IP8800/S2200・IP8800/S2100・IP8800/SS1250・
IP8800/SS1240 ソフトウェアマニュアル

コンフィグレーションコマンドレファレンス

Ver. 2.7 対応

IP8800SS1240-S003-A0

■対象製品

このマニュアルは次に示すモデル，ソフトウェアでサポートする機能を対象に記載しています。

- IP8800/S2200：Ver.2.7　OS-LT4，オプションライセンス
- IP8800/S2100：Ver.2.7　OS-LT5　（オプションライセンス未サポート）
- IP8800/SS1250：Ver.2.7　OS-LT3，オプションライセンス
- IP8800/SS1240：Ver.2.7　OS-LT2，オプションライセンス

■輸出時の注意

本製品を輸出される場合には，外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ，必要な手続きをお取りください。
なお，不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Ethernet は，富士ゼロックス株式会社の登録商標です。
GSRP は，アラクサラネットワークス株式会社の登録商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
RSA，SecurID については RSA Security Inc. の米国およびその他の国における商標もしくは登録商標です。
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。
Wake on LAN は，IBM Corp. の登録商標です。
MagicPacket は，Advanced Micro Devices,Inc. の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■発行

２０１８年　３月　（第１１版）　IP8800SS1240-S003-A0

■著作権

変更履歴

【Ver. 2.7（第 11 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
3　コンフィグレーションの編集と操作	• save コマンドに注意事項を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 2.6（第 10 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
シリーズの追加	• IP8800/S2100 の記述を追加しました。
このマニュアルの読み方	• IP8800/S2100 の記述を追加しました。
装置の管理	• 下記コマンドの説明を変更しました。 system temperature-warning-level system temperature-warning-level average
IEEE802.1X	• 下記コマンドの説明を変更しました。 dot1x supplicant-detection dot1x vlan dynamic supplicant-detection
特定端末への Web 通信不可表示機能【S2100】	• 本章を追加しました。
SNMP	• snmp-server host コマンドの説明を変更しました。
ポートミラーリング	• monitor session コマンドの説明を変更しました。 • switchport monitor dot1q tag コマンドを追加しました。
コンフィグレーション編集時のエラーメッセージ	• 下記情報を追加しました。 特定端末の Web 通信不可表示機能情報 • 下記情報のエラーメッセージを変更しました。 VLAN 情報 フロー検出モード情報 DHCP snooping 情報 ポートミラーリング情報

【Ver. 2.5（第 9 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
イーサネット	• 下記コマンドの説明を変更しました。 duplex speed
IGMP snooping	• ip igmp snooping fast-leave コマンドを追加しました。
アクセスリスト	• 指定できる名称にアクセスリスト数に関する記述を追加しました。
QoS	• 指定できる名称および値に QoS フローリスト数に関する記述を追加しました。

章・節・項・タイトル	追加・変更内容
Web 認証	• 下記のコマンドを追加しました。 http-server initial-timeout web-authentication prefilter web-authentication redirect ignore-https
SNMP	• 下記コマンドの説明を変更しました。 rmon collection history snmp-server host snmp-server traps

【Ver. 2.4(第 7 版)】

表　変更履歴

章・節・項・タイトル	追加・変更内容
シリーズの追加	• IP8800/S2200 の記述を追加しました。
イーサネット	• 下記のコマンドを追加しました。 power inline system-allocation

【Ver. 2.3(第 6 版)】

表　変更履歴

章・節・項・タイトル	追加・変更内容
ログインセキュリティと RADIUS	• 下記のコマンド説明を変更しました。 ip access-group
Ring Protocol	• 下記のコマンドを追加しました。 multi-fault-detection mode multi-fault-detection vlan
アクセスリスト	• 下記のコマンド説明を変更しました。 deny(ip access-list extended) ip access-group mac access-group permit(ip access-list extended)
QoS	• 下記のコマンド説明を変更しました。 ip qos-flow-group mac qos-flow-group
コンフィグレーション編集時のエラーメッセージ	• 下記情報のエラーメッセージを変更しました。 Ring Protocol 情報 CFM 情報

【Ver. 2.3(第 5 版)】

表　変更履歴

章・節・項・タイトル	追加・変更内容
ログインセキュリティと RADIUS	• 下記のコマンドを追加しました。 aaa authentication login end-by-reject
装置の管理	• 下記のコマンドを追加しました。 system fan mode system temperature-warning-level system temperature-warning-level average

章・節・項・タイトル	追加・変更内容
イーサネット	• 下記のコマンドの説明を変更しました。 bandwidth mdix auto • 下記のコマンドに注意事項を追加しました。 link debounce
DHCP snooping	• 下記のコマンドに注意事項を追加しました。 ip arp inspection limit rate ip dhcp snooping limit rate ip dhcp snooping trust ip verify source
レイヤ 2 認証共通	• 下記のコマンドに注意事項を追加しました。 authentication arp-relay
Web 認証	• 下記のコマンドを追加しました。 aaa authentication web-authentication end-by-reject
MAC 認証	• 下記のコマンドを追加しました。 aaa authentication mac-authentication end-by-reject

【Ver. 2.2（第 4 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
シリーズの追加	• IP8800/SS1250 の記述を追加しました。
このマニュアルの読み方	• IP8800/SS1250 の記述を追加しました。
装置の管理	• 下記のコマンド説明を変更しました。 system recovery
イーサネット	• 100BASE-FX(SFP) サポートに伴い記述を追加しました。 duplex flowcontrol interface gigabitethernet media-type speed
アクセスリスト	• 下記のコマンドに注意事項を追加しました。 deny（mac access-list extended） permit（mac access-list extended）
QoS	• 下記のコマンドに注意事項を追加しました。 qos（mac qos-flow-list）
アップリンク・リダンダント	• 下記のコマンドを追加しました。 switchport-backup startup-active-port-selection

【Ver. 2.2（第 3 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
このマニュアルの読み方	• コマンドモード一覧を変更しました。
ログインセキュリティと RADIUS	• 下記のコマンドを追加しました。 aaa group server radius radius-server attribute station-id capitalize server • 下記のコマンドにパラメータを追加しました。 radius-server host

章・節・項・タイトル	追加・変更内容
装置の管理	• 下記のコマンドを追加しました。 system recovery
省電力機能	• 下記のコマンドの設定値の反映契機を変更しました。 system fan-control
イーサネット	• 下記のコマンドを追加しました。 linkscan-mode
VLAN	• 下記のコマンドのパラメータ説明を変更しました。 switchport mode
Ring Protocol	• 本章を追加しました。
IEEE802.1X	• 下記のコマンドを追加しました。 aaa accounting dot1x dot1x authentication • 下記のコマンドの注意事項を変更しました。 dot1x force-authorized dot1x force-authorized vlan dot1x vlan dynamic enable dot1x vlan dynamic radius-vlan • 下記のコマンドにパラメータを追加しました。 dot1x radius-server host • 下記のコマンド名を変更しました。 aaa authentication dot1x default から aaa authentication dot1x
Web 認証	• 下記のコマンドを追加しました。 aaa accounting web-authentication web-authentication html-fileset web-authentication authentication web-authentication user-group web-authentication user replacement • 下記のコマンドの注意事項を変更しました。 web-authentication force-authorized vlan web-authentication static-vlan force-authorized web-authentication vlan • 下記のコマンドにパラメータを追加しました。 web-authentication radius-server host • 下記のコマンド名を変更しました。 aaa authentication web-authentication default から aaa authentication web-authentication
MAC 認証	• 下記のコマンドを追加しました。 aaa accounting mac-authentication mac-authentication authentication • 下記のコマンドの注意事項を変更しました。 mac-authentication interface mac-authentication force-authorized vlan mac-authentication vlan mac-authentication static-vlan force-authorized • 下記のコマンドにパラメータを追加しました。 mac-authentication radius-server host • 下記のコマンド名を変更しました。 aaa authentication mac-authentication default から aaa authentication mac-authentication
マルチステップ認証	• 下記のコマンドにパラメータを追加しました。 authentication multi-step
CFM	• 本章を追加しました。
SNMP	• 下記のコマンドにパラメータを追加しました。 snmp-server host

章・節・項・タイトル	追加・変更内容
ログ出力機能	• 下記のコマンドを追加しました。 logging syslog-header
コンフィグレーション編集時のエラーメッセージ	• 下記情報を追加しました。 ログインセキュリティと RADIUS 情報 Ring Protocol 情報 CFM 情報 • 下記情報のエラーメッセージを変更しました。 省電力機能情報 イーサネット情報 リングアグリゲーション情報 スパニングツリー情報 IEEE802.1X 情報 Web 認証情報（DHCP サーバ情報含む） MAC 認証情報 アップリンク・リダンダント情報

【Ver. 2.1（第 2 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
コンフィグレーションの編集と操作	• 下記のコマンドに応答メッセージを追加しました。 end exit
ログインセキュリティと RADIUS	• 下記のコマンドの説明を変更しました。 radius-server dead-interval radius-server host radius-server key radius-server retransmit radius-server timeout
時刻の設定と NTP	• 下記のコマンドの注意事項を変更しました。 clock timezone
省電力機能	• 下記のコマンドを追加しました。 power-control port cool-standby schedule-power-control port cool-standby schedule-power-control port-led schedule-power-control shutdown interface schedule-power-control system-sleep schedule-power-control time-range system fan-control system port-led trigger console system port-led trigger interface system port-led trigger mc • 下記のコマンドの説明を変更しました。 system port-led
イーサネット	• 下記のコマンドの注意事項を変更しました。 shutdown
MAC アドレステーブル	• 下記のコマンドの注意事項を変更しました。 mac-address-table aging-time mac-address-table static
VLAN	• 下記のコマンドの注意事項を変更しました。 switchport mac switchport mode vlan
IGMP snooping	• 下記のコマンドの説明を変更しました。 ip igmp snooping mrouter

章・節・項・タイトル	追加・変更内容
MLD snooping	• 下記のコマンドの説明を変更しました。 ipv6 mld snooping source ipv6 mld snooping mrouter
レイヤ 2 認証共通	• 本章を移動しました。 • 下記のコマンドを追加しました。 authentication force-authorized enable authentication force-authorized vlan
IEEE802.1X	• 下記のコマンドを追加しました。 dot1x auto-logout dot1x radius-server dead-interval dot1x radius-server host • 下記のコマンドにパラメータを追加しました。 dot1x supplicant-detection • 下記のコマンドの注意事項を変更しました。 dot1x force-authorized dot1x force-authorized eapol dot1x force-authorized vlan dot1x port-control dot1x vlan dynamic enable dot1x vlan dynamic radius-vlan
Web 認証	• 下記のコマンドを追加しました。 web-authentication radius-server dead-interval web-authentication radius-server host • 下記のコマンドにパラメータを追加しました。 aaa authentication web-authentication default • 下記のコマンドの注意事項を変更しました。 web-authentication force-authorized vlan web-authentication static-vlan force-authorized web-authentication vlan
MAC 認証	• 下記のコマンドを追加しました。 mac-authentication radius-server dead-interval mac-authentication radius-server host • 下記のコマンドにパラメータを追加しました。 aaa authentication mac-authentication default • 下記のコマンドの注意事項を変更しました。 mac-authentication force-authorized vlan mac-authentication interface mac-authentication static-vlan force-authorized mac-authentication timeout quiet-period mac-authentication vlan
マルチステップ認証	• 本章を追加しました。
セキュア Wake on LAN【OP-WOL】	• 下記のコマンドの注意事項を変更しました。 http-server
アップリンク・リダンダント	• 下記のコマンドを追加しました。 switchport backup mac-address-table update transmit switchport backup mac-address-table update exclude-vlan switchport backup mac-address-table update retransmit
ストームコントロール	• 下記のコマンドにパラメータを追加しました。 storm-control

章・節・項・タイトル	追加・変更内容
ポートミラーリング	• 下記のコマンドの注意事項を変更しました。 monitor session
コンフィグレーション編集時のエラーメッセージ	• 下記情報を追加しました。 省電力機能情報 マルチステップ認証情報 ストームコントロール情報 • 下記情報のエラーメッセージを変更しました。 リンクアグリゲーション情報 MAC アドレステーブル情報 VLAN 情報 IGMP snooping 情報 MLD snooping 情報 レイヤ 2 認証共通情報 IEEE802.1X 情報 Web 認証情報（DHCP サーバ情報含む） MAC 認証情報 アップリンク・リダンダント情報 ポートミラーリング情報

はじめに

■対象製品およびソフトウェアバージョン

このマニュアルは次に示すモデル，ソフトウェアでサポートする機能を対象に記載しています。

- IP8800/S2200：Ver.2.7　OS-LT4，オプションライセンス
- IP8800/S2100：Ver.2.7　OS-LT5　（オプションライセンス未サポート）
- IP8800/SS1250：Ver.2.7　OS-LT3，オプションライセンス
- IP8800/SS1240：Ver.2.7　OS-LT2，オプションライセンス

操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

なお，このマニュアルでは特に断らないかぎり IP8800/S2200，IP8800/S2100，IP8800/SS1250，IP8800/SS1240 に共通の機能について記載しますが，機種固有の機能については以下のマークで示します。

【S2200】：

IP8800/S2200 についての記述です。

【S2100】：

IP8800/S2100 についての記述です。

【SS1250】：

IP8800/SS1250 についての記述です。

【SS1240】：

IP8800/SS1240 についての記述です。

また，このマニュアルでは特に断らないかぎり OS-LT5，OS-LT4，OS-LT3，OS-LT2 の機能について記載しますが，オプションライセンスの機能については以下のマークで示します。

【OP-WOL】：

オプションライセンス OP-WOL でサポートする機能です。

【OP-OTP】：

オプションライセンス OP-OTP でサポートする機能です。

■このマニュアルの訂正について

このマニュアルに記載の内容は，ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

■対象読者

本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

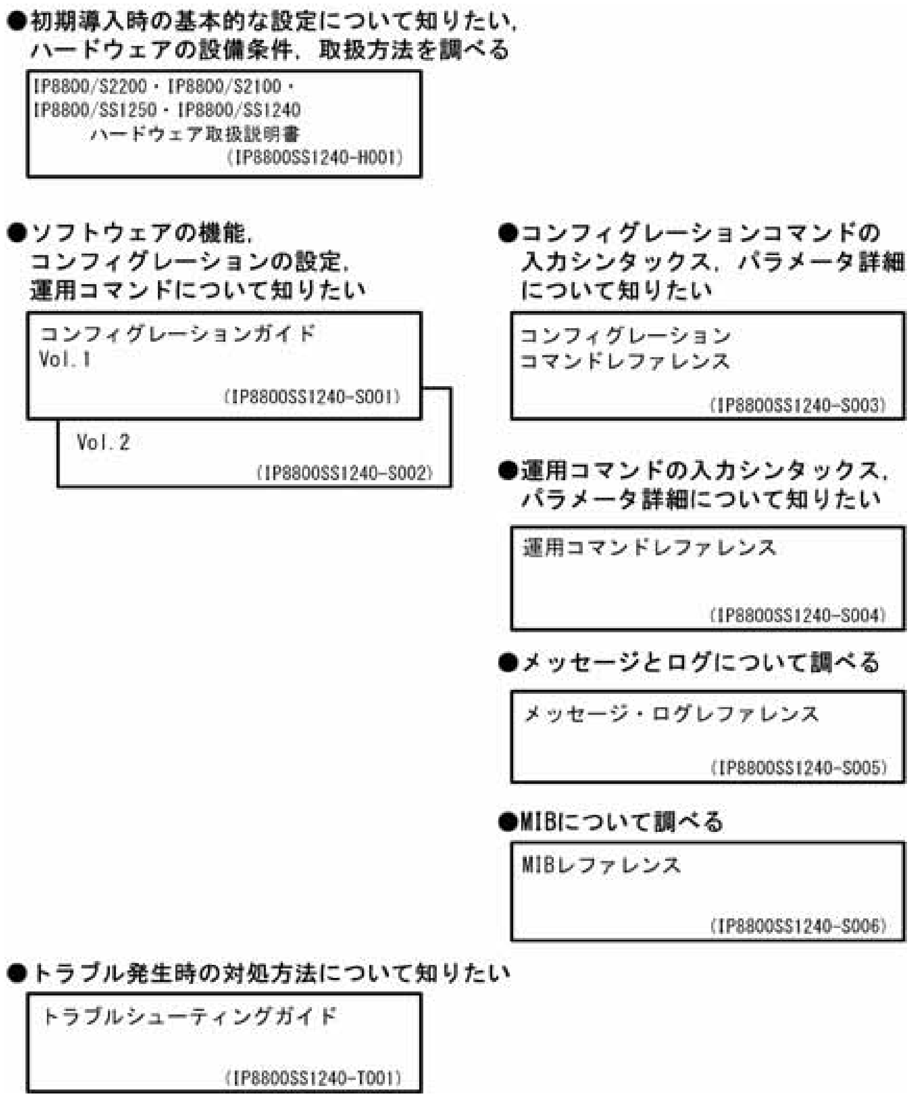
■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。

https://jpn.nec.com/ip88n/

■マニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。



■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second　　*bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System

CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol

NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second　　*ppsと表記する場合もあります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
ULR	Uplink Redundant
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station

WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■ kB(バイト) などの単位表記について

1kB(キロバイト)，1MB(メガバイト)，1GB(ギガバイト)，1TB(テラバイト) はそれぞれ 1024 バイト，1024^2 バイト，1024^3 バイト，1024^4 バイトです。

目次

第 1 編　このマニュアルの読み方

第 2 編　運用管理

第 5 編　IPv4 パケット中継

第 6 編　フィルタ・QoS

第 7 編　レイヤ 2 認証

第 8 編　セキュリティ

第 9 編　冗長化構成による高信頼化機能

第 10 編　ネットワークの障害検出による高信頼化

第 11 編　リモートネットワーク管理

第 12 編　隣接装置の管理

第 13 編　ポートミラーリング

第 14 編　コンフィグレーションエラーメッセージ

1 このマニュアルの読み方

コマンドの記述形式

各コマンドは以下の形式に従って記述しています。

[機能]

コマンドの使用用途を記述しています。

[入力形式]

コマンドの入力形式を定義しています。この入力形式は，次の規則に基づいて記述しています。

1. 値や文字列を設定するパラメータは，＜＞で囲みます。
2. ＜＞で囲まれていない文字はキーワードで，そのまま入力する文字です。
3. ｛A ｜ B｝は，「A または B のどちらかを選択」を意味します。
4. ［］で囲まれたパラメータやキーワードは「省略可能」を意味します。
5. パラメータの入力形式を，「パラメータに指定できる値」に示します。

[入力モード]

コマンドを入力できる入力モードをプロンプトに表示する名称で記述しています。

[パラメータ]

コマンドで設定できるパラメータを詳細に説明しています。パラメータごとに省略時の初期値と値の設定範囲を明記しています。

[コマンド省略時の動作]

コマンドを入力しなくてもパラメータの初期値や動作が設定される場合に，その内容を記述しています。

[通信への影響]

コマンドの設定により通信が途切れるなど通信に影響がある場合，本欄に記述しています。

[設定値の反映契機]

メモリ上のコンフィグレーション情報を変更した場合，すぐに変更後の値で運用開始するか，または装置の再起動など運用を一時的に停止しないと変更が反映されないかを記述しています。

[注意事項]

コマンドを使用する上での注意点について記述しています。

[関連コマンド]

コマンドを動作させるために設定が必要となるコマンドを記述します。

コマンドモード一覧

コマンドモードの一覧を，次の表に示します。

表 1-1　コマンドモード一覧

項番	コマンドモード名	コマンドモード説明	モード移行コマンド
1	(config)	グローバルコンフィグレーションモード	> enable # configure
2	(config-line)	リモートログインの設定	(config)# line vty
3	(config-group)	RADIUS サーバグループの設定	(config)# aaa group server radius
4	(config-if)	インタフェースの設定	(config)# interface
5	(config-if-range)	インタフェースの複数設定	(config)# interface range
6	(config-vlan)	VLAN 設定	(config)# vlan
7	(config-mst)	マルチプルスパニングツリーの設定	(config)# spanning-tree mst configuration
8	(config-axrp)	Ring Protocol の設定	(config)# axrp
9	(config-ext-nacl)	IPv4 パケットフィルタの設定	(config)# ip access-list extended
10	(config-std-nacl)	IPv4 アドレスフィルタの設定	(config)# ip access-list standard
11	(config-ext-macl)	MAC フィルタの設定	(config)# mac access-list extended
12	(config-ip-qos)	IPv4 QoS の設定	(config)# ip qos-flow-list
13	(config-mac-qos)	MAC QoS の設定	(config)# mac qos-flow-list
14	(dhcp-config)	DHCP サーバの設定	(config)# ip dhcp pool
15	(config-auto-cf)	AUTOCONF の設定	(config)# auto-config
16	(config-netconf)	NETCONF の設定	(config)# netconf
17	(config-ether-cfm)	ドメイン名称と MA の設定	(config)# ethernet cfm domain

パラメータに指定できる値

パラメータに指定できる値を，次の表に示します。パラメータ名に制限がない場合，「任意の文字列」を参照してください。

表 1-2　パラメータに指定できる値

パラメータ種別	説明	入力例
任意の文字列	「文字コード一覧」を参照ください。	name "PORT BASED VLAN-1"
アクセスリスト名称 QoS フローリスト名称	「文字コード一覧」を参照ください。 先頭 1 文字目が英字，他は英数字とハイフン（-），アンダースコア（_），ピリオド（.）。 これ以外の文字も入力可能ですが，上記範囲で指定してください。 また，"resequence" と前方一致または完全一致する文字列は指定しないでください。	mac access-list extended list101
QoS キューリスト名称 DHCP アドレスプール名称	「文字コード一覧」を参照ください。 先頭 1 文字目が英字，他は英数字とハイフン（-），アンダースコア（_），ピリオド（.）。 これ以外の文字も入力可能ですが，上記範囲で指定してください。	ip dhcp pool floorA
ホスト名	先頭 1 文字目が英字，他は英数字とハイフン（-），ピリオド（.）で指定できます。	domain name dns DNS-1
MAC アドレス， MAC アドレスマスク	2 バイトずつ 16 進数で表し，この間をドット（.）で区切ります。	1234.5607.08ef 0000.00ff.ffff
IPv4 アドレス， IPv4 ネットマスク	4 バイトを 1 バイトずつ 10 進数で表し，この間をドット（.）で区切ります。	192.168.0.14 255.255.255.0
IPv4 アドレスワイルドカード	IPv4 アドレスと同様の入力形式です。任意のビットを立てると許可を意味します。	255.255.0.0
IPv6 アドレス	2 バイトずつ 16 進数で表し，この間をコロン（:）で区切ります。	3ffe:501:811:ff03::87ff:fed0:c7e0
インタフェース複数指定	複数のインタフェースに関する情報を設定します。 指定できるインタフェースは，fastethernet，gigabitethernet，vlan，port-channel です。 fastethernet と gigabitethernet を混在して指定することはできません。 入力形式は次のとおりです。 • fastethernet の場合 interface range fastethernet <IF# list> • gigabitethernet の場合 interface range gigabitethernet <IF# list> • vlan の場合 interface range vlan <VLAN ID list> • port-channel の場合 interface range port-channel <Channel group# list>	interface range fastethernet 0/1-3 interface range gigabitethernet 0/25-26 interface range vlan 1-100

パラメータ種別	説明	入力例
add /remove 指定	複数指定の設定済み情報に対して，追加または削除をします。 add 指定の場合，設定済みの情報に追加をします。 remove 指定の場合，設定済みの情報から削除をします。 add /remove 指定時，show コマンドで表示される情報が重複している場合には，重複している情報を削除して情報の最適化を行います。 複数指定の情報に対する最適化の例を次に示します。 • コマンド入力前の情報： switchport trunk allowed vlan 100,101 • 入力コマンド： switchport trunk allowed vlan add 103 • コマンド入力後の情報： switchport trunk allowed vlan 100,101,103	switchport trunk allowed vlan add 100,200-210 switchport trunk allowed vlan remove 100,200-210 switchport isolation interface add fastethernet 0/1-3 switchport isolation interface add gigabitethernet 0/25-26 switchport isolation interface remove fastethernet 0/1-3 switchport isolation interface remove gigabitethernet 0/25-26

■ <IF#> の範囲

パラメータ <IF#> は "NIF No./Port No." の形式で指定します。本装置の "NIF No." は 0 固定です。

<IF#> の値の範囲を次の表に示します。

表 1-3　<IF#> の値の範囲【S2200】

項番	モデル	イーサネット種別	値の範囲
1	IP8800/S2230-24T,IP8800/S2230-24P	gigabitethernet	0/1 ～ 0/28

表 1-4　<IF#> の値の範囲【S2100】

項番	モデル	イーサネット種別	値の範囲
1	IP8800/S2130-24T,IP8800/S2130-24P	gigabitethernet	0/1 ～ 0/28

表 1-5　<IF#> の値の範囲【SS1250】

項番	モデル	イーサネット種別	値の範囲
1	IP8800/SS1250-24T2C	fastethernet	0/1 ～ 0/24
		gigabitethernet	0/25 ～ 0/26

表 1-6　<IF#> の値の範囲【SS1240】

項番	モデル	イーサネット種別	値の範囲
1	IP8800/SS1240-24T2C,IP8800/SS1240-24P2C	fastethernet	0/1 ～ 0/24
		gigabitethernet	0/25 ～ 0/26
2	IP8800/SS1240-48T2C	fastethernet	0/1 ～ 0/48
		gigabitethernet	0/49 ～ 0/50

■ <IF# list> の指定方法と設定値の範囲

パラメータの入力形式に，<IF# list> と記載されている場合，<IF#> の形式でハイフン（-），コンマ（,）を使用して複数の fastethernet インタフェースおよび gigabitethernet インタフェースを設定できます。

また，<IF#> と記載されている場合と同様に一つの fastethernet インタフェースおよび gigabitethernet インタフェースを設定できます。設定値の範囲は，前述の <IF#> の範囲に従います。

［"-" または "," による範囲指定の例］
0/1-3,0/5

■ <VLAN ID> の設定値の範囲

<VLAN ID> の値の範囲を次の表に示します。

表 1-7　<VLAN ID> の値の範囲

項番	値の範囲
1	1 ～ 4094

■ <VLAN ID list> の指定方法と設定値の範囲

パラメータの入力形式に <VLAN ID list> と記載されている場合，ハイフン（-），コンマ（,）を使用して複数の VLAN ID を設定できます。また，<VLAN ID> と記載されている場合と同様に一つの VLAN ID を設定できます。設定値の範囲は，前述の <VLAN ID> の範囲に従います。

［"-" または "," による範囲設定の例］
1-3,5,10

■ <Channel group#> の設定値の範囲

<Channel group#> の値の範囲を次の表に示します。

表 1-8　<Channel group#> の値の範囲

項番	モデル	値の範囲
1	全モデル共通	1 ～ 8

■ <Channel group# list> の指定方法と設定値の範囲

パラメータの入力形式に，<Channel group# list> と記載されている場合，ハイフン（-）, コンマ（,）を使用して複数のチャネルグループ番号を設定できます。また，<Channel group#> と記載されている場合と同様に一つのチャネルグループ番号を設定できます。設定値の範囲は，前述の <Channel group#> の範囲に従います。

［"-" または "," による範囲設定の例］
1-3,5

文字コード一覧

文字コード一覧を次の表に示します。

下記文字コード内の英数字以外の文字を特殊文字とします。

表 1-9　文字コード一覧

文字	コード	文字	コード	文字	コード	文字	コード	文字	コード	文字	コード
スペース	0x20 ※1	0	0x30	@	0x40	P	0x50	`	0x60	p	0x70
!	0x21	1	0x31	A	0x41	Q	0x51	a	0x61	q	0x71
"	0x22 ※2	2	0x32	B	0x42	R	0x52	b	0x62	r	0x72
#	0x23	3	0x33	C	0x43	S	0x53	c	0x63	s	0x73
$	0x24	4	0x34	D	0x44	T	0x54	d	0x64	t	0x74
%	0x25	5	0x35	E	0x45	U	0x55	e	0x65	u	0x75
&	0x26	6	0x36	F	0x46	V	0x56	f	0x66	v	0x76
'	0x27	7	0x37	G	0x47	W	0x57	g	0x67	w	0x77
(	0x28	8	0x38	H	0x48	X	0x58	h	0x68	x	0x78
)	0x29	9	0x39	I	0x49	Y	0x59	i	0x69	y	0x79
*	0x2A	:	0x3A	J	0x4A	Z	0x5A	j	0x6A	z	0x7A
+	0x2B	;	0x3B	K	0x4B	[	0x5B	k	0x6B	{	0x7B
,	0x2C	<	0x3C	L	0x4C	¥	0x5C	l	0x6C	|	0x7C
-	0x2D	=	0x3D	M	0x4D	]	0x5D	m	0x6D	}	0x7D
.	0x2E	>	0x3E	N	0x4E	^	0x5E	n	0x6E	~	0x7E
/	0x2F	?	0x3F ※1	O	0x4F	_	0x5F	o	0x6F	---	---

注※1　文字列として入力するためには，ダブルクォート（"）で文字列全体を囲む必要があります。
注※2　文字列全体を囲むために用います。文字列として入力することはできません。

2 運用端末接続

ftp-server

リモート運用端末から ftp プロトコルを使用したアクセスを許可するために使用します。なお，本装置へログインを許可または拒否するリモート運用端末の IPv4 アドレスを設定する場合は，config-line モードで telnet アクセスと共通のアクセスリストを設定してください。

[入力形式]

情報の設定

ftp-server

情報の削除

no ftp-server

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

ftp プロトコルでのリモートアクセスを受け付けません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

config-line モードでアクセスリストを設定している場合，ftp で本装置へログインを許可または拒否するリモート運用端末の IPv4 アドレスも同じアクセスリストに従って制限されます。

[関連コマンド]

line vty

ip access-group

line vty

装置への telnet リモートアクセスを許可します。また，装置に同時にリモートログインできるユーザ数を制限するためにも使用します。

[入力形式]

情報の設定・変更

line vty <Start allocation> <End allocation>

情報の削除

no line vty

[入力モード]

(config)

[パラメータ]

<Start allocation>

リモートログイン許可を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0（固定）

<End allocation>

ログインできるユーザ数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 1（ログインできるユーザ数を 1 ～ 2 に設定できます。）

[コマンド省略時の動作]

telnet プロトコルでのリモートアクセスを受け付けません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本設定を行うと，すべてのリモート運用端末からの telnet プロトコルでのリモートアクセスを受け付けるようになります。アクセスを制限する場合は，ip access-group，transport input 設定をしてください。
2. 同時にログインできるユーザ数を変更しても，すでにログインしているユーザのセッションが切れることはありません。本設定以降にリモートログインするユーザに対して有効となります。

[関連コマンド]

transport input

line vty

ip access-group

transport input

リモート運用端末から各種プロトコルを使用したアクセスを制限するために使用します。

[入力形式]

情報の設定・変更

transport input {telnet | all | none}

情報の削除

no transport input

[入力モード]

(config-line)

[パラメータ]

{telnet | all | none}

telnet

telnet プロトコルでのリモートアクセスを受け付けます。

all

すべてのプロトコルでのリモートアクセスを受け付けます（現在 telnet だけ）。

none

すべてのプロトコルでのリモートアクセスを受け付けません。

1. 本パラメータ省略時の初期値
   all（telnet でのリモートアクセスを受け付けます）
2. 値の設定範囲
   telnet，all，または none

[コマンド省略時の動作]

telnet プロトコルでのリモートアクセスを受け付けます。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ftp 接続を許可／制限する場合は，グローバルコンフィグレーションモードの ftp-server で設定してください。

[関連コマンド]

line vty

ftp-server

ip access-group

3 コンフィグレーションの編集と操作

end

コンフィグレーションコマンドモードを終了して，装置管理者モードに戻ります。

[入力形式]

end

[パラメータ]

なし

[応答メッセージ]

end コマンドの応答メッセージを次の表に示します。

表 3-1　end コマンド応答メッセージ

メッセージ	内容
Unsaved changes would be lost when the machine goes to sleep! Do you exit "configure" without save ? (y/n):	下記コマンドを設定しているときに，コンフィグレーションの編集状態を保存せずに終了しようとしています。 • schedule-power-control system-sleep • schedule-power-control time-range 変更したコンフィグレーションはスリープ状態に遷移すると消失します。"y" で編集状態を終了します。"n" で end コマンドを中止します。必要ならば，save コマンドで変更したコンフィグレーションを保存してください。
The machine is just going to sleep! Do you exit ? (y/n):	コンフィグレーションコマンドモードを終了するとスリープ状態に遷移します。 "y" でスリープ状態に遷移します。スリープ状態に遷移したくない場合は "n" で end コマンドを中止し，"(config)# $set power-control schedule disable" コマンドで省電力スケジュール機能を抑止モードにしてください。

[注意事項]

1. コンフィグレーションファイルを内蔵フラッシュメモリに保存しないで end コマンドを使って一時的にコンフィグレーションコマンドモードを終了することができます。このとき，コンフィグレーションファイルは編集途中の状態のままになっていますので，コンフィグレーションの編集後，保存してください。
2. ランニングコンフィグレーションを編集した後，内蔵フラッシュメモリに保存しないで end コマンドを実行した場合，内蔵フラッシュメモリのスタートアップコンフィグレーションファイルとランニングコンフィグレーションが異なります。コンフィグレーションの編集後，保存してください。

[関連コマンド]

なし

exit

モードを一つ戻ります。グローバルコンフィグレーションモードで編集中の場合はコンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。第二階層以下で編集している場合は一つ上位階層に戻ります。

[入力形式]

exit

[パラメータ]

なし

[応答メッセージ]

exit コマンドの応答メッセージを次の表に示します。

表 3-2　exit コマンド応答メッセージ

メッセージ	内容
Unsaved changes would be lost when the machine goes to sleep! Do you exit "configure" without save ? (y/n):	下記コマンドを設定しているときに，コンフィグレーションの編集状態を保存せずに終了しようとしています。 • schedule-power-control system-sleep • schedule-power-control time-range 変更したコンフィグレーションはスリープ状態に遷移すると消失します。"y" で編集状態を終了します。"n" で exit コマンドを中止します。必要ならば，save コマンドで変更したコンフィグレーションを保存してください。
The machine is just going to sleep! Do you exit ? (y/n):	コンフィグレーションコマンドモードを終了するとスリープ状態に遷移します。 "y" でスリープ状態に遷移します。スリープ状態に遷移したくない場合は "n" で exit コマンドを中止し，"(config)# $set power-control schedule disable" コマンドで省電力スケジュール機能を抑止モードにしてください。

[注意事項]

グローバルコンフィグレーションモードで exit コマンドを使用する場合は，次に示す注意事項があります。

1. コンフィグレーションファイルを内蔵フラッシュメモリに保存しないで exit コマンドを使って一時的にコンフィグレーションコマンドモードを終了することができます。このとき，コンフィグレーションファイルは編集途中の状態のままになっていますので，コンフィグレーションの編集後，保存してください。
2. ランニングコンフィグレーションを編集した後，内蔵フラッシュメモリに保存しないで exit コマンドを実行した場合，内蔵フラッシュメモリのスタートアップコンフィグレーションファイルとランニングコンフィグレーションが異なります。コンフィグレーションの編集後，保存してください。

[関連コマンド]

なし

save(write)

編集したコンフィグレーションの内容を，スタートアップコンフィグレーションファイルへ保存します。

[入力形式]

save

write

[パラメータ]

なし

[応答メッセージ]

なし

[注意事項]

1. コンフィグレーションファイルを保存してもコンフィグレーションコマンドモードは終了しません。編集を終える場合は必ず exit コマンドまたは end コマンドを使ってコンフィグレーションコマンドモードを終了してください。
2. MC 運用モードが有効の場合に本コマンドを実行したときは，運用コマンド update mc-configuration の処理も自動的に実行されます。そのため，運用コマンド update mc-configuration に対応する運用ログが採取されます。運用ログの詳細は「メッセージ・ログレファレンス」を参照してください。
   なお，運用コマンド update mc-configuration の処理でエラーが検出された場合でも，本コマンドは正常終了しています。【S2100】

[関連コマンド]

なし

show

編集中のコンフィグレーションを画面に表示します。

[入力形式]

show [<Command> [<Parameter>]]

[パラメータ]

<Command>
　コンフィグレーションコマンドを指定します。

`<Parameter>`
　表示対象を限定する場合にパラメータを指定します。

[注意事項]

1. コンフィグレーションが多い場合，コマンドの実行に時間が掛かることがあります。
2. グローバルコンフィグレーションモードでは，コンフィグレーションモード（第二階層）へ遷移するコマンドに対して <Command> [<Parameter>] が指定できます。補完機能・ヘルプ機能・短縮実行なども使用可能です。
3. コンフィグレーションモード（第二階層）では，グローバルコンフィグレーションモードと同様にモードを遷移するコマンドに対して <Command> [<Parameter>] の指定ができますが，補完機能・ヘルプ機能などは使用できません。

[関連コマンド]

なし

top

コンフィグレーションコマンドモード移行後は，本コマンド入力でグローバルコンフィグレーションモード（第一階層）に戻ります。

[入力形式]

top

[パラメータ]

なし

[注意事項]

なし

[関連コマンド]

なし

4 ログインセキュリティと RADIUS

aaa group server radius

RADIUS サーバグループを設定します。本コマンドを入力すると，config-group モードに移行し，RADIUS サーバグループ情報を設定できます。

[入力形式]

情報の設定・変更

aaa group server radius <Group name>

情報の削除

no aaa group server radius <Group name>

[入力モード]

(config)

[パラメータ]

<Group name>

RADIUS サーバグループ名を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で設定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。
   先頭文字は大文字を推奨します。
   ただし，下記の文字列は設定できません。
   ・radius(前方一致または完全一致した文字列)
   ・tacacs+(前方一致または完全一致した文字列)

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. RADIUS サーバグループに有効な RADIUS サーバが設定されていない場合は，動作しません。
2. 設定可能な RADIUS サーバグループは最大 4 です。

[関連コマンド]

aaa authentication

dot1x authentication

mac-authentication authentication

web-authentication authentication

web-authentication user-group

aaa authentication login

リモートログイン時に使用する認証方式を設定します。先に設定した認証に失敗した場合は，次に設定した方式で認証を行います。なお，この認証失敗時の動作は aaa authentication login end-by-reject コマンドで変更できます。

[入力形式]

情報の設定・変更

aaa authentication login default <Method> [<Method>]

情報の削除

no aaa authentication login

[入力モード]

(config)

[パラメータ]

default <Method> [<Method>]

<Method> には次を設定します。同一の Method は複数設定できません。

group radius

RADIUS 認証を使用します。

使用する RADIUS サーバは汎用 RADIUS サーバです。

local

ローカルパスワード認証を使用します。

group <Group name>

RADIUS 認証を使用します。

使用する RADIUS サーバは RADIUS サーバグループです。aaa group server radius コマンドで設定したグループ名を指定してください。

ただし，下記の文字列は設定できません。

・radius(前方一致または完全一致した文字列)

・tacacs+(前方一致または完全一致した文字列)

[コマンド省略時の動作]

ローカルパスワード認証を行います。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 認証方式に "group radius" または "group <Group name>" を指定する場合，RADIUS サーバと通信不可または RADIUS サーバでの認証に失敗すると，本装置にログインできなくなります。このため，ローカルパスワード認証を一緒に指定することをお勧めします。

2. group radius（汎用 RADIUS サーバ認証）と group <Group name>（RADIUS サーバグループ認証）は，どちらも RADIUS 認証サービスとして扱いますので，両方を同時に指定できません。どちらか一つとローカルパスワード認証を組み合わせてご使用ください。

［関連コマンド］

radius-server

aaa authentication login end-by-reject

aaa authentication login end-by-reject

ログイン時の認証で否認された場合に，認証を終了します。通信不可（RADIUS 無応答など）による認証失敗時は，aaa authentication login コマンドで次に指定されている認証方式で認証します。

[入力形式]

情報の設定

aaa authentication login end-by-reject

情報の削除

no aaa authentication login end-by-reject

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

認証で否認された場合に，その理由にかかわらず aaa authentication login コマンドで次に指定されている認証方式で認証します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. aaa authentication login コマンドで指定した認証方式にだけ有効です。

[関連コマンド]

aaa authentication login

ip access-group

本装置へリモートログインを許可または拒否するリモート運用端末の IPv4 アドレスを設定したアクセスリストを設定します。本設定は，全リモートアクセス（telnet ／ ftp）で共通になります。

16 エントリになるまで複数行設定できます。

[入力形式]

情報の設定・変更

ip access-group <ACL ID> in

情報の削除

no ip access-group <ACL ID>

[入力モード]

(config-line)

[パラメータ]

<ACL ID>

IPv4 アドレスフィルタの識別子（ip access-list standard の識別子）を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 〜 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

すべてのリモート運用端末からのアクセスを許可します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本設定は，全リモートアクセス（telnet ／ ftp）で共通になります。
2. ftp 接続を許可する場合は，ftp-server を設定してください。
3. ip access-group が設定されていない場合，すべてのリモート運用端末からのアクセスを許可します。
4. アクセスを許可する IP アドレスを変更しても，すでにログインしているユーザのセッションが切れることはありません。本設定以降にリモートログインするユーザに対して有効となります。

［関連コマンド］

ip access-list standard

line vty

ftp-server

transport input

radius-server attribute station-id capitalize

RADIUS サーバへ送信時に使用する RADIUS 属性の MAC アドレスを大文字で送信します。該当する RADIUS 属性名は以下のとおりです。

- Called-Station-Id
- Calling-Station-Id

[入力形式]

情報の設定
　radius-server attribute station-id capitalize

情報の削除
　no radius-server attribute station-id capitalize

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

RADIUS 属性の MAC アドレスを小文字で送信します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンド設定は認証要求，アカウンティング要求に反映されます。
2. 全認証（IEEE802.1X，Web 認証，MAC 認証）共通です。
3. MAC 認証で使用する RADIUS 属性「User-Name」「User-Password」の MAC アドレスは，mac-authentication id-format コマンドに従います。

[関連コマンド]

なし

radius-server dead-interval

汎用 RADIUS サーバがプライマリ汎用 RADIUS サーバへ自動復旧するまでの監視タイマを設定します。

カレントサーバ（運用中の RADIUS 認証要求先）が有効なセカンダリ汎用 RADIUS サーバへ遷移した時点，または全サーバ使用不可状態で監視タイマをスタートし，本コマンドによる設定時間経過後（監視タイマ満了後）に，プライマリ汎用 RADIUS サーバへ復旧します。

[入力形式]

情報の設定・変更

radius-server dead-interval <Minutes>

情報の削除

no radius-server dead-interval

[入力モード]

(config)

[パラメータ]

<Minutes>

セカンダリ汎用 RADIUS サーバから，プライマリ汎用 RADIUS サーバへ自動復旧するまでの監視タイマを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 1440（分）
   0 を設定した場合は，RADIUS 認証要求を必ずプライマリ汎用 RADIUS サーバから開始します。

[コマンド省略時の動作]

カレントサーバがセカンダリ汎用 RADIUS サーバへ遷移して 10 分後，プライマリ汎用 RADIUS サーバに自動復旧します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

1. セカンダリ汎用 RADIUS サーバをカレントサーバとして運用中に監視タイマ値を変更した場合，その時点での経過状態を判定し結果を反映します。
2. 監視タイマをスタート後に本コマンド設定を削除した場合，監視タイマのカウントはリセットせずに継続し，デフォルト値 10 分として動作します。

[注意事項]

1. ３台以上の汎用 RADIUS サーバを設定していた場合，監視タイマをスタート後に他の汎用 RADIUS サーバへカレントサーバが遷移した場合でも，監視タイマはリセットせずに継続します。
2. 監視タイマはいったんスタートすると基本的に満了するまでリセットしませんが，下記の契機では例外として満了せずにリセットします。

- 本コマンドで radius-server dead-interval 0 を設定したとき
- カレントサーバとして運用中の汎用 RADIUS サーバ情報を，radius-server host コマンドで削除したとき
- 運用コマンド clear radius-server を実行したとき

3. 認証対象端末の認証シーケンス実施中に監視タイマが満了した場合でも，実施中の認証シーケンスが完了するまでプライマリ汎用 RADIUS サーバへの復旧は行なわれません。

［関連コマンド］

aaa authentication

radius-server host

radius-server key

radius-server retransmit

radius-server timeout

radius-server host

認証に使用する汎用 RADIUS サーバの設定を行います。

[入力形式]

情報の設定・変更

radius-server host <IP address> [auth-port <Port>] [acct-port <Port>] [timeout <Seconds>] [retransmit <Retries>] [key <String>]

情報の削除

no radius-server host <IP address>

[入力モード]

(config)

[パラメータ]

<IP address>

RADIUS サーバの IPv4 アドレスを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   IPv4 アドレス（ドット記法）を設定します。
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

key <String>

RADIUS サーバ間との通信の暗号化／認証に使用する RADIUS 鍵を指定します。RADIUS 鍵はクライアント上と RADIUS サーバ上で同一の鍵を設定する必要があります。

1. 本パラメータ省略時の初期値
   radius-server key で設定されている RADIUS 鍵が使用されます。設定されていない場合，当該 RADIUS サーバは無効になります。
2. 値の設定範囲
   64 文字以内の文字列で設定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

auth-port <Port>

RADIUS サーバのポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1812 を使用します。
2. 値の設定範囲
   1 ～ 65535

acct-port <Port>

RADIUS サーバのアカウンティング用ポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1813 を使用します。
2. 値の設定範囲
   1 ～ 65535

retransmit <Retries>

RADIUS サーバに対して認証要求を再送信する回数を指定します。

1. 本パラメータ省略時の初期値
   radius-server retransmit で設定されている回数が使用されます。設定されていない場合の初期値は 3 回です。
2. 値の設定範囲
   0 ～ 15（回）

timeout <Seconds>

RADIUS サーバからの応答タイムアウト時間（秒）を指定します。

1. 本パラメータ省略時の初期値
   radius-server timeout で設定されている時間が使用されます。設定されていない場合の初期値は 5 秒です。
2. 値の設定範囲
   1 ～ 30（秒）

[コマンド省略時の動作]

RADIUS サーバが設定されないため，aaa で group radius を設定しても RADIUS 通信しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 設定可能な汎用 RADIUS サーバ数は装置単位で最大 20 です。
2. IPv4 アドレスとして 127.*.*.* を設定できません。
3. key パラメータが省略されていて，radius-server key コマンドも設定されていない場合は，当該 RADIUS サーバは無効になります。
4. 複数の汎用 RADIUS サーバを設定した場合，運用コマンド show radius-server で最初に表示されるアドレスがプライマリ汎用 RADIUS サーバとなります。最初のカレントサーバ（運用中の RADIUS 認証要求先）にはプライマリ汎用 RADIUS サーバが使用されます。
   プライマリ汎用 RADIUS サーバに障害が発生した場合，カレントサーバは次に有効な汎用 RADIUS サーバ（セカンダリ汎用 RADIUS サーバ）へ遷移します。プライマリ汎用 RADIUS サーバへの自動復旧については radius-server dead-interval コマンドを参照してください。
5. 汎用 RADIUS サーバ，認証専用 RADIUS サーバ，または RADIUS サーバグループの設定で，IP アドレスの一致する RADIUS サーバが既に登録されている場合は，それらすべてのパラメータを自動的に新しく入力したコマンド内容に置き換えます。

[関連コマンド]

aaa authentication

radius-server dead-interval

radius-server key

radius-server retransmit

radius-server timeout

radius-server key

汎用 RADIUS サーバ，または各認証専用 RADIUS サーバとの認証に使用する RADIUS サーバ鍵のデフォルトを設定します。

[入力形式]

情報の設定・変更
　radius-server key <String>

情報の削除
　no radius-server key

[入力モード]

(config)

[パラメータ]

<String>
　RADIUS サーバ間との通信の暗号化／認証に使用する RADIUS 鍵を指定します。RADIUS 鍵はクライアント上と RADIUS サーバ上で同一の鍵を設定する必要があります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   64 文字以内の文字列で設定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. radius-server host，dot1x radius-server host，mac-authentication radius-server host，web-authentication radius-server host での key 設定を本設定より優先して使用します。

[関連コマンド]

aaa authentication

dot1x radius-server host

mac-authentication radius-server host

radius-server host

radius-server retransmit

radius-server timeout

web-authentication radius-server host

radius-server retransmit

認証に使用する汎用 RADIUS サーバ，または各認証専用 RADIUS サーバへの再送回数のデフォルトを設定します。

[入力形式]

情報の設定・変更

radius-server retransmit <Retries>

情報の削除

no radius-server retransmit

[入力モード]

(config)

[パラメータ]

<Retries>

RADIUS サーバに対して認証要求を再送信する回数を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 〜 15（回）

[コマンド省略時の動作]

RADIUS サーバへの再送回数のデフォルト値は 3 回となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. radius-server host，dot1x radius-server host， mac-authentication radius-server host, web-authentication radius-server host での retransmit 設定を本設定より優先して使用します。

[関連コマンド]

aaa authentication

dot1x radius-server host

mac-authentication radius-server host

radius-server host

radius-server key

radius-server timeout

web-authentication radius-server host

radius-server timeout

認証に使用する汎用 RADIUS サーバ，または各認証専用 RADIUS サーバの応答タイムアウト値のデフォルトを設定します。

[入力形式]

情報の設定・変更
radius-server timeout <Seconds>

情報の削除
no radius-server timeout

[入力モード]

(config)

[パラメータ]

<Seconds>

RADIUS サーバからの応答タイムアウト時間を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 30（秒）

[コマンド省略時の動作]

RADIUS サーバの応答タイムアウトのデフォルト値は 5 秒となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. radius-server host，dot1x radius-server host， mac-authentication radius-server host，web-authentication radius-server host での timeout 設定を本設定より優先して使用します。

[関連コマンド]

aaa authentication

dot1x radius-server host

mac-authentication radius-server host

radius-server host

radius-serve key

radius-server retransmit

web-authentication radius-server host

server

RADIUS サーバグループの RADIUS サーバホストを設定します。

[入力形式]

情報の設定・変更

server <IP address> [auth-port <Port>] [acct-port <Port>]

情報の削除

no server <IP address>

[入力モード]

(config-group)

[パラメータ]

<IP address>

RADIUS サーバの IPv4 アドレスを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   IPv4 アドレス（ドット記法）を指定します。
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

auth-port <Port>

RADIUS サーバのポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1812 を使用します。
2. 値の設定範囲
   1 ～ 65535

acct-port <Port>

RADIUS サーバのアカウンティング用ポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1813 を使用します。
2. 値の設定範囲
   1 ～ 65535

[コマンド省略時の動作]

RADIUS サーバが設定されないため，RADIUS サーバグループによる通信はしません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 設定可能な RADIUS サーバ数はグループ単位で最大 4 です。

2. IPv4 アドレスとして 127.*.*.* を設定できません。
3. 本コマンドの設定値は，下記の条件をすべて満たしているときに有効です。
   - radius-server host コマンドと同値であること (auth-port，acct-port も同値であること)
   - radius-server host コマンドの設定が有効であること（key パラメータ指定，または radius-server key コマンドが設定済みであること）
4. 同一 RADIUS サーバグループ内で複数の RADIUS サーバを設定した場合，運用コマンド show radius-server で表示されるアドレスが当該 RADIUS サーバグループのプライマリ RADIUS サーバとなります。このプライマリ RADIUS サーバが最初のカレントサーバ（RADIUS 認証要求先）に使用されます。プライマリ RADIUS サーバグループ内の次に有効な RADIUS サーバへ遷移します。
   なお，プライマリ RADIUS サーバへの自動復旧は，radius-server dead-interval コマンドの設定に従います。

[関連コマンド]

aaa group server radius

dot1x authentication

mac-authentication authentication

radius-server host

web-authentication authentication

web-authentication user-group

5 時刻の設定と NTP

clock timezone

タイムゾーンを設定します。

本装置は，内部的に UTC（Coordinated Universal Time）で日時を保持しますので，この設定は，運用コマンドで時刻を表示するときや，set clock で時刻を設定するときだけ影響します。

[入力形式]

情報の設定・変更

clock timezone <Zone name> <Hours offset> [<Minutes offset>]

情報の削除

no clock timezone

[入力モード]

(config)

[パラメータ]

<Zone name>

タイムゾーンを識別する名前を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   7 文字以内の英数字
   （これ以外の文字も入力可能ですが，上記範囲で設定してください）

<Hours offset>

UTC からの時間オフセット（10 進数）を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   -12 ～ -1，0，1 ～ 12

<Minutes offset>

UTC からの分オフセットを設定します。

1. 本パラメータ省略時の初期値
   0
2. 値の設定範囲
   0 ～ 59（10 進数）

[コマンド省略時の動作]

UTC として動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

本装置で収集している統計情報の CPU 使用率は，タイムゾーンが変更された時点で 0 クリアされます。

[関連コマンド]

set clock

ntp client server

時刻情報を取得する NTP サーバアドレスを設定します。最大２エントリを設定できます。

最初に設定されたアドレスをプライマリ，後から設定されたアドレスをセカンダリと呼びます。プライマリの NTP サーバアドレスに対して時刻取得に失敗した場合は，セカンダリの NTP サーバアドレスに対して時刻情報を要求します。

[入力形式]

情報の設定・変更

ntp client server <Server IP>

情報の削除

no ntp client server <Server IP>

[入力モード]

(config)

[パラメータ]

<Server IP>

時刻情報を取得する NTP サーバの IP アドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ntp client server と，ntp client broadcast や ntp client multicast を同時に設定しても， ntp client server の設定が有効になります。
2. IPv4 アドレスとして 127.*.*.* を設定できません。

[関連コマンド]

ntp client broadcast

ntp client multicast

ntp interval

ntp client broadcast

NTP サーバからブロードキャストで送信される時刻情報を受け付ける設定を行います。

[入力形式]

情報の設定

ntp client broadcast

情報の削除

no ntp client broadcast

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

NTP サーバからブロードキャスト送信される時刻情報を受け付けません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

ntp client server と，ntp client broadcast や ntp client multicast を同時に設定しても， ntp client server の設定が有効になります。

[関連コマンド]

ntp client server

ntp client multicast

ntp client multicast

NTP サーバからマルチキャストで送信される時刻情報を受け付ける設定を行います。

[入力形式]

情報の設定
ntp client multicast

情報の削除
no ntp client multicast

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

NTP サーバからマルチキャスト送信される時刻情報を受け付けません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

ntp client server と，ntp client broadcast や ntp client multicast を同時に設定しても， ntp client server の設定が有効になります。

[関連コマンド]

ntp client server

ntp client broadcast

ntp interval

NTP サーバから定期的に時刻情報を取得する実行間隔を設定します。

[入力形式]

情報の設定・変更
　ntp interval <Interval>

情報の削除
　no ntp interval

[入力モード]

(config)

[パラメータ]

<Interval>
　NTP サーバから時刻情報を取得する実行間隔を設定します。設定は秒単位（10 進数）で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   120 ～ 604800（秒）

[コマンド省略時の動作]

NTP サーバからの時刻情報取得の実行間隔は 3600 秒になります。

[通信への影響]

なし

[設定値の反映契機]

ntp client server が設定されている場合，設定値変更後，すぐに運用に反映されます。

[注意事項]

ntp client server が設定されている場合，有効となります。

[関連コマンド]

ntp client server

6 装置の管理

system fan mode

装置 FAN の運転モードを設定します。

[入力形式]

情報の設定
　system fan mode <mode>

情報の削除
　no system fan mode

[入力モード]

(config)

[パラメータ]

<mode>

FAN の運転モード 1 もしくは 2 を指定します。
1：静音重視設定
2：冷却重視設定
1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 および 2

[コマンド省略時の動作]

運転モード 1（静音重視設定）が設定されます。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 装置モデルによって本コマンド設定時の動作が異なります。

表 6-1　装置モデルごとの system fan mode 2（冷却重視）設定時の動作

モデル	FAN 動作種別	コマンド設定時の動作
IP8800/S2230-24T IP8800/S2130-24T IP8800/SS1250-24T2C IP8800/SS1240-24T2C	FAN レス	FAN レス仕様のため，本コマンドを設定しても無効となります。
IP8800/SS1240-48T2C	準 FAN レス	冷却重視を設定時，system fan-control コマンド設定は無効（FAN 速度固定）となります。

モデル	FAN 動作種別	コマンド設定時の動作
IP8800/S2230-24P IP8800/ SS1240-24P2C	FAN 速度固定	コマンド省略時および静音重視設定を指定した場合も冷却重視設定の動作となります。
IP8800/S2130-24P	FAN 速度固定	コマンド省略時および静音重視設定を指定した場合は静音重視設定として動作します。 PoE 給電量によって，冷却 FAN 制御を行います。

［関連コマンド］

system fan-control

system function【SS1250】【SS1240】

IP8800/SS1250・IP8800/SS1240 は，system function コマンド未設定でも全機能を使用可能です。

IP8800/SS1230 とのコンフィグレーション互換のために，IP8800/SS1250・IP8800/SS1240 で system function コマンドを入力可能にしています。

system l2-table mode

レイヤ 2 ハードウェアテーブルの検索方式を設定します。

[入力形式]

情報の設定・変更

system l2-table mode <Mode>

情報の削除

no system l2-table mode

[入力モード]

(config)

[パラメータ]

<Mode>

ハードウェアテーブルに登録する際のテーブル検索方式を選択します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲

1 〜 5

レイヤ 2 ハードウェアテーブルのテーブル検索方式を指定した値で設定します。

auto

自動選択モード※を設定します。

注※　自動選択モードについて

ハードウェアテーブルでハッシュの競合によるハッシュエントリオーバーが発生した場合に，自動的にハードウェアテーブルの検索方式を変更します。

[コマンド省略時の動作]

テーブル検索方式は 1 で動作します。

[通信への影響]

装置の再起動が必要になりますので，再起動が完了するまで本装置を経由する通信は停止します。

自動選択モードの場合は，テーブル検索方式が変更されたときに，フレーム中継，および自宛通信が一時的に停止します。

[設定値の反映契機]

設定値を変更した場合は，コンフィグレーションを保存したあとで，本装置を再起動してください。再起動すると，設定値が運用に反映されます。

なお，no system l2-table mode に変更したときも，装置を再起動するとテーブル検索方式 1 が運用に反映されます。

[注意事項]

1. 本コマンド入力時，下記のメッセージが表示されますので，他のコンフィグレーションコマンドを入力する前に，設定を保存し装置を再起動してください。
   Please execute the reload command after save,
   because this command becomes effective after reboot.

