説明
(1)	ポートの VLAN モードを表示します。 "C"はスタックのボックス ID (シャーシ ID) を示します。スタックを構成していない場合は 1 が表示されます。
(2)	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"はスタックのボックス ID (シャーシ ID) を示します。スタックを構成していない場合は 1 が表示されます。

### 5.16.14 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	<code>show protocol-vlan {profile [PROFILE-ID [, -]]   interface [INTERFACE-ID [, -]]}</code>
パラメーター	<p><b>profile</b> : 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。</p> <p><b>PROFILE-ID</b> (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。</p> <p><b>interface</b> : 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。</p> <p><b>INTERFACE-ID</b> (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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	<p>プロトコルグループ ID を指定しない場合、すべてのプロトコルグループの設定情報が表示されます。</p> <p>インターフェースを指定しない場合、すべてのインターフェースのプロトコル VLAN 識別設定が表示されます。</p>
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) Interface	(2) Protocol Group ID	(3) VLAN	(4) 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)	インターフェース ID 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	<p><b>community</b> : 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。</p> <p><b>isolated</b> : 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。</p> <p><b>primary</b> : 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。</p>
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	<b>private-vlan association</b> { <b>add</b> <i>SECONDARY-VLAN-ID</i> [,  -]   <b>remove</b> <i>SECONDARY-VLAN-ID</i> [,  -]} <b>no private-vlan association</b>
パラメーター	<b>add</b> <i>SECONDARY-VLAN-ID</i> : 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。 <b>remove</b> <i>SECONDARY-VLAN-ID</i> : 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	<b>switchport mode private-vlan {host   promiscuous}</b> <b>no switchport mode</b>
パラメーター	<b>host</b> : 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。  <b>promiscuous</b> : 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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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、 <b>switchport mode private-vlan host</b> コマンドでポートモードを設定し、 <b>switchport private-vlan host-association</b> 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、 <b>switchport mode private-vlan promiscuous</b> コマンドでポートモードを設定し、 <b>switchport private-vlan mapping</b> 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、 <b>switchport mode trunk</b> コマンドでポートモードを設定し、 <b>switchport trunk allowed vlan</b> 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	<b>switchport private-vlan host-association PRIMARY-VLAN-ID SECONDARY-VLAN-ID</b> <b>no switchport private-vlan host-association</b>
パラメーター	<b>PRIMARY-VLAN-ID</b> : 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。  <b>SECONDARY-VLAN-ID</b> : 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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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VLAN の場合、ポートはコミュニティポートになります。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	<b>switchport private-vlan mapping</b> <i>PRIMARY-VLAN-ID</i> { <b>add</b> <i>SECONDARY-VLAN-ID</i> [,  -]   <b>remove</b> <i>SECONDARY-VLAN-ID</i> [,  -]}  <b>no switchport private-vlan mapping</b>
パラメーター	<i>PRIMARY-VLAN-ID</i> : 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。  <b>add</b> <i>SECONDARY-VLAN-ID</i> : 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。  <b>remove</b> <i>SECONDARY-VLAN-ID</i> : 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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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	<b>show vlan private-vlan</b>
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)	役割を表示します。 Isolated : 独立ポート Community : コミュニティーポート
(4)	インターフェース ID を表示します。

### 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

private-vlan synchronize	
	を同期させます。
シンタックス	<b>private-vlan synchronize</b>
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。 <b>private-vlan synchronize</b> 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、 <b>show spanning-tree mst configuration</b> 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 <i>VALUE</i> no dot1q inner ethertype
パラメーター	<i>VALUE</i> : 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 <i>VALUE</i> no dot1q tunneling ethertype
パラメーター	<i>VALUE</i> : 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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <b>interface port-channel</b> 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	<p><b>VLAN 変換エントリー :</b></p> <pre>switchport vlan mapping original-vlan ORIGINAL-VLAN [ORIGINAL-INNER-VLAN] resultant-vlan RESULTANT-VLAN [RESULTANT-INNER-VLAN] [priority COS-VALUE]</pre> <p><b>サービス VLAN マッピングエントリー :</b></p> <pre>switchport vlan mapping original-vlan ORIGINAL-VLAN [,  -] dot1q-tunnel DOTIQ-TUNNEL-VLAN [priority COS-VALUE]</pre> <pre>no switchport vlan mapping original-vlan ORIGINAL-VLAN [,  -] [ORIGINAL-INNER-VLAN]</pre>
パラメーター	<p><b>ORIGINAL-VLAN :</b> 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。</p> <p><b>ORIGINAL-INNER-VLAN (省略可能) :</b> 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。</p> <p><b>resultant-vlan RESULTANT-VLAN :</b> 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。</p> <p><b>RESULTANT-INNER-VLAN (省略可能) :</b> 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。</p> <p><b>dot1q-tunnel DOTIQ-TUNNEL-VLAN :</b> 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。</p> <p><b>priority COS-VALUE (省略可能) :</b> 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。</p>
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	<p>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 (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>〈VLAN 変換エントリー〉</p> <p><b>resultant-vlan RESULTANT-VLAN</b> 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 <b>ORIGINAL-VLAN</b> と一致した場合に、<b>RESULTANT-VLAN</b> 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 <b>RESULTANT-VLAN</b> と一致した場合に、<b>ORIGINAL-VLAN</b> で指定した VLAN ID に変換されます。</p> <p>トランクポートにおいて <b>switchport vlan mapping original-vlan ORIGINAL-VLAN ORIGINAL-INNER-VLAN resultant-vlan RESULTANT-VLAN RESULTANT-INNER-</b></p>

switchport vlan mapping	
	<p>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、<i>ORIGINAL-INNER-VLAN</i> を指定して <i>RESULTANT-INNER-VLAN</i> 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。</p> <p>トンネルポートで VLAN 変換エントリーを使用する場合は、<b>switchport vlan mapping original-vlan ORIGINAL-VLAN resultant-vlan RESULTANT-VLAN</b> コマンドを使用します。<i>ORIGINAL-INNER-VLAN</i> と <i>RESULTANT-INNER-VLAN</i> 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 <i>ORIGINAL-VLAN</i> 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 <i>ORIGINAL-VLAN</i> のカスタマーVLAN タグを付加して送信します。</p> <p>&lt;サービス VLAN マッピングエントリー&gt;</p> <p><b>dot1q-tunnel DOT1Q-TUNNEL-VLAN</b> 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 <i>ORIGINAL-VLAN</i> と一致した場合に、<i>DOT1Q-TUNNEL-VLAN</i> で指定した VLAN で受信します。</p> <p>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 <b>vlan mapping miss drop</b> 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。<b>vlan mapping miss drop</b> コマンドが無効の場合には、<b>switchport access vlan</b> 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。</p>
制限事項	<p>すでに「<i>ORIGINAL-VLAN</i> (A), <i>RESULTANT-VLAN</i> (B)」の VLAN 変換エントリーが設定されている場合には、別の <i>ORIGINAL-VLAN</i> (A 以外) を設定済みの <i>RESULTANT-VLAN</i> (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、<i>ORIGINAL-VLAN</i> (A) を別の <i>RESULTANT-VLAN</i> (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。</p> <p>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。</p> <p>VLAN タグ変換機能と RPVST+ を同一ポートで併用できません。</p>
注意事項	<p><i>RESULTANT-INNER-VLAN</i> を指定しない形式 (<b>switchport vlan mapping original-vlan ORIGINAL-VLAN ORIGINAL-INNER-VLAN resultant-vlan RESULTANT-VLAN</b>) で設定した場合は、<i>RESULTANT-INNER-VLAN</i> を <i>ORIGINAL-INNER-VLAN</i> 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)</p>
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	<b>vlan mapping profile</b> <i>PROFILE-ID</i> [ <b>type</b> <i>PROFILE-TYPE</i> ] <b>no vlan mapping profile</b> <i>PROFILE-ID</i>
パラメーター	<i>PROFILE-ID</i> : VLAN マッピングプロファイルの 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。  <b>type</b> <i>PROFILE-TYPE</i> (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。 <ul style="list-style-type: none"> <li>• <b>ethernet</b>: 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。</li> <li>• <b>ip</b>: IP パケットの情報を対象とする場合に指定します。</li> <li>• <b>ipv6</b>: IPv6 パケットの情報を対象とする場合に指定します。</li> <li>• <b>ethernet ip</b>: 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。</li> </ul> それぞれのタイプで使用できる抽出条件は、 <b>vlan mapping rule</b> 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 <b>type</b> 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	<b>rule</b> [ <i>SEQ</i> ] <b>match</b> <i>CONDITION</i> <b>dot1q-tunnel</b> <b>outer-vid</b> <i>VLAN-ID</i> [ <b>priority</b>

vlan mapping rule	
	<p><i>COS-VALUE</i> [<i>inner-vid</i> <i>VLAN-ID</i>]</p> <p><b>rule</b> [<i>SEQ</i>] <b>match</b> <i>CONDITION</i> <b>translate</b> <i>outer-vid</i> <i>VLAN-ID</i> [<i>priority</i> <i>COS-VALUE</i>]</p> <p><b>no rule</b> <i>SEQ</i> [,  -]</p>
パラメーター	<p><i>SEQ</i> (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。</p> <p><i>CONDITION</i> : 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。</p> <p><b>dot1q-tunnel</b> <i>outer-vid</i> <i>VLAN-ID</i> : 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。</p> <p><b>priority</b> <i>COS-VALUE</i> (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。</p> <p><b>inner-vid</b> <i>VLAN-ID</i> (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。</p> <p><b>translate</b> <i>outer-vid</i> <i>VLAN-ID</i> : 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。</p>
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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul> <p><b>inner-vid</b> 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。</p> <p>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。</p>
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	<b>src-mac</b> <i>SRC-MAC-ADDR</i> : 送信元 MAC アドレスを指定
宛先 MAC アドレス	<b>dst-mac</b> <i>DST-MAC-ADDR</i> : 宛先 MAC アドレスを指定
CoS	<b>priority</b> <i>COS-VALUE</i> : カスタマー-VLAN タグの優先度を 0~7 の範囲で指定
VLAN ID	<b>inner-vid</b> <i>VLAN-ID</i> : 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	<b>ether-type</b> <i>TYPE</i> : イーサタイプを 0x0~0xFFFF の範囲で指定
送信元 IP アドレス	<b>src-ip</b> <i>SRC-IP-ADDR/SUBNET-MASK</i> : 送信元 IPv4 アドレスを指定
宛先 IP アドレス	<b>dst-ip</b> <i>DST-IP-ADDR/SUBNET-MASK</i> : 宛先 IPv4 アドレスを指定
DSCP	<b>dscp</b> <i>DSCP</i> : DSCP を 0~63 の範囲で指定します。
送信元 L4 ポート番号	<b>src-port</b> <i>SRC-L4-PORT</i> : 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	<b>dst-port</b> <i>DST-L4-PORT</i> : 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	<b>ip-protocol</b> <i>PROTOCOL-ID</i> : 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	<b>src-ipv6</b> <i>SRC-IPV6-ADDR/PREFIX-LENGTH</i> : 送信元 IPv6 アドレスを指定
宛先 IPv6 アドレス	<b>dst-ipv6</b> <i>DST-IPV6-ADDR/PREFIX-LENGTH</i> : 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	<b>switchport vlan mapping profile</b> <i>PROFILE-ID</i> <b>no switchport vlan mapping profile</b> <i>PROFILE-ID</i>
パラメーター	<i>PROFILE-ID</i> : VLAN マッピングプロファイルの 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

switchport vlan mapping profile	
	<p>モード (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>トンネルモードのインターフェースで設定できます。</p> <p>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。</p> <p>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。</p> <p>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。</p>
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、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	<b>vlan mapping miss drop</b> <b>no vlan mapping miss drop</b>
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	<p>ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>トンネルモードのインターフェースで設定できます。</p> <p>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 (<b>switchport vlan mapping original-vlan dot1q-tunnel</b> コマンド)、もしくは VLAN マッピングルール (<b>vlan mapping rule</b> コマンド) に一致しない場合に破棄されます。</p> <p>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。</p>

vlan mapping miss drop	
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	<b>dot1q-tunnel trust inner-priority</b> <b>no dot1q-tunnel trust inner-priority</b>
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	<p>ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード (<b>interface port-channel</b> コマンド) で設定してください。</p> <p>トンネルモードのインターフェースで設定できます。</p> <p>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。</p> <p>本機能とサービス VLAN マッピングエントリ (<b>switchport vlan mapping original-vlan dot1q-tunnel</b> コマンド) の <b>priority</b> オプションでは、本機能の方が優先されます。</p> <p>本機能と VLAN マッピングルール (<b>vlan mapping rule</b> コマンド) の <b>priority</b> オプションでは、VLAN マッピングルールの <b>priority</b> オプションの方が優先されます。</p>
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	<code>dot1q-tunnel insert dot1q-tag DOT1Q-VLAN</code> <code>no dot1q-tunnel insert dot1q-tag</code>
パラメーター	<i>DOT1Q-VLAN</i> : 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	ポートチャンネルで設定する場合は、対象ポートチャンネルのインターフェース設定モード ( <code>interface port-channel</code> 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 ( <code>vlan mapping rule</code> 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	<code>show dot1q ethertype [interface INTERFACE-ID [, [-]]</code>
パラメーター	<code>interface INTERFACE-ID</code> (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。 <ul style="list-style-type: none"> <li>• <code>port</code> : 物理ポートを指定します。複数指定できます。</li> <li>• <code>port-channel</code> : ポートチャンネルを指定します。</li> </ul>
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、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。

show dot1q ethertype	
	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インターフェース ID 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	<b>show vlan mapping</b> [ <b>interface</b> <i>INTERFACE-ID</i> [,  -]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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、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)	インターフェース ID 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	<code>show dot1q-tunnel [interface <i>INTERFACE-ID</i> [,  -]]</code>
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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、すべてのトンネルポートが表示されます。 トンネル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 : 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-channell
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インターフェース ID 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	<b>show vlan mapping profile</b> [ <i>PROFILE-ID</i> ]
パラメーター	<i>PROFILE-ID</i> (省略可能) : VLAN マッピングプロファイルの 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	VLAN マッピングプロファイルの ID を指定しない場合、すべての VLAN マッピングプロファイルが表示されます。
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。



## 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 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 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 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	<b>ip route</b> { <i>DST-NETWORK-PREFIX PREFIX-MASK</i>   <i>NETWORK-ADDRESS/MASK-LENGTH</i> } <i>IP-ADDRESS</i> [ <b>primary</b>   <b>backup</b> ] <b>no ip route</b> { <i>DST-NETWORK-PREFIX PREFIX-MASK</i>   <i>NETWORK-ADDRESS/MASK-LENGTH</i> } <i>IP-ADDRESS</i>
パラメーター	<i>DST-NETWORK-PREFIX PREFIX-MASK</i> : 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) <i>NETWORK-ADDRESS/MASK-LENGTH</i> : 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) <i>IP-ADDRESS</i> : ネクストホップの IP アドレスを指定します。 <b>primary</b> (省略可能): プライマリルートを設定する場合に指定します。 <b>backup</b> (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 (プライマリルート、バックアップルート) を設定することができます。

ip route	
	<p>オプションパラメーターを省略して設定した場合は、<b>primary</b> パラメーターが自動的に付与されてプライマリルートとして設定されます。すでに同一ネットワーク宛でのプライマリルートが設定されている場合は、<b>backup</b> 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。</p> <p>プライマリ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。</p>
制限事項	<p>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有されていて、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 エントリーとなります。</p>
注意事項	<p>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。</p>
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)#
```

### 6.1.2 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	<p><b>ipv6 route</b> {default   NETWORK-PREFIX/PREFIX-LENGTH} [INTERFACE-NAME] NEXT-HOP-ADDRESS [<b>primary</b>   <b>backup</b>]</p> <p><b>no ipv6 route</b> {default   NETWORK-PREFIX/PREFIX-LENGTH} [INTERFACE-NAME] NEXT-HOP-ADDRESS</p>
パラメーター	<p><b>default</b> : デフォルトルートを設定する場合に指定します。</p> <p><i>NETWORK-PREFIX/PREFIX-LENGTH</i> : 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。</p> <p><i>INTERFACE-NAME</i> (省略可能) : 転送先インターフェース (<b>vlan</b> と VLAN ID の間を空けない形式) を指定します。</p> <p><i>NEXT-HOP-ADDRESS</i> : 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。</p> <p><b>primary</b> (省略可能) : プライマリルートを設定する場合に指定します。</p> <p><b>backup</b> (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。</p>
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

ipv6 route	
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、 <b>primary</b> 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でのプライマリールートが設定されている場合は、 <b>backup</b> 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有されていて、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せん。
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)#
```

### 6.1.3 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	<b>show ip route</b> [ <i>IP-ADDRESS</i> [ <i>MASK</i> ]   <i>PROTOCOL</i>   <b>hardware</b> ]
パラメーター	<i>IP-ADDRESS</i> (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。  <i>IP-ADDRESS MASK</i> (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。  <i>PROTOCOL</i> (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。 <ul style="list-style-type: none"> <li>• <b>connected</b> : 自装置に直接接続されているネットワーク。</li> <li>• <b>static</b> : スタティックルートで設定されたルート情報。</li> </ul> <b>hardware</b> (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	-

show ip route	
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 ID を表示します。

#### 6.1.4 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	<b>show ip route summary</b>
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。

### 6.1.5 show ipv6 route

show ipv6 route	
目的	IPv6 ルーティングテーブルを表示します。
シンタックス	<code>show ipv6 route [[<i>IPv6-ADDRESS</i>   <i>NETWORK-PREFIX/PREFIX-LENGTH</i> [<i>longer-prefixes</i>]   <i>interface</i> <i>INTERFACE-NAME</i>   <i>PROTOCOL</i>] [<i>database</i>]   <i>hardware</i>]</code>
パラメーター	<p><i>IPv6-ADDRESS</i> (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。</p> <p><i>NETWORK-PREFIX/PREFIX-LENGTH</i> (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。</p> <p><b>longer-prefixes</b> (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。</p> <p><b>interface</b> <i>INTERFACE-NAME</i> (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 (<b>vlan</b> と VLAN ID の間を空けない形式) を指定します。</p> <p><i>PROTOCOL</i> (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。</p> <ul style="list-style-type: none"> <li><b>connected</b> : 自装置に直接接続されているネットワーク。</li> <li><b>static</b> : スタティックルートで設定されたルート情報。</li> </ul> <p><b>database</b> (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を表示する場合に指定します。</p> <p><b>hardware</b> (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。</p>
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)

## 6 レイヤー3 | 6.1 プロトコル非依存コマンド

```

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IDを表示します。

### 6.1.6 show ipv6 route summary

show ipv6 route summary	
目的	IPv6 ルーティングテーブルの概要情報を表示します。
シンタックス	<b>show ipv6 route summary</b>
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	<p><b>group-addr</b> 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。</p> <p><b>source-addr</b> 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。</p>
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	<p>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 256 です。</p> <p>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、<b>show ipv6 mroute forwarding-cache</b> コマンドも合わせてご確認ください。</p>
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	<p><b>group-addr</b> 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。</p> <p><b>source-addr</b> 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。</p>
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	<p>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 128 です。</p> <p>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、<b>show ip mroute forwarding-cache</b> コマンドも合わせてご確認ください。</p>
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
packet-buffer mode	packet-buffer mode MODE no packet-buffer mode
mls qos scheduler	mls qos scheduler {sp   rr   wrr   wdrp} no mls qos scheduler
wrr-queue bandwidth	wrr-queue bandwidth WEIGHT0...WEIGHT7 no wrr-queue bandwidth
wdrp-queue bandwidth	wdrp-queue bandwidth QUANTUM0...QUANTUM7 no wdrp-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 MAP-NAME no mls qos dscp-mutation
mls qos map dscp-mutation	mls qos map dscp-mutation MAP-NAME DSCP-LIST to OUTPUT-DSCP no mls qos map dscp-mutation 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] NAME no 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 NAME no policy-map NAME
class (QoS)	class NAME no class 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 NAME no police
mls qos aggregate-policer	mls qos aggregate-policer NAME KBPS [BURST-NORMAL [BURST-MAX]] [conform-action ACTION] exceed-action ACTION [violate-action ACTION] [color-aware] mls qos aggregate-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 NAME
service-policy	service-policy {input   output} NAME no service-policy {input   output}

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 interface	show mls qos interface [INTERFACE-ID [, -]] {cos   scheduler   trust   rate-limit   queue-rate-limit   dscp-mutation   map {dscp-color   cos-color   dscp-cos}}
show mls qos queueing	show mls qos queueing [interface INTERFACE-ID [, -]]
show mls qos map dscp-mutation	show mls qos map dscp-mutation [MAP-NAME]
show class-map	show class-map [NAME]

コマンド	コマンドとパラメーター
show policy-map	show policy-map [POLICY-NAME   interface INTERFACE-ID]
show mls qos aggregate-policer	show mls qos aggregate-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	<b>priority-queue cos-map</b> <i>QUEUE-ID</i> <i>COS-LIST</i> <b>no priority-queue cos-map</b>
パラメーター	<i>QUEUE-ID</i> : 送信キューを 0~7 の範囲で指定します。 <i>COS-LIST</i> : 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	-
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 packet-buffer mode

packet-buffer mode									
目的	ポートの各送信キューに割り当てるパケットバッファの最大値を設定します。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	<b>packet-buffer mode</b> <i>MODE</i> <b>no packet-buffer mode</b>								
パラメーター	<i>MODE</i> : パケットバッファの最大値を決定するモードを 1~3 の範囲で指定します。以下に、各モードでのポートの各送信キューに割り当て可能な最大バッファ量と、最大パケット数を示します。								
	<table border="1"> <thead> <tr> <th>設定値</th> <th>ポート種別</th> <th>1 キュー当たりの最大データ量(kB)</th> <th>1 キュー当たりの最大パケット数</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	設定値	ポート種別	1 キュー当たりの最大データ量(kB)	1 キュー当たりの最大パケット数				
設定値	ポート種別	1 キュー当たりの最大データ量(kB)	1 キュー当たりの最大パケット数						

packet-buffer mode				
	<b>mode 1</b>	UTP ポート	65	320
		SFP/SFP+ ポート	154	760
	<b>mode 2</b>	全ポート	203	1000
	<b>mode 3</b>	全ポート	406	2000
デフォルト	<b>mode 1</b>			
コマンドモード	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	<p>実際に使用可能なパケットバッファの最大値は、データ量とパケット数のうち、先に割り当て可能な最大値に達したようになります。</p> <p>複数ポートへバッファを割り当てる必要がある場合は、最大値まで割り当てられない可能性があります。</p>			
制限事項	<p><b>mode 2</b> または <b>mode 3</b> で使用する場合は、各ポートで送信キューを 1 個のみ使用する設定、およびネットワークで使用してください。例えば、装置が受信するパケットに複数の 802.1p 優先度が含まれる可能性がある場合は、<b>priority-queue cos-map</b> コマンドで、すべての CoS を 1 つの送信キューへマッピングするよう設定してください。</p>			
注意事項	<p>本設定を変更する場合は、マネージメントポートを除く全ポートで通信が行われていない状態で行ってください。また、スタック構成で本設定を変更する場合は、一度スタック構成を外し、各装置で個別に設定を変更してから、再度スタックを構成してください。</p>			
対象バージョン	1.02.02			

使用例：パケットバッファの最大値を決定するモードを **mode 3** に設定する方法を示します。

```
# configure terminal
(config)# packet-buffer mode 3
(config)#
```

### 7.1.3 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	<b>mls qos scheduler {sp   rr   wrr   wdrr}</b> <b>no mls qos scheduler</b>
パラメーター	<p><b>sp</b> : Strict Priority Queuing に設定する場合に指定します。</p> <p><b>rr</b> : Round Robin スケジューリングに設定する場合に指定します。</p> <p><b>wrr</b> : 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。</p> <p><b>wdrr</b> : 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。</p>
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)

mls qos scheduler	
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)#
```

### 7.1.4 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	<b>wrr-queue bandwidth</b> <i>WEIGHT0...WEIGHT7</i> <b>no wrr-queue bandwidth</b>
パラメーター	<i>WEIGHT0...WEIGHT7</i> : WRR スケジューリングの各送信キューの重みを 0~127 の範囲で指定します。
デフォルト	すべての送信キューの重み : 1
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、 <b>mls qos scheduler</b> 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 で動作しません。
制限事項	ApresiaNP4000 シリーズにおいて、重みが 0 のキュー設定を、重みが 0 以外のキュー設定を跨いで設定することはサポートしていません。(例 : wrr-queue bandwidth 0 0 1 1 0 0 1 1 のような設定は不可)
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)#
```

### 7.1.5 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。

wdr queue bandwidth	
	デフ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	<b>wdr queue bandwidth</b> <i>QUANTUM0... QUANTUM7</i> <b>no wdr queue bandwidth</b>
パラメーター	<i>QUANTUM0... QUANTUM7</i> : 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、 <b>mls qos scheduler</b> 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	ApresiaNP4000 シリーズにおいて、重みが 0 のキュー設定を、重みが 0 以外のキュー設定を跨いで設定することはサポートしていません。(例: wdr queue bandwidth 0 0 1 1 0 0 1 1 のような設定は不可)
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 wdr
(config-if-port)# wdr queue bandwidth 1 2 3 4 5 6 7 8
(config-if-port)#
```

### 7.1.6 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	<b>mls qos trust</b> {cos   dscp} <b>no mls qos trust</b>
パラメーター	<b>cos</b> : 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。 <b>dscp</b> : 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、 <b>mls qos cos</b> 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、 <b>mls qos map dscp-cos</b> 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

mls qos trust	
	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>受信 VLAN を決定する方法が <b>switchport vlan mapping</b> コマンド、または <b>switchport access vlan</b> 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。 <ul style="list-style-type: none"> <li>「受信トラフィックの CoS を信頼するモード」の場合は、<b>switchport vlan mapping</b> コマンドなら <b>switchport vlan mapping</b> コマンドの <b>priority</b> オプション、<b>switchport access vlan</b> コマンドなら <b>mls qos cos</b> コマンドで設定したデフォルトの CoS 値が適用されます。</li> <li>「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。</li> <li><b>mls qos cos</b> コマンドの <b>override</b> 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。</li> </ul> </li> <li>受信 VLAN を決定する方法が <b>vlan mapping rule</b> コマンドの場合は、<b>mls qos trust</b> コマンドや <b>mls qos cos</b> コマンドの設定にかかわらず、<b>vlan mapping rule</b> コマンドの <b>priority</b> オプションにより装置内部の優先度が決定されます。</li> </ul> <p>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 <b>mls qos map cos-color</b> 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 <b>mls qos map dscp-color</b> コマンドの「DSCP からトラフィック初期カラーへのマッピング」が反映されます。</p>
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)#
```

### 7.1.7 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	<b>mls qos cos {COS-VALUE   override}</b> <b>no mls qos cos</b>
パラメーター	<p><b>COS-VALUE</b>：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。</p> <p><b>override</b>：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。</p>

mls qos cos	
デフォルト	デフォルトの CoS 値 : 0 <b>override</b> 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	<p><b>mls qos trust</b> 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。</p> <p>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、<b>override</b> 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。</p> <p>トンネルポートで、<b>vlan mapping rule</b> コマンドによって受信 VLAN が決定される場合は、<b>mls qos trust</b> コマンドや <b>mls qos cos</b> コマンドの設定にかかわらず、<b>vlan mapping rule</b> コマンドの <b>priority</b> オプションにより装置内部の優先度が決定されます。</p>
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)#
```

### 7.1.8 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	<b>mls qos map dscp-cos</b> <i>DSCP-LIST</i> to <i>COS-VALUE</i> <b>no mls qos map dscp-cos</b> <i>DSCP-LIST</i>
パラメーター	<p><i>DSCP-LIST</i> : 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。</p> <p><i>COS-VALUE</i> : CoS を 0~7 の範囲で指定します。</p>
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



mls qos map dscp-cos	
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、 <b>mls qos trust</b> 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)#
```

### 7.1.9 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	<b>mls qos map cos-color</b> <i>COS-LIST</i> to {green   yellow   red} <b>no mls qos map cos-color</b>
パラメーター	<i>COS-LIST</i> : 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。  <b>green</b> : 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。 <b>yellow</b> : 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。 <b>red</b> : 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 = <b>green</b>
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、 <b>mls qos trust</b> 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	-
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)#
```

### 7.1.10 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

mls qos map dscp-color	
	ます。デフ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	<b>mls qos map dscp-color</b> <i>DSCP-LIST</i> to { <b>green</b>   <b>yellow</b>   <b>red</b> } <b>no mls qos map dscp-color</b> <i>DSCP-LIST</i>
パラメーター	<i>DSCP-LIST</i> : 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。  <b>green</b> : 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。 <b>yellow</b> : 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。 <b>red</b> : 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 = <b>green</b>
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、 <b>mls qos trust</b> 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)#
```

### 7.1.11 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	<b>mls qos dscp-mutation</b> <i>MAP-NAME</i> <b>no mls qos dscp-mutation</b>
パラメーター	<i>MAP-NAME</i> : 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、 <b>mls qos trust</b> 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。 <ul style="list-style-type: none"> <li>• <b>mls qos map dscp-cos</b> コマンドで設定した「DSCP から CoS へのマッピング」</li> </ul>

mls qos dscp-mutation	
	<ul style="list-style-type: none"> <li>• <b>mls qos map dscp-color</b> 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」</li> <li>• <b>service-policy input</b> 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</li> </ul>
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)#
```

### 7.1.12 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	<b>mls qos map dscp-mutation</b> <i>MAP-NAME</i> <i>DSCP-LIST</i> to <i>OUTPUT-DSCP</i> <b>no mls qos map dscp-mutation</b> <i>MAP-NAME</i>
パラメーター	<i>MAP-NAME</i> : DSCP 変換マップ名を最大 32 文字で指定します。スペースは設定できません。  <i>DSCP-LIST</i> : 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。  <i>OUTPUT-DSCP</i> : 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、 <b>mls qos dscp-mutation</b> 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)#
```

## 7.1.13 queue rate-limit

queue rate-limit	
目的	キューに割り当てる帯域を、指定または変更します。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	<b>queue</b> <i>QUEUE-ID</i> <b>rate-limit</b> { <i>MIN-BANDWIDTH-KBPS</i>   <b>percent</b> <i>MIN-PERCENTAGE</i> } { <i>MAX-BANDWIDTH-KBPS</i>   <b>percent</b> <i>MAX-PERCENTAGE</i> } <b>no queue</b> <i>QUEUE-ID</i> <b>rate-limit</b>
パラメーター	<i>QUEUE-ID</i> : 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。 <i>MIN-BANDWIDTH-KBPS</i> : 指定したキューに割り当てる最小保証帯域を、8～10,000,000(Kbps)の範囲で指定します。 <b>percent</b> <i>MIN-PERCENTAGE</i> : 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。 <i>MAX-BANDWIDTH-KBPS</i> : 指定したキューの最大帯域をKbpsで指定します。 <b>percent</b> <i>MAX-PERCENTAGE</i> : 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	キューを指定して、最小帯域と最大帯域を設定するコマンドです。最小帯域を設定すると、キューから送信されるパケットが保証されます。最大帯域を設定すると、キューから送信されるパケットは、帯域が使用可能であっても最大帯域を超えません。 <i>MIN-BANDWIDTH-KBPS</i> パラメーターと <i>MAX-BANDWIDTH-KBPS</i> 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8Kbps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	本コマンドの設定は、ポートだけに適用でき、ポートチャンネルには適用できません。
注意事項	-
対象バージョン	1.01.01

使用例: ポート 1/0/1 で、キュー1のキュー帯域(最小保証帯域と最大帯域)を、それぞれ100Kbpsと2000Kbpsに設定する方法を示します。キュー2の最小保証帯域と最大帯域を、それぞれ10%と50%に設定しています。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# queue 1 rate-limit 100 2000
(config-if-port)# queue 2 rate-limit percent 10 percent 50
(config-if-port)#
```

## 7.1.14 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	<b>rate-limit input</b> { <i>KBPS</i>   <b>percent</b> <i>PERCENTAGE</i> } [ <i>BURST-SIZE</i> ] <b>no rate-limit input</b>
パラメーター	<i>KBPS</i> : 受信帯域制限値を 8~10,000,000 (Kbps) の範囲で指定します。 <b>percent</b> <i>PERCENTAGE</i> : 受信帯域制限値を 1~100 (%) の範囲で指定します。 <i>BURST-SIZE</i> (省略可能): バーストサイズを 0~128,000 キロバイト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。 <i>KBPS</i> 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 8Kbps 単位に切り捨てた値で動作します。 <i>BURST-SIZE</i> 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	<i>BURST-SIZE</i> 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。 <i>BURST-SIZE</i> 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、 <b>no rate-limit input</b> 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 で受信帯域制限値を 8000Kbps に、バーストサイズを 16 キロバイト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)#
```

## 7.1.15 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	<b>rate-limit output</b> { <i>KBPS</i>   <b>percent</b> <i>PERCENTAGE</i> } [ <i>BURST-SIZE</i> ] <b>no rate-limit output</b>
パラメーター	<i>KBPS</i> : 送信帯域制限値を 8~10,000,000 (Kbps) の範囲で指定します。 <b>percent</b> <i>PERCENTAGE</i> : 送信帯域制限値を 1~100 (%) の範囲で指定します。 <i>BURST-SIZE</i> (省略可能): バーストサイズを 0~128,000 キロバイトの範囲で指定

rate-limit output	
	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	<p>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 8Kbps 単位に切り捨てた値で動作します。</p> <p>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。</p> <p>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。</p>
制限事項	<p>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。</p> <p>BURST-SIZE パラメーターには 0 を設定しないでください。</p>
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、 <b>no rate-limit output</b> 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 512 キロバイト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)#
```

### 7.1.16 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	<pre>class-map [match-all   match-any] NAME no class-map NAME</pre>
パラメーター	<p><b>match-all</b> (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。</p> <p><b>match-any</b> (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。</p> <p><b>NAME</b>：クラスマップ名を最大 32 文字で指定します。</p>
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、クラスの一一致条件を定義する <b>match</b> 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。

class-map	
	<p>複数の <b>match</b> 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、<b>match-all</b> または <b>match-any</b> パラメーターで指定してください。</p> <p><b>match-all</b> も <b>match-any</b> も指定しない場合は、<b>match-any</b> が暗黙で指定されます。</p> <p><b>class-default</b> は、デフォルトクラスの予約名です。</p>
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)#
```

### 7.1.17 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	<p><b>match</b> {<b>access-group name</b> <i>ACCESS-LIST-NAME</i>   <b>cos</b> [<b>inner</b>] <i>COS-LIST</i>   [<b>ip</b>] <b>dscp</b> <i>DSCP-LIST</i>   [<b>ip</b>] <b>precedence</b> <i>IP-PRECEDENCE-LIST</i>   <b>protocol</b> <i>PROTOCOL-NAME</i>   <b>vlan</b> [<b>inner</b>] <i>VLAN-LIST</i>}</p> <p><b>no match</b> {<b>access-group name</b> <i>ACCESS-LIST-NAME</i>   <b>cos</b> [<b>inner</b>] <i>COS-LIST</i>   [<b>ip</b>] <b>dscp</b> <i>DSCP-LIST</i>   [<b>ip</b>] <b>precedence</b> <i>IP-PRECEDENCE-LIST</i>   <b>protocol</b> <i>PROTOCOL-NAME</i>   <b>vlan</b> [<b>inner</b>] <i>VLAN-ID-LIST</i>}</p>
パラメーター	<p><b>access-group name</b> <i>ACCESS-LIST-NAME</i>：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。</p> <p><b>cos</b> <i>COS-LIST</i>：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。</p> <p><b>inner</b> (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。</p> <p><b>ip</b> (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。</p> <p><b>dscp</b> <i>DSCP-LIST</i>：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。</p> <p><b>ip</b> (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。</p>

match	
	<p><b>precedence</b> <i>IP-PRECEDENCE-LIST</i>: 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。</p> <p><b>protocol</b> <i>PROTOCOL-NAME</i>: 一致条件とするプロトコル名を指定します。</p> <p><b>vlan</b> <i>VLAN-ID-LIST</i>: 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。</p> <p><b>inner</b> (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。</p>
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	<p><b>match protocol</b> 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。</p> <ul style="list-style-type: none"> <li>• <b>arp</b> - IP アドレス解決プロトコル (ARP)</li> <li>• <b>bgp</b> - Border Gateway Protocol</li> <li>• <b>dhcp</b> - Dynamic Host Configuration</li> <li>• <b>dns</b> - Domain Name Server ルックアップ</li> <li>• <b>egp</b> - 外部ゲートウェイプロトコル</li> <li>• <b>ftp</b> - ファイル転送プロトコル</li> <li>• <b>ip</b> - IP (バージョン 4)</li> <li>• <b>ipv6</b> - IP (バージョン 6)</li> <li>• <b>netbios</b> - NetBIOS</li> <li>• <b>nfs</b> - ネットワークファイルシステム</li> <li>• <b>ntp</b> - 時刻プロトコル</li> <li>• <b>ospf</b> - Open Shortest Path First</li> <li>• <b>pppoe</b> - Point-to-Point Protocol over Ethernet</li> <li>• <b>rip</b> - ルーティング情報プロトコル</li> <li>• <b>rtsp</b> - Real-Time Streaming Protocol</li> <li>• <b>ssh</b> - Secure Shell</li> <li>• <b>telnet</b> - Telnet</li> <li>• <b>tftp</b> - Trivial File Transfer Protocol (TFTP)</li> </ul> <p><b>match access-group</b> 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。</p> <p><b>match cos [inner]</b>、または <b>match vlan [inner]</b>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</p>



match	
	<p>使用します。</p> <ul style="list-style-type: none"> <li>• 本条件のポリシーマップで <b>set ip dscp</b> を設定している場合</li> <li>• 本条件のポリシーマップで <b>set ip precedence</b> を設定し、受信側(input)に適用している場合</li> </ul> <p><b>match dscp</b>、または <b>match precedence</b> 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。</p> <p><b>match ip dscp</b>、または <b>match ip precedence</b> 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。</p> <p><b>match protocol</b> 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。</p>
制限事項	-
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)#
```

### 7.1.18 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	<b>policy-map</b> <i>NAME</i> <b>no policy-map</b> <i>NAME</i>
パラメーター	<i>NAME</i> : ポリシーマップ名を、最大 32 文字の英数字で指定します。
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	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 <b>match</b> 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)#
```

### 7.1.19 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	<b>class</b> <i>NAME</i>

class (QoS)	
	<b>no class</b> <i>NAME</i>
パラメーター	<i>NAME</i> : 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)#
```

### 7.1.20 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	<b>set</b> {[ip] precedence <i>PRECEDENCE</i>   [ip] dscp <i>DSCP</i>   cos <i>COS</i>   cos-queue <i>COS-QUEUE</i> }  <b>no set</b> {[ip] precedence <i>PRECEDENCE</i>   [ip] dscp <i>DSCP</i>   cos <i>COS</i>   cos-queue <i>COS-QUEUE</i> }
パラメーター	<b>ip</b> (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。  <b>precedence</b> <i>PRECEDENCE</i> : 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。  <b>ip</b> (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。  <b>dscp</b> <i>DSCP</i> : パケットの新しい DSCP を、0~63 の範囲で指定します。

set	
	<p><b>cos</b> <i>COS</i>: 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。</p> <p><b>cos-queue</b> <i>COS-QUEUE</i>: 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。このパラメータはポリシーを受信側 (input) に適用した場合のみ動作します。</p>
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	<p>設定が競合しない場合、1 つのクラスに対して複数の <b>set</b> コマンドを設定できます。</p> <p>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、<b>set cos-queue</b> コマンドを実行してください。</p> <p><b>set dscp</b> コマンドは、CoS キューの選択には影響を与えません。</p> <p><b>set cos-queue</b> コマンドは、送信パケットの CoS 値を変更しません。</p> <p><b>police</b> コマンドと <b>set</b> コマンドは、同じクラスに対して実行できます。</p> <p><b>set [ip] precedence</b> 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。</p>
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、 <b>set cos-queue</b> コマンドによる送信キューの変更は動作しません。
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)#
```

### 7.1.21 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	<p><b>police</b> <i>KBPS</i> [<i>BURST-NORMAL</i> [<i>BURST-MAX</i>]] [<i>conform-action ACTION</i>] <i>exceed-action ACTION</i> [<i>violate-action ACTION</i>] [<i>color-aware</i>]</p> <p><b>no police</b></p>
パラメーター	<p><i>KBPS</i>: 平均レートを 0~10,000,000 (Kbps) の範囲で指定します。</p> <p><i>BURST-NORMAL</i> (省略可能): 標準バーストサイズを 0~16384 キロバイト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 12 キロバイトです。</p>

police	
	<p><b>BURST-MAX</b> (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 0~16384 キロバイト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 12 キロバイトです。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。</p> <p><b>confirm-action ACTION</b> (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。</p> <p><b>exceed-action ACTION</b> : 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。</p> <p><b>violate-action ACTION</b> (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。</p> <p><b>ACTION</b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>drop</b> : パケットを廃棄します。</li> <li>• <b>set-dscp-transmit VALUE</b> : IP DSCP を設定して、新しい IP DSCP でパケットを送信します。</li> <li>• <b>set-lp-transmit VALUE</b> : CoS 値を設定して、新しい CoS 値でパケットを送信します。</li> <li>• <b>transmit</b> : パケットを変更せずに送信します。</li> </ul> <p><b>color-aware</b> (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。</p>
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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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 <b>confirm-action</b>、イエロートラフィックには <b>exceed-action</b>、レッドトラフィックには <b>violate-action</b> 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。</p> <ul style="list-style-type: none"> <li>• <b>confirm-action</b> を <b>drop</b> に設定し、<b>exceed-action</b> と <b>violate-action</b> に <b>drop</b> 以外を設定する組み合わせ</li> </ul>

police	
	<ul style="list-style-type: none"> <li>• <b>exceed-action</b> を <b>drop</b> に設定し、<b>violate-action</b> に <b>drop</b> 以外を設定する組み合わせ</li> </ul> <p><b>set</b> 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。</p> <p>受信方向のポリサー使用可能数は、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 768 個です。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
<b>制限事項</b>	<p><b>set-lp-transmit</b> アクションを input 側で適用した場合は、変更後の値を基に <b>priority-queue cos-map</b> 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 <b>priority-queue cos-map</b> 設定に基づいて送信キューが決定されます。</p> <p><b>set-dscp-transmit</b> 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。</p>
<b>注意事項</b>	<p>クラスマップに対して、<b>police</b>、<b>police cir</b>、または <b>police aggregate</b> 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。</p>
<b>対象バージョン</b>	1.01.01

使用例：[平均レート=5000Kbps, 標準バーストサイズ=16 キロバイト, **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)#
```

## 7.1.22 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	<pre>police cir CIR [bc CONFORM-BURST] pir PIR [be PEAK-BURST] [confirm-action ACTION] [exceed-action ACTION [violate-action ACTION]] [color-aware] no police</pre>
パラメーター	<p><i>CIR</i>: 保証帯域を 0~10,000,000(Kbps) の範囲で指定します。</p> <p><b>bc CONFORM-BURST</b> (省略可能): 標準バーストサイズを 0~16384 キロバイトの範囲で指定します。</p> <p><i>PIR</i>: 最大帯域を 0~10,000,000(Kbps) の範囲で指定します。</p> <p><b>be PEAK-BURST</b> (省略可能): 最大バーストサイズを 0~16384 キロバイトの範囲で指定します。</p> <p><b>confirm-action ACTION</b> (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。</p> <p><b>exceed-action ACTION</b> (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。</p> <p><b>violate-action ACTION</b> (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 <b>exceed-action</b> と同一です。</p> <p><i>ACTION</i>: 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。</p> <ul style="list-style-type: none"> <li>• <b>drop</b>: パケットを廃棄します。</li> <li>• <b>set-dscp-transmit VALUE</b>: IP DSCP を設定して、新しい IP DSCP でパケットを送信します。</li> <li>• <b>set-lp-transmit VALUE</b>: CoS 値を設定して、新しい CoS 値でパケットを送信します。</li> <li>• <b>transmit</b>: パケットを変更せずに送信します。</li> </ul> <p><b>color-aware</b> (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。</p>
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	<p>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。</p> <p>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。</p> <p>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。</p>

police cir	
	<p>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 <b>confirm-action</b>、イエロートラフィックには <b>exceed-action</b>、レッドトラフィックには <b>violate-action</b> 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。</p> <ul style="list-style-type: none"> <li>• <b>conform-action</b> を <b>drop</b> に設定し、<b>exceed-action</b> と <b>violate-action</b> に <b>drop</b> 以外を設定する組み合わせ</li> <li>• <b>exceed-action</b> を <b>drop</b> に設定し、<b>violate-action</b> に <b>drop</b> 以外を設定する組み合わせ</li> </ul> <p><b>set</b> 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。</p> <p>受信方向のポリサー使用可能数は、最大 768 個です。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
制限事項	<p><b>set-lp-transmit</b> アクションを input 側で適用した場合は、変更後の値を基に <b>priority-queue cos-map</b> 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 <b>priority-queue cos-map</b> 設定に基づいて送信キューが決定されます。</p> <p><b>set-dscp-transmit</b> 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。</p>
注意事項	<p>クラスマップに対して、<b>police</b>、<b>police cir</b>、または <b>police aggregate</b> 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。</p>
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=10 キロバイト, 最大帯域=1000Kbps, 最大バーストサイズ=10 キロバイト, **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)#

## 7.1.23 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。
シンタックス	<b>police aggregate</b> <i>NAME</i> <b>no police</b>
パラメーター	<i>NAME</i> : 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	<p>クラスマップの packets matching の条件は、以下の 4 つの種類に分類できません。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。</p> <ul style="list-style-type: none"> <li>• <b>Layer2</b>: 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。 <ul style="list-style-type: none"> <li>• <b>match access-group name</b> <i>ACCESS-LIST-NAME</i> (拡張 MAC アクセスリスト)</li> <li>• <b>match cos [inner]</b> <i>COS-LIST</i></li> <li>• <b>match vlan [inner]</b> <i>VLAN-LIST</i></li> <li>• <b>match protocol arp</b></li> <li>• <b>match protocol pppoe</b></li> </ul> </li> <li>• <b>IPv4</b>: 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。 <ul style="list-style-type: none"> <li>• <b>match access-group name</b> <i>ACCESS-LIST-NAME</i> (IP アクセスリスト)</li> <li>• <b>match [ip] dscp</b> <i>DSCP-LIST</i></li> <li>• <b>match ip precedence</b> <i>IP-PRECEDENCE-LIST</i></li> <li>• <b>match ip</b></li> <li>• <b>match netbios</b></li> </ul> </li> <li>• <b>IPv6</b>: 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。 <ul style="list-style-type: none"> <li>• <b>match access-group name</b> <i>ACCESS-LIST-NAME</i> (IPv6 アクセスリスト)</li> <li>• <b>match protocol ipv6</b></li> </ul> </li> <li>• <b>expert</b>: 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。 <ul style="list-style-type: none"> <li>• <b>match access-group name</b> <i>ACCESS-LIST-NAME</i> (拡張エキスパートアクセスリスト)</li> </ul> </li> </ul> <p>クラスマップの packets matching 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。</p> <ul style="list-style-type: none"> <li>• <b>match protocol dns</b></li> <li>• <b>match protocol egp</b></li> <li>• <b>match protocol ftp</b></li> <li>• <b>match protocol nfs</b></li> <li>• <b>match protocol ntp</b></li> </ul>

police aggregate	
	<ul style="list-style-type: none"> <li>• <b>match protocol rip</b></li> <li>• <b>match protocol ssh</b></li> <li>• <b>match protocol dhcp</b></li> <li>• <b>match dscp</b></li> <li>• <b>match protocol ospf</b></li> <li>• <b>match protocol rtsp</b></li> <li>• <b>match protocol tftp</b></li> <li>• <b>match protocol telnet</b></li> <li>• <b>match precedence</b></li> </ul> <p>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。</p>
<b>制限事項</b>	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。
<b>注意事項</b>	クラスマップに対して、 <b>police</b> 、 <b>police cir</b> 、または <b>police aggregate</b> 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。
<b>対象バージョン</b>	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)#
```

### 7.1.24 mls qos aggregate-policer

mls qos aggregate-policer	
<b>目的</b>	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。
<b>シンタックス</b>	<pre><b>mls qos aggregate-policer</b> <i>NAME</i> <i>KBPS</i> [<i>BURST-NORMAL</i> [<i>BURST-MAX</i>]] [<i>conform-action ACTION</i>] <i>exceed-action ACTION</i> [<i>violate-action ACTION</i>] [<i>color-aware</i>]</pre> <pre><b>mls qos aggregate-policer</b> <i>NAME</i> <i>cir</i> <i>CIR</i> [<i>bc CONFORM-BURST</i>] <i>pir</i> <i>PIR</i> [<i>bc</i> <i>PEAK-BURST</i>] [<i>conform-action ACTION</i>] [<i>exceed-action ACTION</i>] [<i>violate-</i> <i>action ACTION</i>]] [<i>color-aware</i>]</pre> <pre><b>no mls qos aggregate-policer</b> <i>NAME</i></pre>
<b>パラメーター</b>	<p><i>NAME</i>：集約ポリサー名を最大 32 文字で指定します。大文字と小文字は区別されません。先頭文字に数字/記号を使用することはできません。</p> <p><i>KBPS</i>：平均レートを 0～10,000,000 (Kbps) の範囲で指定します。</p>

mls qos aggregate-policer	
	<p><b>BURST-NORMAL</b> (省略可能) : 標準バーストサイズを 0~16384 キロバイト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 12 キロバイトです。</p> <p><b>BURST-MAX</b> (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 0~16384 キロバイト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 12 キロバイトです。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。</p> <p><b>confirm-action ACTION</b> (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。</p> <p><b>exceed-action ACTION</b> (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。</p> <p><b>violate-action ACTION</b> (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 <b>exceed-action</b> と同じです。</p> <p><b>ACTION</b>: 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。</p> <ul style="list-style-type: none"> <li>• <b>drop</b> : パケットを廃棄します。</li> <li>• <b>set-dscp-transmit VALUE</b> : IP DSCP を設定して、新しい IP DSCP でパケットを送信します。</li> <li>• <b>set-lp-transmit VALUE</b> : CoS 値を設定して、新しい CoS 値でパケットを送信します。</li> <li>• <b>transmit</b> : パケットを変更せずに送信します。</li> </ul> <p><b>color-aware</b> (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。</p> <p><b>CIR</b>: 保証帯域を 0~10,000,000(Kbps) の範囲で指定します。</p> <p><b>bc CONFORM-BURST</b> (省略可能) : 標準バーストサイズを 0~16384 キロバイトの範囲で指定します。</p> <p><b>PIR</b>: 最大帯域を 0~10,000,000(Kbps) の範囲で指定します。</p> <p><b>be PEAK-BURST</b> (省略可能) : 最大バーストサイズを 0~16384 キロバイトの範囲で指定します。</p>
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	<p>定義できる集約ポリサーは最大 255 個です。</p> <p>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せん。異なるポリシーマップ間では共有できません。</p> <p><b>mls qos aggregate-policer</b> は 1 レートポリサー用、<b>mls qos aggregate-policer cir</b> は 2 レートポリサー用です。</p>

mls qos aggregate-policer	
	<p>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。</p> <ul style="list-style-type: none"> <li>• アルファベット：“A”～“Z”、“a”～“z”</li> <li>• 数字：“0”～“9”</li> <li>• 記号：!#\$%&amp;()+,.-=@[]^_`{~ /;&lt;&gt;*-’¥”</li> </ul>
制限事項	<p><b>set-lp-transmit</b> アクションを input 側で適用した場合は、変更後の値を基に <b>priority-queue cos-map</b> 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 <b>priority-queue cos-map</b> 設定に基づいて送信キューが決定されます。</p> <p><b>set-dscp-transmit</b> 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。</p>
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=32 キロバイト, 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)#
```

### 7.1.25 service-policy

service-policy	
目的	ポリシーマップを入力インターフェースに追加します。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	<b>service-policy</b> {input   output} <i>NAME</i> <b>no service-policy</b> {input   output}
パラメーター	<p><b>input</b>：受信側ポリシーにポリシーマップを適用する場合に指定します。</p> <p><b>output</b>：送信側ポリシーにポリシーマップを適用する場合に指定します。</p> <p><i>NAME</i>：ポリシーマップ名を、最大 31 文字の英数字で指定します。</p>
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	インターフェースのタイプ（入力または出力）ごとに、ポリシーマップを 1 つ追加するコマンドです。集約用のポリシーをインターフェースに追加して、パケットの数またはレートを制御します。インターフェースに到着するパケットは、インターフェースに追加されたサービスポリシーに基づいて処理されます。
制限事項	同一のインターフェースタイプ（入力または出力）に対して、同じ種類のアクセスリストは 1 つだけ適用できます。
注意事項	-
対象バージョン	1.01.01

使用例：ポリシーマップを、(1) cust1-classes と (2) cust2-classes の 2 つ定義する方法を示します。cust1-classes では、ゴールドは CoS 6 と一致するように設定しています。認定速度は 800Kbps で、

## 7 優先制御(QoS) | 7.1 優先制御(QoS) コマンド

1 レートポリサーでポリシングされます。シルバーは、CoS 5 と一致するように設定しています。認定速度は 2000Kbps で、1 レートポリサーでポリシングされます。ブロンズは、CoS 0 と一致するように設定しています。認定速度は 8000Kbps で、1 レートポリサーでポリシングされます。

cust1-classes ポリシーマップを設定して、その後、受信側トラフィックを対象に、ポート 1/0/1 とポート 1/0/2 に追加しています。

```
# configure terminal
(config)# class-map match-all gold
(config-cmap)# match cos 6
(config-cmap)# exit
(config)# class-map match-all silver
(config-cmap)# match cos 5
(config-cmap)# exit
(config)# class-map match-all bronze
(config-cmap)# match cos 0
(config-cmap)# exit
(config)# policy-map cust1-classes
(config-pmap)# class gold
(config-pmap-c)# police 800000 16384 exceed-action set-dscp-transmit 0
(config-pmap-c)# exit
(config-pmap)# class silver
(config-pmap-c)# police 2000000 16384 exceed-action set-dscp-transmit 0
(config-pmap-c)# exit
(config-pmap)# class bronze
(config-pmap-c)# police 8000000 16384 exceed-action set-dscp-transmit 0
(config-pmap-c)# exit
(config-pmap)# exit
(config)# interface port 1/0/1
(config-if-port)# service-policy input cust1-classes
(config-if-port)# exit
(config)# interface port 1/0/2
(config-if-port)# service-policy input cust1-classes
(config-if-port)#
```

使用例：cust2-classes ポリシーマップを設定して、その後、受信側トラフィックを対象に、ポート 1/0/1 に追加しています。

```
# configure terminal
(config)# policy-map cust2-classes
(config-pmap)# class gold
(config-pmap-c)# police 1600000 16384 exceed-action set-dscp-transmit 0
(config-pmap-c)# exit
(config-pmap)# class silver
(config-pmap-c)# police 4000000 16384 exceed-action set-dscp-transmit 0
(config-pmap-c)# exit
(config-pmap)# class bronze
(config-pmap-c)# police 1600000 16384 exceed-action set-dscp-transmit 0
(config-pmap-c)# exit
(config-pmap)# exit
(config)# interface port 1/0/1
(config-if-port)# service-policy input cust2-classes
(config-if-port)#
```

### 7.1.26 show mls qos interface

show mls qos interface	
目的	指定したインターフェースの QoS 設定を表示します。
シンタックス	<code>show mls qos interface [INTERFACE-ID [, -]] {cos   scheduler   trust   rate-limit   queue-rate-limit   dscp-mutation   map {dscp-color   cos-color   dscp-cos}}</code>

show mls qos interface	
パラメーター	<p><i>INTERFACE-ID</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul> <p><b>cos</b> : デフォルトの CoS 値を表示する場合に指定します。</p> <p><b>scheduler</b> : スケジューリングアルゴリズムを表示する場合に指定します。</p> <p><b>trust</b> : 受信トラフィックの分類設定を表示する場合に指定します。</p> <p><b>rate-limit</b> : 帯域制限設定を表示する場合に指定します。</p> <p><b>queue-rate-limit</b> : 送信キューの帯域設定を表示する場合に指定します。</p> <p><b>dscp-mutation</b> : DSCP 変換マップを表示する場合に指定します。</p> <p><b>map dscp-color</b> : 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場合に指定します。</p> <p><b>map cos-color</b> : 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場合に指定します。</p> <p><b>map dscp-cos</b> : DSCP から CoS へのマッピング設定を表示する場合に指定します。</p>
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 1/0/2 からポート 1/0/5 の、デフォルトの 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)	インターフェース ID 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

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
```

## 7 優先制御(QoS) | 7.1 優先制御(QoS) コマンド

```

-----
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)	インターフェース ID 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

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    wr

```

項番	説明
(1)	インターフェース ID 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

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)	インターフェース ID 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。

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%(10000 kbps) 20%(20000 kbps) 64 kbyte          64 kbyte
Port1/0/4    2%              2000 kbps       64 kbyte          64 kbyte

```

7 優先制御(QoS) | 7.1 優先制御(QoS) コマンド

項番	説明
(1)	インターフェース ID 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。 <b>rate-limit</b> 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。 <b>rate-limit</b> 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。

使用例：ポート 1/0/1 からポート 1/0/2 の、送信キュー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。 <b>queue rate-limit</b> 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。 <b>queue rate-limit</b> コマンドで最大帯域をパーセント指定で設定した場合は、「リンクアップポート：パーセント設定値と実際の設定値(kbps)を表示」「リンクダウンポート：パーセント設定値のみ表示」となります。



## 7 優先制御(QoS) | 7.1 優先制御(QoS) コマンド

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。

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。

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。

## 7.1.27 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	<b>show mls qos queueing</b> [ <b>interface</b> <i>INTERFACE-ID</i> [, [-]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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
wrrr 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)	インターフェース ID 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。

### 7.1.28 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	<b>show mls qos map dscp-mutation</b> [ <i>MAP-NAME</i> ]
パラメーター	<i>MAP-NAME</i> (省略可能) : 表示する 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。

項番	説明
(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。

### 7.1.29 show class-map

show class-map	
目的	クラスマップ設定を表示します。
シンタックス	<b>show class-map</b> [ <i>NAME</i> ]
パラメーター	<i>NAME</i> (省略可能) : クラスマップ名を最大 31 文字の英数字で指定します。
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 : 2 つのクラスマップを定義する方法を示します。アクセスリスト「acl\_home\_user」と一致するパケットはクラス「c3」、IP パケットはクラス「c2」に属しています。

```
# 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。

### 7.1.30 show policy-map

show policy-map	
目的	ポリシーマップ設定を表示します。
シンタックス	<b>show policy-map</b> [ <i>POLICY-NAME</i>   <b>interface</b> <i>INTERFACE-ID</i> ]
パラメーター	<i>POLICY-NAME</i> (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。 <b>interface</b> <i>INTERFACE-ID</i> (省略可能) : ポリシーマップを表示するインターフェイスを、以下のパラメーターで指定します。 • <b>port</b> : 物理ポートを指定します。

show policy-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: police というクラスに対して、policy1 というポリシーマップ内の 2 レートポリサーが設定されている例を示します。2 レートポリサーは、トラフィックを平均認定速度 500Kbps とピーク速度 1Mbps に制限するように設定しています。

```
# configure terminal
(config)# class-map police
(config-cmap)# match access-group name acl_rd
(config-cmap)# policy-map policy1
(config-pmap)# class police
(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 1/0/1
(config-if-port)# service-policy output policy1
(config-if-port)#
```

使用例: 上の例で作成した、policy1 というポリシーマップ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)	ポリシーマップに割り当てられたクラスマップの設定を表示します。

使用例: ポート 1/0/1 のすべての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)	ポリシーマップに割り当てられたクラスマップの設定を表示します。

## 7.1.31 show mls qos aggregate-policer

show mls qos aggregate-policer	
目的	設定した集約ポリサーを表示します。
シンタックス	<code>show mls qos aggregate-policer [NAME]</code>
パラメーター	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。

## 7.2 WRED コマンド

WRED (Weighted Random Early Detection) 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
random-detect	random-detect COS-VALUE [profile PROFILE-ID] no random-detect COS-VALUE
random-detect ecn	random-detect ecn COS-VALUE no random-detect ecn COS-VALUE
random-detect exponential-weight	random-detect exponential-weight COS-VALUE exponent VALUE no random-detect exponential-weight COS-VALUE
random-detect profile	random-detect profile PROFILE-ID [tcp   non-tcp] [green   yellow   red] min-threshold VALUE max-threshold VALUE max-drop-rate VALUE no random-detect profile PROFILE-ID
show queueing random-detect	show queueing random-detect [interface INTERFACE-ID [,  -]]
show random-detect drop-counter	show random-detect drop-counter [interface INTERFACE-ID [,  -]]
show random-detect profile	show random-detect profile [PROFILE-ID]
clear random-detect drop-counter	clear random-detect drop-counter {all   interface INTERFACE-ID [,  -]}

### 7.2.1 random-detect

random-detect	
目的	WRED 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	<b>random-detect</b> COS-VALUE [ <b>profile</b> PROFILE-ID] <b>no random-detect</b> COS-VALUE
パラメーター	COS-VALUE: WRED を有効にする CoS キューを、0~7 の範囲で指定します。 <b>profile</b> PROFILE-ID (省略可能): 適用する WRED プロファイルの ID を、1~128 の範囲で指定します。指定しない場合は WRED プロファイル 1 が適用されます。
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, 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 のキュー5 で WRED 機能を有効にして、WRED プロファイル 10 を適用する方法を示します。

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