[関連コマンド]

なし

system recovery

no system recovery コマンドを設定することで，障害検出時に，本装置を再起動しないで，障害状態のままにします。

障害の対象と復旧については「コンフィグレーションガイド Vol.1 10. 装置の管理」を参照してください。

[入力形式]

情報の設定

no system recovery

情報の削除

system recovery

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

障害検出時に，装置を再起動します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. システムリカバリー無効時（no system recovery）は自動復旧が停止状態となり，重度障害（FATAL レベルの障害）が発生しても，障害ログ採取後は再起動を実施しません。自動復旧停止状態についての詳細は「コンフィグレーションガイド Vol.1 10. 装置の管理」を参照してください。

[関連コマンド]

なし

system temperature-warning-level

装置の入気温度が指定温度を超過した場合に運用メッセージを出力します。

[入力形式]

情報の設定

system temperature-warning-level <temperature>

情報の削除

no system temperature-warning-level

[入力モード]

(config)

[パラメータ]

<temperature>

温度 (摂氏) を設定します。

1 ℃単位で設定可能です。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   - IP8800/S2230-24P，IP8800/S2130-24P，IP8800/SS1250-24T2C
     25 ～ 50（℃）
   - IP8800/S2230-24T，IP8800/S2130-24T，IP8800/SS1240-24T2C，IP8800/SS1240-24P2C，IP8800/SS1240-48T2C
     25 ～ 45（℃）

[コマンド省略時の動作]

指定温度の超過による運用メッセージを出力しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 以下動作環境条件を満たさない場合は指定した入気温度よりも低い温度でログ出力する場合があります。
   - 換気に配慮し，装置周辺に熱がこもらないこと
   - 装置の重ね置きをしないこと
   - 縦置き設置をしないこと
   - 熱源となるような装置の近くに設置しないこと
2. 装置の入気温度がすでに指定した値を超過している場合は，即座に運用メッセージを出力します。

[関連コマンド]

なし

system temperature-warning-level average

指定期間内の平均温度が指定温度を超えた場合に運用メッセージを出力します。

[入力形式]

情報の設定

system temperature-warning-level average [<temperature>] [period <days>]

情報の削除

no system temperature-warning-level average

[入力モード]

(config)

[パラメータ]

<temperature>

平均温度 (摂氏) を設定します。

1 ℃単位で設定可能です。

1. 本パラメータ省略時の初期値
   - IP8800/SS1250-24T2C
     43（℃）
   - IP8800/S2230-24T，IP8800/S2230-24P，IP8800/S2130-24T，IP8800/S2130-24P，IP8800/SS1240-24T2C，IP8800/SS1240-24P2C，IP8800/SS1240-48T2C
     38（℃）
2. 値の設定範囲
   - IP8800/S2230-24P，IP8800/S2130-24P，IP8800/SS1250-24T2C
     25 ～ 50（℃）
   - IP8800/S2230-24T，IP8800/S2130-24T，IP8800/SS1240-24T2C，IP8800/SS1240-24P2C，IP8800/SS1240-48T2C
     25 ～ 45（℃）

period <days>

平均温度を算出する日数を設定します。

1. 本パラメータ省略時の初期値
   30
2. 値の設定範囲
   1 ～ 30

[コマンド省略時の動作]

指定平均温度の超過による運用メッセージを出力しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

平均温度の閾値確認は，正午または装置起動時に行います。

[注意事項]

1. 以下動作環境条件を満たさない場合は指定した平均温度よりも低い温度でログ出力する場合があります。
   - 換気に配慮し，装置周辺に熱がこもらないこと
   - 装置の重ね置きをしないこと
   - 縦置き設置をしないこと
   - 熱源となるような装置の近くに設置しないこと
2. 装置の平均温度がすでに指定した値を超過していても，次の閾値確認が行われるまで運用メッセージを出力しません。

[関連コマンド]

なし

7

省電力機能

power-control port cool-standby

リンクダウンポートの省電力運用を有効にします。

[入力形式]

情報の設定
power-control port cool-standby

情報の削除
no power-control port cool-standby

[入力モード]
(config)

[パラメータ]

なし

[コマンド省略時の動作]

通常の消費電力で運用します。

[通信への影響]

通信に影響があります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定した場合，Fastethernet ポートのリンクアップに約 3 秒程度かかります。【SS1250】【SS1240】
2. スケジューリングによる省電力機能の動作中は，schedule-power-control port cool-standby コマンドの設定に従い動作します。【SS1250】【SS1240】
3. 本コマンドを設定した場合，Fastethernet 全ポートのリンク状態が変化し，通信に影響します。【SS1250】【SS1240】
4. 速度固定設定または自動 MDIX 機能無効の Fastethernet ポートに関しては , ポート省電力機能は有効になりません。このため，ポート省電力機能を有効にする場合は，オートネゴシエーション有効，自動 MDIX 機能有効 (mdix auto 設定) で運用してください。【SS1250】【SS1240】
5. 1000BASE-X ポートは，リンクダウンポートの省電力機能が未サポートのため，本コマンドを設定しても動作しません。

[関連コマンド]

なし

schedule-power-control port cool-standby

スケジューリングによる省電力運転中のリンクダウンポートの省電力運用動作を設定します。

[入力形式]

情報の設定

schedule-power-control port cool-standby

情報の削除

no schedule-power-control port cool-standby

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

ポートリンクダウン時も通常の消費電力で運用します。

[通信への影響]

通信に影響があります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定した場合，Fastethernet ポートのリンクアップに約 3 秒程度かかります。【SS1250】【SS1240】
2. 本コマンドを設定した場合，Fastethernet 全ポートのリンク状態が変化し，通信に影響します。【SS1250】【SS1240】
3. 速度固定設定または自動 MDIX 機能無効の Fastethernet ポートに関しては , ポート省電力機能は有効になりません。このため，ポート省電力機能を有効にする場合は，オートネゴシエーション有効，自動 MDIX 機能有効 (mdix auto 設定) で運用してください。【SS1250】【SS1240】
4. スケジューリングのポート省電力機能は , スケジュール時間帯になると power-control port cool-standby と同様に Fastethernet ポートのリンク状態が変化します。スケジュールに遷移する際にポート省電力機能によりリンク状態を変化させたくない場合は，power-control port cool-standby コマンドも設定しておいてください。【SS1250】【SS1240】
5. 1000BASE-X ポートは，リンクダウンポートの省電力機能が未サポートのため，本コマンドを設定しても動作しません。

[関連コマンド]

なし

schedule-power-control port-led

スケジューリングによる省電力運転中の LED 動作を設定します。

[入力形式]

情報の設定・変更

schedule-power-control port-led { enable | disable }【S2200】【S2100】

schedule-power-control port-led { enable | economy | disable }【SS1250】【SS1240】

情報の削除

no schedule-power-control port-led

[入力モード]

(config)

[パラメータ]

enable

本装置の LED を動作状態に応じて点灯します。

system port-led trigger コマンドが未設定の場合

動作状態によらず通常輝度で点灯および点滅します。

system port-led trigger コマンドを設定している場合

以下の条件で動作します。【S2200】【S2100】

1. LED の自動動作の契機で通常輝度へ遷移し，点灯および点滅します。
2. 自動動作終了から 60 秒後に消灯します。この間に自動動作の契機が発生すると通常輝度へ遷移し，点灯および点滅します。

以下の条件で動作します。【SS1250】【SS1240】

1. LED の自動動作の契機で通常輝度へ遷移し，点灯および点滅します。
2. 自動動作終了から 60 秒後に省電力輝度へ遷移し，点灯および点滅します。
3. 省電力輝度になってから，10 分経過すると消灯へ遷移します。この間に自動動作の契機が発生すると通常輝度へ遷移し，点灯および点滅します。

economy 【SS1250】【SS1240】

本装置の LED を動作状態によらず省電力輝度で点灯および点滅します。

disable

本装置の LED を動作状態によらず消灯します。

このとき，ST1 LED は「長い間隔の緑点滅」となり，消灯設定であることを識別できます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   enable，disable【S2200】【S2100】
   enable，economy，disable【SS1250】【SS1240】

[コマンド省略時の動作]

本装置の LED を動作状態によらず通常輝度で点灯および点滅します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. "disable"(消灯) 中は，ST1，ACC(メモリカードアクセス LED) は「省電力輝度」となります。
2. PWR LED は常に「通常輝度」で点灯します。

[関連コマンド]

schedule-power-control time-range

schedule-power-control shutdown interface

スケジューリングによる省電力機能の動作中にシャットダウン状態にするポートを設定します。

シャットダウン状態にすることで，電力を OFF にして消費電力量を下げられます。

[入力形式]

情報の設定
  schedule-power-control shutdown interface <IF# list>

情報の変更
  schedule-power-control shutdown interface [add | remove] <IF# list>

情報の削除
  no schedule-power-control shutdown interface

[入力モード]

(config)

[パラメータ]

interface <IF# list>

シャットダウン状態にするポートをリスト形式で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF# list> の設定方法，値の設定範囲については，「パラメータに指定できる値」を参照してください。

interface add <IF# list>

シャットダウン状態にするポートをリストに追加します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF# list> の設定方法，値の設定範囲については，「パラメータに指定できる値」を参照してください。

interface remove <IF# list>

シャットダウン状態にするポートをリストから削除します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF# list> の設定方法，値の設定範囲については，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

ポートはシャットダウン状態以外で動作します。

ポート状態は，運用コマンド show port または show interfaces を参照してください。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. スケジュールに関係なく，ポートを常にシャットダウン状態にしたい場合は，shutdown コマンドと本コマンドの両方を設定する必要があります。

[関連コマンド]

schedule-power-control time-range

schedule-power-control system-sleep【SS1250】【SS1240】

スケジュール時間帯に装置をスリープ状態にします。

装置をスリープ状態にすることで消費電力を下げられます。

[入力形式]

情報の設定
　schedule-power-control system-sleep

情報の削除
　no schedule-power-control system-sleep

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

スリープ状態にしません。

[通信への影響]

スケジュール時間帯になるとすべての通信が停止します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. コンフィグレーションコマンドモードで操作中の場合は，装置をスリープ状態に遷移しません。

[関連コマンド]

schedule-power-control time-range

schedule-power-control time-range

スケジューリングによる省電力機能が動作する実行時間を指定します。

[入力形式]

情報の設定・変更

schedule-power-control time-range <Entry number> { 日付指定 | 曜日指定 | 毎日指定 } action { enable | disable }

- 日付指定の場合
  date start-time <YYMMDD> <HHMM> end-time <YYMMDD> <HHMM>
- 曜日指定の場合
  weekly start-time {sun | mon | tue | wed | thu | fri | sat} <HHMM> end-time {sun | mon | tue | wed | thu | fri | sat} <HHMM>
- 毎日指定の場合
  everyday start-time <HHMM> end-time <HHMM>

情報の削除

no schedule-power-control time-range <Entry number>

[入力モード]

(config)

[パラメータ]

<Entry number>

実行時間を識別するための識別子を指定します。
本識別子は実行時間を参照するために使います。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 50

実行時間（日付指定，曜日指定，毎日指定）パラメータ

{ date | weekly | everyday }

実行時間の指定種別を設定します。

date

日付指定で設定します。

weekly

曜日指定で設定します。

everyday

毎日指定で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   date, weekly, everyday

【date 指定のパラメータ】

start-time <YYMMDD> <HHMM>

開始日時を指定します。

YY

年の下 2 桁を指定します（00 ～ 38）。

例：2000 年ならば 00

MM

月を指定します（01 ～ 12）。

DD

日を指定します（01 ～ 31）。

HH

時間を指定します（00 ～ 23）。

MM

分を指定します（00 ～ 59）。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <YYMMDD> には日付を，<HHMM> には時間を指定します。指定できる値の範囲は，2000 年 1 月 1 日 0 時 0 分～ 2038 年 1 月 17 日 23 時 59 分です。

end-time <YYMMDD> <HHMM>

終了日時を指定します。

YY

年の下 2 桁を指定します（00 ～ 38）。

例：2000 年ならば 00

MM

月を指定します（01 ～ 12）。

DD

日を指定します（01 ～ 31）。

HH

時間を指定します（00 ～ 23）。

MM

分を指定します（00 ～ 59）。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <YYMMDD> には日付を，<HHMM> には時間を指定します。指定できる値の範囲は，2000 年 1 月 1 日 0 時 0 分～ 2038 年 1 月 17 日 23 時 59 分です。

【weekly 指定のパラメータ】

start-time {sun | mon | tue | wed | thu | fri | sat} <HHMM>

開始曜日，時間を指定します。

sun

日曜日を設定します。

mon

月曜日を設定します。

tue

火曜日を設定します。

wed

水曜日を設定します。

thu

木曜日を設定します。

fri

金曜日を設定します。

sat

土曜日を設定します。

HH

時間を指定します（00 ～ 23）。

MM

分を指定します（00 ～ 59）。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   曜日 (sun，mon，tue，wed，thu，fri，sat) を 1 つ選択し，<HHMM> には時間を指定します。

end-time {sun | mon | tue | wed | thu | fri | sat} <HHMM>

終了曜日，時間を指定します。

sun

日曜日を設定します。

mon

月曜日を設定します。

tue

火曜日を設定します。

wed

水曜日を設定します。

thu

木曜日を設定します。

fri

金曜日を設定します。

sat

土曜日を設定します。

HH

時間を指定します（00 ～ 23）。

MM

分を指定します（00 ～ 59）。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   曜日 (sun，mon，tue，wed，thu，fri，sat) を 1 つ選択し，<HHMM> には時間を指定します。

【everyday 指定のパラメータ】

start-time <HHMM>

開始時間を指定します。

HH

時間を指定します（00 ～ 23）。

MM

分を指定します（00 ～ 59）。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <HHMM> に時間を指定します。

end-time <HHMM>

終了時間を指定します。

HH

時間を指定します（00 ～ 23）。

MM

分を指定します（00 ～ 59）。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <HHMM> に時間を指定します。

action {enable | disable}

実行時間の電力制御動作を指定します。

enable

スケジューリングによる省電力機能のコンフィグレーションコマンドで指定した設定を，本コマンドで設定した実行時間，有効にします。

disable

スケジューリングによる省電力機能のコンフィグレーションコマンドで指定した設定を，本コマンドで設定した実行時間，無効にします。そして，次のコンフィグレーションコマンドの設定を有効にします。

- system port-led
- power-control port cool-standby
- shutdown

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   enable, disable

[コマンド省略時の動作]

なし

[通信への影響]

装置スリープを設定している場合，スケジュール開始時にすべての通信が停止します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 異なる action パラメータで実行時間帯が重複しているときは，action disable 設定を優先します。
2. schedule-power-control system-sleep コマンドを設定している場合は，下記にご注意ください。
   【SS1250】【SS1240】
   - コンフィグレーションコマンドモードで操作中にスケジュール実行時間帯になっても，スリープ状態に遷移しません。コンフィグレーションコマンドモードを終了後（装置管理者モードに遷移後），スリープ状態に遷移します。
   - スリープ状態に遷移したとき保存されていないコンフィグレーションが消失します。このため，コンフィグレーションコマンドモードを終了すると，下記のメッセージを表示します。
     Unsaved changes would be lost when the machine goes to sleep!

     Do you exit "configure" without save ? (y/n):
     保存するときは "n" を入力して，save コマンドを実行してください。
     スケジューリングによる省電力実行時間を設定していても，コンフィグレーションコマンドを終了していないと，スリープ状態に遷移しません。
   - 一定時間（デフォルト：30 分）キー入力操作を行わないと自動的にログアウトします。コンフィグレーションの編集中に自動ログアウトし，スリープ状態に遷移した場合，保存されていないコンフィグレーションが消失します。
   - スリープ状態が 20 日間を超過すると，20 日に一度自動でスリープ状態を解除し装置を起動します。装置起動後，再度スリープ状態となります。

[関連コマンド]

なし

system fan-control【SS1240】

装置内温度監視による冷却 FAN 制御機能を有効にします。

[入力形式]

情報の設定

system fan-control

情報の削除

no system fan-control

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

FAN が常時動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

ただし，no system fan-control コマンド実行時，運用に反映されるまでに十数秒かかる場合があります。

[注意事項]

1. 本コマンドは IP8800/SS1240-48T2C モデルだけが対象です。
2. 本コマンドを設定していても，装置起動直後の約 10 分間は必ず冷却 FAN が動作します。
3. 装置モデルによって本コマンド設定時の動作が異なります。

表 7-1　装置モデルごとの system fan mode 2（冷却重視）設定時の動作

モデル	FAN 動作種別	コマンド設定時の動作
IP8800/S2230-24T IP8800/S2130-24T IP8800/SS1250-24T2C IP8800/SS1240-24T2C	FAN レス	FAN レス仕様のため，本コマンドを設定しても無効となります。
IP8800/SS1240-48T2C	準 FAN レス	冷却重視を設定時，system fan-control コマンド設定は無効（FAN 速度固定）となります。
IP8800/S2230-24P IP8800/SS1240-24P2C	FAN 速度固定	コマンド省略時および静音重視設定を指定した場合も冷却重視設定の動作となります。
IP8800/S2130-24P	FAN 速度固定	コマンド省略時および静音重視設定を指定した場合は静音重視設定として動作します。 PoE 給電量によって，冷却 FAN 制御を行います。

［関連コマンド］

system fan mode

system port-led

本装置の LED 動作を設定します。

[入力形式]

情報の設定・変更

system port-led { enable | disable }【S2200】【S2100】

system port-led { enable | economy | disable }【SS1250】【SS1240】

情報の削除

no system port-led

[入力モード]

(config)

[パラメータ]

enable

本装置の LED を動作状態に応じて点灯します。

system port-led trigger コマンドが未設定の場合

動作状態によらず通常輝度で点灯および点滅します。

system port-led trigger コマンドを設定している場合

以下の条件で動作します。【S2200】【S2100】

1. LED の自動動作の契機で通常輝度へ遷移し，点灯および点滅します。
2. 自動動作終了から 60 秒後に消灯します。この間に自動動作の契機が発生すると通常輝度へ遷移し，点灯および点滅します。

以下の条件で動作します。【SS1250】【SS1240】

1. LED の自動動作の契機で通常輝度へ遷移し，点灯および点滅します。
2. 自動動作終了から 60 秒後に省電力輝度へ遷移し，点灯および点滅します。
3. 省電力輝度になってから，10 分経過すると消灯へ遷移します。この間に自動動作の契機が発生すると通常輝度へ遷移し，点灯および点滅します。

economy【SS1250】【SS1240】

本装置の LED を動作状態によらず省電力輝度で点灯および点滅します。

disable

本装置の LED を動作状態によらず消灯します。

このとき，ST1 LED は「長い間隔の緑点滅」となり，消灯設定であることを識別できます。

1. 本パラメータ省略時の初期値

   省略できません。
2. 値の設定範囲

   enable，disable 【S2200】【S2100】

   enable，economy，disable【SS1250】【SS1240】

[コマンド省略時の動作]

本装置の LED を動作状態によらず通常輝度で点灯および点滅します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. "disable"(消灯) 中は，ST1，ACC(メモリカードアクセス LED) は「省電力輝度」となります。
2. PWR LED は常に「通常輝度」で点灯します。
3. スケジューリングによる省電力機能の運転中は，schedule-power-control port-led コマンドの設定に従い動作します。

[関連コマンド]

なし

system port-led trigger console

コンソール（RS-232C）接続による装置へのログイン・ログアウトを LED の自動動作の契機に追加します。

[入力形式]

情報の設定

system port-led trigger console

情報の削除

no system port-led trigger console

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

コンソール（RS-232C）接続による装置へのログイン・ログアウトを自動動作条件としません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

system port-led

system port-led trigger interface

指定した物理ポートのリンクアップ・リンクダウンを LED の自動動作の契機に追加します。

[入力形式]

情報の設定・変更
　system port-led trigger interface <IF# list>

情報の削除
　no system port-led trigger interface

[入力モード]

(config)

[パラメータ]

<IF# list>

対象ポートを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

物理ポートのリンクアップ・リンクダウンを自動動作条件としません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

system port-led

system port-led trigger mc

MC の挿抜を LED の自動動作の契機に追加します。

[入力形式]

情報の設定

system port-led trigger mc

情報の削除

no system port-led trigger mc

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

MC の挿抜を自動動作条件としません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

system port-led

8 イーサネット

bandwidth

回線の帯域幅を設定します。本設定は，ネットワーク監視装置での回線使用率の算出に使用されます。

[入力形式]

情報の設定・変更

bandwidth <kbit/s>

情報の削除

no bandwidth

[入力モード]

(config-if)

[パラメータ]

<kbit/s>

回線の帯域幅を kbit/s 単位で設定します。

本設定は，当該回線の ifSpeed/ifHighSpeed（SNMP MIB）値にだけ反映されるもので，通信には影響ありません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 100000 （kbit/s　interface fastethernet の場合）【SS1250】【SS1240】
   1 ～ 1000000（kbit/s　interface gigabitethernet の場合）
   当該回線の回線速度を超えた値を設定しないでください。

[コマンド省略時の動作]

当該回線の回線速度が帯域幅となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

description

補足説明を設定します。回線に関するメモとしてご使用いただけます。なお，本設定を行うと運用コマンド show interfaces や ifDescr（SNMP MIB）で確認できます。

［入力形式］

情報の設定・変更
　description <String>

情報の削除
　no description

［入力モード］

(config-if)

［パラメータ］

<String>
　イーサネットインタフェースに補足説明を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   64 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

［コマンド省略時の動作］

Null を設定します。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

なし

［関連コマンド］

なし

duplex

ポートの duplex を設定します。

[入力形式]

情報の設定・変更

duplex {half | full | auto}

情報の削除

no duplex

[入力モード]

(config-if)

[パラメータ]

{half | full | auto}

ポートの接続モードを半二重固定，全二重固定またはオートネゴシエーションに設定します。

回線種別と設定可能なパラメータの組み合わせを次の表に示します。100BASE-FX の場合は，full を設定してください。

表 8-1　設定可能なパラメータ

回線種別	設定可能なパラメータ
10BASE-T/100BASE-TX	half，full，auto
10BASE-T/100BASE-TX/1000BASE-T	half，full，auto
100BASE-FX【SS1250】	full
1000BASE-X	full，auto

half

ポートを半二重固定モードに設定します。

full

ポートを全二重固定モードに設定します。

auto

duplex をオートネゴシエーションで決定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「表 8-1　設定可能なパラメータ」を参照してください。

[コマンド省略時の動作]

auto となります。

[通信への影響]

運用中のポートに設定した場合，いったんポートがダウンし，一時的に通信が停止します。そのあとで再起動します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. speed または duplex のどちらか一方に auto または auto を含むパラメータを設定した場合，オートネゴシエーションを行います。
2. 1000BASE-X の場合，オートネゴシエーションを使用しないためには，speed に 1000 を設定するとともに，duplex を full にする必要があります。speed に auto または auto 1000 を設定すると，オートネゴシエーションの結果 duplex は full になります。
3. media-type を変更した場合，本コマンドの設定はデフォルト状態に戻ります。【SS1250】【SS1240】
4. media-type auto を設定した場合，本コマンドは設定できません。【SS1250】【SS1240】
5. UTP ポート (RJ45) を固定設定で使用する場合には MDI-X となります。
6. 100BASE-FX の場合，duplex を full に設定してください。【SS1250】
7. half パラメータ設定は，10BASE-T/100BASE-TX の場合だけ設定が有効となります。

[関連コマンド]

speed

media-type

flowcontrol

フローコントロールを設定します。

[入力形式]

情報の設定・変更

flowcontrol send {desired | on | off}

flowcontrol receive {desired | on | off}

情報の削除

no flowcontrol send

no flowcontrol receive

[入力モード]

(config-if)

[パラメータ]

send {desired | on | off}

フローコントロールのポーズパケットの送信動作を設定します。接続相手のフローコントロールの，ポーズパケットの受信動作と設定を合わせてください。

desired

固定モード設定時はポーズパケットを送信します。オートネゴシエーション設定時は，接続装置とのやり取りによってポーズパケットの送信有無を決定します。

on

ポーズパケットを送信します。

off

ポーズパケットを送信しません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   send desired，send on，send off

receive {desired | on | off}

フローコントロールのポーズパケットの受信動作を設定します。接続相手のフローコントロールの，ポーズパケットの送信動作と設定を合わせてください。

desired

ポーズパケットを受信します。オートネゴシエーション設定時は，接続装置とのやり取りによってポーズパケットの受信有無を決定します。

on

ポーズパケットを受信します。

off

ポーズパケットを受信しません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   receive desired，receive on，receive off

[コマンド省略時の動作]

回線種別によって異なります。

- 10BASE-T/100BASE-TX/1000BASE-T の場合
  受信動作は off，送信動作は desired
- 1000BASE-X の場合
  受信動作は off，送信動作は desired
- 100BASE-FX の場合【SS1250】
  受信動作は off，送信動作は on

[通信への影響]

運用中のポートに設定した場合，いったんポートがダウンし，一時的に通信が停止します。そのあとで再起動します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信側・受信側のいずれかで flowcontrol on を設定した場合は，送受信両方とも flowcontrol on となります。
2. desired 設定された場合，オートネゴシエーション設定時は，ネゴシエーション結果により動作します。オートネゴシエーション以外の設定時は，flowcontrol on 固定となります。
3. 100BASE-FX の場合，オートネゴシエーション未サポートのため，オートネゴシエーション時のフローコントロール動作はありません。【SS1250】

[関連コマンド]

なし

interface fastethernet【SS1250】【SS1240】

10BASE-T/100BASE-TX に関する項目を設定します。本コマンドを入力すると，config-if モードに移行し，対象ポートに関する情報が設定できます。

[入力形式]

情報の設定・変更

interface fastethernet <IF#>

[入力モード]

(config)

[パラメータ]

<IF# >

インタフェースポート番号を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

なし

[注意事項]

1. ポートの名称は，'fastethernet'+' インタフェースポート番号 ' となります。
   例　0/1 のポートの名称は fastethernet 0/1 となります。
2. 本コマンドは削除できません。

[関連コマンド]

なし

interface gigabitethernet

10BASE-T/100BASE-TX/1000BASE-T，100BASE-FX，1000BASE-X に関する項目を設定します。本コマンドを入力すると，config-if モードに移行し，対象ポートに関する情報が設定できます。

［入力形式］

情報の設定・変更

interface gigabitethernet <IF#>

［入力モード］

(config)

［パラメータ］

<IF# >

インタフェースポート番号を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

なし

［注意事項］

1. ポートの名称は，'gigabitethernet'+' インタフェースポート番号 ' となります。
   例　0/25 のポートの名称は gigabitethernet 0/25 となります。
2. 本コマンドは削除できません。

［関連コマンド］

なし

link debounce

リンク障害を検出してからリンクダウンするまでのリンクダウン検出時間を設定します。本設定値を大きくすると，一時的なリンクダウンを検出しなくなるため，リンクが不安定となることを防げます。

[入力形式]

情報の設定・変更

link debounce [time <Milli seconds>]

情報の削除

no link debounce

[入力モード]

(config-if)

[パラメータ]

time <Milli seconds>

デバウンスタイマ値をミリ秒単位で設定します。

1. 本パラメータ省略時の初期値
   3000 ミリ秒
2. 値の設定範囲
   0 ～ 10000 の値で 100 の倍数（ミリ秒）

[コマンド省略時の動作]

2000 ミリ秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. リンクダウン検出時間を設定しなくてもリンクが不安定とならない場合は，リンクダウン検出時間を設定しないでください。
2. 10BASE-T/100BASE-TX/1000BASE-T は省略時の値（2000 ミリ秒）未満にすると，リンクが不安定になることがあります。

[関連コマンド]

なし

linkscan-mode【SS1250】【SS1240】

本装置のリンク状態を監視する動作モードを設定します。

[入力形式]

情報の設定
linkscan-mode <Mode>

情報の削除
no linkscan-mode <Mode>

[入力モード]

(config)

[パラメータ]

<Mode>

リンク状態を監視する動作モードを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1（ハードウェアでリンク状態を監視します）

[コマンド省略時の動作]

ソフトウェアでリンク状態を監視します。

[通信への影響]

リンク状態を監視する動作モードの変更により，一時的に通信断となる場合があります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

mdix auto

使用するポートの MDI 機能を設定します。no mdix auto を指定すると，自動 MDIX 機能は無効になり，MDI-X に固定されます。

[入力形式]

情報の設定

no mdix auto

情報の削除

mdix auto

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

オートネゴシエーション時に，MDI と MDI-X を自動で切り替えます。

[通信への影響]

運用中のポートに設定した場合，いったんポートがダウンし，一時的に通信が停止します。そのあとで再起動します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドはオートネゴシエーション時に有効となります。
2. 本コマンドは 100BASE-FX/1000BASE-X では無効です。
3. media-type が sfp の場合，本コマンドは無効となります。【SS1250】【SS1240】
4. media-type を変更した場合，本コマンドの設定はデフォルト状態に戻ります。【SS1250】【SS1240】
5. media-type auto を設定した場合，本コマンドは設定できません。デフォルト値でご使用ください。【SS1250】【SS1240】

[関連コマンド]

media-type

media-type【SS1250】【SS1240】

10BASE-T/100BASE-TX/1000BASE-T(RJ45) と 100BASE-FX/1000BASE-X(SFP) を切り替え可能なポートで，使用するポートを選択します。

[入力形式]

情報の設定・変更

media-type {rj45 | sfp | auto}

情報の削除

no media-type

[入力モード]

(config-if)

[パラメータ]

media-type {rj45 | sfp | auto}

10BASE-T/100BASE-TX/1000BASE-T(RJ45) と 100BASE-FX/1000BASE-X(SFP) を切り替え可能なポートで，使用するポートを選択します。

rj45

RJ45 ポートを使用します。

sfp

SFP ポートを使用します。

auto

自動選択です。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   rj45，sfp，auto

[コマンド省略時の動作]

auto（自動選択）を設定します。1000BASE-X でリンクアップ時に，sfp として動作します。

[通信への影響]

運用中の回線に設定した場合，いったん回線がダウンし，設定されたポートで回線が再起動します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ギガビットインタフェース以外には設定できません。
2. media-type を変更した場合は，下記コマンドの設定はデフォルト状態に戻ります。
   duplex，mdix auto，speed
3. media-type auto を設定した場合は，下記コマンドは設定できません。デフォルト値でご使用ください。
   duplex，mdix auto，speed

4. media-type auto 設定時，1000BASE-SX2 の SFP を挿して RJ45 を使用している場合は，1000BASE-X がリンクアップしないため自動的に切り替わりません。従って 1000BASE-SX2 の場合は，下記のいずれかでご使用ください。
   - 固定メディア設定で使用する。
   - 光ファイバケーブルと UTP(RJ45) ケーブルを同時に挿さない運用とする。
5. media-type auto 設定時および，10BASE-T/100BASE-TX/1000BASE-T(RJ45) がリンクアップしている状態で，1000BASE-BX※の SFP を挿入すると，10BASE-T/100BASE-TX/1000BASE-T で一時的にリンクダウンが発生しますのでご注意ください。

   注※

   1000BASE-BX10-D，1000BASE-BX10-U，1000BASE-BX40-D，1000BASE-BX40-U

   RJ45 側の運用を優先する場合，1000BASE-BX の SFP の挿入は下記のいずれかで実施してください。
   - 固定メディア（RJ45）設定で SFP を挿入する。
   - 装置電源 ON 前に SFP を挿入する。
6. 100BASE-FX の SFP を挿入する場合，下記の設定でご使用ください。
   - media-type sfp
   - speed 100
   - duplex full

   また，100BASE-FX を使用した後，10BASE-T/100BASE-TX/1000BASE-T，または 1000BASE-X を使用する場合，下記の順で設定変更を行ってからご使用ください。

   ① no speed

   ② no duplex

   ③ no media-type

［関連コマンド］

duplex

mdix auto

speed

mtu

ポートの MTU を設定します。本設定によって，ジャンボフレームが使用できるようになり，データ転送のスループットを向上させることでネットワークおよびネットワークに接続された機器の有用性を向上させることができます。

[入力形式]

情報の設定・変更

mtu <Length>

情報の削除

no mtu

[入力モード]

(config-if)

[パラメータ]

<Length>

ポートの MTU をオクテットで設定します。MTU は，Ethernet V2 形式フレームのデータ部※の最大長です。

注※　フレーム形式は「コンフィグレーションガイド Vol.1 14.1.3 MAC および LLC 副層制御」を参照してください。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1500 ～ 9216

[コマンド省略時の動作]

次の初期値で動作します。

表 8-2　ポートの MTU の初期値

system mtu コマンド設定有無	初期値
設定あり	system mtu 設定値
設定なし	1500

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 当該ポートの MTU および送受信可能なフレーム長（FCS を除いた Ethernet V2 形式フレームでの最大フレーム長※）は，次の表のとおりです。
   注※　フレーム形式は「コンフィグレーションガイド Vol.1 14.1.3 MAC および LLC 副層制御」を参照してください。

表 8-3　MTU および送受信可能なフレーム長

回線種別	mtu 設定	system mtu 設定	送受信可能フレーム長（オクテット）	ポート MTU(オクテット)
10BASE-T（全 / 半二重），100BASE-TX（半二重）	関係しない	関係しない	Tagged　1518 Untagged 1514	1500
上記以外	設定あり	関係しない	Tagged　M1※1+18 Untagged M1※1+14	M1※1
	設定なし	設定あり	Tagged　M2※2+18 Untagged M2※2+14	M2※2
		設定なし	Tagged　1518 Untagged 1514	1500

注※1　interface の mtu コマンドで設定した値

注※2　system mtu コマンドで設定した値

2. vlan に収容されるポートの MTU は同じ値にしてください。MTU が異なる場合，次の動作となります。
   - 出力ポートの MTU が入力ポートの MTU より小さく，中継するフレーム長が出力ポートで送信できる最大フレーム長を超えたときは，出力ポートで廃棄されます。

［関連コマンド］

なし

power inline【S2200】【S2100】【SS1240】

ポートの優先度を設定します。ポートごとに電力供給の優先度を設定することで，必要なポートでの電力供給を保証できます。

[入力形式]

情報の設定・変更

power inline {critical | high | low | never }

情報の削除

no power inline

[入力モード]

(config-if)

[パラメータ]

critical

最重要ポートとして電力供給を割り当てます。常時電力供給する必要があるポートに設定してください。

high

電力供給の優先度を「高」で供給します。本設定したポートは，供給電力不足時に「低」設定されているポートよりもあとで，電力供給が停止されます。

low

電力供給の優先度を「低」で供給します。本設定したポートは，供給電力不足時に「高」設定されているポートよりも先に，電力供給が停止されます。

never

ポートの PoE 機能を無効にします。電力供給時には，供給中の電力を停止し PoE 機能を無効とします。接続装置が受電装置であっても電力の供給はしません。

[コマンド省略時の動作]

high で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. PoE 機能をサポートしているモデルだけ設定可能です。
2. 相手装置が給電装置の場合は，never を設定して回線の PoE 機能を無効にしてください。
3. ポートがシャットダウン状態では，電力を供給しません。
4. 運用コマンド inactivate/activate を実行した場合，電力供給は継続されます。
5. never を設定しているポートに対して運用コマンド activate power inline を実行しても電力供給はされません。
6. 同一設定が複数あった場合はポート番号の小さいポートを優先します。

7. 優先制御は，系統 1，系統 2 それぞれの範囲で個別に動作します。【S2200】

［関連コマンド］

power inline priority-control disable

power inline allocation【S2200】【S2100】【SS1240】

ポートごとの割り当て電力を Class ベースまたは手動で設定します。

[入力形式]

情報の設定・変更

power inline allocation {auto | limit <Threshold>}

情報の削除

no power inline allocation

[入力モード]

(config-if)

[パラメータ]

auto

受電装置の検出，電力クラスの分類まで自動で行い，該当ポートの電力量割り当てを Class ベースで設定します。

割り当てる電力クラスと最大出力電力を次の表に示します。

電力クラス	最大出力電力
Class0	15.4W
Class1	4.0W
Class2	7.0W
Class3	15.4W
Class4	30.0W

limit

受電装置の検出，電力クラスの分類まで自動で行い，該当ポートの電力量割り当てを手動で設定します。

<Threshold>【S2200】

ポートの供給電力量，および優先制御に使用する消費電力を 200mW 単位，または 400mW 単位で設定します。本パラメータは，limit 指定時に有効となります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   次の表に示します。

ポート	設定範囲（単位：mW）	刻み値（単位：mW）
0/1 ～ 0/4	4000 ～ 30000	200
	30000 ～ 60000	400
0/5 ～ 0/24	4000 ～ 30000	200

<Threshold>**【S2100】【SS1240】**

ポートの供給電力量，および優先制御に使用する消費電力を 200mW 単位で設定します。本パラメータは，limit 指定時に有効となります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   4000 〜 30000(mW)

[コマンド省略時の動作]

auto で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 手動割り当て設定は，受電装置のマニュアルをよくご確認のうえ，お客様の責任において行ってください。
2. 受電装置の最大消費電力に若干の余裕を持たせた値を設定してください。
3. 受電装置が必要とする最低消費電力よりも小さな値を手動設定すると，オーバーロードを検出して受電装置への電力供給を停止する場合があります。回復するときは，運用コマンド activate power inline コマンドを実行してください。
4. 0/1 〜 0/4 のポートに limit 指定で 30000(mW) から 60000(mW) の範囲で設定変更をした場合，および設定変更前後で 30000(mW) を跨いだ変更があった場合，当該ポートへの給電が一旦停止します。
   【S2200】

[関連コマンド]

power inline

power inline priority-control disable【S2200】【S2100】【SS1240】

既給電ポートを優先します。

[入力形式]

情報の設定

power inline priority-control disable

情報の削除

no power inline priority-control disable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

ポートの優先度設定が有効になります。

[通信への影響]

本装置を再起動してから起動が完了するまでの間，本装置を経由する通信が停止します。

[設定値の反映契機]

設定値を変更した場合は，コンフィグレーションを保存したあとで，本装置を再起動してください。再起動すると，設定値が運用に反映されます。

[注意事項]

1. 本コマンド入力時，下記のメッセージが表示されますので，設定を保存し装置を再起動してください。
   Please execute the reload command after save,
   because this command becomes effective after reboot.
2. 本コマンドの設定により，系統 1，系統 2，それぞれの範囲内で既給電ポート優先となります。
   【S2200】

[関連コマンド]

power inline

power inline system-allocation【S2200】

系統 1 で供給可能な最大電力量を手動で設定します。

本装置の最大供給可能電力量から，本コマンドの設定値を差引いた値が系統 2 の最大電力量となります。

[入力形式]

情報の設定・変更

power inline system-allocation limit <Threshold>

情報の削除

no power inline system-allocation

[入力モード]

(config)

[パラメータ]

limit

系統 1 で供給可能な最大電力量を手動で設定します。

<Threshold>

系統 1 で供給可能な最大電力量を 400mW 単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   16000 ～ 240000（mW）

[コマンド省略時の動作]

系統 1 で供給可能な最大電力量が 61600（mW）に設定されます。

[通信への影響]

本装置を再起動してから起動が完了するまでの間，本装置を経由する通信が停止します。

[設定値の反映契機]

設定値を変更した場合は，コンフィグレーションを保存したあとで，本装置を再起動してください。再起動すると，設定値が運用に反映されます。

[注意事項]

1. 本コマンド入力時，下記のメッセージが表示されますので，設定を保存し本装置を再起動してください。
   Please execute the reload command after save,
   because this command becomes effective after reboot.

[関連コマンド]

power inline

shutdown

ポートをシャットダウン状態にします。PoE 機能付きポートをシャットダウンすると電力を停止します。

[入力形式]

情報の設定

shutdown

情報の削除

no shutdown

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. SNMP マネージャから，SNMP の SetRequest オペレーションを使用して ifAdminStatus の Set を実行した場合，その設定は本コマンドの設定に反映されます。
2. スケジューリングによる省電力機能の動作中は schedule-power-control shutdown interface コマンドの設定に従い動作します。
3. スケジュールに関係なく，ポートを常にシャットダウン状態にしたい場合は，schedule-power-control shutdown interface コマンドと本コマンドの両方を設定する必要があります。

[関連コマンド]

なし

speed

ポートの速度を設定します。

[入力形式]

情報の設定・変更

speed { 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10 100 | 10 100 1000} }

情報の削除

no speed

[入力モード]

(config-if)

[パラメータ]

{ 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10 100 | 10 100 1000} }

回線速度を設定します。

回線種別と設定可能なパラメータの組み合わせを次の表に示します。100BASE-FX の場合は，100 を設定してください。auto ではリンクアップしません。

表 8-4　設定可能なパラメータ

回線種別	設定可能なパラメータ
10BASE-T/ 100BASE-TX/	10 100 auto auto 10 auto 100 auto 10 100
10BASE-T/ 100BASE-TX/ 1000BASE-T	10 100 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
100BASE-FX【SS1250】	100
1000BASE-X	1000 auto auto 1000

10

回線速度を 10Mbit/s に設定します。

100

回線速度を 100Mbit/s に設定します。

1000

回線速度を 1000Mbit/s に設定します。

auto

回線速度をオートネゴシエーションに設定します。

auto {10 | 100 | 1000 | 10 100 | 10 100 1000}

設定された回線速度でオートネゴシエーションを行います。本設定によって，意図しない回線速度になり，回線利用率が上がることなどを防ぎます。設定された回線速度でネゴシエーションできなかった場合はリンクがアップしません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「表 8-4　設定可能なパラメータ」を参照してください。

[コマンド省略時の動作]

auto となります。

[通信への影響]

運用中のポートに設定した場合，いったんポートがダウンし，一時的に通信が停止します。そのあとで再起動します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. speed または duplex のどちらか一方に auto または auto を含むパラメータを設定した場合，オートネゴシエーションを行います。
2. 10BASE-T/100BASE-TX/1000BASE-T でオートネゴシエーションを使用しない場合，speed を 10 または 100 にするとともに，duplex を full または half にする必要があります。
3. 1000BASE-X でオートネゴシエーションを使用しない場合，speed を 1000 にするとともに，duplex を full にする必要があります。
4. media-type を変更した場合，本コマンドの設定はデフォルト状態に戻ります。【SS1250】【SS1240】
5. media-type auto を設定した場合，本コマンドは設定できません。デフォルト値でご使用ください。【SS1250】【SS1240】
6. UTP ポート (RJ45) を固定設定で使用する場合には MDI-X となります。
7. 100BASE-FX はオートネゴシエーション未サポートのため，speed を 100 に設定してください。auto ではリンクアップしません。【SS1250】

[関連コマンド]

duplex

media-type

system mtu

全ポートの MTU を設定します。本設定によって，ジャンボフレームが使用できるようになり，データ転送のスループットを向上させることでネットワークおよびネットワークに接続された機器の有用性を向上させることができます。

[入力形式]

情報の設定・変更

system mtu <Length>

情報の削除

no system mtu

[入力モード]

(config)

[パラメータ]

<Length>

全ポートの MTU をオクテットで設定します。MTU は Ethernet V2 形式フレームのデータ部※の最大長です。

注※　フレーム形式は「コンフィグレーションガイド Vol.1 14.1.3 MAC および LLC 副層制御」を参照してください。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1500 ～ 9216（オクテット）

[コマンド省略時の動作]

全ポートの MTU が 1500 となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ポート MTU および送受信可能なフレーム長（FCS を除いた Ethernet V2 形式フレームでの最大フレーム長※）は，次の表のとおりです。
   注※　フレーム形式は「コンフィグレーションガイド Vol.1 14.1.3 MAC および LLC 副層制御」を参照してください。

表 8-5　MTU および送受信可能なフレーム長

回線種別	mtu 設定	system mtu 設定	送受信可能フレーム長（オクテット）	回線 MTU（オクテット）
10BASE-T（全 / 半二重），100BASE-TX（半二重）	関係しない	関係しない	Tagged　1518 Untagged 1514	1500
上記以外	設定あり	関係しない	Tagged　M1※1+18 Untagged M1※1+14	M1※1
	設定なし	設定あり	Tagged　M2※2+18 Untagged M2※2+14	M2※2
		設定なし	Tagged　1518 Untagged 1514	1500

注※ 1　interface の mtu コマンドで設定した値

注※ 2　system mtu コマンドで設定した値

[関連コマンド]

なし

9 リンクアグリゲーション

channel-group lacp system-priority

リンクアグリゲーションの当該チャネルグループの LACP システム優先度を設定します。

[入力形式]

情報の設定・変更
channel-group lacp system-priority <Priority>

情報の削除
no channel-group lacp system-priority

[入力モード]

(config-if)

[パラメータ]

<Priority>

LACP システム優先度を設定します。値が小さいほど優先度が高くなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535

[コマンド省略時の動作]

lacp system-priority コマンドの設定に従います。

[通信への影響]

運用中のチャネルグループに設定した場合，いったんチャネルグループがダウンし，再起動します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドは LACP によるリンクアグリゲーションの場合だけ有効です。
2. LACP システム優先度を変更した場合，当該チャネルグループに登録されている全ポートが Block 状態（通信断）になります。

[関連コマンド]

interface port-channel

channel-group max-active-port

リンクアグリゲーションの当該チャネルグループ内で実際に使用するポートの最大数を設定します。

[入力形式]

情報の設定・変更

channel-group max-active-port <Number> [no-link-down]

情報の削除

no channel-group max-active-port

[入力モード]

(config-if)

[パラメータ]

<Number>

リンクアグリゲーションのチャネルグループ内で実際に使用するポートの最大数を設定します。チャネルグループ内のポートが本コマンドの設定数を超えている場合，設定数のポートを使用してそのほかのポートにはスタンバイリンク機能を適用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 8

no-link-down

スタンバイリンクを非リンクダウンで使用する場合，no-link-down を設定します。設定しない場合，スタンバイリンクはリンクダウンします。スタンバイリンクの選択方法は次のとおりです。

- lacp port-priority コマンドによる優先度の低いポート
- 優先度が同じ場合はインタフェースポート番号の大きいポート

1. 本パラメータ省略時の初期値
   スタンバイリンクはリンクダウンします。
2. 値の設定範囲
   no-link-down

[コマンド省略時の動作]

最大数は 8 になります。

[通信への影響]

スタンバイリンク機能で使用ポートが変更され，一時的に通信断となる場合があります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドはスタティックなリンクアグリゲーションで使用してください。
2. max-active-port を設定する場合は，max-active-port，lacp port-priority の設定を接続先の装置と合わせてください。
3. スタンバイリンクモードのリンクダウン／非リンクダウンを変更するときは，本パラメータを削除した

あとに，再度本パラメータを設定してください。非リンクダウンモードでポート数を変更する場合，no-link-down の設定が必要です。

［関連コマンド］

interface port-channel

channel-group lacp system-priority

lacp system-priority

lacp port-priority

channel-group mode

リンクアグリゲーションのチャネルグループを作成します。

[入力形式]

情報の設定

channel-group <Channel group#> mode { on | { active | passive } }

情報の変更

channel-group <Channel group#> mode { active | passive }

情報の削除

no channel-group

[入力モード]

(config-if)

[パラメータ]

<Channel group#>

リンクアグリゲーションのチャネルグループ番号を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

mode { on | { active | passive } }

リンクアグリゲーションのモードを設定します。

on

スタティックにリンクアグリゲーションを行います。

active

LACP によるリンクアグリゲーションを行い，相手装置に関係なく常に LACPDU を送信します。

passive

LACP によるリンクアグリゲーションを行い，相手装置から LACPDU を受信した場合だけ LACPDU 送信を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   on，active，または passive

[コマンド省略時の動作]

なし

[通信への影響]

運用中のポートに設定した場合，いったん通信断となります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. スタティックなリンクアグリゲーションから LACP によるリンクアグリゲーションへの変更，または LACP によるリンクアグリゲーションからスタティックなリンクアグリゲーションへ変更をする場合，いったん本コマンドを削除してから，再度 mode を変更して設定してください。
2. channel-group mode を設定すると，指定チャネルグループ番号による port-channel の設定を自動生成します。すでに port-channel の設定が存在する場合は何もしません。
3. 本コマンドの設定時に，すでに指定チャネルグループ番号による port-channel の設定が存在する場合は，当該インタフェースと指定チャネルグループ番号のポートチャネルインタフェースで共通なコンフィグレーションコマンドは設定を同じにするか，または当該インタフェースには，共通なコンフィグレーションコマンドを何も設定していない必要があります。詳細については，「コンフィグレーションガイド Vol.1 15.2.4 ポートチャネルインタフェースの設定」を参照してください。
4. 本コマンドを削除する場合，当該インタフェースに shutdown コマンドを実行後，削除してください。
5. 本コマンドを削除しても，port-channel コンフィグレーションは削除されません（チャネルグループ内のすべてのポートを削除しても port-channel コンフィグレーションは削除されません)。チャネルグループを削除する場合，手動で port-channel コンフィグレーションを削除する必要があります。

[関連コマンド]

interface fastethernet

interface gigabitethernet

channel-group periodic-timer

LACPDU の送信間隔を設定します。

[入力形式]

情報の設定・変更

channel-group periodic-timer { long | short }

情報の削除

no channel-group periodic-timer

[入力モード]

(config-if)

[パラメータ]

{ long | short }

対向装置が本装置に向けて送信する LACPDU の送信間隔を設定します。

long：30 秒

short：1 秒

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   long または short

[コマンド省略時の動作]

送信間隔は long（30 秒）になります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドは LACP によるリンクアグリゲーションの場合だけ有効です。

[関連コマンド]

interface port-channel

channel-group mode

description

補足説明を設定します。

[入力形式]

情報の設定・変更
　description <String>

情報の削除
　no description

[入力モード]

(config-if)

[パラメータ]

<String>

リンクアグリゲーションの当該チャネルグループに補足説明を設定します。インタフェースに関するメモとして使用してください。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   64 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

Null になります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

interface port-channel

ポートチャネルインタフェースに関する項目を設定します。本コマンドを入力すると，config-if モードに移行し，チャネルグループ番号を指定するコンフィグレーションコマンドを設定できます。ポートチャネルインタフェースは channel-group mode コマンドを設定すると自動的に作成されます。

[入力形式]

情報の設定・変更

interface port-channel <Channel group#>

情報の削除

no interface port-channel <Channel group#>

[入力モード]

(config)

[パラメータ]

<Channel group#>

チャネルグループ番号を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを削除する場合，当該チャネルグループの全ポートに shutdown コマンドを実行後，削除してください。

[関連コマンド]

interface fastethernet

interface gigabitethernet

lacp port-priority

ポート優先度を設定します。

[入力形式]

情報の設定・変更
　lacp port-priority <Priority>

情報の削除
　no lacp port-priority

[入力モード]

(config-if)

[パラメータ]

<Priority>

ポートの優先度を設定します。値が小さいほど優先度が高くなります。

channel-group mode コマンドで on を設定した場合

max-active-port コマンドによるスタンバイリンクの選択に利用します。

channel-group mode コマンドで active または passive を設定した場合

LACP プロトコルの Port Priority に適用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535

[コマンド省略時の動作]

ポート優先度は 128 になります。

[通信への影響]

channel-group mode active または passive で運用中のポートに設定した場合，いったん通信断となります。channel-group mode on で運用中のポートに設定した場合，スタンバイリンク機能で使用ポートが変更され，一時的に通信断となる場合があります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. max-active-port を設定する場合は，max-active-port の設定を接続先の装置と合わせてください。
2. priority を変更した場合，当該ポートが Block 状態（通信断）になります。

[関連コマンド]

interface fastethernet

interface gigabitethernet

channel-group mode

channel-group max-active-port

lacp system-priority

装置に有効な LACP システム優先度を設定します。

[入力形式]

情報の設定・変更

lacp system-priority <Priority>

情報の削除

no lacp system-priority

[入力モード]

(config)

[パラメータ]

<Priority>

LACP システム優先度を設定します。値が小さいほど優先度が高くなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535

[コマンド省略時の動作]

channel-group lacp system-priority コマンドを設定している場合は，その設定に従います。
channel-group lacp system-priority コマンドの設定がない場合は，128 で動作します。

[通信への影響]

運用中のチャネルグループに設定した場合，いったんチャネルグループがダウンし，再起動します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドは LACP によるリンクアグリゲーションの場合だけ有効です。
2. LACP システム優先度を変更した場合，当該チャネルグループに登録されている全ポートが Block 状態（通信断）になります。

[関連コマンド]

なし

shutdown

リンクアグリゲーションの当該チャネルグループを常に Disable 状態とし，通信を停止します。

[入力形式]

情報の設定
　shutdown

情報の削除
　no shutdown

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

運用中のチャネルグループに設定した場合，チャネルグループがダウンします。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

SNMP マネージャから，SNMP の SetRequest オペレーションを使用して ifAdminStatus の Set を実行した場合，その設定は本コマンドの設定に反映されます。

[関連コマンド]

interface port-channel

10 MAC アドレステーブル

mac-address-table aging-time

MAC アドレステーブルエントリに関するエージング条件を設定します。

[入力形式]

情報の設定・変更
　mac-address-table aging-time <Seconds>

情報の削除
　no mac-address-table aging-time

[入力モード]

(config)

[パラメータ]

<Seconds>

エージング時間を秒単位で設定します。0 設定時はエージングなしとなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0，10 ～ 1000000（秒）

[コマンド省略時の動作]

エージング時間を 300 秒とします。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本装置は，エージング時間ごとにフレームの受信を確認します。従って，学習したエントリを削除するまでに最大でエージング時間の 2 倍の時間が掛かることがあります。
2. 下記のいずれかの設定が有効なとき，本コマンドで設定した 10 ～ 300 秒の範囲のエージング時間は 300 秒となります。

- IEEE802.1X ポート単位（静的）またはポート単位（動的）有効で，dot1x auto-logout 有効
- Web 認証固定 VLAN モードまたはダイナミック VLAN モード有効で，web-authentication auto-logout 有効
- MAC 認証固定 VLAN モードまたはダイナミック VLAN モード有効で，mac-authentication auto-logout 有効

[関連コマンド]

なし

mac-address-table static

スタティック MAC アドレステーブル情報を設定します。

[入力形式]

情報の設定・変更

mac-address-table static <MAC> vlan <VLAN ID> interface {gigabitethernet <IF#> | port-channel <Channel group#> }【S2200】【S2100】

mac-address-table static <MAC> vlan <VLAN ID> interface {fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#> }【SS1250】【SS1240】

情報の削除

no mac-address-table static <MAC> vlan <VLAN ID>

[入力モード]

(config)

[パラメータ]

<MAC>

スタティックエントリで登録する MAC アドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0000.0000.0000 ～ feff.ffff.ffff
   ただし，マルチキャスト MAC アドレス（先頭バイトの最下位ビットが 1 のアドレス）は設定できません。

vlan <VLAN ID>

スタティックエントリの VLAN の VLAN ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

interface { gigabitethernet <IF#> | port-channel <Channel group#> }【S2200】【S2100】

interface { fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#> }【SS1250】【SS1240】

スタティックエントリの出力先インタフェースを設定します。設定できるインタフェースは，物理ポートまたはリンクアグリゲーションです。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF#> :「パラメータに指定できる値」を参照してください。
   <Channel group#> :「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

スタティックエントリは設定されません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. デフォルト VLAN（VLAN ID=1）に対してスタティックエントリを設定する場合，出力先インタフェースに対して明示的に「vlan 1」を設定してください。
2. interface を設定した場合，宛先 MAC アドレスが一致するフレームを設定したインタフェースに出力します。また，送信元 MAC アドレスが一致するフレームを設定したインタフェース以外から受信した場合は廃棄します。
3. 本コマンドで指定した出力先インタフェースと VLAN が，レイヤ 2 認証機能の自動 VLAN 割当で動作している場合，MAC アドレスをスタティックエントリで登録することはできません。

[関連コマンド]

vlan

11 VLAN

interface vlan

VLAN インタフェースを設定します。VLAN インタフェースを設定することで，VLAN へ IP アドレスなどを設定できます。

[入力形式]

情報の設定・変更

interface vlan <VLAN ID>

情報の削除

no interface vlan <VLAN ID>

[入力モード]

(config)

[パラメータ]

<VLAN ID>

VLAN ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。ただし，削除の場合，デフォルト VLAN（VLAN ID=1）は設定できません。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. <VLAN ID> に未設定の VLAN ID を設定すると，VLAN が生成されます。生成される VLAN はポート VLAN です。プロトコル VLAN または MAC VLAN は，あらかじめ vlan コマンドで VLAN を生成しておく必要があります。
2. 複数 VLAN インタフェースに情報を設定する場合は，interface range コマンドで <VLAN ID list> を設定できます。
3. interface vlan で生成した VLAN に対して no vlan を設定すると，VLAN は削除されます。また，vlan コマンドで生成した VLAN に対して no interface vlan コマンドを設定すると，VLAN が削除されます。

[関連コマンド]

vlan

l2protocol-tunnel eap

EAPOL フォワーディング機能を有効にします。装置に対して設定します。

[入力形式]

情報の設定

l2protocol-tunnel eap

情報の削除

no l2protocol-tunnel eap

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

EAPOL フォワーディング機能は無効です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

l2protocol-tunnel stp

BPDU フォワーディング機能を有効にします。装置に対して設定します。

[入力形式]

情報の設定

l2protocol-tunnel stp

情報の削除

no l2protocol-tunnel stp

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

BPDU フォワーディング機能は無効です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

mac-address

MAC VLAN を識別するための MAC アドレスを設定します。

[入力形式]

情報の設定・変更
mac-address <MAC>

情報の削除
no mac-address <MAC>

[入力モード]

(config-vlan)（MAC VLANだけ）

[パラメータ]

<MAC>

MAC VLAN に設定する MAC アドレスを設定します。本コマンドは当該 VLAN が MAC VLAN の場合だけ設定できます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0000.0000.0000 ～ feff.ffff.ffff
   先頭 1 バイトの最下位ビット（マルチキャストビット）が 1 でないこと。

[コマンド省略時の動作]

MAC アドレスを設定しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ほかの VLAN に設定している MAC アドレスは設定できません。削除してから設定してください。
2. レイヤ 2 認証機能で動的に設定されている MAC アドレスを設定した場合，レイヤ 2 認証機能の設定は無効となり，本コマンドの設定内容が有効となります。
3. 設定可能な MAC アドレス数は，装置単位で 64 個です。

[関連コマンド]

なし

name

VLAN 名称を設定します。

[入力形式]

情報の設定・変更

name <String>

情報の削除

no name

[入力モード]

(config-vlan)

[パラメータ]

<String>

VLAN の名称を設定します。vlan コマンドで <VLAN ID list> を設定した場合は設定できません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

初期値は「VLANxxxx」です。ただし，「xxxx」は VLAN ID を表す 4 けたの数字で，先頭の 0 を含んだものです。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドで設定する VLAN 名称を，RADIUS 認証の認証後 VLAN として使用するときは下記に注意してください。
   - VLAN 名称が，複数の VLAN で重複しないように設定してください。VLAN 名称が重複していると，重複しているうちで最も小さい VLAN ID が RADIUS 認証の認証後 VLAN として割り当てられます。
   - VLAN 名称の先頭に数字を指定しないでください。先頭の数字を VLAN ID として認識し，認証に失敗する場合があります。

[関連コマンド]

なし

protocol

プロトコル VLAN で VLAN を識別するプロトコルを設定します。

[入力形式]

情報の設定・変更

protocol <Protocol name>

情報の削除

no protocol <Protocol name>

[入力モード]

(config-vlan)

[パラメータ]

<Protocol name>

プロトコル VLAN のプロトコル名称を設定します。本コマンドは当該 VLAN がプロトコル VLAN の場合だけ設定できます。一つの VLAN に複数のプロトコル名称を適用する場合は，本コマンドをプロトコル名称の数だけ設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   vlan-protocol コマンドで設定したプロトコル名称

[コマンド省略時の動作]

プロトコルが設定されません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. プロトコル VLAN に IPv4 アドレスまたは IPv6 アドレスを設定して使用する場合，該当するプロトコルを本コマンドで指定する必要があります。

[関連コマンド]

vlan-protocol

state

VLAN の状態を設定します。

[入力形式]

情報の設定・変更

state {suspend | active}

情報の削除

no state

[入力モード]

(config-vlan)

[パラメータ]

{suspend | active}

suspend

VLAN の状態を disable にし，全フレームの送受信を停止します。

active

VLAN の状態を enable にし，全フレームの送受信を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   suspend または active

[コマンド省略時の動作]

VLAN の状態は enable です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

SNMP マネージャから，SNMP の SetRequest オペレーションを使用して ifAdminStatus の Set を実行した場合，その設定は本コマンドの設定に反映されます。

[関連コマンド]

なし

switchport access

アクセスポートの情報を設定します。

[入力形式]

情報の設定・変更

switchport access vlan <VLAN ID>

情報の削除

no switchport access vlan

[入力モード]

(config-if)

[パラメータ]

vlan <VLAN ID>

アクセスポートの VLAN を設定します。設定可能な VLAN はポート VLAN または MAC VLAN です。プロトコル VLAN は設定できません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

デフォルト VLAN（VLAN ID=1）のアクセスポートになります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. Untagged フレームまたはポート VLAN の Tagged フレームを受信した場合，ポート VLAN で処理し，ポート VLAN 以外の Tagged フレームを受信した場合は廃棄します。

[関連コマンド]

switchport mode

vlan

switchport isolation

ポート間中継遮断機能を設定します。

[入力形式]

情報の設定

switchport isolation interface fastethernet <IF# list>【SS1250】【SS1240】
switchport isolation interface gigabitethernet <IF# list>

情報の変更

switchport isolation interface { gigabitethernet <IF# list> | add gigabitethernet <IF# list> | remove gigabitethernet <IF# list>}【S2200】【S2100】
switchport isolation interface { fastethernet <IF# list> | gigabitethernet <IF# list> | add { fastethernet <IF# list> | gigabitethernet <IF# list>} | remove { fastethernet <IF# list> | gigabitethernet <IF# list>} }【SS1250】【SS1240】

情報の削除

no switchport isolation

[入力モード]

(config-if)

[パラメータ]

interface { gigabitethernet <IF# list> }【S2200】【S2100】

interface { fastethernet <IF# list> | gigabitethernet <IF# list> }【SS1250】【SS1240】

中継を遮断する物理ポート（のリスト）を設定します。本パラメータで設定したポートから当該ポートへの中継を抑止します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF# list> の指定方法，値の設定範囲については，「パラメータに指定できる値」を参照してください。

interface add { gigabitethernet <IF# list> }【S2200】【S2100】

interface add { fastethernet <IF# list> | gigabitethernet <IF# list> }【SS1250】【SS1240】

中継を遮断するポートをリストに追加します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF# list> の指定方法，値の設定範囲については，「パラメータに指定できる値」を参照してください。

interface remove { gigabitethernet <IF# list> }【S2200】【S2100】

interface remove { fastethernet <IF# list> | gigabitethernet <IF# list> }【SS1250】【SS1240】

中継を遮断するポートをリストから削除します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲

<IF# list> の指定方法，値の設定範囲については，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

ポート間中継を遮断しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ポート間中継抑止機能は，switchport isolation コマンドの interface で設定したポートから入力し，本コマンドを設定したポートから出力されるフレームを廃棄します。両方向で中継を抑止する場合は，本コマンドを両方のポートに設定してください。

[関連コマンド]

なし

switchport mac

MAC ポートの情報を設定します。

[入力形式]

情報の設定

switchport mac vlan <VLAN ID list>
switchport mac native vlan <VLAN ID>
switchport mac dot1q vlan <VLAN ID list>

情報の変更

switchport mac {vlan <VLAN ID list> | vlan add <VLAN ID list> | vlan remove <VLAN ID list> | native vlan <VLAN ID> }
switchport mac dot1q vlan{<VLAN ID list> | add <VLAN ID list> | remove <VLAN ID list>}

情報の削除

no switchport mac vlan
no switchport mac native vlan
no switchport mac dot1q vlan

[入力モード]

(config-if)

[パラメータ]

vlan <VLAN ID list>

このポートで有効な MAC VLAN を設定します。変更時は有効な MAC VLAN リストを設定されたリストに置き換えます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

native vlan <VLAN ID>

送信元 MAC アドレスが未登録のフレームを受信する VLAN を設定します。設定した VLAN でフレームを送信することもできます。設定可能な VLAN はポート VLAN です。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

dot1q vlan <VLAN ID list>

本パラメータで設定した VLAN リストのフレームを Tagged フレームで送信します。また，本パラメータで設定した VLAN で Tagged フレームを中継可能です。設定した VLAN 以外の VLAN で Tagged フレームを受信した場合は廃棄します。
設定可能な VLAN はポート VLAN または MAC VLAN です。switchport mac vlan コマンドで設定した VLAN は設定できません。

1. 本パラメータ省略時の初期値
   省略できません。

2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

vlan add <VLAN ID list>

このポートで有効な MAC VLAN を VLAN リストに追加します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

vlan remove <VLAN ID list>

このポートで有効な MAC VLAN を VLAN リストから削除します。

1. 本パラメータ省略時の初期値。
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

dot1q vlan add <VLAN ID list>

このポートで Tagged フレームが中継可能な VLAN を VLAN リストに追加します。設定可能な VLAN はポート VLAN または MAC VLAN です。switchport mac vlan コマンドで設定した VLAN は設定できません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

dot1q vlan remove <VLAN ID list>

このポートで Tagged フレームが中継可能な VLAN を VLAN リストから削除します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし。switchport mode mac で MAC ポートに設定し，本コマンドを設定しない場合，デフォルト VLAN でだけ動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 有効な MAC VLAN が一つも設定されていない場合は，アクセスポートと同様の動作となります。
2. switchport mac dot1q vlan 設定は，switchport mode mac を設定したときに，有効となります。
3. 認証対象ポートである MAC ポートにレイヤ 2 認証機能の自動 VLAN 割当てにより，VLAN が自動で割り当てられた場合，下記コマンドを実行しても認証は解除されません。
   - 該当 VLAN の switchport mac vlan や switchport mac vlan add での設定
   - 該当 VLAN の no switchport mac や switchport mac vlan remove での削除

[関連コマンド]

switchport mode

vlan mac-based

switchport mode

レイヤ 2 インタフェースの属性（ポートの種類）を設定します。

[入力形式]

情報の設定・変更
switchport mode {access | trunk | protocol-vlan | mac-vlan }

情報の削除
no switchport mode

[入力モード]
(config-if)

[パラメータ]

{access | trunk | protocol-vlan | mac-vlan}
レイヤ 2 インタフェースの属性（ポートの種類）を設定します。

access
当該インタフェースをアクセスポートに設定します。アクセスポートでは，Untagged フレームを送信します。アクセスポートは 1 つの VLAN だけで使用できます。

trunk
当該インタフェースをトランクポートに設定します。トランクポートでは Untagged フレームと，Tagged フレームを送受信します。

protocol-vlan
当該インタフェースをプロトコルポートに設定します。プロトコルポートでは，Untagged フレームを送受信します。フレーム受信時は，そのフレームのプロトコル種別に基づいて VLAN を決定します。Tagged フレームは廃棄します。

mac-vlan
当該インタフェースを MAC ポートに設定します。MAC ポートでは Untagged フレームを送受信します。フレーム受信時は，そのフレームの送信元 MAC アドレスに基づいて VLAN を決定します。Tagged フレームは廃棄します。ただし，switchport mac dot1q vlan コマンドを設定している場合は，Tagged フレームを中継します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   access，trunk，protocol-vlan または mac-vlan

[コマンド省略時の動作]

access（アクセスポート）に設定します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 当該インタフェースをトランクポートに設定した場合，switchport trunk コマンドで allowed vlan を設定してください。トランクポートに設定し，allowed vlan が設定されていない場合，当該インタフェースではすべてのフレームが廃棄されます。
2. 当該インタフェースをプロトコルポートに設定した場合，switchport protocol コマンドでプロトコル VLAN を設定してください。プロトコル VLAN が設定されていない場合，当該インタフェースはアクセスポートと同様の動作となります。
3. 当該インタフェースに下記のコマンドを設定している場合，本コマンドでの変更はできません。
   - dot1x port-control
   - mac-authentication port
   - web-authentication port

[関連コマンド]

なし

switchport protocol

プロトコルポートの情報を設定します。

[入力形式]

情報の設定

switchport protocol vlan <VLAN ID list>
switchport protocol native vlan <VLAN ID>

情報の変更

switchport protocol {vlan <VLAN ID list> | vlan add <VLAN ID list> | vlan remove <VLAN ID list> | native vlan <VLAN ID>}

情報の削除

no switchport protocol vlan
no switchport protocol native vlan

[入力モード]

(config-if)

[パラメータ]

vlan <VLAN ID list>

このポートで有効なプロトコル VLAN を設定します。変更時は有効なプロトコル VLAN リストを設定されたリストに置き換えます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

native vlan <VLAN ID>

プロトコルがコンフィグレーションと一致しないフレームを送受信する VLAN を設定します。設定可能な VLAN はポート VLAN です。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

vlan add <VLAN ID list>

このポートで有効なプロトコル VLAN を VLAN リストに追加します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

vlan remove <VLAN ID list>

このポートで有効なプロトコル VLAN を VLAN リストから削除します。

1. 本パラメータ省略時の初期値
   省略できません。

2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし。switchport mode protocol でプロトコルポートに設定し，本コマンドを省略すると，デフォルト VLAN で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 有効なプロトコル VLAN が一つも設定されていない場合は，アクセスポートと同様の動作となります。
2. プロトコルポートに複数のプロトコル VLAN を設定する場合，プロトコル VLAN のプロトコルが重複しないように設定してください。

[関連コマンド]

switchport mode

vlan protocol-based

vlan-protocol

switchport trunk

トランクポートの情報を設定します。

[入力形式]

情報の設定

switchport trunk allowed vlan <VLAN ID list>

switchport trunk native vlan <VLAN ID>

情報の変更

switchport trunk native vlan <VLAN ID>

switchport trunk allowed vlan {<VLAN ID list> | add <VLAN ID list> | remove <VLAN ID list>}

情報の削除

no switchport trunk allowed vlan

no switchport trunk native vlan

[入力モード]

(config-if)

[パラメータ]

native vlan <VLAN ID>

ネイティブ VLAN（Untagged フレームを送受信する VLAN）を設定します。設定可能な VLAN はポート VLAN です。ネイティブ VLAN を設定しない場合，デフォルト VLAN がネイティブ VLAN になります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

allowed vlan <VLAN ID list>

トランクポートで送受信する VLAN を設定します。

設定されない VLAN のフレームは廃棄します。

Untagged フレームを送受信するためには，ネイティブ VLAN を設定する必要があります。ネイティブ VLAN を allowed vlan に設定しない場合は，Untagged フレームを廃棄します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

add <VLAN ID list>

設定済みの VLAN リストに VLAN を追加します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

remove <VLAN ID list>

設定済みの VLAN リストから VLAN を削除します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，値の設定範囲については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし。switchport mode trunk でトランクポートに設定していて，本コマンドを省略すると通信できません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

当該インタフェースにトランクポートを設定した場合，必ず allowed vlan を設定してください。allowed vlan を設定しないと，当該インタフェースでフレーム送受信を行いません。

また，Untagged フレームも送受信する場合は，下記のパラメータ両方に同じ VLAN ID を設定してください。

- allowed vlan
- native vlan

設定していない場合，当該インタフェースの Untagged フレームを廃棄します。

[関連コマンド]

switchport mode

vlan

vlan

VLAN に関する項目を設定します。

[入力形式]

情報の設定・変更

vlan <VLAN ID>
vlan <VLAN ID list>
vlan <VLAN ID> protocol-based
vlan <VLAN ID list> protocol-based
vlan <VLAN ID> mac-based
vlan <VLAN ID list> mac-based

情報の削除

no vlan <VLAN ID>
no vlan <VLAN ID list>

[入力モード]

(config)

[パラメータ]

<VLAN ID>

VLAN ID を設定します。本コマンドを入力後，config-vlan モードに移動します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。ただし，削除の場合，デフォルト VLAN（VLAN ID=1）は設定できません。

<VLAN ID list>

複数の VLAN ID を一括設定します。初めて設定する VLAN ID が含まれている場合，該当する VLAN を新規に作成します。本コマンドを入力後，config-vlan モードに移動します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。ただし，削除の場合，デフォルト VLAN（VLAN ID=1）は設定できません。

protocol-based

プロトコル VLAN の場合に設定します。

1. 本パラメータ省略時の初期値
   ポート VLAN となります。
2. 本パラメータ使用時の注意事項
   ・プロトコル VLAN を設定する場合は，protocol-based を設定する必要があります。
   ・すでにポート VLAN および MAC VLAN として作成した VLAN には設定できません。

mac-based

MAC VLAN の場合に設定します。

1. 本パラメータ省略時の初期値
   ポート VLAN となります。
2. 本パラメータ使用時の注意事項
   ・MAC VLAN を設定する場合は，mac-based を設定する必要があります。
   ・すでにポート VLAN およびプロトコル VLAN として作成した VLAN には設定できません。

[コマンド省略時の動作]

VLAN を設定しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. デフォルト VLAN（VLAN ID=1）は常に存在します。また，設定できる項目も通常の VLAN とは異なります。
2. <VLAN ID list> でリスト設定をすると，一度に複数の VLAN に関する設定ができます。しかし，コマンドの一部はリスト設定の配下（マルチコマンドモード）で使用できません。詳細については，次の表を参照してください。

項番	コマンド	マルチコマンドモード可否
1	state {suspend ｜ active}	○
2	name	×
3	protocol	○
4	mac-address	×

（凡例）　○：使用可能　×：使用不可

3. デフォルト VLAN の設定（VLAN ID=1）はコンフィグレーションファイル上に常に存在し，削除できません。デフォルト VLAN の初期状態は，すべてのポートがアクセスポートとして所属します。
4. デフォルト VLAN で設定できるパラメータの項目，およびデフォルト VLAN 固有の動作について次に示します。

   vlan コマンド
   　vlan コマンドでは，次の表のようになります。

項番	パラメータ	ユーザの設定可否	デフォルト VLAN 固有の動作
1	<VLAN ID>	△（固定値）	装置起動時に設定されます。 「1」固定。変更と削除不可。
2	<VLAN ID list>	△（固定値）	−
3	protocol-based	×	ポート VLAN
4	mac-based	×	ポート VLAN

（凡例）　△：固定値で設定可能　×：設定不可　−：該当しない

config-vlan モードコマンド

config-vlan モードコマンドでは，次の表のようになります。

項番	コマンド	パラメータ	ユーザの設定可否	デフォルト VLAN 特有の動作
1	state {suspend ｜ active}	－	○	－
2	name	<string>	○	－
3	protocol	<Protocol name>	×	－
4	mac-address	<MAC>	×	－

（凡例） ○：設定可能　×：設定不可　－：該当しない

5. vlan コマンドで VLAN を生成すると，interface vlan コマンドで VLAN インタフェースに情報が設定可能になります。vlan コマンドで生成した VLAN に対して no interface vlan コマンドで削除できます。また，interface vlan コマンドで生成した VLAN に対して no vlan コマンドで削除することもできます。
6. no vlan コマンドで自動 VLAN 割当の VLAN を指定した場合，MAC ポートに自動登録された VLAN も削除し，該当端末の認証も解除されます。

[関連コマンド]

なし

vlan-protocol

プロトコル VLAN 用のプロトコル名称とプロトコル値を設定します。

[入力形式]

情報の設定・変更

vlan-protocol <Protocol name> [ethertype <HEX enum>] [llc <HEX enum>] [snap-ethertype <HEX enum>]

情報の削除

no vlan-protocol <Protocol name>

[入力モード]

(config)

[パラメータ]

<Protocol name>

プロトコル VLAN の設定に使用するプロトコル名称を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   14 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」を参照してください。

ethertype <HEX enum>

EthernetV2 形式フレームの EtherType 値を設定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   4 けたの 16 進数

llc <HEX enum>

802.3 形式フレームの LLC 値（DSAP，SSAP）を設定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   4 けたの 16 進数

snap-ethertype <HEX enum>

802.3 形式フレームの EtherType 値を設定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   4 けたの 16 進数

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。ただし，プロトコル VLAN の protocol コマンドで設定されていないプロトコルについては，protocol コマンドでプロトコル名称が設定されたときに反映されます。

[注意事項]

1. EtherType 値（4 けたの 16 進数）に 05ff 以下の値を設定した場合は，0000 で動作します。
2. <HEX enum> は EtherType 値（4 けたの 16 進数）を 1 個または複数個設定できます。複数個設定する場合は，コンマ（,）で区切ってください。
3. ethertype，llc，snap-ethertype は順不同で入力できますが，運用コマンド show running-config では，ethertype，llc，snap-ethertype の順に表示されます。
4. １行内に最大 16 個の EtherType 値を設定できます。
5. １行に同じプロトコル値を複数設定できません。（例：vlan-protocol xxx ethertype <HEX> llc<HEX> ethertype<HEX>）
6. protocol コマンドで設定しているプロトコル名称は削除できません。

[関連コマンド]

protocol

12 スパニングツリー

spanning-tree portfast default
spanning-tree single
spanning-tree single cost
spanning-tree single forward-time
spanning-tree single hello-time
spanning-tree single max-age
spanning-tree single mode
spanning-tree single pathcost method
spanning-tree single port-priority
spanning-tree single priority
spanning-tree single transmission-limit
spanning-tree vlan
spanning-tree vlan cost
spanning-tree vlan forward-time
spanning-tree vlan hello-time
spanning-tree vlan max-age
spanning-tree vlan mode
spanning-tree vlan pathcost method
spanning-tree vlan port-priority
spanning-tree vlan priority
spanning-tree vlan transmission-limit

instance

マルチプルスパニングツリーの MST インスタンスに所属する VLAN を設定します。

[入力形式]

情報の設定・変更

instance <MSTI ID> vlans <VLAN ID list>

情報の削除

no instance <MSTI ID>

[入力モード]

(config-mst)

[パラメータ]

<MSTI ID>

MST インスタンス ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 4095

vlans <VLAN ID list>

MST インスタンスに所属する VLAN を設定します。一つの VLAN ID を設定できるほか，ハイフン (-)，コンマ（,）を使用して複数の VLAN ID の一括設定もできます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。
3. 本パラメータ使用時の注意事項
   ・MST インスタンス ID0 には，ほかの MST インスタンスに属していない VLAN すべてが所属します。
   ・同じ MST リージョンを構成するためには，MST インスタンス ID と本パラメータで設定する VLAN ID，および name パラメータの値と revision パラメータの値を MST リージョン内で一致させる必要があります。

[コマンド省略時の動作]

すべての VLAN が MST インスタンス ID0 に所属します。

[通信への影響]

spanning-tree mode コマンドで mst を設定している場合，トポロジの再計算によって，トポロジの形成が終了するまで通信断となります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. MST インスタンス ID0 に関する情報は，show コマンドでは表示しません。

[関連コマンド]

spanning-tree mst configuration

name

マルチプルスパニングツリーのリージョンを識別するための文字列を設定します。

[入力形式]

情報の設定・変更
name <Name>

情報の削除
no name

[入力モード]

(config-mst)

[パラメータ]

<Name>
リージョンを識別するための文字列を設定します。

1. 本パラメータ省略時の初期値
省略できません。
2. 値の設定範囲
32 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。
3. 本パラメータ使用時の注意事項
同じ MST リージョンを構成するためには，本パラメータと revision パラメータの値，および MST インスタンス ID と vlans パラメータで設定する VLAN ID を MST リージョン内で一致させる必要があります。

[コマンド省略時の動作]

name が Null で動作します。

[通信への影響]

spanning-tree mode コマンドで mst を設定している場合，トポロジの再計算によって，トポロジの形成が終了するまで通信断となります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree mst configuration

revision

マルチプルスパニングツリーのリージョンを識別するためのリビジョン番号を設定します。

[入力形式]

情報の設定・変更

revision <Version>

情報の削除

no revision

[入力モード]

(config-mst)

[パラメータ]

<Version>

リージョンを識別するためのリビジョン番号を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535
3. 本パラメータ使用時の注意事項
   同じ MST リージョンを構成するためには，本パラメータと name パラメータの値，および MST インスタンス ID と vlans パラメータで設定する VLAN ID を MST リージョン内で一致させる必要があります。

[コマンド省略時の動作]

revision が 0 で動作します。

[通信への影響]

spanning-tree mode コマンドで mst を設定している場合，トポロジの再計算によって，トポロジの形成が終了するまで通信断となります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree mst configuration

spanning-tree bpdufilter

該当ポートに BPDU フィルタ機能を設定します。本コマンドは，PVST+，シングルスパニングツリー，マルチプルスパニングツリーの該当ポートに適用します。

[入力形式]

情報の設定

spanning-tree bpdufilter enable

情報の削除

no spanning-tree bpdufilter

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定した場合，BPDU ガード機能は無効となります。

[関連コマンド]

なし

spanning-tree bpduguard

該当ポートに，BPDU ガード機能を設定します。本コマンドは，PVST+，シングルスパニングツリー，マルチプルスパニングツリーの該当ポートに適用し，PortFast 機能を設定したポートで動作します。

[入力形式]

情報の設定・変更

spanning-tree bpduguard { enable | disable }

情報の削除

no spanning-tree bpduguard

[入力モード]

(config-if)

[パラメータ]

{ enable | disable }

enable を設定した場合，BPDU ガード機能を適用します。disable を設定した場合，BPDU ガード機能の停止を適用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   enable または disable

[コマンド省略時の動作]

spanning-tree portfast bpduguard default コマンドの設定に従います。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree portfast default

spanning-tree portfast

spanning-tree portfast bpduguard default

spanning-tree cost

該当ポートのパスコストを設定します。本コマンドは，PVST+，シングルスパニングツリー，マルチプルスパニングツリーに適用します。

［入力形式］

情報の設定・変更

spanning-tree cost <Cost>

情報の削除

no spanning-tree cost

［入力モード］

(config-if)

［パラメータ］

<Cost>

パスコスト値を設定します。コスト値が小さいほど，該当するフレームを転送するポートとして使用する可能性が高くなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   spanning-tree pathcost method コマンドで short を設定した場合
   1 ～ 65535
   spanning-tree pathcost method コマンドで long を設定した場合
   1 ～ 200000000
3. 本パラメータ使用時の注意事項
   パスコスト値が変わることでトポロジ変更が発生する場合があります。

［コマンド省略時の動作］

spanning-tree pathcost method コマンドの設定に従い，パスコストを適用します。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. spanning-tree vlan cost コマンド，spanning-tree single cost コマンド，または spanning-tree mst cost コマンドを設定している場合は，本コマンドの値は適用しません。
2. spanning-tree vlan pathcost method コマンドまたは spanning-tree single pathcost method コマンドを設定している場合は，本コマンドの値は適用しません。

［関連コマンド］

spanning-tree pathcost method

spanning-tree vlan pathcost method

spanning-tree vlan cost

spanning-tree single pathcost method

spanning-tree single cost

spanning-tree mst cost

spanning-tree disable

PVST+，シングルスパニングツリー，マルチプルスパニングツリーのスパニングツリー機能の停止を設定します。

[入力形式]

情報の設定

spanning-tree disable

情報の削除

no spanning-tree disable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

スパニングツリーが動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree guard

該当ポートに，ガード機能を設定します。本コマンドは，PVST+，シングルスパニングツリー，マルチプルスパニングツリーの該当ポートに適用します。

[入力形式]

情報の設定・変更

spanning-tree guard { loop | none | root }

情報の削除

no spanning-tree guard

[入力モード]

(config-if)

[パラメータ]

{ loop | none | root }

loop：該当ポートにループガード機能を適用します。マルチプルスパニングツリーではループガードは動作しません。

none：該当ポートのループガード・ルートガード機能を停止します。

root：該当ポートにルートガード機能を適用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   loop，none，または root

[コマンド省略時の動作]

ループガード機能：spanning-tree loopguard default コマンドの設定に従います。

ルートガード機能：動作しません。

[通信への影響]

なし

[設定値の反映契機]

ループガード設定：

- spanning-tree portfast default コマンドまたは spanning-tree portfast コマンドが設定されている場合，ループガード設定は反映されません。
- spanning-tree portfast default コマンド，spanning-tree portfast コマンドの設定を削除すると，すぐにループガードの運用を開始します。

ルートガード設定：

- 設定後，すぐに運用に反映されます。

[注意事項]

1. spanning-tree portfast default コマンドまたは spanning-tree portfast コマンドが設定されている場合，ループガード設定は反映されません。ルートガード設定は反映されます。

[関連コマンド]

spanning-tree loopguard default

spanning-tree link-type

該当ポートのリンクタイプを設定します。本コマンドは，PVST+，シングルスパニングツリー，マルチプルスパニングツリーの該当ポートに適用します。spanning-tree mode コマンドで rapid-pvst または mst を設定した場合，および spanning-tree vlan mode コマンドで rapid-pvst を設定した場合，高速トポロジ変更をするには，ブリッジ間接続が Point-to-Point でなければなりません。spanning-tree single mode コマンドで rapid-stp を設定した場合，高速トポロジ変更をするには，ブリッジ間接続が Point-to-Point でなければなりません。

[入力形式]

情報の設定・変更

spanning-tree link-type { point-to-point | shared }

情報の削除

no spanning-tree link-type

[入力モード]

(config-if)

[パラメータ]

{ point-to-point | shared }

point-to-point を設定した場合，リンクタイプに Point-to-Point 接続を適用します。shared を設定した場合，リンクタイプに shared 接続を適用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   point-to-point または shared

[コマンド省略時の動作]

全二重ポートの場合は point-to-point，半二重ポートの場合は shared として動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. point-to-point を設定した場合，STP 互換モードの自動復旧機能が動作します。shared を設定した場合，STP 互換モードの自動復旧機能は動作しません。

[関連コマンド]

spanning-tree mode

spanning-tree vlan mode

spanning-tree single mode

spanning-tree loopguard default

ループガード機能をデフォルトで設定します。本コマンドは，PVST+，シングルスパニングツリーのポートで有効になります。

[入力形式]

情報の設定

spanning-tree loopguard default

情報の削除

no spanning-tree loopguard default

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

spanning-tree guard コマンドを設定している場合，その設定に従います。

spanning-tree guard コマンドを設定していない場合，動作しません。

[通信への影響]

なし

[設定値の反映契機]

- spanning-tree portfast default コマンドまたは spanning-tree portfast コマンドが設定されている場合，ループガード設定は反映されません。
- spanning-tree portfast default コマンド，spanning-tree portfast コマンドの設定を削除すると，すぐにループガードの運用を開始します。

[注意事項]

1. spanning-tree portfast default コマンドまたは spanning-tree portfast コマンドが設定されている場合，ループガード設定は反映されません。

[関連コマンド]

spanning-tree guard

spanning-tree mode

スパニングツリーの動作モードを設定します。本コマンドは，シングルスパニングツリー以外の PVST+，マルチプルスパニングツリーに適用します。PVST+ の動作モードで spanning-tree vlan mode コマンドを設定している場合は，その設定に従います。

[入力形式]

情報の設定・変更

spanning-tree mode { pvst | rapid-pvst | mst }

情報の削除

no spanning-tree mode

[入力モード]

(config)

[パラメータ]

{ pvst | rapid-pvst | mst }

使用するプロトコルを設定します。スパニングツリー運用中にプロトコルを変更した場合，スパニングツリーを再初期化します。pvst を設定した場合，すべてのスパニングツリーが PVST+ を適用します。rapid-pvst を設定した場合，すべてのスパニングツリーが高速 PVST+ を適用します。mst を設定した場合，すべてのスパニングツリーがマルチプルスパニングツリーを適用します。シングルスパニングツリーを使用する場合は，pvst または rapid-pvst を設定する必要があります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   pvst，rapid-pvst，または mst

[コマンド省略時の動作]

コンフィグレーションとして明示的に spanning-tree mode pvst が設定されます。

[通信への影響]

トポロジの再計算によって，トポロジの形成が終了するまで通信断となります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree link-type

spanning-tree mst configuration

マルチプルスパニングツリーのリージョン形成に必要な情報を設定するための，config-mst モードに移行します。本設定を削除した場合，すでに設定しているリージョン形成に必要な情報をすべて削除します。

[入力形式]

情報の設定

spanning-tree mst configuration

情報の削除

no spanning-tree mst configuration

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

instance

name

revision

spanning-tree mst cost

マルチプルスパニングツリーの該当ポートのパスコストを設定します。

[入力形式]

情報の設定・変更

spanning-tree mst <MSTI ID list> cost <Cost>

情報の削除

no spanning-tree mst <MSTI ID list> cost

[入力モード]

(config-if)

[パラメータ]

<MSTI ID list>

MST インスタンス ID を設定します。一つの MST インスタンス ID を設定できるほか，ハイフン（-)，コンマ（,）を使用して複数の MST インスタンス ID の一括設定もできます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 4095

<Cost>

パスコスト値を設定します。コスト値が小さいほど，該当するフレームを転送するポートとして使用する可能性が高くなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 200000000
3. 本パラメータ使用時の注意事項
   パスコスト値が変わることでトポロジ変更が発生する場合があります。

[コマンド省略時の動作]

spanning-tree cost コマンドの設定に従います。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree cost

spanning-tree mst forward-time

マルチプルスパニングツリーの状態遷移に要する時間を設定します。

[入力形式]

情報の設定・変更
　spanning-tree mst forward-time <Seconds>

情報の削除
　no spanning-tree mst forward-time

[入力モード]

(config)

[パラメータ]

<Seconds>

ポートが状態遷移に要する時間を秒単位で設定します。
stp-compatible モードのポートの場合，リスニング状態，ラーニング状態を設定時間だけ維持します。stp-compatible モードのポートでない場合，ディスカーディング状態，ラーニング状態を設定時間だけ維持します（ただし，タイマによる状態遷移が発生した場合だけです）。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   4 ～ 30（秒）

[コマンド省略時の動作]

ポートが状態遷移に要する時間は 15 秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree mst hello-time

マルチプルスパニングツリーの BPDU の送信間隔を設定します。

[入力形式]

情報の設定・変更
spanning-tree mst hello-time <Hello time>

情報の削除
no spanning-tree mst hello-time

[入力モード]

(config)

[パラメータ]

<Hello time>

本装置が定期的に送信する BPDU の送信間隔を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10(秒)
3. 本パラメータ使用時の注意事項
   1 を設定すると，トポロジ変更が発生しやすくなります。

[コマンド省略時の動作]

BPDU の送信間隔は 2 秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree mst max-age

マルチプルスパニングツリーの送信する BPDU の最大有効時間を設定します。

[入力形式]

情報の設定・変更

spanning-tree mst max-age <Seconds>

情報の削除

no spanning-tree mst max-age

[入力モード]

(config)

[パラメータ]

<Seconds>

本装置が送信する BPDU の最大有効時間を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   6 ～ 40（秒）
3. 本パラメータ使用時の注意事項
   20 未満の値を設定すると，トポロジ変更が発生しやすくなります。

[コマンド省略時の動作]

送信できる BPDU の最大有効時間は 20 秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree mst max-hops

マルチプルスパニングツリーの BPDU の最大ホップカウント数を設定します。

[入力形式]

情報の設定・変更

spanning-tree mst max-hops <Hop number>

spanning-tree mst <MSTI ID list> max-hops <Hop number>

情報の削除

no spanning-tree mst max-hops

no spanning-tree mst <MSTI ID list> max-hops

[入力モード]

(config)

[パラメータ]

<MSTI ID list>

MST インスタンス ID を設定します。一つの MST インスタンス ID を設定できるほか，ハイフン（-），コンマ（,）を使用して複数の MST インスタンス ID の一括設定もできます。

1. 本パラメータ省略時の初期値
   すべての MST インスタンスが対象になります。
2. 値の設定範囲
   0 ～ 4095

<Hop number>

本装置が送信する BPDU の最大ホップカウント数を設定します。

1. 本パラメータ省略時の初期値
   20
2. 値の設定範囲
   2 ～ 40

[コマンド省略時の動作]

BPDU の最大ホップカウント数は 20 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree mst port-priority

マルチプルスパニングツリーの，MST インスタンスごとの該当ポートの優先度を設定します。

[入力形式]

情報の設定・変更

spanning-tree mst <MSTI ID list> port-priority <Priority>

情報の削除

no spanning-tree mst <MSTI ID list> port-priority

[入力モード]

(config-if)

[パラメータ]

<MSTI ID list>

MST インスタンス ID を設定します。一つの MST インスタンス ID を設定できるほか，ハイフン (-)，コンマ（,）を使用して複数の MST インスタンス ID の一括設定もできます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 4095

<Priority>

ポートの優先度を設定します。16 の倍数をポート優先度として使用します。値が小さいほど優先度が高くなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 240
3. 本パラメータ使用時の注意事項
   ポート優先度が変わることによって，トポロジ変更が発生する場合があります。

[コマンド省略時の動作]

spanning-tree port-priority コマンドの設定に従います。spanning-tree port-priority コマンドの設定がない場合は，ポート優先度を 128 として動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree port-priority

spanning-tree mst root priority

マルチプルスパニングツリーの MST インスタンスごとのブリッジ優先度を設定します。

[入力形式]

情報の設定・変更

spanning-tree mst <MSTI ID list> root priority <Priority>

情報の削除

no spanning-tree mst <MSTI ID list> root priority

[入力モード]

(config)

[パラメータ]

<MSTI ID list>

MST インスタンス ID を設定します。一つの MST インスタンス ID を設定できるほか，ハイフン（-），コンマ（,）を使用して複数の MST インスタンス ID の一括設定もできます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 4095

<Priority>

ブリッジ優先度を設定します。値が小さいほど優先度が高くなります。4096 の倍数をブリッジ優先度として使用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 61440
3. 本パラメータ使用時の注意事項
   ブリッジ優先度が変わることによって，トポロジ変更が発生する場合があります。

[コマンド省略時の動作]

ブリッジ優先度は 32768 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree mst transmission-limit

マルチプルスパニングツリーの hello-time 当たりに送信できる最大 BPDU 数を設定します。

[入力形式]

情報の設定・変更

spanning-tree mst transmission-limit <Counts>

情報の削除

no spanning-tree mst transmission-limit

[入力モード]

(config)

[パラメータ]

<Counts>

hello-time 当たりに送信できる最大 BPDU 数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10

[コマンド省略時の動作]

送信できる最大 BPDU 数は 3 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree pathcost method

ポートのパスコストに 16bit 値を使用するか，32bit 値を使用するかを設定します。本コマンドは，マルチプルスパニングツリー以外の，PVST+，シングルスパニングツリーに適用します。

spanning-tree vlan pathcost method コマンドまたは spanning-tree single pathcost method コマンドを設定している場合は，本コマンドの値は適用しません。

spanning-tree cost コマンド，spanning-tree vlan cost コマンド，または spanning-tree single cost コマンドの設定を省略した場合，パスコストはインタフェース速度と spanning-tree pathcost method コマンドの設定によって，下記の値を適用します。

- spanning-tree pathcost method コマンドで short を設定した場合
  10Mbit/s：100
  100Mbit/s：19
  1Gbit/s：4
- spanning-tree pathcost method コマンドで long を設定した場合
  10Mbit/s：2000000
  100Mbit/s：200000
  1Gbit/s：20000

[入力形式]

情報の設定・変更

spanning-tree pathcost method { long | short }

情報の削除

no spanning-tree pathcost method

[入力モード]

(config)

[パラメータ]

{ long | short }

long を設定した場合，32bit 値を使用します。short を設定した場合，16bit 値を使用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   long または short
3. 本パラメータ使用時の注意事項
   ・パスコストのデフォルト値が変わります。
   ・パスコスト値が変わることでトポロジ変更が発生する場合があります。
   ・パスコストに 65536 以上の値を設定している場合は，short に変更することはできません。

[コマンド省略時の動作]

パスコストモードは short で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. spanning-tree mode コマンドで mst を設定した場合，マルチプルスパニングツリーが 32bit 値で動作します。spanning-tree cost コマンドで 65536 以上のパスコスト値を設定するためには，本コマンドで long を設定しておく必要があります。
   spanning-tree mst cost コマンドでパスコスト値を設定する場合は，本コマンドの設定は必要ありません。

[関連コマンド]

spanning-tree cost

spanning-tree vlan pathcost method

spanning-tree vlan cost

spanning-tree single pathcost method

spanning-tree single cost

spanning-tree port-priority

該当ポートのポート優先度を設定します。本コマンドは，PVST+，シングルスパニングツリー，マルチプルスパニングツリーで適用します。

[入力形式]

情報の設定・変更
spanning-tree port-priority <Priority>

情報の削除
no spanning-tree port-priority

[入力モード]

(config-if)

[パラメータ]

<Priority>
ポートの優先度を設定します。16 の倍数をポート優先度として使用します。値が小さいほど優先度が高くなります。

1. 本パラメータ省略時の初期値
省略できません。
2. 値の設定範囲
0 ～ 240
3. 本パラメータ使用時の注意事項
ポート優先度が変わることによって，トポロジ変更が発生する場合があります。

[コマンド省略時の動作]

spanning-tree vlan port-priority コマンド，spanning-tree single port-priority コマンド，または spanning-tree mst port-priority コマンドの設定に従います。ここに示したコマンドの設定がない場合は，ポート優先度を 128 として動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree vlan port-priority

spanning-tree single port-priority

spanning-tree mst port-priority

spanning-tree portfast

該当ポートに PortFast 機能を設定します。本コマンドは，PVST+，シングルスパニングツリー，マルチプルスパニングツリーの該当ポートに適用します。

[入力形式]

情報の設定・変更

spanning-tree portfast [{ trunk | disable }]

情報の削除

no spanning-tree portfast

[入力モード]

(config-if)

[パラメータ]

{ trunk | disable }

trunk を設定した場合，アクセスポート，トランクポート，プロトコルポート，MAC ポートで PortFast 機能を適用します。

disable を設定した場合，PortFast 機能を停止します。

1. 本パラメータ省略時の初期値
   アクセスポート，プロトコルポート，MAC ポートで有効となる，PortFast 機能を適用します。
2. 値の設定範囲
   trunk または disable

[コマンド省略時の動作]

spanning-tree portfast default コマンドの設定に従います。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree portfast default

spanning-tree portfast bpduguard default

BPDU ガード機能をデフォルトで設定します。本コマンドは，PVST+，シングルスパニングツリー，マルチプルスパニングツリーの PortFast 機能を設定したすべてのポートで有効になります。

[入力形式]

情報の設定

spanning-tree portfast bpduguard default

情報の削除

no spanning-tree portfast bpduguard default

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

spanning-tree bpduguard コマンドを設定している場合は，その設定に従います。spanning-tree bpduguard コマンドの設定がない場合は動作しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree portfast default

spanning-tree portfast

spanning-tree bpduguard

spanning-tree portfast default

PortFast 機能をデフォルトで設定します。本コマンドは，PVST+，シングルスパニングツリー，マルチプルスパニングツリーのアクセスポート，プロトコルポート，MAC ポートで有効になります。

[入力形式]

情報の設定

spanning-tree portfast default

情報の削除

no spanning-tree portfast default

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

spanning-tree portfast コマンドを設定している場合は，その設定に従います。spanning-tree portfast コマンドの設定がない場合は動作しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree portfast

spanning-tree single

シングルスパニングツリーのトポロジ計算を開始します。スパニングツリーの動作モードが PVST+ の場合に，VLAN 1 をシングルスパニングツリー対象にします。

[入力形式]

情報の設定

spanning-tree single

情報の削除

no spanning-tree single

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. VLAN 1 が PVST+ 対象であった場合，VLAN 1 の PVST+ は停止します。シングルスパニングツリーを削除すると，VLAN 1 は PVST+ 対象になります。動作モードがマルチプルスパニングツリーの場合はシングルスパニングツリーは動作しません。

[関連コマンド]

spanning-tree mode

spanning-tree single cost

シングルスパニングツリーの該当ポートのパスコストを設定します。

[入力形式]

情報の設定・変更

spanning-tree single cost <Cost>

情報の削除

no spanning-tree single cost

[入力モード]

(config-if)

[パラメータ]

<Cost>

パスコスト値を設定します。コスト値が小さいほど，該当するフレームを転送するポートとして使用する可能性が高くなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   spanning-tree pathcost method コマンドまたは spanning-tree single pathcost method コマンドで short を設定した場合
   1 ～ 65535
   spanning-tree pathcost method コマンドまたは spanning-tree single pathcost method コマンドで long を設定した場合
   1 ～ 200000000
3. 本パラメータ使用時の注意事項
   パスコスト値が変わることでトポロジ変更が発生する場合があります。

[コマンド省略時の動作]

spanning-tree single pathcost method コマンドの設定に従って，パスコストを適用します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree cost

spanning-tree pathcost method

spanning-tree single pathcost method

spanning-tree single forward-time

シングルスパニングツリーの状態遷移に要する時間を設定します。

[入力形式]

情報の設定・変更

spanning-tree single forward-time <Seconds>

情報の削除

no spanning-tree single forward-time

[入力モード]

(config)

[パラメータ]

<Seconds>

ポートが状態遷移に要する時間を秒単位で設定します。

spanning-tree single mode コマンドで stp（802.1D）を設定した場合，リスニング状態，ラーニング状態を設定時間だけ維持します。spanning-tree single mode コマンドで rapid-stp（802.1w）を設定した場合，ディスカーディング状態，ラーニング状態を設定時間だけ維持します（ただし，タイマによる状態遷移が発生した場合だけです）。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   4 ～ 30（秒）

[コマンド省略時の動作]

ポートが状態遷移に要する時間を 15 秒として動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree single mode

spanning-tree single hello-time

シングルスパニングツリーの BPDU の送信間隔を設定します。

[入力形式]

情報の設定・変更

spanning-tree single hello-time <Hello time>

情報の削除

no spanning-tree single hello-time

[入力モード]

(config)

[パラメータ]

<Hello time>

本装置が定期的に送信する BPDU の送信間隔を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10（秒）
3. 本パラメータ使用時の注意事項
   1 を設定すると，トポロジ変更が発生しやすくなります。

[コマンド省略時の動作]

BPDU の送信間隔は 2 秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree single max-age

シングルスパニングツリーの送信する BPDU の最大有効時間を設定します。

[入力形式]

情報の設定・変更

spanning-tree single max-age <Seconds>

情報の削除

no spanning-tree single max-age

[入力モード]

(config)

[パラメータ]

<Seconds>

本装置が送信する BPDU の最大有効時間を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   6 ～ 40(秒)
3. 本パラメータ使用時の注意事項
   20 未満の値を設定すると,トポロジ変更が発生しやすくなります。

[コマンド省略時の動作]

送信できる BPDU の最大有効時間は 20 秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後,すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree single mode

シングルスパニングツリーの動作モードを設定します。

[入力形式]

情報の設定・変更
spanning-tree single mode { stp | rapid-stp }

情報の削除
no spanning-tree single mode

[入力モード]

(config)

[パラメータ]

{ stp | rapid-stp }
使用するプロトコルを設定します。スパニングツリー運用中にプロトコルを変更した場合，スパニングツリーを再初期化します。stp を設定した場合，スパニングツリーで動作します。rapid-stp を設定した場合，高速スパニングツリーで動作します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   stp または rapid-stp

[コマンド省略時の動作]

シングルスパニングツリーの動作モードは stp で動作します。

[通信への影響]

spanning-tree single コマンドを設定している場合，トポロジの再計算によって，トポロジの形成が終了するまで通信断となります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree single pathcost method

シングルスパニングツリーのポートのパスコストに 16bit 値を使用するか，32bit 値を使用するかを設定します。

spanning-tree single cost コマンドの設定を省略した場合，パスコストはインタフェース速度と spanning-tree single pathcost method コマンドの設定によって，下記の値を適用します。

- spanning-tree single pathcost method コマンドで short を設定した場合
  10Mbit/s：100
  100Mbit/s：19
  1Gbit/s：4
- spanning-tree single pathcost method コマンドで long を設定した場合
  10Mbit/s：2000000
  100Mbit/s：200000
  1Gbit/s：20000

[入力形式]

情報の設定・変更
　spanning-tree single pathcost method { long | short }

情報の削除
　no spanning-tree single pathcost method

[入力モード]

(config)

[パラメータ]

{ long | short }

long を設定した場合，32bit 値を使用します。short を設定した場合，16bit 値を使用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   long または short
3. 本パラメータ使用時の注意事項
   ・パスコストのデフォルト値が変わります。
   ・パスコスト値が変わることでトポロジ変更が発生する場合があります。
   ・パスコストに 65536 以上の値を設定している場合，short には変更できません。

[コマンド省略時の動作]

spanning-tree pathcost method コマンドの設定に従います。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree single port-priority

シングルスパニングツリーの該当ポートの優先度を設定します。

[入力形式]

情報の設定・変更

spanning-tree single port-priority <Priority>

情報の削除

no spanning-tree single port-priority

[入力モード]

(config-if)

[パラメータ]

<Priority>

ポートの優先度を設定します。16 の倍数をポート優先度として使用します。値が小さいほど優先度が高くなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 240
3. 本パラメータ使用時の注意事項
   ポート優先度が変わることによって，トポロジ変更が発生する場合があります。

[コマンド省略時の動作]

spanning-tree port-priority コマンドの設定に従います。spanning-tree port-priority コマンドの設定がない場合は，ポート優先度を 128 として動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree single priority

シングルスパニングツリーのブリッジ優先度を設定します。

[入力形式]

情報の設定・変更

spanning-tree single priority <Priority>

情報の削除

no spanning-tree single priority

[入力モード]

(config)

[パラメータ]

<Priority>

ブリッジ優先度を設定します。値が小さいほど優先度が高くなります。4096 の倍数をブリッジ優先度として使用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 61440
3. 本パラメータ使用時の注意事項
   ブリッジ優先度が変わることによって，トポロジ変更が発生する場合があります。

[コマンド省略時の動作]

ブリッジ優先度は 32768 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree single transmission-limit

シングルスパニングツリーの hello-time 当たりに送信できる最大 BPDU 数を設定します。

[入力形式]

情報の設定・変更

spanning-tree single transmission-limit <Counts>

情報の削除

no spanning-tree single transmission-limit

[入力モード]

(config)

[パラメータ]

<Counts>

hello-time 当たりに送信できる最大 BPDU 数を設定します。

spanning-tree single mode コマンドで rapid-stp（802.1w）を設定した場合だけ有効なパラメータです。spanning-tree single mode コマンドで stp（802.1D）を設定した場合は，１秒間当たりに送信できる最大 BPDU 数は 3（固定）であり，本設定値は参照しません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10

[コマンド省略時の動作]

送信できる最大 BPDU 数は 3 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree single mode

spanning-tree single hello-time

spanning-tree vlan

PVST+ を設定します。spanning-tree single コマンドを設定している状態で no spanning-tree vlan コマンドを設定すると，該当 VLAN がシングルスパニングツリー対象の VLAN となり動作します。

［入力形式］

情報の設定・変更

no spanning-tree vlan <VLAN ID list>

情報の削除

spanning-tree vlan <VLAN ID list>

［入力モード］

(config)

［パラメータ］

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。
3. 本コマンド使用時の注意事項
   spanning-tree single コマンドを設定している場合，VLAN1 は PVST+ で動作しません。

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

なし

［関連コマンド］

vlan

spanning-tree vlan cost

PVST+ の該当ポートのパスコストを設定します。

[入力形式]

情報の設定・変更

spanning-tree vlan <VLAN ID list> cost <Cost>

情報の削除

no spanning-tree vlan <VLAN ID list> cost

[入力モード]

(config-if)

[パラメータ]

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

<Cost>

パスコスト値を設定します。コスト値が小さいほど，該当するフレームを転送するポートとして使用する可能性が高くなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   spanning-tree pathcost method コマンドまたは spanning-tree vlan < VLAN ID list > pathcost method コマンドで short を設定した場合
   1 〜 65535
   spanning-tree pathcost method コマンドまたは spanning-tree vlan < VLAN ID list > pathcost method コマンドで long を設定した場合
   1 〜 200000000
3. 本パラメータ使用時の注意事項
   ポート優先度が変わることによって，トポロジ変更が発生する場合があります。

[コマンド省略時の動作]

spanning-tree vlan pathcost method コマンドの設定に従って，パスコストを適用します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree cost

spanning-tree pathcost method

spanning-tree vlan pathcost method

spanning-tree vlan forward-time

PVST+ の状態遷移に要する時間を設定します。

[入力形式]

情報の設定・変更
spanning-tree vlan <VLAN ID list> forward-time <Seconds>

情報の削除
no spanning-tree vlan <VLAN ID list> forward-time

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

<Seconds>

ポートが状態遷移に要する時間を秒単位で設定します。

spanning-tree mode コマンドまたは spanning-tree vlan < VLAN ID list > mode コマンドで pvst（802.1D）を設定した場合，リスニング状態，ラーニング状態を設定時間だけ維持します。

spanning-tree mode コマンドまたは spanning-tree vlan < VLAN ID list > mode コマンドで rapid-pvst（802.1w）を設定した場合，ディスカーディング状態，ラーニング状態を設定時間だけ維持します（ただし，タイマによる状態遷移が発生した場合だけです）。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   4 ～ 30（秒）

[コマンド省略時の動作]

ポートが状態遷移に要する時間は 15 秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree mode

spanning-tree vlan mode

spanning-tree vlan hello-time

PVST+ の BPDU の送信間隔を設定します。

[入力形式]

情報の設定・変更

spanning-tree vlan <VLAN ID list> hello-time <Hello time>

情報の削除

no spanning-tree vlan <VLAN ID list> hello-time

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

<Hello time>

本装置が定期的に送信する BPDU の送信間隔を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10（秒）
3. 本パラメータ使用時の注意事項
   1 を設定すると，トポロジ変更が発生しやすくなります。

[コマンド省略時の動作]

BPDU の送信間隔は 2 秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree vlan max-age

PVST+ の送信する BPDU の最大有効時間を設定します。

[入力形式]

情報の設定・変更

spanning-tree vlan <VLAN ID list> max-age <Seconds>

情報の削除

no spanning-tree vlan <VLAN ID list> max-age

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

<Seconds>

本装置が送信する BPDU の最大有効時間を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   6 ～ 40（秒）
3. 本パラメータ使用時の注意事項
   20 未満の値を設定すると，トポロジ変更が発生しやすくなります。

[コマンド省略時の動作]

送信できる BPDU の最大有効時間は 20 秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree vlan mode

PVST+ の動作モードを設定します。

[入力形式]

情報の設定・変更

spanning-tree vlan <VLAN ID list> mode { pvst | rapid-pvst }

情報の削除

no spanning-tree vlan <VLAN ID list> mode

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

{ pvst | rapid-pvst }

使用するプロトコルを設定します。スパニングツリー運用中にプロトコルを変更した場合，スパニングツリーを再初期化します。pvst を設定した場合，PVST+ で動作します。rapid-pvst を設定した場合，高速 PVST+ で動作します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   pvst または rapid-pvst

[コマンド省略時の動作]

PVST+ の動作モードは spanning-tree mode コマンドの設定に従います。

[通信への影響]

spanning-tree mode コマンドの設定で pvst または rapid-pvst を設定している場合，トポロジの再計算によって，トポロジの形成が終了するまで通信断となります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree mode

spanning-tree vlan pathcost method

PVST+ のポートのパスコストに 16bit 値を使用するか，32bit 値を使用するかを設定します。

spanning-tree vlan cost コマンドの設定を省略した場合，パスコストはインタフェース速度と spanning-tree vlan pathcost method コマンドによる設定によって，下記の値を適用します。

- spanning-tree vlan pathcost method コマンドで short を設定した場合
  10Mbit/s：100
  100Mbit/s：19
  1Gbit/s：4
- spanning-tree vlan pathcost method コマンドで long を設定した場合
  10Mbit/s：2000000
  100Mbit/s：200000
  1Gbit/s：20000

[入力形式]

情報の設定・変更

spanning-tree vlan <VLAN ID list> pathcost method { long | short }

情報の削除

no spanning-tree vlan <VLAN ID list> pathcost method

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

{ long | short }

long を設定した場合，32bit 値を使用します。short を設定した場合，16bit 値を使用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   long または short
3. 本パラメータ使用時の注意事項
   ・パスコストのデフォルト値が変わります。
   ・パスコスト値が変わることでトポロジ変更が発生する場合があります。
   ・パスコストに 65536 以上の値を設定している場合，short には変更できません。

[コマンド省略時の動作]

spanning-tree pathcost method コマンドの設定に従います。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree pathcost method

spanning-tree cost

spanning-tree vlan cost

spanning-tree vlan port-priority

PVST+ の該当ポートの優先度を設定します。

[入力形式]

情報の設定・変更

spanning-tree vlan <VLAN ID list> port-priority <Priority>

情報の削除

no spanning-tree vlan <VLAN ID list> port-priority

[入力モード]

(config-if)

[パラメータ]

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

<Priority>

ポートの優先度を設定します。16 の倍数をポート優先度として使用します。値が小さいほど優先度が高くなります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 240
3. 本パラメータ使用時の注意事項
   ポート優先度が変わることによって，トポロジ変更が発生する場合があります。

[コマンド省略時の動作]

spanning-tree port-priority コマンドの設定に従います。spanning-tree port-priority コマンドの設定がない場合は，ポート優先度を 128 として動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree port-priority

spanning-tree vlan priority

PVST+ のブリッジ優先度を設定します。

[入力形式]

情報の設定・変更

spanning-tree vlan <VLAN ID list> priority <Priority>

情報の削除

no spanning-tree vlan <VLAN ID list> priority

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

<Priority>

ブリッジ優先度を設定します。値が小さいほど優先度が高くなります。
4096 の倍数をブリッジ優先度として使用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 61440
3. 本パラメータ使用時の注意事項
   ブリッジ優先度が変わることによって，トポロジ変更が発生する場合があります。

[コマンド省略時の動作]

ブリッジ優先度は 32768 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

spanning-tree vlan transmission-limit

PVST+ の hello-time 当たりに送信できる最大 BPDU 数を設定します。

[入力形式]

情報の設定・変更

spanning-tree vlan <VLAN ID list> transmission-limit <Counts>

情報の削除

no spanning-tree vlan <VLAN ID list> transmission-limit

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

設定した VLAN の PVST+ の設定を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

<Counts>

hello-time 当たりに送信できる最大 BPDU 数を設定します。

spanning-tree mode コマンドまたは spanning-tree vlan <VLAN ID list > mode コマンドで rapid-pvst（802.1w）を設定した場合だけ有効なパラメータです。spanning-tree mode コマンドまたは spanning-tree vlan <VLAN ID list > mode コマンドで pvst（802.1D）を設定した場合は，1 秒間当たりに送信できる最大 BPDU 数は 3（固定）であり，本設定値は参照しません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10

[コマンド省略時の動作]

送信できる最大 BPDU 数は 3 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

spanning-tree mode

spanning-tree vlan mode

spanning-tree vlan hello-time

13 Ring Protocol【S2200】【SS1250】【SS1240】

axrp

リング ID を設定します。また，Ring Protocol 機能に必要な情報を設定するため，config-axrp モードに移行します。本装置にはリング ID を 4 個まで設定できます。

本設定を削除した場合，リング ID にすでに設定されているリング情報は削除されます。

[入力形式]

情報の設定
　axrp <Ring ID>

情報の削除
　no axrp <Ring ID>

[入力モード]

（config）

[パラメータ]

<Ring ID>

リング ID を指定します。

同じリングに属する装置には同一のリング ID を指定してください。異なるリングには，ネットワーク内でユニークなリング ID を指定してください。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

axrp vlan-mapping

VLAN グループに適用する VLAN マッピング，および VLAN マッピングに参加する VLAN を設定します。

[入力形式]

情報の設定

axrp vlan-mapping <Mapping ID> vlan <VLAN ID list>

情報の変更

axrp vlan-mapping <Mapping ID> {vlan <VLAN ID list> | vlan add <VLAN ID list> | vlan remove <VLAN ID list>}

情報の削除

no axrp vlan-mapping <Mapping ID>

[入力モード]

(config)

[パラメータ]

<Mapping ID>

VLAN マッピング ID を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 128

vlan <VLAN ID list>

VLAN マッピングに参加する VLAN を指定します。VLAN を複数指定する場合は，範囲指定ができます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

vlan add <VLAN ID list>

指定済みの VLAN リストに追加する VLAN を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。
3. 変更後の <VLAN ID list> の扱い
   VLAN の追加で VLAN リストの長さが長くなった場合，VLAN リストを分割して複数行の”axrp vlan-mapping”コマンドとしてコンフィグレーションを表示することがあります。また，VLAN の追加後に VLAN リストの長さが短くなった場合，複数行の”axrp vlan-mapping”コマンドの VLAN リストを統合してコンフィグレーションを表示することがあります。

vlan remove <VLAN ID list>

指定済みの VLAN リストから削除する VLAN を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。
3. 変更後の <VLAN ID list> の扱い
   VLAN の削除で VLAN リストの長さが長くなった場合，VLAN リストを分割して複数行の”axrp vlan-mapping”コマンドとしてコンフィグレーションを表示することがあります。また，VLAN の削除後に VLAN リストの長さが短くなった場合，複数行の”axrp vlan-mapping”コマンドの VLAN リストを統合してコンフィグレーションを表示することがあります。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 一つの VLAN に対して複数の VLAN マッピングを指定できません。
2. 制御 VLAN に使用されている VLAN に対して VLAN マッピングを指定できません。
3. 多重障害監視 VLAN に使用されている VLAN に対して VLAN マッピングを指定できません。

[関連コマンド]

vlan

axrp-ring-port

Ring Protocol のリングポートとして動作するインタフェースを設定します。指定可能なインタフェースはイーサネットインタフェースとポートチャネルインタフェースです。

[入力形式]

情報の設定
　axrp-ring-port <Ring ID> [shared]

情報の削除
　no axrp-ring-port <Ring ID>

[入力モード]

（config-if）

[パラメータ]

<Ring ID>

リング ID を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 〜 65535

shared

本装置が共有リンク内に位置するトランジットノードとして動作する場合に，共有リンクとなるリングポートを指定します。
一つのリング ID に対し 2 ポート指定する必要があります。

1. 本パラメータ省略時の初期値
   通常のリングポートとして動作します。
2. 値の設定範囲
   なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. リングポートは，一つのリング ID に対して二つ設定できます。
2. リングポートは，チャネルグループに指定したイーサネットインタフェースに対して指定できません。
   また，リングポートに指定したイーサネットインタフェースは，チャネルグループに設定できません。
   リングポートは，当該イーサネットインタフェースの属するポートチャネルインタフェースに対して，設定してください。

[関連コマンド]

axrp

control-vlan

制御 VLAN として使用する VLAN を設定します。本コマンドで設定した VLAN を用いて，リング状態の監視などを行う制御フレームの送受信を実施します。

forwarding-delay-time を指定すると，初期動作時に制御 VLAN をフォワーディング状態に遷移するまでの時間を設定できます。本設定によって，トランジットノードでのフラッシュ制御フレーム受信監視を開始するまでの時間を調節でき，マスタノードが送信したフラッシュ制御フレームを確実に受信できます。

[入力形式]

情報の設定

control-vlan <VLAN ID> [forwarding-delay-time <Seconds>]

情報の削除

no control-vlan

[入力モード]

（config-axrp）

[パラメータ]

<VLAN ID>

制御 VLAN として使用する VLAN を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。
   ただし，このコマンドでデフォルト VLAN（VLAN ID=1）は指定できません。

forwarding-delay-time <Seconds>

トランジットノードでの装置起動などに，制御 VLAN をフォワーディング状態に遷移するまでの時間を秒単位で設定します。

1. 本パラメータ省略時の初期値
   リングポートのアップ後，即時フォワーディング状態に遷移します。
2. 値の設定範囲
   1 ～ 65535（秒）
3. 本パラメータ使用時の注意事項
   本パラメータだけの削除を行う際は，本パラメータを省略して control-vlan を再設定することで，パラメータの削除として扱います。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 他リング ID が使用している制御 VLAN の VLAN を指定できません。
2. VLAN グループに使用されている VLAN を指定できません。
3. 多重障害監視 VLAN が使用している VLAN を制御 VLAN に指定できません。
4. Ring Protocol 運用中に変更，または削除を行うと，本機能は一時的に無効となります。そのため，本機能を適用するネットワークの構成（リング構成）上，ループが発生するおそれがあります。リングポートであるインタフェースを shutdown に設定するなどして，ループが発生しない状態にした上で，本コマンドを入力してください。
5. forwarding-delay-time は次に示す契機で動作します。
   - 装置起動（運用コマンド reload，ppupdate などの実行含む）

[関連コマンド]

vlan

disable

Ring Protocol 機能を無効にします。

[入力形式]

情報の設定
　disable

情報の削除
　no disable

[入力モード]

（config-axrp）

[パラメータ]

なし

[コマンド省略時の動作]

Ring Protocol 機能は有効となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. Ring Protocol 運用中に本コマンドを入力すると，Ring Protocol 機能が無効となります。この場合，Ring Protocol 機能を適用するネットワークの構成（リング構成）上，ループが発生するおそれがあります。リングポートであるインタフェースを shutdown に設定するなどして，ループが発生しない状態にした上で，本コマンドを入力してください。

[関連コマンド]

なし

forwarding-shift-time

トランジットノードでのフラッシュ制御フレームの受信待ちを行う保護時間を設定します。

保護時間が経過すると，フラッシュ制御フレームを受信していない場合でも，リングポートがブロッキング状態からフォワーディング状態に遷移します。

[入力形式]

情報の設定
forwarding-shift-time {<Seconds> | infinity}

情報の削除
no forwarding-shift-time

[入力モード]

（config-axrp）

[パラメータ]

{<Seconds> | infinity}
フラッシュ制御フレーム受信までの保護時間を秒単位で指定します。
「infinity」を指定した場合は保護時間が無限となり，フラッシュ制御フレームを受信するまでは，トランジットノードのリングポートはフォワーディング状態になりません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）または infinity

[コマンド省略時の動作]

フラッシュ制御フレームの受信待ち保護時間は 10 秒となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. マスタノードでのヘルスチェックフレームの送信間隔が，トランジットノードでのフラッシュ制御フレームの受信待ちの保護時間よりも大きい場合，マスタノードが復旧を検出するよりも先にトランジットノードのリングポートがフォワーディング状態になります。そのため，一時的にループが発生するおそれがあります。
   保護時間を設定する場合，マスタノードでのヘルスチェックの送信間隔を十分に考慮した値を設定してください。

[関連コマンド]

なし

mode

リングでの本装置の動作モードを設定します。

[入力形式]

情報の設定

mode transit

情報の削除

no mode

[入力モード]

（config-axrp）

[パラメータ]

transit

トランジットノードとして動作します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. Ring Protocol 動作中にモード削除を行うと，本機能が無効となります。そのため，本機能を適用するネットワークの構成（リング構成）上，ループが発生するおそれがあります。リングポートであるインタフェースを shutdown に設定するなどして，ループが発生しない状態にした上で，本コマンドを入力してください。

[関連コマンド]

なし

multi-fault-detection mode

共有リンク監視リングの多重障害監視モードを設定します。

[入力形式]

情報の設定

multi-fault-detection mode transport-only

情報の削除

no multi-fault-detection mode

[入力モード]

(config-axrp)

[パラメータ]

transport-only

多重障害監視フレームの転送を行います。多重障害の監視は行いません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値への反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

multi-fault-detection vlan

多重障害監視用の VLAN を設定します。本コマンドで指定した VLAN を使用して，多重障害監視を行う制御フレームの転送を実施します。

本コマンドは，共有リンクありのマルチリング構成の共有リンク監視リングに設定します。

[入力形式]

情報の設定

multi-fault-detection vlan <vlan id>

情報の削除

no multi-fault-detection vlan

[入力モード]

(config-axrp)

[パラメータ]

<vlan id>

多重障害監視フレームの転送を行います。多重障害の監視は行いません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。ただし，このパラメータでデフォルト VLAN（VLAN ID=1）は指定できません。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値への反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 他のリングが使用している多重障害監視 VLAN の VLAN を指定できません。
2. 多重障害監視用 VLAN は，制御 VLAN で使用している VLAN を指定できません。
3. VLAN マッピングに使用されている VLAN を指定できません。

[関連コマンド]

なし

name

リングを識別するための名称を設定します。

[入力形式]

情報の設定

name <Name>

情報の削除

no name

[入力モード]