```
(config-if-port)# random-detect 5 profile 10
(config-if-port)#
```

## 7.2.2 random-detect ecn

random-detect ecn																
目的	Explicit Congestion Notification (ECN) を有効にします。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	<b>random-detect ecn</b> <i>COS-VALUE</i> <b>no random-detect ecn</b> <i>COS-VALUE</i>															
パラメーター	<i>COS-VALUE</i> : ECN の有効/無効を設定する CoS キューを、0~7 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(port, range)															
特権レベル	レベル: 12															
ガイドライン	<p>本コマンドの設定は、物理ポートだけに適用できます。WRED では、指定した上限値を超えた平均キューサイズに基づき、輻輳を検知し、パケットを破棄します。ECN は、WRED を拡張したもので、指定した上限値を超えた平均キューサイズに基づき、パケットを破棄する代わりに、パケットに ECN マークを付与します。WRED 機能を使用すると、ルーターおよびエンドホストは、ECN マークによって輻輳を検知し、パケットの送信を遅らせます。</p> <p>ECN マークは、IP ヘッダーの ECN-Capable Transport (ECT) ビットおよび Congestion Experienced (CE) ビットの 2 ビットを使用します。ECT ビットと CE ビットの組み合わせは以下のとおりです。</p> <table border="1"> <thead> <tr> <th>ECT ビット</th> <th>CE ビット</th> <th>意味</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>ECN 非対応</td> </tr> <tr> <td>0</td> <td>1</td> <td>ECN 対応</td> </tr> <tr> <td>1</td> <td>0</td> <td>ECN 対応</td> </tr> <tr> <td>1</td> <td>1</td> <td>輻輳検知</td> </tr> </tbody> </table> <p>ECN が有効に設定されている場合は、パケットは以下のように取り扱われます。</p> <ul style="list-style-type: none"> <li>ECT ビットおよび CE ビットが共に 0 の場合、パケットは WRED の破棄確率に基づき破棄されます。</li> <li>ECT ビットおよび CE ビットのどちらか一方のみが 1 の場合、パケットが WRED の破棄確率に基づき破棄されると決定されたときに、パケットが破棄される代わりに ECT ビットおよび CE ビットを共に 1 に設定され、パケットが送信されます。</li> <li>ECT ビットおよび CE ビットが共に 1 の場合、パケットは転送されます。ECN マークは付与されません。</li> </ul>	ECT ビット	CE ビット	意味	0	0	ECN 非対応	0	1	ECN 対応	1	0	ECN 対応	1	1	輻輳検知
ECT ビット	CE ビット	意味														
0	0	ECN 非対応														
0	1	ECN 対応														
1	0	ECN 対応														
1	1	輻輳検知														
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 5 で ECN を有効にする方法を示します。

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



## 7.2.3 random-detect exponential-weight

random-detect exponential-weight	
目的	キューの平均キューサイズの計算に使用される、WRED 指数の重み係数を設定します。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	<b>random-detect exponential-weight</b> <i>COS-VALUE</i> <b>exponent</b> <i>VALUE</i> <b>no random-detect exponential-weight</b> <i>COS-VALUE</i>
パラメーター	<i>COS-VALUE</i> : 指数を設定する CoS キューを、0~7 の範囲で指定します。 <i>VALUE</i> : 指数値を 0~15 の範囲で指定します。
デフォルト	9
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 のキュー5 で指数値を 10 に設定する方法を示します。

```
# configure terminal
(config)# interface port 1/0/1
(config-if-port)# random-detect exponential-weight 5 exponent 10
(config-if-port)#
```

## 7.2.4 random-detect profile

random-detect profile	
目的	WRED プロファイルを設定します。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	<b>random-detect profile</b> <i>PROFILE-ID</i> [ <b>tcp</b>   <b>non-tcp</b> ] [ <b>green</b>   <b>yellow</b>   <b>red</b> ] <b>min-threshold</b> <i>VALUE</i> <b>max-threshold</b> <i>VALUE</i> <b>max-drop-rate</b> <i>VALUE</i> <b>no random-detect profile</b> <i>PROFILE-ID</i>
パラメーター	<i>PROFILE-ID</i> : WRED プロファイルの ID を、1~128 の範囲で指定します。  <b>tcp</b> (省略可能): TCP パケットに対する WRED 廃棄パラメーターを設定する場合に指定します。  <b>non-tcp</b> (省略可能): 非 TCP パケットに対する WRED 廃棄パラメーターを設定する場合に指定します。  <b>green</b> (省略可能): グリーントラフィックに対する WRED 廃棄パラメーターを設定する場合に指定します。  <b>yellow</b> (省略可能): イエロートラフィックに対する WRED 廃棄パラメーターを設定する場合に指定します。  <b>red</b> (省略可能): レッドトラフィックに対する WRED 廃棄パラメーターを設定する場合に指定します。  <b>min-threshold</b> <i>VALUE</i> : WRED の最小しきい値 (キューサイズ: セル単位) を、0~100 の範囲で指定します。この最小しきい値を超えると、WRED による廃棄が開始されます。  <b>max-threshold</b> <i>VALUE</i> : WRED の最大しきい値 (キューサイズ: セル単位) を、0

random-detect profile	
	<p>～100 の範囲で指定します。この最大しきい値を超えると、WRED ですべてのパケットを破棄します。</p> <p><b>max-drop-rate</b> VALUE: 平均キューサイズが最大しきい値に達したときの最大廃棄率を指定します。0 を指定した場合、パケットは廃棄されません。最大廃棄率は、以下のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li>• 0-10 (0%-10%), 11 (25%), 12 (50%), 13 (75%), 14 (100%)</li> </ul>
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	<p><b>tcp, non-tcp, green, yellow, red</b> パラメーターのいずれも指定しないで設定した場合は、すべての 6 種類の設定パターン (<b>tcp green, tcp yellow, tcp red, non-tcp green, non-tcp yellow, non-tcp red</b>) で同じ値で設定されます。</p> <p><b>tcp</b> パラメーターを指定した後に、<b>green, yellow, red</b> パラメーターを指定しないで設定した場合は、3 種類の設定パターン (<b>tcp green, tcp yellow, tcp red</b>) で同じ値で設定されます。</p> <p><b>non-tcp</b> パラメーターを指定した後に、<b>green, yellow, red</b> パラメーターを指定しないで設定した場合は、3 種類の設定パターン (<b>non-tcp green, non-tcp yellow, non-tcp red</b>) で同じ値で設定されます。</p> <p><b>green</b> パラメーターを指定する前に、<b>tcp, non-tcp</b> パラメーターを指定しないで設定した場合は、2 種類の設定パターン (<b>tcp green, non-tcp green</b>) で同じ値で設定されます。</p> <p><b>yellow</b> パラメーターを指定する前に、<b>tcp, non-tcp</b> パラメーターを指定しないで設定した場合は、2 種類の設定パターン (<b>tcp yellow, non-tcp yellow</b>) で同じ値で設定されます。</p> <p><b>red</b> パラメーターを指定する前に、<b>tcp, non-tcp</b> パラメーターを指定しないで設定した場合は、2 種類の設定パターン (<b>tcp red, non-tcp red</b>) で同じ値で設定されます。</p>
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例: WRED プロファイル 10 のすべての設定パターンの WRED 廃棄パラメーターを、**min-threshold=30**、**max-threshold=50**、**max-drop-rate=10** (10%) に設定する方法を示します。

```
# configure terminal
(config)# random-detect profile 10 min-threshold 30 max-threshold 50 max-drop-rate 10
(config)#
```

使用例: WRED プロファイル 10 で、TCP イエロートラフィックと TCP レッドトラフィックに対する WRED 廃棄パラメーターを、**min-threshold=20**、**max-threshold=40**、**max-drop-rate=5** (5%) に設定する方法を示します。

```
# configure terminal
(config)# random-detect profile 10 tcp yellow min-threshold 20 max-threshold 40 max-drop-rate 5
(config)# random-detect profile 10 tcp red min-threshold 20 max-threshold 40 max-drop-rate 5
(config)#
```

## 7.2.5 show queueing random-detect

show queueing random-detect	
目的	指定したインターフェースの WRED 設定を表示します。
シンタックス	<code>show queueing random-detect [interface <i>INTERFACE-ID</i> [,  -]]</code>
パラメーター	<code>interface <i>INTERFACE-ID</i></code> (省略可能) : WRED 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。 <ul style="list-style-type: none"> <li>• <code>port</code> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、システム上のすべてのインターフェースの WRED 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 : ポート 1/0/1 の WRED 設定と CoS キューの状態を表示する方法を示します。

```
# show queueing random-detect interface port 1/0/1

Current WRED configuration:

Port1/0/1 ... (1)
(2) (3) (4) (5) (6)
CoS WRED State Exp-weight-constant Profile ECN State
---
0 Disabled 9 1 Disabled
1 Disabled 9 1 Disabled
2 Disabled 9 1 Disabled
3 Disabled 9 1 Disabled
4 Disabled 9 1 Disabled
5 Disabled 9 1 Disabled
6 Disabled 9 1 Disabled
7 Disabled 9 1 Disabled
```

項番	説明
(1)	ポート番号を表示します。
(2)	CoS 値を表示します。
(3)	WRED 機能の有効/無効を表示します。
(4)	加重係数を表示します。
(5)	WRED プロファイル ID を表示します。
(6)	明示的輻輳通知 (ECN) の有効/無効を表示します。

## 7.2.6 show random-detect drop-counter

show random-detect drop-counter	
目的	WRED ドロップカウンターを表示します。
シンタックス	<code>show random-detect drop-counter [interface <i>INTERFACE-ID</i> [,  -]]</code>
パラメーター	<code>interface <i>INTERFACE-ID</i></code> (省略可能) : WRED ドロップ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。

show random-detect drop-counter	
	<ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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、すべてのインターフェースの WRED ドロップカウンターが表示されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例 : ポート 1/0/1 の WRED ドロップカウンターを表示する方法を示します。

```
# show random-detect drop-counter interface port 1/0/1

Current WRED Drop Counter:
(1)      (2)      (3)      (4)
Interface Green      Yellow      Red
-----
Port1/0/1 0          0          0
```

項番	説明
(1)	インターフェース ID を表示します。
(2)	グリーントラフィックの WRED 廃棄パケット数を表示します。
(3)	イエロートラフィックの WRED 廃棄パケット数を表示します。
(4)	レッドトラフィックの WRED 廃棄パケット数を表示します。

### 7.2.7 show random-detect profile

show random-detect profile	
目的	WRED プロファイル設定を表示します。
シンタックス	<b>show random-detect profile</b> [ <i>PROFILE-ID</i> ]
パラメーター	<i>PROFILE-ID</i> (省略可能) : 表示する WRED プロファイル ID を、1~128 の範囲で指定します。指定しない場合、すべての WRED プロファイルの設定が表示されます。
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 : WRED プロファイル 1 の設定を表示する方法を示します。

```
# show random-detect profile 1

WRED Profile 1 ... (1)
(2)      (3)      (4)      (5)
Packet Type      Min-Threshold  Max-Threshold  Max-Drop-Rate
```

TCP-GREEN	20	80	0
TCP-YELLOW	20	80	0
TCP-RED	20	80	0
NON-TCP-GREEN	20	80	0
NON-TCP-YELLOW	20	80	0
NON-TCP-RED	20	80	0

項番	説明
(1)	WRED プロファイル ID を表示します。
(2)	パケットタイプを表示します。
(3)	WRED の最小しきい値 (キューサイズ:セル単位) を表示します。
(4)	WRED の最大しきい値 (キューサイズ:セル単位) を表示します。
(5)	平均キューサイズが最大しきい値に達したときの最大廃棄率を指定します。 <ul style="list-style-type: none"> <li>0-10 (0%-10%), 11 (25%), 12 (50%), 13 (75%), 14 (100%)</li> </ul>

### 7.2.8 clear random-detect drop-counter

clear random-detect drop-counter	
目的	WRED ドロップカウンターをクリアします。
シンタックス	<b>clear random-detect drop-counter</b> {all   interface <i>INTERFACE-ID</i> [, -]}
パラメーター	<p><b>all</b> : すべてのインターフェースの WRED 廃棄パケット数をクリアする場合に指定します。</p> <p><b>interface</b> <i>INTERFACE-ID</i> : WRED 廃棄パケット数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。</p> <ul style="list-style-type: none"> <li><b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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	物理ポートだけで有効です。
対象バージョン	1.01.01

使用例: ポート 1/0/1 の WRED ドロップカウンターをクリアする方法を示します。

# clear random-detect drop-counter interface port 1/0/1
#

## 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
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}

コマンド	コマンドとパラメーター
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-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 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]   mac [NAME   NUMBER]   ipv6 [NAME   NUMBER]   expert [NAME   NUMBER]]
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	<b>access-list resequence</b> { <i>ACL-NAME</i>   <i>ACL-NUMBER</i> } <i>STARTING-SEQUENCE-NUMBER</i> <i>INCREMENT</i> <b>no access-list resequence</b>
パラメーター	<i>ACL-NAME</i> : 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。 <i>ACL-NUMBER</i> : 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。 <i>STARTING-SEQUENCE-NUMBER</i> : 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。 <i>INCREMENT</i> : 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。  <b>no access-list resequence</b> 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。  <b>access-list resequence</b> コマンド、もしくは <b>no access-list resequence</b> 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を有効にします。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	<b>acl-hardware-counter</b> { <b>access-group</b> { <i>ACL-NAME</i>   <i>ACL-NUMBER</i> }   <b>vlan-filter</b> <i>MAP-NAME</i> } <b>no acl-hardware-counter</b> { <b>access-group</b> { <i>ACL-NAME</i>   <i>ACL-NUMBER</i> }   <b>vlan-filter</b> <i>MAP-NAME</i> }
パラメーター	<b>access-group</b> <i>ACL-NAME</i> : ハードウェアカウンタを有効にするアクセスリスト名を指定します。 <b>access-group</b> <i>ACL-NUMBER</i> : ハードウェアカウンタを有効にするアクセスリスト番号を指定します。 <b>vlan-filter</b> <i>MAP-NAME</i> : ハードウェアカウンタを有効にする 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	<b>access-group</b> 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。 <b>vlan-filter</b> 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を使用できません。 <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> <li>• <b>access-class</b> コマンド、<b>ping access-class</b> コマンド、<b>snmp-server community</b> コマンド、<b>snmp-server user</b> コマンド、<b>snmp-server group</b> コマンドで指定したアクセスリスト</li> </ul>
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	<b>list-remark</b> <i>TEXT</i> <b>no list-remark</b>
パラメーター	<i>TEXT</i> ：備考情報を最大 256 文字で指定します。
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、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	<b>expert access-group</b> { <i>NAME</i>   <i>NUMBER</i> } [ <i>in</i>   <i>out</i> ] <b>no expert access-group</b> [ <i>NAME</i>   <i>NUMBER</i> ] [ <i>in</i>   <i>out</i> ]
パラメーター	<i>NAME</i> ：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。 <i>NUMBER</i> ：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。 <b>in</b> (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、 <b>in</b> が適用されます。

expert access-group	
	<b>out</b> (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 ( <b>in</b> パラメーター指定時))
特権レベル	レベル : 12
ガイドライン	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。ApresiaNP4000 シリーズでは、装置全体で Ingress グループ用に 1920 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。</p> <p>ApresiaNP4000 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 960 個、Egress グループに最大 256 個設定できます。</p> <p>L4 ポート番号の複数指定で使用する比較演算子 (<b>lt</b>, <b>gt</b>, <b>neq</b>) と範囲指定パラメーター (<b>range</b>) 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 (<b>lt</b>, <b>gt</b>, <b>neq</b>) と範囲指定パラメーター (<b>range</b>) 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。</p>
制限事項	<p>抽出条件「クラス ID (<b>class</b>)」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。</p> <p>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 (<b>out</b> パラメーター) に適用することはできません。</p>
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	<b>expert access-list extended</b> <i>NAME</i> [ <i>NUMBER</i> ]

expert access-list	
	<b>no expert access-list extended</b> { <i>NAME</i>   <i>NUMBER</i> }
パラメーター	<i>NAME</i> : 作成・変更する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。先頭には英字を使用してください。  <i>NUMBER</i> (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	<i>[SEQ]</i> { <b>permit</b> [ <b>authentication-bypass</b> ]   <b>deny</b> } <b>tcp</b> <i>CONDITION</i> <i>[SEQ]</i> { <b>permit</b> [ <b>authentication-bypass</b> ]   <b>deny</b> } <b>udp</b> <i>CONDITION</i> <i>[SEQ]</i> { <b>permit</b> [ <b>authentication-bypass</b> ]   <b>deny</b> } <b>icmp</b> <i>CONDITION</i> <i>[SEQ]</i> { <b>permit</b> [ <b>authentication-bypass</b> ]   <b>deny</b> } [ <i>PROTOCOL</i> ] <i>CONDITION</i> <b>no</b> <i>SEQ</i>
パラメーター	<i>SEQ</i> (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。  <b>permit</b> : 許可エントリーを設定する場合に指定します。  <b>authentication-bypass</b> (省略可能) : エントリーに一致するパケットが、AccessDefender 認証のために CPU にコピーされずに送信されるようにする場合に指定します。  <b>deny</b> : 拒否エントリーを設定する場合に指定します。  <b>tcp</b> : 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。  <b>udp</b> : 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。  <b>icmp</b> : 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。

permit   deny (expert access-list)	
	<p><i>PROTOCOL</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>igmp</b>(2) <b>gre</b>(47) <b>esp</b>(50) <b>eigrp</b>(88) <b>ospf</b>(89) <b>ipinip</b>(94) <b>pim</b>(103) <b>pcp</b>(108) <b>vrrp</b>(112)</li> </ul> <p><i>CONDITION</i> : 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。</p>
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	<p>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。</p> <p>開始値と増分値を変更するには、<b>access-list resequence</b> コマンドを使用します。なお、<b>access-list resequence</b> 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。</p> <p>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。</p> <p><b>permit</b> エントリーと <b>permit authentication-bypass</b> エントリーの違いは、以下のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>permit</b> エントリーに一致したパケットは、認証を行うために CPU にコピーされます。</li> <li>• <b>permit authentication-bypass</b> エントリーに一致したパケットは、認証のために CPU にコピーされず (認証が行われずに)、正常に送信されます。</li> </ul> <p>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)</p> <ul style="list-style-type: none"> <li>• 送信元 IP アドレス (<i>SRC-IP-ADDR SRC-IP-WILDCARD</i>)</li> <li>• 送信元 MAC アドレス (<i>SRC-MAC-ADDR SRC-MAC-WILDCARD</i>)</li> <li>• 宛先 IP アドレス (<i>DST-IP-ADDR DST-IP-WILDCARD</i>)</li> <li>• 宛先 MAC アドレス (<i>DST-MAC-ADDR DST-MAC-WILDCARD</i>)</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul>
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

permit   deny (expert access-list)	
	<p>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。</p> <p>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。</p>
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	ICMP	CoS	VLAN	フラグ	DSCP	クラス
	IP	MAC	L4	IP	MAC	L4	Flag			ID	メント		ID
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	<p><b>any</b> : すべての送信元 IP アドレスを指定</p> <p><b>host SRC-IP-ADDR</b> : 特定の送信元 IP アドレスを指定</p> <p><b>SRC-IP-ADDR SRC-IP-WILDCARD</b> : 送信元 IP アドレスのグループを指定</p>
送信元 MAC アドレス	<p><b>any</b> : すべての送信元 MAC アドレスを指定</p> <p><b>host SRC-MAC-ADDR</b> : 特定の送信元 MAC アドレスを指定</p> <p><b>SRC-MAC-ADDR SRC-MAC-WILDCARD</b> : 送信元 MAC アドレスのグループを指定</p>
送信元 L4 ポート番号 (省略可能)	<p><b>{eq lt gt neq} SRC-L4-PORT</b> : 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。<b>lt</b>, <b>gt</b>, <b>neq</b> は、受信方向のアクセスリストでのみ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>eq</b> : 指定した L4 ポート番号と等しい場合にマッチ</li> <li>• <b>lt</b> : 指定した L4 ポート番号より小さい場合にマッチ</li> <li>• <b>gt</b> : 指定した L4 ポート番号より大きい場合にマッチ</li> <li>• <b>neq</b> : 指定した L4 ポート番号と等しくない場合にマッチ</li> </ul> <p><b>range MIN-SRC-L4-PORT MAX-SRC-L4-PORT</b> : 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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>tcp</b> の場合 : <b>bgp</b>(179) <b>chargen</b>(19) <b>daytime</b>(13) <b>discard</b>(9) <b>domain</b>(53) <b>echo</b>(7) <b>finger</b>(79) <b>ftp</b>(21) <b>ftp-data</b>(20) <b>gopher</b>(70) <b>hostname</b>(101) <b>http</b>(80) <b>ident</b>(113) <b>irc</b>(194) <b>klogin</b>(543) <b>kshell</b>(544) <b>login</b>(513) <b>lpd</b>(515) <b>nntp</b>(119) <b>pop2</b>(109) <b>pop3</b>(110) <b>rexec</b>(512) <b>shell</b>(514) <b>smtp</b>(25) <b>snpp</b>(444) <b>sunrpc</b>(111) <b>tacacs</b>(49) <b>telnet</b>(23) <b>time</b>(37) <b>uucp</b>(540) <b>whois</b>(43)</li> <li>• <b>udp</b> の場合 : <b>biff</b>(512) <b>bootpc</b>(68) <b>bootps</b>(67) <b>discard</b>(9) <b>domain</b>(53) <b>echo</b>(7) <b>irc</b>(194) <b>isakmp</b>(500) <b>mobile-ip</b>(434) <b>nameserver</b>(42) <b>nat-t</b>(4500) <b>netbios-dgm</b>(138) <b>netbios-ns</b>(137) <b>netbios-ss</b>(139) <b>nntp</b>(123) <b>rip</b>(520) <b>snmp</b>(161) <b>snmptrap</b>(162) <b>snpp</b>(444) <b>sunrpc</b>(111) <b>syslog</b>(514) <b>tacacs</b>(49) <b>talk</b>(517)</li> </ul>

抽出条件	概要
	<b>tftp(69) time(37) who(513) xdmcp(177)</b>
宛先 IP アドレス	<p><b>any</b> : すべての宛先 IP アドレスを指定</p> <p><b>host</b> <i>DST-IP-ADDR</i> : 特定の宛先 IP アドレスを指定</p> <p><i>DST-IP-ADDR DST-IP-WILDCARD</i> : 宛先 IP アドレスのグループを指定</p>
宛先 MAC アドレス	<p><b>any</b> : すべての宛先 MAC アドレスを指定</p> <p><b>host</b> <i>DST-MAC-ADDR</i> : 特定の宛先 MAC アドレスを指定</p> <p><i>DST-MAC-ADDR DST-MAC-WILDCARD</i> : 宛先 MAC アドレスのグループを指定</p>
宛先 L4 ポート番号 (省略可能)	<p><b>{eq lt gt neq}</b> <i>DST-L4-PORT</i> : 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。<b>lt</b>, <b>gt</b>, <b>neq</b> は、受信方向のアクセスリストでのみ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>eq</b> : 指定した L4 ポート番号と等しい場合にマッチ</li> <li>• <b>lt</b> : 指定した L4 ポート番号より小さい場合にマッチ</li> <li>• <b>gt</b> : 指定した L4 ポート番号より大きい場合にマッチ</li> <li>• <b>neq</b> : 指定した L4 ポート番号と等しくない場合にマッチ</li> </ul> <p><b>range</b> <i>MIN-DST-L4-PORT MAX-DST-L4-PORT</i> : 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。</p> <p>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。</p>
TCP フラグ (省略可能)	<p>TCP フラグを、<b>ack</b>(acknowledge), <b>fin</b>(finish), <b>psh</b>(push), <b>rst</b>(reset), <b>syn</b>(synchronize), <b>urg</b>(urgent)パラメーターで指定します。</p> <p>同一ルールで複数の TCP フラグを指定する場合は、<b>ack</b>, <b>fin</b>, <b>psh</b>, <b>rst</b>, <b>syn</b>, <b>urg</b> 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。</p>
ICMP メッセージ (省略可能)	<p>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。</p> <p><b>alternate-address</b> (6, -)    <b>bad-length</b> (12, 2)    <b>conversion-error</b> (31, -)  <b>echo</b> (8, 0)    <b>echo-reply</b> (0, 0)    <b>host-isolated</b> (3, 8)    <b>host-precedence-violation</b> (3, 14)  <b>host-prohibited</b> (3, 10)    <b>host-redirect</b> (5, 1)    <b>host-tos-redirect</b> (5, 3)  <b>host-tos-unreachable</b> (3, 12)    <b>host-unknown</b> (3, 7)    <b>host-unreachable</b> (3, 1)  <b>information-reply</b> (16, 0)    <b>information-request</b> (15, 0)  <b>mask-reply</b> (18, 0)    <b>mask-request</b> (17, 0)    <b>mobile-redirect</b> (32, -)  <b>net-prohibited</b> (3, 9)    <b>net-redirect</b> (5, 0)    <b>net-tos-redirect</b> (5, 2)    <b>net-tos-unreachable</b> (3, 11)  <b>net-unknown</b> (3, 6)    <b>net-unreachable</b> (3, 0)    <b>option-missing</b> (12, 1)  <b>packet-fragment</b> (3, 4)    <b>parameter-problem</b> (12, -)    <b>pointer-indicates-error</b> (12, 0)  <b>port-unreachable</b> (3, 3)    <b>precedence-cutoff</b> (3, 15)  <b>protocol-unreachable</b> (3, 2)    <b>reassembly-timeout</b> (11, 1)    <b>redirect-message</b> (5, -)  <b>router-advertisement</b> (9, 0)    <b>router-solicitation</b> (10, 0)  <b>source-quench</b> (4, 0)    <b>source-route-failed</b> (3, 5)    <b>time-exceeded</b> (11, -)  <b>timestamp-reply</b> (14, 0)    <b>timestamp-request</b> (13, 0)    <b>traceroute</b> (30, 0)    <b>ttl-expired</b> (11, 0)    <b>unreachable</b> (3, -)</p>
CoS (省略可能)	<p><b>cos</b> <i>OUTER-COS</i> [<b>inner</b> <i>INNER-COS</i>] : 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。</p>
VLAN ID (省略可能)	<p><b>vlan</b> <i>OUTER-VLAN</i> [<b>inner</b> <i>INNER-VLAN</i>] : 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。</p>

抽出条件	概要
フラグメント (省略可能)	<b>fragments</b> : フラグメントされたパケットを指定します。
DSCP (省略可能)	<b>precedence</b> <i>PRECEDENCE</i> <b>tos</b> <i>TOS</i>   <b>dscp</b> <i>DSCP</i> : 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。 <ul style="list-style-type: none"> <li>ip precedence : <b>routine</b>(0) <b>priority</b>(1) <b>immediate</b>(2) <b>flash</b>(3) <b>flash-override</b>(4) <b>critical</b>(5) <b>internet</b>(6) <b>network</b>(7)</li> <li>tos : <b>normal</b>(0) <b>min-monetary-cost</b>(1) <b>max-reliability</b>(2) <b>max-throughput</b>(4) <b>min-delay</b>(8)</li> <li>DSCP : <b>af11</b>(10) <b>af12</b>(12) <b>af13</b>(14) <b>af21</b>(18) <b>af22</b>(20) <b>af23</b>(22) <b>af31</b>(26) <b>af32</b>(28) <b>af33</b>(30) <b>af41</b>(34) <b>af42</b>(36) <b>af43</b>(38) <b>cs1</b>(8) <b>cs2</b>(16) <b>cs3</b>(24) <b>cs4</b>(32) <b>cs5</b>(40) <b>cs6</b>(48) <b>cs7</b>(56) <b>default</b>(0) <b>ef</b>(46)</li> </ul>
クラス ID (省略可能)	<b>class</b> <i>CLASS-ID</i> : 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	<b>ip access-group</b> { <i>NAME</i>   <i>NUMBER</i> } [ <i>in</i>   <i>out</i> ] <b>no ip access-group</b> [ <i>NAME</i>   <i>NUMBER</i> ] [ <i>in</i>   <i>out</i> ]
パラメーター	<i>NAME</i> : 適用する IP アクセスリスト名を指定します。 <i>NUMBER</i> : 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。 <b>in</b> (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、 <b>in</b> が適用されます。 <b>out</b> (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 ( <b>in</b> 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。ApresiaNP4000 シリーズでは、装置全体で Ingress グループ用に 1920 個、



ip access-group	
	<p>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。</p> <p>ApresiaNP4000 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 960 個、Egress グループに最大 512 個設定できます。</p> <p>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。</p> <p>L4 ポート番号の複数指定で使用する比較演算子 (<b>lt</b>, <b>gt</b>, <b>neq</b>) と範囲指定パラメーター (<b>range</b>) 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 (<b>lt</b>, <b>gt</b>, <b>neq</b>) と範囲指定パラメーター (<b>range</b>) 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。</p>
制限事項	<p>抽出条件「クラス ID (<b>class</b>)」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。</p> <p>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(<b>out</b> パラメーター)に適用することはできません。</p>
注意事項	<p>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。</p>
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	<p>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。</p>
シンタックス	<pre>ip access-list [extended] NAME [NUMBER] no ip access-list [extended] {NAME   NUMBER}</pre>
パラメーター	<p><b>extended</b> (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。</p> <p><b>NAME</b>：作成・変更する IP アクセスリスト名を、最大 32 文字で指定します。先頭には英字を使用してください。</p> <p><b>NUMBER</b> (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。</p>

ip access-list	
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	<p>拡張 IP アクセスリスト：</p> <pre>[SEQ] {permit [authentication-bypass]   deny} tcp CONDITION</pre> <pre>[SEQ] {permit [authentication-bypass]   deny} udp CONDITION</pre> <pre>[SEQ] {permit [authentication-bypass]   deny} icmp CONDITION</pre> <pre>[SEQ] {permit [authentication-bypass]   deny} [PROTOCOL   protocol-id PROTOCOL-ID] CONDITION</pre> <p>標準 IP アクセスリスト：</p> <pre>[SEQ] {permit [authentication-bypass]   deny} CONDITION</pre> <pre>no SEQ</pre>
パラメーター	<p><i>SEQ</i> (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。</p> <p><b>permit</b>：許可エントリーを設定する場合に指定します。</p> <p><b>authentication-bypass</b> (省略可能)：エントリーに一致するパケットが、AccessDefender 認証のために CPU にコピーされずに送信されるようにする場合に指定します。</p> <p><b>deny</b>：拒否エントリーを設定する場合に指定します。</p> <p><b>tcp</b>：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。</p> <p><b>udp</b>：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。</p> <p><b>icmp</b>：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。</p> <p><i>PROTOCOL</i> (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。</p>

permit   deny (ip access-list)	
	<ul style="list-style-type: none"> <li>• <b>igmp</b>(2) <b>gre</b>(47) <b>esp</b>(50) <b>eigrp</b>(88) <b>ospf</b>(89) <b>ipinip</b>(94) <b>pim</b>(103) <b>pcp</b>(108) <b>vrrp</b>(112)</li> </ul> <p><b>protocol-id</b> <i>PROTOCOL-ID</i> (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。</p> <p><i>CONDITION</i>: 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。</p>
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	<p>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。</p> <p>開始値と増分値を変更するには、<b>access-list resequence</b> コマンドを使用します。なお、<b>access-list resequence</b> 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。</p> <p>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。</p> <p><b>permit</b> エントリーと <b>permit authentication-bypass</b> エントリーの違いは、以下のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>permit</b> エントリーに一致したパケットは、認証を行うために CPU にコピーされます。</li> <li>• <b>permit authentication-bypass</b> エントリーに一致したパケットは、認証のために CPU にコピーされず (認証が行われずに)、正常に送信されます。</li> </ul> <p>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)</p> <ul style="list-style-type: none"> <li>• 送信元 IP アドレス (<i>SRC-IP-ADDR SRC-IP-WILDCARD</i>)</li> <li>• 宛先 IP アドレス (<i>DST-IP-ADDR DST-IP-WILDCARD</i>)</li> </ul>
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	<p>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。</p> <p>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。</p>
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	○	○	○	○	○	—	—	○	○

タイプ	送信元		宛先		TCP Flag	ICMP	フラグ メント	DSCP	クラス ID
	IP	L4	IP	L4					
udp	○	○	○	○	—	—	—	○	○
icmp	○	—	○	—	—	○	—	○	○
PROTOCOL	○	—	○	—	—	—	○	○	○
標準	○	—	○	—	—	—	—	—	○

\* 複数の抽出条件を指定する場合は、この表に記載した左側の抽出条件から順番に指定する。

#### IP アクセスリストの抽出条件

抽出条件	概要
送信元 IP アドレス	<p><b>any</b> : すべての送信元 IP アドレスを指定</p> <p><b>host SRC-IP-ADDR</b> : 特定の送信元 IP アドレスを指定</p> <p><b>SRC-IP-ADDR SRC-IP-WILDCARD</b> : 送信元 IP アドレスのグループを指定</p>
送信元 L4 ポート番号 (省略可能)	<p><b>{eq lt gt neq} SRC-L4-PORT</b> : 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。<b>lt</b>, <b>gt</b>, <b>neq</b> は、受信方向のアクセスリストでのみ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>eq</b> : 指定した L4 ポート番号と等しい場合にマッチ</li> <li>• <b>lt</b> : 指定した L4 ポート番号より小さい場合にマッチ</li> <li>• <b>gt</b> : 指定した L4 ポート番号より大きい場合にマッチ</li> <li>• <b>neq</b> : 指定した L4 ポート番号と等しくない場合にマッチ</li> </ul> <p><b>range MIN-SRC-L4-PORT MAX-SRC-L4-PORT</b> : 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。</p> <p>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。</p>
宛先 IP アドレス	<p><b>any</b> : すべての宛先 IP アドレスを指定</p> <p><b>host DST-IP-ADDR</b> : 特定の宛先 IP アドレスを指定</p> <p><b>DST-IP-ADDR DST-IP-WILDCARD</b> : 宛先 IP アドレスのグループを指定</p>
宛先 L4 ポート番号 (省略可能)	<p><b>{eq lt gt neq} DST-L4-PORT</b> : 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。<b>lt</b>, <b>gt</b>, <b>neq</b> は、受信方向のアクセスリストでのみ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>eq</b> : 指定した L4 ポート番号と等しい場合にマッチ</li> <li>• <b>lt</b> : 指定した L4 ポート番号より小さい場合にマッチ</li> <li>• <b>gt</b> : 指定した L4 ポート番号より大きい場合にマッチ</li> <li>• <b>neq</b> : 指定した L4 ポート番号と等しくない場合にマッチ</li> </ul> <p><b>range MIN-DST-L4-PORT MAX-DST-L4-PORT</b> : 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。</p> <p>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。</p>
TCP フラグ (省略可能)	<p>TCP フラグを、<b>ack</b>(acknowledge), <b>fin</b>(finish), <b>psh</b>(push), <b>rst</b>(reset), <b>syn</b>(synchronize), <b>urg</b>(urgent)パラメーターで指定します。</p> <p>同一ルールで複数の TCP フラグを指定する場合は、<b>ack</b>, <b>fin</b>, <b>psh</b>, <b>rst</b>, <b>syn</b>, <b>urg</b> 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。</p>
ICMP メッセージ (省略可能)	<p>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</p>

抽出条件	概要
	「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)	<b>fragments</b> : フラグメントされたパケットを指定します。
DSCP (省略可能)	<b>precedence</b> <i>PRECEDENCE</i> <b>tos</b> <i>TOS</i>   <b>dscp</b> <i>DSCP</i> : 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)	<b>class</b> <i>CLASS-ID</i> : 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 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	<b>ipv6 access-group</b> { <i>NAME</i>   <i>NUMBER</i> } [ <i>in</i>   <i>out</i> ] <b>no ipv6 access-group</b> [ <i>NAME</i>   <i>NUMBER</i> ] [ <i>in</i>   <i>out</i> ]
パラメーター	<i>NAME</i> : 適用する IPv6 アクセスリスト名を指定します。 <i>NUMBER</i> : 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。 <b>in</b> (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、 <b>in</b> が適用されます。 <b>out</b> (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

ipv6 access-group	
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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。ApresiaNP4000 シリーズでは、装置全体で Ingress グループ用に 1920 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。</p> <p>ApresiaNP4000 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 448 個、Egress グループに最大 256 個設定できます。</p> <p>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。</p> <p>L4 ポート番号の複数指定で使用する比較演算子 (<b>lt</b>, <b>gt</b>, <b>neq</b>) と範囲指定パラメーター (<b>range</b>) 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 (<b>lt</b>, <b>gt</b>, <b>neq</b>) と範囲指定パラメーター (<b>range</b>) 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。</p> <p>抽出条件「フローラベル (<b>flow-label</b>)」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。</p>
制限事項	<p>抽出条件「クラス ID (<b>class</b>)」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。</p> <p>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(<b>out</b> パラメーター)に適用することはできません。</p>
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)#
```

## 8.1.11 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	<b>ipv6 access-list</b> [extended] <i>NAME</i> [ <i>NUMBER</i> ] <b>no ipv6 access-list</b> [extended] { <i>NAME</i>   <i>NUMBER</i> }
パラメーター	<b>extended</b> (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。  <i>NAME</i> : 作成・変更する IPv6 アクセスリスト名を、最大 32 文字で指定します。先頭には英字を使用してください。  <i>NUMBER</i> (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	-
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)#
```

## 8.1.12 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	<b>拡張 IPv6 アクセスリスト :</b> <code>[SEQ] {permit [authentication-bypass]   deny} tcp <i>CONDITION</i></code> <code>[SEQ] {permit [authentication-bypass]   deny} udp <i>CONDITION</i></code> <code>[SEQ] {permit [authentication-bypass]   deny} icmp <i>CONDITION</i></code> <code>[SEQ] {permit [authentication-bypass]   deny} [<i>PROTOCOL</i>   protocol-id <i>PROTOCOL-ID</i>] <i>CONDITION</i></code> <b>標準 IPv6 アクセスリスト :</b> <code>[SEQ] {permit [authentication-bypass]   deny} <i>CONDITION</i></code> <code>no <i>SEQ</i></code>

permit   deny (ipv6 access-list)	
パラメーター	<p><i>SEQ</i> (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 of 優先度が高くなります。</p> <p><b>permit</b> : 許可エントリーを設定する場合に指定します。</p> <p><b>authentication-bypass</b> (省略可能) : エントリーに一致するパケットが、AccessDefender 認証のために CPU にコピーされずに送信されるようにする場合に指定します。</p> <p><b>deny</b> : 拒否エントリーを設定する場合に指定します。</p> <p><b>tcp</b> : 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。</p> <p><b>udp</b> : 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。</p> <p><b>icmp</b> : 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。</p> <p><i>PROTOCOL</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>esp</b>(50) <b>pcp</b>(108) <b>sctp</b>(132)</li> </ul> <p><b>protocol-id</b> <i>PROTOCOL-ID</i> (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。</p> <p><i>CONDITION</i>: 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。</p>
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
特権レベル	レベル : 12
ガイドライン	<p>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。</p> <p>開始値と増分値を変更するには、<b>access-list resequence</b> コマンドを使用します。なお、<b>access-list resequence</b> 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。</p> <p>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。</p> <p><b>permit</b> エントリーと <b>permit authentication-bypass</b> エントリーの違いは、以下のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>permit</b> エントリーに一致したパケットは、認証を行うために CPU にコピーされます。</li> <li>• <b>permit authentication-bypass</b> エントリーに一致したパケットは、認証のために CPU にコピーされず (認証が行われずに)、正常に送信されます。</li> </ul>
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	<p>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。</p> <p>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</p>



permit   deny (ipv6 access-list)	
	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

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	ICMP	フラグ	DSCP	フロー	クラス
	IPv6	L4	IPv6	L4	Flag		メント		ラベル	ID
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。

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	<p><b>any</b> : すべての送信元 IPv6 アドレスを指定</p> <p><b>host SRC-IPV6-ADDR</b> : 特定の送信元 IPv6 アドレスを指定</p> <p><b>SRC-IPV6-ADDR/PREFIX-LENGTH</b> : 送信元 IPv6 アドレスのプレフィックス指定</p>
送信元 L4 ポート番号 (省略可能)	<p><b>{eq lt gt neq} SRC-L4-PORT</b> : 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。<b>lt</b>, <b>gt</b>, <b>neq</b> は、受信方向のアクセスリストでのみ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>eq</b> : 指定した L4 ポート番号と等しい場合にマッチ</li> <li>• <b>lt</b> : 指定した L4 ポート番号より小さい場合にマッチ</li> <li>• <b>gt</b> : 指定した L4 ポート番号より大きい場合にマッチ</li> <li>• <b>neq</b> : 指定した L4 ポート番号と等しくない場合にマッチ</li> </ul> <p><b>range MIN-SRC-L4-PORT MAX-SRC-L4-PORT</b> : 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。</p> <p>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。</p>
宛先 IPv6 アドレス	<p><b>any</b> : すべての宛先 IPv6 アドレスを指定</p> <p><b>host DST-IPV6-ADDR</b> : 特定の宛先 IPv6 アドレスを指定</p> <p><b>DST-IPV6-ADDR/PREFIX-LENGTH</b> : 宛先 IPv6 アドレスのプレフィックス指定</p>
宛先 L4 ポート番号 (省略可能)	<p><b>{eq lt gt neq} DST-L4-PORT</b> : 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。<b>lt</b>, <b>gt</b>, <b>neq</b> は、受信方向のアクセスリストでのみ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>eq</b> : 指定した L4 ポート番号と等しい場合にマッチ</li> <li>• <b>lt</b> : 指定した L4 ポート番号より小さい場合にマッチ</li> <li>• <b>gt</b> : 指定した L4 ポート番号より大きい場合にマッチ</li> <li>• <b>neq</b> : 指定した L4 ポート番号と等しくない場合にマッチ</li> </ul> <p><b>range MIN-DST-L4-PORT MAX-DST-L4-PORT</b> : 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。</p> <p>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</p>

抽出条件	概要
	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、 <b>ack</b> (acknowledge), <b>fin</b> (finish), <b>psh</b> (push), <b>rst</b> (reset), <b>syn</b> (synchronize), <b>urg</b> (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、 <b>ack</b> , <b>fin</b> , <b>psh</b> , <b>rst</b> , <b>syn</b> , <b>urg</b> 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。  <b>beyond-scope</b> (1, 2) <b>destination-unreachable</b> (1, 3) <b>echo-reply</b> (129, 0) <b>echo-request</b> (128, 0) <b>erroneous_header</b> (4, 0) <b>hop-limit</b> (3, 0) <b>multicast-listener-done</b> (132, 0) <b>multicast-listener-query</b> (130, 0) <b>multicast-listener-report</b> (131, 0) <b>nd-na</b> (136, 0) <b>nd-ns</b> (135, 0) <b>next-header</b> (4, 1) <b>no-admin</b> (1, 1) <b>no-route</b> (1, 0) <b>packet-too-big</b> (2, 0) <b>parameter-option</b> (4, 2) <b>parameter-problem</b> (4, -) <b>port-unreachable</b> (1, 4) <b>reassembly-timeout</b> (3, 1) <b>redirect</b> (137, 0) <b>renum-command</b> (138, 0) <b>renum-result</b> (138, 1) <b>renum-seq-number</b> (138, 255) <b>router-advertisement</b> (134, 0) <b>router-renumbering</b> (138, -) <b>router-solicitation</b> (133, 0) <b>time-exceeded</b> (3, -) <b>unreachable</b> (1, -)
フラグメント (省略可能)	<b>fragments</b> : フラグメントされたパケットを指定します。
DSCP (省略可能)	<b>dscp</b> <i>DSCP</i> : 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。
フローラベル (省略可能)	<b>flow-label</b> <i>FLOW-LABEL</i> : 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。
クラス ID (省略可能)	<b>class</b> <i>CLASS-ID</i> : 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)#
```

### 8.1.13 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	<b>mac access-group</b> { <i>NAME</i>   <i>NUMBER</i> } [ <i>in</i>   <i>out</i> ] <b>no mac access-group</b> [ <i>NAME</i>   <i>NUMBER</i> ] [ <i>in</i>   <i>out</i> ]
パラメーター	<i>NAME</i> : 適用する拡張 MAC アクセスリスト名を指定します。 <i>NUMBER</i> : 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。 <b>in</b> (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、 <b>in</b> が適用されます。 <b>out</b> (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 ( <b>in</b> 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。 すでにインターフェースに設定されている状態で、別の拡張 MAC アクセスリストを指定して再度設定すると、前の設定を上書きします。 同一インターフェースには同じ種類のアクセスリストは 1 つしか適用できませんが、異なる種類のアクセスリストは同一インターフェースに適用できます。 アクセスリストを適用すると、装置のアクセスリスト用のリソースを消費します。ApresiaNP4000 シリーズでは、装置全体で Ingress グループ用に 1920 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。 ApresiaNP4000 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 1920 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 ( <b>class</b> )」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( <b>out</b> 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)#
```

### 8.1.14 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)# に変更されません。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	<b>mac access-list extended</b> <i>NAME</i> [ <i>NUMBER</i> ] <b>no mac access-list extended</b> { <i>NAME</i>   <i>NUMBER</i> }
パラメーター	<i>NAME</i> : 作成・変更する拡張 MAC アクセスリスト名を、最大 32 文字で指定します。先頭には英字を使用してください。  <i>NUMBER</i> (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	-
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)#
```

### 8.1.15 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	[ <i>SEQ</i> ] { <b>permit</b> [ <i>authentication-bypass</i> ]   <b>deny</b> } <i>CONDITION</i> <b>no</b> <i>SEQ</i>
パラメーター	<i>SEQ</i> (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。  <b>permit</b> : 許可エントリーを設定する場合に指定します。  <b>authentication-bypass</b> (省略可能) : エントリーに一致するパケットが、AccessDefender 認証のために CPU にコピーされずに送信されるようにする場合に指定します。

permit   deny (mac access-list)	
	<p><b>deny</b> : 拒否エントリーを設定する場合に指定します。</p> <p><i>CONDITION</i>: 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。</p>
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	<p>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。</p> <p>開始値と増分値を変更するには、<b>access-list resequence</b> コマンドを使用します。なお、<b>access-list resequence</b> 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。</p> <p>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。</p> <p><b>permit</b> エントリーと <b>permit authentication-bypass</b> エントリーの違いは、以下のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>permit</b> エントリーに一致したパケットは、認証を行うために CPU にコピーされます。</li> <li>• <b>permit authentication-bypass</b> エントリーに一致したパケットは、認証のために CPU にコピーされず (認証が行われずに)、正常に送信されます。</li> </ul> <p>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 : 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)</p> <ul style="list-style-type: none"> <li>• 送信元 MAC アドレス (<i>SRC-MAC-ADDR SRC-MAC-WILDCARD</i>)</li> <li>• 宛先 MAC アドレス (<i>DST-MAC-ADDR DST-MAC-WILDCARD</i>)</li> <li>• イーサタイプ (<b>ethernet-type</b> <i>TYPE MASK</i>)</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul>
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	<b>any</b> : すべての送信元 MAC アドレスを指定

抽出条件	概要
	<b>host</b> <i>SRC-MAC-ADDR</i> : 特定の送信元 MAC アドレスを指定 <i>SRC-MAC-ADDR SRC-MAC-WILDCARD</i> : 送信元 MAC アドレスのグループを指定
宛先 MAC アドレス	<b>any</b> : すべての宛先 MAC アドレスを指定 <b>host</b> <i>DST-MAC-ADDR</i> : 特定の宛先 MAC アドレスを指定 <i>DST-MAC-ADDR DST-MAC-WILDCARD</i> : 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)	<b>ethernet-type</b> <i>TYPE MASK</i> : 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。 <b>aarp, appletalk, arp, decnet-iv, etype-6000, etype-8042, lat, ladvcsca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp</b>
CoS (省略可能)	<b>cos</b> <i>OUTER-COS [inner INNER-COS]</i> : 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)	<b>vlan</b> <i>OUTER-VLAN [inner INNER-VLAN]</i> : 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)	<b>class</b> <i>CLASS-ID</i> : 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)#
```

### 8.1.16 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	<b>vlan access-map</b> <i>MAP-NAME [SEQUENCE-NUM]</i> <b>no vlan access-map</b> <i>MAP-NAME [SEQUENCE-NUM]</i>
パラメーター	<i>MAP-NAME</i> : サブマップを作成する VLAN アクセスマップ名を、最大 32 文字で指定します。 <i>SEQUENCE-NUM</i> (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

vlan access-map	
ガイドライン	<p>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、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。</p> <p>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。</p> <p>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。</p> <p>シーケンス番号を指定せずに <b>no vlan access-map</b> 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。</p>
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)#
```

### 8.1.17 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	<b>match ip address</b> {ACL-NAME   ACL-NUMBER} <b>no match ip address</b> {ACL-NAME   ACL-NUMBER}
パラメーター	<p>ACL-NAME：関連付ける IP アクセスリスト名を指定します。</p> <p>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。</p>
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	<p>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、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。</p> <p>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。</p> <p>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。</p> <p>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 <b>match {ipv6   mac} address</b> コマンドを設定すると、本コマンドの設定が削除されて <b>match {ipv6   mac} address</b> コマンドが設定されます。</p>

match ip address	
	フィルタリング対象のエントリー数は装置全体で 1920 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 <b>vlan filter</b> 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)#
```

### 8.1.18 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	<b>match ipv6 address</b> {ACL-NAME   ACL-NUMBER} <b>no match ipv6 address</b> {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、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 <b>match {ip   mac} address</b> コマンドを設定すると、本コマンドの設定が削除されて <b>match {ip   mac} address</b> 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 1920 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 <b>vlan filter</b> 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)#
```

### 8.1.19 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	<b>match mac address</b> { <i>ACL-NAME</i>   <i>ACL-NUMBER</i> } <b>no match mac address</b> { <i>ACL-NAME</i>   <i>ACL-NUMBER</i> }
パラメーター	<i>ACL-NAME</i> ：関連付ける拡張 MAC アクセスリスト名を指定します。 <i>ACL-NUMBER</i> ：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、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。 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 <b>match {ip   ipv6} address</b> コマンドを設定すると、本コマンドの設定が削除されて <b>match {ip   ipv6} address</b> 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 1920 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 <b>vlan filter</b> 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)#
```

## 8.1.20 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	<b>action</b> {forward   drop   redirect <i>INTERFACE-ID</i> } <b>no action</b>
パラメーター	<b>forward</b> : 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。 <b>drop</b> : 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。 <b>redirect</b> <i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。</li> </ul>
デフォルト	<b>forward</b>
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。  <b>redirect</b> 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。 <b>redirect</b> 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	-
注意事項	<b>redirect</b> 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)#
```

## 8.1.21 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	<b>vlan filter</b> <i>MAP-NAME</i> <b>vlan-list</b> <i>VLAN-ID-LIST</i> <b>no vlan filter</b> <i>MAP-NAME</i> <b>vlan-list</b> <i>VLAN-ID-LIST</i>
パラメーター	<i>MAP-NAME</i> : VLAN アクセスマップ名を指定します。

vlan filter	
	<i>VLAN-ID-LIST</i> : 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。 <ul style="list-style-type: none"> <li>• (例) 2 台スタック構成で 896 エントリー分のリソースが設定済みの状態で、更に 896 エントリー分のリソースを消費する設定を追加する場合、最大で約 200 秒程度かかることがあります。</li> </ul> <p>AEOS-NP4000 Ver. 1.02.04 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。</p>
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)#
```

### 8.1.22 show access-group

show access-group	
目的	インターフェースのアクセスリスト情報を表示します。
シンタックス	<b>show access-group</b> [ <b>interface</b> <i>INTERFACE-ID</i> ]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> </ul>
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 : すべてのインターフェースに適用されるアクセスリスト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)	インターフェース ID を表示します。
(2)	アクセスリストの種類を表示します。

項番	説明
(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。

### 8.1.23 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	<code>show access-list [ip [NAME   NUMBER]   mac [NAME   NUMBER]   ipv6 [NAME   NUMBER]   expert [NAME   NUMBER]]</code>
パラメーター	<p><b>ip</b> (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。</p> <ul style="list-style-type: none"> <li><i>NAME</i> (省略可能) : IP アクセスリスト名</li> <li><i>NUMBER</i> (省略可能) : IP アクセスリスト番号(1~3999)</li> </ul> <p><b>mac</b> (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。</p> <ul style="list-style-type: none"> <li><i>NAME</i> (省略可能) : 拡張 MAC アクセスリスト名</li> <li><i>NUMBER</i> (省略可能) : 拡張 MAC アクセスリスト番号(6000~7999)</li> </ul> <p><b>ipv6</b> (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。</p> <ul style="list-style-type: none"> <li><i>NAME</i> (省略可能) : IPv6 アクセスリスト名</li> <li><i>NUMBER</i> (省略可能) : IPv6 アクセスリスト番号(11000~14999)</li> </ul> <p><b>expert</b> (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。</p> <ul style="list-style-type: none"> <li><i>NAME</i> (省略可能) : 拡張エキスパートアクセスリスト名</li> <li><i>NUMBER</i> (省略可能) : 拡張エキスパートアクセスリスト番号(8000~9999)</li> </ul>
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 : すべてのアクセスリストを表示する方法を示します。

```
# show access-list
(1)
Access-List-Name                               (2)
-----
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 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。

### 8.1.24 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	<b>show access-list resource reserved-group</b>
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	1.02.01

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          AccessDefenderI
1/2          AccessDefenderII
1/3          AccessDefenderIII & Loop Detection
1/4          Access-list (IPv4)
1/5          Access-list (Expert)
1/6          AccessDefender (reserve)
1/7          AccessDefender (reserve)
1/8          AccessDefender (reserve)
1/9          -
1/10         -
1/11         -
1/12         -
1/13         -
1/14         -
```

1/15	-
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。
(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。

### 8.1.25 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	<b>show access-list resource reserved-priority</b>										
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	<p>アクセスリスト機能においては、各アクセスリストが以下の優先度順で動作します。</p> <table border="1"> <thead> <tr> <th>優先度</th> <th>アクセスリスト種別</th> </tr> </thead> <tbody> <tr> <td>高</td> <td>拡張エキスパートアクセスリスト</td> </tr> <tr> <td> </td> <td>拡張 MAC アクセスリスト</td> </tr> <tr> <td> </td> <td>IP アクセスリスト</td> </tr> <tr> <td>低</td> <td>IPv6 アクセスリスト</td> </tr> </tbody> </table>	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		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
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										
	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	1.02.01										

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	AccessDefenderI
4	AccessDefenderII

5	AccessDefenderIII & Loop Detection
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
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 グループのプライオリティを表示します。
(2)	Ingress グループを利用している機能を表示します。
(3)	アクセスリストの Egress グループのプライオリティを表示します。
(4)	Egress グループを利用している機能を表示します。

### 8.1.26 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	<b>show vlan access-map</b> [ <i>MAP-NAME</i> ]
パラメーター	<i>MAP-NAME</i> (省略可能) : 表示する VLAN アクセスマップ名を、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	ユーザー実行モード、特権実行モード、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。

### 8.1.27 show vlan filter

show vlan filter	
目的	VLAN インターフェースの VLAN フィルター設定を表示します。
シンタックス	<b>show vlan filter</b> [ <b>access-map</b> <i>MAP-NAME</i>   <b>vlan</b> <i>VLAN-ID</i> ]
パラメーター	<b>access-map</b> <i>MAP-NAME</i> (省略可能) : VLAN アクセスマップを適用している VLAN フィルターの設定を表示する場合に、VLAN アクセスマップ名を、最大 32 文字で指定します。  <b>vlan</b> <i>VLAN-ID</i> (省略可能) : VLAN に適用されている VLAN フィルターの設定を表示する場合に、VLAN 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	VLAN アクセスマップによる VLAN フィルター情報を表示するには、 <b>show vlan filter access-map</b> コマンドを使用します。VLAN による VLAN フィルター情報を表示するには、 <b>show vlan filter vlan</b> 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 フィルター情報を表示する方法を示します。

```
# show vlan filter

VLAN Map aa ... (1)
  Configured on VLANs: 5-127,221-333 ... (2)
VLAN Map bb
  Configured on VLANs: 1111-1222

# show vlan filter vlan 5

VLAN ID 5 ... (3)
  VLAN Access Map: aa ... (4)
```

項番	説明
(1)	VLAN アクセスマップ名を表示します。
(2)	VLAN アクセスマップを適用する VLAN ID を表示します。
(3)	VLAN ID を表示します。
(4)	VLAN に適用された VLAN アクセスマップ名を表示します。

## 8.1.28 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をクリアします。
シンタックス	<b>clear acl-hardware-counter</b> { <b>access-group</b> [ <i>ACL-NAME</i>   <i>ACL-NUMBER</i> ]   <b>vlan-filter</b> [ <i>MAP-NAME</i> ]}
パラメーター	<i>ACL-NAME</i> (省略可能) : ハードウェアカウンタをクリアするアクセスリスト名を指定します。 <i>ACL-NUMBER</i> (省略可能) : ハードウェアカウンタをクリアするアクセスリスト番号を指定します。 <i>MAP-NAME</i> (省略可能) : ハードウェアカウンタをクリアする 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
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-FILE copy SYSTEM-FILE {flash: [URL]   tftp: [URL]}
access-defender deny	access-defender deny {ip IP-ADDRESS   mac MAC-ADDRESS} timer MINUTES no access-defender deny {ip IP-ADDRESS   mac MAC-ADDRESS}
access-defender erase	access-defender erase [SYSTEM-FILE]
access-defender logout	access-defender logout {ip IP-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	<b>access-defender</b>
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	-
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	1.02.01

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	<b>total-client</b> NUMBER1 [ <b>deny-client</b> NUMBER2] <b>no total-client</b>
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。 <b>deny-client</b> 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	<b>total-client</b> : なし、 <b>deny-client</b> : 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、 <b>deny-client</b> パラメーターで認証拒否クライアントの最大数を設定してから、 <b>access-defender deny</b> コマンドで登録します。
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を共有します。コマンドを実行するために十分なリソースがない場合、コマンドは実行できません。

total-client	
	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	1.02.01

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	<pre>authentication interface <i>INTERFACE-ID</i> [, -] {dot1x   mac   web   gateway   static   web-mac   web-dot1x   dot1x-mac   web-dot1x-mac} no authentication interface <i>INTERFACE-ID</i> [, -] {dot1x   mac   web   gateway   static   web-mac   web-dot1x   dot1x-mac   web-dot1x-mac}</pre>
パラメーター	<p><i>INTERFACE-ID</i>：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。</p> <ul style="list-style-type: none"> <li>• <b>port</b>：物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b>：ポートチャンネルを指定します。</li> </ul> <p><b>dot1x</b>：IEEE 802.1X 認証の有効/無効を設定する場合に指定します。</p> <p><b>mac</b>：MAC 認証の有効/無効を設定する場合に指定します。</p> <p><b>web</b>：Web 認証の有効/無効を設定する場合に指定します。</p> <p><b>gateway</b>：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。</p> <p><b>static</b>：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。</p> <p><b>web-mac</b>：Web/MAC 認証(AND)の有効/無効を設定する場合に指定します。</p> <p><b>web-dot1x</b>：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。</p> <p><b>dot1x-mac</b>：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。</p> <p><b>web-dot1x-mac</b>：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。</p>
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	<p>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。</p> <p>一方、<b>web-mac</b> 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。</p>

## authentication interface

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。

<p><b>制限事項</b></p>	<p>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。</p> <p>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。</p> <p>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。</p>
<p><b>注意事項</b></p>	<p>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。</p> <p>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。</p>

authentication interface			
認証機能	スタティック認証との併用 (OR)	DHCP スヌーピングとの併用 (AND)	
web	可	可	
dot1x	可	可	
mac	可	可	
web, mac (OR)	可	可	
web, dot1x (OR)	可	可	
dot1x, mac (OR)	可	可	
web, dot1x, mac (OR)	可	可	
gateway	不可	不可	
web-mac (AND)	可	不可	
web-dot1x (AND)	可	不可	
dot1x-mac (AND)	可	不可	
web-dot1x-mac (AND)	可	不可	

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。

対象バージョン	1.02.01
---------	---------

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	ユーザー名、パスワード、VLAN ID、クラス ID を含むエントリーを AccessDefender のローカルデータベースに登録します。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	<b>aaa-local-db user</b> <i>USER-ID</i> [ <b>password</b> [0   7] <i>PASSWORD</i> ] [ <b>vlan</b> <i>VLAN-ID</i> ] [ <b>class</b> <i>CLASS-ID</i> ] <b>no aaa-local-db</b> [ <b>user</b> <i>USER-ID</i> ]
パラメーター	<i>USER-ID</i> : 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。 <b>password</b> [0   7] <i>PASSWORD</i> (省略可能) : エントリーのパスワードを入力する場合に指定します。



aaa-local-db user	
	<ul style="list-style-type: none"> <li>• <b>0</b> : パスワードを平文で入力する場合に指定します。パスワードのデフォルト設定です。</li> <li>• <b>7</b> : 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。</li> <li>• <b>PASSWORD</b> : エントリーのパスワードを入力します。平文で入力する場合は、文字列を最大 63 文字で指定します。ASCII コードの印字可能な文字のうち、<code>;</code>、<code>,</code>、<code> </code>、<code>"</code>、<code>?</code> 空白文字 を除いた文字のみ使用可能です。</li> </ul> <p><b>vlan</b> <i>VLAN-ID</i> (省略可能) : エントリーの VLAN ID を 1~4094 の範囲で指定します。</p> <p><b>class</b> <i>CLASS-ID</i> (省略可能) : エントリーのクラス ID を 1~4095 の範囲で指定します。</p>
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	<p>ユーザー名を指定せずに <code>no aaa-local-db</code> 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。</p> <p>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 <code>mac-authentication username mac-format</code> コマンドの設定に従います。</p>
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	1.02.01

使用例 : ユーザー名、パスワード、VLAN ID、クラス ID を含むエントリーを AccessDefender のローカルデータベースに追加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、 <code>no</code> 形式のコマンドを使用します。
シンタックス	<p><code>access-defender static mac</code> <i>MAC-ADDRESS</i> [<code>vlan</code> <i>VLAN-ID</i>] [<code>class</code> <i>CLASS-ID</i>]  <code>interface</code> <i>INTERFACE-ID</i></p> <p><code>no access-defender static mac</code> <i>MAC-ADDRESS</i></p>
パラメーター	<p><i>MAC-ADDRESS</i> : スタティック認証エントリーの MAC アドレスを、以下のいずれかの形式で指定します。どの形式で指定しても、構成情報では <code>XX-XX-XX-XX-XX-XX</code> 形式で表示されます。</p> <ul style="list-style-type: none"> <li>• <code>XX-XX-XX-XX-XX-XX</code> (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• <code>XX:XX:XX:XX:XX:XX</code> (1 バイトごとにコロン“:”で区切る形式)</li> <li>• <code>XXXX.XXXX.XXXX</code> (2 バイトごとにドット“.”で区切る形式)</li> <li>• <code>XXXXXXXXXXXX</code> (区切り文字を使用しない形式)</li> </ul> <p><b>vlan</b> <i>VLAN-ID</i> (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。</p>

access-defender static mac	
	<p><b>class</b> <i>CLASS-ID</i> (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。</p> <p><b>interface</b> <i>INTERFACE-ID</i> : 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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	<p>スタティック認証エントリーを 1 つ登録するたびに、<b>total-client</b> 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。</p> <p>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。</p> <p>本コマンドの設定は、<b>vlan mode</b> コマンドの設定に影響されません。</p>
制限事項	<p>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。</p> <p><b>total-client</b> コマンドで設定した認証クライアントの最大数を超過して、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。</p> <p>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。</p>
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 <b>authentication interface</b> 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	1.02.01

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징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。
シンタックス	<p><b>logout aging-time</b> <i>SECONDS</i> [<i>MINUTES</i> [<i>HOURS</i> [<i>DAYS</i>]]] {web   gateway   mac   dot1x}</p> <p><b>no logout aging-time</b> [web   gateway   mac   dot1x]</p>
パラメーター	<p><i>SECONDS</i> : エー징ングログアウト時間を、0、10~86,400 秒の範囲で指定します。</p> <p><i>MINUTES</i> (省略可能) : エー징ングログアウト時間を、0~59 分の範囲で指定します。</p> <p><i>HOURS</i> (省略可能) : エー징ングログアウト時間を、0~23 時間の範囲で指定しま</p>

logout aging-time	
	<p>す。</p> <p><i>DAYS</i> (省略可能) : エージングログアウト時間を、0~31 日の範囲で指定します。</p> <p><b>web</b> : Web 認証の認証済みクライアントを対象にする場合に指定します。</p> <p><b>gateway</b> : ゲートウェイ認証の認証済みクライアントを対象にする場合に指定します。</p> <p><b>mac</b> : MAC 認証の認証済みクライアントを対象にする場合に指定します。</p> <p><b>dot1x</b> : IEEE 802.1X 認証の認証済みクライアントを対象にする場合に指定します。</p>
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	<p>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。</p> <p>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、<b>logout aging-time 40 2 0 0</b> 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。</p> <p>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、<b>web</b> 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、<b>dot1x</b> パラメーターを指定して設定してください。</p>
制限事項	-
注意事項	-
対象バージョン	1.02.01

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	<p><b>logout timeout SECONDS [MINUTES [HOURS [DAYS]]] {web   gateway   mac   dot1x}</b></p> <p><b>no logout timeout [web   gateway   mac   dot1x]</b></p>
パラメーター	<p><i>SECONDS</i> : タイムアウト時間を、0, 10~86,400 秒の範囲で指定します。</p> <p><i>MINUTES</i> (省略可能) : タイムアウト時間を、0~59 分の範囲で指定します。</p> <p><i>HOURS</i> (省略可能) : タイムアウト時間を、0~23 時間の範囲で指定します。</p>

logout timeout	
	<p><i>DAYS</i> (省略可能) : タイムアウト時間を、0~31 日の範囲で指定します。</p> <p><b>web</b> : Web 認証の認証済みクライアントを対象にする場合に指定します。</p> <p><b>gateway</b> : ゲートウェイ認証の認証済みクライアントを対象にする場合に指定します。</p> <p><b>mac</b> : MAC 認証の認証済みクライアントを対象にする場合に指定します。</p> <p><b>dot1x</b> : IEEE 802.1X 認証の認証済みクライアントを対象にする場合に指定します。</p>
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	<p>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。</p> <p>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、<b>logout timeout 40 2 0 0</b> と設定した場合は、タイムアウト時間は 160 秒になります。</p> <p>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、<b>web</b> 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、<b>dot1x</b> パラメーターを指定して設定してください。</p>
制限事項	-
注意事項	-
対象バージョン	1.02.01

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	<pre>logout clock HH:MM {web   gateway   mac   dot1x} no logout clock [web   gateway   mac   dot1x]</pre>
パラメーター	<p><i>HH:MM</i> : ログアウトする時刻を時 (24 時間表記) と分で指定します。</p> <p><b>web</b> : Web 認証の認証済みクライアントを対象にする場合に指定します。</p> <p><b>gateway</b> : ゲートウェイ認証の認証済みクライアントを対象にする場合に指定します。</p> <p><b>mac</b> : MAC 認証の認証済みクライアントを対象にする場合に指定します。</p> <p><b>dot1x</b> : IEEE 802.1X 認証の認証済みクライアントを対象にする場合に指定します。</p>

logout clock	
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、 <b>web</b> 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、 <b>dot1x</b> 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	1.02.01

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	<b>logout ping dst-ip</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> } <b>no logout ping dst-ip</b>
パラメーター	<i>IP-ADDRESS</i> : 宛先 IPv4 アドレスを指定します。 <i>IPV6-ADDRESS</i> : 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 <b>logout ping ttl</b> 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	1.02.01

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	<b>logout ping ttl</b> <i>VALUE</i> <b>no logout ping ttl</b>
パラメーター	<i>VALUE</i> : 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 <b>logout ping dst-ip</b> 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	1.02.01

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	<b>logout linkdown disable interface</b> <i>INTERFACE-ID</i> [, -] <b>no logout linkdown disable interface</b> <i>INTERFACE-ID</i> [, -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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 ( <b>no logout linkdown disable interface</b> )
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	この機能をローミング機能 ( <b>roaming enable interface</b> コマンド) と同時に使

logout linkdown disable interface	
	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	1.02.01

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	<b>logout linkdown time</b> <i>SECONDS</i> <b>no logout linkdown time</b>
パラメーター	<i>SECONDS</i> ：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	1.02.01

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

logout linkdown time enable interface	
	を使用します。
シンタックス	<b>logout linkdown time enable interface</b> <i>INTERFACE-ID</i> [,  -] <b>no logout linkdown time enable interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b>: ポートチャンネルを指定します。</li> </ul>
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、 <b>logout linkdown time</b> 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	1.02.01

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: ポートチャンネル 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	<b>roaming enable interface</b> <i>INTERFACE-ID</i> [,  -] <b>no roaming enable interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b>: ポートチャンネルを指定します。</li> </ul>
デフォルト	無効
コマンドモード	AccessDefender 設定モード



roaming enable interface	
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、 <b>logout linkdown disable interface</b> 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	<b>roaming enable interface</b> コマンドで指定したインターフェースは、 <b>logout linkdown disable interface</b> コマンドもあわせて設定してください。
注意事項	<p>ローミング機能は、<b>roaming enable interface</b> 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。</p> <p>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 <b>logout linkdown disable interface</b> コマンドを設定してください。</p> <p>ローミングしている接続ポートが変更された場合でも、<b>show access-defender client</b> 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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
対象バージョン	1.02.01

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。

authentication prefer-attribute	
シンタックス	<pre>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</pre>
パラメーター	<p><b>web-mac</b> : Web/MAC 認証(AND)を設定する場合に指定します。</p> <p><b>dot1x-mac</b> : IEEE 802.1X/MAC 認証(AND)を設定する場合に指定します。</p> <p><b>web-dot1x</b> : Web/IEEE 802.1X 認証(AND)を設定する場合に指定します。</p> <p><b>web-dot1x-mac</b> : Web/IEEE 802.1X/MAC 認証(AND)を設定する場合に指定します。</p> <p><b>prefer-attribute</b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>web</b> : Web 認証で取得した認証属性を適用します。</li> <li>• <b>dot1x</b> : IEEE 802.1X 認証で取得した認証属性を適用します。</li> <li>• <b>mac</b> : MAC 認証で取得した認証属性を適用します。</li> </ul>
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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>show access-defender client</b> コマンドで表示されるユーザー名</li> <li>• ログイン成功ログで表示されるユーザー名</li> </ul>
制限事項	<p>Web/MAC 認証(AND)では、<b>dot1x</b> パラメーターは指定できません。</p> <p>IEEE 802.1X/MAC 認証(AND)では、<b>web</b> パラメーターは指定できません。</p> <p>Web/IEEE 802.1X 認証(AND)では、<b>mac</b> パラメーターは指定できません。</p>
注意事項	-
対象バージョン	1.02.01

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	<pre>authentication {web-mac   web-dot1x} advanced-vlan-setting no authentication {web-mac   web-dot1x} advanced-vlan-setting</pre>
パラメーター	<b>web-mac</b> : 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

authentication advanced-vlan-setting	
	<p>する場合に指定します。</p> <p><b>web-dot1x</b> : 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。</p>
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	<p>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。</p> <p>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。</p>
制限事項	-
注意事項	-
対象バージョン	1.02.01

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 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	<p><b>max-client</b> <i>NUMBER</i> <b>interface</b> <i>INTERFACE-ID</i> [,  -]</p> <p><b>no max-client interface</b> <i>INTERFACE-ID</i> [,  -]</p>
パラメーター	<p><i>NUMBER</i> : 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。</p> <p><i>INTERFACE-ID</i> : 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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャネルを指定します。</li> </ul>
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	1.02.01

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)#
```