（config-axrp）

[パラメータ]

<Name>

リングを識別するための名称を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

NULL の文字列を設定します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

vlan-group

Ring Protocol で運用する VLAN グループ，およびその VLAN グループに参加する VLAN マッピング ID を設定します。

一つのリングに最大 2 つの VLAN グループを設定できます。

[入力形式]

情報の設定・変更

vlan-group <Group ID> vlan-mapping <Mapping ID list>

情報の削除

no vlan-group <Group ID>

[入力モード]

（config-axrp）

[パラメータ]

<Group ID>

Ring Protocol で運用する VLAN グループ ID を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 2

vlan-mapping <Mapping ID list>

VLAN グループに参加する VLAN マッピング ID を指定します。一つの VLAN マッピング ID を設定できるほか，ハイフン (-)，コンマ (,) を使用して複数の VLAN マッピング ID の一括設定もできます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 128

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 異なるリングの VLAN グループに同一の VLAN マッピングが設定されている場合，それらのリングで同一ポートをリングポートに指定できません。ただし，共有リンクであるリングポート（shared 設定のリングポート）の場合は指定できます。

[関連コマンド]

axrp vlan-mapping

14 IGMP snooping

ip igmp snooping（global）

no ip igmp snooping 設定時，本装置で，IGMP snooping 機能を抑止します。

［入力形式］

情報の設定
　no ip igmp snooping

情報の削除
　ip igmp snooping

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

本装置で，IGMP snooping 機能を有効にします。

［通信への影響］

IGMP snooping 機能が停止します。

［設定値の反映契機］

設定値変更後，すぐに反映されます。

［注意事項］

なし

［関連コマンド］

なし

ip igmp snooping（interface）

VLAN インタフェースで，IGMP snooping 機能を有効にします。

［入力形式］

情報の設定
　ip igmp snooping

情報の削除
　no ip igmp snooping

［入力モード］

(config-if)

［パラメータ］

なし

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに反映されます。

［注意事項］

system function コマンド設定有で igmp-snooping が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】

［関連コマンド］

なし

ip igmp snooping fast-leave

VLAN インタフェースで，IGMP Leave を受信した場合，すぐに該当ポートへのマルチキャスト通信を停止します。

[入力形式]

情報の設定
ip igmp snooping fast-leave

情報の削除
no ip igmp snooping fast-leave

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

IGMP Leave を受信した場合，該当ポートに同一マルチキャストグループのメンバが存在しないことを確認して，マルチキャスト通信を停止します。よって，IGMP Leave を受信したあとも，確認処理の間（3 秒間：デフォルト値）はマルチキャスト通信が継続します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに反映されます。

[注意事項]

本コマンドを設定して IGMP Leave を受信した場合，すぐに該当ポートへのマルチキャスト通信を停止します。そのため，該当ポートに同一マルチキャストグループに加入しているメンバが存在する場合，該当メンバへのマルチキャスト通信が一時的に停止します。この場合，該当メンバからの IGMP Report（加入要求）を再度受信することで，マルチキャスト通信は再開します。

[関連コマンド]

なし

ip igmp snooping mrouter

VLAN インタフェースで，マルチキャストルータポートを設定します。

[入力形式]

情報の設定・変更

ip igmp snooping mrouter interface {gigabitethernet <IF#> | port-channel <Channel group#>}【S2200】【S2100】

ip igmp snooping mrouter interface {fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#>}【SS1250】【SS1240】

情報の削除

no ip igmp snooping mrouter interface {gigabitethernet <IF#> | port-channel <Channel group#>}【S2200】【S2100】

no ip igmp snooping mrouter interface {fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#>}【SS1250】【SS1240】

[入力モード]

(config-if)

[パラメータ]

{gigabitethernet <IF#> | port-channel <Channel group#>}【S2200】【S2100】

{fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#>}【SS1250】【SS1240】

マルチキャストルータポートを設定するインタフェースを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF#>：VLAN に属するインタフェースポート番号を指定します。
   <Channel group#>：VLAN に属するチャネルグループ番号を指定します。
   <IF#> および <channel group> の値の設定範囲については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに反映されます。

[注意事項]

1. 当該インタフェースに ip igmp snooping 設定がない場合，本機能は動作しません。
2. マルチキャストルータポートにスイッチを接続する場合は，接続先のスイッチの IGMP snooping 機能を有効にしてください。
3. ポートチャネルに属しているポート番号をマルチキャストルータポートに指定しても動作しません。

[関連コマンド]

ip igmp snooping

ip igmp snooping querier

VLAN インタフェースで，IGMP クエリア機能を有効にします。

[入力形式]

情報の設定

ip igmp snooping querier

情報の削除

no ip igmp snooping querier

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに反映されます。

[注意事項]

当該インタフェースに ip igmp snooping の設定がない場合，または IP アドレス設定をしていない場合，クエリア機能は動作しません。

[関連コマンド]

ip igmp snooping

ip address

15 MLD snooping

ipv6 mld snooping（global）

no ipv6 mld snooping 設定時，本装置で，MLD snooping 機能を抑止します。

[入力形式]

情報の設定

no ipv6 mld snooping

情報の削除

ipv6 mld snooping

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

本装置で，MLD snooping 機能を有効にします。

[通信への影響]

MLD snooping 機能が停止します。

[設定値の反映契機]

設定値変更後，すぐに反映されます。

[注意事項]

なし

[関連コマンド]

なし

ipv6 mld snooping（interface）

VLAN インタフェースで，MLD snooping 機能を有効にします。

［入力形式］

情報の設定

ipv6 mld snooping

情報の削除

no ipv6 mld snooping

［入力モード］

(config-if)

［パラメータ］

なし

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに反映されます。

［注意事項］

system function コマンド設定有で mld-snooping が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】

［関連コマンド］

なし

ipv6 mld snooping source

VLAN インタフェースで，使用する MLD snooping 機能の送信元 IPv6 アドレスを設定します。

[入力形式]

情報の設定・変更

ipv6 mld snooping source <IPv6 address>

情報の削除

no ipv6 mld snooping source

[入力モード]

(config-if)

[パラメータ]

<IPv6 address>

MLD snooping 機能の送信元 IPv6 アドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   IPv6 リンクローカルアドレスをコロン記法で設定します。

[コマンド省略時の動作]

MLD クエリア機能が動作しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに反映されます。

[注意事項]

1. 当該インタフェースに ipv6 mld snooping または本設定がない場合，MLD クエリア機能は動作しません。
2. 複数インタフェース（interface range）設定の場合は，本コマンドを設定できません。
3. IPv6 リンクローカルアドレスを指定してください。IPv6 グローバルアドレスを指定すると，システムとして動作しない場合があります。

[関連コマンド]

ipv6 mld snooping

ipv6 mld snooping querier

ipv6 mld snooping mrouter

VLAN インタフェースで，マルチキャストルータポートを設定します。

[入力形式]

情報の設定・変更

ipv6 mld snooping mrouter interface {gigabitethernet <IF#> | port-channel <Channel group#>}【S2200】【S2100】

ipv6 mld snooping mrouter interface {fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#>}【SS1250】【SS1240】

情報の削除

no ipv6 mld snooping mrouter interface {gigabitethernet <IF#> | port-channel <Channel group#>}【S2200】【S2100】

no ipv6 mld snooping mrouter interface {fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#>}【SS1250】【SS1240】

[入力モード]

(config-if)

[パラメータ]

{gigabitethernet <IF#> | port-channel <Channel group#>}【S2200】【S2100】

{fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#>}【SS1250】【SS1240】

マルチキャストルータポートを設定するインタフェースを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF#>：VLAN に属するインタフェースポート番号を指定します。
   <Channel group#>：VLAN に属するチャネルグループ番号を指定します。
   <IF#> および <channel group> の値の設定範囲については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに反映されます。

[注意事項]

1. 当該インタフェースに ipv6 mld snooping の設定がない場合，本機能は動作しません。
2. マルチキャストルータポートにスイッチを接続する場合は，接続先のスイッチの MLD snooping 機能を有効にしてください。
3. ポートチャネルに属しているポート番号をマルチキャストルータポートに指定しても動作しません。

[関連コマンド]

ipv6 mld snooping

ipv6 mld snooping querier

VLAN インタフェースで，MLD クエリア機能を有効にします。

[入力形式]

情報の設定
　ipv6 mld snooping querier

情報の削除
　no ipv6 mld snooping querier

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに反映されます。

[注意事項]

1. 当該インタフェースに ipv6 mld snooping の設定がない場合，または MLD Query メッセージの送信元 IPv6 アドレス設定をしていない場合，MLD クエリア機能は動作しません。

[関連コマンド]

ipv6 mld snooping

ipv6 mld snooping source

16 IPv4・ARP・ICMP

ip address

自 IPv4 アドレスを設定します。

[入力形式]

情報の設定・変更

ip address <IP address> <Subnet-Mask>

情報の削除

no ip address <IP address>

[入力モード]

(config-if)

[パラメータ]

<IP address>

自 IPv4 アドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

<Subnet-Mask>

サブネットマスクを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   サブネットマスク：128.0.0.0 ～ 255.255.255.252（ビットが連続していること）

[コマンド省略時の動作]

なし

[通信への影響]

アップ状態のインタフェースに対し，本コマンドで変更を行うと，当該インタフェースは一度ダウンし，再度アップします。

従って，次のような状態が発生します。

- 当該インタフェースで実施中の通信があれば，いったん中断します。
- 当該インタフェースに生成された，ダイナミック ARP のエントリが削除されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. IPv4 アドレスとして 127.*.*.* を設定できません。

[関連コマンド]

interface vlan

ip mtu

インタフェースでの送信 IP MTU 長を設定します。

[入力形式]

情報の設定・変更

ip mtu <Length>

情報の削除

no ip mtu

[入力モード]

(config-if)

[パラメータ]

<Length>

インタフェースでの送信 IP MTU 長を設定します。実際にはポート MTU 情報で設定したフレーム長と本パラメータ値を比較し，小さい方の値を当該インタフェースの IP MTU 長として使用します。

なお，ポート MTU 情報で設定したフレーム長は「mtu」を参照してください。

使用している IP MTU 長は，運用コマンド show ip interface で確認してください。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   128 ～ 9216（Byte）

[コマンド省略時の動作]

ポート MTU 情報で設定したフレーム長（Byte）を IP MTU 長として使用します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. イーサネットの IP MTU 長は，ポート MTU 情報で設定したフレーム長と IP MTU の値とを比較するため，運用上 IP MTU 長を 1500 より大きい値に設定するときは，ip mtu の設定だけではなく，ポート MTU 情報の mtu の設定も確認してください。

[関連コマンド]

interface vlan

mtu

ip route

スタティック経路の IPv4 アドレスを設定します。

[入力形式]

情報の設定・変更

ip route <IP address> <Mask> <Next hop>

情報の削除

no ip route <IP address> <Mask> <Next hop>

[入力モード]

(config)

[パラメータ]

<IP address>

スタティック経路の宛先 IPv4 アドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0.0.0.0 ～ 255.255.255.255

<Mask>

スタティック経路の宛先 IPv4 アドレスのネットマスクを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   サブネットマスク：0.0.0.0 ～ 255.255.255.255（ビットが連続していること）

<Next hop>

スタティック経路のネクストホップアドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

17 フロー検出モード

flow detection mode

flow detection mode

フィルタ・QoS 機能のフロー検出するモードを設定します。

本コマンドは，ハードウェアテーブルでの最大エントリ数の配分パターンを変更します。運用形態に応じた配分パターンに変更することで，ハードウェアリソースを必要なテーブルに集中させて使用できるようになります。(配分パターンの詳細は「コンフィグレーションガイド Vol.1　3　収容条件」を参照してください。)

本コマンドは，ハードウェアの基本的な動作条件を設定するものであるため，変更する場合は受信側インタフェースに対して設定されている下記のコマンドをすべて削除する必要があります。

- ip access-group
- mac access-group
- ip qos-flow-group
- mac qos-flow-group

従って，必ず実運用を開始する最初の段階で設定してください。運用中の変更はお勧めしません。

このコマンドを設定しない，または情報を削除したときは layer2-2 がデフォルト状態になります。

[入力形式]

情報の設定・変更
　flow detection mode {layer2-1 | layer2-2}

情報の削除
　no flow detection mode

[入力モード]

(config)

[パラメータ]

{layer2-1 | layer2-2}

フロー検出モードを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   なし

フロー検出モードの適用コマンドを次の表に示します。

表 17-1　フロー検出モードによる適用コマンド

フロー検出モード	適用コマンド	
	mac	ip
	access-group	access-group
	qos-flow-group	qos-flow-group
layer2-1	○	×
layer2-2	×	○

（凡例） ○：設定可能 ×：設定不可
各フロー検出モードについては「コンフィグレーションガイド Vol.2 1.1.3 フロー検出モード」および「コンフィグレーションガイド Vol.2 3.1.1 フロー検出モード」を参照してください。

[コマンド省略時の動作]

フロー検出モードは，layer2-2 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ip access-group

mac access-group

ip qos-flow-group

mac qos-flow-group

18 アクセスリスト

指定できる名称
deny（ip access-list extended）
deny（ip access-list standard）
deny（mac access-list extended）
ip access-group
ip access-list extended
ip access-list resequence
ip access-list standard
mac access-group
mac access-list extended
mac access-list resequence
permit（ip access-list extended）
permit（ip access-list standard）
permit（mac access-list extended）
remark

指定できる名称

■プロトコル名称（IPv4）

IPv4 のプロトコル名称として，指定できる名称を次の表に示します。

表 18-1　指定可能なプロトコル名称（IPv4）

プロトコル名称	対象プロトコル番号
ah	51
esp	50
gre	47
icmp	1
igmp	2
ip	すべての IP プロトコル
ipinip	4
ospf	89
pcp	108
pim	103
sctp	132
tcp	6
tunnel	41
udp	17
vrrp	112

■ポート名称（TCP）

TCP で指定できるポート名称を，次の表に示します。

表 18-2　TCP で指定可能なポート名称

ポート名称	対象ポート名および番号
bgp	Border Gateway Protocol version 4 (179)
chargen	Character generator (19)
daytime	Daytime (13)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
exec	Remote process execution (512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (20)
gopher	Gopher (70)
hostname	NIC Host Name Server (101)
http	HyperText Transfer Protocol (80)

ポート名称	対象ポート名および番号
https	HTTP over TLS/SSL (443)
ident	Ident Protocol (113)
imap3	Interactive Mail Access Protocol version 3 (220)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
ldap	Lightweight Directory Access Protocol (389)
login	Remote login (513)
lpd	Printer service (515)
nntp	Network News Transfer Protocol (119)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
pop3s	POP3 over TLS/SSL (995)
raw	Printer PDL Data Stream (9100)
shell	Remote commands (514)
smtp	Simple Mail Transfer Protocol (25)
smtps	SMTP over TLS/SSL (465)
ssh	Secure Shell Remote Login Protocol (22)
sunrpc	Sun Remote Procedure Call (111)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (540)
whois	Nicname (43)

■ポート名称（UDP）

UDP で指定できるポート名称を，次の表に示します。

表 18-3　UDP で指定可能なポート名称（IPv4）

ポート名称	対象ポート名および番号
biff	Biff (512)
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (67)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)

ポート名称	対象ポート名および番号
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
rip	Routing Information Protocol (520)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

■ TOS 名称

指定できる TOS 名称を，次の表に示します。

表 18-4　指定可能な TOS 名称

TOS 名称	TOS 値
max-reliability	2
max-throughput	4
min-delay	8
min-monetary-cost	1
normal	0

■ Precedence 名称

指定できる Precedence 名称を，次の表に示します。

表 18-5　指定可能な Precedence 名称

Precedence 名称	Precedence 値
critical	5
flash	3
flash-override	4
immediate	2
internet	6
network	7

Precedence 名称	Precedence 値
priority	1
routine	0

■ DSCP 名称

指定できる DSCP 名称を，次の表に示します。

表 18-6　指定可能な DSCP 名称

DSCP 名称	DSCP 値
af11	10
af12	12
af13	14
af21	18
af22	20
af23	22
af31	26
af32	28
af33	30
af41	34
af42	36
af43	38
cs1	8
cs2	16
cs3	24
cs4	32
cs5	40
cs6	48
cs7	56
default	0
ef	46

■イーサネットタイプ名称

指定できるイーサネットタイプ名称を，次の表に示します。

表 18-7　指定可能なイーサネットタイプ名称

イーサネットタイプ名称	Ethernet 値	備考
appletalk	0x809b	
arp	0x0806	
eapol	0x888e	
gsrp	—※	GSRP 制御パケットをフィルタします
ipv4	0x0800	

イーサネットタイプ名称	Ethernet 値	備考
ipv6	0x86dd	
ipx	0x8137	
xns	0x0600	

注※　公開していません。

■宛先 MAC アドレス名称

指定できる宛先 MAC アドレス名称を，次の表に示します。

表 18-8　指定可能な宛先 MAC アドレス名称

宛先アドレス指定	宛先アドレス	宛先アドレスマスク
bpdu	0180.C200.0000	0000.0000.0000
cdp	0100.0CCC.CCCC	0000.0000.0000
lacp	0180.C200.0002	0000.0000.0000
lldp	0100.8758.1310	0000.0000.0000
oadp	0100.4C79.FD1B	0000.0000.0000
pvst-plus-bpdu	0100.0CCC.CCCD	0000.0000.0000

■アクセスリスト数について

アクセスリスト数，フィルタ条件数の算出については，以下を参照してください。

■アクセスリスト作成数

アクセスリスト作成数は，以下のコマンドの総数です。

- ip access-list standard
- ip access-list extended
- mac access-list extended

■アクセスリスト設定数

アクセスリスト設定数は，以下のコマンドで参照するアクセスリストの総数です。

- interface fastethernet / gigabitethernet / vlan 下の ip access-group
- interface fastethernet / gigabitethernet / vlan 下の mac access-group

注※　以下のコマンドで指定するアクセスリストは，ここでいうアクセスリスト設定数に該当しません。

- line vty 下の ip access-group
- authentication ip access-group
- mac-authentication access-group
- snmp-server community

■アクセスリスト数

アクセスリスト数は，アクセスリスト設定数と，未参照アクセスリスト作成数の合計です。

未参照アクセスリスト作成数とは，「■アクセスリスト作成数」に列挙したコマンドで作成されたアクセスリストのうち，「■アクセスリスト設定数」に列挙したコマンドから参照されないリストの数です。

■フィルタ条件数

フィルタ条件数は，以下のコマンドの総数です。

- permit
- deny
- ip access-list standard※
- ip access-list extended※
- mac access-list extended※

注※　リスト定義が「暗黙の deny」を含むためです。

■アクセスリスト，フィルタ条件のコンフィグレーションで設定可能な最大エントリ数

アクセスリスト数：
　装置全体で，IPv4，MAC のアクセスリストを最大 512 リスト

フィルタ条件数：
　IPv4 アドレスフィルタ，IPv4 パケットフィルタ，MAC フィルタごとに，フィルタ条件を装置全体で最大 1024 エントリ

アクセスリストに関しては，上記のほかに「コンフィグレーションガイド Vol.1 3.2 収容条件」に記載する制限が存在します。

■アクセスリスト数の算出例

アクセスリスト数の算出例を，次の表に示します。

表 18-9　アクセスリスト数の算出例

設定例	アクセスリスト作成数	アクセスリスト設定数	アクセスリスト数	フィルタ条件数

アクセスリスト AAA を作成して，イーサネットインタフェース 0/1 の inbound に設定
`interface fastethernet 0/1`
` ip access-group AAA in`
 	
`ip access-list extended AAA`
` 10 permit tcp any any`
` 20 deny udp any any`
	1 リスト	1 リスト	1 リスト	3 リスト

アクセスリスト AAA を作成して，イーサネットインタフェース 0/1 と 0/2 の inbound に設定
`interface fastethernet 0/1`
` ip access-group AAA in`
 	
`interface fastethernet 0/2`
` ip access-group AAA in`
 	
`ip access-list extended AAA`
` 10 permit tcp any any`
` 20 deny udp any any`
	1 リスト	2 リスト	2 リスト	3 リスト

<table>
<tr><th>設定例</th><th>アクセスリスト作成数</th><th>アクセスリスト設定数</th><th>アクセスリスト数</th><th>フィルタ条件数</th></tr>
<tr><td>アクセスリスト AAA を作成して，イーサネットインタフェース 0/1 の inbound に設定
アクセスリスト BBB を作成して，イーサネットインタフェース 0/2 の inbound に設定
<code>interface fastethernet 0/1</code>
<code> ip access-group AAA in</code>

<code>interface fastethernet 0/2</code>
<code> ip access-group BBB in</code>

<code>ip access-list extended AAA</code>
<code> 10 permit tcp any any</code>
<code> 20 deny udp any any</code>

<code>ip access-list extended BBB</code>
<code> 10 permit udp any any</code>
<code> 20 deny tcp any any</code></td><td>2 リスト</td><td>2 リスト</td><td>2 リスト</td><td>6 リスト</td></tr>
<tr><td>アクセスリスト AAA を作成して，イーサネットインタフェース 0/1 の inbound に設定
アクセスリスト BBB を作成して，インタフェースに適用しない
<code>interface fastethernet 0/1</code>
<code> ip access-group AAA in</code>

<code>ip access-list extended AAA</code>
<code> 10 permit tcp any any</code>
<code> 20 deny udp any any</code>

<code>ip access-list extended BBB</code>
<code> 10 permit udp any any</code>
<code> 20 deny tcp any any</code></td><td>2 リスト</td><td>1 リスト</td><td>2 リスト</td><td>6 リスト</td></tr>
<tr><td>アクセスリスト AAA を作成して，インタフェースに適用しない
<code>ip access-list extended AAA</code>
<code> 10 permit tcp any any</code></td><td>1 リスト</td><td>0 リスト</td><td>1 リスト</td><td>2 リスト</td></tr>
</table>

deny（ip access-list extended）

IPv4 パケットフィルタでのアクセスを拒否する条件を指定します。

[入力形式]

情報の設定・変更

- 上位プロトコルが TCP，UDP 以外の場合
  [<Seq>] deny {ip | <Protocol> | icmp | igmp } {<Src IPv4> <Src IPv4 wildcard> | host <Src IPv4> | any} {<Dst IPv4> <Dst IPv4 wildcard> | host <Dst IPv4> | any} [{[tos <TOS>] [precedence <Precedence>] | dscp <DSCP>}] [vlan <VLAN ID>] [user-priority <Priority>]
- 上位プロトコルが TCP の場合
  [<Seq>] deny tcp {<Src IPv4> <Src IPv4 wildcard> | host <Src IPv4> | any}[eq <Src port>] {<Dst IPv4> <Dst IPv4 wildcard> | host <Dst IPv4> | any} [eq <Dst port>] [ack] [fin] [psh] [rst] [syn] [urg] [{[tos <TOS>] [precedence <Precedence>] | dscp <DSCP>}] [vlan <VLAN ID>] [user-priority <Priority>]
- 上位プロトコルが UDP の場合
  [<Seq>] deny udp {<Src IPv4> <Src IPv4 wildcard> | host <Src IPv4> | any}[eq <Src port>] {<Dst IPv4> <Dst IPv4 wildcard> | host <Dst IPv4> | any} [eq <Dst port>] [{[tos <TOS>] [precedence <Precedence>] | dscp <DSCP>}] [vlan <VLAN ID>] [user-priority <Priority>]

情報の削除

no <Seq>

[入力モード]

(config-ext-nacl)

[パラメータ]

<Seq>

フィルタ条件の適用順序を指定します。

1. 本パラメータ省略時の初期値
   アクセスリスト内に条件がない場合，初期値は 10 です。
   条件を設定してある場合，設定してある適用順序の最大値 +10 です。
   ただし，適用順序の最大値が 4294967285 より大きい値の場合は省略できません。
2. 値の設定範囲
   1 〜 4294967295（10 進数）を指定します。

{ip | <Protocol> | icmp | igmp | tcp | udp}

IPv4 パケットの上位プロトコル条件を指定します。

ただし，すべてのプロトコルを対象とする場合は ip を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   - <Protocol>：
     0 〜 255（10 進数）またはプロトコル名称を指定します。
     「表 18-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{<Src IPv4> <Src IPv4 wildcard> | host <Src IPv4> | any}

送信元 IPv4 アドレスを指定します。

すべての送信元 IPv4 アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Src IPv4> <Src IPv4 wildcard>，host <Src IPv4> または any を指定します。
   - <Src IPv4> <Src IPv4 wildcard> 指定：
     <Src IPv4> には送信元 IPv4 アドレスを指定します。
     <Src IPv4 wildcard> には IPv4 アドレスの中で任意の値を許可するビットを立てたワイルドカードを IPv4 アドレス形式で指定します。
   - host <Src IPv4> 指定：
     <Src IPv4> の完全一致をフィルタ条件とします。
   - any 指定：
     送信元 IPv4 アドレスをフィルタ条件とはしません。

   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

eq <Src Port>

送信元ポート番号を指定します。
プロトコルが TCP および UDP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 65535（10 進数）またはポート名称を指定します。
   指定可能なポート名称は「表 18-2　TCP で指定可能なポート名称」および「表 18-3　UDP で指定可能なポート名称（IPv4）」を参照してください。

{<Dst IPv4> <Dst IPv4 wildcard> | host <Dst IPv4> | any}

宛先 IPv4 アドレスを指定します。
すべての宛先 IPv4 アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Dst IPv4> <Dst IPv4 wildcard>，host <Dst IPv4> または any を指定します。
   - <Dst IPv4> <Dst IPv4 wildcard> 指定：
     <Dst IPv4> には宛先 IPv4 アドレスを指定します。
     <Dst IPv4 wildcard> には IPv4 アドレスの中で任意の値を許可するビットを立てたワイルドカードを IPv4 アドレス形式で指定します。
   - host <Dst IPv4> 指定：
     <Dst IPv4> の完全一致をフィルタ条件とします。
   - any 指定：
     宛先 IPv4 アドレスをフィルタ条件とはしません。

   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

eq <Dst Port>

宛先ポート番号を指定します。
プロトコルが TCP および UDP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲

0 ～ 65535（10 進数）またはポート名称を指定します。

指定可能なポート名称は「表 18-2　TCP で指定可能なポート名称」および「表 18-3　UDP で指定可能なポート名称（IPv4)」を参照してください。

tos <TOS>

本パラメータは，TOS フィールドのビット 3 ～ 6 の 4 ビットである TOS 値を指定します。

受信パケットの TOS フィールドのビット 3 ～ 6 の 4 ビットと比較します。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			TOS				-

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 15（10 進数）または TOS 名称を指定します。
   指定可能な TOS 名称は「表 18-4　指定可能な TOS 名称」を参照してください。

precedence <Precedence>

本パラメータは，TOS フィールドの上位 3 ビットである Precedence 値を指定します。

受信パケットの TOS フィールド上位 3 ビットと比較します。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			TOS				-

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）または Precedence 名称を指定します。
   指定可能な Precedence 名称は「表 18-5　指定可能な Precedence 名称」を参照してください。

dscp <DSCP>

本パラメータは，TOS フィールドの上位 6 ビットである DSCP 値を指定します。

受信パケットの TOS フィールド上位 6 ビットと比較します。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 63（10 進数）または DSCP 名称を指定します。
   指定可能な DSCP 名称は「表 18-6　指定可能な DSCP 名称」を参照してください。

ack

TCP ヘッダの ACK フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

fin

TCP ヘッダの FIN フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

psh

TCP ヘッダの PSH フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

rst

TCP ヘッダの RST フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

syn

TCP ヘッダの SYN フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

urg

TCP ヘッダの URG フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

vlan <VLAN ID>

VLAN ID を指定します。

本パラメータはイーサネットインタフェースに適用した場合だけ有効です。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

user-priority <Priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値

なし（検出条件としません）

2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

1 エントリも設定されていないアクセスリストをインタフェースに適用した状態でエントリを追加すると，エントリがインタフェースに適用されるまでの間，当該インタフェースで受信した IP パケットが一時的に廃棄されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元アドレスワイルドカードおよび宛先アドレスワイルドカードに 255.255.255.255 と入力したときは any と表示します。
2. 送信元アドレスおよび宛先アドレスに nnn.nnn.nnn.nnn 0.0.0.0 と入力したときは host nnn.nnn.nnn.nnn と表示します。
3. tos および precedence と dscp の同時設定はできません。

[関連コマンド]

ip access-group

ip access-list resequence

permit（ip access-list extended）

remark

deny（ip access-list standard）

IPv4 アドレスフィルタでのアクセスを拒否する条件を指定します。

[入力形式]

情報の設定・変更

[<Seq>] deny {<Src IPv4> [<Src IPv4 wildcard>] | host <Src IPv4> | any}

情報の削除

no <Seq>

[入力モード]

(config-std-nacl)

[パラメータ]

<Seq>

フィルタ条件の適用順序を指定します。

1. 本パラメータ省略時の初期値
   アクセスリスト内に条件がない場合，初期値は 10 です。
   条件を設定してある場合，設定してある適用順序の最大値 +10 です。
   ただし，適用順序の最大値が 4294967285 より大きい値の場合は省略できません。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します。

{<Src IPv4> [<Src IPv4 wildcard>] | host <Src IPv4> | any}

IPv4 アドレスを指定します。

すべての IPv4 アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Src IPv4> [<Src IPv4 wildcard>]，host <Src IPv4> または any を指定します。
   - <Src IPv4> [<Src IPv4 wildcard>] 指定：
     <Src IPv4> には IPv4 アドレスを指定します。
     [<Src IPv4 wildcard>] には IPv4 アドレスの中で任意の値を許可するビットを立てたワイルドカードを IPv4 アドレス形式で指定します。省略した場合は <Src IPv4> の完全一致をフィルタ条件とします。
   - host <Src IPv4> 指定：
     <Src IPv4> の完全一致をフィルタ条件とします。
   - any 指定：
     IPv4 アドレスをフィルタ条件とはしません。

   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

[コマンド省略時の動作]

なし

[通信への影響]

1 エントリも設定されていないアクセスリストをインタフェースに適用した状態でエントリを追加すると，

エントリがインタフェースに適用されるまでの間，当該インタフェースで受信した IP パケットが一時的に廃棄されます。

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. アドレスワイルドカードに 255.255.255.255 と入力したときは any と表示します。
2. アドレスに nnn.nnn.nnn.nnn 0.0.0.0 と入力したときは host nnn.nnn.nnn.nnn と表示します。

［関連コマンド］

ip access-group

ip access-list resequence

permit（ip access-list standard）

remark

deny（mac access-list extended）

MAC フィルタでのアクセスを拒否する条件を指定します。

[入力形式]

情報の設定・変更

[<Seq>] deny {<Src MAC> <Src MAC mask> ｜ host <Src MAC> ｜ any} {<Dst MAC> <Dst MAC mask> ｜ host <Dst MAC> ｜ any ｜ bpdu ｜ cdp ｜ lacp ｜ lldp ｜ oadp ｜ pvst-plus-bpdu } [<Ethernet type>] [vlan <VLAN ID>] [user-priority <Priority>]

情報の削除

no <Seq>

[入力モード]

(config-ext-macl)

[パラメータ]

<Seq>

フィルタ条件の適用順序を指定します。

1. 本パラメータ省略時の初期値
   アクセスリスト内に条件がない場合，初期値は 10 です。
   条件を設定してある場合，設定してある適用順序の最大値 +10 です。
   ただし，適用順序の最大値が 4294967285 より大きい値の場合は省略できません。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します。

{<Src MAC> <Src MAC mask> ｜ host <Src MAC> ｜ any}

送信元 MAC アドレスを指定します。

すべての送信元 MAC アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Src MAC> <Src MAC mask>，host <Src MAC> または any を指定します。
   - <Src MAC> <Src MAC mask> 指定：
     <Src MAC> には送信元 MAC アドレスを指定します。
     <Src MAC mask> には MAC アドレスの中で任意の値を許可するビットを立てたマスクを MAC アドレス形式で指定します。
   - host <Src MAC> 指定：
     <Src MAC> の完全一致をフィルタ条件とします。
   - any 指定：
     送信元 MAC アドレスをフィルタ条件とはしません。

   MAC アドレス（nnnn.nnnn.nnnn）：0000.0000.0000 ～ ffff.ffff.ffff（16 進数）

{<Dst MAC> <Dst MAC mask> ｜ host <Dst MAC> ｜ any ｜ bpdu ｜ cdp ｜ lacp ｜ lldp ｜ oadp ｜ pvst-plus-bpdu}

宛先 MAC アドレスを指定します。

すべての宛先 MAC アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値

省略できません。

2. 値の設定範囲

<Dst MAC> <Dst MAC mask>，host <Dst MAC>，any，bpdu，cdp，lacp，lldp，oadp または pvst-plus-bpdu を指定します。

- <Dst MAC> <Dst MAC mask> 指定：
  <Dst MAC> には宛先 MAC アドレスを指定します。
  <Dst MAC mask> には MAC アドレスの中で任意の値を許可するビットを立てたマスクを MAC アドレス形式で指定します。
- host <Dst MAC> 指定：
  <Dst MAC> の完全一致をフィルタ条件とします。
- any 指定：
  宛先 MAC アドレスをフィルタ条件とはしません。
- bpdu 指定：
  BPDU 制御パケットをフィルタ条件とします。
- cdp 指定：
  CDP 制御パケットをフィルタ条件とします。
- lacp 指定：
  LACP 制御パケットをフィルタ条件とします。
- lldp 指定：
  LLDP 制御パケットをフィルタ条件とします。
- oadp 指定：
  OADP 制御パケットをフィルタ条件とします。
- pvst-plus-bpdu 指定：
  PVST+ 制御パケットをフィルタ条件とします。

MAC アドレス（nnnn.nnnn.nnnn）：0000.0000.0000 ～ ffff.ffff.ffff（16 進数）

<Ethernet type>

イーサネットタイプ番号またはイーサネットタイプ名称を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0x0000 ～ 0xffff（16 進数）またはイーサネットタイプ名称を指定します。
   指定可能なイーサネットタイプ名称は「表 18-7　指定可能なイーサネットタイプ名称」を参照してください。

vlan <VLAN ID>

VLAN ID を指定します。

本パラメータはイーサネットインタフェースに適用した場合だけ有効です。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

user-priority <Priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲

0 ～ 7（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

1 エントリも設定されていないアクセスリストをインタフェースに適用した状態でエントリを追加すると，エントリがインタフェースに適用されるまでの間，当該インタフェースで受信した全パケットが一時的に廃棄されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元アドレスおよび宛先アドレスに nnnn.nnnn.nnnn ffff.ffff.ffff と入力したときは any と表示します。
2. 宛先アドレスにプロトコル名称指定または指定できるプロトコル名称のアドレスを指定している場合はプロトコル名称を表示します。宛先アドレスに指定できるプロトコル名称のアドレスは「表 18-8　指定可能な宛先 MAC アドレス名称」を参照してください。上記以外の送信元アドレスおよび宛先アドレスに nnnn.nnnn.nnnn 0000.0000.0000 と入力したときは host nnnn.nnnn.nnnn と表示します。

[関連コマンド]

mac access-group

mac access-list resequence

permit（mac access-list extended）

remark

ip access-group

イーサネットインタフェースまたは VLAN インタフェースに対して IPv4 アクセスリストを適用し，IPv4 フィルタ機能を有効にします。

[入力形式]

情報の設定

ip access-group <ACL ID> in

情報の削除

no ip access-group <ACL ID> in

[入力モード]

(config-if)

[パラメータ]

<ACL ID>

設定する IPv4 アドレスフィルタまたは IPv4 パケットフィルタの識別子を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

in

Inbound を指定します。

in ：Inbound（受信側の指定）

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   なし

[コマンド省略時の動作]

なし

[通信への影響]

1 エントリ以上を設定したアクセスリストをインタフェースに適用する場合，エントリがインタフェースに適用されるまでの間，当該インタフェースで受信した IP パケットが一時的に廃棄されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. system function コマンド設定有で filter が設定されていない場合，本コマンドは設定できません。
   （system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
2. 同一のインタフェースに対して IPv4 フィルタを一つ設定可能です。イーサネットインタフェース，VLAN インタフェースに適用する場合は最大 128 個です。すでに設定されている場合は，いったん削除してから設定することになります。

3. 実在しない IPv4 フィルタを設定した場合は何も動作しません。IPv4 フィルタの識別子は登録されます。
4. 受信側フロー検出モードによる設定の可否を次の表に示します。

表 18-10　受信側フロー検出モードによる設定の可否（IPv4）

フロー検出モード	設定の可否	
	イーサネット	VLAN
layer2-1	×	×
layer2-2	○	○

（凡例）　○：設定可能　×：設定不可

5. イーサネットインタフェースに対して IPv4 パケットフィルタを適用する場合は，フロー検出条件に VLAN パラメータがあるとき，適用するイーサネットインタフェースの設定内容に VLAN ID が含まれていれば設定できます。
6. VLAN インタフェースに対して IPv4 パケットフィルタを適用する場合は，フロー検出条件に VLAN パラメータがないときに設定できます。
7. 一部のパケットはフィルタ機能の対象外です。詳細については，「コンフィグレーションガイド Vol.2 1 フィルタ」を参照してください。

[関連コマンド]

ip access-list standard

ip access-list extended

ip access-list extended

IPv4 フィルタとして動作するアクセスリストを設定します。IPv4 フィルタとして動作するアクセスリストには種類が二つあります。IPv4 アドレスフィルタと，IPv4 パケットフィルタです。

このコマンドでは IPv4 パケットフィルタを設定します。

IPv4 パケットフィルタでは，送信元 IPv4 アドレス，宛先 IPv4 アドレス，VLAN ID，ユーザ優先度，TOS フィールドの値，ポート番号および TCP フラグに基づいてフィルタします。

アクセスリストの一つの ID で複数個のフィルタ条件が指定できますが，イーサネットインタフェースおよび VLAN インタフェースに適用する場合は最大 127 個となります。

アクセスリスト数，フィルタ条件については，「■アクセスリスト数について」を参照してください。

[入力形式]

情報の設定・変更

ip access-list extended <ACL ID>

情報の削除

no ip access-list extended <ACL ID>

[入力モード]

(config)

[パラメータ]

<ACL ID>

設定する IPv4 パケットフィルタの識別子を指定します。

config-ext-nacl モードへ移行します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

作成済みの IPv4 アドレスフィルタ名称，MAC アクセスリスト名称は指定できません。

[関連コマンド]

ip access-group

ip access-list resequence

deny（ip access-list extended）

permit（ip access-list extended）

remark

ip access-list resequence

IPv4 アドレスフィルタおよび IPv4 パケットフィルタのフィルタ条件適用順序のシーケンス番号を再設定します。

[入力形式]

情報の設定・変更

ip access-list resequence <ACL ID> [<Starting seq> [<Increment seq>]]

[入力モード]

(config)

[パラメータ]

<ACL ID>

設定する IPv4 アドレスフィルタまたは IPv4 パケットフィルタの識別子を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

<Starting seq>

開始シーケンス番号を指定します。

1. 本パラメータ省略時の初期値
   初期値は 10 です。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します。

<Increment seq>

シーケンスインクリメント値を指定します。

1. 本パラメータ省略時の初期値
   初期値は 10 です。
2. 値の設定範囲
   1 ～ 100（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ip access-list standard

ip access-list extended

ip access-list standard

IPv4 フィルタとして動作するアクセスリストを設定します。IPv4 フィルタとして動作するアクセスリストには種類が二つあります。IPv4 アドレスフィルタと，IPv4 パケットフィルタです。

このコマンドでは IPv4 アドレスフィルタを設定します。

IPv4 アドレスフィルタでは，IPv4 アドレスに基づいてフィルタします。

アクセスリストの一つの ID で複数個のフィルタ条件が指定できますが，イーサネットインタフェースおよび VLAN インタフェースに適用する場合は最大 127 個となります。

アクセスリスト数，フィルタ条件については，「■アクセスリスト数について」を参照してください。

[入力形式]

情報の設定・変更

ip access-list standard <ACL ID>

情報の削除

no ip access-list standard <ACL ID>

[入力モード]

(config)

[パラメータ]

<ACL ID>

設定する IPv4 アドレスフィルタの識別子を指定します。

config-std-nacl モードへ移行します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

作成済みの IPv4 アドレスフィルタ名称，MAC アクセスリスト名称は指定できません。

[関連コマンド]

ip access-group

ip access-list resequence

deny（ip access-list standard）

permit（ip access-list standard）

remark

mac access-group

イーサネットインタフェースまたは VLAN インタフェースに対して MAC アクセスリストを適用し，MAC フィルタ機能を有効にします。

[入力形式]

情報の設定

mac access-group <ACL ID> in

情報の削除

no mac access-group <ACL ID> in

[入力モード]

(config-if)

[パラメータ]

<ACL ID>

設定する MAC フィルタの識別子を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

in

Inbound を指定します。

in ：Inbound（受信側の指定）

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   なし

[コマンド省略時の動作]

なし

[通信への影響]

1 エントリ以上を設定したアクセスリストをインタフェースに適用する場合，エントリがインタフェースに適用されるまでの間，当該インタフェースで受信した全パケットが一時的に廃棄されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. system function コマンド設定有で filter が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
2. 同一のインタフェースに対して MAC フィルタを一つ設定可能です。イーサネットインタフェース，VLAN インタフェースに適用する場合は最大 128 個です。すでに設定されている場合，いったん削除してから設定することになります。

3. 実在しない MAC フィルタを設定した場合は何も動作しません。MAC フィルタの識別子は登録されます。
4. フロー検出モードによる設定の可否を次の表に示します。

表 18-11　フロー検出モードによる設定の可否（MAC)

フロー検出モード	設定の可否	
	イーサネット	VLAN
layer2-1	○	○
layer2-2	×	×

（凡例）　○：設定可能　×：設定不可

5. イーサネットインタフェースに対して MAC フィルタを適用する場合は，フロー検出条件に VLAN パラメータがあるとき，適用するイーサネットインタフェースの設定内容に VLAN ID が含まれていれば設定できます。
6. VLAN インタフェースに対して MAC フィルタを適用する場合は，フロー検出条件に VLAN パラメータがないときに設定できます。
7. 一部のパケットはフィルタ機能の対象外です。詳細については，「コンフィグレーションガイド Vol.2 1 フィルタ」を参照してください。

［関連コマンド］

mac access-list extended

mac access-list extended

MAC フィルタとして動作するアクセスリストを設定します。MAC フィルタとして動作するアクセスリストでは，送信元 MAC アドレス，宛先 MAC アドレス，イーサネットタイプ番号，VLAN ID，およびユーザ優先度に基づいてフィルタします。

アクセスリストの一つの ID で複数個のフィルタ条件が指定できますが，イーサネットインタフェースおよび VLAN インタフェースに適用する場合は最大 127 個となります。

アクセスリスト数，フィルタ条件については，「■アクセスリスト数について」を参照してください。

[入力形式]

情報の設定・変更

mac access-list extended <ACL ID>

情報の削除

no mac access-list extended <ACL ID>

[入力モード]

(config)

[パラメータ]

<ACL ID>

設定する MAC フィルタの識別子を指定します。config-ext-macl モードへ移行します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

作成済みの IPv4 パケットフィルタ名称，IPv4 アドレスフィルタ名称は指定できません。

[関連コマンド]

mac access-group

mac access-list resequence

deny（mac access-list extended）

permit（mac access-list extended）

remark

mac access-list resequence

MAC フィルタのフィルタ条件適用順序のシーケンス番号を再設定します。

[入力形式]

情報の設定・変更

mac access-list resequence <ACL ID> [<Starting Seq> [<Increment Seq>]]

[入力モード]

(config)

[パラメータ]

<ACL ID>

設定する MAC フィルタの識別子を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

<Starting-Seq>

開始シーケンス番号を指定します。

1. 本パラメータ省略時の初期値
   初期値は 10 です。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します

<Increment-Seq>

シーケンスインクリメント値を指定します。

1. 本パラメータ省略時の初期値
   初期値は 10 です。
2. 値の設定範囲
   1 ～ 100（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

mac access-list extended

permit（ip access-list extended）

IPv4 パケットフィルタでのアクセスを許可する条件を指定します。

[入力形式]

情報の設定・変更

- 上位プロトコルが TCP，UDP 以外の場合
  [<Seq>] permit {ip｜<Protocol>｜icmp｜igmp } {<Src IPv4> <Src IPv4 wildcard>｜host <Src IPv4>｜any} {<Dst IPv4> <Dst IPv4 wildcard>｜host <Dst IPv4>｜any} [{[tos <TOS>] [precedence <Precedence>]｜dscp <DSCP>}] [vlan <VLAN ID>] [user-priority <Priority>]
- 上位プロトコルが TCP の場合
  [<Seq>] permit tcp {<Src IPv4> <Src IPv4 wildcard>｜host <Src IPv4>｜any}[eq <Src port>] {<Dst IPv4> <Dst IPv4 wildcard>｜host <Dst IPv4>｜any} [eq <Dst port>] [ack] [fin] [psh] [rst] [syn] [urg] [{[tos <TOS>] [precedence <Precedence>]｜dscp <DSCP>}] [vlan <VLAN ID>] [user-priority <Priority>]
- 上位プロトコルが UDP の場合
  [<Seq>] permit udp {<Src IPv4> <Src IPv4 wildcard>｜host <Src IPv4>｜any}[eq <Src port>] {<Dst IPv4> <Dst IPv4 wildcard>｜host <Dst IPv4>｜any} [eq <Dst port>] [{[tos <TOS>] [precedence <Precedence>]｜dscp <DSCP>}] [vlan <VLAN ID>] [user-priority <Priority>]

情報の削除
　no <Seq>

[入力モード]

(config-ext-nacl)

[パラメータ]

<Seq>

フィルタ条件の適用順序を指定します。

1. 本パラメータ省略時の初期値
   アクセスリスト内に条件がない場合，初期値は 10 です。
   条件を設定してある場合，設定してある適用順序の最大値 +10 です。
   ただし，適用順序の最大値が 4294967285 より大きい値の場合は省略できません。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します。

{ip｜<Protocol>｜icmp｜igmp｜tcp｜udp}

IPv4 パケットの上位プロトコル条件を指定します。
ただし，すべてのプロトコルを対象とする場合は ip を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   - <Protocol>：
     0 ～ 255（10 進数）またはプロトコル名称を指定します。
     「表 18-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{<Src IPv4> <Src IPv4 wildcard>｜host <Src IPv4>｜any}

送信元 IPv4 アドレスを指定します。

すべての送信元 IPv4 アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Src IPv4> <Src IPv4 wildcard>，host <Src IPv4> または any を指定します。
   - <Src IPv4> <Src IPv4 wildcard> 指定：
     <Src IPv4> には送信元 IPv4 アドレスを指定します。
     <Src IPv4 wildcard> には IPv4 アドレスの中で任意の値を許可するビットを立てたワイルドカードを IPv4 アドレス形式で指定します。
   - host <Src IPv4> 指定：
     <Src IPv4> の完全一致をフィルタ条件とします。
   - any 指定：
     送信元 IPv4 アドレスをフィルタ条件とはしません。

   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

eq <Src Port>

送信元ポート番号を指定します。

プロトコルが TCP および UDP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 65535（10 進数）またはポート名称を指定します。
   指定可能なポート名称は「表 18-2　TCP で指定可能なポート名称」および「表 18-3　UDP で指定可能なポート名称（IPv4）」を参照してください。

{<Dst IPv4> <Dst IPv4 wildcard> | host <Dst IPv4> | any}

宛先 IPv4 アドレスを指定します。

すべての宛先 IPv4 アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Dst IPv4> <Dst IPv4 wildcard>，host <Dst IPv4> または any を指定します。
   - <Dst IPv4> <Dst IPv4 wildcard> 指定：
     <Dst IPv4> には宛先 IPv4 アドレスを指定します。
     <Dst IPv4 wildcard> には IPv4 アドレスの中で任意の値を許可するビットを立てたワイルドカードを IPv4 アドレス形式で指定します。
   - host <Dst IPv4> 指定：
     <Dst IPv4> の完全一致をフィルタ条件とします。
   - any 指定：
     宛先 IPv4 アドレスをフィルタ条件とはしません。

   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

eq <Dst Port>

宛先ポート番号を指定します。

プロトコルが TCP および UDP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲

0 ～ 65535（10 進数）またはポート名称を指定します。
指定可能なポート名称は「表 18-2　TCP で指定可能なポート名称」および「表 18-3　UDP で指定可能なポート名称（IPv4）」を参照してください。

tos <TOS>

本パラメータは，TOS フィールドのビット 3 ～ 6 の 4 ビットである TOS 値を指定します。
受信パケットの TOS フィールドのビット 3 ～ 6 の 4 ビットと比較します。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			TOS				-

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 15（10 進数）または TOS 名称を指定します。
   指定可能な TOS 名称は「表 18-4　指定可能な TOS 名称」を参照してください。

precedence <Precedence>

本パラメータは，TOS フィールドの上位 3 ビットである Precedence 値を指定します。
受信パケットの TOS フィールド上位 3 ビットと比較します。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			TOS				-

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）または Precedence 名称を指定します。
   指定可能な Precedence 名称は「表 18-5　指定可能な Precedence 名称」を参照してください。

dscp <DSCP>

本パラメータは，TOS フィールドの上位 6 ビットである DSCP 値を指定します。
受信パケットの TOS フィールド上位 6 ビットと比較します。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 63（10 進数）または，DSCP 名称を指定します。
   指定可能な DSCP 名称は「表 18-6　指定可能な DSCP 名称」を参照してください。

ack

TCP ヘッダの ACK フラグが 1 のパケットの検出を指定します。
プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

fin

TCP ヘッダの FIN フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

psh

TCP ヘッダの PSH フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

rst

TCP ヘッダの RST フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

syn

TCP ヘッダの SYN フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

urg

TCP ヘッダの URG フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

vlan <VLAN ID>

VLAN ID を指定します。

本パラメータはイーサネットインタフェースに適用した場合だけ有効です。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

user-priority <Priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値

なし（検出条件としません）
2. 値の設定範囲
0 ～ 7（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

1 エントリも設定されていないアクセスリストをインタフェースに適用した状態でエントリを追加すると，エントリがインタフェースに適用されるまでの間，当該インタフェースで受信した IP パケットが一時的に廃棄されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元アドレスワイルドカードおよび宛先アドレスワイルドカードに 255.255.255.255 と入力したときは any と表示します。
2. 2. 送信元アドレスおよび宛先アドレスに nnn.nnn.nnn.nnn 0.0.0.0 と入力したときは host nnn.nnn.nnn.nnn と表示します。
3. tos および precedence と dscp の同時設定はできません。

[関連コマンド]

ip access-group

ip access-list resequence

deny（ip access-list extended）

remark

permit（ip access-list standard）

IPv4 アドレスフィルタでのアクセスを許可する条件を指定します。

[入力形式]

情報の設定・変更
[<Seq>] permit {<Src IPv4> [<Src IPv4 wildcard>] | host <Src IPv4> | any}

情報の削除
no <Seq>

[入力モード]

(config-std-nacl)

[パラメータ]

<Seq>

フィルタ条件の適用順序を指定します。

1. 本パラメータ省略時の初期値
   アクセスリスト内に条件がない場合，初期値は 10 です。
   条件を設定してある場合，設定してある適用順序の最大値 +10 です。
   ただし，適用順序の最大値が 4294967285 より大きい値の場合は省略できません。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します。

{<Src IPv4> [<Src IPv4 wildcard>] | host <Src IPv4> | any}

IPv4 アドレスを指定します。
すべての IPv4 アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Src IPv4> [<Src IPv4 wildcard>]，host <Src IPv4> または any を指定します。
   - <Src IPv4> [<Src IPv4 wildcard>] 指定：
     <Src IPv4> には IPv4 アドレスを指定します。
     [<Src IPv4 wildcard>] には IPv4 アドレスの中で任意の値を許可するビットを立てたワイルドカードを IPv4 アドレス形式で指定します。省略した場合は <Src IPv4> の完全一致をフィルタ条件とします。
   - host <Src IPv4> 指定：
     <Src IPv4> の完全一致をフィルタ条件とします。
   - any 指定：
     IPv4 アドレスをフィルタ条件とはしません。

   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

[コマンド省略時の動作]

なし

[通信への影響]

1 エントリも設定されていないアクセスリストをインタフェースに適用した状態でエントリを追加すると，

エントリがインタフェースに適用されるまでの間，当該インタフェースで受信した IP パケットが一時的に廃棄されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. アドレスワイルドカードに 255.255.255.255 と入力したときは any と表示します。
2. アドレスに nnn.nnn.nnn.nnn 0.0.0.0 と入力したときは host nnn.nnn.nnn.nnn と表示します。

[関連コマンド]

ip access-group

ip access-list resequence

deny（ip access-list standard）

remark

permit（mac access-list extended）

MAC フィルタでのアクセスを許可する条件を指定します。

[入力形式]

情報の設定・変更

[<Seq>] permit {<Src MAC> <Src MAC mask> | host <Src MAC> | any} {<Dst MAC> <Dst MAC mask> | host <Dst MAC> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu } [<Ethernet type>] [vlan <VLAN ID>] [user-priority <Priority>]

情報の削除

no <Seq>

[入力モード]

(config-ext-macl)

[パラメータ]

<Seq>

フィルタ条件の適用順序を指定します。

1. 本パラメータ省略時の初期値
   アクセスリスト内に条件がない場合，初期値は 10 です。
   条件を設定してある場合，設定してある適用順序の最大値 +10 です。
   ただし，適用順序の最大値が 4294967285 より大きい値の場合は省略できません。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します。

{<Src MAC> <Src MAC mask> | host <Src MAC> | any}

送信元 MAC アドレスを指定します。

すべての送信元 MAC アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Src MAC> <Src MAC mask>，host <Src MAC> または any を指定します。
   - <Src MAC> <Src MAC mask> 指定：
     <Src MAC> には送信元 MAC アドレスを指定します。
     <Src MAC mask> には MAC アドレスの中で任意の値を許可するビットを立てたマスクを MAC アドレス形式で指定します。
   - host <Src MAC> 指定：
     <Src MAC> の完全一致をフィルタ条件とします。
   - any 指定：
     送信元 MAC アドレスをフィルタ条件とはしません。

   MAC アドレス（nnnn.nnnn.nnnn）: 0000.0000.0000 ～ ffff.ffff.ffff（16 進数）

{<Dst MAC> <Dst MAC mask> | host <Dst MAC> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu }

宛先 MAC アドレスを指定します。

すべての宛先 MAC アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値

省略できません。

2. 値の設定範囲
<Dst MAC> <Dst MAC mask>，host <Dst MAC>，any，bpdu，cdp，lacp，lldp，oadp または pvst-plus-bpdu を指定します。
   - <Dst MAC> <Dst MAC mask> 指定：
     <Dst MAC> には宛先 MAC アドレスを指定します。
     <Dst MAC mask> には MAC アドレスの中で任意の値を許可するビットを立てたマスクを MAC アドレス形式で指定します。
   - host <Dst MAC> 指定：
     <Dst MAC> の完全一致をフィルタ条件とします。
   - any 指定：
     宛先 MAC アドレスをフィルタ条件とはしません。
   - bpdu 指定：
     BPDU 制御パケットをフィルタ条件とします。
   - cdp 指定：
     CDP 制御パケットをフィルタ条件とします。
   - lacp 指定：
     LACP 制御パケットをフィルタ条件とします。
   - lldp 指定：
     LLDP 制御パケットをフィルタ条件とします。
   - oadp 指定：
     OADP 制御パケットをフィルタ条件とします。
   - pvst-plus-bpdu 指定：
     PVST+ 制御パケットをフィルタ条件とします。

   MAC アドレス（nnnn.nnnn.nnnn）：0000.0000.0000 ～ ffff.ffff.ffff（16 進数）

<Ethernet type>

イーサネットタイプ番号またはイーサネットタイプ名称を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0x0000 ～ 0xffff（16 進数）またはイーサネットタイプ名称を指定します。
   指定可能なイーサネットタイプ名称は「表 18-7　指定可能なイーサネットタイプ名称」を参照してください。

vlan <VLAN ID>

VLAN ID を指定します。

本パラメータはイーサネットインタフェースに適用した場合だけ有効です。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

user-priority <Priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲

0 ～ 7（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

1 エントリも設定されていないアクセスリストをインタフェースに適用した状態でエントリを追加すると，エントリがインタフェースに適用されるまでの間，当該インタフェースで受信した全パケットが一時的に廃棄されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元アドレスおよび宛先アドレスに nnnn.nnnn.nnnn ffff.ffff.ffff と入力したときは any と表示します。
2. 宛先アドレスにプロトコル名称設定または設定できるプロトコル名称のアドレスを設定している場合はプロトコル名称を表示します。宛先アドレスに設定できるプロトコル名称のアドレスは「表 18-8　指定可能な宛先 MAC アドレス名称」を参照してください。上記以外の送信元アドレスおよび宛先アドレスに nnnn.nnnn.nnnn 0000.0000.0000 と入力したときは host nnnn.nnnn.nnnn と表示します。

[関連コマンド]

mac access-group

mac access-list resequence

deny（mac access-list extended）

remark

remark

アクセスリストの補足説明を設定します。アクセスリストには IPv4 アドレスフィルタまたは IPv4 パケットフィルタ，MAC フィルタがあります。

[入力形式]

情報の設定・変更

remark <Remark>

情報の削除

no remark

[入力モード]

```
(config-ext-nacl)
(config-std-nacl)
(config-ext-macl)
```

[パラメータ]

<Remark>

入力モードにより対象となるアクセスリストの補足説明を設定します。
一つのアクセスリストに対して一行だけ設定可能です。再度入力した場合は上書きになります。

1. 本パラメータ省略時の初期値
   初期値は Null です。
2. 値の設定範囲
   64 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ip access-list standard

ip access-list extended

mac access-list extended

19 QoS

指定できる名称および値
ip qos-flow-group
ip qos-flow-list
ip qos-flow-list resequence
limit-queue-length
mac qos-flow-group
mac qos-flow-list
mac qos-flow-list resequence
qos（ip qos-flow-list）
qos（mac qos-flow-list）
qos-queue-group
qos-queue-list
remark
traffic-shape rate
control-packet user-priority

指定できる名称および値

■プロトコル名称（IPv4）

IPv4 のプロトコル名称として，指定できる名称を次の表に示します。

表 19-1　指定可能なプロトコル名称（IPv4）

プロトコル名称	対象プロトコル番号
ah	51
esp	50
gre	47
icmp	1
igmp	2
ip	すべての IP プロトコル
ipinip	4
ospf	89
pcp	108
pim	103
sctp	132
tcp	6
tunnel	41
udp	17
vrrp	112

■ポート名称（TCP）

TCP で指定できるポート名称を，次の表に示します。

表 19-2　TCP で指定可能なポート名称

ポート名称	対象ポート名および番号
bgp	Border Gateway Protocol version 4 (179)
chargen	Character generator (19)
daytime	Daytime (13)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
exec	Remote process execution (512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (20)
gopher	Gopher (70)
hostname	NIC Host Name Server (101)
http	HyperText Transfer Protocol (80)

ポート名称	対象ポート名および番号
https	HTTP over TLS/SSL (443)
ident	Ident Protocol (113)
imap3	Interactive Mail Access Protocol version 3 (220)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
ldap	Lightweight Directory Access Protocol (389)
login	Remote login (513)
lpd	Printer service (515)
nntp	Network News Transfer Protocol (119)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
pop3s	POP3 over TLS/SSL (995)
raw	Printer PDL Data Stream (9100)
shell	Remote commands (514)
smtp	Simple Mail Transfer Protocol (25)
smtps	SMTP over TLS/SSL (465)
ssh	Secure Shell Remote Login Protocol (22)
sunrpc	Sun Remote Procedure Call (111)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (540)
whois	Nicname (43)

■ポート名称（UDP）

UDP で指定できるポート名称を，次の表に示します。

表 19-3　UDP で指定可能なポート名称（IPv4）

ポート名称	対象ポート名および番号
biff	Biff (512)
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (67)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)

ポート名称	対象ポート名および番号
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
rip	Routing Information Protocol (520)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

■ TOS 名称

指定できる TOS 名称を，次の表に示します。

表 19-4　指定可能な TOS 名称

TOS 名称	TOS 値
max-reliability	2
max-throughput	4
min-delay	8
min-monetary-cost	1
normal	0

■ Precedence 名称

指定できる Precedence 名称を，次の表に示します。

表 19-5　指定可能な Precedence 名称

Precedence 名称	Precedence 値
critical	5
flash	3
flash-override	4
immediate	2
internet	6
network	7

Precedence 名称	Precedence 値
priority	1
routine	0

■ DSCP 名称

指定できる DSCP 名称を，次の表に示します。

表 19-6　指定可能な DSCP 名称

DSCP 名称	DSCP 値
af11	10
af12	12
af13	14
af21	18
af22	20
af23	22
af31	26
af32	28
af33	30
af41	34
af42	36
af43	38
cs1	8
cs2	16
cs3	24
cs4	32
cs5	40
cs6	48
cs7	56
default	0
ef	46