### 9.1.18 max-discard

max-discard	
目的	MAC 認証に失敗して Discard 登録されるクライアントの最大数を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>max-discard</b> <i>NUMBER</i> <b>no max-discard</b>
パラメーター	<i>NUMBER</i> : 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	1.02.01

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)#
```

### 9.1.19 vlan mode

vlan mode	
目的	AccessDefender の VLAN モードを設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>vlan mode</b> {dynamic port-base   static} <b>no vlan mode</b>
パラメーター	<b>dynamic port-base</b> : 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。 <b>static</b> : 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

vlan mode																		
	<p>ることができます。</p> <p>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。</p> <table border="1"> <thead> <tr> <th>ログイン中の端末</th> <th>後から認証を行う端末</th> <th>ログイン可否</th> </tr> </thead> <tbody> <tr> <td rowspan="3">装置に設定済みの VLAN</td> <td>VLAN 指定なし</td> <td>可</td> </tr> <tr> <td>VLAN 指定あり (ログイン中の端末と同じ VLAN)</td> <td>可</td> </tr> <tr> <td>VLAN 指定あり (ログイン中の端末と異なる VLAN)</td> <td>不可</td> </tr> <tr> <td rowspan="3">装置に設定済みの VLAN と異なる VLAN</td> <td>VLAN 指定なし</td> <td>不可</td> </tr> <tr> <td>VLAN 指定あり (ログイン中の端末と同じ VLAN)</td> <td>可</td> </tr> <tr> <td>VLAN 指定あり (ログイン中の端末と異なる VLAN)</td> <td>不可</td> </tr> </tbody> </table> <p>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。</p> <p>本コマンドの設定は、<b>access-defender static mac</b> コマンドの設定に影響しません。</p>	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 (ログイン中の端末と異なる VLAN)	不可
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 (ログイン中の端末と異なる VLAN)	不可																
制限事項	-																	
注意事項	-																	
対象バージョン	1.02.01																	

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)#
```

### 9.1.20 radius-server attribute mac-format

radius-server attribute mac-format	
目的	装置から送信される RADIUS 要求パケットの、「Calling-Station-Id」属性の MAC アドレス形式を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>radius-server attribute mac-format case {lowercase   uppercase} delimiter {{hyphen   colon   dot} number {1   2   5}   none}</b> <b>no radius-server attribute mac-format</b>
パラメーター	<p><b>case</b> : 「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。</p> <ul style="list-style-type: none"> <li>• <b>lowercase</b> : 小文字指定 (例 : aabbccddeeff)</li> <li>• <b>uppercase</b> : 大文字指定 (例 : AABCCDDEEFF)</li> </ul> <p><b>delimiter</b> : 区切り文字を指定します。</p> <ul style="list-style-type: none"> <li>• <b>hyphen</b> : ハイフン指定 (例 : aa-bb-cc-dd-ee-ff)</li> </ul>

radius-server attribute mac-format	
	<ul style="list-style-type: none"> <li>• <b>colon</b> : コロン指定 (例 : aa:bb:cc:dd:ee:ff)</li> <li>• <b>dot</b> : ドット指定 (例 : aa.bb.cc.dd.ee.ff)</li> <li>• <b>none</b> : 区切り文字を使用しない場合に指定 (例 : aabbccddeeff)</li> </ul> <p><b>number</b> : 区切り文字の数を指定します。</p> <ul style="list-style-type: none"> <li>• <b>1</b> : 区切り文字 1 個指定 (例 : aabbcc-ddeeff)</li> <li>• <b>2</b> : 区切り文字 2 個指定 (例 : aabb-ccdd-eeff)</li> <li>• <b>5</b> : 区切り文字 5 個指定 (例 : aa-bb-cc-dd-ee-ff)</li> </ul>
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	1.02.01

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)#
```

### 9.1.21 show access-defender aaa-local-db

show access-defender aaa-local-db	
目的	AccessDefender のローカルデータベースの情報を表示します。
シンタックス	<b>show access-defender aaa-local-db</b>
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	1.02.01

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。

### 9.1.22 show access-defender client

show access-defender client	
目的	認証済みクライアントと、MAC 認証に失敗して Discard 登録されたクライアントを表示します。
シンタックス	<code>show access-defender client [interface <i>INTERFACE-ID</i> [,  -]] [type {dhcp-snooping   disc   dot1x   gateway   mac   static   web}]</code>
パラメーター	<p><b>interface</b> <i>INTERFACE-ID</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul> <p><b>type</b> (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。</p> <ul style="list-style-type: none"> <li>• <b>dhcp-snooping</b> : DHCP スヌーピングの登録済みクライアント。</li> <li>• <b>disc</b> : MAC 認証に失敗して Discard 登録されたクライアント。</li> <li>• <b>dot1x</b> : IEEE 802.1X 認証の認証済みクライアント。</li> <li>• <b>gateway</b> : ゲートウェイ認証の認証済みクライアント。</li> <li>• <b>mac</b> : MAC 認証の認証済みクライアント。</li> <li>• <b>static</b> : スタティック認証の登録済みクライアント。</li> <li>• <b>web</b> : Web 認証の認証済みクライアント。</li> </ul>
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	1.02.01

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           :    3 ... (1)
Total number of Discarded Clients :    1 ... (2)

Codes: W = Web authentication, G = Gateway authentication,
       M = MAC authentication, - = MAC authentication (discard),
       X = IEEE802.1X, D(S) = DHCP snooping (static),
       S = Static authentication
Port: C = port-channel, * = roaming,
(3) (4)           (5)                               (6) (7) (8)
T  MAC address   IP                               Port VID Cls
(9)                                     (10) (11)
```

User	Time	Aging
- 00-17-A4-F6-D3-04 0017a4f6d304	1/0/3 0:00:21	0:00:00
WD 00-17-A4-D6-B3-A4 172.170.100.100 webuser01	1/0/1 4094 0:20:39	10 0:00:00
WM 00-17-A4-D6-F3-C4 172.170.1.1 webuser03	1/0/2 4094 0:20:39	10 0:00:15
D 00-17-29-7F-6F-2A 172.170.2.100 N/A	C/1 0:00:36	0:00:00

項番	説明
(1)	認証済みクライアントの数を表示します。
(2)	MAC 認証に失敗して Discard 登録されたクライアントの数を表示します。
(3)	認証済みクライアント、または MAC 認証に失敗して Discard 登録されたクライアントのタイプコードを表示します。タイプコードが複数ある場合は、そのクライアントが AND 認証に成功したことを意味します。 W : Web 認証 G : ゲートウェイ認証 M : MAC 認証 - : MAC 認証に失敗して Discard 登録されたクライアント X : IEEE 802.1X 認証 D : DHCP スヌーピング S : スタティック認証
(4)	クライアントの MAC アドレスを表示します。
(5)	クライアントの IP アドレスを表示します。
(6)	クライアントが接続されたインターフェース ID 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。

### 9.1.23 show access-defender deny

show access-defender deny	
目的	認証拒否クライアントの情報を表示します。
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



show access-defender deny	
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	1.02.01

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      :  2 ... (1)
(2)          (3)                      (4)
MAC address      IP                      Timer
-----
00-00-11-11-22-22 -                      0:29:04
-                100.100.100.100         0:29:04
```

項番	説明
(1)	認証拒否クライアントの数を表示します。
(2)	認証拒否クライアントの MAC アドレスを表示します。
(3)	認証拒否クライアントの IP アドレスを表示します。
(4)	認証拒否クライアントの、認証を拒否する残り時間を表示します。

### 9.1.24 show access-defender port-configuration

show access-defender port-configuration	
目的	ポートの AccessDefender の設定を表示します。
シンタックス	<b>show access-defender port-configuration</b>
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	1.02.01

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,
 DHCPSPNP = 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
          +-----+ +-----+ +-----+
mac       1 ..... 0000.... 0000....
802.1X   1 ..... 0000.... 0000....
web       1 00000000 ..... 0000....
gateway   1 ..... 0000.... 0000....
web/mac   1 ..... 0000.... 0000....
web/.1X   1 ..... 0000.... 0000....
.1X/mac   1 ..... 0000.... 0000....
w/.1X/m   1 ..... 0000.... 0000....
DHCPSNP   1 ..... 0000.... 0000....
roaming   1 ..... 00000000 .....
static    1 ..... 0000.... 0000....
linkdown  1 xxxxxxxxxx xxxxxxxxxx .....
ld time   1 ..... 0000.... 0000....
TTL       1 00000000 ..... 0000....
    
```

項番	説明
(1)	<p>ポートごとに、AccessDefender 設定の各機能の有効/無効を表示します。</p> <p>mac : MAC 認証</p> <p>802.1X : IEEE 802.1X 認証</p> <p>web : Web 認証</p> <p>gateway : ゲートウェイ認証</p> <p>web/mac : Web/MAC 認証 (AND)</p> <p>web/.1X : Web/IEEE 802.1X 認証 (AND)</p> <p>.1X/mac : IEEE 802.1X/MAC 認証 (AND)</p> <p>w/.1X/m : Web/IEEE 802.1X/MAC 認証 (AND)</p> <p>DHCPSNP : DHCP スヌープینگ</p> <p>roaming : ローミング機能</p> <p>static : スタティック認証</p> <p>linkdown : x 表示の場合、リンクダウンによるログアウトが無効</p> <p>ld time : リンクダウン監視時間の設定</p> <p>TTL : Web 認証の TTL フィルター機能</p> <p>"C"はスタックのボックス ID (シャーシ ID) を示します。スタックを構成していない場合は 1 が表示されます。</p>

### 9.1.25 show access-defender port-channel-configuration

show access-defender port-channel-configuration	
目的	ポートチャネルの AccessDefender 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	1.02.01

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 000000.. .....
802.1X     1 .....
web        1 000000.. .....
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 000000.. .....
```

項番	説明
(1)	<p>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。</p> <p>mac : MAC 認証</p> <p>802.1X : IEEE 802.1X 認証</p> <p>web : Web 認証</p> <p>gateway : ゲートウェイ認証</p> <p>web/mac : Web/MAC 認証 (AND)</p> <p>web/.1X : Web/IEEE 802.1X 認証 (AND)</p> <p>.1X/mac : IEEE 802.1X/MAC 認証 (AND)</p> <p>w/.1X/m : Web/IEEE 802.1X/MAC 認証 (AND)</p> <p>DHCPSNP : DHCP スヌーピング</p> <p>roaming : ローミング機能</p> <p>static : スタティック認証</p> <p>linkdown : x 表示の場合、リンクダウンによるログアウトが無効</p> <p>ld time : リンクダウン監視時間の設定</p> <p>TTL : Web 認証の TTL フィルター機能</p> <p>"C"はスタックのボックス ID (シャーシ ID) を示しますが、本コマンドでは常に 1 が表示されます。</p>

### 9.1.26 show access-defender rule-statistics

show access-defender rule-statistics	
目的	AccessDefender に関連するアクセスリストルールの使用状態を表示します。

show access-defender rule-statistics	
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	1.02.01

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。

項番	説明
(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。

### 9.1.27 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	<pre>copy {flash: [URL]   tftp: [URL]} SYSTEM-FILE copy SYSTEM-FILE {flash: [URL]   tftp: [URL]}</pre>
パラメーター	<p><b>flash:</b> : 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。</p> <p><b>tftp:</b> : TFTP を使用する場合に指定します。</p> <p><b>URL</b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>flash: c:/URL</b> : 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。</li> <li>• <b>flash: d:/URL</b> : 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。</li> <li>• <b>tftp: [//IP-ADDRESS/[DIRECTORY/]FILE-NAME]</b> : TFTP サーバー上のファイルを指定します。 <ul style="list-style-type: none"> <li>• <b>IP-ADDRESS</b> : TFTP サーバーの IP アドレスを指定します。</li> <li>• <b>DIRECTORY</b> (省略可能) : ディレクトリー名を指定します。</li> <li>• <b>FILE-NAME</b> : 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。</li> </ul> </li> </ul> <p><b>SYSTEM-FILE</b> : 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。</p> <ul style="list-style-type: none"> <li>• <b>login-page</b> : ログイン認証ページ</li> <li>• <b>login-success-page</b> : 認証成功ページ</li> <li>• <b>login-failure-page</b> : 認証失敗ページ</li> <li>• <b>logout-success-page</b> : ログアウト成功ページ</li> <li>• <b>logout-failure-page</b> : ログアウト失敗ページ</li> <li>• <b>redirect-error-page</b> : リダイレクト失敗ページ</li> <li>• <b>aaa-local-db</b> : AccessDefender のローカルデータベース</li> <li>• <b>https-certificate</b> : SSL サーバー証明書</li> <li>• <b>https-private-key</b> : SSL サーバーの秘密鍵</li> <li>• <b>csr-certificate</b> : CSR (証明書署名要求)</li> <li>• <b>csr-private-key</b> : CSR の秘密鍵</li> <li>• <b>webpage-image01</b> : Web ページの画像 01</li> <li>• <b>webpage-image02</b> : Web ページの画像 02</li> <li>• <b>webpage-image03</b> : Web ページの画像 03</li> <li>• <b>webpage-image04</b> : Web ページの画像 04</li> <li>• <b>webpage-image05</b> : Web ページの画像 05</li> <li>• <b>webpage-image06</b> : Web ページの画像 06</li> <li>• <b>webpage-image07</b> : Web ページの画像 07</li> <li>• <b>webpage-image08</b> : Web ページの画像 08</li> </ul>

copy (AccessDefender)															
	<ul style="list-style-type: none"> <li>• <b>webpage-image09</b> : Web ページの画像 09</li> <li>• <b>webpage-image10</b> : Web ページの画像 10</li> </ul>														
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	<p>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。</p> <p>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、<b>access-defender erase</b> 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。</p> <p>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。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #cccccc;">Web ページの種類</th> <th style="background-color: #cccccc;">内容</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>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。</p> <ul style="list-style-type: none"> <li>• CSV 形式 (userid, password, [vid], [classid] [, *])</li> <li>• userid および password は、最大 63 文字で指定します。</li> <li>• 最大 3,000 行</li> </ul> <p>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。</p> <pre style="border: 1px solid black; padding: 5px;">temp01,temp01,10 temp02,temp02 temp03,temp03,,30 00096b82c51e,1q2w3d,100,10 01010102,*@&amp;foe2zgl6pwJiXjVe0+amVwAAAAC+RzmF,1002,1002,*</pre> <p>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。</p> <p>スラッシュ文字 (/) は、ディレクトリを識別するために使用します。</p> <p>AccessDefender のローカルデータベースファイル :</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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 <b>mac-authentication username mac-format</b> コマンドの設定に従います。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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</li> </ul>	Web ページの種類	内容	ログイン認証ページ	ユーザー名、パスワード	認証成功ページ	認証が成功したときに表示されるページ	認証失敗ページ	認証が失敗したときに表示されるページ	ログアウト成功ページ	ログアウトに成功したときに表示されるページ	ログアウト失敗ページ	ログアウトに失敗したときに表示されるページ	リダイレクト失敗ページ	リダイレクトに失敗したときに表示されるページ
Web ページの種類	内容														
ログイン認証ページ	ユーザー名、パスワード														
認証成功ページ	認証が成功したときに表示されるページ														
認証失敗ページ	認証が失敗したときに表示されるページ														
ログアウト成功ページ	ログアウトに成功したときに表示されるページ														
ログアウト失敗ページ	ログアウトに失敗したときに表示されるページ														
リダイレクト失敗ページ	リダイレクトに失敗したときに表示されるページ														

copy (AccessDefender)	
	<p>にカンマ (,) を追加する必要があります。</p> <ul style="list-style-type: none"> <li>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。</li> </ul> <p>SSL サーバー証明書と秘密鍵：</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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、<b>access-defender erase ssl-files</b> 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。</li> <li>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、<b>access-defender erase ssl-files</b> 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。</li> <li>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。</li> </ul> <p>CSR (証明書署名要求) は、<b>csr-certificate</b> パラメーターおよび <b>csr-privatekey</b> 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。</p> <p>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。</p>
制限事項	<p>ファイル名には、&amp;:;`'¥" *?&lt;&gt;^() [] {}\$ の各文字は使用できません。</p> <p>ファイル名には、「./」の文字列は使用できません。</p>
注意事項	<p>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。</p> <p>Web 認証が有効な状態では、SSL サーバー証明書と秘密鍵はダウンロードできません。</p> <p>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。</p>
対象バージョン	1.02.01

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.
```

### 9.1.28 access-defender deny

access-defender deny	
目的	認証を一時的に拒否するクライアントを登録します。登録を削除する場合は、 <b>no access-defender deny</b> コマンドを使用します。
シンタックス	<b>access-defender deny</b> {ip <i>IP-ADDRESS</i>   mac <i>MAC-ADDRESS</i> } timer <i>MINUTES</i> <b>no access-defender deny</b> {ip <i>IP-ADDRESS</i>   mac <i>MAC-ADDRESS</i> }
パラメーター	<b>ip</b> <i>IP-ADDRESS</i> ：認証を一時的に拒否するクライアントの IPv4 アドレスを指定します。  <b>mac</b> <i>MAC-ADDRESS</i> ：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。 <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul> <b>timer</b> <i>MINUTE</i> ：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、 <b>total-client</b> コマンドの <b>deny-client</b> 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えが発生した場合、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。

access-defender deny	
対象バージョン	1.02.01

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
```

### 9.1.29 access-defender erase

access-defender erase	
目的	AccessDefender のシステムファイルを削除します。
シンタックス	<b>access-defender erase</b> [ <i>SYSTEM-FILE</i> ]
パラメーター	<p><i>SYSTEM-FILE</i> (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。</p> <ul style="list-style-type: none"> <li>• <b>login-page</b>：ログイン認証ページを削除します。</li> <li>• <b>login-success-page</b>：認証成功ページを削除します。</li> <li>• <b>login-failure-page</b>：認証失敗ページを削除します。</li> <li>• <b>logout-success-page</b>：ログアウト成功ページを削除します。</li> <li>• <b>logout-failure-page</b>：ログアウト失敗ページを削除します。</li> <li>• <b>redirect-error-page</b>：リダイレクト失敗ページを削除します。</li> <li>• <b>aaa-local-db</b>：AccessDefender のローカルデータベースを削除します。</li> <li>• <b>ssl-files</b>：SSL サーバー証明書、秘密鍵、および <b>ssl gencsr rsakey</b> コマンドで作成したファイルを削除します。</li> <li>• <b>webpage-image01</b>：Web ページの画像 01 を削除します。</li> <li>• <b>webpage-image02</b>：Web ページの画像 02 を削除します。</li> <li>• <b>webpage-image03</b>：Web ページの画像 03 を削除します。</li> <li>• <b>webpage-image04</b>：Web ページの画像 04 を削除します。</li> <li>• <b>webpage-image05</b>：Web ページの画像 05 を削除します。</li> <li>• <b>webpage-image06</b>：Web ページの画像 06 を削除します。</li> <li>• <b>webpage-image07</b>：Web ページの画像 07 を削除します。</li> <li>• <b>webpage-image08</b>：Web ページの画像 08 を削除します。</li> <li>• <b>webpage-image09</b>：Web ページの画像 09 を削除します。</li> <li>• <b>webpage-image10</b>：Web ページの画像 10 を削除します。</li> </ul>
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。
対象バージョン	1.02.01

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 Access Defender local database settings..... Done.
Erasing SSL files in FLASH..... Done.
Erasing Web authentication webpage-image01 in FLASH..... Done.
Erasing Web authentication webpage-image02 in FLASH..... Done.
Erasing Web authentication webpage-image03 in FLASH..... Done.
Erasing Web authentication webpage-image04 in FLASH..... Done.
Erasing Web authentication webpage-image05 in FLASH..... Done.
Erasing Web authentication webpage-image06 in FLASH..... Done.
Erasing Web authentication webpage-image07 in FLASH..... Done.
Erasing Web authentication webpage-image08 in FLASH..... Done.
Erasing Web authentication webpage-image09 in FLASH..... Done.
Erasing Web authentication webpage-image10 in FLASH..... Done.
```

### 9.1.30 access-defender logout

access-defender logout	
目的	認証済みのクライアントを手動で強制的にログアウトします。または Discard 登録されたクライアントを手動で削除します。
シンタックス	<b>access-defender logout</b> { <b>ip</b> <i>IP-ADDRESS</i>   <b>mac</b> <i>MAC-ADDRESS</i>   <b>user</b> <i>USER-ID</i> }
パラメーター	<p><b>ip</b> <i>IP-ADDRESS</i> : 強制的にログアウトする認証済みクライアントの IPv4 アドレスを指定します。</p> <p><b>mac</b> <i>MAC-ADDRESS</i> : 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。</p> <ul style="list-style-type: none"> <li>• XX-XX-XX-XX-XX-XX (1 バイトごとにハイフン“-”で区切る形式)</li> <li>• XX:XX:XX:XX:XX:XX (1 バイトごとにコロン“:”で区切る形式)</li> <li>• XXXX.XXXX.XXXX (2 バイトごとにドット“.”で区切る形式)</li> <li>• XXXXXXXXXXXX (区切り文字を使用しない形式)</li> </ul> <p><b>user</b> <i>USER-ID</i> : 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。</p>
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	1.02.01

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 : 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、アカウントティング(AAA)コマンド

認証、許可、アカウントティング(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 PORT-NUMBER] [acct-port PORT-NUMBER] [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 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...] no aaa authentication mac-auth default
aaa authentication dot1x	aaa authentication dot1x default METHOD1 [METHOD2...] no aaa authentication dot1x default
aaa authentication web-auth	aaa authentication web-auth ID default METHOD1 [METHOD2...] no aaa authentication web-auth ID default

コマンド	コマンドとパラメーター
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、アカウントティング(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トティングのための 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
コマンドモード	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、アカウント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、

aaa new-model	
	<b>username</b> 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、 <b>enable password</b> 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 <b>username</b> 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 サーバーを作成し、IP アドレスと共有鍵を設定します。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	<b>radius-server host</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> } [ <b>auth-port</b> <i>PORT-NUMBER</i> ] [ <b>acct-port</b> <i>PORT-NUMBER</i> ] [ <b>timeout</b> <i>SECONDS</i> ] [ <b>retransmit</b> <i>COUNT</i> ] <b>key</b> [0   7] <i>KEY-STRING</i> <b>no radius-server host</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> }
パラメーター	<i>IP-ADDRESS</i> : RADIUS サーバーの IP アドレスを指定します。 <i>IPV6-ADDRESS</i> : RADIUS サーバーの IPv6 アドレスを指定します。 <b>auth-port</b> <i>PORT-NUMBER</i> (省略可能) : 認証パケットを送信する宛先 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。 <b>acct-port</b> <i>PORT-NUMBER</i> (省略可能) : アカウントティングパケットを送信する宛先 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。 <b>timeout</b> <i>SECONDS</i> (省略可能) : サーバーの応答を待つ時間 (タイムアウト) 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。 <b>retransmit</b> <i>COUNT</i> (省略可能) : サーバーから応答がない場合に、サーバーへリクエストを再送する回数を 0~20 の範囲で指定します。リクエストを再送しない場合は 0 を指定します。デフォルト設定は 2 です。 <b>key</b> : サーバーとの通信に使用する共有鍵を指定します。 0 (省略可能) : 共有鍵を平文で入力する場合に指定します。0 および 7 を省略した場合は平文で入力します。 7 (省略可能) : 共有鍵を暗号化した形式で入力する場合に指定します。0 および 7 を省略した場合は平文で入力します。 <i>KEY-STRING</i> : サーバーとの通信に使用するキーを入力します。平文で入力する場合は、文字列を最大 32 文字で指定します。文字列には、表示可能な ASCII 文字を使用できます。ただし、?は使用できません。
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

radius-server host	
特権レベル	レベル : 15
ガイドライン	作成した RADIUS サーバーは、デフォルトの RADIUS サーバークラスタ「radius」に登録されます。また、 <code>aaa group server radius</code> コマンドで作成した任意の RADIUS サーバークラスタに <code>server</code> コマンドで登録することもできます。  <code>radius-server host</code> コマンドと <code>tacacs-server host</code> コマンドで合わせて最大 16 個のサーバーを設定できます。
制限事項	<code>radius-server host</code> コマンドの設定順序を変更する場合には、すべての <code>radius-server host</code> 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。  MAC 認証において、本コマンドの <code>timeout</code> と <code>retransmit</code> 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。
注意事項	本コマンドを実行するには、事前に <code>aaa new-model</code> 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：異なる IP アドレスで 2 つの RADIUS サーバーを作成する方法を示します。

```
# configure terminal
(config)# radius-server host 172.19.10.100 auth-port 1500 acct-port 1501 timeout 8
retransmit 3 key ABCDE
(config)# radius-server host 172.19.10.101 auth-port 1600 acct-port 1601 timeout 3
retransmit 1 key ABCDE
(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、 <code>no</code> 形式のコマンドを使用します。
シンタックス	<code>radius-server deadtime MINUTES</code> <code>no radius-server deadtime</code>
パラメーター	<i>MINUTES</i> : 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	-



radius-server deadline	
注意事項	本コマンドを実行するには、事前に <b>aaa new-model</b> 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 deadline 10
(config)#
```