■イーサネットタイプ名称

指定できるイーサネットタイプ名称を，次の表に示します。

表 19-7　指定可能なイーサネットタイプ名称

イーサネットタイプ名称	Ethernet 値	備考
appletalk	0x809b	
arp	0x0806	
eapol	0x888e	
gsrp	−※	GSRP 制御パケットをフロー検出します
ipv4	0x0800	

イーサネットタイプ名称	Ethernet 値	備考
ipv6	0x86dd	
ipx	0x8137	
xns	0x0600	

注※　公開していません。

■宛先 MAC アドレス名称

指定できる宛先 MAC アドレス名称を，次の表に示します。

表 19-8　指定可能な宛先 MAC アドレス名称

宛先アドレス指定	宛先アドレス	宛先アドレスマスク
bpdu	0180.C200.0000	0000.0000.0000
cdp	0100.0CCC.CCCC	0000.0000.0000
lacp	0180.C200.0002	0000.0000.0000
lldp	0100.8758.1310	0000.0000.0000
oadp	0100.4C79.FD1B	0000.0000.0000
pvst-plus-bpdu	0100.0CCC.CCCD	0000.0000.0000

■ QoS フローリスト数について

QoS フローリスト数，フロー検出および動作指定エントリ数の算出については，以下を参照してください。

■ QoS フローリスト作成数

QoS フローリスト作成数は，以下のコマンドの総数です。

- ip qos-flow-list
- mac qos-flow-list

■ QoS フローリスト設定数

QoS フローリスト設定数は，以下のコマンドで参照する QoS フローリストの総数です。

- interface fastethernet / gigabitethernet / vlan 下の ip qos-flow-group
- interface fastethernet / gigabitethernet / vlan 下の mac qos-flow-group

■ QoS フローリスト数

QoS フローリスト数は，QoS フローリスト設定数と，未参照 QoS フローリスト作成数の合計です。未参照 QoS フローリスト作成数とは，「■ QoS フローリスト作成数」に列挙したコマンドで作成された QoS フローリストのうち，「■ QoS フローリスト設定数」に列挙したコマンドから参照されないリストの数です。

■フロー検出条件および動作指定エントリ数

フロー検出条件および動作指定エントリ数は，以下のコマンドの総数です。

- qos

- ip qos-flow-list
- mac qos-flow-list

■ QoS フローリストのコンフィグレーションで設定可能な最大エントリ数

QoS フローリスト数：
装置全体で，IPv4，MAC の QoS フローリストを最大 512 エントリ

フロー検出条件および動作指定エントリ数：
IPv4 QoS，MAC QoS ごとに，フロー検出条件および動作指定条件を装置全体で最大 1024 エントリ

QoS フローリストに関しては，上記のほかに「コンフィグレーションガイド Vol.1 3.2 収容条件」に記載する制限が存在します。

■ QoS フローリスト数の算出例

QoS フローリスト数の算出例を，次の表に示します。

表 19-9　QoS フローリスト数の算出例

設定例	QoS フローリスト作成数	QoS フローリスト設定数	QoS フローリスト数	フロー検出動作指定数

QoS フローリスト AAA を作成して，イーサネットインタフェース 0/1 の inbound に設定
`interface fastethernet 0/1`
`ip qos-flow-group AAA in`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action cos 5`
`20 qos udp any any action cos 4`
	1 リスト	1 リスト	1 リスト	2 リスト

QoS フローリスト AAA を作成して，イーサネットインタフェース 0/1 と 0/2 の inbound に設定
`interface fastethernet 0/1`
`ip qos-flow-group AAA in`
 	
`interface fastethernet 0/2`
`ip qos-flow-group AAA in`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action cos 5`
`20 qos udp any any action cos 4`
	1 リスト	2 リスト	2 リスト	2 リスト

QoS フローリスト AAA を作成して，イーサネットインタフェース 0/1 の inbound に設定
QoS フローリスト BBB を作成して，イーサネットインタフェース 0/2 の inbound に設定
`interface fastethernet 0/1`
`ip qos-flow-group AAA in`
 	
`interface fastethernet 0/2`
`ip qos-flow-group BBB in`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action cos 5`
`20 qos udp any any action cos 4`
 	
`ip qos-flow-list BBB`
`10 qos udp any any action cos 4`
`20 qos tcp any any action cos 3`
	2 リスト	2 リスト	2 リスト	4 リスト

設定例	QoS フローリスト作成数	QoS フローリスト設定数	QoS フローリスト数	フロー検出動作指定数

QoS フローリスト AAA を作成して，イーサネットインタフェース 0/1 の inbound に設定
QoS フローリスト BBB を作成して，インタフェースには適用しない
`interface fastethernet 0/1`
` ip qos-flow-group AAA in`
 	
`ip qos-flow-list AAA`
` 10 qos tcp any any action cos 5`
` 20 qos udp any any action cos 4`
 	
`ip qos-flow-list BBB`
` 10 qos udp any any action cos 4`
` 20 qos tcp any any action cos 3`
	2 リスト	1 リスト	2 リスト	4 リスト

QoS フローリスト AAA を作成して，インタフェースに適用しない
`ip qos-flow-list AAA`
` 10 qos tcp any any action cos 5`
	1 リスト	0 リスト	1 リスト	1 リスト

ip qos-flow-group

イーサネットインタフェースまたは VLAN インタフェースに対して，IPv4QoS フローリストを適用して QoS 機能を有効にします。

[入力形式]

情報の設定
　ip qos-flow-group <QoS flow list name> in

情報の削除
　no ip qos-flow-group <QoS flow list name> in

[入力モード]

(config-if)

[パラメータ]

<QoS flow list name>

IPv4 QoS フローリスト名称を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

in

Inbound を指定します。

in：Inbound（受信側の指定）

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. system function コマンド設定有で qos が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
2. 同一インタフェースに対して一つの IPv4 QoS フローリストが設定できます。イーサネットインタフェース，VLAN インタフェースに適用する場合は最大 64 個です。
3. 実在しない IPv4 QoS フローリスト名称を設定した場合は何も動作しません。IPv4 QoS フローリスト

名称は登録されます。
4. フロー検出モードによる設定の可否を次の表に示します。

表 19-10　フロー検出モードによる設定の可否（IPv4）

フロー検出モード	設定の可否	
	イーサネット	VLAN
layer2-1	×	×
layer2-2	○	○

（凡例）○：設定可能　×：設定不可

5. 同一のインタフェースに対してこのコマンドで設定されている場合は設定できません。いったん，削除してから設定になります。
6. イーサネットインタフェースに対して適用する場合は，フロー検出条件に VLAN パラメータがあるとき，適用するイーサネットインタフェースの設定内容に VLAN ID が含まれていれば設定できます。
7. VLAN インタフェースに対して適用する場合は，フロー検出条件に VLAN パラメータがない場合だけ設定できます。
8. 一部のパケットは QoS 機能の対象外です。詳細については，「コンフィグレーションガイド Vol.2 3 フロー制御」を参照してください。

[関連コマンド]

ip qos-flow-list

ip qos-flow-list

QoS のフロー検出および動作指定を設定するための IPv4 QoS フローリストを作成します。

QoS フローリスト数，フロー検出条件および動作指定エントリ数については，「■ QoS フローリスト数について」を参照してください。

[入力形式]

情報の設定・変更

ip qos-flow-list <QoS flow list name>

情報の削除

no ip qos-flow-list <QoS flow list name>

[入力モード]

(config)

[パラメータ]

<QoS flow list name>

IPv4 QoS フローリスト名称を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

作成済みの QoS フローリスト名称は指定できません。

[関連コマンド]

ip qos-flow-group

ip qos-flow-list resequence

qos（ip qos-flow-list）

remark

ip qos-flow-list resequence

IPv4 QoS フローリスト内の適用順序のシーケンス番号を再設定します。

[入力形式]

情報の設定・変更
ip qos-flow-list resequence <QoS flow list name> [<Starting seq> [<Increment seq>]]

[入力モード]

(config-ip-qos)

[パラメータ]

<QoS flow list name>

変更する IPv4 QoS フローリスト名称を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 〜 31 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

<Starting seq>

開始シーケンス番号を指定します。

1. 本パラメータ省略時の初期値
   初期値は 10 です。
2. 値の設定範囲
   1 〜 4294967295（10 進数）を指定します。

<Increment seq>

シーケンスインクリメント値を指定します。

1. 本パラメータ省略時の初期値
   初期値は 10 です。
2. 値の設定範囲
   1 〜 100（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ip qos-flow-list

limit-queue-length

物理ポートの最大送信キュー長を装置単位で設定します。

本コマンド省略時，または設定情報を削除したときは，キュー長 32 で動作します。

本コマンドは，ハードウェアの基本的な動作条件を設定するものであるため，設定変更後は装置を再起動する必要があります。

[入力形式]

情報の設定・変更

limit-queue-length <Queue length>

情報の削除

no limit-queue-length

[入力モード]

(config)

[パラメータ]

<Queue length>

物理ポートの最大キュー長を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32，128，728 のいずれかを指定

[コマンド省略時の動作]

本装置の各ポートの送信キュー長は，32 で動作します。

[通信への影響]

本装置の再起動が必要になります。本装置の再起動が完了するまで，本装置を経由する通信は停止します。

[設定値の反映契機]

設定値を変更した場合は，コンフィグレーションを保存したあとで，本装置を再起動してください。再起動すると，設定値が運用に反映されます。

[注意事項]

1. 本コマンド入力時，下記のメッセージが表示されます。他のコンフィグレーションコマンドを入力する前に，設定を保存し本装置を再起動してください。
   Please execute the reload command after save,
   because this command becomes effective after reboot.
2. 本コマンドを設定する前に，qos-queue-list コマンドでスケジューリングモード PQ を設定してください。他のスケジューリングモードでは設定できません。
   送信キュー長を 32 に設定した場合も，同様です。
3. no コマンドで削除した場合，スケジューリングモードの制限はなくなります。
4. 本コマンドで送信キュー長を 32 に設定すると，送信キュー長は次のとおりとなります。
   キュー 1 ～キュー 8：32
5. 本コマンドで送信キュー長を 128 に設定すると，送信キュー長は次のとおりとなります。

キュー 1 ～キュー 4：128
キュー 5 ～キュー 8：0

6. 本コマンドで送信キュー長を 728 に設定すると，送信キュー長は次のとおりとなります。
   キュー 1：728
   キュー 2：32
   キュー 3 ～キュー 8：0
   このとき，flowcontrol コマンドで「ポーズパケットを送信する」を設定してください。

［関連コマンド］

qos-queue-list

flowcontrol

mac qos-flow-group

イーサネットインタフェースまたは VLAN インタフェースに対して，MAC QoS フローリストを適用し，QoS 機能を有効にします。

[入力形式]

情報の設定

mac qos-flow-group <QoS flow list name> in

情報の削除

no mac qos-flow-group <QoS flow list name> in

[入力モード]

(config-if)

[パラメータ]

<QoS flow list name>

MAC QoS フローリスト名称を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 〜 31 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

in

Inbound を指定します。

in : Inbound（受信側の指定）

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. system function コマンド設定有で qos が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
2. 同一インタフェースに対して一つの MAC QoS フローリストが設定できます。イーサネットインタフェース，VLAN インタフェースに適用する場合は最大 64 個です。
3. 実在しない MAC QoS フローリスト名称を設定した場合は何も動作しません。MAC QoS フローリスト

名称は登録されます。

4. フロー検出モードによる設定の可否を次の表に示します。

表 19-11　フロー検出モードによる設定の可否（MAC）

受信側フロー検出モード	設定の可否	
	イーサネット	VLAN
layer2-1	○	○
layer2-2	×	×

（凡例）　○：設定可能　×：設定不可

5. 同一のインタフェースに対してこのコマンドで設定されている場合は設定できません。いったん，削除してから設定になります。
6. イーサネットインタフェースに対して適用する場合は，フロー検出条件に VLAN パラメータがあるとき，適用するイーサネットインタフェースの設定内容に VLAN ID が含まれていれば設定できます。
7. VLAN インタフェースに対して適用する場合は，フロー検出条件に VLAN パラメータがない場合だけ設定できます。
8. 一部のパケットは QoS 機能の対象外です。詳細については，「コンフィグレーションガイド Vol.2 3 フロー制御」を参照してください。

[関連コマンド]

mac qos-flow-list

mac qos-flow-list

QoS のフロー検出および動作指定を設定するための MAC QoS フローリストを作成します。

QoS フローリスト数，フロー検出条件および動作指定エントリ数については，「■ QoS フローリスト数について」を参照してください。

[入力形式]

情報の設定・変更
　mac qos-flow-list <QoS flow list name>

情報の削除
　no mac qos-flow-list <QoS flow list name>

[入力モード]

(config)

[パラメータ]

<QoS flow list name>
　MAC QoS フローリスト名称を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 作成済みの IPv4 QoS フローリスト名称は指定できません。

[関連コマンド]

mac qos-flow-group

mac qos-flow-list resequence

qos（mac qos-flow-list）

remark

mac qos-flow-list resequence

MAC QoS フローリスト内の適用順序のシーケンス番号を再設定します。

[入力形式]

情報の設定・変更

mac qos-flow-list resequence <QoS flow list name> [<Starting seq> [<Increment seq>]]

[入力モード]

(config-mac-qos)

[パラメータ]

<QoS flow list name>

変更する MAC QoS フローリスト名称を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

<Starting seq>

開始シーケンス番号を指定します。

1. 本パラメータ省略時の初期値
   初期値は 10 です。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します。

<Increment seq>

シーケンスインクリメント値を指定します。

1. 本パラメータ省略時の初期値
   初期値は 10 です。
2. 値の設定範囲
   1 ～ 100（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

mac qos-flow-list

qos（ip qos-flow-list）

IPv4 QoS フローリストでのフロー検出条件，および動作指定を指定します。

[入力形式]

情報の設定・変更

[<Seq>] qos { フロー検出条件 } [動作指定]

- フロー検出条件

上位プロトコルが TCP，UDP 以外の場合

{ip | <Protocol> | icmp | igmp } {<Src IPv4> <Src IPv4 wildcard> | host <Src IPv4> | any}{<Dst IPv4> <Dst IPv4 wildcard> | host <Dst IPv4> | any} [{ [tos <TOS>] [precedence <Precedence>] | dscp <DSCP>}] [vlan <VLAN ID>] [user-priority <Priority>]

上位プロトコルが TCP の場合

tcp {<Src IPv4> <Src IPv4 wildcard> | host <Src IPv4> | any} [eq <Src port>] {<Dst IPv4> <Dst IPv4 wildcard> | host <Dst IPv4> | any} [eq <Dst port>] [ack] [fin] [psh] [rst] [syn] [urg] [{ [tos <TOS>] [precedence <Precedence>] | dscp <DSCP>}] [vlan <VLAN ID>] [user-priority <Priority>]

上位プロトコルが UDP の場合

udp {<Src IPv4> <Src IPv4 wildcard> | host <Src IPv4> | any} [eq <Src port>] {<Dst IPv4> <Dst IPv4 wildcard> | host <Dst IPv4> | any} [eq <Dst port>] [{ [tos <TOS>] [precedence <Precedence>] | dscp <DSCP>}] [vlan <VLAN ID>] [user-priority <Priority>]

- 動作指定
  action [cos <COS>] [replace-user-priority <Priority>] [replace-dscp <DSCP>]

情報の削除

no <Seq>

[入力モード]

(config-ip-qos)

[パラメータ]

<Seq>

作成および変更する QoS フローリスト内の適用順序を指定します。

1. 本パラメータ省略時の初期値
   QoS フローリスト内に条件がない場合，初期値は 10 です。
   条件を設定してある場合，設定してある適用順序の最大値 +10 です。
   ただし，適用順序の最大値が 4294967285 より大きい値を設定した場合は省略できません。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します。

{ip | <Protocol> | icmp | igmp | tcp | udp }

IPv4 パケットの上位プロトコル条件を指定します。

ただし，すべてのプロトコルを対象とする場合は ip を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   - <Protocol>：

0 ～ 255（10 進数）またはプロトコル名称を指定します。
「表 19-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{<Src IPv4> <Src IPv4 wildcard> | host <Src IPv4> | any }

送信元 IPv4 アドレスを指定します。
すべての送信元 IPv4 アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Src IPv4> <Src IPv4 wildcard>，host <Src IPv4> または any を指定します。
   - <Src IPv4> <Src IPv4 wildcard> 指定：
   <Src IPv4> には送信元 IPv4 アドレスを指定します。
   <Src IPv4 wildcard> には IPv4 アドレスの中で任意の値を許可するビットを立てたワイルドカードを IPv4 アドレス形式で指定します。
   - host <Src IPv4> 指定：
   <Src IPv4> の完全一致をフロー検出条件とします。
   - any 指定：
   送信元 IPv4 アドレスをフロー検出条件とはしません。
   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

eq <Src Port>

送信元ポート番号を指定します。
プロトコルが TCP および UDP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 65535（10 進数）またはポート名称を指定します。
   指定可能なポート名称は「表 19-2　TCP で指定可能なポート名称」および「表 19-3　UDP で指定可能なポート名称（IPv4）」を参照してください。

{<Dst IPv4> <Dst IPv4 wildcard> | host <Dst IPv4> | any}

宛先 IPv4 アドレスを指定します。
すべての宛先 IPv4 アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Dst IPv4> <Dst IPv4 wildcard>，host <Dst IPv4> または any を指定します。
   - <Dst IPv4> <Dst IPv4 wildcard> 指定：
   <Dst IPv4> には宛先 IPv4 アドレスを指定します。
   <Dst IPv4 wildcard> には IPv4 アドレスの中で任意の値を許可するビットを立てたワイルドカードを IPv4 アドレス形式で指定します。
   - host <Dst IPv4> 指定：
   <Dst IPv4> の完全一致をフロー検出条件とします。
   - any 指定：
   宛先 IPv4 アドレスをフロー検出条件とはしません。
   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

eq <Dst Port>

宛先ポート番号を指定します。
プロトコルが TCP および UDP だけのオプションです。
1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 65535（10 進数）またはポート名称を指定します。
   指定可能なポート名称については，「表 19-2　TCP で指定可能なポート名称」および「表 19-3　UDP で指定可能なポート名称（IPv4）」を参照してください。

tos <TOS>

本パラメータは，TOS フィールドのビット 3 ～ 6 の 4 ビットである TOS 値を指定します。
送受信パケットの TOS フィールドのビット 3 ～ 6 の 4 ビットと比較します。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			TOS				-

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 15（10 進数）または TOS 名称を指定します。
   指定可能な TOS 名称については，「表 19-4　指定可能な TOS 名称」を参照してください。

precedence <Precedence>

本パラメータは，TOS フィールドの上位 3 ビットである Precedence 値を指定します。
送受信パケットの TOS フィールド上位 3 ビットと比較します。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			TOS				-

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）または Precedence 名称を指定します。
   指定可能な Precedence 名称については，「表 19-5　指定可能な Precedence 名称」を参照してください。

dscp <DSCP>

本パラメータは，TOS フィールドの上位 6 ビットである DSCP 値を指定します。
受信パケットの TOS フィールド上位 6 ビットと比較します。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 63（10 進数）または DSCP 名称を指定します。
   指定可能な DSCP 名称については，「表 19-6　指定可能な DSCP 名称」を参照してください。

ack

TCP ヘッダの ACK フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

fin

TCP ヘッダの FIN フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

psh

TCP ヘッダの PSH フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

rst

TCP ヘッダの RST フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

syn

TCP ヘッダの SYN フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

urg

TCP ヘッダの URG フラグが 1 のパケットの検出を指定します。

プロトコルが TCP だけのオプションです。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   なし

vlan <VLAN ID>

VLAN ID を指定します。

本パラメータはイーサネットインタフェースに適用した場合だけ有効です。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）

2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

user-priority <Priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

cos <COS>

装置内の優先度を示すインデックス（Cos）を指定します。

1. 本パラメータ省略時の初期値
   デフォルトの COS 値となります。デフォルトの COS 値については「コンフィグレーションガイド Vol.2　3.7.1　COS 値」を参照してください。
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

replace-user-priority <Priority>

ユーザ優先度の書き換え値を指定します。

受信したパケットのユーザ優先度を指定値 <Priority> に書き換えます。

1. 本パラメータ省略時の初期値
   なし（ユーザ優先度を書き換えません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

replace-dscp <DSCP>

DSCP 書き換え値を指定します。

受信したパケットの DSCP フィールドを，指定値 <DSCP> に書き換えます。

1. 本パラメータ省略時の初期値
   なし（DSCP 値を書き換えません)。
2. 値の設定範囲
   0 ～ 63（10 進数）または DSCP 名称を指定します。
   指定可能な DSCP 名称については，「表 19-6　指定可能な DSCP 名称」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元アドレスワイルドカードおよび宛先アドレスワイルドカードに 255.255.255.255 と入力したときは any と表示します。
2. 信元アドレスおよび宛先アドレスに nnn.nnn.nnn.nnn 0.0.0.0 と入力したときは host nnn.nnn.nnn.nnn と表示します。
3. tos および precedence と dscp の同時設定はできません。
4. action パラメータで cos と replace-user-priority を同時に設定した場合，ユーザ優先度は cos の設定値に書き換えられます。

[関連コマンド]

ip qos-flow-list

ip qos-flow-group

ip qos-flow-list resequence

remark

qos（mac qos-flow-list）

MAC QoS フローリストでのフロー検出条件，および動作指定を指定します。

[入力形式]

情報の設定・変更

[<Seq>] qos { フロー検出条件 } [動作指定]

- フロー検出条件
  {<Src MAC> <Src MAC mask> | host <Src MAC> | any}{<Dst MAC> <Dst MAC mask> | host <Dst MAC> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu }[<Ethernet type>] [vlan <VLAN ID>] [user-priority <Priority>]
- 動作指定
  action [cos <COS>] [replace-user-priority <Priority>]

情報の削除

no <Seq>

[入力モード]

(config-mac-qos)

[パラメータ]

<Seq>

作成および，変更する QoS フローリスト内シーケンス番号を指定します。

1. 本パラメータ省略時の初期値
   QoS フローリスト内に条件がない場合，初期値は 10 です。
   条件を設定してある場合，設定してある適用順序の最大値 +10 です。
   ただし，適用順序の最大値が 4294967285 より大きい値を設定した場合は省略できません。
2. 値の設定範囲
   1 ～ 4294967295（10 進数）を指定します。

{<Src MAC> <Src MAC mask> | host <Src MAC> | any}

送信元 MAC アドレスを指定します。すべての送信元 MAC アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Src MAC> <Src MAC mask>，host <Src MAC> または any を指定します。
   - <Src MAC> <Src MAC mask> 指定：
     <Src MAC> には送信元 MAC アドレスを指定します。
     <Src MAC mask> には MAC アドレスの中で任意の値を許可するビットを立てたマスクを MAC アドレス形式で指定します。
   - host <Src MAC> 指定：
     <Src MAC> の完全一致をフロー検出条件とします。
   - any 指定：
     送信元 MAC アドレスをフロー検出条件とはしません。

   MAC アドレス（nnnn.nnnn.nnnn）：0000.0000.0000 ～ ffff.ffff.ffff（16 進数）

{<Dst MAC> <Dst MAC mask> | host <Dst MAC> | any | bpdu | cdp | lacp | lldp | oadp |

pvst-plus-bpdu }

宛先 MAC アドレスを指定します。すべての宛先 MAC アドレスを指定する場合は any を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Dst MAC> <Dst MAC mask>，host <Dst MAC>，any，bpdu，cdp，lacp，lldp，oadp または pvst-plus-bpdu を指定します。
   - <Dst MAC> <Dst MAC mask> 指定：
     <Dst MAC> には宛先 MAC アドレスを指定します。
     <Dst MAC mask> には MAC アドレスの中で任意の値を許可するビットを立てたマスクを MAC アドレス形式で指定します。
   - host <Dst MAC> 指定：
     <Dst MAC> の完全一致をフロー検出条件とします。
   - any 指定：
     宛先 MAC アドレスをフロー検出条件とはしません。
   - bpdu 指定：
     BPDU 制御パケットをフロー検出条件とします。
   - cdp 指定：
     CDP 制御パケットをフロー検出条件とします。
   - lacp 指定：
     LACP 制御パケットをフロー検出条件とします。
   - lldp 指定：
     LLDP 制御パケットをフロー検出条件とします。
   - oadp 指定：
     OADP 制御パケットをフロー検出条件とします。
   - pvst-plus-bpdu 指定：
     PVST+ 制御パケットをフロー検出条件とします。

   MAC アドレス（nnnn.nnnn.nnnn）：0000.0000.0000 ～ ffff.ffff.ffff（16 進数）

<Ethernet type>

イーサネットタイプ番号またはイーサネットタイプ名称を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0x0000 ～ 0xffff（16 進数）または，イーサネットタイプ名称を指定します。
   指定可能なイーサネットタイプ名称は「表 19-7　指定可能なイーサネットタイプ名称」を参照してください。

vlan <VLAN ID>

VLAN ID を指定します。

本パラメータはイーサネットインタフェースに適用した場合だけ有効です。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

user-priority <Priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

cos <COS>

装置内の優先度を示すインデックス（Cos）を指定します。

1. 本パラメータ省略時の初期値
   デフォルトの COS 値となります。デフォルトの COS 値については「コンフィグレーションガイド Vol.2　3.7.1　COS 値」を参照してください。
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

replace-user-priority <Priority>

ユーザ優先度の書き換え値を指定します。
受信したパケットのユーザ優先度を指定値 <Priority> に書き換えます。

1. 本パラメータ省略時の初期値
   なし（ユーザ優先度を書き換えません）。
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元アドレスおよび宛先アドレスに nnnn.nnnn.nnnn ffff.ffff.ffff と入力したときは any と表示します。
2. 宛先アドレスにプロトコル名称設定または設定できるプロトコル名称のアドレスを設定している場合はプロトコル名称を表示します。宛先アドレスに設定できるプロトコル名称のアドレスは「表 19-8　指定可能な宛先 MAC アドレス名称」を参照してください。上記以外の送信元アドレスおよび宛先アドレスに nnnn.nnnn.nnnn 0000.0000.0000 と入力したときは host nnnn.nnnn.nnnn と表示します。
3. action パラメータで cos と replace-user-priority を同時に設定した場合，ユーザ優先度は cos の設定値に書き換えられます。

4. 本コマンドで設定するパラメータは，中継パケットに対してのみ有効となります。従って，設定したパラメータは自宛・自発パケットに対しては有効となりません。

［関連コマンド］

mac qos-flow-list

mac qos-flow-group

mac qos-flow-list resequence

remark

qos-queue-group

インタフェース（物理ポート）に QoS キューリスト情報を設定します。

［入力形式］

情報の設定
　qos-queue-group <QoS queue list name>

情報の削除
　no qos-queue-group

［入力モード］

(config-if)

［パラメータ］

<QoS queue list name>

QoS キューリスト名称を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

［コマンド省略時の動作］

スケジューリングモードは PQ で動作します。

［通信への影響］

QoS キューリスト名を設定してスケジューリングモードを変更した場合，当該回線の送信キューにキューイングしたパケットが残っている場合，すべてクリアします。

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. QoS キューリスト名称を設定してスケジューリングモードを変更した場合，変更したインタフェースで送信キューにキューイングしたパケットが残っている場合，すべてクリアします。クリア処理中は，新たなパケットをキューイングできません。ネットワーク経由でログインされている場合はご注意ください。
2. QoS キューリスト名を指定してスケジューリングモード設定を行わなかった場合，スケジューリングモードは PQ で動作します。
3. qos-queue-group コマンドで無効な QoS キューリスト名を指定した場合，スケジューリングモードは PQ で動作します。

[関連コマンド]

qos-queue-list

interface fastethernet

interface gigabitethernet

qos-queue-list

QoS キューリスト情報にスケジューリングモードを設定します。装置単位で最大 52 リスト作成できます。

[入力形式]

情報の設定・変更

qos-queue-list <QoS queue list name> { pq | wrr [<Packet1> <Packet2> <Packet3> <Packet4> <Packet5> <Packet6> <Packet7> <Packet8>] | wfq [min-rate1 <Min rate1>] [min-rate2 < Min rate2>] [min-rate3 < Min rate3>] [min-rate4 < Min rate4>] [min-rate5 < Min rate5>] [min-rate6 < Min rate6>] [min-rate7 < Min rate7>] [min-rate8 < Min rate8>] | 2pq+6wrr < Packet1> < Packet2> < Packet3> < Packet4> < Packet5> < Packet6> }

情報の削除

no qos-queue-list <QoS queue list name>

[入力モード]

(config)

[パラメータ]

<QoS queue list name>

QoS キューリスト名称を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

{ pq | wrr [<Packet1> <Packet2> <Packet3> <Packet4> <Packet5> <Packet6> <Packet7> <Packet8>] | wfq [min-rate1 <Min rate1>] [min-rate2 < Min rate2>] [min-rate3 < Min rate3>] [min-rate4 < Min rate4>] [min-rate5 < Min rate5>] [min-rate6 < Min rate6>] [min-rate7 < Min rate7>] [min-rate8 < Min rate8>] | 2pq+6wrr < Packet1> < Packet2> < Packet3> < Packet4> < Packet5> < Packet6> }

スケジューリングモードを指定します。

1. 本パラメータ省略時の初期値
   省略できません。

pq

完全優先で動作します。キュー数は物理ポート単位で 8 キュー固定です。複数のキューにパケットが存在する場合，優先度の高いキュー番号（8>7>…>1 番キュー）からパケットを常に送信します。

wrr [<Packet1> <Packet2> <Packet3> <Packet4> <Packet5> <Packet6> <Packet7> <Packet8>]

ラウンドロビンもしくは重み（パケット数）付きラウンドロビンで動作します。キュー数は物理ポート単位で 8 キュー固定です。<Packet> の設定を省略した場合はラウンドロビンで動作します。順番にキューを見ながらパケットを送信します。キュー長にかかわらず，パケット数が均等になるように制御します。<Packet> を設定した場合は重み（パケット数）付きラウンドロビンで動作します。複数のキューにパケットが存在する場合，順番にキューを見ながら設定した <Packet> のパケット数に応じてパケットを送信します。なお，<Packet> の後ろに付く 1 ～ 8 の番号は，キュー番号を意味します。

1. 本パラメータ省略時の初期値
   <Packet>：省略できません。

ただし，全 <Packet> の省略は可能で，省略時はラウンドロビンで動作します。

2. 値の設定範囲
   <Packet>：1 〜 15

wfq [min-rate1 <Min rate1>] [min-rate2 < Min rate2>] [min-rate3 < Min rate3>] [min-rate4 < Min rate4>] [min-rate5 < Min rate5>] [min-rate6 < Min rate6>] [min-rate7 < Min rate7>] [min-rate8 < Min rate8>]

重み付き均等保証。キュー数は物理ポート単位で 8 キュー固定です。キューごとに <Min rate> で設定した最低保証帯域分をパケットに送信します。なお，<Min rate> の後ろに付く 1 〜 8 の番号は，キュー番号を意味します。

1. 本パラメータ省略時の初期値
   <Min rate>：なし（最低保証帯域を設定しません）
2. 値の設定範囲
   min-rate <Min rate>：次の表に示します。
   値の単位には k（省略），M が指定可能です。
   { <Min rate> | <Min rate>M }
   <Min rate> の合計値は回線帯域を超えない値を設定してください。

表 19-12　最低保証帯域の設定範囲

設定単位※1	設定範囲	刻み値
Mbit/s	1M 〜 1000M	1Mbit/s
kbit/s	1000 〜 1000000	100kbit/s ※2
	64 〜 960	64kbit/s ※3

注※ 1　1M，1k はそれぞれ 1000000，1000 として扱います。

注※ 2　設定値が 1000k 以上の場合，100k 刻みで指定します（1000，1100，1200，…，10000000）。

注※ 3　設定値が 1000k 未満の場合，64k 刻みで指定します（64，128，192，…，960）。

2pq+6wrr < Packet1> < Packet2> < Packet3> < Packet4> < Packet5> < Packet6>

最優先キュー付き，重み（パケット数）付きラウンドロビン。キュー数は物理ポート単位で 8 キュー固定です。最優先のキュー 8 にパケットが存在する場合，該当パケットを最優先で送信します。キュー 7 はキュー 8 の次に優先的に該当パケットを送信します。キュー 8，キュー 7 にパケットが存在しない場合，キュー 6 〜 1 の <Packet> に設定したパケット数に応じてパケットを送信します。なお，<Packet> の後ろに付く 1 〜 6 の番号は，キュー番号を意味します。

1. 本パラメータ省略時の初期値
   <Packet>：省略できません。
2. 値の設定範囲
   <Packet>：1 〜 15

[コマンド省略時の動作]

なし

[通信への影響]

qos-queue-group コマンドに QoS キューリスト名称を設定してスケジューリングモードを変更した場合，当該回線の送信キューにキューイングしたパケットが残っている場合，すべてクリアします。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. qos-queue-group コマンドに QoS キューリスト名称を設定してスケジューリングモードを変更した場合，変更したインタフェースで送信キューにキューイングしたパケットが残っている場合，すべてクリアします。クリア処理中は，新たなパケットをキューイングできません。ネットワーク経由でログインされている場合はご注意ください。
2. 回線状態が半二重モードの場合，WFQ は正常に動作しません。全二重モードで使用してください。
3. WFQ を設定した場合，設定した最低保証帯域値と実際の動作値では最大 10% の誤差が生じることがあります。
4. ポート帯域制御と QoS キューリスト情報のスケジューリングを同時に使用する場合，スケジューリングモードは PQ を設定してください。
5. スケジューリングモードに wfq を選択した場合，使用するキューに対しては，<Min rate> を必ず設定してください。
6. 帯域幅を Mbit/s 単位（<Mbit/s>M）で設定した場合，show running-config/show startup-config では kbit/s 単位で表示されます。

[関連コマンド]

qos-queue-group

remark

QoS フローリストの補足説明を設定します。

QoS フローリストには IPv4 QoS フローリストまたは MAC QoS フローリストがあります。

[入力形式]

情報の設定・変更

remark <Remark>

情報の削除

no remark

[入力モード]

(config-ip-qos)
(config-mac-qos)

[パラメータ]

<Remark>

入力モードにより対象となる QoS フローリストの補足説明を設定します。

一つの QoS フローリストに対して 1 行だけ設定できます。再度入力した場合は上書きになります。

1. 本パラメータ省略時の初期値
   初期値は Null です。
2. 値の設定範囲
   64 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ip qos-flow-list

mac qos-flow-list

traffic-shape rate

インタフェース（物理ポート）にポート帯域制御を設定し，送信帯域を指定した帯域に制限します。

[入力形式]

情報の設定・変更

traffic-shape rate { <kbit/s> | <Mbit/s>M }

情報の削除

no traffic-shape rate

[入力モード]

(config-if)

[パラメータ]

rate { <kbit/s> | <Mbit/s>M }

ポート帯域制御を使用します。本機能を使用することで，回線全体の送信帯域を指定した帯域に制限します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   次の表に示します。
   値の単位には k（省略），M が指定できます。
   設定帯域は回線速度以下になるように設定してください。

表 19-13　ポート帯域制御の設定範囲

設定単位※1	設定範囲	刻み値
Mbit/s	1M ～ 1000M	1Mbit/s
kbit/s	1000 ～ 1000000	100kbit/s※2
	64 ～ 960	64kbit/s※3

注※1　1M，1k はそれぞれ 1000000，1000 として扱います。
注※2　設定値が 1000k 以上の場合，100k 刻みで指定します（1000，1100，1200，…，10000000）。
注※3　設定値が 1000k 未満の場合，64k 刻みで指定します（64，128，192，…，960）。

[コマンド省略時の動作]

送信帯域に制限をかけません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 設定したポート帯域制御値と実際の動作値では最大 10% の誤差が生じる場合があります。
2. 回線状態が半二重の場合，ポート帯域制御をサポートしません。

3. ポート帯域制御と QoS キューリスト情報のスケジューリングを同時に使用する場合，スケジューリングモードは PQ を設定してください。
4. 帯域幅を Mbit/s 単位（<Mbit/s>M）で設定した場合，show running-config/show startup-config では kbit/s 単位で表示されます。
5. ポート帯域制御の設定帯域が回線速度を超えた場合，ポート帯域制御は動作しません。

［関連コマンド］

interface fastethernet

interface gigabitethernet

control-packet user-priority

本装置が自発的に送信するフレームの VLAN Tag 内にあるユーザ優先度を指定します。本コマンド未設定または情報を削除したときは，自発的に送信するフレームのユーザ優先度は 7 となります。

［入力形式］

情報の設定・変更

control-packet user-priority { layer-2 <User-priority> | layer-3 <User-priority> | layer-2 <User-priority> layer-3 <User-priority> }

情報の削除

no control-packet user-priority

［入力モード］

(config)

［パラメータ］

{ layer-2 <User-priority> | layer-3 <User-priority> | layer-2 <User-priority> layer-3 <User-priority> }

本装置が自発的に送信するフレームのユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 7 を指定します。設定しなかったパラメータのユーザ優先度は 7 となります。

［コマンド省略時の動作］

本装置が自発的に送信するフレームのユーザ優先度は 7 となります。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

なし

［関連コマンド］

なし

20 レイヤ 2 認証共通

authentication arp-relay

認証前端末から受信する ARP パケットを他ポートに中継します。

レイヤ２認証機能を使用時，認証前の端末から送信される他機器宛て ARP パケットを認証対象外のポートへ出力させます。

本コマンドは下記の認証モードで使用できます。

- IEEE802.1X：ポート単位認証（静的），ポート単位認証（動的）
- Web 認証：固定 VLAN モード，ダイナミック VLAN モード
- MAC 認証：固定 VLAN モード，ダイナミック VLAN モード

[入力形式]

情報の設定

authentication arp-relay

情報の削除

no authentication arp-relay

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定する場合は，あらかじめ当該ポートに下記のいずれかを設定してください。
   - dot1x port-control
   - web-authentication port
   - mac-authentication port
2. IEEE802.1X ポート単位認証（静的）で認証専用 IPv4 アクセスリストを使用するときは，下記に注意してください。
   - system function コマンド設定有で extended-authentication が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
3. 本コマンドは認証機能別に設定可能なインタフェースが異なります。
   - IEEE802.1X ポート単位認証（静的）は，イーサネットインタフェース，ポートチャネルインタフェースで設定可能です。

- IEEE802.1X ポート単位認証（動的），Web 認証，および MAC 認証はイーサネットインタフェースだけ設定可能です。

[関連コマンド]

dot1x system-auth-control

dot1x port-control

web-authentication system-auth-control

web-authentication port

web-authentication redirect enable

mac-authentication system-auth-control

mac-authentication port

authentication force-authorized enable

全レイヤ 2 認証で，次に示す状態が発生した場合，認証要求した認証対象端末を強制的に認証許可状態とします。

- RADIUS 認証方式で，設定された RADIUS サーバからの応答がなくなったとき

[入力形式]

情報の設定
　authentication force-authorized enable

情報の削除
　no authentication force-authorized enable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本機能は，セキュリティ上の問題となるおそれがありますので，十分検討の上使用してください。
2. ダイナミック VLAN モードの場合，認証後 VLAN として該当ポートのネイティブ VLAN を割り当てます。
   特定の VLAN を，認証後 VLAN として割り当てたい場合は，authentication force-authorized vlan コマンドで指定してください。
3. 本コマンドは，装置に下記コマンドが 1 つでも設定されている場合には，設定できません。
   - dot1x force-authorized
   - dot1x force-authorized vlan
   - mac-authentication force-authorized vlan
   - mac-authentication static-vlan force-authorized
   - web-authentication force-authorized vlan
   - web-authentication static-vlan force-authorized
4. RADIUS 認証だけ設定された場合に動作します。複数の認証方式を設定した場合は，強制認証は実施されません。
5. 汎用 RADIUS サーバ情報，または認証専用 RADIUS サーバ情報を登録してください。詳細については，「コンフィグレーションガイド Vol.2 5. レイヤ 2 認証機能の概説」を参照してください。
6. 強制認証のプライベート Trap は，snmp-server traps コマンドの設定に関係なく送出されます。

7. 本機能はレガシーモード対象外です。

[関連コマンド]

aaa authentication dot1x default

aaa authentication mac-authentication default

aaa authentication web-authentication default

dot1x port-control

dot1x system-auth-control

dot1x radius-server

radius-server

mac-authentication port

mac-authentication system-auth-control

mac-authentication radius-server

web-authentication port

web-authentication system-auth-control

web-authentication radius-server

authentication force-authorized vlan

Web 認証と MAC 認証のダイナミック VLAN モード，および IEEE802.1X 認証のポート単位認証 (動的) で，該当ポートで強制認証を実施した場合の認証後 VLAN を割り当てます。

[入力形式]

情報の設定・変更

authentication force-authorized vlan <VLAN ID>

情報の削除

no authentication force-authorized vlan

[入力モード]

(config-if)

[パラメータ]

<VLAN ID>

強制認証時に割り当てる認証後 VLAN として MAC VLAN を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。
   ただし，デフォルト VLAN（VLAN ID ＝ 1）は設定できません。

[コマンド省略時の動作]

認証後 VLAN として，該当ポートのネイティブ VLAN を割り当てます。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドは，authentication force-authorized enable コマンド設定時にだけ有効です。
2. 本コマンドを設定，または削除したとき，現在認証済みの端末やユーザは，以前の設定で収容された VLAN で動作します。本設定値は，再認証または次回の認証から有効になります。
3. 本機能はレガシーモード対象外です。

[関連コマンド]

authentication force-authorized enable

vlan mac-based

authentication ip access-group

認証前端末から受信する IP パケットに本コマンドで指定した IPv4 アクセスリストを適用し，合致 (permit) したパケットだけを他ポートに中継します。本コマンドで指定した IPv4 アクセスリストに合致 (permit) した IP パケットは，URL リダイレクトの対象となりません。

本コマンドは下記の認証モードで使用できます。

- IEEE802.1X：ポート単位認証（静的），ポート単位認証（動的）
- Web 認証：固定 VLAN モード，ダイナミック VLAN モード
- MAC 認証：固定 VLAN モード，ダイナミック VLAN モード

[入力形式]

情報の設定

authentication ip access-group <ACL ID>

情報の削除

no authentication ip access-group

[入力モード]

(config-if)

[パラメータ]

<ACL ID>

認証対象外ポートへ出力させるための IPv4 パケットフィルタの識別子を指定します。本パラメータで設定できる IPv4 パケットフィルタの識別子は装置で 1 つです。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

認証前端末から受信した IPv4 パケットを中継しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドで設定するアクセスリスト名は装置全体で 1 件です。
2. 本コマンドを設定する場合は，あらかじめ当該ポートに下記のいずれかを設定してください。
   - dot1x port-control
   - web-authentication port
   - mac-authentication port

3. IEEE802.1X ポート単位認証（静的）で認証専用 IPv4 アクセスリストを使用するときは，下記に注意してください。
   - system function コマンド設定有で extended-authentication が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
4. 本コマンドは認証機能別に設定可能なインタフェースが異なります。
   - IEEE802.1X ポート単位認証（静的）は，イーサネットインタフェース，ポートチャネルインタフェースで設定可能です。
   - IEEE802.1X ポート単位認証（動的），Web 認証，および MAC 認証はイーサネットインタフェースだけ設定可能です。

[関連コマンド]

dot1x system-auth-control

dot1x port-control

web-authentication system-auth-control

web-authentication port

web-authentication redirect enable

mac-authentication system-auth-control

mac-authentication port

ip access-list extended

21 IEEE802.1X

コンフィグレーションコマンドと認証モードの対応
aaa accounting dot1x
aaa authentication dot1x
aaa authorization network default
dot1x authentication
dot1x auto-logout
dot1x force-authorized
dot1x force-authorized eapol
dot1x force-authorized vlan
dot1x ignore-eapol-start
dot1x max-req
dot1x multiple-authentication
dot1x port-control
dot1x radius-server dead-interval
dot1x radius-server host
dot1x reauthentication
dot1x supplicant-detection
dot1x system-auth-control
dot1x timeout keep-unauth
dot1x timeout quiet-period
dot1x timeout reauth-period
dot1x timeout server-timeout
dot1x timeout supp-timeout
dot1x timeout tx-period
dot1x vlan dynamic enable

dot1x vlan dynamic ignore-eapol-start
dot1x vlan dynamic max-req
dot1x vlan dynamic radius-vlan
dot1x vlan dynamic reauthentication
dot1x vlan dynamic supplicant-detection
dot1x vlan dynamic timeout quiet-period
dot1x vlan dynamic timeout reauth-period
dot1x vlan dynamic timeout server-timeout
dot1x vlan dynamic timeout supp-timeout
dot1x vlan dynamic timeout tx-period

コンフィグレーションコマンドと認証モードの対応

IEEE802.1X のコンフィグレーションコマンドが設定できる，IEEE802.1X の認証モードを次の表に示します。

表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード

コマンド名	IEEE802.1X の認証モード※4		
	ポート単位認証		VLAN 単位認証
	（静的）	（動的）	（動的）
aaa accounting dot1x	○	○	○
aaa authentication dot1x	○	○	○
aaa authorization network default	－	－	○
authentication arp-relay※1	○	○	×
authentication ip access-group※1	○	○	×
dot1x authentication	○	○	×
dot1x auto-logout	○	○	○
dot1x force-authorized	○	×	×
dot1x force-authorized eapol	○	○	○
dot1x force-authorized vlan	×	○	○
dot1x ignore-eapol-start	○	○	－
dot1x max-req	○	○	－
dot1x multiple-authentication	○	○	－
dot1x port-control※2	○	○	－
dot1x radius-server dead-interval	○	○	○
dot1x radius-server host	○	○	○
dot1x reauthentication	○	○	－
dot1x supplicant-detection	○	○	－
dot1x system-auth-control	○	○	○
dot1x timeout keep-unauth※3	○	○	－
dot1x timeout quiet-period	○	○	－
dot1x timeout reauth-period	○	○	－
dot1x timeout server-timeout	○	○	－
dot1x timeout supp-timeout	○	○	－
dot1x timeout tx-period	○	○	－
dot1x vlan dynamic enable	－	－	○
dot1x vlan dynamic ignore-eapol-start	－	－	○
dot1x vlan dynamic max-req	－	－	○
dot1x vlan dynamic radius-vlan	－	－	○
dot1x vlan dynamic reauthentication	－	－	○
dot1x vlan dynamic supplicant-detection	－	－	○

コマンド名	IEEE802.1X の認証モード※4		
	ポート単位認証		VLAN 単位認証
	（静的）	（動的）	（動的）
dot1x vlan dynamic timeout quiet-period	－	－	○
dot1x vlan dynamic timeout reauth-period	－	－	○
dot1x vlan dynamic timeout server-timeout	－	－	○
dot1x vlan dynamic timeout supp-timeout	－	－	○
dot1x vlan dynamic timeout tx-period	－	－	○

凡例

○：設定内容に従って動作します。

－：コマンドは入力できますが，動作しません。

×：コマンドを入力できません。

注※ 1

コマンドの入力形式など詳細は，「20　レイヤ 2 認証共通」を参照してください。

注※ 2

本コマンドの設定は，認証モードの切り替えに影響します。

注※ 3

本コマンドの設定は，ポート単位認証（静的）およびポート単位認証（動的）のシングルモードだけ適用します。

注※ 4

認証モードの表記など詳細については，「コンフィグレーションガイド Vol.2」を参照してください。

aaa accounting dot1x

IEEE802.1X のアカウンティング情報をアカウンティングサーバへ送信します。

[入力形式]

情報の設定
aaa accounting dot1x default start-stop group radius

情報の削除
no aaa accounting dot1x default

[入力モード]

(config)

[パラメータ]

default
装置デフォルトのアカウンティング方式を設定します。

start-stop
認証成功時にはスタートアカウンティング通知が，認証解除時にはストップアカウンティング通知がアカウンティングサーバに送信されます。

group radius
アカウンティングサーバとして RADIUS サーバを使用します。

[コマンド省略時の動作]

アカウンティングサーバに通知しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。

[関連コマンド]

aaa authentication dot1x

dot1x system-auth-control

radius-server host または dot1x radius-server host

aaa authentication dot1x

IEEE802.1X の認証方式グループを設定します。

default 指定は 1 エントリ，認証方式リスト指定は最大 4 エントリまで設定できます。

[入力形式]

情報の設定・変更

aaa authentication dot1x default <Method>

aaa authentication dot1x <List name> group <Group name>

情報の削除

no aaa authentication dot1x {default | <List name>}

[入力モード]

(config)

[パラメータ]

default <Method>

装置デフォルトの認証方式を設定します。<Method> には group radius を設定します。

group radius

RADIUS サーバによる IEEE802.1X 認証を行います。使用する RADIUS サーバは IEEE802.1X 専用 RADIUS サーバまたは，汎用 RADIUS サーバです。

<List name>

認証方式リスト名を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。
   先頭文字は大文字を推奨します。
   ただし，下記の文字列は設定できません。
   ・アットマーク (@)
   ・default(前方一致または完全一致した文字列)

group <Group Name>

RADIUS サーバによる IEEE802.1X 認証を行います。使用する RADIUS サーバは RADIUS サーバグループです。aaa group server radius コマンドで設定した RADIUS サーバグループ名を指定してください。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

本コマンドの設定を変更したときは，影響を受ける端末の認証を解除します。

- 装置デフォルトを追加したとき，認証を解除しません。
- 装置デフォルトを変更，または削除したとき，装置デフォルトで認証した端末を認証解除します。
- 認証方式リストを追加したとき，当該認証方式リスト名を設定したポートの端末を認証解除します。
（ポートに設定されている認証方式リストが本コマンドで未設定の場合，装置デフォルトで認証されます。）
- 認証方式リストを変更，または削除したとき，当該認証方式リストで認証した端末を認証解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. 本設定が行われていないと，IEEE802.1X の認証時に RADIUS サーバを使用できません。

[関連コマンド]

aaa authorization network

aaa group server radius

dot1x authentication

dot1x system-auth-control

radius-server host または dot1x radius-server host

aaa authorization network default

認証方式によって設定された VLAN 情報に従って，VLAN 単位認証（動的）を行う場合に設定します。

[入力形式]

情報の設定

aaa authorization network default group radius

情報の削除

no aaa authorization network default

[入力モード]

(config)

[パラメータ]

group radius

RADIUS サーバによる IEEE802.1X 認証を行います。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. 本設定が行われていないと，VLAN 単位認証（動的）を使用できません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan dynamic enable

aaa authentication dot1x

radius-server host または dot1x radius-server host

dot1x authentication

ポート別認証方式の認証方式リスト名を設定します。

[入力形式]

情報の設定・変更

dot1x authentication <List name>

情報の削除

no dot1x authentication

[入力モード]

(config-if)

[パラメータ]

<List name>

aaa authentication dot1x コマンドで設定した認証方式リスト名を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。（ただし，アットマーク (@) を除く）
   先頭文字は大文字を推奨します。

[コマンド省略時の動作]

装置デフォルトを使用して IEEE802.1X 認証を行います。

[通信への影響]

当該認証方式リスト名を変更したポートの端末を認証解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. 本装置に下記コマンドが 1 つでも設定されている場合は，本コマンドを設定できません。
   - dot1x vlan dynamic enable
   - dot1x vlan dynamic radius-vlan
   - web-authentication user-group
   - web-authentication vlan
   - mac-authentication interface
   - mac-authentication vlan
4. 本コマンドで設定した認証方式リスト名が aaa authentication dot1x コマンドで設定した認証方式リスト名と一致しない場合は，装置デフォルトの設定に従い動作します。
5. 本コマンドはイーサネットインタフェースだけ設定可能です。

[関連コマンド]

aaa authentication dot1x

dot1x port-control

dot1x system-auth-control

dot1x auto-logout

no dot1x auto-logout コマンドで，IEEE802.1X で認証された端末から一定時間フレームを受信しなかった状態を検出したときに認証を自動解除する設定を無効にします。

[入力形式]

情報の設定
no dot1x auto-logout

情報の削除
dot1x auto-logout

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

IEEE802.1X で認証された端末から，一定時間フレームを受信しなかった状態を検出したときに自動認証解除します。

[通信への影響]

no dot1x auto-logout コマンド設定後は，IEEE802.1X で認証された端末から，一定時間フレームを受信しなかった状態を検出しても自動認証解除しません。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。

[関連コマンド]

dot1x port-control

dot1x system-auth-control

mac-address-table aging-time

dot1x force-authorized

RADIUS 認証方式を使用時，経路障害などで RADIUS サーバ無応答または RADIUS サーバへのリクエスト送信エラーが発生した場合に，当該ポートで認証要求した認証対象端末を強制的に認証許可状態とします。

[入力形式]

情報の設定

dot1x force-authorized

情報の削除

no dot1x force-authorized

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. 本機能はセキュリティ上の問題となる可能性がありますので，十分検討の上ご使用ください。
4. 本コマンドは次の条件で動作が有効になります。
    - 下記のコンフィグレーションがすべて設定されていること
        - dot1x system-auth-control
        - radius-server host または dot1x radius-server host
        - dot1x force-authorized ※1
        - dot1x port-control auto ※1
        - switchport mode access ※1
        - aaa authentication dot1x ※2
        - dot1x authentication ※3

    注※ 1

    同じインタフェースに設定してください。

    - RADIUS サーバへの送信で，下記のアカウントログが採取された場合
      No.=82

WARNING:SYSTEM: (付加情報) Failed to connect to RADIUS server.
付加情報：IP

アカウントログは，運用コマンド show dot1x logging で確認できます。

注※ 2

装置デフォルトで強制認証使用時は「default group radius」を設定してください。

注※ 3

ポート別認証方式で強制認証使用時は「aaa authentication dot1x <List name>」を設定してください。

5. 強制認証許可状態は，当該端末の認証解除と共に解除されます。
6. 下記のいずれかがすでに設定されている場合，本コマンドを設定できません。
   - authentication force-authorized enable
   - authentication force-authorized vlan

［関連コマンド］

aaa authentication dot1x

dot1x port-control

dot1x system-auth-control

switchport mode

radius-server host または dot1x radius-server host

dot1x force-authorized eapol

IEEE802.1X の強制認証設定によって認証対象端末を強制的に認証許可状態としたとき，認証端末に対して本装置から EAPoL-Success 応答パケットを送信します。

[入力形式]

情報の設定

dot1x force-authorized eapol

情報の削除

no dot1x force-authorized eapol

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. 本コマンドは，下記コマンド設定による強制認証許可時の動作に反映されます。
    - ポート単位認証（静的）: dot1x force-authorized または authentication force-authorized enable
    - ポート単位認証（動的），VLAN 単位認証（動的）: dot1x force-authorized vlan または authentication force-authorized enable

[関連コマンド]

dot1x force-authorized

dot1x force-authorized vlan

authentication force-authorized enable

authentication force-authorized vlan

dot1x force-authorized vlan

RADIUS 認証方式を使用時，経路障害などで RADIUS サーバ無応答または RADIUS サーバへのリクエスト送信エラーが発生した場合に，当該ポートで認証要求した認証対象端末を強制的に認証許可状態とし，認証後 VLAN を割り当てます。

[入力形式]

情報の設定・変更
　dot1x force-authorized vlan <VLAN ID>

情報の削除
　no dot1x force-authorized

[入力モード]

(config-if)

[パラメータ]

<VLAN ID>
　強制認証許可時に割り当てる認証後 VLAN ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。ただし，デフォルト VLAN（VLAN ID=1）は設定できません。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. vlan コマンドで mac-based（MAC VLAN）を設定している VLAN ID を設定してください。
4. 本機能はセキュリティ上の問題となる可能性がありますので，十分検討の上ご使用ください。
5. 本コマンドは次の条件で動作が有効となります。
   - 下記のコンフィグレーションがすべて設定されていること
     - dot1x system-auth-control
     - radius-server host または dot1x radius-server host
     - dot1x port-control auto ※1 ※4
     - aaa authorized network default ※2

- dot1x vlan dynamic enable ※2
- dot1x vlan dynamic radius-vlan ※2※3
- vlan <VLAN ID> mac-based ※3
- switchport mac vlan ※2※3※4
- switchport mode mac-vlan ※4
- dot1x force-authorized vlan ※3※4
- aaa authentication dot1x ※5
- dot1x authentication ※6

注※1
ポート単位認証（動的）で使用するときに設定してください。

注※2
VLAN 単位認証（動的）で使用するときに設定してください。

注※3
同じ VLAN ID を設定してください。

注※4
同じインタフェースに設定してください。

- RADIUS サーバへの送信で，下記のアカウントログが採取された場合
  No.=82
  WARNING:SYSTEM: (付加情報) Failed to connect to RADIUS server.
  付加情報：IP
  アカウントログは，運用コマンド show dot1x logging で確認できます。

注※5
装置デフォルトで強制認証使用時は「default group radius」を設定してください。

注※6
ポート別認証方式で強制認証使用時は「aaa authentication dot1x <List name>」を設定してください。

6. 強制認証許可状態は，当該端末の認証解除とともに解除されます。
7. 下記のいずれかがすでに設定されている場合，本コマンドを設定できません。
   - authentication force-authorized enable
   - authentication force-authorized vlan

[関連コマンド]

aaa authentication dot1x

aaa authorized network default

dot1x port-control

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic radius-vlan

switchport mac

switchport mode

vlan

radius-server host または dot1x radius-server host

dot1x ignore-eapol-start

Supplicant からの EAPOL-Start 受信時に，EAP-Request/Identity を発行しないよう指定します。

[入力形式]

情報の設定
dot1x ignore-eapol-start

情報の削除
no dot1x ignore-eapol-start

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。
4. 本コマンドは dot1x reauthentication コマンドが設定されていて，かつ dot1x supplicant-detection コマンドの disable の設定がないインタフェースにだけ設定できます。
5. dot1x supplicant-detection コマンドの disable を設定したインタフェースでは，本コマンドを設定できません。
6. 本コマンドを設定した場合，no dot1x reauthentication コマンドで再認証を実施しない設定にすることはできません。

[関連コマンド]

dot1x reauthentication

dot1x supplicant-detection

dot1x system-auth-control

dot1x port-control

dot1x max-req

supp-timeout 値を超えた際の EAP-Request 再送の最大回数を指定します。再送回数が本値を超えた場合，認証失敗と判定します。

[入力形式]

情報の設定・変更

dot1x max-req <Counts>

情報の削除

no dot1x max-req

[入力モード]

(config-if)

[パラメータ]

<Counts>

EAP-Request 再送の最大回数を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10（回）

[コマンド省略時の動作]

EAP-Request 再送の最大回数は 2 回です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x timeout supp-timeout

dot1x port-control

dot1x multiple-authentication

IEEE802.1X の認証サブモードを端末認証モードに設定します。端末ごとに認証を行い，認証結果に応じて疎通可否を決定します。複数端末の接続が可能になります。

認証サブモードに端末認証モードが設定されていない場合，認証サブモードはシングルモードになります。シングルモードは，1 台の端末だけを認証し，接続を許可します。複数端末が接続されたときは，設定インタフェースが非認証状態へ移行します。

[入力形式]

情報の設定

dot1x multiple-authentication

情報の削除

no dot1x multiple-authentication

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

認証サブモードはシングルモードになります。

[通信への影響]

認証サブモードを変更した場合，設定インタフェースの認証状態は初期化されるため，認証済み端末は再認証が必要です。再認証されるまで疎通不可状態になります。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドで auto が設定されていないと，本コマンドは有効になりません。
4. 認証サブモードを変更した場合，設定インタフェースの認証状態は初期化されるため，認証済み端末は再認証が必要です。
5. mac-address-table static コマンドで設定された端末の動作は下記となります。
   - 本コマンド未設定（シングルモード）
     認証対象の端末が認証に成功しなければ疎通しません。
   - 本コマンド設定（端末認証モード）
     dot1x port-control コマンドの auto が設定された状態では認証状態にかかわらず常に疎通可能です。

[関連コマンド]

dot1x system-auth-control

dot1x port-control

dot1x port-control

設定インタフェースに対して，port-control 状態の設定を行います。また，このコマンドを入力することで，IEEE802.1X ポート単位認証機能を有効にします。

[入力形式]

情報の設定・変更

dot1x port-control {auto | force-authorized | force-unauthorized}

情報の削除

no dot1x port-control

[入力モード]

(config-if)

[パラメータ]

{auto | force-authorized | force-unauthorized}

auto

IEEE802.1X 認証を行い，認証結果に応じて設定インタフェースに接続される端末の疎通の可否を判定します。

force-authorized

IEEE802.1X 認証を行わないで，設定インタフェースに接続される端末を常に疎通可能とします。ポート単位認証（静的）シングルモードのときだけ設定可能です。

force-unauthorized

IEEE802.1X 認証を行わないで，設定インタフェースに接続される端末を常に疎通不可とします。ポート単位認証（静的）シングルモードのときだけ設定可能です。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   auto，force-authorized，または force-unauthorized

[コマンド省略時の動作]

ポート単位認証機能は無効です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。

3. ポート単位認証（静的）を使用時は，同じインタフェースに下記を設定してください。（イーサネットインタフェース，ポートチャネルインタフェースで設定可能です。）
   - dot1x port-control auto
   - switchport mode access
   - switchport access
4. ポート単位認証（動的）を使用時は，下記を確認してください。
   - system function コマンド設定有で extended-authentication が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
   - 同じインタフェースに下記を設定してください。（イーサネットインタフェースだけ設定可能です。）
     ・dot1x port-control auto
     ・switchport mode mac-vlan
5. 本コマンドは，当該ポートに authentication ip access-group コマンド，または authentication arp-relay コマンドが設定されているとき下記の条件で削除できます。
   - web-authentication port または mac-authentication port 設定状態
6. dot1x multiple-authentication コマンドが設定されていない場合は，認証サブモードはシングルモードになります。

［関連コマンド］

dot1x system-auth-control

dot1x multiple-authentication

switchport mode

switchport access

switchport mac

dot1x radius-server dead-interval

IEEE802.1X 認証専用 RADIUS サーバがプライマリ IEEE802.1X 認証専用 RADIUS サーバへ自動復旧するまでの監視タイマを設定します。

カレントサーバ（運用中の RADIUS 認証要求先）が有効なセカンダリ IEEE802.1X 認証専用 RADIUS サーバへ遷移した時点，または全サーバ使用不可状態で監視タイマをスタートし，本コマンドによる設定時間経過後（監視タイマ満了後）に，プライマリ IEEE802.1X 認証専用 RADIUS サーバへ復旧します。

[入力形式]

情報の設定・変更

dot1x radius-server dead-interval <Minutes>

情報の削除

no dot1x radius-server dead-interval

[入力モード]

(config)

[パラメータ]

<Minutes>

セカンダリ IEEE802.1X 認証専用 RADIUS サーバから，プライマリ IEEE802.1X 認証専用 RADIUS サーバへ自動復旧するまでの監視タイマを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 1440（分）
   0 を設定した場合は，RADIUS 認証要求を必ずプライマリ IEEE802.1X 認証専用 RADIUS サーバから開始します。

[コマンド省略時の動作]

カレントサーバがセカンダリ IEEE802.1X 認証専用 RADIUS サーバへ遷移して 10 分後，プライマリ IEEE802.1X 認証専用 RADIUS サーバに自動復旧します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

1. セカンダリ IEEE802.1X 認証専用 RADIUS サーバをカレントサーバとして運用中に監視タイマ値を変更した場合，その時点での経過状態を判定し結果を反映します。
2. 監視タイマをスタート後に本コマンド設定を削除した場合，監視タイマのカウントはリセットせずに継続し，デフォルト値 10 分として動作します。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと

IEEE802.1X の認証モード」を参照してください。

3. ３台以上の IEEE802.1X 認証専用 RADIUS サーバを設定していた場合，監視タイマをスタート後に他の IEEE802.1X 認証専用 RADIUS サーバへカレントサーバが遷移した場合でも，監視タイマはリセットせずに継続します。
4. 監視タイマはいったんスタートすると基本的に満了するまでリセットしませんが，下記の契機では例外として満了せずにリセットします。
    - 本コマンドで dot1x radius-server dead-interval 0 を設定したとき
    - カレントサーバとして運用中の IEEE802.1X 認証専用 RADIUS サーバ情報を，dot1x radius-server host コマンドで削除したとき
    - 運用コマンド clear radius-server を実行したとき
5. 認証対象端末の認証シーケンス実施中に監視タイマが満了した場合でも，実施中の認証シーケンスが完了するまでプライマリ IEEE802.1X 認証専用 RADIUS サーバへの復旧は行なわれません。

[関連コマンド]

aaa authentication dot1x

dot1x port-control

dot1x system-auth-control

dot1x radius-server host

dot1x radius-server host

IEEE802.1X に使用する汎用 RADIUS サーバの設定を行います。

[入力形式]

情報の設定・変更

dot1x radius-server host <IP address> [auth-port <Port>] [acct-port <Port>] [timeout <Seconds>] [retransmit <Retries>] [key <String>]

情報の削除

no dot1x radius-server host <IP address>

[入力モード]

(config)

[パラメータ]

<IP address>

RADIUS サーバの IPv4 アドレスを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   IPv4 アドレス（ドット記法）を指定します。
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

auth-port <Port>

RADIUS サーバのポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1812 を使用します。
2. 値の設定範囲
   1 ～ 65535

acct-port <Port>

RADIUS サーバのアカウンティング用ポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1813 を使用します。
2. 値の設定範囲
   1 ～ 65535

timeout <Seconds>

RADIUS サーバからの応答タイムアウト時間（秒）を指定します。

1. 本パラメータ省略時の初期値
   radius-server timeout コマンドで設定されている時間が使用されます。設定されていない場合の初期値は 5 秒です。
2. 値の設定範囲
   1 ～ 30（秒）

retransmit <Retries>

RADIUS サーバに対して認証要求を再送信する回数を指定します。

1. 本パラメータ省略時の初期値

radius-server retransmit コマンドで設定されている回数が使用されます。設定されていない場合の初期値は 3 回です。

2. 値の設定範囲
0 ～ 15（回）

key <String>

RADIUS サーバ間との通信の暗号化／認証に使用する RADIUS 鍵を指定します。RADIUS 鍵はクライアント上と RADIUS サーバ上で同一の鍵を設定する必要があります。

1. 本パラメータ省略時の初期値
radius-server key コマンドで設定されている RADIUS 鍵が使用されます。設定されていない場合，当該 RADIUS サーバは無効になります。
2. 値の設定範囲
64 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

radius-server host コマンドで登録した RADIUS サーバの設定が使用されます。

radius-server host コマンドが登録されていない場合は，認証できません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. 本コマンドが設定されている場合，IEEE801.X 認証で参照する RADIUS サーバの設定情報は，radius-server host コマンドで設定されている情報よりも優先されます（radius-server host コマンド設定は適用されません）。汎用 RADIUS サーバ情報，IEEE802.1X 認証専用 RADIUS サーバ情報の設定については，「コンフィグレーションガイド Vol.2」を参照してください。
4. 設定可能な IEEE802.1X 認証専用 RADIUS サーバ数は装置単位で最大 4 です。
5. IPv4 アドレスとして 127.*.*.* を設定できません。
6. key パラメータが省略されていて，radius-server key コマンドも設定されていない場合は，当該 RADIUS サーバは無効になります。
7. 複数の IEEE802.1X 認証専用 RADIUS サーバを設定した場合，運用コマンド show radius-server で最初に表示されるアドレスがプライマリ RADIUS サーバとなります。最初のカレントサーバ（運用中の RADIUS 認証要求先）にはプライマリ IEEE802.1X 認証専用 RADIUS サーバが使用されます。
プライマリ IEEE802.1X 認証専用 RADIUS サーバに障害が発生した場合，カレントサーバは次に有効な IEEE802.1X 認証専用 RADIUS サーバ（セカンダリ RADIUS サーバ）へ遷移します。プライマリ IEEE802.1X 認証専用 RADIUS サーバへの自動復旧については dot1x radius-server dead-interval コマンドを参照してください。
8. 汎用 RADIUS サーバ，他の認証専用 RADIUS サーバまたは RADIUS サーバグループの設定で，IP アドレスの一致する RADIUS サーバが既に登録されている場合は，それらすべてのパラメータを自動的

に新しく入力したコマンド内容に置き換えます。

[関連コマンド]

aaa authentication dot1x

dot1x port-control

dot1x system-auth-control

dot1x reauthentication

IEEE802.1X の認証成功後，Supplicant の再認証を有効にするかどうかを設定します。本設定が有効になると，dot1x timeout reauth-period コマンドで設定する値の周期で再認証用 EAP-Request/Identity を Supplicant に対して送出し，Supplicant の再認証を促します。

[入力形式]

情報の設定

dot1x reauthentication

情報の削除

no dot1x reauthentication

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。
4. dot1x ignore-eapol-start コマンドが設定されていると，no dot1x reauthentication コマンドで再認証を実施しない設定にすることはできません。

[関連コマンド]

dot1x ignore-eapol-start

dot1x timeout reauth-period

dot1x system-auth-control

dot1x port-control

dot1x supplicant-detection

認証サブモードに端末認証モードを設定した時の端末検出動作を指定します。

[入力形式]

情報の設定・変更

dot1x supplicant-detection {disable | shortcut | auto}

情報の削除

no dot1x supplicant-detection

[入力モード]

(config-if)

[パラメータ]

{disable | shortcut | auto}

認証サブモードに端末認証モードを設定した時の端末検出動作を指定します。

disable

当該ポートで検出済みの端末が存在する場合は，EAP-Request/Identity をマルチキャスト送信しません。認証前端末が EAPOL-Start を送信することで認証を開始します。

このため，本パラメータを指定した場合，自発的に EAPOL-Start を送信しない Supplicant ソフトウェアを使用する場合，認証前端末を検出できません。

shortcut

認証済み端末が存在する場合も，EAP-Request/Identity をマルチキャスト送信します。認証前端末がこのフレームを受信し応答することで認証を開始します。

認証済み端末もこのフレームを受信することで再認証を開始します。shortcut では認証済み端末が再認証を開始した場合に認証シーケンスを省略して EAP-Success を即時返すことで負荷を軽減します。

しかし，一部の Supplicant ソフトウェアでは，EAP-Success を即時返す動作を認証失敗とみなします。この結果，本パラメータを指定した場合，認証後すぐに通信が途切れたり，認証後数分から数十分で通信が途切れたり，再認証を繰り返して負荷が上がったりする場合があります。

auto

認証済み端末が存在する場合は，EAP-Request/Identity をマルチキャスト送信しません。その代わり，認証前端末が送信した ARP/IP フレームを受信することで認証前端末を検出し，認証を開始します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   disable，shortcut，auto

[コマンド省略時の動作]

端末検出動作は shortcut になります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。
4. 本コマンドは dot1x multiple-authentication コマンドを設定した場合だけ有効になります。
5. dot1x ignore-eapol-start コマンドを設定したインタフェースで dot1x supplicant-detection コマンドの disable を設定することはできません。

[関連コマンド]

dot1x ignore-eapol-start

dot1x multiple-authentication

dot1x system-auth-control

dot1x port-control

dot1x system-auth-control

IEEE802.1X を有効にします。

[入力形式]

情報の設定

dot1x system-auth-control

情報の削除

no dot1x system-auth-control

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
2. EAPOL フォワーディング機能が設定されている場合は，本コマンドはエラーになり IEEE802.1X は有効になりません。
3. aaa authentication dot1x コマンドが設定されていないと，IEEE802.1X の認証時に RADIUS サーバを使用できません。

[関連コマンド]

l2protocol-tunnel eap

aaa authentication dot1x

dot1x timeout keep-unauth

認証サブモードがシングルモードのインタフェースに 2 台以上の端末が接続された際に，インタフェースの疎通不可状態を保持する時間を秒単位で設定します。認証済端末については，本時間経過後再認証が必要になります。

[入力形式]

情報の設定・変更

dot1x timeout keep-unauth <Seconds>

情報の削除

no dot1x timeout keep-unauth

[入力モード]

(config-if)

[パラメータ]

<Seconds>

認証サブモードがシングルモードのときに，疎通不可状態を保持する時間を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）

[コマンド省略時の動作]

疎通不可状態を保持する時間は 3600 秒です。

[通信への影響]

なし

[設定値の反映契機]

疎通不可状態が発生したとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。
4. 本コマンドの設定値は，認証サブモードがシングルモードのインタフェースにだけ適用されます。

[関連コマンド]

dot1x system-auth-control

dot1x port-control

dot1x multiple-authentication

dot1x timeout quiet-period

IEEE802.1X の認証失敗後の当該インタフェースでの非認証状態保持時間を秒単位で指定します。本時間内は，EAPOL パケットの送出は行わず，かつ，受信 EAPOL パケットを無視し，認証処理を行いません。

[入力形式]

情報の設定・変更

dot1x timeout quiet-period <Seconds>

情報の削除

no dot1x timeout quiet-period

[入力モード]

(config-if)

[パラメータ]

<Seconds>

非認証状態保持時間を秒単位で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535（秒）

[コマンド省略時の動作]

非認証状態保持時間は 60 秒です。

[通信への影響]

なし

[設定値の反映契機]

認証失敗で非認証状態になったとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x port-control

dot1x timeout reauth-period

IEEE802.1X の認証成功後，Supplicant の再認証を行う周期を秒単位で指定します。本値の周期で再認証用 EAP-Request/Identity を Supplicant に対して送出し，Supplicant の再認証を促します。

[入力形式]

情報の設定・変更

dot1x timeout reauth-period <Seconds>

情報の削除

no dot1x timeout reauth-period

[入力モード]

(config-if)

[パラメータ]

<Seconds>

Supplicant の再認証を行う周期を秒単位で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）

[コマンド省略時の動作]

Supplicant の再認証を行う周期は 3600 秒です。

[通信への影響]

なし

[設定値の反映契機]

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき
- 認証済端末が存在しない状態の認証単位で認証端末の認証が成功したとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。
4. 本コマンドは，dot1x reauthentication コマンドによって再認証を行う設定にならないと有効になりません。
5. パラメータの設定値は dot1x timeout tx-period コマンドで設定した値より大きな値を設定してください。

[関連コマンド]

dot1x timeout tx-period

dot1x reauthentication

dot1x system-auth-control

dot1x port-control

dot1x timeout server-timeout

認証サーバとの再送を含めた全体の応答待ち時間を秒単位で指定します。

[入力形式]

情報の設定・変更

dot1x timeout server-timeout <Seconds>

情報の削除

no dot1x timeout server-timeout

[入力モード]

(config-if)

[パラメータ]

<Seconds>

応答待ち時間を秒単位で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）

[コマンド省略時の動作]

応答待ち時間は 30 秒です。

[通信への影響]

なし

[設定値の反映契機]

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 認証処理が開始したとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x port-control

dot1x timeout supp-timeout

Supplicant へ送出する EAP-Request に対して，Supplicant からの応答待ち時間を秒単位で指定します。指定秒応答がない場合，EAP-Request を再送します。

[入力形式]

情報の設定・変更

dot1x timeout supp-timeout <Seconds>

情報の削除

no dot1x timeout supp-timeout

[入力モード]

(config-if)

[パラメータ]

<Seconds>

Supplicant からの応答待ち時間を秒単位で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）

[コマンド省略時の動作]

Supplicant からの応答待ち時間は 30 秒です。

[通信への影響]

なし

[設定値の反映契機]

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 認証処理が開始したとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x max-req

dot1x port-control

dot1x timeout tx-period

IEEE802.1X 有効時の，EAP-Request/Identity の送出間隔を秒単位で指定します。

［入力形式］

情報の設定・変更

dot1x timeout tx-period <Seconds>

情報の削除

no dot1x timeout tx-period

［入力モード］

(config-if)

［パラメータ］

<Seconds>

EAP-Request/Identity の送出間隔を秒単位で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）

［コマンド省略時の動作］

EAP-Request/Identity の送出間隔は 30 秒です。

［通信への影響］

なし

［設定値の反映契機］

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき

［注意事項］

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x port-control コマンドが設定されていないと本コマンドは有効になりません。
4. パラメータの設定値は，dot1x timeout reauth-period コマンドで設定した値より小さな値を設定してください。

［関連コマンド］

dot1x timeout reauth-period

dot1x system-auth-control

dot1x port-control

dot1x vlan dynamic enable

IEEE802.1X VLAN 単位認証（動的）を有効にします。

[入力形式]

情報の設定

dot1x vlan dynamic enable

情報の削除

no dot1x vlan dynamic enable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドを設定する場合, aaa authorization network default group radius コマンドの設定を行わないと有効になりません。
4. 本コマンドが設定されていないと，すべての VLAN 単位認証（動的）機能は，有効になりません。
5. 本装置に下記コマンドが 1 つでも設定されている場合は，本コマンドを設定できません。
    - authentication multi-step
    - dot1x authentication
    - mac-authentication authentication
    - web-authentication authentication
    - web-authentication user-group

[関連コマンド]

dot1x system-auth-control

aaa authorization network default

dot1x vlan dynamic ignore-eapol-start

Supplicant からの EAPOL-Start 受信時に，EAP-Request/Identity を発行しないよう指定します。

[入力形式]

情報の設定

dot1x vlan dynamic ignore-eapol-start

情報の削除

no dot1x vlan dynamic ignore-eapol-start

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
4. 本コマンドは dot1x vlan dynamic reauthentication コマンドが設定されていて，かつ dot1x vlan dynamic supplicant-detection コマンドの disable の設定がないインタフェースにだけ設定できます。
5. dot1x vlan dynamic supplicant-detection コマンドを disable に設定したインタフェースでは，本コマンドを設定できません。
6. 本コマンドを設定した場合，no dot1x vlan dynamic reauthentication コマンドで再認証を実施しないように設定することはできません。

[関連コマンド]

dot1x vlan dynamic reauthentication

dot1x vlan dynamic supplicant-detection

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic max-req

supp-timeout 値を超えた際の EAP-Request 再送の最大回数を指定します。再送回数が本値を超えた場合，認証失敗と判定します。

[入力形式]

情報の設定・変更

dot1x vlan dynamic max-req <Counts>

情報の削除

no dot1x vlan dynamic max-req

[入力モード]

(config)

[パラメータ]

<Counts>

EAP-Request 再送の最大回数を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10（回）

[コマンド省略時の動作]

EAP-Request 再送の最大回数は 2 回です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan dynamic timeout supp-timeout

dot1x vlan dynamic enable

dot1x vlan dynamic radius-vlan

IEEE802.1X の認証時に RADIUS サーバから送信される VLAN 情報によって，動的な VLAN 割り当てを許可する VLAN を指定します。

[入力形式]

情報の設定
dot1x vlan dynamic radius-vlan <VLAN ID list>

情報の変更
dot1x vlan dynamic radius-vlan {<VLAN ID list> | add <VLAN ID list> | remove <VLAN ID list>}

情報の削除
no dot1x vlan dynamic radius-vlan

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。変更時は設定済みの VLAN を指定された VLAN に置き換えます。本装置に未設定の VLAN は指定できません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。ただし，このコマンドでデフォルト VLAN（VLAN ID=1）は指定できません。

add <VLAN ID list>

IEEE802.1X 認証設定を適用する VLAN に追加する VLAN を指定します。本装置に未設定の VLAN は指定できません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。ただし，このコマンドでデフォルト VLAN（VLAN ID=1）は指定できません。

remove <VLAN ID list>

IEEE802.1X 認証設定を適用する VLAN から削除する VLAN を指定します。本装置に未設定の VLAN は指定できません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。ただし，このコマンドでデフォルト VLAN（VLAN ID=1）は指定できません。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
4. パラメータ <VLAN ID list> は，設定済みの MAC VLAN の VLAN ID に限り設定できます。
5. VLAN 単位認証（動的）で設定できる最大 VLAN 数は 256 です。
6. VLAN が範囲指定の場合，すべての VLAN が設定可能でなければエラーになります。
7. 本装置に下記コマンドが 1 つでも設定されている場合は，本コマンドを設定できません。
    - authentication multi-step
    - dot1x authentication
    - mac-authentication authentication
    - web-authentication authentication
    - web-authentication user-group

[関連コマンド]

vlan

dot1x system-auth-control

dot1x vlan dynamic enable

switchport mac

dot1x vlan dynamic reauthentication

IEEE802.1X の認証成功後，Supplicant の再認証を有効にするかどうかを設定します。本設定が有効になると，dot1x vlan dynamic timeout reauth-period コマンドで設定する値の周期で再認証用 EAP-Request/Identity を Supplicant に対して送出し，Supplicant の再認証を促します。

[入力形式]

情報の設定

dot1x vlan dynamic reauthentication

情報の削除

no dot1x vlan dynamic reauthentication

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
4. dot1x vlan dynamic ignore-eapol-start コマンドが設定されていると，no dot1x vlan dynamic reauthentication コマンドで再認証を実施しない設定にすることはできません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan dynamic ignore-eapol-start

dot1x vlan dynamic timeout reauth-period

dot1x vlan dynamic enable

dot1x vlan dynamic supplicant-detection

端末検出動作を指定します。

[入力形式]

情報の設定・変更

dot1x vlan dynamic supplicant-detection {disable | shortcut}

情報の削除

no dot1x vlan dynamic supplicant-detection

[入力モード]

(config)

[パラメータ]

{disable | shortcut}

端末検出動作を指定します。

disable

当該ポートで検出済みの端末が存在する場合は，EAP-Request/Identity をマルチキャスト送信しません。認証前端末が EAPOL-Start を送信することで認証を開始します。

本パラメータを指定した場合，自発的に EAPOL-Start を送信しない Supplicant ソフトウェアを使用する場合，認証前端末を検出できません。

shortcut

認証済み端末が存在する場合も，EAP-Request/Identity をマルチキャスト送信します。認証前端末がこのフレームを受信し応答することで認証を開始します。

認証済み端末もこのフレームを受信することで再認証を開始します。shortcut では認証済み端末が再認証を開始した場合に認証シーケンスを省略して EAP-Success を即時返すことで負荷を軽減します。

しかし，一部の Supplicant ソフトウェアでは，EAP-Success を即時返す動作を認証失敗とみなします。この結果，本パラメータを指定した場合，認証後すぐに通信が途切れたり，認証後数分から数十分で通信が途切れたり，再認証を繰り返して負荷が上がったりする場合があります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   disable，または shortcut

[コマンド省略時の動作]

端末検出動作は shortcut になります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。

2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドとIEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
4. dot1x vlan dynamic ignore-eapol-start コマンドを設定したインタフェースで dot1x vlan dynamic supplicant-detection コマンドの disable を設定することはできません。

［関連コマンド］

dot1x vlan dynamic ignore-eapol-start

dot1x vlan dynamic enable

dot1x system-auth-control

dot1x vlan dynamic timeout quiet-period

IEEE802.1X の認証失敗後の該当インタフェースの非認証状態保持時間を秒単位で指定します。本時間内は，EAPOL パケットの送出は行わず，かつ，受信 EAPOL パケットを無視し，認証処理は行いません。

[入力形式]

情報の設定・変更

dot1x vlan dynamic timeout quiet-period <Seconds>

情報の削除

no dot1x vlan dynamic timeout quiet-period

[入力モード]

(config)

[パラメータ]

<Seconds>

非認証状態保持時間を秒単位で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535（秒）

[コマンド省略時の動作]

非認証状態保持時間は 60 秒です。

[通信への影響]

なし

[設定値の反映契機]

認証失敗による非認証状態になったとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic timeout reauth-period

IEEE802.1X の認証成功後，Supplicant の再認証を行う周期を秒単位で指定します。本値の周期で再認証用 EAP-Request/Identity を Supplicant に対して送出し，Supplicant の再認証を促します。

[入力形式]

情報の設定・変更

dot1x vlan dynamic timeout reauth-period <Seconds>

情報の削除

no dot1x vlan dynamic timeout reauth-period

[入力モード]

(config)

[パラメータ]

<Seconds>

Supplicant の再認証を行う周期を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）

[コマンド省略時の動作]

Supplicant の再認証を行う周期は 3600 秒です。

[通信への影響]

なし

[設定値の反映契機]

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき
- 認証済端末が存在しない状態の認証単位で認証端末の認証が成功したとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
4. 本コマンドは，dot1x vlan dynamic reauthentication コマンドによって再認証を行う設定にならないと有効になりません。
5. パラメータの設定値は dot1x vlan dynamic timeout tx-period コマンドで設定した値より大きな値を設定してください。

[関連コマンド]

dot1x vlan dynamic timeout tx-period

dot1x vlan dynamic reauthentication

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic timeout server-timeout

認証サーバとの再送を含めた全体の応答待ち時間を秒単位で指定します。

[入力形式]

情報の設定・変更

dot1x vlan dynamic timeout server-timeout <Seconds>

情報の削除

no dot1x vlan dynamic timeout server-timeout

[入力モード]

(config)

[パラメータ]

<Seconds>

応答待ち時間を秒単位で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）

[コマンド省略時の動作]

応答待ち時間は 30 秒です。

[通信への影響]

なし

[設定値の反映契機]

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 認証処理が開始したとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは,「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic timeout supp-timeout

Supplicant へ送出する EAP-Request に対して，Supplicant からの応答待ち時間を秒単位で指定します。指定秒応答がない場合，EAP-Request の再送を行います。

[入力形式]

情報の設定・変更

dot1x vlan dynamic timeout supp-timeout <Seconds>

情報の削除

no dot1x vlan dynamic timeout supp-timeout

[入力モード]

(config)

[パラメータ]

<Seconds>

Supplicant からの応答待ち時間を秒単位で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）

[コマンド省略時の動作]

Supplicant からの応答待ち時間は 30 秒です。

[通信への影響]

なし

[設定値の反映契機]

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 認証処理が開始したとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan dynamic max-req

dot1x vlan dynamic enable

dot1x vlan dynamic timeout tx-period

IEEE802.1X の認証有効時の，EAP-Request/Identity の送出間隔を秒単位で指定します。

[入力形式]

情報の設定・変更

dot1x vlan dynamic timeout tx-period <Seconds>

情報の削除

no dot1x vlan dynamic timeout tx-period

[入力モード]

(config)

[パラメータ]

<Seconds>

EAP-Request/Identity の送出間隔を秒単位で指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535（秒）

[コマンド省略時の動作]

EAP-Request/Identity の送出間隔は 30 秒です。

[通信への影響]

なし

[設定値の反映契機]

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき

[注意事項]

1. すべての IEEE802.1X 設定は，dot1x system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 21-1　コンフィグレーションコマンドと IEEE802.1X の認証モード」を参照してください。
3. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
4. パラメータの設定値は，dot1x vlan dynamic timeout reauth-period コマンドで設定した値より小さな値を設定してください。

[関連コマンド]

dot1x system-auth-control

dot1x vlan dynamic timeout reauth-period

dot1x vlan dynamic enable

22 Web 認証【S2200】【SS1250】【SS1240】

コンフィグレーションコマンドと認証モードの対応
aaa accounting web-authentication
aaa authentication web-authentication
aaa authentication web-authentication end-by-reject
http-server initial-timeout
web-authentication authentication
web-authentication auto-logout
web-authentication force-authorized vlan
web-authentication html-fileset
web-authentication ip address
web-authentication jump-url
web-authentication logout ping tos-windows
web-authentication logout ping ttl
web-authentication logout polling count
web-authentication logout polling enable
web-authentication logout polling interval
web-authentication logout polling retry-interval
web-authentication max-timer
web-authentication max-user
web-authentication max-user (interface)
web-authentication prefilter
web-authentication prefilter
web-authentication radius-server dead-interval

web-authentication radius-server host
web-authentication redirect-mode
web-authentication redirect enable
web-authentication redirect ignore-https
web-authentication redirect tcp-port
web-authentication roaming
web-authentication static-vlan force-authorized
web-authentication static-vlan max-user
web-authentication static-vlan max-user (interface)
web-authentication static-vlan roaming
web-authentication system-auth-control
web-authentication user-group
web-authentication user replacement
web-authentication vlan
web-authentication web-port
default-router
dns-server
ip dhcp excluded-address
ip dhcp pool
lease
max-lease
network
service dhcp

コンフィグレーションコマンドと認証モードの対応

Web 認証のコンフィグレーションコマンドが設定できる，Web 認証の認証モードを次の表に示します。

表 22-1　コンフィグレーションコマンドと Web 認証の認証モード

コマンド名	Web 認証の認証モード※3		
	固	ダ	レ
aaa accounting web-authentication	○	○	○
aaa authentication web-authentication	○	○	○
aaa authentication web-authentication end-by-reject	○	○	−
authentication arp-relay※1	○	○	×
authentication ip access-group※1	○	○	×
http-server initial-timeout	○	○	×
web-authentication authentication	○	○	×
web-authentication auto-logout	○	○	○
web-authentication force-authorized vlan	−	○	○
web-authentication html-fileset	○	○	×
web-authentication ip address	○	○	○
web-authentication jump-url	○	○	○
web-authentication logout ping tos-windows	○	○	○
web-authentication logout ping ttl	○	○	○
web-authentication logout polling count	○	−	−
web-authentication logout polling enable	○	−	−
web-authentication logout polling interval	○	−	−
web-authentication logout polling retry-interval	○	−	−
web-authentication max-timer	○	○	○
web-authentication max-user	−	○	○
web-authentication max-user (interface)	−	○	○
web-authentication port※2	○	○	−
web-authentication prefilter	○	○	−
web-authentication radius-server dead-interval	○	○	○
web-authentication radius-server host	○	○	○
web-authentication redirect-mode	○	○	−
web-authentication redirect enable	○	○	−
web-authentication redirect ignore-https	○	○	−
web-authentication redirect tcp-port	○	○	−
web-authentication roaming	−	○	−
web-authentication static-vlan force-authorized	○	−	−
web-authentication static-vlan max-user	○	−	−
web-authentication static-vlan max-user (interface)	○	−	−

コマンド名	Web 認証の認証モード※3		
	固	ダ	レ
web-authentication static-vlan roaming	○	−	−
web-authentication system-auth-control	○	○	○
web-authentication user-group	○	○	×
web-authentication user replacement	○	○	○
web-authentication vlan	−	−	○
web-authentication web-port	○	○	−
default-router	−	○	○
dns-server	−	○	○
ip dhcp excluded-address	−	○	○
ip dhcp pool	−	○	○
lease	−	○	○
max-lease	−	○	○
network	−	○	○
service dhcp	−	○	○

凡例

固：固定 VLAN モード
ダ：ダイナミック VLAN モード
レ：レガシーモード
○：設定内容に従って動作します。
−：コマンドは入力できますが，動作しません。
×：コマンドを入力できません。

注※1

コマンドの入力形式など詳細は，「20　レイヤ 2 認証共通」を参照してください。

注※2

本コマンドの設定は，認証モードの切り替えに影響します。

注※3

認証モードの表記など詳細については，「コンフィグレーションガイド Vol.2」を参照してください。

aaa accounting web-authentication

Web 認証のアカウンティング情報をアカウンティングサーバへ送信します。

[入力形式]

情報の設定

aaa accounting web-authentication default start-stop group radius

情報の削除

no aaa accounting web-authentication default

[入力モード]

(config)

[パラメータ]

default

装置デフォルトのアカウンティング方式を設定します。

start-stop

ログイン時にはスタートアカウンティング通知が，ログアウト時にはストップアカウンティング通知がアカウンティングサーバに送信されます。

group radius

アカウンティングサーバとして RADIUS サーバを使用します。

[コマンド省略時の動作]

アカウンティングサーバに通知しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。

[関連コマンド]

aaa authentication web-authentication

web-authentication system-auth-control

radius-server host または web-authentication radius-server host

aaa authentication web-authentication

Web 認証の認証方式グループを設定します。

先に設定した認証に失敗した場合は，次に設定した方式で認証を行います。なお，この認証失敗時の動作は aaa authentication web-authentication end-by-reject コマンドにより変更できます。

default 指定は 1 エントリ，認証方式リスト指定は最大 4 エントリまで設定できます。

[入力形式]

情報の設定・変更

aaa authentication web-authentication default <Method> [<Method>]
aaa authentication web-authentication <List name> group <Group name>

情報の削除

no aaa authentication web-authentication {default | <List name>}

[入力モード]

(config)

[パラメータ]

default <Method> [<Method>]

装置デフォルトの認証方式を設定します。同一の Method は複数設定できません。
<Method> には group radius または local を設定します。

group radius

RADIUS サーバによる Web 認証を行います。使用する RADIUS サーバは Web 認証専用 RADIUS サーバまたは，汎用 RADIUS サーバです。

local

ローカル認証を行います。内蔵 Web 認証 DB を使用します。

<List name>

認証方式リスト名を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。
   先頭文字は大文字を推奨します。
   ただし，下記の文字列は設定できません。
   ・アットマーク (@)
   ・default(前方一致または完全一致した文字列)
   ・end-by-reject(前方一致または完全一致した文字列)

group <Group Name>

RADIUS サーバによる Web 認証を行います。使用する RADIUS サーバは RADIUS サーバグループです。aaa group server radius コマンドで設定したグループ名を指定してください。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲

32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

RADIUS サーバを使用しないで，内蔵 Web 認証 DB を使用してユーザ認証を行います。

[通信への影響]

装置デフォルトを設定変更したときは，装置デフォルトの認証方式で認証した端末を認証解除します。

認証方式リストを設定変更したときは，当該認証方式リストで認証した端末を認証解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本コマンドを有効にする場合には，RADIUS サーバの認証設定が別途必要になります。
4. Web 認証の強制認証機能は，RADIUS 認証だけ設定された場合に動作します。複数の認証方式を設定した場合は，強制認証は実施されません。

[関連コマンド]

aaa authentication web-authentication end-by-reject

aaa group server radius

radius-server host または web-authentication radius-server host

web-authentication system-auth-control

web-authentication user-group

web-authentication authentication

aaa authentication web-authentication end-by-reject

ログイン時の認証で否認された場合に，認証を終了します。通信不可（RADIUS 無応答など）による認証失敗時は，aaa authentication web-authentication コマンドで次に指定されている認証方式で認証します。

[入力形式]

情報の設定

aaa authentication web-authentication end-by-reject

情報の削除

no aaa authentication web-authentication end-by-reject

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

認証で否認された場合に，その理由にかかわらず aaa authentication web-authentication コマンドで次に指定されている認証方式で認証します。

[通信への影響]

Web 認証機能の端末を認証解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
2. aaa authentication web-authentication コマンドで指定した認証方式にだけ有効です。

[関連コマンド]

aaa authentication web-authentication

http-server initial-timeout

HTTP サーバの初期タイムアウト時間を変更します。

[入力形式]

情報の設定・変更

http-server initial-timeout {<milli seconds> | inherent}

情報の削除

no http-server initial-timeout

[入力モード]

(config)

[パラメータ]

<milli seconds>

HTTP サーバの初期タイムアウト時間をミリ秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   500 ～ 8000 の値で 100 の倍数（ミリ秒）

inherent

認証専用 IP アドレス宛て HTTP ※1/HTTPS ※2 リクエストの初期タイムアウトは 30 秒，他の HTTP ※2/HTTPS リクエストの初期タイムアウトは 8 秒です。

注※ 1：＋ 2 秒程度誤差があります。

注※ 2：＋ 1 秒程度誤差があります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   inherent

[コマンド省略時の動作]

HTTP/HTTPS リクエストの初期タイムアウトは 1 秒です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドの設定は，セキュア Wake on LAN 機能および OAN 機能を含むすべての HTTP/HTTPS リクエストに適用されます。
2. 負荷が高い場合，実際のタイムアウト時間は本コマンドで指定した値より大きくなる可能性があります
3. 初期タイムアウト時間が短すぎる場合，端末の性能によっては，Web 認証が失敗する可能性があります。初期タイムアウト時間の変更後，Web 認証画面が表示されない事象が発生する場合は，初期タイ

ムアウト時間を見直してください。

[関連コマンド]

web-authentication system-auth-control

web-authentication authentication

ポート別認証方式の認証方式リスト名を設定します。

[入力形式]

情報の設定・変更

web-authentication authentication <List name>

情報の削除

no web-authentication authentication

[入力モード]

(config-if)

[パラメータ]

<List name>

aaa authentication web-authentication コマンドで設定した認証方式リスト名を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。(ただし，アットマーク (@) を除く)
   先頭文字は大文字を推奨します。

[コマンド省略時の動作]

装置デフォルトを使用して Web 認証を行います。

[通信への影響]

当該認証方式リスト名を変更したポートの端末を認証解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本装置に下記コマンドが 1 つでも設定されている場合は，本コマンドを設定できません。
   - dot1x vlan dynamic enable
   - dot1x vlan dynamic radius-vlan
   - web-authentication user-group
   - web-authentication vlan
   - mac-authentication interface
   - mac-authentication vlan
4. 本コマンドで設定した認証方式リスト名が aaa authentication web-authentication コマンドで設定した認証方式リスト名と一致しない場合は，装置デフォルトの設定に従って動作します。

5. 本コマンドはイーサネットインタフェースだけ設定可能です。

[関連コマンド]

aaa authentication web-authentication

web-authentication system-auth-control

web-authentication port

web-authentication auto-logout

no web-authentication auto-logout コマンドで，Web 認証で認証された端末から一定時間フレームを受信しなかった状態を検出したときに認証を自動ログアウトする設定を無効にします。

[入力形式]

情報の設定
no web-authentication auto-logout

情報の削除
web-authentication auto-logout

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

Web 認証で認証された端末から，一定時間フレームを受信しなかった状態を検出したときに認証を自動ログアウトします。

[通信への影響]

no web-authentication auto-logout コマンド設定後は，Web 認証で認証された端末から，一定時間フレームを受信しなかった状態を検出しても，認証を自動ログアウトしません。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。

[関連コマンド]

web-authentication system-auth-control

web-authentication port

web-authentication vlan

mac-address-table aging-time

web-authentication force-authorized vlan

RADIUS 認証方式を使用時，経路障害などで RADIUS サーバ無応答または RADIUS サーバへのリクエスト送信エラーが発生した場合に，当該ポートで認証要求した認証対象端末を強制的に認証許可状態とし，認証後 VLAN を割り当てます。

[入力形式]

情報の設定・変更

web-authentication force-authorized vlan <VLAN ID> [action trap]

情報の削除

no web-authentication force-authorized vlan

[入力モード]

(config-if)

[パラメータ]

<VLAN ID>

強制認証による認証許可時に，割り当てる認証後 VLAN ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。
   ただし，デフォルト VLAN（VLAN ID ＝ 1）は設定できません。

[action trap]

強制認証による認証許可時に，プライベート Trap を発行します。

1. 本パラメータ省略時の初期値
   強制認証により認証許可しても，プライベート Trap を発行しません。
2. 値の設定範囲
   action trap

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. vlan コマンドで mac-based（MAC VLAN）を設定している VLAN ID を設定してください。
4. 本機能はセキュリティ上の問題となる可能性がありますので，十分検討の上ご使用ください。

5. 本コマンドは次の条件で有効となります。
   - 下記のコンフィグレーションがすべて設定されていること
     - radius-server host または web-authentication radius-server host
     - web-authentication system-auth-control
     - web-authentication port ※1※4
     - web-authentication vlan ※2※3
     - vlan <VLAN ID> mac-based ※3
     - web-authentication force-authorized vlan ※3※4
     - switchport mac vlan ※2※3※4
     - switchport mode mac-vlan ※4
     - aaa authentication web-authentication ※5
     - web-authentication authentication ※6

   注※1

   ダイナミック VLAN モードで使用するときに設定してください。

   注※2

   レガシーモードで使用するときに設定してください。

   注※3

   同じ VLAN ID を設定してください。

   注※4

   同じイーサネットポートに設定してください。
   - RADIUS サーバへの送信で，下記のアカウントログが採取された場合
     No=21:

     NOTICE:LOGIN:(付加情報) Login failed ; Failed to connection to RADIUS server.

     付加情報：MAC，USER，IP，PORT または CHGR，VLAN

     アカウントログは運用コマンド show web-authentication logging で確認できます。

   注※5

   装置デフォルトで強制認証使用時は「default group radius」だけ設定してください。

   注※6

   ポート別認証方式で強制認証使用時は「aaa authentication web-authentication <List name>」を設定してください。
6. 強制認証許可状態は，当該ユーザのログアウトで解除されます。
7. プライベート Trap を発行する場合は，snmp-server host コマンドで Trap の送信先 IP アドレスと "web-authentication" を設定しておく必要があります。
8. 下記のいずれかがすでに設定されている場合，本コマンドを設定できません。
   - authentication force-authorized enable
   - authentication force-authorized vlan

[関連コマンド]

aaa authentication web-authentication

radius-server host または web-authentication radius-server host

switchport mac

switchport mode

vlan

web-authentication port

web-authentication system-auth-control

web-authentication vlan

web-authentication html-fileset

ポートごとに表示する個別 Web 認証画面のカスタムファイル名を設定します。

[入力形式]

情報の設定・変更

web-authentication html-fileset <Name>

情報の削除

no web-authentication html-fileset

[入力モード]

(config-if)

[パラメータ]

<Name>

運用コマンド set web-authentication html-files で本装置に登録したカスタムファイルセット名を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   16 文字以内の文字列で指定してください。指定可能な文字は，英数字（大文字）です。

[コマンド省略時の動作]

ログイン時に基本 Web 認証画面を表示します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本コマンドを設定する場合，あらかじめ該当ポートに web-authentication port コマンドを設定してください。
4. 本コマンドはイーサネットインタフェースだけ設定可能です。

[関連コマンド]

web-authentication port

web-authentication system-auth-control

web-authentication ip address

Web 認証専用の IP アドレスとドメイン名を設定します。本コマンドで設定した専用 IP アドレスによって，認証前端末からのログイン操作，認証後端末のログアウト操作を装置内同一 IP アドレスで操作できます。

[入力形式]

情報の設定・変更

web-authentication ip address <IP address> [fqdn <FQDN>]

情報の削除

no web-authentication ip address

[入力モード]

(config)

[パラメータ]

<IP address>

Web 認証専用の IP アドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   IPv4 アドレス（ドット記法）を設定します。
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   本装置に設定された VLAN インタフェースと重複しないサブネットの IP アドレス

fqdn <FQDN>

ドメイン名を FQDN（Fully Qualified Domain Name : 完全修飾ドメイン名）で指定します。

1. 本パラメータ省略時の初期値
   <IP address> だけを使用します。
2. 値の設定範囲
   1 ～ 255 文字の文字列で指定してください。 1 文字目は英数字， 2 文字目以降は，英数字， ピリオド（.）およびハイフン（-）です。

   （これ以外の文字も入力可能ですが，上記範囲で設定してください）

[コマンド省略時の動作]

認証前 VLAN の IP アドレスで動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。

2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. system function コマンド設定有で extended-authentication が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
4. 本コマンドで設定した IP アドレスは，装置内での Web 認証アクセス専用として使用されるため，装置外には送信されません。
5. 本設定を使用する場合，認証前 VLAN に必ず IP アドレスを設定してください。
6. 固定 VLAN モード，ダイナミック VLAN モードのポートで Web 認証専用 IP アドレスを使用する場合は，必ず authentication arp-relay を設定してください。
7. 本コマンドの設定および削除後は，認証途中のユーザは再度ログイン操作を行ってください。

［関連コマンド］

web-authentication system-auth-control

web-authentication port

authentication arp-relay

web-authentication jump-url

認証成功画面表示後，自動的に表示する URL と URL 移動までの時間を設定します。

[入力形式]

情報の設定・変更
web-authentication jump-url <URL> [delay <Seconds>]

情報の削除
no web-authentication jump-url

[入力モード]
(config)

[パラメータ]

<URL>

認証成功画面表示後，指定された URL の画面を表示します。
URL の入力は先頭文字（例えば，"http:// ～ "）から設定してください。（下記の（設定例）を参照してください。）

1. 本パラメータ省略時の初期値
省略できません。
2. 値の設定範囲
1 ～ 256 文字の文字列をダブルクォート（"）で囲んで設定します。入力可能な文字は「パラメータに指定できる値」の「任意の文字列」を参照してください。
（設定例）
(config)# web-authentication jump-url "http://www.example.com/"

[delay <Seconds>]

設定した <URL> に移動するまでの時間を指定します。（下記の（設定例）を参照してください。）

1. 本パラメータ省略時の初期値
5 秒後に設定した <URL> に移動します。
2. 値の設定範囲
0 ～ 60 （秒）
（設定例）
(config)# web-authentication jump-url "http://www.example.com/" delay 20

[コマンド省略時の動作]

認証成功後は，自動表示 URL 未設定のため認証成功画面だけ表示します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。

2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 運用コマンド set web-authentication html-files で認証成功画面を入れ替える際，入れ替える認証成功画面ファイル（loginOK.html）上に認証成功後のジャンプ先 URL のタグ（<!-- Redirect_URL -->）と本コマンドの設定内容を記述すると，認証成功後に設定した URL へ自動的にアクセスされます。
4. 固定 VLAN モードで使用する場合，URL 移動までの時間を設定は不要ですが，省略時の値よりも短い時間で URL を自動表示させたいときは設定してください。
5. ダイナミック VLAN モードまたはレガシーモードで使用する場合，認証前 VLAN から認証後 VLAN への切り替えで，認証端末の IP アドレス変更が必要となるため，URL 移動までの時間を約 20 〜 30 秒程度で設定してください。
   - 装置内蔵 DHCP サーバで認証前の端末に IP アドレス配布している場合 (デフォルトリース時間 10 秒) は，認証後 VLAN で正規 DHCP サーバから IP アドレスを取得します。このため，認証完了時点から，認証後 VLAN 通信が可能になるまで，約 20 〜 30 秒程度かかる場合があります。

[関連コマンド]

web-authentication system-auth-control

web-authentication port

web-authentication vlan

web-authentication logout ping tos-windows

認証済み端末をログアウトする特殊フレームの TOS 値を設定します。

[入力形式]

情報の設定・変更
web-authentication logout ping tos-windows <TOS>

情報の削除
no web-authentication logout ping tos-windows

[入力モード]

(config)

[パラメータ]

<TOS>

ログアウト用特殊フレームの TOS 値を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 〜 255

[コマンド省略時の動作]

特殊フレームの TOS 値は 1 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 下記の条件をすべて満たした ping フレームを受信した場合に，認証済み端末をログアウトします。
   - 認証済み端末から Web 認証専用 IP アドレス宛に送信された ping フレームであること
   - ping フレームの TTL 値が web-authentication logout ping ttl コマンドで設定した TTL 値と一致していること
   - ping フレームの TOS 値が本コマンドで設定した TOS 値と一致していること

[関連コマンド]

web-authentication system-auth-control

web-authentication logout ping ttl

web-authentication logout ping ttl

認証済み端末をログアウトする特殊フレームの TTL 値を設定します。

[入力形式]

情報の設定・変更

web-authentication logout ping ttl <TTL>

情報の削除

no web-authentication logout ping ttl

[入力モード]

(config)

[パラメータ]

<TTL>

ログアウト用特殊フレームの TTL 値を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 255

[コマンド省略時の動作]

特殊フレームの TTL 値は 1 で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 下記の条件をすべて満たした ping フレームを受信した場合に，認証済み端末をログアウトします。
   - 認証済み端末から Web 認証専用 IP アドレス宛に送信された ping フレームであること
   - ping フレームの TTL 値が本コマンドで設定した TTL 値と一致していること
   - ping フレームの TOS 値が web-authentication logout ping tos-windows コマンドで設定した TOS 値と一致していること

[関連コマンド]

web-authentication system-auth-control

web-authentication logout ping tos-windows

web-authentication logout polling count

認証済み端末の接続状態を周期的にチェックする監視用フレームの応答で，無応答を検出時に再送する送信回数を設定します。

[入力形式]

情報の設定・変更

web-authentication logout polling count <Count>

情報の削除

no web-authentication logout polling count

[入力モード]

(config)

[パラメータ]

<Count>

監視用フレームに対する無応答検出時の再送回数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 〜 10 (回)

[コマンド省略時の動作]

監視用フレームの再送を最大３回まで実施します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，次の無応答検出時から運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 認証済み端末の接続監視機能による周期監視より先に，監視対象端末のポートがリンクダウンした場合は対象端末の監視を停止し，ポートリンクダウンによるログアウトを実施します。
4. 最大接続時間（web-authentication max-timer コマンド）の設定時間に達した場合，対象端末の監視を停止しログアウトを実施します。
5. 無応答検出時の再送回数を最大に設定した場合，未接続状態を検出すると認証済みユーザ数に比例して監視用フレームの送信が多くなるため，装置に負荷を掛けることになります。
   ポーリング間隔の目安として，次に示す条件で設定してください。
   < ポーリング条件 >
   （1）ポーリング間隔＞（2）再送間隔×（3）再送回数
   （1）: web-authentication logout polling interval
   （2）: web-authentication logout polling retry-interval

（3）：web-authentication logout polling count
再送回数の設定はデフォルト値を推奨します。
再送回数を大きな値に設定した場合，再送の頻度によりポーリング間隔／再送間隔のずれが大きくなる場合があります。

［関連コマンド］

web-authentication system-auth-control

web-authentication max-timer

web-authentication port

web-authentication logout polling enable

web-authentication logout polling interval

web-authentication logout polling retry-interval

web-authentication logout polling enable

no web-authentication logout polling enable コマンドで，一定周期による接続監視で認証済み端末の未接続を検出したときの自動ログアウトを無効に設定します。

[入力形式]

情報の設定
　no web-authentication logout polling enable

情報の削除
　web-authentication logout polling enable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

認証済み端末に対して下記に示す条件で接続監視を行い，未接続を検出したときに，該当端末を自動ログアウトします。

- ポーリング間隔
  web-authentication logout polling interval コマンドで設定した間隔。未設定時は 300 秒。
- 再送間隔
  web-authentication logout polling retry-interval コマンド で設定した間隔。未設定時は 1 秒。
- 再送回数
  web-authentication logout polling count コマンドで設定した回数。未設定時は 3 回。

[通信への影響]

no web-authentication logout polling enable コマンド設定後は，一定周期による接続監視をしませんので，端末が未接続になっても自動でログアウトされません。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 認証済み端末の接続監視機能による周期監視より先に，監視対象端末のポートがリンクダウンした場合は対象端末の監視を停止し，ポートリンクダウンによるログアウトを実施します。
4. 最大接続時間（web-authentication max-timer コマンド）の設定時間に達した場合，対象端末の監視を停止しログアウトを実施します。
5. ポーリング間隔の時間（web-authentication logout polling interval コマンド）は，対象の認証済み端末から ARP Reply を受信した時間から，次のポーリング監視までの時間となります。
6. 無応答検出時の再送回数を最大に設定した場合，未接続状態を検出すると認証済みユーザ数に比例して

監視用フレームの送信が多くなるため，装置に負荷を掛けることになります。
ポーリング間隔の目安として，次に示す条件で設定してください。
< ポーリング条件 >
（1）ポーリング間隔＞（2）再送間隔×（3）再送回数
（1）: web-authentication logout polling interval
（2）: web-authentication logout polling retry-interval
（3）: web-authentication logout polling count
再送回数の設定はデフォルト値を推奨します。
再送回数を大きな値に設定した場合，再送の頻度によりポーリング間隔／再送間隔のずれが大きくなる場合があります。

[関連コマンド]

web-authentication system-auth-control

web-authentication max-timer

web-authentication port

web-authentication logout polling count

web-authentication logout polling interval

web-authentication logout polling retry-interval

web-authentication logout polling interval

認証済み端末の接続状態を周期的に監視する，監視用フレームのポーリング間隔を設定します。

[入力形式]

情報の設定・変更
　web-authentication logout polling interval <Seconds>

情報の削除
　no web-authentication logout polling interval

[入力モード]

(config)

[パラメータ]

<Seconds>
　監視用フレームのポーリング間隔を設定します。
1. 本パラメータ省略時の初期値
　省略できません。
2. 値の設定範囲
　60 ～ 86400（秒）

[コマンド省略時の動作]

周期的監視による自動ログアウトコマンド（web-authentication logout polling enable コマンド）が設定済みの場合だけ，認証済み端末に対して監視用フレームが 300 秒周期で送信されます。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，次のポーリング間隔から運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 認証済み端末の接続監視機能による周期監視より先に，監視対象端末のポートがリンクダウンした場合は対象端末の監視を停止し，ポートリンクダウンによるログアウトを実施します。
4. 最大接続時間（web-authentication max-timer コマンド）の設定時間に達した場合，当該端末の監視を停止しログアウトを実施します。
5. ポーリング間隔の時間は，対象の認証済み端末から ARP Reply を受信した時間から，次のポーリング監視までの時間となります。
6. 無応答検出時の再送回数を最大に設定した場合，未接続状態を検出すると認証済みユーザ数に比例して監視用フレームの送信が多くなるため，装置に負荷を掛けることになります。
　ポーリング間隔の目安として，次に示す条件で設定してください。
　< ポーリング条件 >
　（1）ポーリング間隔＞（2）再送間隔×（3）再送回数

（1）：web-authentication logout polling interval
（2）：web-authentication logout polling retry-interval
（3）：web-authentication logout polling count
再送回数の設定はデフォルト値を推奨します。
再送回数を大きな値に設定した場合，再送の頻度によりポーリング間隔／再送間隔のずれが大きくなる場合があります。

［関連コマンド］

web-authentication system-auth-control

web-authentication max-timer

web-authentication port

web-authentication logout polling count

web-authentication logout polling enable

web-authentication logout polling retry-interval

web-authentication logout polling retry-interval

認証済み端末の接続状態を周期的に監視する監視用フレームの応答で，無応答検出時に再送する送信間隔を設定します。

[入力形式]

情報の設定・変更

web-authentication logout polling retry-interval <Seconds>

情報の削除

no web-authentication logout polling retry-interval

[入力モード]

(config)

[パラメータ]

<Seconds>

監視用フレームの再送間隔を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10（秒）

[コマンド省略時の動作]

監視フレームの再送間隔は 1 秒間隔となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，次の送信間隔から運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 認証済み端末の接続監視機能による周期監視より先に，監視対象端末のポートがリンクダウンした場合は対象端末の監視を停止し，ポートリンクダウンによるログアウトを実施します。
4. 最大接続時間（web-authentication max-timer コマンド）の設定時間に達した場合，当該端末の監視を停止しログアウトを実施します。
5. 無応答検出時の再送回数を最大に設定した場合，未接続状態を検出すると認証済みユーザ数に比例して監視用フレームの送信が多くなるため，装置に負荷を掛けることになります。
   ポーリング間隔の目安として，次に示す条件で設定してください。
   < ポーリング条件 >
   （1）ポーリング間隔＞（2）再送間隔×（3）再送回数
   （1）: web-authentication logout polling interval
   （2）: web-authentication logout polling retry-interval

（3）：web-authentication logout polling count
再送回数の設定はデフォルト値を推奨します。
再送回数を大きな値に設定した場合，再送の頻度によりポーリング間隔／再送間隔のずれが大きくなる場合があります。

［関連コマンド］

web-authentication system-auth-control

web-authentication max-timer

web-authentication port

web-authentication logout polling count

web-authentication logout polling enable

web-authentication logout polling interval

web-authentication max-timer

最大接続時間を設定します。

[入力形式]

情報の設定・変更
　web-authentication max-timer { <Minutes> | infinity }

情報の削除
　no web-authentication max-timer

[入力モード]

(config)

[パラメータ]

{ <Minutes> | infinity }
　認証済みユーザの最大接続時間を分単位で設定します。ユーザがログインしてから，本コマンドの設定時間が経過した場合には，自動ログアウトされます。
　「infinity」と設定した場合は，最大接続時間は無限となります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   10 ～ 1440（分），または infinity

[コマンド省略時の動作]

最大接続時間は 60 分に設定されます。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 最大接続時間を短縮または延長した場合には，現在認証中のユーザは前設定を有効とし，次回ログイン時から設定値が有効になります。
4. Web 認証での接続時間は，装置の時刻を使用していません。そのため，運用コマンド set clock で日時を変更しても接続時間に影響は出ません。

[関連コマンド]

web-authentication system-auth-control

web-authentication vlan

web-authentication auto-logout

web-authentication port

web-authentication max-user

装置単位の最大認証ユーザ数を設定します。

[入力形式]

情報の設定・変更

web-authentication max-user <Count>

情報の削除

no web-authentication max-user

[入力モード]

(config)

[パラメータ]

<Count>

ユーザ認証を行う装置単位の最大認証ユーザ数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 256

[コマンド省略時の動作]

装置単位で認証可能な最大認証ユーザ数は，256 ユーザになります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本設定を行った場合，現在認証中のユーザはそのままですが，次回ログイン時から設定値が有効となります。
4. 装置単位とポート単位の最大認証ユーザ数を同時に設定することも可能です。
   - 認証済みユーザ数がポート単位の最大認証ユーザ数に達した場合，当該ポートで以降の新規ユーザの認証はできません。
   - 認証済みユーザ数が装置単位の最大認証ユーザ数に達した場合，本装置で以降の新規ユーザの認証はできません。
5. 運用中に認証済みユーザ数より最大認証ユーザ数を少なく変更した場合，認証済みのユーザは継続通信できますが，新規ユーザの認証はできません。
6. DHCP snooping 機能を併用している場合は，最大 246 ユーザに制限されます。

[関連コマンド]

web-authentication system-auth-control

web-authentication port

web-authentication vlan

web-authentication auto-logout

web-authentication max-user (interface)

当該ポートの最大認証ユーザ数を設定します。

[入力形式]

情報の設定・変更

web-authentication max-user <Count>

情報の削除

no web-authentication max-user

[入力モード]

(config-if)

[パラメータ]

<Count>

ユーザ認証を行う当該ポートの最大認証ユーザ数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 256

[コマンド省略時の動作]

当該ポートで認証可能な最大認証ユーザ数は，256 ユーザになります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本設定を行った場合，現在認証中のユーザはそのままですが，次回ログイン時から設定値が有効となります。
4. 装置単位とポート単位の最大認証ユーザ数を同時に設定することも可能です。
   - 認証済みユーザ数がポート単位の最大認証ユーザ数に達した場合，当該ポートで以降の新規ユーザの認証はできません。
   - 認証済みユーザ数が装置単位の最大認証ユーザ数に達した場合，本装置で以降の新規ユーザの認証はできません。
5. 運用中に認証済みユーザ数より最大認証ユーザ数を少なく変更した場合，認証済みのユーザは継続通信できますが，新規ユーザの認証はできません。
6. DHCP snooping 機能を併用している場合は，最大 246 ユーザに制限されます。

[関連コマンド]

web-authentication system-auth-control

web-authentication port

web-authentication vlan

web-authentication auto-logout

web-authentication port

ポートに認証モードを設定します。

[入力形式]

情報の設定
web-authentication port

情報の削除
no web-authentication port

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

Web 認証有効時，当該ポートはレガシーモードで動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. system function コマンド設定有で extended-authentication が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
4. 本コマンドはイーサネットインタフェースだけ設定可能です。

[関連コマンド]

web-authentication html-fileset

web-authentication system-auth-control

authentication ip access-group

authentication arp-relay

web-authentication prefilter

no web-authentication prefilter コマンドで，Web 認証プレフィルタを無効に設定します。

[入力形式]

情報の設定
no web-authentication prefilter

情報の削除
web-authentication prefilter

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

Web 認証プレフィルタが有効となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。

[関連コマンド]

web-authentication system-auth-control

web-authentication radius-server dead-interval

Web 認証専用 RADIUS サーバがプライマリ Web 認証専用 RADIUS サーバへ自動復旧するまでの監視タイマを設定します。

カレントサーバ（運用中の RADIUS 認証要求先）が有効なセカンダリ Web 認証専用 RADIUS サーバへ遷移した時点，または全サーバ使用不可状態で監視タイマをスタートし，本コマンドによる設定時間経過後（監視タイマ満了後）に，プライマリ Web 認証専用 RADIUS サーバへ復旧します。

[入力形式]

情報の設定・変更

web-authentication radius-server dead-interval <Minutes>

情報の削除

no web-authentication radius-server dead-interval

[入力モード]

(config)

[パラメータ]

<Minutes>

セカンダリ Web 認証専用 RADIUS サーバから，プライマリ Web 認証専用 RADIUS サーバへ自動復旧するまでの監視タイマを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 1440（分）
   0 を設定した場合は，RADIUS 認証要求を必ずプライマリ Web 認証専用 RADIUS サーバから開始します。

[コマンド省略時の動作]

カレントサーバがセカンダリ Web 認証専用 RADIUS サーバへ遷移して 10 分後，プライマリ Web 認証専用 RADIUS サーバに自動復旧します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

1. セカンダリ Web 認証専用 RADIUS サーバをカレントサーバとして運用中に監視タイマ値を変更した場合，その時点での経過状態を判定し結果を反映します。
2. 監視タイマをスタート後に本コマンド設定を削除した場合，監視タイマのカウントはリセットせずに継続し，デフォルト値 10 分として動作します。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。

2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. ３台以上の Web 認証専用 RADIUS サーバを設定していた場合，監視タイマをスタート後に他の Web 認証専用 RADIUS サーバへカレントサーバが遷移した場合でも，監視タイマはリセットせずに継続します。
4. 監視タイマはいったんスタートすると基本的に満了するまでリセットしませんが，下記の契機では例外として満了せずにリセットします。
   - 本コマンドで web-authentication dead-interval 0 を設定したとき
   - カレントサーバとして運用中の Web 認証専用 RADIUS サーバ情報を，web-authentication radius-server host コマンドで削除したとき
   - 運用コマンド clear radius-server を実行したとき
5. 認証対象端末の認証シーケンス実施中に監視タイマが満了した場合でも，実施中の認証シーケンスが完了するまでプライマリ Web 認証専用 RADIUS サーバへの復旧は行なわれません。

[関連コマンド]

aaa authentication web-authentication

web-authentication port

web-authentication system-auth-control

web-authentication radius-server host

web-authentication radius-server host

Web 認証に使用する RADIUS サーバの設定を行います。

[入力形式]