#### 9.2.4 tacacs-server host

tacacs-server host	
目的	TACACS+サーバーを作成し、IP アドレスと共有鍵を設定します。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	<b>tacacs-server host</b> <i>IP-ADDRESS</i> [ <b>port</b> <i>PORT</i> ] [ <b>timeout</b> <i>SECONDS</i> ] <b>key</b> [ <b>0</b>   <b>7</b> ] <i>KEY-STRING</i> <b>no tacacs-server host</b> <i>IP-ADDRESS</i>
パラメーター	<i>IP-ADDRESS</i> : TACACS+サーバーの IP アドレスを指定します。 <b>port</b> <i>PORT</i> (省略可能) : 認証パケットを送信する宛先 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。 <b>timeout</b> <i>SECONDS</i> (省略可能) : サーバーの応答を待つ時間 (タイムアウト) 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。 <b>key</b> : サーバーとの通信に使用する共有鍵を指定します。 <b>0</b> (省略可能) : 共有鍵を平文で入力する場合に指定します。共有鍵の形式のデフォルト設定です。 <b>7</b> (省略可能) : 共有鍵を暗号化した形式で入力する場合に指定します。 <b>key</b> <i>KEY-STRING</i> : 選択した形式で、サーバーとの通信に使用するキーを入力します。平文で入力する場合は、文字列を最大 254 文字で指定します。文字列には、表示可能な ASCII 文字を使用できます。ただし、?は使用できません。暗号化した形式で入力する場合は、文字列を最大 344 文字で指定します。暗号化した形式で入力する場合は、大文字と小文字が区別されます。
デフォルト	TACACS+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	作成した 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、 <b>aaa group server tacacs</b> コマンドで作成した任意の TACACS+サーバーグループに <b>server</b> コマンドで登録することもできます。 <b>radius-server host</b> コマンドと <b>tacacs-server host</b> コマンドで合わせて最大 16 個のサーバーを設定できます。
制限事項	-
注意事項	本コマンドを実行するには、事前に <b>aaa new-model</b> 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：異なる IP アドレスで 2 つの TACACS+サーバーを作成する方法を示します。

```
# 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)#
```

### 9.2.5 ip radius source-interface

ip radius source-interface	
目的	RADIUS パケットの送信元 IP 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	<b>ip radius source-interface</b> <i>INTERFACE-ID</i> <b>no ip radius source-interface</b>
パラメーター	<i>INTERFACE-ID</i> : RADIUS パケットの送信元 IP 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。 <ul style="list-style-type: none"> <li>• <b>vlan</b> : VLAN インターフェースを指定します。</li> </ul>
デフォルト	RADIUS サーバーに最も近い 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 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、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 <b>aaa new-model</b> 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 パケットの送信元 IP アドレスに VLAN 100 インターフェースの IP 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 IP 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	<b>ip tacacs source-interface</b> <i>INTERFACE-ID</i> <b>no ip tacacs source-interface</b>
パラメーター	<i>INTERFACE-ID</i> : TACACS パケットの送信元 IP 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。 <ul style="list-style-type: none"> <li>• <b>vlan</b> : VLAN インターフェースを指定します。</li> </ul>
デフォルト	TACACS サーバーに最も近い 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 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サーバーグループ設定モードの両方で送信元イン

ip tacacs source-interface	
	ターフェースを指定した場合、サーバ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 <b>aaa new-model</b> 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 パケットの送信元 IP アドレスに VLAN 100 インターフェースの IP 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	<b>ipv6 radius source-interface</b> <i>INTERFACE-ID</i> <b>no ipv6 radius source-interface</b>
パラメーター	<i>INTERFACE-ID</i> ：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、以下のパラメーターで指定します。 <ul style="list-style-type: none"> <li>• <b>vlan</b>：VLAN インターフェースを指定します。</li> </ul>
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 サーバ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サーバ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、サーバ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 <b>aaa new-model</b> 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 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 サーバグループを設定します。また、RADIUS のサーバ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	<b>aaa group server radius</b> <i>GROUP-NAME</i>

aaa group server radius	
	<b>no aaa group server radius</b> <i>GROUP-NAME</i>
パラメーター	<i>GROUP-NAME</i> : サーバークラス名を最大 32 文字で指定します。
デフォルト	RADIUS サーバークラスの設定なし
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	<p><b>aaa authentication</b> コマンドの認証方式リスト、または <b>aaa accounting</b> コマンドのアカウントティング方式リストで使用する RADIUS サーバークラスを作成します。サーバークラスは <b>aaa group server radius</b> コマンドと <b>aaa group server tacacs+</b> 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クラス「radius」「tacacs+」も含まれます。</p> <p>「radius」というグループ名はデフォルトの RADIUS サーバークラスとして予約されています。「radius」サーバークラスは、<b>radius-server host</b> コマンドで作成したすべての RADIUS サーバークラスを対象として、設定した順に処理されます。</p> <p>本コマンドで作成した RADIUS サーバークラスには、<b>server</b> コマンドを使用して RADIUS サーバークラスを登録できます。1 つの RADIUS サーバークラスには最大 16 個の RADIUS サーバークラスを登録でき、設定した順に処理されます。</p> <p>複数の RADIUS サーバークラスが対象になる場合には、先頭の RADIUS サーバークラス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 RADIUS サーバークラスで処理が実施されます。</p> <p><b>aaa authentication</b> 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 サーバークラス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 サーバークラスが存在してもそのサーバークラスで認証は実施されません。ただし、<b>aaa authentication control sufficient</b> 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 サーバークラスで認証が実施されます。</p>
制限事項	-
注意事項	本コマンドを実行するには、事前に <b>aaa new-model</b> 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 サーバークラスの作成方法、および作成した RADIUS サーバークラスに RADIUS サーバークラス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 サーバークラスに RADIUS サーバークラス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	<b>server</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> } <b>no server</b> { <i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i> }
パラメーター	<i>IP-ADDRESS</i> : RADIUS サーバークラスに登録する RADIUS サーバークラスの IP アドレス

server (RADIUS)	
	<p>スを指定します。</p> <p><i>IPV6-ADDRESS</i> : RADIUS サーバークラスに登録する RADIUS サーバークラスの IPv6 アドレスを指定します。</p>
デフォルト	RADIUS サーバークラスに登録なし
コマンドモード	RADIUS サーバークラス設定モード
特権レベル	レベル : 15
ガイドライン	<p><b>aaa group server radius</b> コマンドで RADIUS サーバークラス設定モードに遷移し、<b>server</b> コマンドで RADIUS サーバークラスに登録します。RADIUS サーバークラスは、<b>aaa authentication</b> コマンドの認証方式リスト、または <b>aaa accounting</b> コマンドのアカウントティング方式リストで使用するサーバークラスとして指定できます。</p> <p>RADIUS サーバークラスに登録した RADIUS サーバークラスは、登録した順に処理されます。</p> <p>1 つの RADIUS サーバークラスには、最大 16 個の RADIUS サーバークラスを登録できます。</p>
制限事項	事前に <b>radius-server host</b> コマンドで RADIUS サーバークラスを作成してください。RADIUS サーバークラスは 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 サーバークラスを作成し、RADIUS サーバークラス「group1」に登録する方法を説明します。

<pre># 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)#</pre>
--

### 9.2.10 aaa group server tacacs+

aaa group server tacacs+	
目的	TACACS+サーバークラスを設定します。また、TACACS+のサーバー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-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	<pre>aaa group server tacacs+ GROUP-NAME no aaa group server tacacs+ GROUP-NAME</pre>
パラメーター	<i>GROUP-NAME</i> : サーバークラス名を最大 32 文字で指定します。
デフォルト	TACACS+サーバークラスの設定なし
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	<p><b>aaa authentication</b> コマンドの認証方式リスト、または <b>aaa accounting</b> コマンドのアカウントティング方式リストで使用する TACACS+サーバークラスを作成します。サーバークラスは <b>aaa group server radius</b> コマンドと <b>aaa group server tacacs+</b> 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</p>

aaa group server tacacs+	
	<p>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。</p> <p>「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、<b>tacacs-server host</b> 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。</p> <p>本コマンドで作成した TACACS+サーバーグループには、<b>server</b> 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。</p> <p>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。</p> <p><b>aaa authentication</b> 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、<b>aaa authentication control sufficient</b> 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。</p>
制限事項	-
注意事項	本コマンドを実行するには、事前に <b>aaa new-model</b> 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	<b>server</b> <i>IP-ADDRESS</i> <b>no server</b> <i>IP-ADDRESS</i>
パラメーター	<i>IP-ADDRESS</i> : TACACS+サーバーグループに登録する TACACS+サーバーの IP 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	<b>aaa group server tacacs+</b> コマンドで TACACS+サーバーグループ設定モードに遷移し、 <b>server</b> 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、 <b>aaa authentication</b> コマンドの認証方式リスト、または <b>aaa accounting</b> コマンドのアカウントティング方式リストで使用す

server (TACACS+)	
	<p>るサーバーグループとして指定できます。</p> <p>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。</p> <p>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。</p>
制限事項	事前に <b>tacacs-server host</b> 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	<b>aaa authentication login</b> {default   <i>LIST-NAME</i> } <i>METHOD1</i> [ <i>METHOD2...</i> ] <b>no aaa authentication login</b> {default   <i>LIST-NAME</i> }
パラメーター	<p><b>default</b> : 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。</p> <p><i>LIST-NAME</i> : 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。</p> <p><i>METHOD1</i> [<i>METHOD2...</i>] : 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。</p> <ul style="list-style-type: none"> <li>• <b>local</b> : <b>username</b> 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。</li> <li>• <b>group radius</b> : <b>radius-server host</b> 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。</li> <li>• <b>group tacacs+</b> : <b>tacacs-server host</b> 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。</li> <li>• <b>group GROUP-NAME</b> : <b>aaa group server</b> 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。</li> <li>• <b>none</b> : 認証なしで許可する場合に指定します。</li> </ul>
デフォルト	local
コマンドモード	グローバル設定モード

aaa authentication login	
特権レベル	レベル : 15
ガイドライン	<p>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 <b>login authentication</b> コマンドの設定も必要です。</p> <p>本コマンドで認証方式リストを設定しない場合は、<b>username</b> 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。</p> <p><b>none</b> 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。</p> <p>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。</p> <p>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、<b>aaa authentication control sufficient login</b> 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。</p> <p><b>aaa authentication control sufficient login</b> 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(<b>none</b>)では認証が許可されません。</p> <p>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。</p>
制限事項	-
注意事項	本コマンドを実行するには、事前に <b>aaa new-model</b> 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	<b>login authentication {default   METHOD-LIST}</b> <b>no login authentication</b>
パラメーター	<b>default</b> : 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。 <b>METHOD-LIST</b> : 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 <b>aaa authentication login</b> コマンドで認証方式リストを作成します。



login authentication	
	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 <b>aaa new-model</b> 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	<b>enable</b> 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、 <b>no</b> 形式のコマンドを使用します。
シンタックス	<b>aaa authentication enable default METHOD1 [METHOD2...]</b> <b>no aaa authentication enable default</b>
パラメーター	<i>METHOD1 [METHOD2...]</i> : 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。 <ul style="list-style-type: none"> <li>• <b>enable</b> : <b>enable password</b> 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。</li> <li>• <b>group radius</b> : <b>radius-server host</b> 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 サーバークラウド「radius」を指定します。</li> <li>• <b>group tacacs+</b> : <b>tacacs-server host</b> 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+サーバークラウド「tacacs+」を指定します。</li> <li>• <b>group GROUP-NAME</b> : <b>aaa group server</b> コマンドで設定したサーバークラウドを使用する場合に指定します。</li> <li>• <b>none</b> : 認証なしで許可する場合に指定します。</li> </ul>
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 <b>enable [PRIVILEGE-LEVEL]</b> コマンドを実施した際に、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、 <b>enable password</b> コマンドで設定したパスワードで認証されます。  <b>none</b> 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

aaa authentication enable	
	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
制限事項	-
注意事項	本コマンドを実行するには、事前に <b>aaa new-model</b> 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	<b>aaa authentication mac-auth default METHOD1 [METHOD2...]</b> <b>no aaa authentication mac-auth default</b>
パラメーター	<p><b>METHOD1 [METHOD2...]</b>：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。</p> <ul style="list-style-type: none"> <li>• <b>local</b>：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。</li> <li>• <b>group radius : radius-server host</b> 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。</li> <li>• <b>group GROUP-NAME : aaa group server</b> 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。</li> <li>• <b>force [vlan VLAN-ID]</b>：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。</li> </ul>
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	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。

aaa authentication mac-auth															
	<p>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、<b>aaa authentication control sufficient mac</b> 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。</p> <p><b>aaa authentication control sufficient mac</b> 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 (<b>force</b>) では認証が許可されません。</p> <p>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。</p> <p>MAC 認証でサポートしている RADIUS 属性は以下です。</p> <table border="1" style="width: 100%;"> <thead> <tr> <th>属性</th> <th>属性値</th> </tr> </thead> <tbody> <tr> <td>User-Name</td> <td>認証されるユーザー名</td> </tr> <tr> <td>User-Password</td> <td>パスワード</td> </tr> <tr> <td>NAS-IP-Address</td> <td>認証要求している RADIUS クライアントの IP アドレス (IPv4 のみ)</td> </tr> <tr> <td>Calling-Station-Id</td> <td>認証端末の MAC アドレス</td> </tr> <tr> <td>NAS-Identifier</td> <td>認証された端末が属している VLAN ID</td> </tr> <tr> <td>NAS-Port</td> <td>認証端末が接続されているインターフェース番号</td> </tr> </tbody> </table>	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
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														
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	<p>本コマンドを実行するには、事前に <b>aaa new-model</b> コマンドで AAA を有効化する必要があります。</p> <p>ローカルデータベース認証 (<b>local</b>) よりも後に強制認証 (<b>force</b>) 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 (<b>force</b>) では認証されません。</p>														
対象バージョン	1.02.01														

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	<pre>aaa authentication dot1x default METHOD1 [METHOD2...] no aaa authentication dot1x default</pre>
パラメーター	<p><i>METHOD1 [METHOD2...]</i> : 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。</p> <ul style="list-style-type: none"> <li><b>local</b> : AccessDefender のローカルデータベースで認証する場合に指定</li> </ul>

aaa authentication dot1x																													
	<p>します。</p> <ul style="list-style-type: none"> <li>• <b>group radius : radius-server host</b> 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 サーバークラウド「radius」を指定します。</li> <li>• <b>group GROUP-NAME : aaa group server</b> コマンドで設定したサーバークラウドを使用する場合に指定します。</li> <li>• <b>force [vlan VLAN-ID]</b> : 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。</li> </ul>																												
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	<p>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。</p> <p>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。</p> <p>認証方式として指定したサーバークラウドが存在しない場合は、そのサーバークラウドは処理対象から外されます。</p> <p>IEEE 802.1X 認証でサポートしている RADIUS 属性は以下です。</p> <table border="1" style="width: 100%;"> <thead> <tr> <th>属性</th> <th>属性値</th> </tr> </thead> <tbody> <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>サブ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>サブ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>サブリカントの 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 サーバークラウド間の 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> </tbody> </table>	属性	属性値	User-Name	認証されるユーザー名	NAS-IP-Address	認証要求しているオーセンティケーターの IP アドレス (IPv4 のみ)	Framed-MTU	サブリカントとオーセンティケーター間の最大フレームサイズ (1466 固定)	NAS-Port	サブリカントが接続されているオーセンティケーターのインターフェース番号	NAS-Port-Type	ユーザー認証に使用しているインターフェースのタイプ (Ethernet (15) 固定)	Service-Type	提供するサービスタイプ (Framed (2) 固定)	Calling-Station-Id	サブリカントの MAC アドレス	EAP-Message	EAP メッセージの送受信に使用	Message-Authenticator	RADIUS パケットの内容を保証するために使用	State	オーセンティケーターと RADIUS サーバークラウド間の State 情報の保持	Tunnel-Type	動的 VLAN 割り当て用応答属性 (VLAN (13) に設定)	Tunnel-Medium-Type	動的 VLAN 割り当て用応答属性 (IEEE 802 (6) に設定)	Tunnel-Private-Group-Id	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)
属性	属性値																												
User-Name	認証されるユーザー名																												
NAS-IP-Address	認証要求しているオーセンティケーターの IP アドレス (IPv4 のみ)																												
Framed-MTU	サブリカントとオーセンティケーター間の最大フレームサイズ (1466 固定)																												
NAS-Port	サブリカントが接続されているオーセンティケーターのインターフェース番号																												
NAS-Port-Type	ユーザー認証に使用しているインターフェースのタイプ (Ethernet (15) 固定)																												
Service-Type	提供するサービスタイプ (Framed (2) 固定)																												
Calling-Station-Id	サブリカントの MAC アドレス																												
EAP-Message	EAP メッセージの送受信に使用																												
Message-Authenticator	RADIUS パケットの内容を保証するために使用																												
State	オーセンティケーターと RADIUS サーバークラウド間の State 情報の保持																												
Tunnel-Type	動的 VLAN 割り当て用応答属性 (VLAN (13) に設定)																												
Tunnel-Medium-Type	動的 VLAN 割り当て用応答属性 (IEEE 802 (6) に設定)																												
Tunnel-Private-Group-Id	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)																												
制限事項	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。																												

aaa authentication dot1x	
	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 <b>aaa new-model</b> 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	1.02.01

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	<b>aaa authentication web-auth ID default METHOD1 [METHOD2...]</b> <b>no aaa authentication web-auth ID default</b>
パラメーター	<p><i>ID</i> : 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、<i>ID</i> に 1 を指定します。</p> <p><i>METHOD1 [METHOD2...]</i> : 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。</p> <ul style="list-style-type: none"> <li>• <b>local</b> : 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。</li> <li>• <b>group radius : radius-server host</b> 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。</li> <li>• <b>group GROUP-NAME : aaa group server</b> 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。</li> <li>• <b>force [vlan VLAN-ID]</b> : 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。</li> </ul>
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	<p>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。</p> <p>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、<b>aaa authentication control sufficient web</b> 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。</p> <p><b>aaa authentication control sufficient web</b> 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</p>

aaa authentication web-auth															
	<p>は、強制認証 (<b>force</b>) では認証が許可されません。</p> <p>認証方式として指定したサーバグループが存在しない場合は、そのサーバグループは処理対象から外されます。</p> <p>Web 認証でサポートしている RADIUS 属性は以下です。</p> <table border="1"> <thead> <tr> <th>属性</th> <th>属性値</th> </tr> </thead> <tbody> <tr> <td>User-Name</td> <td>認証されるユーザー名</td> </tr> <tr> <td>User-Password</td> <td>パスワード</td> </tr> <tr> <td>NAS-IP-Address</td> <td>認証要求している RADIUS クライアントの IP アドレス (IPv4 のみ)</td> </tr> <tr> <td>Calling-Station-Id</td> <td>認証端末の MAC アドレス</td> </tr> <tr> <td>NAS-Identifier</td> <td>認証された端末が属している VLAN ID</td> </tr> <tr> <td>NAS-Port</td> <td>認証端末が接続されているインターフェース番号</td> </tr> </tbody> </table>	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
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														
制限事項	認証方式として、TACACS+サーバグループは指定できません。														
注意事項	<p>本コマンドを実行するには、事前に <b>aaa new-model</b> コマンドで AAA を有効化する必要があります。</p> <p>ローカルデータベース認証 (<b>local</b>) よりも後に強制認証 (<b>force</b>) 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 (<b>force</b>) では認証されません。</p>														
対象バージョン	1.02.01														

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	<pre>aaa authentication control sufficient {web ID   mac   login} no aaa authentication control sufficient {web ID   mac   login}</pre>
パラメーター	<p><b>web ID</b>：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。</p> <p><b>mac</b>：MAC 認証で本機能を使用する場合に指定します。</p> <p><b>login</b>：ログイン認証で本機能を使用する場合に指定します。</p>
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。

aaa authentication control sufficient	
	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 ( <b>force</b> ) または認証なし ( <b>none</b> ) 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 <b>aaa new-model</b> 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	<b>aaa default class CLASS-ID</b> <b>no aaa default class</b>
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 <b>aaa new-model</b> 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	1.02.01

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トティングで使用するアカウント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	<b>aaa accounting system default {none   start-stop METHOD1 [METHOD2...]}</b> <b>no aaa accounting system default</b>
パラメーター	<b>none</b> ：アカウントティングを実行しない場合に指定します。

aaa accounting system	
	<p><b>start-stop</b> : アカウントティングを有効にする場合に指定します。</p> <p><i>METHOD1</i> [<i>METHOD2...</i>] : ここで指定した順序でアカウント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。アカウント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。アカウントティング方式には、以下のパラメーターを指定できます。</p> <ul style="list-style-type: none"> <li>• <b>group radius</b> : <b>radius-server host</b> 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 サーバークラウド「radius」を指定します。</li> <li>• <b>group tacacs+</b> : <b>tacacs-server host</b> 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+サーバークラウド「tacacs+」を指定します。</li> <li>• <b>group GROUP-NAME</b> : <b>aaa group server</b> コマンドで設定したサーバークラウドを使用する場合に指定します。</li> </ul>
デフォルト	アカウント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	<p>本コマンドはシステムイベントのアカウント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トティングメッセージを送信します。</p> <p>アカウントティング方式として指定したサーバークラウドが存在しない場合は、そのサーバークラウドは処理対象から外されます。</p>
制限事項	-
注意事項	<p>本コマンドを実行するには、事前に <b>aaa new-model</b> コマンドで AAA を有効化する必要があります。</p> <p>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トティングメッセージを送信できないことがあります。</p>
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トティングを有効にする方法を示します。アカウントティング方式として RADIUS サーバークラウド「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 のアカウントティングで使用するアカウント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	<b>aaa accounting network default {none   start-stop METHOD1 [METHOD2...]}</b> <b>no aaa accounting network default</b>
パラメーター	<p><b>none</b> : アカウントティングを実行しない場合に指定します。</p> <p><b>start-stop</b> : 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トティングメッセージを送信する場合に指定します。</p> <p><i>METHOD1</i> [<i>METHOD2...</i>] : ここで指定した順序でアカウント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。アカウントティング方式は少なくとも 1 つは</p>



aaa accounting network	
	<p>指定する必要がある、最大で 4 つまで指定できます。アカウントティング方式には、以下のパラメーターを指定できます。</p> <ul style="list-style-type: none"> <li>• <b>group radius : radius-server host</b> 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 サーバークラウド「radius」を指定します。</li> <li>• <b>group tacacs+ : tacacs-server host</b> 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+サーバークラウド「tacacs+」を指定します。</li> <li>• <b>group GROUP-NAME : aaa group server</b> コマンドで設定したサーバークラウドを使用する場合に指定します。</li> </ul>
デフォルト	アカウント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	<p>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トティングを有効にするために使用します。</p> <p>アカウントティング方式として指定したサーバークラウドが存在しない場合は、そのサーバークラウドは処理対象から外されます。</p>
制限事項	-
注意事項	本コマンドを実行するには、事前に <b>aaa new-model</b> 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	1.02.01

使用例 : AccessDefender のアカウント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、アカウントティング方式として RADIUS サーバークラウド「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トティングで使用するアカウント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	<pre>aaa accounting commands LEVEL {default   LIST-NAME} {none   start-stop METHOD1 [METHOD2...]} no aaa accounting commands LEVEL {default   LIST-NAME}</pre>
パラメーター	<p><b>LEVEL</b> : 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トティングが設定されます。</p> <p><b>default</b> : デフォルトのアカウントティング方式リストを使用する場合に指定します。</p> <p><b>LIST-NAME</b> : デフォルト以外のアカウント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。</p> <p><b>none</b> : アカウントティングを実行しない場合に指定します。</p> <p><b>start-stop</b> : アカウントティングを有効にする場合に指定します。</p>

aaa accounting commands	
	<p><i>METHOD1</i> [<i>METHOD2...</i>] : ここで指定した順序でアカウント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。アカウント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。アカウントティング方式には、以下のパラメーターを指定できます。</p> <ul style="list-style-type: none"> <li>• <b>group tacacs+</b> : <b>tacacs-server host</b> 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。</li> <li>• <b>group GROUP-NAME</b> : <b>aaa group server tacacs+</b> 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。</li> </ul>
デフォルト	アカウント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	<p>指定した特権レベルのコマンド実行時にアカウント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 <b>accounting commands</b> コマンドの設定も必要です。</p> <p>アカウント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。</p>
制限事項	-
注意事項	本コマンドを実行するには、事前に <b>aaa new-model</b> 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ト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。アカウント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トティングに使用するアカウント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	<b>accounting commands</b> <i>LEVEL</i> { <b>default</b>   <i>METHOD-LIST</i> } <b>no accounting commands</b> <i>LEVEL</i>
パラメーター	<p><i>LEVEL</i> : 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トティングが設定されます。</p> <p><b>default</b> : デフォルトのアカウントティング方式リストを使用する場合に指定します。</p> <p><i>METHOD-LIST</i> : 使用するアカウントティング方式リストの名前を指定します。</p>
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 <b>aaa accounting commands</b> コマンドでアカウントティング方式リストを作成します。アカウント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トティング方式リストを指定できます。

accounting commands	
制限事項	1 つの特権レベルに指定できるアカウント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 <b>aaa new-model</b> 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、アカウント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ト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トティングで使用するアカウント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	<b>aaa accounting exec</b> {default   <i>LIST-NAME</i> } {none   start-stop <i>METHOD1</i> [ <i>METHOD2...</i> ]} <b>no aaa accounting exec</b> {default   <i>LIST-NAME</i> }
パラメーター	<b>default</b> : デフォルトのアカウントティング方式リストを使用する場合に指定します。  <i>LIST-NAME</i> : デフォルト以外のアカウント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。  <b>none</b> : アカウントティングを実行しない場合に指定します。  <b>start-stop</b> : アカウントティングを有効にする場合に指定します。  <i>METHOD1</i> [ <i>METHOD2...</i> ] : ここで指定した順序でアカウント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。アカウントティング方式は少なくとも 1 つは指定する必要があります。最大で 4 つまで指定できます。アカウントティング方式には、以下のパラメーターを指定できます。 <ul style="list-style-type: none"> <li>• <b>group radius : radius-server host</b> 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 サーバークラスタ「radius」を指定します。</li> <li>• <b>group tacacs+ : tacacs-server host</b> 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+サーバークラスタ「tacacs+」を指定します。</li> <li>• <b>group <i>GROUP-NAME</i> : aaa group server</b> コマンドで設定したサーバークラスタを使用する場合に指定します。</li> </ul>
デフォルト	アカウント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ト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ト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 <b>accounting exec</b> コマンドの設定も必要です。

aaa accounting exec	
	アカウント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 <b>aaa new-model</b> 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ト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。アカウント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トティングに使用するアカウント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	<b>accounting exec {default   METHOD-LIST}</b> <b>no accounting exec</b>
パラメーター	<b>default</b> : デフォルトのアカウントティング方式リストを使用する場合に指定します。  <b>METHOD-LIST</b> : 使用するアカウント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 <b>aaa accounting commands</b> コマンドでアカウントティング方式リストを作成します。アカウント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 <b>aaa new-model</b> 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、アカウント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ト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	<b>show aaa</b>

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	<b>show radius statistics</b>
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トティング用の 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)	アカウント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)	アカウントティングポートで受信したサーバーからの RADIUS パケットの数を表示します。
(14)	RADIUS サーバーに再送された RADIUS 要求パケットの数を表示します。再送には、識別子と Acct-Delay が更新されたリトライ状態が同じままのリトライが含まれます。
(15)	サーバーから受信した誤った形式の RADIUS 応答パケットの数を表示します。長さが無効なパケットも数に含まれます。なお、誤った Authenticator、署名属性、または不明なタイプは、誤った形式の応答の数には含まれません。
(16)	サーバーから受信した無効な Authenticator または署名属性を含んだ RADIUS 応答パケットの数を表示します。
(17)	サーバー宛てでタイムアウト前または応答未受信の RADIUS 要求パケットの数を表示します。要求の送信によって増えます。また、要求の受信、タイムアウト、または再送によって減少します。
(18)	サーバーのタイムアウト回数を表示します。タイムアウト後のクライアントに想定される動作は、同じサーバーへのリトライ、別のサーバーへの送信、または断念のいずれかです。同じサーバーへのリトライは、再送とタイムアウトとしてカウントします。別のサーバーへの送信は、要求とタイムアウトとしてカウントします。
(19)	サーバーから受信したタイプ不明の RADIUS パケットの数を表示します。
(20)	サーバーから受信し、何らかの理由で廃棄された RADIUS パケットの数を表示します。

### 9.2.28 show tacacs statistics

show tacacs statistics	
目的	TACACS+サーバーの状態を表示します。
シンタックス	<b>show tacacs statistics</b>
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

show tacacs statistics	
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えが発生した場合、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タはカウンタアップします。
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	認証とアカウントティング (AAA) サーバーの統計情報をクリアします。
シンタックス	<code>clear aaa counters servers {all   radius {IP-ADDRESS   IPV6-ADDRESS   all}   tacacs {IP-ADDRESS   all}   sg NAME}</code>
パラメーター	<p><b>all</b> : すべてのサーバーの統計情報をクリアする場合に指定します。</p> <p><b>radius IP-ADDRESS</b> : 統計情報をクリアする RADIUS サーバーの IPv4 アドレスを指定します。</p> <p><b>radius IPV6-ADDRESS</b> : 統計情報をクリアする RADIUS サーバーの IPv6 アドレスを指定します。</p> <p><b>radius all</b> : すべての RADIUS サーバーの統計情報をクリアする場合に指定します。</p> <p><b>tacacs IP-ADDRESS</b> : 統計情報をクリアする TACACS+サーバーの IPv4 アドレスを指定します。</p> <p><b>tacacs all</b> : すべての TACACS+サーバーの統計情報をクリアする場合に指定します。</p> <p><b>sg NAME</b> : サーバークラス内のすべてのサーバーの統計情報をクリアする場合に指定します。サーバークラス名を指定してください。</p>

clear aaa counters servers	
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 : AAA サーバーのカウンターをクリアする方法を示します。

```
# clear aaa counters servers all
#
```

使用例 : サーバグループ「server-farm」内のすべてのホストに関する AAA サーバーのカウンター情報をクリア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	<b>mac-authentication enable</b> <b>no mac-authentication enable</b>
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	<p>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。</p> <p>MAC 認証を有効にする前に、<b>total-client</b> 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。</p> <p>アクセスリスト機能の <b>permit</b> コマンドの <b>authentication-bypass</b> 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）。</p> <p>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。</p> <p>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。</p> <p>Discard 端末を手動で削除する場合は、<b>access-defender logout</b> 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</p>

mac-authentication enable	
	除します。
制限事項	-
注意事項	<p>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。</p> <p>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が重複して、ログインに失敗する可能性があります。</p> <p>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。</p>
対象バージョン	1.02.01

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	<b>mac-authentication discard-time SECONDS</b> <b>no mac-authentication discard-time</b>
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	1.02.01

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	<b>mac-authentication ignore-dhcp</b> <b>no mac-authentication ignore-dhcp</b>

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	1.02.01

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	<b>mac-authentication password</b> [0   7] <i>PASSWORD</i> { <b>mac</b>   <b>web-mac</b>   <b>dot1x-mac</b>   <b>web-dot1x-mac</b> } <b>no mac-authentication password</b> { <b>mac</b>   <b>web-mac</b>   <b>dot1x-mac</b>   <b>web-dot1x-mac</b> }
パラメーター	[0   7] <i>PASSWORD</i> : MAC 認証で使用するパスワードを指定します。 <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li><i>PASSWORD</i> : 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。</li> </ul> <b>mac</b> : MAC 認証で使用する場合に指定します。 <b>web-mac</b> : Web/MAC 認証 (AND) で使用する場合に指定します。 <b>dot1x-mac</b> : IEEE 802.1X/MAC 認証 (AND) で使用する場合に指定します。 <b>web-dot1x-mac</b> : 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 <b>mac-authentication username mac-format</b> 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	1.02.01

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	<b>mac-authentication username mac-format case {lowercase   uppercase} delimiter {hyphen   colon   dot} number {1   2   5}   none}</b> <b>no mac-authentication username mac-format</b>
パラメーター	<b>case</b> ：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。 <ul style="list-style-type: none"> <li>• <b>lowercase</b>：小文字指定（例：aabbccddeeff）</li> <li>• <b>uppercase</b>：大文字指定（例：AABBCCDDEEFF）</li> </ul> <b>delimiter</b> ：区切り文字を指定します。 <ul style="list-style-type: none"> <li>• <b>hyphen</b>：ハイフン指定（例：aa-bb-cc-dd-ee-ff）</li> <li>• <b>colon</b>：コロン指定（例：aa:bb:cc:dd:ee:ff）</li> <li>• <b>dot</b>：ドット指定（例：aa.bb.cc.dd.ee.ff）</li> <li>• <b>none</b>：区切り文字を使用しない場合に指定（例：aabbccddeeff）</li> </ul> <b>number</b> ：区切り文字の数を指定します。 <ul style="list-style-type: none"> <li>• <b>1</b>：区切り文字 1 個指定（例：aabbcc-ddeeff）</li> <li>• <b>2</b>：区切り文字 2 個指定（例：aabb-ccdd-eeff）</li> <li>• <b>5</b>：区切り文字 5 個指定（例：aa-bb-cc-dd-ee-ff）</li> </ul>
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	1.02.01

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 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。

dot1x enable	
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、 <b>total-client</b> 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 <b>permit</b> コマンドの <b>authentication-bypass</b> 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	1.02.01

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 <i>INTERFACE-ID</i> [,  -] no dot1x ignore-eapol-start interface <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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、サブリカントから EAPOL-Start を受信しても、EAP-Request/EAP-Identity を応答せず、認証を抑止することができます。
制限事項	-

dot1x ignore-eapol-start interface	
注意事項	-
対象バージョン	1.02.01

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：ポートチャンネル 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	<b>dot1x mode mac-authentication-fail</b> <b>no dot1x mode mac-authentication-fail</b>
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	1.02.01

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	<b>dot1x reauthentication interface</b> <i>INTERFACE-ID</i> [,  -] <b>no dot1x reauthentication interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>INTERFACE-ID</i> ：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。

dot1x reauthentication interface	
	<ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	1.02.01

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：ポートチャンネル 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	<b>dot1x timeout quiet-period</b> <i>SECONDS</i> <b>interface</b> <i>INTERFACE-ID</i> [,  -] <b>no dot1x timeout quiet-period interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<b>SECONDS</b> : 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。 <b>interface</b> <i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	1.02.01

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	<b>dot1x timeout re-authperiod</b> <i>SECONDS</i> <b>interface</b> <i>INTERFACE-ID</i> [,  -] <b>no dot1x timeout re-authperiod interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>SECONDS</i> : 再認証の間隔を、5~2,147,483,647 秒の範囲で指定します。 <b>interface</b> <i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャネルを指定します。</li> </ul>
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	1.02.01

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、サブ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は、no 形式のコマンドを使用します。
シンタックス	<b>dot1x timeout supp-timeout</b> <i>SECONDS</i> <b>interface</b> <i>INTERFACE-ID</i> [,  -] <b>no dot1x timeout supp-timeout interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>SECONDS</i> : EAP-Request を再送信する間隔を、5~65,535 秒の範囲で指定します。

dot1x timeout supp-timeout	
	<b>interface</b> <i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b>: ポートチャンネルを指定します。</li> </ul>
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	1.02.01

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: ポートチャンネル 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 tx-period

dot1x timeout tx-period	
目的	EAP-Request/EAP-Identity をサブ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	<b>dot1x timeout tx-period</b> <i>SECONDS</i> <b>interface</b> <i>INTERFACE-ID</i> [,  -] <b>no dot1x timeout tx-period interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>SECONDS</i> : EAP-Request/EAP-Identity をサブ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 がサブリカントに送信されません。  <b>interface</b> <i>INTERFACE-ID</i> : EAP-Request/EAP-Identity をサブ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。 <ul style="list-style-type: none"> <li>• <b>port</b>: 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b>: ポートチャンネルを指定します。</li> </ul>
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	1.02.01

使用例：ポート 1/0/1 で EAP-Request/EAP-Identity をサブ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：ポートチャンネル 1 で EAP-Request/EAP-Identity をサブ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)#
```

### 9.4.9 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	<b>fwd-eapol enable</b> <b>no fwd-eapol enable</b>
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	1.02.01

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)#
```

### 9.4.10 show access-defender dot1x

show access-defender dot1x	
目的	登録されたサブリカントの情報を表示します。
シンタックス	<b>show access-defender dot1x</b>
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	-

show access-defender dot1x

対象バージョン | 1.02.01

使用例：登録されたサブ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-channell ... (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 ... (22)
  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)	情報を表示するサブリカントのインターフェース ID を表示します。
(3)	サブリカントのユーザー名を表示します。
(4)	サブリカントの MAC アドレスを表示します。
(5)	サブ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)	サブ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)	サブ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)	サブリカントの再認証状態設定の有効/無効を表示します。
(10)	サブリカントの再認証期間設定を表示します。
(11)	サブリカントの Port Access Entity (PAE) の現在のステータスを表示します。 <ul style="list-style-type: none"> <li>Down : Down 状態</li> <li>Initialize : 初期化中</li> <li>Disconnecting : 接続なし</li> <li>Connecting : 接続済み</li> <li>Authenticating : 認証中</li> <li>Aborting : 中断中</li> <li>Held : EAPoL-Fail 送信</li> </ul>
(12)	サブリカントの PAE のポートモードを表示します。

項番	説明
	常に「Auto」が表示されます。
(13)	サブリカントへの request-ID の再送信試行回数を表示します。
(14)	サブリカントの休止期間の設定を表示します。
(15)	サブ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)	サブ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。 <ul style="list-style-type: none"> <li>• Invalid : 無効</li> <li>• Request : リクエスト送信</li> <li>• Response : 応答受信</li> <li>• Success : 認証成功</li> <li>• Fail : 認証失敗</li> <li>• Timeout : 応答タイムアウト</li> <li>• Idle : 待機中</li> <li>• Initialize : 初期化</li> </ul>
(18)	サブ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)	非認証サブリカントの packets 廃棄方向の設定を表示します。 常に「In」が表示されます。
(21)	非認証サブリカントの使用可能な packets 廃棄方向を表示します。 常に「In」が表示されます。
(22)	ブリッジポートの検知を表示します。 常に「false」が表示されます。

### 9.4.11 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	<b>show access-defender dot1x interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	1.02.01

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)	インターフェース ID 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制する機能の有効/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 をサブ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、サブ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 をサブ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：ポートチャンネル 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-channell ... (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)	インターフェース ID 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制する機能の有効/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 をサブ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、サブ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 をサブ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。

項番	説明
(11)	再認証の間隔を表示します。

### 9.4.12 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	<b>show access-defender dot1x statistics</b> [ <b>interface</b> <i>INTERFACE-ID</i> [, [-]]
パラメーター	<b>interface</b> <i>INTERFACE-ID</i> (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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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は、すべてのインターフェースに関する情報が表示されます。
制限事項	-
注意事項	-
対象バージョン	1.02.01

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。

項番	説明
(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：ポートチャンネル 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-channell 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。

### 9.4.13 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	<b>dot1x initialize interface</b> <i>INTERFACE-ID</i> [, -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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



dot1x initialize interface	
	も構成情報には残りません。
対象バージョン	1.02.01

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：ポートチャンネル 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)#
```

#### 9.4.14 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	<b>dot1x re-authenticate interface</b> <i>INTERFACE-ID</i> [, -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	1.02.01

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：ポートチャンネル 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 genscr rsakey	ssl genscr 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	<b>show ssl https-certificate</b>
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	1.02.01

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	<code>show ssl https-private-key</code>
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	1.02.01

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)	秘密鍵情報を表示します。

### 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	<code>show ssl csr</code>
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	1.02.01

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	<b>ssl gencsr rsakey</b> [ <i>RSA-KEY-LENGTH</i> ]
パラメーター	RSA-KEY-LENGTH（省略可能）：RSA 鍵の長さを、512～2,048 の範囲で指定します。
デフォルト	RSA 鍵の長さは 2,048
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	以下の情報は省略できません。 <ul style="list-style-type: none"> <li>Common Name</li> </ul>
対象バージョン	1.02.01

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 no web-authentication http-ip ipv4
web-authentication http-port	web-authentication http-port TCP-PORT no web-authentication http-port
web-authentication https-port	web-authentication https-port TCP-PORT 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 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

### 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	<b>web-authentication enable</b> <b>no web-authentication enable</b>
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	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。 <ul style="list-style-type: none"> <li>• <b>total-client</b> コマンドで認証クライアントの最大数を設定する。</li> </ul>

web-authentication enable	
	<ul style="list-style-type: none"> <li>• <b>web-authentication http-ip</b> 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。</li> </ul> <p>アクセスリスト機能の <b>permit</b> コマンドの <b>authentication-bypass</b> 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）。</p> <p>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。</p> <p>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せん。</p>
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	1.02.01

使用例：Web 認証を有効にする方法を示します。

```
# configure terminal
(config)# web-authentication enable
(config)#
```

### 9.6.2 web-authentication http-ip

web-authentication http-ip	
目的	Web 認証用の Web サーバーの IPv4 アドレスを設定します。設定を削除する場合は、no 形式のコマンドを使用します。
シンタックス	<b>web-authentication http-ip ipv4 IP-ADDRESS</b> <b>no web-authentication http-ip ipv4</b>
パラメーター	<b>ipv4 IP-ADDRESS</b> : Web 認証用の Web サーバーの IPv4 アドレスを設定する場合に指定します。
デフォルト	なし
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	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	1.02.01

使用例：Web 認証用の Web サーバーの IPv4 アドレスを 3.3.3.3 に設定する方法を示します。

```
# configure terminal
```

```
(config)# access-defender
(config-a-def)# web-authentication http-ip ipv4 3.3.3.3
(config-a-def)#
```

### 9.6.3 web-authentication http-port

web-authentication http-port	
目的	Web 認証用の Web サーバーの、HTTP プロトコルの TCP ポート番号を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>web-authentication http-port</b> <i>TCP-PORT</i> <b>no web-authentication http-port</b>
パラメーター	<i>TCP-PORT</i> : Web 認証用の Web サーバーの、追加する HTTP プロトコルの TCP ポート番号を 1~65535 の範囲で指定します。
デフォルト	80
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。 <ul style="list-style-type: none"> <li>• 21 (FTP protocol)</li> <li>• 22 (SSH protocol)</li> <li>• 23 (Telnet protocol)</li> <li>• 443 (HTTPS protocol)</li> <li>• <b>ip telnet service-port</b> コマンドで指定したポート番号</li> <li>• <b>ip ssh service-port</b> コマンドで指定したポート番号</li> <li>• <b>web-authentication https-port</b> コマンドで指定したポート番号</li> <li>• <b>web-authentication snooping proxy-port</b> コマンドで指定したポート番号</li> <li>• <b>web-authentication redirect proxy-port</b> コマンドで指定したポート番号</li> </ul>
注意事項	-
対象バージョン	1.02.01

使用例 : Web 認証用の Web サーバーの、追加する HTTP プロトコルの TCP ポート番号を 8080 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication http-port 8080
(config-a-def)#
```

### 9.6.4 web-authentication https-port

web-authentication https-port	
目的	Web 認証用の Web サーバーの、HTTPS プロトコルの TCP ポート番号を設定します。デフォルト設定に戻すには、no 形式のコマンドを使用します。
シンタックス	<b>web-authentication https-port</b> <i>TCP-PORT</i> <b>no web-authentication https-port</b>



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。
デフォルト	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	<p>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。</p> <p>以下に示す TCP ポート番号は指定できません。</p> <ul style="list-style-type: none"> <li>• 21 (FTP protocol)</li> <li>• 22 (SSH protocol)</li> <li>• 23 (Telnet protocol)</li> <li>• 80 (HTTP protocol)</li> <li>• <code>ip telnet service-port</code> コマンドで指定したポート番号</li> <li>• <code>ip ssh service-port</code> コマンドで指定したポート番号</li> <li>• <code>web-authentication http-port</code> コマンドで指定したポート番号</li> <li>• <code>web-authentication snooping proxy-port</code> コマンドで指定したポート番号</li> <li>• <code>web-authentication redirect proxy-port</code> コマンドで指定したポート番号</li> </ul>
注意事項	-
対象バージョン	1.02.01

使用例: Web 認証用の Web サーバーの、追加する HTTPS プロトコルの TCP ポート番号を 8443 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication https-port 8443
(config-a-def)#
```

### 9.6.5 web-authentication redirect disable

web-authentication redirect disable	
目的	Web 認証のログイン認証ページのリダイレクト機能を無効にします。有効にする場合は、no 形式のコマンドを使用します。
シンタックス	<code>web-authentication redirect disable [http   https]</code> <code>no web-authentication redirect disable</code>
パラメーター	<p><b>http</b> (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。</p> <p><b>https</b> (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。</p> <p><b>http</b>、および <b>https</b> 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。</p>
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 ( <code>no web-authentication redirect disable</code> )

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	1.02.01

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	<b>web-authentication redirect url</b> <i>URL</i> <b>no web-authentication redirect url</b>
パラメーター	<i>URL</i> : 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、 <b>web-authentication redirect proxy-port</b> 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 アドレスは <b>web-authentication http-ip</b> 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 <b>web-authentication http-ip</b> 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。 <ul style="list-style-type: none"> <li>• <code>http://&lt;http-ip&gt;:&lt;http-port&gt;/www/AuthLogin.html</code></li> <li>• <code>https://&lt;http-ip&gt;:&lt;https-port&gt;/www/AuthLogin.html</code></li> </ul> 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 redirect url	
	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	1.02.01

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	<b>web-authentication http-session-timeout SECONDS</b> <b>no web-authentication http-session-timeout</b>
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	1.02.01

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 認証でログイン中の端末から、現在ログイン中のユーザー名と同じまたは異

web-authentication overwrite enable	
	なるユーザー名で認証成功した場合、後者のユーザー名で上書きしてログインでき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	<b>web-authentication overwrite enable</b> <b>no web-authentication overwrite enable</b>
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	1.02.01

使用例：Web 認証でログイン中の端末から、現在ログイン中のユーザー名と異なるユーザー名で認証成功した場合、後者のユーザー名で上書きしてログインできる機能を有効にする方法を示します。

```
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication 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	<b>web-authentication ttl VALUE interface INTERFACE-ID [, -]</b> <b>no web-authentication ttl [VALUE] [interface INTERFACE-ID [, -]]</b>
パラメーター	<b>VALUE</b> : 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。  <b>interface INTERFACE-ID</b> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	-
対象バージョン	1.02.01

使用例：ポート 1/0/1 で TTL フィルター機能の TTL 値を 255 に設定する方法を示します。

```
# configure terminal
(config)# access-defender
```

```
(config-a-def)# web-authentication ttl 255 interface port 1/0/1
(config-a-def)#
```

### 9.6.10 web-authentication redirect 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	<b>web-authentication redirect proxy-port</b> <i>PROXY-PORT</i> <b>no web-authentication redirect proxy-port</b>
パラメーター	<i>PROXY-PORT</i> : 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、 <b>web-authentication redirect url</b> 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、 <i>PROXY-PORT</i> に指定できません。 <ul style="list-style-type: none"> <li>• 21 (FTP protocol)</li> <li>• 22 (SSH protocol)</li> <li>• 23 (Telnet protocol)</li> <li>• 80 (HTTP protocol)</li> <li>• 443 (HTTPS protocol)</li> <li>• <b>ip telnet service-port</b> コマンドで指定したポート番号</li> <li>• <b>ip ssh service-port</b> コマンドで指定したポート番号</li> <li>• <b>web-authentication http-port</b> コマンドで指定したポート番号</li> <li>• <b>web-authentication https-port</b> コマンドで指定したポート番号</li> <li>• <b>web-authentication snooping proxy-port</b> コマンドで指定したポート番号</li> </ul>
注意事項	-
対象バージョン	1.02.01

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)#
```

### 9.6.11 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	<b>web-authentication snooping proxy-port</b> <i>PROXY-PORT</i> <b>no web-authentication snooping proxy-port</b>
パラメーター	<i>PROXY-PORT</i> : 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、 <i>PROXY-PORT</i> に指定できません。 <ul style="list-style-type: none"> <li>• 21 (FTP protocol)</li> <li>• 22 (SSH protocol)</li> <li>• 23 (Telnet protocol)</li> <li>• 80 (HTTP protocol)</li> <li>• 443 (HTTPS protocol)</li> <li>• <b>ip telnet service-port</b> コマンドで指定したポート番号</li> <li>• <b>ip ssh service-port</b> コマンドで指定したポート番号</li> <li>• <b>web-authentication http-port</b> コマンドで指定したポート番号</li> <li>• <b>web-authentication https-port</b> コマンドで指定したポート番号</li> <li>• <b>web-authentication redirect proxy-port</b> コマンドで指定したポート番号</li> </ul>
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)#
```

### 9.6.12 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。
シンタックス	<b>web-authentication logging web-access on</b> <b>no web-authentication logging web-access on</b>

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	1.02.01

使用例 : Web 認証用の Web サーバーのアクセスログを有効にする方法を示します。

```
# configure terminal
(config)# web-authentication logging web-access on
(config)#
```

## 9.7 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

### 9.7.1 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	<b>dhcp-snooping enable</b> <b>no dhcp-snooping enable</b>
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	<p>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。</p> <p>DHCP スヌーピングを有効にする前に、<b>total-client</b> 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。</p> <p>登録された DHCP スヌーピングエントリは、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</p>



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	1.02.01

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)#
```

### 9.7.2 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	<b>dhcp-snooping interface</b> <i>INTERFACE-ID</i> [,  -] <b>no dhcp-snooping interface</b> <i>INTERFACE-ID</i> [,  -]
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>port-channel</b> : ポートチャンネルを指定します。</li> </ul>
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	ポートチャン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	1.02.01

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：ポートチャンネル 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)#
```

### 9.7.3 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	1.02.01

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)#
```

#### 9.7.4 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 <i>SECONDS</i> no dhcp-snooping mode timer
パラメーター	<i>SECONDS</i> : 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	1.02.01

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)#
```

## 9.7.5 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	<b>dhcp-snooping mode mac-authentication</b> <b>no dhcp-snooping mode mac-authentication</b>
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	1.02.01

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)#
```

## 9.7.6 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	<b>dhcp-snooping static-entry interface INTERFACE-ID IP-ADDRESS</b> <b>no dhcp-snooping static-entry [interface INTERFACE-ID] [IP-ADDRESS]</b>
パラメーター	<b>interface INTERFACE-ID</b> : DHCP スヌーピングのスタティックエントリ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。 <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。</li> <li>• <b>port-channel</b> : ポートチャネルを指定します。</li> </ul> <b>IP-ADDRESS</b> : DHCP スヌーピングのスタティックエントリの 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が、すでにダイナミックエントリに登録済みの場合は、そのスタティックエントリはダイナミックエントリを上書きします。  スタティックエントリ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 <b>no dhcp-snooping static-entry</b> 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 <b>no dhcp-snooping static-entry</b> 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、 <b>total-client</b> 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	1.02.01

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)#
```

### 9.7.7 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	<b>show access-defender dhcp-snooping configuration</b>
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	1.02.01

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
    +-----+ +-----+ +-----+
    1 ooooooooo ..... .....
```

```

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-channell 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"はスタックのボックス ID (シャーシ ID) を示します。スタックを構成していない場合は 1 が表示されます。
(2)	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 ( <b>dhcp-snooping mode deny</b> ) 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"はスタックのボックス ID (シャーシ 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を表示します。

### 9.7.8 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	<b>show access-defender dhcp-snooping mode-status</b>
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	1.02.01

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わるまでの残り時間を表示します

### 9.7.9 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	<b>show access-defender dhcp-snooping status</b>
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	1.02.01

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インターフェース ID を表示します。

項番	説明
(6)	DHCP サーバーによって提供されるクライアント IP アドレスを表示します。
(7)	DHCP スヌーピングエントリーの MAC アドレスを表示します。スタティックエントリーでは、MAC アドレスは表示されません。
(8)	DHCP スヌーピングエントリーのリース期間を表示します。スタティックエントリーではリース期間は表示されません。 10 時間未満の場合は、9:33:12 のように (時):(分):(秒) の形式で表示されます。10 時間を超える場合は、3d5hr のように (日)d(時)hr の形式で表示されます。

# 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 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 [12   13 [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 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
show tech-support	show tech-support [MODULE   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。



debug enable	
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	デバッグバッファをクリアします。
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：デバッグバッファの情報をクリア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クリアします。
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	-

debug clear cpu port	
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クリア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消去します。
シンタックス	<b>debug clear error-log</b>
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消去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	<b>debug copy SOURCE-URL DESTINATION-URL</b> <b>debug copy SOURCE-URL {tftp: //LOCATION/DESTINATION-URL   ftp: //USER-NAME:PASSWORD@LOCATION:TCP-PORT/DESTINATION-URL   c:/DESTINATION-URL   d:/DESTINATION-URL}</b>
パラメーター	<p><b>SOURCE-URL</b>：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。</p> <ul style="list-style-type: none"> <li>• <b>buffer</b>：デバッグバッファの情報をコピーします。</li> <li>• <b>error-log</b>：エラーログの情報をコピーします。</li> <li>• <b>tech-support</b>：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。</li> </ul> <p><b>tftp:</b>：TFTP サーバーにコピーする場合に指定します。</p> <ul style="list-style-type: none"> <li>• <b>LOCATION</b>：TFTP/FTP サーバーの、IPv4 または IPv6 アドレスを指定します。</li> <li>• <b>DESTINATION-URL</b>：送信先 URL を指定します。</li> </ul> <p><b>ftp:</b>：FTP サーバーにコピーする場合に指定します。</p>

debug copy	
	<ul style="list-style-type: none"> <li>• <i>USER-NAME</i>: FTP サーバーのユーザー名を指定します。</li> <li>• <i>PASSWORD</i>: ユーザーのパスワードを指定します。</li> <li>• <i>LOCATION</i>: TFTP/FTP サーバーの、IPv4 または IPv6 アドレスを指定します。</li> <li>• <i>TCP-PORT</i>: TCP ポート番号を指定します。</li> <li>• <i>DESTINATION-URL</i>: 送信先 URL を指定します。</li> </ul> <p><b>c:</b> : ローカルフラッシュにコピーする場合に指定します。</p> <ul style="list-style-type: none"> <li>• <i>DESTINATION-URL</i>: 送信先 URL を指定します。</li> </ul> <p><b>d:</b> : SD カードにコピーする場合に指定します。</p> <ul style="list-style-type: none"> <li>• <i>DESTINATION-URL</i>: 送信先 URL を指定します。</li> </ul>
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	<code>debug output {module <i>MODULE-LIST</i>   all} {buffer   console}</code> <code>no debug output {module <i>MODULE-LIST</i>   all}</code>
パラメーター	<i>MODULE-LIST</i> : 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

debug output	
	<p>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")</p> <p><b>all</b> : 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。</p> <p><b>buffer</b> : デバッグメッセージをデバッグバッファに出力する場合に指定します。</p> <p><b>console</b> : 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。</p>
デフォルト	バッファ
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	<p>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、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、<b>debug show output</b> 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に出力されます。</p> <p>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 <b>debug enable</b> コマンドが有効の場合に出力されます。</p>
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	<b>debug reboot on-error</b> <b>no debug reboot on-error</b>
パラメーター	なし
デフォルト	有効 ( <b>debug reboot on-error</b> )
コマンドモード	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 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	<b>debug show access-defender internal-resource</b>
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	1.02.01

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
DHCPSPNP-BSTEntryDB 0/ 1024   0
DHCPSPNP-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
```

### 10.1.9 debug show buffer

debug show buffer	
目的	デバッグバッファの内容、または使用情報を表示します。

debug show buffer	
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 : デバッグバッファの使用率を表示する方法を示します。

```
# debug show buffer utilization

Allocate from      : System memory pool
Total size         : 2.0 MB
Utilization rate   : 30%
```

### 10.1.10 debug show cpu port

debug show cpu port	
目的	CPU にトラップされたレイヤー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 [12   13 [unicast   multicast]   protocol <i>NAME</i>   security]
パラメーター	<p>12 (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。</p> <p>13 (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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> <p>protocol <i>NAME</i> (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。</p> <p>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。</p>
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

debug show cpu port	
	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：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

## 10.1.11 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) Five seconds - 7 % (2) One minute - 6 % (3) Five minutes - 7 %
(4) Process Name (5) 5Sec (6) 1Min (7) 5Min
-----
OS_UTIL 93 % 93 % 93 %
bcmLINK.0 1 % 1 % 1 %
bcmCNTR.0 0 % 1 % 1 %
GBIC_Pooling 0 % 0 % 0 %
HISR1 0 % 0 % 0 %
bcmL2X.0 0 % 0 % 0 %
NICRX 0 % 0 % 0 %
CLI 0 % 0 % 0 %
socdmadesc.0 0 % 0 % 0 %
CNT_TASK 0 % 0 % 0 %
8021xCtrl 0 % 0 % 0 %
MAUMIB_TASK 0 % 0 % 0 %
radius_reader 0 % 0 % 0 %
SYS_Ctr 0 % 0 % 0 %
cpuprotect 0 % 0 % 0 %
SYSLOGTASK 0 % 0 % 0 %
IP-Msg 0 % 0 % 0 %
bcmRX 0 % 0 % 0 %
DLKtimer 0 % 0 % 0 %
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

```

項番	説明
(1)	5 秒間の平均の CPU 使用率を表示します。
(2)	1 分間の平均の CPU 使用率を表示します。
(3)	5 分間の平均の CPU 使用率を表示します。
(4)	プロセス名を表示します。
(5)	5 秒間の平均の CPU 使用率を表示します。
(6)	1 分間の平均の CPU 使用率を表示します。
(7)	5 分間の平均の CPU 使用率を表示します。



## 10.1.12 debug show error-log

debug show error-log	
目的	エラーログの情報を表示します。
シンタックス	<b>debug show error-log</b>
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: 1.01.01
# 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
```

## 10.1.13 debug show inetstat

debug show inetstat	
目的	IP プロトコルに関する詳細情報を表示します。
シンタックス	<b>debug show inetstat</b>
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 inetstat	
注意事項	-
対象バージョン	1.02.01

使用例：IP プロトコルに関する詳細情報を表示する方法を示します。

```
# debug show inetstat

IP MIB:
ipForwarding:          1
ipDefaultTTL:         30
ipInReceives:         2
ipInHdrErrors:        0
ipInAddrErrors:       0
ipForwDatagrams:      0
ipInUnknownProtos:   0
ipInDiscards:         0
ipInDelivers:         2
ipOutRequests:        2
ipOutDiscards:        0
ipOutNoRoutes:        2
ipReasmTimeout:       60
ipReasmReqds:         0
ipReasmOKs:           0
ipReasmFails:         0
ipFragOKs:            0
ipFragFails:          0
ipFragCreates:        0
ipRoutingDiscards:   0
ipv6IpForwarding:     1
ipv6IpDefaultHopLimit: 64
ipv4InterfaceTableLastChange: 6586
ipv6InterfaceTableLastChange: 65860
ipIfStatsTableLastChange: 0

ipAddrTable:
Addr          Index      NetMask      BcastAddr     ReasmMaxSize
-----
          0.0.0.0      5121         0.0.0.0       0.0.0.1       65535
    10.249.25.33      257         255.255.254.0 0.0.0.1       65535

ipAddrTable:
IfIndex  PhysAddress      NetAddress      Type
-----
        6  FF-FF-FF-FF-FF-FF  10.249.24.0    OTHER
        6  00-40-66-13-09-69  10.249.24.1    DYNAMIC
        6  00-40-66-B9-2B-4F  10.249.25.33    OTHER
        6  54-EE-75-03-9C-B9  10.249.25.212  DYNAMIC
        6  00-02-2B-21-26-46  10.249.25.217  DYNAMIC
        6  54-EE-75-53-DC-06  10.249.25.219  DYNAMIC
        6  54-EE-75-03-03-7A  10.249.25.220  DYNAMIC
        6  54-EE-75-18-04-B7  10.249.25.222  DYNAMIC
        6  54-EE-75-18-04-D7  10.249.25.224  DYNAMIC
        6  54-EE-75-03-9F-AB  10.249.25.225  DYNAMIC
        6  54-EE-75-03-9B-C4  10.249.25.226  DYNAMIC
        6  54-EE-75-17-84-DD  10.249.25.231  DYNAMIC
        6  54-EE-75-09-FD-DD  10.249.25.233  DYNAMIC
        6  FF-FF-FF-FF-FF-FF  10.249.25.255  OTHER
```

(省略)

## 10.1.14 debug show memory-pool

debug show memory-pool	
目的	メモリーバッファの詳細情報を表示します。
シンタックス	<b>debug show memory-pool</b> <i>MEMORY</i>
パラメーター	<i>MEMORY</i> : メモリーバッファの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	-
対象バージョン	1.02.01

使用例: メモリーバッファの SYS\_HUGE 使用率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: メモリーバッファの SYS\_MEM 使用率の詳細情報を表示する方法を示します。

```
# debug show memory-pool SYS_MEM

SYS_MEM Detail:

MEMORY  NAME      BASE      SIZE MAX REQ  ALLOC  BLKS  FREE N_FRE  MAX_BLK
01E3A8E8 SYS_MEM  03AE2EE4  D00000  409B58  401004  229  8FE73C    1D  8FD9D4
-----
          <=32  <=64  <=128  <=256  <=512  <=1024  <=1536  <=2048  <=5120  <=10240  >10240
Alloc:   52     1    30   441     1     0     2     1     3     2     20
Free:    0     1    24     1     1     1     0     0     0     0     1

Alloc fail times 0.