情報の設定・変更

web-authentication radius-server host <IP address> [auth-port <Port>] [acct-port <Port>] [timeout <Seconds>] [retransmit <Retries>] [key <String>]

情報の削除

no web-authentication radius-server host <IP address>

[入力モード]

(config)

[パラメータ]

<IP address>

RADIUS サーバの IPv4 アドレスを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   IPv4 アドレス（ドット記法）を指定します。
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

auth-port <Port>

RADIUS サーバのポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1812 を使用します。
2. 値の設定範囲
   1 ～ 65535

acct-port <Port>

RADIUS サーバのアカウンティング用ポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1813 を使用します。
2. 値の設定範囲
   1 ～ 65535

timeout <Seconds>

RADIUS サーバからの応答タイムアウト時間（秒）を指定します。

1. 本パラメータ省略時の初期値
   radius-server timeout コマンドで設定されている時間が使用されます。設定されていない場合の初期値は 5 秒です。
2. 値の設定範囲
   1 ～ 30（秒）

retransmit <Retries>

RADIUS サーバに対して認証要求を再送信する回数を指定します。

1. 本パラメータ省略時の初期値

radius-server retransmit コマンドで設定されている回数が使用されます。設定されていない場合の初期値は 3 回です。
2. 値の設定範囲
0 ～ 15（回）

key <String>

RADIUS サーバ間との通信の暗号化／認証に使用する RADIUS 鍵を指定します。RADIUS 鍵はクライアント上と RADIUS サーバ上で同一の鍵を設定する必要があります。

1. 本パラメータ省略時の初期値
radius-server key コマンドで設定されている RADIUS 鍵が使用されます。設定されていない場合，当該 RADIUS サーバは無効になります。
2. 値の設定範囲
64 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

radius-server host コマンドで登録した RADIUS サーバの設定が使用されます。

radius-server host コマンドが登録されていない場合は，RADIUS サーバを使用しないで，内蔵 Web 認証 DB を使用してユーザ認証を行います。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本コマンドが設定されている場合，Web 認証で参照する RADIUS サーバの設定情報は，radius-server host コマンドで設定されている情報よりも優先されます。（radius-server host コマンド設定は適用されません）。汎用 RADIUS サーバ情報，Web 認証専用 RADIUS サーバ情報の設定については，「コンフィグレーションガイド Vol.2」を参照してください。
4. 設定可能な Web 認証専用 RADIUS サーバ数は装置単位で最大 4 です。
5. IPv4 アドレスとして 127.*.*.* を設定できません。
6. key パラメータが省略されていて，radius-server key コマンドも設定されていない場合は，当該 RADIUS サーバは無効になります。
7. 複数の Web 認証専用 RADIUS サーバを設定した場合，運用コマンド show radius-server で最初に表示されるアドレスがプライマリ Web 認証専用 RADIUS サーバとなります。最初のカレントサーバ（運用中の RADIUS 認証要求先）にはプライマリ Web 認証専用 RADIUS サーバが使用されます。
プライマリ Web 認証専用 RADIUS サーバに障害が発生した場合，カレントサーバは次に有効な Web 認証専用 RADIUS サーバ（セカンダリ RADIUS サーバ）へ遷移します。プライマリ Web 認証専用 RADIUS サーバへの自動復旧については web-authentication radius-server dead-interval コマンドを参照してください。

8. 汎用 RADIUS サーバ，他の認証専用 RADIUS サーバ，または RADIUS サーバグループの設定で，IP アドレスの一致する RADIUS サーバが既に登録されている場合は，それらすべてのパラメータを自動的に新しく入力したコマンド内容に置き換えます。

［関連コマンド］

aaa authentication web-authentication

web-authentication port

web-authentication system-auth-control

web-authentication redirect-mode

URL リダイレクト機能有効時，Web 認証のログイン画面を表示させるプロトコルを設定します。

［入力形式］

情報の設定・変更

web-authentication redirect-mode {http | https}

情報の削除

no web-authentication redirect-mode

［入力モード］

(config)

［パラメータ］

{ http | https }

URL リダイレクト機能有効時，Web 認証のログイン画面を表示させるプロトコルの設定を行います。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   http ：http によるログイン画面が表示されます。
   https：https によるログイン画面が表示されます。

［コマンド省略時の動作］

https によるログイン画面が表示されます。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本コマンドは，no web-authentication redirect enable コマンドが設定されている場合は無効となります。

［関連コマンド］

web-authentication system-auth-control

web-authentication port

web-authentication redirect enable

web-authentication redirect enable

no web-authentication redirect enable コマンドで，URL リダイレクト機能を無効に設定します。

[入力形式]

情報の設定

no web-authentication redirect enable

情報の削除

web-authentication redirect enable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

URL リダイレクト機能が有効となります。

[通信への影響]

no web-authentication redirect enable コマンドを設定後は，URL リダイクレト機能は動作しません。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。

[関連コマンド]

web-authentication system-auth-control

web-authentication port

authentication ip access-group

authentication arp-relay

web-authentication redirect ignore-https

HTTPS リクエストに対する URL リダイレクトを抑止します。

[入力形式]

情報の設定
　web-authentication redirect ignore-https

情報の削除
　no web-authentication redirect ignore-https

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

HTTPS リクエストに対する URL リダイレクトを抑止しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

web-authentication system-auth-control

web-authentication redirect tcp-port

URL リダイレクト機能有効時，本装置で URL リダイレクト対象とするフレームの TCP 宛先ポート番号を追加設定します。

通常，http ＝ 80 の番号で割り当てられているポート番号に，任意のポート番号を 1 件追加指定できます。

[入力形式]

情報の設定・変更

web-authentication redirect tcp-port <Port>

情報の削除

no web-authentication redirect tcp-port

[入力モード]

(config)

[パラメータ]

<Port>

URL リダイレクト機能有効時，本装置で URL リダイレクト対象とする TCP 宛先ポート番号を追加設定します。TCP 宛先ポート番号 80 と本コマンドで設定したポート番号が http プロトコルの URL リダイレクト対象となります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535

[コマンド省略時の動作]

次に示す初期値のポート番号のフレームが URL リダイレクト対象となります。

- http:80
- https:443

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本コマンドで設定可能な TCP 宛先ポート番号は 1 件です。
4. 本コマンドで https プロトコルをリダイレクト対象とするポート番号を追加することはできません。
5. 本コマンドは，web-authentication web-port コマンドと同一動作です。

　２つのコマンドで異なるポート番号を指定した場合，それぞれの指定が有効となります。
また，２つのコマンドで同一ポート番号を指定した場合の扱いを次に示します。

<table>
<tr><th colspan="2" rowspan="2"></th><th rowspan="2">web-authentication redirect tcp-port</th><th colspan="2">web-authentication web-port</th></tr>
<tr><th>http</th><th>https</th></tr>
<tr><td colspan="2">web-authentication redirect tcp-port</td><td></td><td>http としてリダイレクト</td><td>http としてリダイレクト (https 指定のポート番号は無視)</td></tr>
<tr><td rowspan="2">web-authentication web-port</td><td>http</td><td>http としてリダイレクト</td><td></td><td>先に入力したコマンド設定が有効</td></tr>
<tr><td>https</td><td>http としてリダイレクト (https 指定のポート番号は無視)</td><td>先に入力したコマンド設定が有効</td><td></td></tr>
</table>

[関連コマンド]

web-authentication system-auth-control

web-authentication port

authentication ip access-group

authentication arp-relay

web-authentication web-port

web-authentication roaming

HUB などを経由して接続した認証済み端末を，リンクダウンしないでポート移動した場合の通信許可（ローミング）を設定します。

[入力形式]

情報の設定・変更

web-authentication roaming [action trap]

情報の削除

no web-authentication roaming

[入力モード]

(config)

[パラメータ]

[action trap]

ローミングによるポート移動を検出時に，プライベート Trap を発行します。

1. 本パラメータ省略時の初期値
   ローミングによるポート移動を検出しても，プライベート Trap を発行しません。
2. 値の設定範囲
   action trap

[コマンド省略時の動作]

認証済み端末のポート移動を許可しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 移動先がダイナミック VLAN モード対象ポートで，移動前と同一 VLAN 内のときだけ，移動後も通信可能です。
4. 本コマンド設定状態で DHCP snooping 機能併用時，認証済み端末のポートを移動すると，認証状態は移動後のポートに遷移しますが，バインディングデータベースは更新されないため通信できません。
5. プライベート Trap を発行する場合は，snmp-server host コマンドで Trap の送信先 IP アドレスと "web-authentication" を設定しておく必要があります。

[関連コマンド]

web-authentication system-auth-control

web-authentication port

snmp-server host

web-authentication static-vlan force-authorized

RADIUS 認証方式を使用時，経路障害などで RADIUS サーバ無応答または RADIUS サーバへのリクエスト送信エラーが発生した場合に，当該ポートで認証要求した認証対象端末を強制的に認証許可状態とします。

[入力形式]

情報の設定・変更
web-authentication static-vlan force-authorized [action trap]

情報の削除
no web-authentication static-vlan force-authorized

[入力モード]

(config-if)

[パラメータ]

[action trap]

強制認証による認証許可時に，プライベート Trap を発行します。

1. 本パラメータ省略時の初期値
   強制認証により認証許可しても，プライベート Trap を発行しません。
2. 値の設定範囲
   action trap

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本機能はセキュリティ上の問題となる可能性がありますので，十分検討の上ご使用ください。

4. 本コマンドは次の条件で有効となります。
   - 下記のコンフィグレーションがすべて設定されていること
     - radius-server host または web-authentication radius-server host
     - web-authentication port ※1
     - web-authentication static-vlan force-authorized ※1
     - web-authentication system-auth-control
     - aaa authentication web-authentication ※2
     - web-authentication authentication ※3

   注※1

   同じイーサネットポートに設定してください。
   - RADIUS サーバへの送信で，下記のアカウントログが採取された場合
     No=21:

     NOTICE:LOGIN:(付加情報) Login failed ; Failed to connection to RADIUS server.

     付加情報：MAC，USER，IP，PORT，VLAN

     アカウントログは運用コマンド show web-authentication logging で確認できます。

   注※2

   装置デフォルトで強制認証使用時は「default group radius」だけ設定してください。

   注※3

   ポート別認証方式で強制認証使用時は「aaa authentication web-authentication <List name>」を設定してください。
5. 強制認証許可状態は，当該ユーザのログアウトで解除されます。
6. プライベート Trap を発行する場合は，snmp-server host コマンドで Trap の送信先 IP アドレスと "web-authentication" を設定しておく必要があります。
7. 下記のいずれかがすでに設定されている場合，本コマンドを設定できません。
   - authentication force-authorized enable
   - authentication force-authorized vlan

[関連コマンド]

aaa authentication web-authentication

radius-server host または web-authentication radius-server host

snmp-server host

web-authentication port

web-authentication system-auth-control

web-authentication static-vlan max-user

装置単位の最大認証ユーザ数を設定します。

[入力形式]

情報の設定・変更

web-authentication static-vlan max-user <Count>

情報の削除

no web-authentication static-vlan max-user

[入力モード]

(config)

[パラメータ]

<Count>

ユーザ認証を行う装置単位の最大認証ユーザ数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 1024

[コマンド省略時の動作]

装置単位で認証可能な最大認証ユーザ数は，1024 ユーザになります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本設定を行った場合，現在認証中のユーザはそのままですが，次回ログイン時から設定値が有効となります。
4. 装置単位とポート単位の最大認証ユーザ数を同時に設定することも可能です。
   - 認証済みユーザ数がポート単位の最大認証ユーザ数に達した場合，当該ポートで以降の新規ユーザの認証はできません。
   - 認証済みユーザ数が装置単位の最大認証ユーザ数に達した場合，本装置で以降の新規ユーザの認証はできません。
5. 運用中に認証済みユーザ数より最大認証ユーザ数を少なく変更した場合，認証済みのユーザは継続通信できますが，新規ユーザの認証はできません。
6. DHCP snooping 機能を併用している場合は，最大 246 ユーザに制限されます。

[関連コマンド]

web-authentication system-auth-control

web-authentication port

web-authentication static-vlan max-user (interface)

当該ポートの最大認証ユーザ数を設定します。

[入力形式]

情報の設定・変更

web-authentication static-vlan max-user <Count>

情報の削除

no web-authentication static-vlan max-user

[入力モード]

(config-if)

[パラメータ]

<Count>

ユーザ認証を行う当該ポートの最大認証ユーザ数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 1024

[コマンド省略時の動作]

当該ポートで認証可能な最大認証ユーザ数は，1024 ユーザになります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本設定を行った場合，現在認証中のユーザはそのままですが，次回ログイン時から設定値が有効となります。
4. 装置単位とポート単位の最大認証ユーザ数を同時に設定することも可能です。
   - 認証済みユーザ数がポート単位の最大認証ユーザ数に達した場合，当該ポートで以降の新規ユーザの認証はできません。
   - 認証済みユーザ数が装置単位の最大認証ユーザ数に達した場合，本装置で以降の新規ユーザの認証はできません。
5. 運用中に認証済みユーザ数より最大認証ユーザ数を少なく変更した場合，認証済みのユーザは継続通信できますが，新規ユーザの認証はできません。
6. DHCP snooping 機能を併用している場合は，最大 246 ユーザに制限されます。

［関連コマンド］

web-authentication system-auth-control

web-authentication port

web-authentication static-vlan roaming

HUB などを経由して接続した認証済み端末を，リンクダウンしないでポート移動した場合の通信許可（ローミング）を設定します。

[入力形式]

情報の設定・変更

web-authentication static-vlan roaming [action trap]

情報の削除

no web-authentication static-vlan roaming

[入力モード]

(config)

[パラメータ]

[action trap]

ローミングによるポート移動を検出時に，プライベート Trap を発行します。

1. 本パラメータ省略時の初期値
   ローミングによるポート移動を検出しても，プライベート Trap を発行しません。
2. 値の設定範囲
   action trap

[コマンド省略時の動作]

認証済み端末のポート移動時の通信を許可しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 移動先が固定 VLAN モード対象ポートで，移動前と同一 VLAN 内のときだけ，移動後も通信可能です。
4. 本コマンド設定状態で DHCP snooping 機能併用時，認証済み端末のポートを移動すると，認証状態は移動後のポートに遷移しますが，バインディングデータベースは更新されないため通信できません。
5. プライベート Trap を発行する場合は，snmp-server host コマンドで Trap の送信先 IP アドレスと "web-authentication" を設定しておく必要があります。

[関連コマンド]

web-authentication system-auth-control

web-authentication port

snmp-server host

web-authentication system-auth-control

Web 認証を有効にします。

なお，no web-authentication system-auth-control を実行した場合は，Web 認証を停止します。

[入力形式]

情報の設定
　web-authentication system-auth-control

情報の削除
　no web-authentication system-auth-control

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

Web 認証を行いません。

[通信への影響]

no web-authentication system-auth-control を実行した場合，認証済みユーザはログアウトされます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
2. no web-authentication system-auth-control を実行した場合でも，内蔵 Web 認証 DB に登録されたユーザ情報はそのまま保存されます。

[関連コマンド]

なし

web-authentication user-group

ユーザ ID 別認証方式を有効にします。

入力されたユーザ ID を "@" で分割し，[ユーザ ID] と [認証方式リスト名] として扱います。

[入力形式]

情報の設定
web-authentication user-group

情報の削除
no web-authentication user-group

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

入力されたユーザ ID を "@" で分割して扱いません。

[通信への影響]

変更した場合は，全認証を解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本装置に下記コマンドが 1 つでも設定されている場合は，本コマンドを設定できません。
    - dot1x authentication
    - dot1x vlan dynamic enable
    - dot1x vlan dynamic radius-vlan
    - mac-authentication authentication
    - mac-authentication interface
    - mac-authentication vlan
    - web-authentication authentication
    - web-authentication vlan
4. 入力されたユーザ ID から分割した認証方式リスト名が aaa authentication web-authentication コマンドで設定した認証方式リストと一致しない場合は，装置デフォルトの設定に従って動作します。

[関連コマンド]

aaa authentication web-authentication

web-authentication system-auth-control

web-authentication port

web-authentication user replacement

ユーザ切替オプションを有効にします。

1 台の端末を複数のユーザ ID で使用する場合，最初のユーザ ID で認証成功後に別のユーザ ID で認証が可能となります。

[入力形式]

情報の設定
web-authentication user replacement

情報の削除
no web-authentication user replacement

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

認証済みの端末から別ユーザ名でのログインを許可しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. ユーザ切り替えを行った場合，認証を解除しても最初のユーザに戻ることはできません。

[関連コマンド]

web-authentication system-auth-control

web-authentication vlan

ユーザ認証後，動的に切り替える VLAN ID を設定します。

本コマンドが設定されていない場合は，認証後の VLAN 切り替えが行われません。

[入力形式]

情報の設定・変更

web-authentication vlan <VLAN ID list>

情報の削除

no web-authentication vlan <VLAN ID list>

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

ユーザ認証後に切り替える MAC VLAN の VLAN ID list を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。ただし，デフォルト VLAN（VLAN ID=1）は設定できません。

[コマンド省略時の動作]

認証後の VLAN 切り替えが行われません。

[通信への影響]

本コマンドで VLAN を削除した場合，削除した VLAN で登録をしていたユーザはログアウトされます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 設定されたすべての VLAN ID は，MAC VLAN で設定されている必要があります。
4. 本装置に下記コマンドが 1 つでも設定されている場合は，本コマンドを設定できません。
   - authentication multi-step
   - dot1x authentication
   - mac-authentication authentication
   - web-authentication authentication
   - web-authentication user-group

[関連コマンド]

switchport mac

vlan

web-authentication system-auth-control

web-authentication web-port

URL リダイレクト機能有効時，本装置で URL リダイレクト対象とするフレームの TCP 宛先ポート番号を追加設定します。

通常，http ＝ 80，https=443 の番号で割り当てられているポート番号に，それぞれ任意のポート番号を 1 件ずつ追加指定できます。

[入力形式]

情報の設定・変更

web-authentication web-port {http <port> | https <port>}

情報の削除

no web-authentication web-port {http | https}

[入力モード]

(config)

[パラメータ]

{http <port> | https <port>}

http プロトコルまたは https プロトコルの通信用ポート番号を設定します。なお，OAN と共存する場合，ポート番号 832 と 9698 は OAN で使用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   http パラメータの場合：1 〜 65535（ただし，443 を除く）
   https パラメータの場合：1 〜 65535（ただし，80 を除く）

[コマンド省略時の動作]

次に示す初期値のポート番号のフレームが URL リダイレクト対象となります。

- http:80
- https:443

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての Web 認証設定は，web-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 22-1　コンフィグレーションコマンドと Web 認証の認証モード」を参照してください。
3. 本コマンドで設定可能な TCP 宛先ポート番号は，http，https それぞれのパラメータで 1 件ずつです。

4. 本コマンドは，web-authentication redirect tcp-port コマンドと同一動作です。

 ２つのコマンドで異なるポート番号を指定した場合，それぞれの指定が有効となります。
 また，２つのコマンドで同一ポート番号を指定した場合の扱いを次に示します。

<table>
<tr><th colspan="2" rowspan="2"></th><th rowspan="2">web-authentication redirect tcp-port</th><th colspan="2">web-authentication web-port</th></tr>
<tr><th>http</th><th>https</th></tr>
<tr><td colspan="2">web-authentication redirect tcp-port</td><td></td><td>http としてリダイレクト</td><td>http としてリダイレクト (https 指定のポート番号は無視)</td></tr>
<tr><td rowspan="2">web-authentication web-port</td><td>http</td><td>http としてリダイレクト</td><td></td><td>先に入力したコマンド設定が有効</td></tr>
<tr><td>https</td><td>http としてリダイレクト (https 指定のポート番号は無視)</td><td>先に入力したコマンド設定が有効</td><td></td></tr>
</table>

［関連コマンド］

authentication ip access-group

authentication arp-relay

web-authentication port

web-authentication redirect tcp-port

web-authentication system-auth-control

default-router

クライアントに配布するルータオプションを設定します。ルータオプションは，クライアントがサブネット上のルータ IP アドレス（デフォルトルータ）として使用可能な IP アドレスです。

[入力形式]

情報の設定・変更

default-router <IP address>

情報の削除

no default-router

[入力モード]

(dhcp-config)

[パラメータ]

<IP address>

クライアントのサブネット上のルータ IP アドレス（デフォルトルータ）を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   次に示すアドレスは設定できません。
   - 127.0.0.0 ～ 127.255.255.255

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 設定可能なルータ IP アドレス（デフォルトルータ）は 1 プール単位で最大 1 個です。

[関連コマンド]

ip dhcp pool

dns-server

クライアントに配布するドメインネームサーバオプションを設定します。ドメインネームサーバオプションは，クライアントで利用可能な DNS サーバの IP アドレスです。

[入力形式]

情報の設定・変更
　dns-server <IP address> [<IP address>]

情報の削除
　no dns-server

[入力モード]

(dhcp-config)

[パラメータ]

<IP address>

クライアントで利用可能な DNS サーバの IP アドレスを設定します。サーバのアドレスは，優先度の高いものを先に指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   次に示すアドレスは設定できません。
   - 127.0.0.0 ～ 127.255.255.255

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 設定可能な DNS サーバの IP アドレスは，１プール単位で最大２個です。

[関連コマンド]

ip dhcp pool

ip dhcp excluded-address

network コマンドで設定した IP アドレスプールのうち，配布対象から除外する IP アドレスの範囲を設定します。

[入力形式]

情報の設定・変更

ip dhcp excluded-address <Low address> [<High address>]

情報の削除

no ip dhcp excluded-address <Low address> [<High address>]

[入力モード]

(config)

[パラメータ]

<Low address> [<High address>]

DHCP サーバが DHCP クライアントに割り当ててはいけない IP アドレス，または IP アドレスの範囲を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   次に示すアドレスは設定できません。
   - 127.0.0.0 ～ 127.255.255.255

[コマンド省略時の動作]

network コマンドで設定された範囲の全 IP アドレスが割り当て可能です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 最大設定数は 64 です。
2. 除外アドレス設定を削除することによって，IP アドレスプール数が最大数を超えてしまう場合には，除外アドレス設定を削除することはできません。

[関連コマンド]

ip dhcp pool

network

ip dhcp pool

DHCP アドレスプール情報を設定します。

[入力形式]

情報の設定・変更

ip dhcp pool <Pool name>

情報の削除

no ip dhcp pool <Pool name>

[入力モード]

(config)

[パラメータ]

<Pool Name>

DHCP アドレスプール情報の名称を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   14 文字以内の文字列で設定してください。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 最大 32 個 (network 設定 32）設定できます。

[関連コマンド]

ip dhcp excluded-address

network

lease

クライアントに配布する IP アドレスのデフォルトリース時間を設定します。

[入力形式]

情報の設定・変更

lease {<Time day> [<Time hour> [<Time min> [<Time sec>]]] | infinite}

情報の削除

no lease

[入力モード]

(dhcp-config)

[パラメータ]

{<Time day> [<Time hour> [<Time min> [<Time sec>]]] | infinite}

日，時間，分，秒の単位で，リース時間を設定します。本情報の設定がない場合は，初期値としてリース時間が 10 秒として設定されます。また，<Time day> /<Time hour>/<Time min>/<Time sec> の合計値が 10 秒未満の場合は設定できません。10(秒) 〜 365(日) の間で設定してください。

<Time day>

リース時間を日単位に設定します。

1. 値の設定範囲
   0 〜 365（日）

<Time hour>

リース時間を時間単位に設定します。

1. 値の設定範囲
   0 〜 23（時間）

<Time min>

リース時間を分単位に設定します。

1. 値の設定範囲
   0 〜 59（分）

<Time sec>

リース時間を秒単位に設定します。

1. 値の設定範囲
   0 〜 59（秒）

infinite

リース時間を無制限に設定します。

[コマンド省略時の動作]

リース時間は 10 秒となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. リース時間が最大リース時間（max-lease）を超える設定をした場合，最大リース時間が優先されます。
2. リース時間を短くした場合，クライアントは頻繁にリースの更新を行うため，短時間しか使用されない一時的な IP アドレスなどの限定した用途以外では，リース時間を極端に短くしないでください。また，短いリース時間でもクライアントが動作可能なことを確認してください。
3. 入力形式で設定された順序でリース時間を入力してください。<Time day> の入力後に 24 ～ 59 を入力すると，<Time min> と認識されます。この場合，[Enter] を押下すると，入力エラーとなります。

[関連コマンド]

ip dhcp pool

max-lease

クライアントがリース時間を設定して IP アドレスを要求した際に，許容する最大リース時間を設定します。

[入力形式]

情報の設定・変更

max-lease {<Time day> [<Time hour> [<Time min> [<Time sec>]]] | infinite}

情報の削除

no max-lease

[入力モード]

(dhcp-config)

[パラメータ]

{<Time day> [<Time hour> [<Time min> [<Time sec>]]] | infinite}

日，時間，分，秒の単位で時間を指定することによって，クライアントから時間の指定があった場合の最大リース時間を設定します。本情報の設定がない場合は，デフォルトリース時間と同じ値になります。また，<Time day> /<Time hour>/<Time min>/<Time sec> の合計値が 10 秒未満の場合は設定できません。10(秒) ～ 365(日) の間で設定してください。

<Time day>

リース時間を日単位に設定します。

1. 値の設定範囲
   0 ～ 365（日）

<Time hour>

リース時間を時間単位に設定します。

1. 値の設定範囲
   0 ～ 23（時間）

<Time min>

リース時間を分単位に設定します。

1. 値の設定範囲
   0 ～ 59（分）

<Time sec>

リース時間を秒単位に設定します。

1. 値の設定範囲
   0 ～ 59（秒）

infinite

リース時間を無制限に設定します。

[コマンド省略時の動作]

最大リース時間は lease コマンドで設定した時間となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. リース時間を短くした場合，クライアントは頻繁にリースの更新を行うため，短時間しか使用されない一時的な IP アドレスなどの限定した用途以外では，リース時間を極端に短くしないでください。また，短いリース時間でもクライアントが動作可能なことを確認してください。
2. 入力形式で設定された順序でリース時間を入力してください。<Time day> の入力後に 24 ～ 59 を入力すると，<Time min> と認識されます。この場合，[Enter] を押下すると，入力エラーとなります。

[関連コマンド]

ip dhcp pool

network

DHCP によって動的に IP アドレスを配布するネットワークのサブネットを設定します。実際に DHCP アドレスプールとして登録されるのはサブネットのうち，IP アドレスホスト部のビットがすべて 0 およびすべて 1 のアドレスを除いたものです。

［入力形式］

情報の設定・変更

network <IP address> [/<Masklen>]

情報の削除

no network

［入力モード］

(dhcp-config)

［パラメータ］

<IP address> [/<Masklen>]

DHCP アドレスプールのネットワークアドレスを設定します。また，マスクを省略した場合は，クラス A，B，C に応じたマスクが設定されます。

表 22-2　クラスごとの IP アドレス範囲

クラス	IP アドレス
クラス A（/8）	1.x.x.x 〜 126.x.x.x
クラス B（/16）	128.x.x.x 〜 191.x.x.x
クラス C（/24）	192.x.x.x 〜 223.x.x.x

<IP address>

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   次に示すアドレスは設定できません。
   ・127.0.0.0 〜 127.255.255.255
   ・ホスト部が 2 進数ですべて 0 またはすべて 1 のアドレス
   ・「表 22-2　クラスごとの IP アドレス範囲」に示す範囲以外の IP アドレス

<Masklen>

1. 本パラメータ省略時の初期値
   「表 22-2　クラスごとの IP アドレス範囲」に示すクラス A，B，C に応じたマスク
2. 値の設定範囲
   8 〜 32
   ドット記法（255.0.0.0 〜 255.255.255.255）でも設定できます。

［コマンド省略時の動作］

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本設定を行った場合，IP アドレスプールとして確保されるのは，対象サブネットのホスト部のビットがすべて 0 およびホスト部のビットがすべて 1 のアドレスを除いた，すべての IP アドレスになります。そのため，事前に ip dhcp excluded-address コマンドで配布対象から除外したいアドレスを設定してください。
2. 本装置の DHCP サーバで扱えるサブネットは最大 32 までなので，network 設定を含むプールを 32 以上作成することはできません。

[関連コマンド]

ip dhcp excluded-address

ip dhcp pool

service dhcp

DHCP サーバを有効にするインタフェースを設定します。本設定を行ったインタフェースだけで DHCP パケットを受信します。

[入力形式]

情報の設定・変更
　service dhcp vlan <VLAN ID>

情報の削除
　no service dhcp vlan <VLAN ID>

[入力モード]

(config)

[パラメータ]

vlan <VLAN ID>

IPv4 アドレスが設定された VLAN の VLAN ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID> には interface vlan コマンドで設定した VLAN ID を設定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 設定可能なインタフェース数は最大 32 です。

[関連コマンド]

interface vlan

23 MAC 認証

コンフィグレーションコマンドと認証モードの対応
aaa accounting mac-authentication
aaa authentication mac-authentication
aaa authentication mac-authentication end-by-reject
mac-authentication access-group
mac-authentication authentication
mac-authentication auto-logout
mac-authentication force-authorized vlan
mac-authentication id-format
mac-authentication interface
mac-authentication max-timer
mac-authentication max-user
mac-authentication max-user (interface)
mac-authentication password
mac-authentication port
mac-authentication radius-server dead-interval
mac-authentication radius-server host
mac-authentication roaming
mac-authentication static-vlan force-authorized
mac-authentication static-vlan max-user
mac-authentication static-vlan max-user (interface)
mac-authentication static-vlan roaming
mac-authentication system-auth-control
mac-authentication timeout quiet-period
mac-authentication timeout reauth-period

mac-authentication vlan
mac-authentication vlan-check

コンフィグレーションコマンドと認証モードの対応

MAC 認証のコンフィグレーションコマンドが設定できる，MAC 認証の認証モードを次の表に示します。

表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード

コマンド名	MAC 認証の認証モード※3		
	固	ダ	レ
aaa accounting mac-authentication	○	○	○
aaa authentication mac-authentication	○	○	○
aaa authentication mac-authentication end-by-reject	○	○	－
authentication arp-relay※1	○	○	×
authentication ip access-group※1	○	○	×
mac-authentication access-group	○	○	○
mac-authentication authentication	○	○	×
mac-authentication auto-logout	○	○	○
mac-authentication force-authorized vlan	－	○	○
mac-authentication id-format	○	○	○
mac-authentication interface	－	－	○
mac-authentication max-timer	○	○	○
mac-authentication max-user	－	○	○
mac-authentication max-user (interface)	－	○	○
mac-authentication password	○	○	○
mac-authentication port※2	○	○	－
mac-authentication radius-server dead-interval	○	○	○
mac-authentication radius-server host	○	○	○
mac-authentication roaming	－	○	－
mac-authentication static-vlan force-authorized	○	－	－
mac-authentication static-vlan max-user	○	－	－
mac-authentication static-vlan max-user (interface)	○	－	－
mac-authentication static-vlan roaming	○	－	－
mac-authentication system-auth-control	○	○	○
mac-authentication timeout quiet-period	○	○	○
mac-authentication timeout reauth-period	○	○	○
mac-authentication vlan	－	－	○
mac-authentication vlan-check	○	－	－

凡例

固：固定 VLAN モード

ダ：ダイナミック VLAN モード

レ：レガシーモード

○：設定内容に従って動作します。

－：コマンドは入力できますが，動作しません。

×：コマンドを入力できません。

注※ 1

コマンドの入力形式など詳細は，「20　レイヤ 2 認証共通」を参照してください。

注※ 2

本コマンドの設定は，認証モードの切り替えに影響します。

注※ 3

認証モードの表記など詳細については，「コンフィグレーションガイド Vol.2」を参照してください。

aaa accounting mac-authentication

MAC 認証のアカウンティング情報をアカウンティングサーバへ送信します。

[入力形式]

情報の設定

aaa accounting mac-authentication default start-stop group radius

情報の削除

no aaa accounting mac-authentication default

[入力モード]

(config)

[パラメータ]

default

装置デフォルトのアカウンティング方式を設定します。

start-stop

認証成功時にはスタートアカウンティング通知が，認証解除時にはストップアカウンティング通知がアカウンティングサーバに送信されます。

group radius

アカウンティングサーバとして RADIUS サーバを使用します。

[コマンド省略時の動作]

アカウンティングサーバに通知しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。

[関連コマンド]

aaa authentication mac-authentication

mac-authentication system-auth-control

radius-server host または mac-authentication radius-server host

aaa authentication mac-authentication

MAC 認証での認証方式グループを設定します。

先に設定した認証に失敗した場合は，次に設定した方式で認証を行います。なお，この認証失敗時の動作は aaa authentication mac-authentication end-by-reject コマンドにより変更できます。

default 指定は 1 エントリ，認証方式リスト指定は最大 4 エントリまで設定できます。

[入力形式]

情報の設定・変更

aaa authentication mac-authentication default <Method> [<Method>]
aaa authentication mac-authentication <List name> group <Group name>

情報の削除

no aaa authentication mac-authentication {default | <List name>}

[入力モード]

(config)

[パラメータ]

default <Method> [<Method>]

装置デフォルトの認証方式を設定します。同一の Method は複数設定できません。
<Method> には group radius または local を設定します。

group radius

RADIUS サーバによる MAC 認証を行います。使用する RADIUS サーバは MAC 認証専用 RADIUS サーバまたは，汎用 RADIUS サーバです。

local

ローカル認証を行います。内蔵 MAC 認証 DB を使用します。

<List name>

認証方式リスト名を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。
   先頭文字は大文字を推奨します。
   ただし，下記の文字列は設定できません。
   ・アットマーク (@)
   ・default(前方一致または完全一致した文字列)
   ・end-by-reject（前方一致または完全一致した文字列）

group <Group Name>

RADIUS サーバによる MAC 認証を行います。使用する RADIUS サーバは RADIUS サーバグループです。aaa group server radius コマンドで設定したグループ名を指定してください。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲

32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

RADIUS サーバを使用しないで，内蔵 MAC 認証 DB を使用して認証を行います。

[通信への影響]

装置デフォルトを設定変更したときは，装置デフォルトの認証方式で認証した端末を認証解除します。

認証方式リストを設定変更したときは，当該認証方式リストで認証した端末を認証解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本コマンドを有効にする場合には，RADIUS サーバの認証設定が別途必要になります。
4. MAC 認証の強制認証機能は，RADIUS 認証だけ設定された場合に動作します。複数の認証方式を設定した場合，強制認証は実施されません。

[関連コマンド]

aaa authentication mac-authentication end-by-reject

aaa group server radius

mac-authentication system-auth-control

mac-authentication authentication

radius-server host または mac-authentication radius-server host

aaa authentication mac-authentication end-by-reject

認証で否認された場合に，認証を終了します。通信不可（RADIUS 無応答など）による認証失敗時は，aaa authentication mac-authentication コマンドで次に指定されている認証方式で認証します。

[入力形式]

情報の設定

aaa authentication mac-authentication end-by-reject

情報の削除

no aaa authentication mac-authentication end-by-reject

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

認証で否認された場合に，その理由にかかわらず aaa authentication mac-authentication コマンドで次に指定されている認証方式で認証します。

[通信への影響]

MAC 認証機能の端末を認証解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
2. aaa authentication mac-authentication コマンドで指定した認証方式にだけ有効です。

[関連コマンド]

aaa authentication mac-authentication

mac-authentication access-group

MAC 認証用ポートに MAC アクセスリストを適用し，認証対象端末・非対象端末を MAC アドレスで設定します。

[入力形式]

情報の設定・変更

mac-authentication access-group <ACL ID>

情報の削除

no mac-authentication access-group

[入力モード]

(config)

[パラメータ]

<ACL ID>

設定する MAC アクセスリストの識別子を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

MAC 認証用ポートに接続されたすべての端末が認証対象端末となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 登録されている MAC アクセスリストには暗黙の廃棄が存在します。端末の MAC アドレスが設定した MAC アクセスリストに該当しなかった場合は，暗黙の廃棄に従って認証非対象の端末となります。
4. 実在しない MAC アクセスリストを設定した場合は何も動作しません。MAC アクセスリストの識別子は登録されます。

[関連コマンド]

mac-authentication system-auth-control

mac access-list extended

mac-authentication authentication

ポート別認証方式の認証方式リスト名を設定します。

[入力形式]

情報の設定・変更

mac-authentication authentication <List name>

情報の削除

no mac-authentication authentication

[入力モード]

(config-if)

[パラメータ]

<List name>

aaa authentication mac-authentication コマンドで設定した認証方式リスト名を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   32 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。(ただし，アットマーク (@) を除く)
   先頭文字は大文字を推奨します。

[コマンド省略時の動作]

装置デフォルトを使用して MAC 認証を行います。

[通信への影響]

当該認証方式リスト名を変更したポートの端末を認証解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本装置に下記コマンドが 1 つでも設定されている場合は，本コマンドを設定できません。
   - dot1x vlan dynamic enable
   - dot1x vlan dynamic radius-vlan
   - web-authentication user-group
   - web-authentication vlan
   - mac-authentication interface
   - mac-authentication vlan
4. 本コマンドで設定した認証方式リスト名が aaa authentication mac-authentication コマンドで設定した認証方式リスト名と一致しない場合は，装置デフォルトの設定に従って動作します。

5. 本コマンドはイーサネットインタフェースだけ設定可能です。

［関連コマンド］

aaa authentication mac-authentication

mac-authentication system-auth-control

mac-authentication port

mac-authentication auto-logout

no mac-authentication auto-logout コマンドで，MAC 認証で認証された端末から一定時間フレームを受信しなかった状態を検出したときに認証を自動解除する設定を無効にします。

また，delay-time を設定することで時間を変更できますが，認証モードにより動作は異なります。

[入力形式]

情報の設定

no mac-authentication auto-logout

情報の変更

mac-authentication auto-logout delay-time <Seconds>

情報の削除

mac-authentication auto-logout

[入力モード]

(config)

[パラメータ]

delay-time <Seconds>

＜ 固定 VLAN モード，ダイナミック VLAN モード＞

本認証モードで認証後に，MAC アドレステーブルに登録した MAC 認証エントリが対象です。

本コマンドの設定時間（無通信監視時間）を経過しても端末からフレームを受信しなかった状態を検出すると，MAC アドレステーブルから該当 MAC 認証エントリを削除して認証を解除します。

「0」を設定すると，無通信監視時間はデフォルト値（3600 秒）で動作します。

1. 本パラメータ省略時の初期値
   本認証モードで認証後に登録した MAC 認証エントリの無通信監視時間を 3600 秒とします。
2. 値の設定範囲
   0，60 ～ 86400

＜レガシーモード＞

MAC アドレステーブルのダイナミックエンントリで，本認証モードで認証済みの MAC アドレスが対象です。

MAC アドレステーブルエージングタイムアウト※後，本コマンドの設定時間（猶予時間）を経過しても再度登録されない場合は，該当 MAC アドレスの認証を解除します。

※：エージング時間は mac-address-table aging コマンドの設定によります。

「0」を設定すると，エージングタイムアウト検出後，即時に認証を解除します。

1. 本パラメータ省略時の初期値
   エージングタイムアウト後，3600 秒経過するまで認証を解除しません。
2. 値の設定範囲
   0，60 ～ 86400

[コマンド省略時の動作]

＜固定 VLAN モード，ダイナミック VLAN モード＞

本認証モードで認証後に，3600 秒経過しても該当 MAC 認証エントリの端末からフレームを受信しな

かった状態を検出すると，自動的に該当 MAC 認証エントリを MAC アドレステーブルから削除し認証解除します。

＜レガシーモード＞

MAC アドレステーブルエージングタイムアウトを検出してから 3600 秒経過後，自動的に該当 MAC アドレスの端末を認証解除します。

[通信への影響]

no mac-authentication auto-logout コマンド設定後は，MAC 認証で認証された端末が一定時間中継なしの状態を検出しても認証を自動解除しません。

mac-authentication auto-logout delay-time を設定後は，設定時間で動作します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 固定 VLAN モード / ダイナミック VLAN モードの認証済み端末の無通信監視時間は，下記の条件で有効となります。
    - MAC 認証固定 VLAN モードまたはダイナミック VLAN モード有効で，mac-authentication auto-logout 有効

[関連コマンド]

mac-authentication system-auth-control

mac-authentication port

mac-address-table aging-time

mac-authentication force-authorized vlan

RADIUS 認証方式を使用時，経路障害などで RADIUS サーバ無応答または RADIUS サーバへのリクエスト送信エラーが発生した場合に，当該ポートで認証要求した認証対象端末を強制的に認証許可状態とし，認証後 VLAN を割り当てます。

[入力形式]

情報の設定・変更

mac-authentication force-authorized vlan <VLAN ID> [action trap]

情報の削除

no mac-authentication force-authorized vlan

[入力モード]

(config-if)

[パラメータ]

<VLAN ID>

強制認証許可時に割り当てる認証後 VLAN ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。
   ただし，デフォルト VLAN（VLAN ID= 1）は設定できません。

[action trap]

強制認証による認証許可時に，プライベート Trap を発行します。

1. 本パラメータ省略時の初期値
   強制認証により認証許可しても，プライベート Trap を発行しません。
2. 値の設定範囲
   action trap

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. vlan コマンドで mac-based（MAC VLAN）を設定している VLAN ID を設定してください。
4. 本機能はセキュリティ上の問題となる可能性がありますので，十分検討の上ご使用ください。

5. 本コマンドは次の条件で有効となります。
   - 下記のコンフィグレーションがすべて設定されていること
     - radius-server host または mac-authentication radius-server host
     - mac-authentication system-auth-control
     - mac-authentication port ※1※4
     - mac-authentication interface ※2
     - mac-authentication vlan ※2※3
     - vlan <VLAN ID list> mac-based ※3
     - mac-authentication force-authorized vlan ※3※4
     - switchport mac vlan ※2※3※4
     - switchport mode mac-vlan ※4
     - aaa authentication mac-authentication ※5
     - mac-authentication authentication ※6

   注※1
   ダイナミック VLAN モードで使用するときに設定してください。

   注※2
   レガシーモードで使用するときに設定してください。

   注※3
   同じ VLAN ID を設定してください。

   注※4
   同じイーサネットポートに設定してください。
   - RADIUS サーバへの送信で，下記のアカウントログが採取された場合
     No=21:
     NOTICE:LOGIN(付加情報) Login failed ; Failed to connection to RADIUS server.
     付加情報：MAC，PORT，VLAN

   アカウントログは運用コマンド show mac-authentication logging で確認できます。

   注※5
   装置デフォルトで強制認証使用時は「default group radius」だけ設定してください。

   注※6
   ポート別認証方式で強制認証使用時は「aaa authentication mac-authentication <List name>」を設定してください。
6. 強制認証許可状態は，当該端末の認証解除とともに解除されます。
7. プライベート Trap を発行する場合は，snmp-server host コマンドで Trap の送信先 IP アドレスと "mac-authentication" を設定しておく必要があります。
8. 下記のいずれかがすでに設定されている場合，本コマンドを設定できません。
   - authentication force-authorized enable
   - authentication force-authorized vlan

[関連コマンド]

aaa authentication mac-authentication

mac-authentication interface

mac-authentication port

mac-authentication system-auth-control

mac-authentication vlan

radius-server host または mac-authentication radius-server host

switchport mac

switchport mode

vlan

mac-authentication id-format

RADIUS 認証方式を使用時，RADIUS サーバへ認証要求する際の MAC アドレス形式を設定します。

[入力形式]

情報の設定・変更

mac-authentication id-format <Type> [capitals]

情報の削除

no mac-authentication id-format

[入力モード]

(config)

[パラメータ]

<Type>

RADIUS サーバへ認証要求時の MAC アドレス形式を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 〜 3
   0：xx-xx-xx-xx-xx-xx
   1：xxxxxxxxxxxx
   2：xxxx.xxxx.xxxx
   3：xx:xx:xx:xx:xx:xx

capitals

RADIUS サーバへ認証要求時の MAC アドレスを 16 進数大文字の形式で実施する場合に設定します。

1. 本パラメータ省略時の初期値
   小文字で実施します。
2. 値の設定範囲
   capitals

[コマンド省略時の動作]

Type 0 (xx-xx-xx-xx-xx-xx)，16 進数小文字の形式で RADIUS サーバへ認証要求します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。

[関連コマンド]

mac-authentication system-auth-control

aaa authentication mac-authentication

mac-authentication interface

MAC 認証レガシーモードの対象インタフェースポートを設定します。

[入力形式]

情報の設定・変更

mac-authentication interface fastethernet <IF# list>【SS1250】【SS1240】

mac-authentication interface gigabitethernet <IF# list>

情報の削除

no mac-authentication interface fastethernet【SS1250】【SS1240】

no mac-authentication interface gigabitethernet

[入力モード]

(config)

[パラメータ]

<IF# list>

MAC 認証の対象ポートを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

MAC 認証レガシーモードが動作しません。

[通信への影響]

本コマンドでインタフェースを削除した場合，削除したインタフェースで登録していたレガシーモード認証端末が解除されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本装置に下記コマンドが 1 つでも設定されている場合は，本コマンドを設定できません。
   - authentication multi-step
   - dot1x authentication
   - mac-authentication authentication
   - web-authentication authentication
   - web-authentication user-group

[関連コマンド]

mac-authentication system-auth-control

mac-authentication max-timer

最大接続時間を設定します。

[入力形式]

情報の設定・変更
　mac-authentication max-timer { <Minutes> | infinity }

情報の削除
　no mac-authentication max-timer

[入力モード]

(config)

[パラメータ]

{ <Minutes> | infinity }

認証済み端末の最大接続時間を分単位で設定します。当該端末の認証成功後から，本コマンドの設定時間が経過した場合に，自動的に認証が解除されます。
「infinity」と指定した場合は，最大接続時間は無限となります。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   10 ～ 1440（分），または infinity

[コマンド省略時の動作]

認証を解除しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 最大接続時間を短縮または延長した場合には，現在認証中の端末は前設定を有効とし，次回認証時から設定値が有効になります。
4. MAC 認証での接続時間は，装置の時刻を使用していません。そのため，運用コマンド set clock で日時を変更しても接続時間に影響は出ません。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication max-user

装置単位の最大認証端末数を設定します。

[入力形式]

情報の設定・変更

mac-authentication max-user <Count>

情報の削除

no mac-authentication max-user

[入力モード]

(config)

[パラメータ]

<Count>

装置単位の最大認証端末数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 256

[コマンド省略時の動作]

装置単位の認証可能な最大認証端末数は，256 端末になります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本設定を行った場合，現在認証中の端末はそのままですが，次回の新規端末の認証時から設定値が有効となります。
4. 装置単位とポート単位の最大認証端末数を同時に設定することも可能です。
   - 認証済み端末数がポート単位の最大認証端末数に達した場合，当該ポートで以降の新規端末の認証はできません。
   - 認証済み端末数が装置単位の最大認証端末数に達した場合，本装置で以降の新規端末の認証はできません。
5. 運用中に認証済み端末数より最大認証端末数を少なく変更した場合，認証済みの端末は継続通信できますが，新規端末の認証はできません。
6. 認証済み端末の接続ポートを移動した場合などでは，実際の接続端末数と差異が生じることがあります。

7. DHCP snooping 機能を併用している場合は，最大 246 端末に制限されます。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication interface

mac-authentication port

mac-authentication max-user (interface)

当該ポートの最大認証端末数を設定します。

[入力形式]

情報の設定・変更

mac-authentication max-user <Count>

情報の削除

no mac-authentication max-user

[入力モード]

(config-if)

[パラメータ]

<Count>

当該ポートの最大認証端末数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 256

[コマンド省略時の動作]

当該ポートの認証可能な最大認証端末数は，256 端末になります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本設定を行った場合，現在認証中の端末はそのままですが，次回の新規端末の認証時から設定値が有効となります。
4. 装置単位とポート単位の最大認証端末数を同時に設定することも可能です。
   - 認証済み端末数がポート単位の最大認証端末数に達した場合，当該ポートで以降の新規端末の認証はできません。
   - 認証済み端末数が装置単位の最大認証端末数に達した場合，本装置で以降の新規端末の認証はできません。
5. 運用中に認証済み端末数より最大認証端末数を少なく変更した場合，認証済みの端末は継続通信できますが，新規端末の認証はできません。
6. 認証済み端末の接続ポートを移動した場合などでは，実際の接続端末数と差異が生じることがあります。

7. DHCP snooping 機能を併用している場合は，最大 246 端末に制限されます。

［関連コマンド］

mac-authentication system-auth-control

mac-authentication interface

mac-authentication port

mac-authentication password

RADIUS 認証方式を使用時，RADIUS サーバへ認証要求する際のパスワードを設定します。

[入力形式]

情報の設定・変更
mac-authentication password <Password>

情報の削除
no mac-authentication password

[入力モード]

(config)

[パラメータ]

<Password>

RADIUS サーバへ認証要求時の任意のパスワードを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 32 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

mac-authentication id-format コマンドを設定している場合は，そのコマンドで設定した形式の認証対象端末の MAC アドレスがパスワードとなります。

mac-authentication id-format コマンドを設定していない場合は，「xx-xx-xx-xx-xx-xx」（A ～ F は小文字）形式の認証対象端末の MAC アドレスがパスワードとなります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本コマンドで設定したパスワードは，すべての MAC 認証 RADIUS 認証対象端末で共通となります。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication id-format

aaa authentication mac-authentication

mac-authentication port

ポートに認証モードを設定します。

[入力形式]

情報の設定
　mac-authentication port

情報の削除
　no mac-authentication port

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

MAC 認証有効時，当該ポートはレガシーモードで動作します。

[通信への影響]

本コマンドで認証対象ポートの削除を行った場合，当該ポートでの認証が解除されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. system function コマンド設定有で extended-authentication が設定されていない場合，本コマンドは設定できません。（system function コマンドが未設定の場合は，設定できます。）【SS1250】【SS1240】
4. 本コマンドはイーサネットインタフェースだけ設定可能です。

[関連コマンド]

mac-authentication system-auth-control

authentication ip access-group

authentication arp-relay

mac-authentication radius-server dead-interval

MAC 認証専用 RADIUS サーバがプライマリ MAC 認証専用 RADIUS サーバへ自動復旧するまでの監視タイマを設定します。

カレントサーバ（運用中の RADIUS 認証要求先）が有効なセカンダリ MAC 認証専用 RADIUS サーバへ遷移した時点，または全サーバ使用不可状態で監視タイマをスタートし，本コマンドによる設定時間経過後（監視タイマ満了後）に，プライマリ MAC 認証専用 RADIUS サーバへ復旧します。

[入力形式]

情報の設定・変更

mac-authentication radius-server dead-interval <Minutes>

情報の削除

no mac-authentication radius-server dead-interval

[入力モード]

(config)

[パラメータ]

<Minutes>

セカンダリ MAC 認証専用 RADIUS サーバから，プライマリ MAC 認証専用 RADIUS サーバへ自動復旧するまでの監視タイマを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 1440（分）
   0 を設定した場合は，RADIUS 認証要求を必ずプライマリ MAC 認証専用 RADIUS サーバから開始します。

[コマンド省略時の動作]

カレントサーバがセカンダリ MAC 認証専用 RADIUS サーバへ遷移して 10 分後，プライマリ MAC 認証専用 RADIUS サーバに自動復旧します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

1. セカンダリ MAC 認証専用 RADIUS サーバをカレントサーバとして運用中に監視タイマ値を変更した場合，その時点での経過状態を判定し結果を反映します。
2. 監視タイマをスタート後に本コマンド設定を削除した場合，監視タイマのカウントはリセットせずに継続し，デフォルト値 10 分として動作します。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。

2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. ３台以上の MAC 認証専用 RADIUS サーバを設定していた場合，監視タイマをスタート後に他の MAC 認証専用 RADIUS サーバへカレントサーバが遷移した場合でも，監視タイマはリセットせずに継続します。
4. 監視タイマはいったんスタートすると基本的に満了するまでリセットしませんが，下記の契機では例外として満了せずにリセットします。
   - 本コマンドで mac-authentication dead-interval 0 を設定したとき
   - カレントサーバとして運用中の MAC 認証専用 RADIUS サーバ情報を，mac-authentication radius-server host コマンドで削除したとき
   - 運用コマンド clear radius-server を実行したとき
5. 認証対象端末の認証シーケンス実施中に監視タイマが満了した場合でも，実施中の認証シーケンスが完了するまでプライマリ MAC 認証専用 RADIUS サーバへの復旧は行なわれません。

[関連コマンド]

aaa authentication mac-authentication

mac-authentication port

mac-authentication system-auth-control

mac-authentication radius-server host

mac-authentication radius-server host

MAC 認証に使用する RADIUS サーバの設定を行います。

[入力形式]

情報の設定・変更

mac-authentication radius-server host <IP address> [auth-port <Port>] [acct-port <Port>] [timeout <Seconds>] [retransmit <Retries>] [key <String>]

情報の削除

no mac-authentication radius-server host <IP address>

[入力モード]

(config)

[パラメータ]

<IP address>

RADIUS サーバの IPv4 アドレスを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   IPv4 アドレス（ドット記法）を指定します。
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

auth-port <Port>

RADIUS サーバのポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1812 を使用します。
2. 値の設定範囲
   1 ～ 65535

acct-port <Port>

RADIUS サーバのアカウンティング用ポート番号を指定します。

1. 本パラメータ省略時の初期値
   ポート番号 1813 を使用します。
2. 値の設定範囲
   1 ～ 65535

timeout <Seconds>

RADIUS サーバからの応答タイムアウト時間（秒）を指定します。

1. 本パラメータ省略時の初期値
   radius-server timeout コマンドで設定されている時間が使用されます。設定されていない場合の初期値は 5 秒です。
2. 値の設定範囲
   1 ～ 30（秒）

retransmit <Retries>

RADIUS サーバに対して認証要求を再送信する回数を指定します。

1. 本パラメータ省略時の初期値

radius-server retransmit コマンドで設定されている回数が使用されます。設定されていない場合の初期値は 3 回です。

2. 値の設定範囲
   0 ～ 15（回）

key <String>

RADIUS サーバ間との通信の暗号化／認証に使用する RADIUS 鍵を指定します。RADIUS 鍵はクライアント上と RADIUS サーバ上で同一の鍵を設定する必要があります。

1. 本パラメータ省略時の初期値
   radius-server key コマンドで設定されている RADIUS 鍵が使用されます。設定されていない場合，当該 RADIUS サーバは無効になります。
2. 値の設定範囲
   64 文字以内の文字列で指定してください。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

radius-server host コマンドで登録した RADIUS サーバの設定が使用されます。

radius-server host コマンドが登録されていない場合は，RADIUS サーバを使用しないで，内蔵 MAC 認証 DB を使用して認証を行います。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本コマンドが設定されている場合，MAC 認証で参照する RADIUS サーバの設定情報は，radius-server host コマンドで設定されている情報よりも優先されます。（radius-server host コマンド設定は適用されません）。汎用 RADIUS サーバ情報，MAC 認証専用 RADIUS サーバ情報の設定については，「コンフィグレーションガイド Vol.2」を参照してください。
4. 設定可能な MAC 認証専用 RADIUS サーバ数は装置単位で最大 4 です。
5. IPv4 アドレスとして 127.*.*.* を設定できません。
6. key パラメータが省略されていて，radius-server key コマンドも設定されていない場合は，当該 RADIUS サーバは無効になります。
7. 複数の MAC 認証専用 RADIUS サーバを設定した場合，運用コマンド show radius-server で最初に表示されるアドレスがプライマリ MAC 認証専用 RADIUS サーバとなります。最初のカレントサーバ（運用中の RADIUS 認証要求先）にはプライマリ MAC 認証専用 RADIUS サーバが使用されます。プライマリ MAC 認証専用 RADIUS サーバに障害が発生した場合，カレントサーバは次に有効な MAC 認証専用 RADIUS サーバ（セカンダリ RADIUS サーバ）へ遷移します。プライマリ MAC 認証専用 RADIUS サーバへの自動復旧については mac-authentication radius-server dead-interval コマンドを参照してください。

8. 汎用 RADIUS サーバ，他の認証専用 RADIUS サーバ，または RADIUS サーバグループの設定で，IP アドレスの一致する RADIUS サーバが既に登録されている場合は，それらすべてのパラメータを自動的に新しく入力したコマンド内容に置き換えます。

［関連コマンド］

aaa authentication mac-authentication

mac-authentication port

mac-authentication system-auth-control

mac-authentication roaming

HUB などを経由して接続した認証済み端末を，リンクダウンしないでポート移動した場合の通信許可（ローミング）を設定します。

[入力形式]

情報の設定・変更

mac-authentication roaming [action trap]

情報の削除

no mac-authentication roaming

[入力モード]

(config)

[パラメータ]

[action trap]

ローミングによるポート移動を検出時に，プライベート Trap を発行します。

1. 本パラメータ省略時の初期値
   ローミングによるポート移動を検出しても，プライベート Trap を発行しません。
2. 値の設定範囲
   action trap

[コマンド省略時の動作]

認証済み端末のポート移動時の通信を許可しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 移動先がダイナミック VLAN モードの対象ポートで，移動前と同一 VLAN 内のときだけ移動後も通信可能です。
4. 本コマンド設定状態で DHCP snooping 機能併用時，認証済み端末のポートを移動すると，認証状態は移動後のポートに遷移しますが，バインディングデータベースは更新されないため通信できません。
5. プライベート Trap を発行する場合は，snmp-server host コマンドで Trap の送信先 IP アドレスと "mac-authentication" を設定しておく必要があります。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication port

snmp-server host

mac-authentication static-vlan force-authorized

RADIUS 認証方式を使用時，経路障害などで RADIUS サーバ無応答または RADIUS サーバへのリクエスト送信エラーが発生した場合に，当該ポートで認証要求した認証対象端末を強制的に認証許可状態とします。

[入力形式]

情報の設定・変更

mac-authentication static-vlan force-authorized [action trap]

情報の削除

no mac-authentication static-vlan force-authorized

[入力モード]

(config-if)

[パラメータ]

[action trap]

強制認証による認証許可時に，プライベート Trap を発行します。

1. 本パラメータ省略時の初期値
   強制認証により認証許可しても，プライベート Trap を発行しません。
2. 値の設定範囲
   action trap

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本機能はセキュリティ上の問題となる可能性がありますので，十分検討の上ご使用ください。

4. 本コマンドは次の条件で有効となります。
   - 下記のコンフィグレーションがすべて設定されていること
     - radius-server host または mac-authentication radius-server host
     - mac-authentication port ※1
     - mac-authentication static-vlan force-authorized ※1
     - mac-authentication system-auth-control
     - aaa authentication mac-authentication ※2
     - mac-authentication authentication ※3

   注※1

   同じイーサネットポートに設定してください。

   - RADIUS サーバへの送信で，下記のアカウントログが採取された場合
     No=21:

     NOTICE:LOGIN: (付加情報) Login failed ; Failed to connection to RADIUS server.
     付加情報：MAC，PORT，VLAN

     アカウントログは運用コマンド show mac-authentication logging で確認できます。

   注※2

   装置デフォルトで強制認証使用時は「default group radius」だけ設定してください。

   注※3

   ポート別認証方式で強制認証使用時は「aaa authentication mac-authentication <List name>」を設定してください。
5. 強制認証許可状態は，当該端末の認証解除とともに解除されます。
6. プライベート Trap を発行する場合は，snmp-server host コマンドで Trap の送信先 IP アドレスと "mac-authentication" を設定しておく必要があります。
7. 下記のいずれかがすでに設定されている場合，本コマンドを設定できません。
   - authentication force-authorized enable
   - authentication force-authorized vlan

［関連コマンド］

aaa authentication mac-authentication

mac-authentication port

mac-authentication system-auth-control

radius-server host または mac-authentication radius-server host

snmp-server host

mac-authentication static-vlan max-user

装置単位の最大認証端末数を設定します。

[入力形式]

情報の設定・変更

mac-authentication static-vlan max-user <Count>

情報の削除

no mac-authentication static-vlan max-user

[入力モード]

(config)

[パラメータ]

<Count>

装置単位の最大認証端末数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 1024

[コマンド省略時の動作]

装置単位の認証可能な最大認証端末数は，1024 端末になります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本設定を行った場合，現在認証中の端末はそのままですが，次回の新規端末の認証時から設定値が有効となります。
4. 装置単位とポート単位の最大認証端末数を同時に設定することも可能です。
   - 認証済み端末数がポート単位の最大認証端末数に達した場合，当該ポートで以降の新規端末の認証はできません。
   - 認証済み端末数が装置単位の最大認証端末数に達した場合，本装置で以降の新規端末の認証はできません。
5. 運用中に認証済み端末数より最大認証端末数を少なく変更した場合，認証済みの端末は継続通信できますが，新規端末の認証はできません。
6. DHCP snooping 機能を併用している場合は，最大 246 端末に制限されます。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication port

mac-authentication static-vlan max-user (interface)

当該ポートの最大認証端末数を設定します。

[入力形式]