  ALLOC      SIZE      SN  Magic      Task      File(Line)
-----
03AE2EFC      52  00000000  Y  Root      drv_spi_iproc.c(215)
03AE2F4C    51200  00000014  Y  Root      debug_core.c(529)
03AEF764       8  00000015  Y  Root      drv_arl.c(7060)
03AEF784   90464  00000016  Y  Root      oam_db.c(2104)
03B058FC    3404  00000017  Y  Root      qospolicy_db.c(636)
03B06664   1232  00000018  Y  Root      st_lac.c(522)
03B06B4C     28  00000019  Y  Root      utl_avlt.c(50)
03B06B84     28  0000001A  Y  Root      utl_avlt.c(50)
03B06BBC     28  0000001B  Y  Root      utl_avlt.c(50)
03B06BF4     28  0000001C  Y  Root      utl_queue.c(89)
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 10.1.15 debug show netstat

debug show netstat	
目的	OS のメモリー使用量を表示します。
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	1.01.01

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 Allocate Blocks
-----
KERNEL      68000000  16645B00  16634930    2AC
NIC_DMA     20E858   20686C   20686C      1
ssl_timer   4E20     0        0           0
ssl_lib     4B000    0        0           0
web_mem     580000   6B628    6B628      418
CRYPT       200000   9E80     8760       2A
LLDP_RMIB_MEM_P  64000   0        0           0
LLDP_MIB_MEM_PO  C5800   4694     4618      4A
LLDP_MEM_POOL  1B800   D10      0           0
SDK_DMA     800000   49DD34   A8CF8      A0
NTP         100000   3B0C     3B0C       17
stp         249E000  1E888    1E888      70E
STG         40000    200      200        C
rmon        6E1204   5A014    7BAC       119
agent       1FA000   297D0    297D0      57A
CLI2-MEMORY 300000   157BB4   1480C0     1722
syslog_remote_a 251C0   0        0           0
syslog_attack 251C0   0        0           0
syslog_regular 173180  2AA8     2AA8       56
SEC_MEM     1400000  3F9C     1608       C
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

項番	説明
(1)	メモリー名を表示します。
(2)	合計メモリーサイズを 16 進数 (バイト) で表示します。
(3)	装置が起動してからの最大割り当てメモリーサイズを 16 進数 (バイト) で表示します。
(4)	現在の割り当てメモリーサイズを 16 進数 (バイト) で表示します。
(5)	現在の割り当てメモリーブロック数を 16 進数で表示します。

## 10.1.16 debug show output

debug show output	
目的	モジュールのデバッグ状態と出力情報を表示します。

debug show output	
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
```

### 10.1.17 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	1.01.01

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_QUEUE
NICRX        7%    DEFB    S:NIC-RX-Sem
socdmadesc.0  8%    59FF    S:Desc DMA interr
CNT_TASK     64%    55A4    Delay
8021xCtrl    25%    401D    Q:1X_8021xCtrl
MAUMIB_TASK  29%    38AB    E:MAU_EVENT
radius_reader 35%    268E    Q:radius_reader
SYS_Ctr      18%    21EB    E:SYS_ENT
```

cpuprotect	11%	1F64	Q:CPU Protect
CLI	42%	156B	Run
bcmRX	13%	11DC	S:RX pkt ntfy
FAN_Polling	16%	11A8	E:SYS_ENT
IP-Msg	5%	F14	Q:IPMQ
DLKtimer	24%	E8F	Delay
IP6-Tic	5%	AA6	E:IP6TIC
OS_TIMER	24%	59E	Pend
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All			

項番	説明
(1)	プロセス名を表示します。
(2)	装置が起動してからプロセスに割り当てられた最大メモリー使用率を表示します。
(3)	装置が起動してからプロセスで使用された合計 CPU カウンターを表示します。
(4)	現在の状態を表示します。

### 10.1.18 debug show tcpstat

debug show tcpstat	
目的	TCP 接続の詳細情報を表示します。
シンタックス	<code>debug show tcpstat</code>
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	1.02.01

使用例：TCP 接続の詳細情報を表示する方法を示します。

```

# debug show tcpstat

rfc2988 tcpRtoAlgorithm
500 tcpRtoMin
32000 tcpRtoMax
-1 tcpMaxConn
0 tcpActiveOpens
0 tcpPassiveOpens
0 tcpAttemptFails
0 tcpEstabResets
0 tcpCurrEstab
0 tcpInSegs
0 tcpOutSegs
0 tcpRetransSegs
0 tcpInErrs
0 tcpOutRsts
0 tcpHCInSegs
0 tcpHCOutSegs

tcpConnTable:
Local Address          Remote Address        State
-----
0.0.0.0:23            0.0.0.0:0             listen
    
```

```
Total Entries: 1

tcpConnectionTable:
Process Local Type Local Address                               State
      Remote Type Remote Address
-----
Total Entries (V4/V6): 0/0

tcpListenerTable:
Process Local Type Local Address
-----
0      IPv4      0.0.0.0:23
0      IPv6      [::]:23

Total Entries (V4/V6): 1/1
```

### 10.1.19 debug show udpstat

debug show udpstat	
目的	UDP 接続の詳細情報を表示します。
シンタックス	<b>debug show udpstat</b>
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	1.02.01

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 udpHCOOutDatagrams

udpTable:
Local Address Local Port
-----
0.0.0.0      161
0.0.0.0      520
0.0.0.0      8021
0.0.0.0      8022

Total Entries: 4

udpEndpointTable:
Instance Process Local Type Local Address
      Remote Type Remote Address
-----
```

1	0	IPv4	0.0.0.0:161
		IPv4	0.0.0.0:0
1	0	IPv4	0.0.0.0:520
		IPv4	0.0.0.0:0
1	0	IPv4	0.0.0.0:8021
		IPv4	0.0.0.0:0
1	0	IPv4	0.0.0.0:8022
		IPv4	0.0.0.0:0
1	0	IPv6	:::161
		IPv6	:::0
1	0	IPv6	:::162
		IPv6	:::0
1	0	IPv6	:::546
		IPv6	:::0
1	0	IPv6	:::8021
		IPv6	:::0
1	0	IPv6	:::8022
		IPv6	:::0
Total Entries (V4/V6): 4/5			

### 10.1.20 show tech-support

show tech-support	
目的	技術サポート担当者に必要な情報を表示します。
シンタックス	<code>show tech-support [MODULE   unit UNIT-ID   interface {INTERFACE-ID [,   -]   stack-port} system-dump]</code>
パラメーター	<p><i>MODULE</i> (省略可能) : モジュールのキーワードを入力します。以下のいずれかのパラメーターを指定できます。</p> <ul style="list-style-type: none"> <li>• <b>access-defender</b> : AccessDefender 設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>dhcp-server</b> : DHCP サーバー設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>dhcpv6-client</b> : DHCPv6 クライアント設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>dhcpv6-server</b> : DHCPv6 サーバー設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>ether-oam</b> : EtherOAM 設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>ethernet-ring-g8032</b> : リングプロテクション (ERPS) 設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>ipv6-multicast</b> : IPv6 マルチキャスト設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>loop-detection</b> : ループ検知設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>memory-error</b> : メモリーエラー自動復旧設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>mrrp-plus</b> : MMRP-Plus 設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>ntp</b> : NTP 設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>port-channel</b> : ポートチャンネル設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>rmon</b> : RMON 設定に関連する技術サポート情報を表示する場合に指定しま</li> </ul>



show tech-support	
	<p>す。</p> <ul style="list-style-type: none"> <li>• <b>snmpv3</b> : SNMPv3 設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>sntp</b> : SNTP 設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>spanning-tree</b> : スパニングツリー設定に関連する技術サポート情報を表示する場合に指定します。</li> <li>• <b>stack</b> : スタック設定に関連する技術サポート情報を表示する場合に指定します。</li> </ul> <p><b>unit</b> <i>UNIT-ID</i> (省略可能) : 技術サポート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。</p> <p><b>interface</b> <i>INTERFACE-ID</i> <b>system-dump</b> (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。</p> <ul style="list-style-type: none"> <li>• <b>port</b> : 物理ポートを指定します。複数指定できます。</li> <li>• <b>stack-port</b> : スタックポートを指定します。</li> </ul>
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	-
対象バージョン	1.01.01 1.02.01 : <b>stack</b> パラメーター、 <b>unit</b> パラメーター、 <b>interface</b> パラメーター追加

使用例：全モジュールの技術サポート情報を表示する方法を示します。

```
# show tech-support

#-----
#                               ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch
#                               Technical Support Information
#
#                               Firmware: Build 1.02.02
#   Copyright (C) 2018 APRESIA Systems, Ltd. All rights reserved.
#-----

***** Basic System Information *****

[SYS 2021-2-1 16:01:47]

Boot Time           : 1 Feb 2021 15:59:21
RTC Time            : 2021/02/01 07:01:47
Boot PROM Version   : Build 1.00.00
Firmware Version    : Build 1.02.02
Hardware Version    : A
Serial number       : 189842180028
MAC Address         : 00-40-66-CE-0B-33
MAC Address Number  : 25
```

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

使用例：MMRP-Plus 関連のテクニカルサポート情報を表示する方法を示します。

```
# show tech-support mmrp-plus

#-----
#
#           ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch
#           Technical Support Information
#
#           Firmware: Build 1.02.02
#   Copyright (C) 2018 APRESIA Systems, Ltd. All rights reserved.
#-----

[MMRP 2021-2-1 16:02:03]

##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 関連のテクニカルサポート情報を表示する方法を示します。

```
# show tech-support access-defender

#-----
#
#           ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch
#           Technical Support Information
#
#           Firmware: Build 1.02.02
#   Copyright (C) 2018 APRESIA Systems, Ltd. All rights reserved.
#-----

[ACCESS_DEFENDER 2021-2-1 16:02:14]

#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テクニカルサポート情報を表示する方法を示します。

```
# show tech-support memory-error
```

```
#-----  
#                               ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch  
#                               Technical Support Information  
#  
#                               Firmware: Build 1.02.02  
#   Copyright (C) 2018 APRESIA Systems, Ltd. All rights reserved.  
#-----  
  
[MEAR 2021-2-1 16:02:29]  
  
Detail Memory-Error Auto-Recovery Status:  
-----  
Auto Recovery Mode           : Enabled  
Auto Recovery Notification   : Enabled  
Fault Action Configuration   : -  
  
Unit : 1  
Status : Normal  
Recovery Counters  
-----  
PORT_TABm                    :          0  
SYSTEM_CONFIG_TABLEm        :          0  
SOURCE_TRUNK_MAP_TABLEm     :          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	<p><b>all</b> : 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。</p> <p><b>loop-detection</b> : 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。</p> <p><b>storm-control</b> : 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。</p> <p><b>uld</b> : 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。</p> <p><b>interval SECONDS</b> (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、5~86400 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。</p>
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	<p>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。</p> <p>各機能で err-disabled 状態に変更されたポートのリンク状態は、<b>show interfaces</b> コマンドでは以下のように表示されます。</p> <ul style="list-style-type: none"> <li>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)</li> <li>ストームコントロール機能 : link status is down (error disabled: Storm Control)</li> <li>単方向リンク検出機能 : link status is down (error disabled: OAM Unidirectional Link)</li> </ul>

errdisable recovery	
	<p>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、<b>show interfaces status</b> コマンドの Status 項目では "err-disabled" と表示されます。</p> <p>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 <b>shutdown</b> コマンドを実行した後、<b>no shutdown</b> 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。</p>
制限事項	-
注意事項	<b>interval</b> 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 <b>interval</b> 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 1.02.01 : <b>uld</b> 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	<b>show errdisable recovery</b>
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)	ポート番号を表示します。
(5)	ポートが自動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	<b>memory-error auto-recovery mode disable</b> <b>no memory-error auto-recovery mode disable</b>
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 ( <b>no memory-error auto-recovery mode disable</b> )
コマンドモード	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	<p>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。</p> <p>以下のメモリー領域は、監視対象外となり、<b>show environment memory</b> 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。</p> <ul style="list-style-type: none"> <li>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</li> <li>復旧不能なメモリーエラーが検出されたメモリー領域</li> </ul> <p>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。</p>
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	<b>memory-error auto-recovery notify disable</b> <b>no memory-error auto-recovery notify disable</b>
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 ( <b>no memory-error auto-recovery notify disable</b> )
コマンドモード	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し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	<b>memory-error fault-action shutdown-all</b> <b>no memory-error fault-action shutdown-all</b>
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	<b>memory-error fault-action shutdown-all</b> 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、 <b>show interfaces</b> コマンドでは "link status is down (cause: Memory Error)" と表示されます。また、 <b>show interfaces status</b> 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、 <b>clear memory-error</b> コマンド、または <b>no memory-error fault-action shutdown-all</b> 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	<b>clear memory-error</b>
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-LEVEL   SEVERITY-NAME}] [discriminator NAME] [write-delay {SECONDS   infinite}] no logging buffered default logging buffered
logging console	logging console [severity {SEVERITY-LEVEL   SEVERITY-NAME}] [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-LEVEL   SEVERITY-NAME}] [facility {FACILITY-NUM   FACILITY-NAME}] [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	デバッグメッセージおよびエラーメッセージを、ロギングプロセスに送信するコ

logging on	
	<p>マンドです。ロギングプロセスでは、メッセージを出力するプロセスに対して非同期に、指定された場所にメッセージをロギングします。</p> <p>ロギングプロセスは、ローカルメッセージバッファ、端末ライン、および syslog サーバーなど、多様な宛先へのロギングメッセージの配布を制御します。システムのロギングメッセージは、システムエラーメッセージとも呼ばれます。</p> <p>これらの宛先へのロギングは、<b>logging buffered</b>、<b>logging server</b>、および <b>logging</b> のグローバル設定コマンドを使用して、個々にオンとオフを切り替えられます。</p> <p><b>logging on</b> コマンドが無効の場合、これらの宛先にメッセージは送信されません。<b>logging on</b> コマンドが有効な場合、<b>logging buffered</b> が有効になります。</p>
制限事項	<p>ローカルメッセージバッファ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。</p> <p>Syslog サーバーに送信されるログは、起動時に出力するログ「System warm start」以降です。また、Syslog サーバーと通信可能となった後は、通信可能になる前に保存されていたログについても送信されます。</p>
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。

<pre># configure terminal (config)# logging on  WARNING: The command takes effect and the logging buffered is enabled at the same time. (config)#</pre>
---

## 10.4.2 logging buffered

logging buffered	
目的	ローカルメッセージバッファ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、 <b>no logging buffered</b> コマンドを使用します。デフォルト設定に戻すには、 <b>default logging buffered</b> コマンドを使用します。
シンタックス	<pre>logging buffered [severity {SEVERITY-LEVEL   SEVERITY-NAME}] [discriminator NAME] [write-delay {SECONDS   infinite}] no logging buffered default logging buffered</pre>
パラメーター	<p><b>severity</b> (省略可能)：システムメッセージの重大度レベルを指定します。</p> <p><b>SEVERITY-LEVEL</b>：システムメッセージの重大度レベルを数値で指定します。指定した重大度レベル以上のメッセージが、ローカルメッセージバッファにロギングされます。重大度は 0~7 の範囲で指定します。0 が最も重要なレベルです。重大度が指定されていない場合、デフォルトの重大度レベル「情報メッセージ (informational(6))」が指定されます。</p> <p><b>SEVERITY-NAME</b>：システムメッセージの重大度レベルをレベル名で指定します。レベル名は、以下のいずれかを指定できます。</p> <ul style="list-style-type: none"> <li>• emergencies</li> <li>• alerts</li> </ul>

logging buffered	
	<ul style="list-style-type: none"> <li>• critical</li> <li>• errors</li> <li>• warnings</li> <li>• notifications</li> <li>• informational</li> <li>• debugging</li> </ul> <p><b>discriminator</b> <i>NAME</i> (省略可能) : ローカルメッセージバッファーに送信するメッセージをフィルタリングする際に使用する discriminator の識別子を指定します。</p> <p><b>write-delay</b> (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-NP4000 Ver. 1.02.01 以降では SRAM に、AEOS-NP4000 Ver. 1.01.02 以前ではフラッシュメモリーに保存されます。</p> <p><b>SECONDS</b> : 周期的書き込み間隔 (秒単位) を指定します。</p> <p><b>infinite</b> : 周期的書き込みを無効にします。</p>
デフォルト	<p>重大度レベル : 情報メッセージ (informational (6))</p> <p>周期的書き込み間隔 : 0 秒 (1.02.01 以降), 300 秒 (1.01.02 以前)</p>
コマンドモード	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	<p>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、任意の書き込み先に送られます。</p> <p>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-NP4000 Ver. 1.02.01 以降は SRAM に、AEOS-NP4000 Ver. 1.01.02 以前はフラッシュメモリーに保存されます。</p> <p>以下の操作時には、AEOS-NP4000 Ver. 1.02.01 以降では SRAM とフラッシュメモリーの両方に、AEOS-NP4000 Ver. 1.01.02 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。</p> <ul style="list-style-type: none"> <li>• <b>write</b> コマンド、<b>copy running-config startup-config</b> コマンドによる設定保存</li> <li>• <b>logout</b> コマンド、<b>exit</b> コマンドによるログアウト</li> <li>• <b>reboot</b> コマンド等による再起動</li> </ul> <p>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。</p> <p>メッセージをフィルタリングする識別子が存在しない場合、コマンドは有効になりません。この場合、コマンドのデフォルト設定が適用されます。</p> <p>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を制限するためには、メッセージの重大度レベルを指定します。これにより、指定した重大度レベル以上のメッセージだけがローカルメッセージバッファーにロギングされ、ロギングされるメッセージの数を削減できます。</p> <p>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が削除されます。</p> <p>レベル名は、重大度レベルと関連付けられています。レベル名と重大度レベルの関連付けを、以下に示します。</p> <ul style="list-style-type: none"> <li>• <b>emergencies (0)</b> - システムは使用不能です。</li> </ul>

logging buffered	
	<ul style="list-style-type: none"> <li>• <b>alerts (1)</b> - 直ちにアクションが実行される必要があります。</li> <li>• <b>critical (2)</b> - 危険条件に該当します。</li> <li>• <b>errors (3)</b> - エラー条件に該当します。</li> <li>• <b>warnings (4)</b> - 警告条件に該当します。</li> <li>• <b>notifications (5)</b> - 正常ですが、重要な条件に該当します。</li> <li>• <b>informational (6)</b> - 情報メッセージです。</li> <li>• <b>debugging (7)</b> - デバッグメッセージです。</li> </ul>
制限事項	ローカルメッセージバッファ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。
対象バージョン	1.01.01 1.02.01 : 動作対象とデフォルトの仕様変更

使用例：ローカルメッセージバッファへのメッセージのロギングを有効にして、重大度レベルが errors より高いメッセージをロギング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	<b>logging console</b> [ <b>severity</b> { <i>SEVERITY-LEVEL</i>   <i>SEVERITY-NAME</i> }] <b>[discriminator</b> <i>NAME</i> ] <b>no logging console</b>
パラメーター	<p><i>SEVERITY-LEVEL</i> (省略可能) : システムメッセージの重大度レベルを指定します。指定した重大度レベル以上のメッセージが、ローカルコンソールにロギングされます。</p> <p>重大度レベルは 0~7 の範囲で指定します。0 が最も重要なレベルです。重大度が指定されていない場合、デフォルトの重大度レベル「警告 (warning(4))」が指定されます。</p> <p><i>SEVERITY-NAME</i> (省略可能) : システムメッセージの重大度レベルをレベル名で指定します。レベル名は、以下のいずれかを指定できます。</p> <ul style="list-style-type: none"> <li>• emergencies</li> <li>• alerts</li> <li>• critical</li> <li>• errors</li> <li>• warnings</li> <li>• notifications</li> <li>• informational</li> <li>• debugging</li> </ul> <p><b>discriminator</b> <i>NAME</i> (省略可能) : ローカルコンソールに送信するメッセージをフィルタリングする際に使用する discriminator の識別子を指定します。</p>

logging console	
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	<p>本設定により、ローカルメッセージバッファ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。</p> <p>メッセージをフィルタリングする識別子が存在しない場合、コマンドは有効になりません。この場合、コマンドのデフォルト設定が適用されます。</p> <p>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を制限するためには、メッセージの重大度レベルを指定します。これにより、指定した重大度レベル以上のメッセージだけがローカルコンソールにロギングされます。</p> <p>レベル名は、重大度レベルと関連付けられています。レベル名と重大度レベルの関連付けを、以下に示します。</p> <ul style="list-style-type: none"> <li>• <b>emergencies (0)</b> - システムは使用不能です。</li> <li>• <b>alerts (1)</b> - 直ちにアクションが実行される必要があります。</li> <li>• <b>critical (2)</b> - 危険条件に該当します。</li> <li>• <b>errors (3)</b> - エラー条件に該当します。</li> <li>• <b>warnings (4)</b> - 警告条件に該当します。</li> <li>• <b>notifications (5)</b> - 正常ですが、重要な条件に該当します。</li> <li>• <b>informational (6)</b> - 情報メッセージです。</li> <li>• <b>debugging (7)</b> - デバッグメッセージです。</li> </ul>
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：ローカルコンソールへのメッセージのロギングを有効にして、重大度レベルが errors より高いメッセージをロギング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	さまざまな送信先に転送する SYSLOG メッセージをフィルタリングする際に使用する discriminator 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	<b>logging discriminator</b> <i>NAME</i> [ <b>facility</b> { <b>drops</b> <i>STRING</i>   <b>includes</b> <i>STRING</i> }] [ <b>severity</b> { <b>drops</b> <i>SEVERITY-LIST</i>   <b>includes</b> <i>SEVERITY-LIST</i> }] <b>no logging discriminator</b> <i>NAME</i>
パラメーター	<p><i>NAME</i>: 識別子を指定します。</p> <p><b>facility</b> (省略可能): サブフィルターとして、ファシリティを利用する場合に指定します。ファシリティでフィルタリングします。</p> <p><i>STRING</i>: フィルタリングするファシリティ名、またはフィルタリングしないファシリティ名を 1 つ以上指定します。複数のファシリティ名を使用する場合、コン</p>

logging discriminator	
	<p>マでファシリティ名を区切ります。コンマの前後には、スペースを入れないでください。</p> <p><b>drops</b> : 一致するメッセージがフィルタリングされます。</p> <p><b>includes</b> : 一致するメッセージはフィルタリングされません。一致しないメッセージがフィルタリングされます。</p> <p><b>severity</b> (省略可能) : サブフィルターとして、重大度レベルを利用する場合に指定します。重大度レベルでフィルタリングします。</p> <p><b>SEVERITY-LIST</b> : フィルタリングする重大度レベル、またはフィルタリングしない重大度レベルのリストを指定します。</p>
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	設定を変更すると、以前の設定は上書きされます。識別子は、 <b>logging buffered</b> コマンドや <b>logging server</b> コマンドで使用できます。
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 : 「buffer-filter」という名前の識別子を作成して、サブフィルターとしてファシリティと重大度レベルを指定する方法を示します。

```
# configure terminal
(config)# logging discriminator buffer-filter facility includes STP severity includes
1-4,6
(config)#
```

### 10.4.5 logging server

logging server	
目的	システムメッセージのロギング、または出力のデバッグを行う SYSLOG サーバーホストを作成します。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	<p><b>logging server</b> {<i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i>} [<b>severity</b> {<i>SEVERITY-LEVEL</i>   <i>SEVERITY-NAME</i>}] [<b>facility</b> {<i>FACILITY-NUM</i>   <i>FACILITY-NAME</i>}] [<b>discriminator</b> <i>NAME</i>] [<b>port</b> <i>UDP-PORT</i>]</p> <p><b>no logging server</b> {<i>IP-ADDRESS</i>   <i>IPV6-ADDRESS</i>}</p>
パラメーター	<p><i>IP-ADDRESS</i> : SYSLOG サーバーホストの IP アドレスを指定します。</p> <p><i>IPV6-ADDRESS</i> : SYSLOG ログサーバーホストの IPv6 アドレスを指定します。</p> <p><i>SEVERITY-LEVEL</i> (省略可能) : システムメッセージの重大度レベルを指定します。指定した重大度レベル以上のメッセージが、ローカルコンソールにロギングされます。</p> <p>重大度レベルは 0~7 の範囲で指定します。0 が最も重要なレベルです。重大度が指定されていない場合、デフォルトの重大度レベル「警告 (warning(4))」が指定されます。</p>

logging server	
	<p><i>SEVERITY-NAME</i> (省略可能) : システムメッセージの重大度レベルをレベル名で指定します。レベル名は、以下のいずれかを指定できます。</p> <ul style="list-style-type: none"> <li>• emergencies</li> <li>• alerts</li> <li>• critical</li> <li>• errors</li> <li>• warnings</li> <li>• notifications</li> <li>• informational</li> <li>• debugging</li> </ul> <p><b>facility</b> : ファシリティの設定を構成します。</p> <p><i>FACILITY-NUM</i> (省略可能) : ファシリティの種類を 0~23 の 10 進数値で指定します。種類を指定しない場合、デフォルトのファシリティは 23 (Local7) です。</p> <p><i>FACILITY-NAME</i> (省略可能) : ファシリティの種類をファシリティ名で指定します。種類を指定しない場合、デフォルトの facility は local7 (23) です。</p> <p><b>discriminator NAME</b> (省略可能) : SYSLOG ログサーバーに送信するメッセージをフィルタリングする際に使用する discriminator の識別子を指定します。</p> <p><b>port UDP-PORT</b> (省略可能) : SYSLOG サーバーへの送信に使用する UDP ポート番号を指定します。指定可能なポート番号は、514 (IANA の「ウェルノウン」ポート)、または 1024~65535 です。ポート番号が指定されていない場合、デフォルトの「514」が指定されます。</p>
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	<p>本設定により、ローカルメッセージバッファ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。</p> <p>facility 名、数値、および関連付けられている facility のリストを以下に示します</p> <ul style="list-style-type: none"> <li>• kern (0) - カーネルメッセージ</li> <li>• user (1) - ユーザーレベルのメッセージ</li> <li>• mail (2) - メールシステム</li> <li>• daemon (3) - システムデーモン</li> <li>• auth1 (4) - セキュリティー/認証メッセージ</li> <li>• syslog (5) - SYSLOG によって内部的に出力されたメッセージ</li> <li>• lpr (6) - ラインプリンターサブシステム</li> <li>• news (7) - ネットワークニュースサブシステム</li> <li>• uucp (8) - UUCP サブシステム</li> <li>• clock1 (9) - クロックデーモン</li> <li>• auth2 (10) - セキュリティー/認証メッセージ</li> <li>• ftp (11) - FTP デーモン</li> <li>• ntp (12) - NTP サブシステム</li> <li>• logaudit (13) - ログ監査</li> <li>• logalert (14) - ログの警告</li> <li>• clock2 (15) - クロックデーモン 2</li> </ul>



logging server	
	<ul style="list-style-type: none"> <li>• local10 (16) - ローカル使用 0 (local10)</li> <li>• local11 (17) - ローカル使用 1 (local11)</li> <li>• local12 (18) - ローカル使用 2 (local12)</li> <li>• local13 (19) - ローカル使用 3 (local13)</li> <li>• local14 (20) - ローカル使用 4 (local14)</li> <li>• local15 (21) - ローカル使用 5 (local15)</li> <li>• local16 (22) - ローカル使用 6 (local16)</li> <li>• local17 (23) - ローカル使用 7 (local17)</li> </ul>
制限事項	SYSLOG サーバーホストは 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。
対象バージョン	1.01.01

使用例：重大度レベルが warnings より高いシステムメッセージを、リモートホスト 20.3.3.3 にロギングする方法を示します。

```
# configure terminal
(config)# logging server 20.3.3.3 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	<b>logging source-interface</b> <i>INTERFACE-ID</i> <b>no logging source-interface</b>
パラメーター	<i>INTERFACE-ID</i> : 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。 <ul style="list-style-type: none"> <li>• <b>vlan</b> : VLAN インターフェースを指定します。</li> <li>• <b>mgmt</b> : マネージメントポートを指定します。</li> </ul>
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	<p>マネージメントポート経由で管理する場合は、<b>vlan</b> 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。</p> <p>VLAN インターフェース経由で管理する場合は、<b>mgmt</b> 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。</p>
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	<b>command logging enable</b> <b>no command logging enable</b>
パラメーター	なし
デフォルト	有効 ( <b>command logging enable</b> )
コマンドモード	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。  <b>show logging</b> 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	本コマンドの設定は、構成情報では CLI コマンド関連で表示されます。(ラベル : # CLI)
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	<b>show logging</b> [ <b>all</b>   [ <i>REF-SEQ</i> ] [ <b>+</b> <i>NV</i>   <b>-</b> <i>NV</i> ]]
パラメーター	<b>all</b> (省略可能) : すべてのログエントリを最新メッセージから順に表示する場合に指定します。  <i>REF-SEQ</i> (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。  <b>+ NV</b> (省略可能) : <i>REF-SEQ</i> 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。  <b>- NV</b> (省略可能) : <i>REF-SEQ</i> 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

show logging	
	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時、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    2017-03-03 14:49:36 INFO(6) "exit" executed by 15 from Console
#5    2017-03-03 14:49:35 INFO(6) "configure terminal" executed by 15 from Console
#4    2017-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#3    2017-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#2    2017-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
#1    2017-03-03 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    2017-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#4    2017-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#5    2017-03-03 14:49:35 INFO(6) "configure terminal" executed by 15 from Console
#6    2017-03-03 14:49:36 INFO(6) "exit" executed by 15 from Console
#7    2017-03-03 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+ NV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    2017-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
#3    2017-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#4    2017-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#5    2017-03-03 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- NV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    2017-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#3    2017-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#2    2017-03-03 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-NP4000 Ver. 1.02.01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

show logging sram	
	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	1.02.01

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、フラッシュメモリのログメッセージを削除します。AEOS-NP4000 Ver. 1.02.01 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	<b>clear logging</b>
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 1.02.01：動作対象の仕様変更

使用例：すべてのログメッセージの削除方法を示します。

```
# 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 trace trigger	cpu-protect trace trigger VALUE no cpu-protect trace trigger
show cpu-protect trace	show cpu-protect trace

### 10.5.1 cpu-protect trace trigger

cpu-protect trace trigger	
目的	CPU 使用率が指定されたしきい値に達したときに障害解析用情報を採取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 VALUE no cpu-protect trace trigger
パラメーター	VALUE: CPU 使用率のしきい値を、50~100 の範囲で指定します。単位は%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	採取された障害解析用情報は、show tech-support コマンドの技術サポート情報の一部として出力されます。
制限事項	-
注意事項	-
対象バージョン	1.01.01

使用例: CPU 使用率が 50%に達したときに障害解析用情報を採取する機能を有効にする方法を示します。

```
# configure terminal
(config)# cpu-protect trace trigger 50
(config)#
```

### 10.5.2 show cpu-protect trace

show cpu-protect trace	
目的	CPU 使用率監視のトレース状態を表示します。
シンタックス	show cpu-protect trace
パラメーター	なし
デフォルト	無効
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: 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	: 90% ... (3)

項番	説明
(1)	CPU 使用率監視の動作状態を表示します。
(2)	CPU 使用率監視のトレースの状態を表示します。
(3)	CPU 使用率のしきい値を表示します。

# 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 ApresiaNP4000-20Xt4X
Firmware: Build 1.02.01

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 ApresiaNP4000-20Xt4X
```

```
Firmware: Build 1.02.01
```

```
>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-NP4000 Ver. 1.02 コマンドリファレンス

Copyright(c) 2019 APRESIA Systems, Ltd.

2019年11月初版

2021年5月第7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/>