情報の設定・変更

mac-authentication static-vlan max-user <Count>

情報の削除

no mac-authentication static-vlan max-user

[入力モード]

(config-if)

[パラメータ]

<Count>

当該ポートの最大認証端末数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 1024

[コマンド省略時の動作]

当該ポートの認証可能な最大認証端末数は，1024 端末になります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 本設定を行った場合，現在認証中の端末はそのままですが，次回の新規端末の認証時から設定値が有効となります。
4. 装置単位とポート単位の最大認証端末数を同時に設定することも可能です。
   - 認証済み端末数がポート単位の最大認証端末数に達した場合，当該ポートで以降の新規端末の認証はできません。
   - 認証済み端末数が装置単位の最大認証端末数に達した場合，本装置で以降の新規端末の認証はできません。
5. 運用中に認証済み端末数より最大認証端末数を少なく変更した場合，認証済みの端末は継続通信できますが，新規端末の認証はできません。
6. DHCP snooping 機能を併用している場合は，最大 246 端末に制限されます。

［関連コマンド］

mac-authentication system-auth-control

mac-authentication port

mac-authentication static-vlan roaming

HUB などを経由して接続した認証済み端末を，リンクダウンしないでポート移動した場合の通信許可（ローミング）を設定します。

[入力形式]

情報の設定・変更

mac-authentication static-vlan roaming [action trap]

情報の削除

no mac-authentication static-vlan roaming

[入力モード]

(config)

[パラメータ]

[action trap]

ローミングによるポート移動を検出時に，プライベート Trap を発行します。

1. 本パラメータ省略時の初期値
   ローミングによるポート移動を検出しても，プライベート Trap を発行しません。
2. 値の設定範囲
   action trap

[コマンド省略時の動作]

認証済み端末のポート移動時の通信を許可しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 移動先が固定 VLAN モード対象ポートで，移動前と同一 VLAN 内のときだけ，移動後も通信可能です。
4. 本コマンド設定状態で DHCP snooping 機能併用時，認証済み端末のポートを移動すると，認証状態は移動後のポートに遷移しますが，バインディングデータベースは更新されないため通信できません。
5. プライベート Trap を発行する場合は，snmp-server host コマンドで Trap の送信先 IP アドレスと "mac-authentication" を設定しておく必要があります。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication port

snmp-server host

mac-authentication system-auth-control

MAC 認証を有効にします。

なお，no mac-authentication system-auth-control を実行した場合は，MAC 認証を停止します。

[入力形式]

情報の設定

mac-authentication system-auth-control

情報の削除

no mac-authentication system-auth-control

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

MAC 認証を行いません。

[通信への影響]

no mac-authentication system-auth-control を実行した場合，認証済み端末の認証が解除されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
2. no mac-authentication system-auth-control を実行した場合でも，内蔵 MAC 認証 DB に登録された端末情報はそのまま保存されます。

[関連コマンド]

なし

mac-authentication timeout quiet-period

認証失敗時に，同一端末（MAC アドレス）の認証を再開しない時間（認証再開猶予タイマ）を設定します。本時間内は，認証処理を行いません。

[入力形式]

情報の設定・変更

mac-authentication timeout quiet-period <Seconds>

情報の削除

no mac-authentication timeout quiet-period

[入力モード]

(config)

[パラメータ]

<Seconds>

認証再開猶予タイマを秒単位で指定します。認証失敗時にすぐに認証処理を再開したい場合は，0 を設定してください。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0，60 ～ 86400（秒）

[コマンド省略時の動作]

MAC 認証失敗時，300 秒間は同一端末の認証処理を行いません。

[通信への影響]

なし

[設定値の反映契機]

1. 認証に失敗したとき
2. 現在動作中の認証再開猶予タイマがタイムアウトし，タイマ値が 0 になったとき
3. 運用コマンド clear mac-authentication auth-state を実施し，認証単位または装置単位での認証解除を実施したとき

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. マルチステップ認証を使用するときは，本設定値を 0 秒以外に設定してください。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication timeout reauth-period

認証成功後，端末の再認証を行う周期を設定します。

[入力形式]

情報の設定・変更

mac-authentication timeout reauth-period <Seconds>

情報の削除

no mac-authentication timeout reauth-period

[入力モード]

(config)

[パラメータ]

<Seconds>

端末の再認証を行う周期を秒単位で指定します。0 を設定した場合は再認証を行わずに接続し続けます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0，600 ～ 86400（秒）

[コマンド省略時の動作]

端末の再認証を行う周期は 3600 秒です。

[通信への影響]

なし

[設定値の反映契機]

- 現在動作中の端末の再認証を行う周期時間がタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear mac-authentication auth-state を実行し，認証単位または装置単位での認証解除を実施したとき
- 認証済み端末が存在しない状態の認証単位で認証端末の認証が成功したとき

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication vlan

レガシーモード認証後，動的に切り替える VLAN ID を設定します。

本コマンドが設定されていない場合は，レガシーモード認証後の VLAN 切り替えが行われません。

[入力形式]

情報の設定・変更

mac-authentication vlan <VLAN ID list>

情報の削除

no mac-authentication vlan <VLAN ID list>

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

認証後に切り替える MAC VLAN の VLAN ID list を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。デフォルト VLAN（VLAN ID=1）は設定できません。

[コマンド省略時の動作]

レガシーモード認証後の動的な VLAN 切り替えが行われません。

[通信への影響]

本コマンドで VLAN を削除した場合，削除した VLAN で登録をしていた端末の認証が解除されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。
3. 設定されたすべての VLAN ID は，MAC VLAN で設定されている必要があります。
4. 本装置に下記コマンドが 1 つでも設定されている場合は，本コマンドを設定できません。
   - authentication multi-step
   - dot1x authentication
   - mac-authentication authentication
   - web-authentication authentication
   - web-authentication user-group

［関連コマンド］

mac-authentication system-auth-control

switchport mac

mac-authentication vlan-check

認証処理で MAC アドレスを照合する際，VLAN ID も照合を行います。

RADIUS 認証方式の場合は，RADIUS サーバへ認証要求時のユーザ ID として，MAC アドレス文字列と本コマンドで設定した文字列（省略時は "%VLAN"），および VLAN ID を結合したものを使用します。

ローカル認証方式の場合は，内蔵 MAC 認証 DB へ照合時に MAC アドレス文字列と VLAN ID で照合を行います。（内蔵 MAC 認証 DB に VLAN ID 情報がない場合は，MAC アドレス文字列だけで照合を行います。）

[入力形式]

情報の設定・変更

mac-authentication vlan-check [key <String>]

情報の削除

no mac-authentication vlan-check

[入力モード]

(config)

[パラメータ]

key <String>

本パラメータは，RADIUS 認証方式にだけ適用します。

RADIUS サーバへ認証要求時に，ユーザ ID に付加する文字列を設定します。

ローカル認証方式の場合は，本パラメータは無効です。

1. 本パラメータ省略時の初期値
   文字列 "%VLAN" を設定します。
2. 値の設定範囲
   1 ～ 64 文字以内で指定します。指定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

MAC 認証の照合時に，VLAN ID を付加しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての MAC 認証設定は，mac-authentication system-auth-control コマンドを設定することで有効になります。
2. 本コマンド設定が動作可能となる認証モードは，「表 23-1　コンフィグレーションコマンドと MAC 認証の認証モード」を参照してください。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication port

aaa authentication mac-authentication

24 マルチステップ認証

authentication multi-step

authentication multi-step

マルチステップ認証ポートに設定します。

[入力形式]

情報の設定・変更

authentication multi-step [{permissive | dot1x}]

情報の削除

no authentication multi-step

[入力モード]

(config-if)

[パラメータ]

{permissive | dot1x}

permissive

1 段目の MAC 認証が失敗した端末に対して，Web 認証，および IEEE802.1X 認証の両方を許可します。

dot1x

1 段目の認証として MAC 認証，および IEEE802.1X を許可します。1 段目の MAC 認証または IEEE802.1X に失敗した端末には，Web 認証を許可しません。

1. 本パラメータ省略時の初期値
   1 段目の MAC 認証が失敗した端末には，Web 認証，および IEEE802.1X の両方を許可しません。
2. 値の設定範囲
   permissive または dot1x

[コマンド省略時の動作]

シングル認証ポートとして動作します。

[通信への影響]

当該ポートの端末を認証解除します。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドは，装置に下記コマンドが 1 つでも設定されている場合には，設定できません。
   - dot1x vlan dynamic enable
   - dot1x vlan dynamic radius-vlan
   - mac-authentication interface
   - mac-authentication vlan
   - web-authentication vlan
2. 本コマンドはイーサネットインタフェースだけ設定可能です。

[関連コマンド]

なし

25 セキュア Wake on LAN【OP-WOL】

http-server【OP-WOL】

HTTP サーバ機能を有効にします。

[入力形式]

情報の設定
http-server

情報の削除
no http-server

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

web-authentication system-auth-control コマンド設定あり：有効

web-authentication system-auth-control コマンド設定なし：無効

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドの設定で，セキュア Wake on LAN のユーザ認証画面と，Web 認証のログイン画面の表示が有効となります。
2. web-authentication system-auth-control コマンドの設定でも，セキュア Wake on LAN のユーザ認証画面と，Web 認証のログイン画面の表示が有効となります。
3. web-authentication system-auth-control コマンドを設定すると，Web 認証機能の動作も有効になります。従って，セキュア Wake on LAN 機能だけをご使用のときは，本コマンドだけの設定をお勧めします。
4. 本コマンドと web-authentication system-auth-control コマンドを同時に設定しても，セキュア Wake on LAN 機能の動作には影響ありません。コマンド設定の組み合わせについては次の表を参照してください。

コンフィグレーション設定		セキュア Wake on LAN		Web 認証	
http-server	web-authentication system-auth-control	ユーザ認証画面	機能	ログイン画面	機能
未設定	未設定	非表示	動作しません	非表示	動作しません
	設定	表示可能	動作します	表示可能	動作します
設定	未設定	表示可能	動作します	表示可能	動作しません
	設定	表示可能	動作します	表示可能	動作します

[関連コマンド]

なし

26 DHCP snooping

ip arp inspection limit rate

本装置で DHCP snooping 機能を有効時に，当該ポートでの ARP パケット受信レート（1 秒当たりに受信可能な ARP パケット数）を設定します。受信レートを超えた ARP パケットは廃棄されます。

[入力形式]

情報の設定・変更

ip arp inspection limit rate <Packet/s>

情報の削除

no ip arp inspection limit rate

[入力モード]

(config-if)

[パラメータ]

<Packet/s>

1 秒当たりに受信可能な ARP パケット数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 〜 300（Packet/s)

[コマンド省略時の動作]

受信レートは無制限となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定したポートに，ip arp inspection trust コマンドが設定されている場合は，本コマンドの設定は無効となり，ARP パケットの受信レートは無制限となります。
2. 本コマンドで指定した値は，受信パケット数の上限値を設定するものであり，指定値まで動作保証するものではありません。

[関連コマンド]

ip dhcp snooping

ip arp inspection trust

本装置で DHCP snooping 機能を有効時に，当該インタフェースをダイナミック ARP 検査を実施しない trust ポートとして設定します。

[入力形式]

情報の設定

ip arp inspection trust

情報の削除

no ip arp inspection trust

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

ダイナミック ARP 検査を実施します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定されたインタフェースでは，ダイナミック ARP 検査機能が有効化されている VLAN に収容されていても，ダイナミック ARP 検査を実施しません。
2. 本コマンドを設定したインタフェースの ARP パケット受信レートは無制限となります。

[関連コマンド]

ip dhcp snooping

ip dhcp snooping vlan

ip arp inspection validate

本装置でダイナミック ARP 検査機能を有効時，ダイナミック ARP 検査の精度を高めるために追加する検査項目を設定します。

[入力形式]

情報の設定・変更

ip arp inspection validate <item> [<item> [<item>]]

情報の削除

no ip arp inspection validate

[入力モード]

(config)

[パラメータ]

<item> [<item> [<item>]]

検査項目を <item> に指定します。

<item> には次の src-mac，dst-mac，ip のうち一つまたは二つ選択，またはすべてを設定します。同一の item は複数設定できません。

src-mac

受信 ARP パケットの送信元 MAC アドレス (Source MAC) と，発信者 MAC アドレス (Sender MAC Address) が同一であることを検査します。ARP Request，ARP Reply の両方に対して実施します。

dst-mac

受信 ARP パケットの宛先 MAC アドレス (Destination MAC) と，対象者 MAC アドレス (Target MAC Address) が同一であることを検査します。ARP Reply に対して実施します。

ip

受信 ARP パケットの対象者 IP アドレス（Target IP Address）が，下記の範囲内であることを検査します。

- 1.0.0.0 ～ 126.255.255.255
- 128.0.0.0 ～ 223.255.255.255

ARP Reply に対して実施します。

1. 本パラメータ省略時の初期値
   どれか一つは設定する必要があります。省略した項目は検査しません。
2. 値の設定範囲
   src-mac，dst-mac，ip

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンド入力時，全パラメータを省略することはできません。いずれか１つ以上設定してください。

[関連コマンド]

ip dhcp snooping

ip dhcp snooping vlan

ip arp inspection vlan

ip arp inspection vlan

本装置で DHCP snooping 機能を有効時に，ダイナミック ARP 検査機能の検査対象 VLAN を設定します。

[入力形式]

情報の設定・変更

ip arp inspection vlan { <VLAN ID list> | add <VLAN ID list> | remove <VLAN ID list > }

情報の削除

no ip arp inspection vlan

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

ダイナミック ARP 検査機能の検査対象 VLAN ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

add <VLAN ID list>

ダイナミック ARP 検査機能の検査対象 VLAN ID を VLAN リストに追加します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

remove <VLAN ID list>

ダイナミック ARP 検査機能で検査対象の VLAN ID を VLAN リストから削除します。

1. 本パラメータ省略時の初期値。
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

ダイナミック ARP 検査機能が動作しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ip dhcp snooping vlan コマンドで設定している VLAN ID を設定してください。
2. 本コマンドを設定した場合は，ip source binding コマンドで登録したバインディングデータベースエントリも，ダイナミック ARP 検査の対象となります。
3. 本コマンドで設定した VLAN が，ip arp inspection trust コマンドを設定したポートに収容されている場合は，ダイナミック ARP 検査は実施されません。

[関連コマンド]

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping

本装置で DHCP snooping 機能を有効にします。

[入力形式]

情報の設定
ip dhcp snooping

情報の削除
no ip dhcp snooping

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

system function コマンド設定有で dhcp-snooping が設定されていない場合，本コマンドは設定できません。(system function コマンドが未設定の場合は，設定できます。)【SS1250】【SS1240】

[関連コマンド]

なし

ip dhcp snooping database url

バインディングデータベースの保存先を設定します。

[入力形式]

情報の設定・変更

ip dhcp snooping database url { flash | mc <File name> }

情報の削除

no ip dhcp snooping database url

[入力モード]

(config)

[パラメータ]

flash

内蔵フラッシュメモリに保存します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   flash

mc <File name>

MC に保存します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <File name>：最大 64 文字まで設定できます。
   運用コマンドで MC にディレクトリを作成している場合は，ディレクトリ名を含めて最大 64 文字まで設定できます。
   設定可能な文字は，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

バインディングデータベースを保存しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ip dhcp snooping database write-delay コマンドで設定した書き込み指定時間は，下記のいずれかを保存契機としてタイマをスタートし，タイマを満了後にバインディングデータベースを保存します。
   - ダイナミックのバインディングデータベースの登録・更新・削除時
   - ip dhcp snooping database url コマンド設定時（保存先の変更を含む）
   - 運用コマンド clear ip dhcp snooping binding 実行時

   タイマを満了する前に装置電源断などが発生した場合は，バインディングデータベースを保存できません。
2. no ip dhcp snooping database url コマンドを入力した場合は，ip dhcp snooping database write-delay コマンドで設定した時間のタイマがスタートしていても，バインディングデータベースを保存しません。

[関連コマンド]

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping database write-delay

バインディングデータベース保存時の書き込み指定時間を設定します。

[入力形式]

情報の設定・変更

ip dhcp snooping database write-delay <Seconds>

情報の削除

no ip dhcp snooping database write-delay

[入力モード]

(config)

[パラメータ]

<Seconds>

バインディングデータベース保存時の書き込み指定時間を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1800 ～ 86400 （秒）

[コマンド省略時の動作]

ip dhcp snooping database url 設定時，1800 秒で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，次回の保存契機から運用に反映されます。

[注意事項]

1. 本コマンドで設定した書き込み指定時間は，下記のいずれかを保存契機としてタイマをスタートし，タイマを満了後にバインディングデータベースを保存します。
   - ダイナミックのバインディングデータベースの登録・更新・削除時
   - ip dhcp snooping database url コマンド設定時（保存先の変更を含む）
   - 運用コマンド clear ip dhcp snooping binding 実行時

   タイマを満了する前に装置電源断などが発生した場合は，バインディングデータベースを保存できません。
2. no ip dhcp snooping database url コマンドを入力した場合は，本コマンドで設定した時間のタイマがスタートしていても，バインディングデータベースを保存しません。

[関連コマンド]

ip dhcp snooping

ip dhcp snooping database url

ip dhcp snooping vlan

ip dhcp snooping information option allow-untrusted

信頼されていないポート（untrust ポート）でオプション [82] 情報を持った DHCP パケットの受信を許可する場合に設定します。本設定を行わない場合は，オプション [82] 情報を持った DHCP パケットを廃棄します。

[入力形式]

情報の設定

ip dhcp snooping information option allow-untrusted

情報の削除

no ip dhcp snooping information option allow-untrusted

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ip dhcp snooping

ip dhcp snooping limit rate

当該ポートで，DHCP パケットの受信レート（１秒当たりに受信可能な DHCP パケット数）を設定します。受信レートを超えた DHCP パケットは廃棄されます。

［入力形式］

情報の設定・変更

ip dhcp snooping limit rate <Packet/s>

情報の削除

no ip dhcp snooping limit rate

［入力モード］

(config-if)

［パラメータ］

<Packet/s>

１秒当たりに受信可能な DHCP パケット数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 300 （Packet/s)

［コマンド省略時の動作］

受信レートは無制限となります。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. 本コマンドを設定したポートに，ip dhcp snooping trust コマンドが設定されている場合は，本コマンドの設定は無効となり，DHCP パケットの受信レートは無制限となります。
2. 本コマンドで指定した値は，受信パケット数の上限値を設定するものであり，指定値まで動作保証するものではありません。

［関連コマンド］

ip dhcp snooping

ip dhcp snooping trust

インタフェースが信頼されているポート（trust ポート）か，信頼されていないポート（untrust ポート）かを設定します。

[入力形式]

情報の設定
　ip dhcp snooping trust

情報の削除
　no ip dhcp snooping trust

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

当該インタフェースは信頼されていないポート（untrust ポート）として動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

本コマンドを設定したインタフェースでは，DHCP snooping が有効になっている VLAN に収容されていても，DHCP パケットの検査を実施しません。

[関連コマンド]

ip dhcp snooping

ip dhcp snooping verify mac-address

信頼されていないポート（untrust ポート）から受信した DHCP パケットの送信元 MAC アドレスと DHCP パケット内のクライアントハードウェアアドレスの一致をチェックするか否かを設定します。

[入力形式]

情報の設定

no ip dhcp snooping verify mac-address

情報の削除

ip dhcp snooping verify mac-address

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

送信元 MAC アドレスとクライアントハードウェアアドレスが一致するかチェックします。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

本コマンド未設定の場合，MAC アドレスのチェックを実施するため，untrust ポートに DHCP リレーエージェントを接続できなくなります。（DHCP リレーエージェント経由の場合は，送信元 MAC アドレスが書き換えられています。）

[関連コマンド]

ip dhcp snooping

ip dhcp snooping vlan

VLAN での DHCP snooping を有効にします。本コマンドで設定しない場合は DHCP snooping は無効です。本コマンドで設定できる VLAN 数は最大 32 個です。

[入力形式]

情報の設定・変更

ip dhcp snooping vlan <VLAN ID list>

情報の削除

no ip dhcp snooping vlan <VLAN ID list>

[入力モード]

(config)

[パラメータ]

<VLAN ID list>

DHCP snooping を有効にする VLAN ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

本コマンドを設定しない VLAN では，DHCP snooping は無効です。

[関連コマンド]

ip dhcp snooping

ip source binding

バインディングデータベースに static 設定します。

［入力形式］

情報の設定

ip source binding <MAC> vlan <VLAN ID> <IP address> interface { gigabitethernet <IF#> | port-channel <Channel group#> } 【S2200】【S2100】

ip source binding <MAC> vlan <VLAN ID> <IP address> interface { fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#> }【SS1250】【SS1240】

情報の削除

no ip source binding <MAC> vlan <VLAN ID> <IP address> interface {gigabitethernet <IF#> | port-channel <Channel group#> }【S2200】【S2100】

no ip source binding <MAC> vlan <VLAN ID> <IP address> interface { fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#> }【SS1250】【SS1240】

［入力モード］

(config)

［パラメータ］

<MAC>

端末の MAC アドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0000.0000.0000 ～ ffff.ffff.ffff

<VLAN ID>

端末が接続されている VLAN ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

<IP address>

端末の IP アドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

interface { gigabitethernet <IF#> | port-channel <Channel group#> }【S2200】【S2100】

interface { fastethernet <IF#> | gigabitethernet <IF#> | port-channel <Channel group#> }【SS1250】【SS1240】

端末が接続されているインタフェース番号を設定します。

1. 本パラメータ省略時の初期値
   省略できません。

2. 値の設定範囲
「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

設定可能エントリ数は最大 64 件です。ただし，設定時にバインディングデータベースのエントリ数がダイナミックエントリを含めて最大エントリ数を超える場合は設定できません。

[関連コマンド]

ip dhcp snooping

ip dhcp snooping vlan

ip verify source

DHCP snooping バインディングデータベースを基に，端末フィルタを実施する場合に設定します。（端末フィルタ：登録されていない送信元 IP アドレスと送信元 MAC アドレスのパケットをフィルタする機能。）

[入力形式]

情報の設定・変更
　ip verify source [{ port-security | mac-only }]

情報の削除
　no ip verify source

[入力モード]

(config-if)

[パラメータ]

{ port-security | mac-only }

端末フィルタ条件を設定します。

port-security

送信元 IP アドレスと送信元 MAC アドレスで端末フィルタを実施します。

mac-only

送信元 MAC アドレスだけで端末フィルタを実施します。

1. 本パラメータ省略時の初期値
送信元 IP アドレスだけで端末フィルタを実施します。
2. 値の設定範囲
なし

[コマンド省略時の動作]

なし

[通信への影響]

端末フィルタを設定した場合，バインディングデータベースに未登録の端末からのパケットは，VLAN に関係なく廃棄されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 信頼されているポート（trust ポート）では，本コマンドを設定していても端末フィルタ機能は無効です。
2. DHCP snooping 有効時に本設定を行う場合，DHCP snooping が無効な VLAN でも端末フィルタ機能が有効になりますのでご注意ください。

[関連コマンド]

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping trust

ip source binding

27 特定端末への Web 通信不可表示機能【S2100】

access-redirect http port

特定端末への Web 通信不可表示機能で使用する TCP ポート番号を指定します。

[入力形式]

情報の設定・変更
access-redirect http port [<Port 1> [<Port 2>]]

情報の削除
no access-redirect http port

[入力モード]

(config)

[パラメータ]

<Port 1> [<Port 2>]

特定端末への Web 通信不可表示機能で使用する宛先 TCP ポート番号を指定します。最大 2 個まで指定できます。
2 個指定するときは異なる TCP ポート番号としてください。

1. 本パラメータ省略時の初期値
   80
2. 値の設定範囲
   0 ～ 65535

[コマンド省略時の動作]

特定端末への Web 通信不可表示機能が動作しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ip access-group

access-redirect http target

アクセスリストの特定 deny エントリに該当した HTTP パケットに対してのリダイレクト先を指定します。

[入力形式]

情報の設定・変更

access-redirect http target <URL>

情報の削除

no access-redirect http target

[入力モード]

(config)

[パラメータ]

<URL>

リダイレクト先の URL を指定します。

URL の入力は先頭文字（例えば，"http:// ～ "）から設定してください。（下記の（設定例）を参照してください。）

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   256 文字以内の文字列で指定してください。入力可能な文字は「パラメータに指定できる値」の「任意の文字列」を参照してください。
   （設定例）
   (config)# access-redirect http target "http://www.example.com/"

[コマンド省略時の動作]

アクセスリストの特定 deny エントリに該当したパケットの送信元端末に対して，Web 通信不可表示画面を直接応答します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 指定 URL をそのままリダイレクト先として使用します。必要に応じて URL エンコーディングを行ってください。不正な URL を指定してもエラーになりません。

[関連コマンド]

access-redirect http port

access-redirect timeout

TCP 接続後，指定時間以内に HTTP 要求ヘッダの受信が完了しない場合に，TCP コネクションを切断する時間を変更します。

[入力形式]

情報の設定・変更
access-redirect timeout <Milli seconds>

情報の削除
no access-redirect timeout

[入力モード]

(config)

[パラメータ]

<Milli seconds>
TCP コネクションを切断する時間をミリ秒単位で設定します。

1. 本パラメータ省略時の初期値
省略できません。
2. 値の設定範囲
500 ～ 8000 の値で 100 の倍数（ミリ秒）

[コマンド省略時の動作]

TCP コネクションを切断する時間は 1 秒です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

access-redirect http port

28 アップリンク・リダンダント

switchport backup interface

プライマリ・セカンダリポートと自動切り戻し時間，またはタイマ切り戻し時間を設定します。

[入力形式]

情報の設定・変更

switchport backup interface {gigabitethernet <IF#> | port-channel <Channel group#>} [preemption delay <Seconds>]【S2200】【S2100】

switchport backup interface {{fastethernet | gigabitethernet} <IF#> | port-channel <Channel group#>} [preemption delay <Seconds>]【SS1250】【SS1240】

情報の削除

no switchport backup interface

[入力モード]

(config-if)

[パラメータ]

{gigabitethernet <IF#> | port-channel <Channel group#>}【S2200】【S2100】

{{fastethernet | gigabitethernet} <IF#> | port-channel <Channel group#>}【SS1250】【SS1240】

セカンダリポートを指定します。本コマンドを設定するポートがプライマリポートになります。指定できるインタフェースは，イーサネットまたはポートチャネルです。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF#>：「パラメータに指定できる値」を参照してください。
   <Channel group#>：「パラメータに指定できる値」を参照してください。

preemption delay <Seconds>

自動切り戻し時間，またはタイマ切り戻し時間を設定します。

時間を設定することで自動切り戻し，またはタイマ切り戻しが有効となります。

1. 本パラメータ省略時の初期値
   運用コマンド select switchport backup interface による手動切り戻しとなります。
2. 値の設定範囲
   0（秒）：自動切り戻し
   1 ～ 300（秒）：タイマ切り戻し

[コマンド省略時の動作]

アップリンク・リダンダントは無効です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 上位スイッチでスパニングツリーを使用しているときは，リンクダウンから復帰すると「Listening」または「Learning」状態となり，すぐには通信することができません。このような時はタイマ切り戻し時間を 30 秒以上で設定することをお勧めします。

[関連コマンド]

なし

switchport backup flush request transmit

上位スイッチへ MAC アドレステーブルクリアを要求するフラッシュ制御フレーム送信を設定します。

[入力形式]

情報の設定・変更

switchport backup flush request transmit [vlan <VLAN ID>]

情報の削除

no switchport backup flush request transmit

[入力モード]

(config-if)

[パラメータ]

vlan <VLAN ID>

フラッシュ制御フレームに付加する VLAN Tag 値を指定します。

1. 本パラメータ省略時の初期値
   Untagged フレームでフラッシュ制御フレームを送信します。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

フラッシュ制御フレームを送信しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. フラッシュ制御フレーム送信設定で VLAN Tag 値を指定したときは，該当ポートがアクセスポートのときも Tagged フレームでフラッシュ制御フレームを送信します。
2. 本コマンドは，プライマリポートに設定してください。

[関連コマンド]

switchport backup interface

switchport backup mac-address-table update exclude-vlan

MAC アドレスアップデートフレーム送信時に対象から除外する VLAN を設定します。

[入力形式]

情報の設定・変更

switchport backup mac-address-table update exclude-vlan <VLAN ID list>

情報の削除

no switchport backup mac-address-table update exclude-vlan

[入力モード]

(config-if)

[パラメータ]

<VLAN ID list>

MAC アドレスアップデートフレーム送信時に対象から除外する VLAN リストを設定します。

再度入力した場合は，上書きします。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID list> の設定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

プライマリポートに含まれる全 VLAN が MAC アドレスアップデートフレーム送信の対象となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 対象から除外する VLAN パラメータの設定数は最大 200 です。
   "4 つ " 設定した例
   switchport backup mac-address-table update exclude-vlan 10-20,25-30
   VLAN リストを "-" で指定する場合は，上下の値で "2 つ " とカウントします。
2. 本コマンドは，switchport backup mac-address-table update transmit コマンドを設定することで有効となります。
3. 本コマンドは，プライマリポートに設定してください。

[関連コマンド]

switchport backup interface

switchport backup mac-address-table update transmit

switchport backup mac-address-table update retransmit

MAC アドレスアップデートフレームの再送回数を設定します。

[入力形式]

情報の設定・変更

switchport backup mac-address-table update retransmit <Count>

情報の削除

no switchport backup mac-address-table update retransmit

[入力モード]

(config-if)

[パラメータ]

<Count>

プライマリポート・セカンダリポートの切り替え時に MAC アドレスアップデートフレームの再送回数を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 3（回）

[コマンド省略時の動作]

MAC アドレスアップデートフレームを再送信しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. MAC アドレスアップデートフレーム送信中に設定を変更した場合は，次の送信を契機に設定値を反映します。
2. 本コマンドは，switchport backup mac-address-table update transmit コマンドを設定することで有効となります。
3. 本コマンドは，プライマリポートに設定してください。

[関連コマンド]

switchport backup interface

switchport backup mac-address-table update transmit

switchport backup mac-address-table update transmit

上位スイッチへ MAC アドレステーブルを更新させる MAC アドレスアップデートフレーム送信を設定します。

[入力形式]

情報の設定
　switchport backup mac-address-table update transmit

情報の削除
　no switchport backup mac-address-table update transmit

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

MAC アドレスアップデートフレームを送信しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドは，プライマリポートに設定してください。

[関連コマンド]

switchport backup interface

switchport-backup startup-active-port-selection

装置起動時のアクティブポート固定機能を有効にします。

[入力形式]

情報の設定

switchport-backup startup-active-port-selection primary-only

情報の削除

no switchport-backup startup-active-port-selection

[入力モード]

(config)

[パラメータ]

primary-only

装置起動時に，プライマリポートだけをアクティブポートに設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   primary-only

[コマンド省略時の動作]

装置起動時，セカンダリポートもアクティブポートの選択対象として動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映され，その後の装置起動時に適用されます。

[注意事項]

1. 本コンフィグレーションを削除しても，装置起動時のアクティブポート固定機能が動作しているアップリンクポートは，プライマリポートがリンクアップするまでアクティブポートが無い状態になります。
2. 装置起動時のアクティブポート固定機能が動作しているアップリンクポートで，アクティブポート固定機能が解除される条件は次のとおりです。
   - プライマリポートのリンクアップ
   - 運用コマンド select switchport backup interface でアクティブポートをセカンダリポートに切り替え

[関連コマンド]

なし

29 IEEE 802.3ah/UDLD

efmoam active

IEEE 802.3ah/OAM 機能の監視対象ポートを Active モードに設定します。

[入力形式]

情報の設定・変更

efmoam active [udld]

情報の削除

no efmoam active

[入力モード]

(config-if)

[パラメータ]

udld

当該ポートを IEEE802.3ah/UDLD 機能の監視ポートとし，片方向リンク障害検出機能を有効にします。

1. 本パラメータ省略時の初期値
   当該ポートでは片方向リンク障害検出機能を行いません。
2. 値の設定範囲
   なし

[コマンド省略時の動作]

当該ポートは片方向リンク障害検出を行わないで，Passive モードで動作します。

[通信への影響]

機能有効にした結果，回線障害を検出した場合，当該ポートを inactive 状態とします。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 接続された双方のポートで udld パラメータが設定されない場合，本機能でのリンク障害検出を働かせることができません。

[関連コマンド]

なし

efmoam disable

装置として IEEE 802.3ah/OAM 機能を有効にするか無効にするかを設定します。

IEEE 802.3ah/OAM 機能を無効に設定する場合，efmoam disable コマンドを設定します。

IEEE 802.3ah/OAM 機能を再び有効にする場合，no efmoam disable コマンドを設定します。

Passive モードでは，Active モードからの OAMPDU の受信を契機に送信プロセスを開始します。

[入力形式]

情報の設定
efmoam disable

情報の削除
no efmoam disable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

IEEE 802.3ah/OAM 機能が動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

efmoam udld-detection-count

IEEE802.3ah/UDLD 機能の監視パケットである OAMPDU の応答タイムアウトが発生した場合に，障害と認識する回数を設定します。

[入力形式]

情報の設定・変更

efmoam udld-detection-count <Count>

情報の削除

no efmoam udld-detection-count

[入力モード]

(config)

[パラメータ]

<Count>

OAMPDU の応答タイムアウトが繰り返される場合に，回線の障害と判断する回数を設定します。回数に達した時に当該ポートを inactive 状態とします。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   3 ～ 300（回）

[コマンド省略時の動作]

応答タイムアウト判断回数は 30 回に設定されます。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 初期値より小さい回数を設定すると，片方向リンク障害を誤検出するおそれがあります。

[関連コマンド]

なし

30 ストームコントロール

storm-control

storm-control

回線のストームコントロール機能を設定します。本機能は，本装置が受信するフラッディング対象フレームの閾値を設定し，ブロードキャストストームなどが発生したときに閾値を超えるフラッディング対象フレームを廃棄することで，ネットワークおよび本装置の負荷を下げることができます。

ストームを検出したとき以下の動作を指定できます。

- 受信フレーム数のストーム検出閾値（上限閾値），ストーム回復閾値，流量制限値（下限閾値）
- 対象ポートの閉塞，または受信フレームの流量制限
- 流量制限解除監視時間
- SNMP Trap の発行や運用ログの出力

[入力形式]

情報の設定・変更

storm-control broadcast level pps <Packet/s 1> [<Packet/s 2>]
storm-control multicast level pps <Packet/s 1> [<Packet/s 2>]
storm-control unicast level pps <Packet/s 1> [<Packet/s 2>]
storm-control action { inactivate | filter }
storm-control action trap
storm-control action log
storm-control filter-broadcast <Packet/s>
storm-control filter-multicast <Packet/s>
storm-control filter-unicast <Packet/s>
storm-control filter-recovery-time <Seconds>

情報の削除

no storm-control broadcast
no storm-control multicast
no storm-control unicast
no storm-control action { inactivate | filter }
no storm-control action trap
no storm-control action log
no storm-control filter-broadcast
no storm-control filter-multicast
no storm-control filter-unicast
no storm-control filter-recovery-time

[入力モード]

(config-if)

[パラメータ]

broadcast

ブロードキャストフレームをストームコントロールの対象にします。

1. 本パラメータ省略時の初期値
   ストームコントロール機能を設定しません。

multicast

マルチキャストフレームをストームコントロールの対象にします。

1. 本パラメータ省略時の初期値

ストームコントロール機能を設定しません。

unicast

ユニキャストフラッディングフレームをストームコントロールの対象にします。

1. 本パラメータ省略時の初期値
   ストームコントロール機能を設定しません。

level pps <Packet/s 1> [<Packet/s 2>]

<Packet/s 1>：ストームコントロールを行う受信フレーム数のストーム検出閾値（上限閾値）を設定します。ストーム検出閾値を超えたフレームは廃棄します。0 を設定した場合は，対象とするフレームをすべて廃棄します。

<Packet/s 2>：ストームが発生した後，ストームが回復したと判断する値（ストーム回復閾値）を設定します。省略すると，ストーム回復閾値はストーム検出閾値で動作します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 10000000（ストーム回復値は，ストーム検出閾値以下の値を設定してください）

action { inactivate | filter }

ストームの発生を検出したときの動作を設定します。

inactivate

対象ポートを inactive 状態にします。対象ポートがチャネルグループに所属している場合は，チャネルグループに所属している全ポートを inactive 状態にします。本パラメータを設定し，ストームの発生を検出してポートを inactive 状態にするときは，action log の設定に関係なく必ずメッセージを出力するので，action log の設定は不要です。SNMP trap の発行は action trap の設定に従います。

filter

対象ポートから受信するフレームを流量制限します。対象ポートがチャネルグループに所属している場合でも，対象ポートだけを制限します。

1. 本パラメータ省略時の初期値
   ストームの発生を検出した場合，ストーム検出閾値を超えたフレームの廃棄だけを行い，ポートの状態は変更しません。
2. 値の設定範囲
   inactivate または filter

action trap

ストームの発生，終結を検出した場合に，SNMP trap を発行します。

1. 本パラメータ省略時の初期値
   ストームの発生を検出した場合，SNMP trap は発行しません。

action log

ストームの発生，終結を検出した場合に，運用ログを出力します。

1. 本パラメータ省略時の初期値
   ストームの発生を検出した場合，運用ログを出力しません。

filter-broadcast <Packet/s>

ブロードキャストフレームを流量制限するときに，中継するブロードキャストフレーム数の流量制限値（下限閾値）を設定します。流量制限値を超えたフレームは廃棄します。0 を設定した場合は，対象とするフレームをすべて廃棄します。

1. 本パラメータ省略時の初期値

流量制限時，ブロードキャストフレームをすべて廃棄します。
2. 値の設定範囲
0 ～ 10000000

filter-multicast <Packet/s>

マルチキャストフレームを流量制限するときに，中継するマルチキャストフレーム数の流量制限値（下限閾値）を設定します。流量制限値を超えたフレームは廃棄します。0 を設定した場合は，対象とするフレームをすべて廃棄します。
1. 本パラメータ省略時の初期値
流量制限時，マルチキャストフレームをすべて廃棄します。
2. 値の設定範囲
0 ～ 10000000

filter-unicast <Packet/s>

ユニキャストフラッディグフレームを流量制限するときに，中継するユニキャストフラッディグフレーム数の流量制限値（下限閾値）を設定します。流量制限値（下限閾値）を超えたフレームは廃棄します。0 を設定した場合は，対象とするフレームをすべて廃棄します。
1. 本パラメータ省略時の初期値
流量制限時，ユニキャストフラッディグフレームをすべて廃棄します。
2. 値の設定範囲
0 ～ 10000000

filter-recovery-time <Seconds>

ストームを検出して流量制限を開始し，受信フレーム数がストーム回復閾値以下になってから流量制限を解除するまでの時間（流量制限解除監視時間）を設定します。
1. 本パラメータ省略時の初期値
初期値は 1 秒です。
2. 値の設定範囲
1 ～ 30（秒）

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ストームコントロールは受信フレーム数で制御され，フレーム長には関係しません。
2. 受信フレームがストーム検出閾値を超えた場合，制御フレームも廃棄されます。必要な制御フレームが廃棄されないようにするためには，極端に小さい値を設定しないでください。
3. storm-control action で設定した動作は，受信フレーム数が storm-control broadcast，storm-control multicast または storm-control unicast で設定したストーム検出閾値を超えた場合にストームの検出とし，ストーム検出後に受信フレーム数がストーム検出閾値を下回ったときにストームが回復したと判定します。ストーム検出閾値を設定していない場合は storm-control action で設定した動作が実行されません。
4. storm-control action inactivate を設定し，ストームを検出してポートが inactive 状態となった場合，

ポートを active 状態にするためには運用コマンド activate を使用します。また，ストームを検出したときにポートが inactive 状態となり，フレームを受信しなくなるので，ストームの終結が検出できなくなります。

5. SNMP Trap を使用する場合，snmp-server host コマンドで Trap の送信先 IP アドレスと "storm-control" を設定しておく必要があります。

[関連コマンド]

snmp-server host

31 L2 ループ検知

loop-detection

L2 ループ検知のポート種別を設定します。

[入力形式]

情報の設定・変更

loop-detection { send-inact-port | send-port | uplink-port | exception-port }

情報の削除

no loop-detection

[入力モード]

(config-if)

[パラメータ]

{ **send-inact-port** | **send-port** | **uplink-port** | **exception-port** }

send-inact-port

検知送信閉塞ポートに設定します。L2 ループ検知フレームを送信し，自装置からの L2 ループ検知フレームを受信すると，ログを出力しポートを閉塞します。

send-port

検知送信ポートに設定します。L2 ループ検知フレームを送信し，自装置からの L2 ループ検知フレームを受信すると，ログを出力します。

uplink-port

アップリンクポートに設定します。L2 ループ検知フレームは送信しません。自装置からの L2 ループ検知フレームを受信すると，フレーム送信元でログを出力します。フレーム送信元のポート種別が検知送信閉塞ポートの場合は，送信元ポートを閉塞します。

exception-port

L2 ループ検知対象外ポートに設定します。L2 ループ検知フレームを受信しても何も動作を行いません。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   send-inact-port，send-port，uplink-port，exception-port

[コマンド省略時の動作]

検知ポートとして動作します。L2 ループ検知フレームは送信しないで，自装置からの L2 ループ検知フレームを受信すると，ログを出力します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. ポート種別の変更によって，下記の情報がクリアされます。

- ポート閉塞までの L2 ループ検知回数
- ポート閉塞から自動復旧までの時間

2. ポート種別を変更しても，ポートごとの L2 ループ検知フレーム送受信の統計情報はクリアしません。

[関連コマンド]

loop-detection enable

loop-detection auto-restore-time

閉塞したポートを，自動的に active 状態にする時間を設定します。

[入力形式]

情報の設定・変更

loop-detection auto-restore-time <Seconds>

情報の削除

no loop-detection auto-restore-time

[入力モード]

(config)

[パラメータ]

<Seconds>

閉塞したポートを，自動的に active 状態にする時間を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   60 ～ 86400 （秒）

[コマンド省略時の動作]

閉塞したポートは自動的に active 状態になりません。

[通信への影響]

なし

[設定値の反映契機]

設定値更新後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定した状態でパラメータを変更した場合，自動的に active 状態になるまでの待ち時間が残っていれば，残り時間をいったんクリアしたあとに，変更後の値が運用に反映されます。

[関連コマンド]

loop-detection enable

loop-detection enable

L2 ループ検知を有効にします。

[入力形式]

情報の設定
　loop-detection enable

情報の削除
　no loop-detection enable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

L2 ループ検知は無効です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

loop-detection hold-time

ポート閉塞までの L2 ループ検知回数の保持時間を設定します。

最後に L2 ループ検知フレームを受信後，L2 ループ検知フレームを受信しないで保持時間を経過した場合，そのポートで保持していた L2 ループ検知回数をクリアします。

[入力形式]

情報の設定・変更

loop-detection hold-time <Seconds>

情報の削除

no loop-detection hold-time

[入力モード]

(config)

[パラメータ]

<Seconds>

L2 ループ検知回数の保持時間を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 86400 （秒）

[コマンド省略時の動作]

L2 ループ検知回数を保持し続けます。

[通信への影響]

なし

[設定値の反映契機]

設定値更新後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定した状態でパラメータを変更した場合，L2 ループ検知回数の保持時間が残っていれば，残り時間をいったんクリアしたあとに，変更後の時間が運用に反映されます。

[関連コマンド]

loop-detection enable

loop-detection interval-time

L2 ループ検知フレームの送信間隔を設定します。

［入力形式］

情報の設定・変更

loop-detection interval-time <Seconds>

情報の削除

no loop-detection interval-time

［入力モード］

(config)

［パラメータ］

<Seconds>

L2 ループ検知フレーム送信間隔を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 3600 （秒）

［コマンド省略時の動作］

L2 ループ検知フレームの送信間隔は 10 秒です。

［通信への影響］

なし

［設定値の反映契機］

設定値更新後，すぐに運用に反映されます。

［注意事項］

なし

［関連コマンド］

loop-detection enable

loop-detection threshold

ポート閉塞までの L2 ループ検知回数を設定します。検知回数が設定回数以上となった場合，ポートを閉塞します。

[入力形式]

情報の設定・変更

loop-detection threshold <Count>

情報の削除

no loop-detection threshold

[入力モード]

(config)

[パラメータ]

<Count>

ポートを閉塞するまでの L2 ループ検知回数を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 10000

[コマンド省略時の動作]

ポート閉塞までの L2 ループ検知回数は 1 になります。

[通信への影響]

なし

[設定値の反映契機]

設定値更新後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定した状態でパラメータを変更した場合，L2 ループ検知回数を保持していれば，検知回数をいったんクリアしたあとに，変更後の値が運用に反映されます。

[関連コマンド]

loop-detection enable

32 CFM

domain name

該当ドメインで使用する名称を設定します。

[入力形式]

情報の設定・変更
domain name {no-present | str <Strings> | dns <Name> | mac <MAC> <ID>}

情報の削除
no domain name

[入力モード]

(config-ether-cfm)

[パラメータ]

{no-present | str <Strings> | dns <Name> | mac <MAC> <ID>}
ドメイン名称に使用するパラメータを設定します。

no-present
本パラメータを設定すれば，CCM 内の Maintenance Domain Name フィールドは使用されません。

str <Strings>
ドメイン名称を 43 文字以内の文字列で設定してください。

dns <Name>
ドメイン名称にドメインネームサーバ名を使用します。

mac <MAC> <ID>
ドメイン名称に MAC アドレスと 2 バイトの ID を使用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Strings> には，43 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。
   <Name> には，ホスト名を 63 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」を参照してください。
   <MAC> には 0000.0000.0000 ～ feff.ffff.ffff の値を設定します。ただし，マルチキャスト MAC アドレス（先頭バイトの最下位ビットが 1 のアドレス）は設定できません。
   <ID> には 0 ～ 65535 の値を設定します。

[コマンド省略時の動作]

no-present で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ethernet cfm domain

ethernet cfm cc alarm-priority

CC で検出する障害レベルを設定します。

設定したパラメータ以上の障害レベルが検出対象です。

［入力形式］

情報の設定・変更
　ethernet cfm cc level <Level> ma <No.> alarm-priority <Priority>

情報の削除
　no ethernet cfm cc level <Level> ma <No.> alarm-priority

［入力モード］

(config)

［パラメータ］

level <Level>

ethernet cfm domain コマンドで設定済みのドメインレベルを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 7

ma <No.>

ma コマンドで設定済みの MA 識別番号を指定します。ma name コマンドで，MA の名称を文字列または VLAN ID で指定している場合でも，MA 識別番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535

alarm-priority <Priority>

CC で検出対象となる最も低い障害レベルを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 5
   CC で検出する障害レベルと障害内容を次の表に示します。

表 32-1　CC で検出する障害レベルと障害内容

設定レベル	障害種別	コマンド表示	障害内容
5	DefXconCCM	OtherCCM	ドメイン，MA が異なる CCM を受信した
4	DefErrorCCM	ErrorCCM	MEP ID または送信間隔が誤っている CCM を受信した
3	DefRemoteCCM	Timeout	CCM を受信しなくなった
2	DefMACstatus	PortState	該当装置のポートが通信できない状態になった

設定レベル	障害種別	コマンド表示	障害内容
1	DefRDICCM	RDI	障害検出通知の CCM を受信した Remote Defect Indication
0	none	-	障害を検出しない

[コマンド省略時の動作]

障害レベル 2 以上を検出します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm cc alarm-reset-time

CC で連続して障害を検出する場合に，再検出とみなす時間を設定します。障害検出後，本コマンドで設定した時間内に検出した障害は再検出とみなし，トラップは通知しません。

ただし，現在検出している障害レベルよりも高い障害を検出した場合はトラップを通知します。

[入力形式]

情報の設定・変更

ethernet cfm cc level <Level> ma <No.> alarm-reset-time <Time>

情報の削除

no ethernet cfm cc level <Level> ma <No.> alarm-reset-time

[入力モード]

(config)

[パラメータ]

level <Level>

ethernet cfm domain コマンドで設定済みのドメインレベルを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 7

ma <No.>

ma name コマンドまたは ma vlan-group コマンドで設定済みの MA 識別番号を指定します。ma name コマンドで，MA の名称を文字列または VLAN ID で指定している場合でも，MA 識別番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535

alarm-reset-time <Time>

障害を再検出とみなすまでの時間を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   2500 ～ 10000 の値で 100 の倍数（ミリ秒）

[コマンド省略時の動作]

再検出とみなす時間は 10000 ミリ秒です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 上位レベルの MA を下位レベルの MA に含まない場合，通信負荷になる場合があります。

[関連コマンド]

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm cc alarm-start-time

CC で障害を検出してからトラップを通知するまでの時間を設定します。

[入力形式]

情報の設定・変更

ethernet cfm cc level <Level> ma <No.> alarm-start-time <Time>

情報の削除

no ethernet cfm cc level <Level> ma <No.> alarm-start-time

[入力モード]

(config)

[パラメータ]

level <Level>

ethernet cfm domain コマンドで設定済みのドメインレベルを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 7

ma <No.>

ma name コマンドまたは ma vlan-group コマンドで設定済みの MA 識別番号を指定します。ma name コマンドで，MA の名称を文字列または VLAN ID で指定している場合でも，MA 識別番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535

alarm-start-time <Time>

障害を検出してからトラップを通知するまでの時間を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   2500 ～ 10000 の値で 100 の倍数（ミリ秒）

[コマンド省略時の動作]

障害を検出してからトラップを通知するまでの時間は 2500 ミリ秒です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm cc enable

ドメインで CC を使用する MA を設定します。

ethernet cfm mep コマンドが設定済みの場合，該当ポートから CCM の送信を開始します。

［入力形式］

情報の設定

ethernet cfm cc level <Level> ma <No.> enable

情報の削除

no ethernet cfm cc level <Level> ma <No.> enable

［入力モード］

(config)

［パラメータ］

level <Level>

ethernet cfm domain コマンドで設定済みのドメインレベルを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 7

ma <No.>

ma name コマンドまたは ma vlan-group コマンドで設定済みの MA 識別番号を指定します。ma name コマンドで，MA の名称を文字列または VLAN ID で指定している場合でも，MA 識別番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535

［コマンド省略時の動作］

CC による監視を実施しません。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

なし

［関連コマンド］

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm cc interval

該当 MA の CCM 送信間隔を設定します。

[入力形式]

情報の設定・変更

ethernet cfm cc level <Level> ma <No.> interval {1s | 10s | 1min | 10min}

情報の削除

no ethernet cfm cc level <Level> ma <No.> interval

[入力モード]

(config)

[パラメータ]

level <Level>

ethernet cfm domain コマンドで設定済みのドメインレベルを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 7

ma <No.>

ma name コマンドまたは ma vlan-group コマンドで設定済みの MA 識別番号を指定します。ma name コマンドで，MA の名称を文字列または VLAN ID で指定している場合でも，MA 識別番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535

interval {1s | 10s | 1min | 10min}

CCM 送信間隔を設定します。

1s

CCM 送信間隔を 1 秒に設定します。

10s

CCM 送信間隔を 10 秒に設定します。

1min

CCM 送信間隔を 1 分に設定します。

10min

CCM 送信間隔を 10 分に設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1s，10s，1min，10min
3. 本パラメータ使用時の注意事項
   本パラメータの値をデフォルト値より低い値に設定すると，装置の CPU 状態が高負荷状態になり

通信に影響が出る可能性があります。

[コマンド省略時の動作]

CCM 送信間隔は 1min です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm domain

ドメインを設定します。本コマンド実行で，ドメイン名称，MA を設定する config-ether-cfm モードに移行します。

[入力形式]

情報の設定

ethernet cfm domain level <Level> [direction-up]

情報の削除

no ethernet cfm domain level <Level>

[入力モード]

(config)

[パラメータ]

level <Level>

ドメインレベルを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 7

direction-up

ethernet cfm mep コマンドで up ／ down を明示的に設定していない場合，本パラメータを設定すれば，Up MEP で動作します。

1. 本パラメータ省略時の初期値
   Down MEP で動作します。
2. 値の設定範囲
   なし
3. 本パラメータ使用時の注意事項
   本パラメータは変更できません。変更したい場合は，いったん該当コマンドを削除してから再設定してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドで設定したドメインを次のコマンドで参照している場合，本コマンドは削除できません。
   - ethernet cfm cc enable
   - ethernet cfm mep
   - ethernet cfm mip

[関連コマンド]

なし

ethernet cfm enable（global）

CFM を開始します。

[入力形式]

情報の設定
　ethernet cfm enable

情報の削除
　no ethernet cfm enable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

ほかの CFM のコマンドを設定していても，CFM は動作しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

ethernet cfm enable（interface）

no ethernet cfm enable 設定時に，該当ポートまたは該当ポートチャネルで，CFM PDU 送受信処理を停止状態にします。

[入力形式]

情報の設定
　no ethernet cfm enable

情報の削除
　ethernet cfm enable

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

CFM PDU を受信できます。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドは，チャネルグループに指定したイーサネットインタフェースに対して設定できません。また，本コマンドに指定したイーサネットインタフェースは，チャネルグループに設定できません。本コマンドは，該当イーサネットインタフェースの属するポートチャネルインタフェースに対して設定してください。

[関連コマンド]

なし

ethernet cfm mep

CFM で使用する MEP を設定します。

[入力形式]

情報の設定

ethernet cfm mep level <Level> ma <No.> mep-id <MEPID> [{down | up}]

情報の削除

no ethernet cfm mep level <Level> ma <No.> mep-id <MEPID>

[入力モード]

(config-if)

[パラメータ]

level <Level>

ethernet cfm domain コマンドで設定済みのドメインレベルを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 7

ma <No.>

ma name コマンドまたは ma vlan-group コマンドで設定済みの MA 識別番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535

mep-id <MEPID>

MEP ID を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 8191
3. 本パラメータ使用時の注意事項
   MA 内でユニークな値を設定してください。

{down | up}

ドメインの方向を指定します。

down

MEP を，回線側を保守対象とする Down MEP に設定します。

up

MEP を，リレー側（装置の内側に向けて）を保守対象とする Up MEP に設定します。

1. 本パラメータ省略時の初期値
   ethernet cfm domain コマンドで direction-up が設定されている場合，Up MEP で動作します。設定されていない場合，Down MEP で動作します。
2. 値の設定範囲

down または up

3. 本パラメータ使用時の注意事項
本パラメータは変更できません。変更する場合は，いったん本コンフィグレーションを削除してから再設定してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 同一インタフェースに，ethernet cfm mip コマンドが設定されている場合，ethernet cfm mip コマンド以上のドメインレベルは指定できません。
2. 本コマンドは，チャネルグループに指定したイーサネットインタフェースに対して設定できません。また，本コマンドに指定したイーサネットインタフェースは，チャネルグループに設定できません。本コマンドは，該当イーサネットインタフェースの属するポートチャネルインタフェースに対して設定してください。

[関連コマンド]

ethernet cfm domain

ethernet cfm mip

CFM で使用する MIP を設定します。

[入力形式]

情報の設定
    ethernet cfm mip level <Level>

情報の削除
    no ethernet cfm mip level <Level>

[入力モード]

(config-if)

[パラメータ]

level <Level>

ethernet cfm domain コマンドで設定済みのドメインレベルを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 〜 7

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 同一インタフェースに，ethernet cfm mep コマンドが設定されている場合，ethernet cfm mep コマンド以下のドメインレベルは指定できません。
2. 本コマンドは，チャネルグループに指定したイーサネットインタフェースに対して設定できません。また，本コマンドに指定したイーサネットインタフェースは，チャネルグループに設定できません。本コマンドは，該当イーサネットインタフェースの属するポートチャネルインタフェースに対して設定してください。

[関連コマンド]

ethernet cfm domain

ma name

該当ドメインで使用する MA の名称を設定します。

[入力形式]

情報の設定・変更

ma <No.> name {str <Strings> | vlan <VLAN ID>}

情報の削除

no ma <No.> name

[入力モード]

(config-ether-cfm)

[パラメータ]

<No.>

MA 識別番号を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535

{str <Strings> | vlan <VLAN ID>}

MA の名称を文字列または VLAN ID で指定します。

str <Strings>

MA の名称に <Strings> で指定する文字列を使用します。

vlan <VLAN ID>

MA の名称に <VLAN ID> で指定する VLAN ID を使用します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Strings> には，45 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。
   <VLAN ID> には，1 ～ 4094 の値を設定します。
3. 本パラメータ使用時の注意事項
   ・domain name コマンドで，no-present 以外のパラメータを指定している場合，<Strings> で 44 文字以上の文字列を指定すると，44 文字目以降の文字列は CCM 内の Short MA Name フィールドに適用されません。
   ・同一ドメイン内で設定済みの <Strings> または <VLAN ID> は指定できません。

[コマンド省略時の動作]

MA の名称には，ma vlan-group コマンドの <No.> を使用します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ethernet cfm domain

ma vlan-group

該当ドメインで使用する MA に所属する VLAN を設定します。

[入力形式]

情報の設定・変更

ma <No.> vlan-group <VLAN ID List> [primary-vlan <VLAN ID>]

情報の削除

no ma <No.> vlan-group

[入力モード]

(config-ether-cfm)

[パラメータ]

<No.>

MA 識別番号を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   0 ～ 65535

<VLAN ID List>

該当の MA で使用する VLAN を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <VLAN ID List> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。

primary-vlan <VLAN ID>

該当の MA で CFM PDU を送信するときに使用するプライマリ VLAN を設定します。

1. 本パラメータ省略時の初期値
   vlan-group <VLAN ID List> で指定した VLAN リストの中から，若番の VLAN がプライマリ VLAN として使用されます。
2. 値の設定範囲
   1 ～ 4094
3. 本パラメータ使用時の注意事項
   vlan-group <VLAN ID List> で指定した VLAN ID を指定してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ethernet cfm domain

33 SNMP

hostname

本装置の識別名称を設定します。

[入力形式]

情報の設定・変更
hostname <Name>

情報の削除
no hostname

[入力モード]

(config)

[パラメータ]

<Name>

本装置の識別名称です。使用するネットワーク内でユニークな名称を設定してください。この情報は，SNMP マネージャから System グループの [sysName] の名称で問い合わせることで参照できます。

本パラメータは RFC1213 の sysName に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   60 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

初期状態は識別名称が未設定です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. SNMP マネージャから name，contact，location の情報を参照する場合，snmp-server community コマンドで SNMP マネージャの登録が必要です。

[関連コマンド]

snmp-server community

rmon alarm

RMON（RFC1757）アラームグループの制御情報を設定します。本コマンドでは最大 128 エントリを設定できます。

[入力形式]

情報の設定・変更

rmon alarm <Number> <Variable> <Interval> {delta ｜ absolute} rising-threshold <Value> rising-event-index <Event#> falling-threshold <Value> falling-event-index <Event#> [owner <Owner string>] [startup-alarm { rising-falling ｜ rising ｜ falling }]

情報の削除

no rmon alarm <Number>

[入力モード]

(config)

[パラメータ]

<Number>

RMON アラームグループの制御情報の情報識別番号を設定します。本パラメータは RFC1757 の alarmIndex に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535

<Variable>

閾値チェックを行う MIB のオブジェクト識別子を設定します。本パラメータは RFC1757 の alarmVariable に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   ドット形式で MIB のオブジェクト識別子をダブルクォート (") で囲んで設定します。最大 63 文字で下記の設定可能なオブジェクト識別子だけ有効です。
   なお，入力文字列に，英数字，およびピリオド（.）以外の特殊文字列を含まない場合は，ダブルクォート (") で囲まなくても入力できます。
   - オブジェクト名
     「表 33-1　alarm 監視対象のオブジェクト識別子設定範囲」を参照してください。
   - インスタンス番号
     「表 33-1　alarm 監視対象のオブジェクト識別子設定範囲」内の x はインスタンス番号で，MIB の ifIndex を設定します。ifIndex の範囲については，「MIB レファレンス」を参照してください。

表 33-1　alarm 監視対象のオブジェクト識別子設定範囲

オブジェクト名（コンソールからの設定範囲）	オブジェクト ＩＤ（SNMP マネージャからの設定範囲）
ifInOctets.x	1.3.6.1.2.1.2.2.1.10.x
ifInUcastPkts.x	1.3.6.1.2.1.2.2.1.11.x

オブジェクト名（コンソールからの設定範囲）	オブジェクト ＩＤ（SNMP マネージャからの設定範囲）
ifInNUcastPkts.x	1.3.6.1.2.1.2.2.1.12.x
ifInDiscards.x	1.3.6.1.2.1.2.2.1.13.x
ifInErrors.x	1.3.6.1.2.1.2.2.1.14.x
ifInUnknownProtos.x	1.3.6.1.2.1.2.2.1.15.x
ifOutOctets.x	1.3.6.1.2.1.2.2.1.16.x
ifOutUcastPkts.x	1.3.6.1.2.1.2.2.1.17.x
ifOutNUcastPkts.x	1.3.6.1.2.1.2.2.1.18.x
ifOutDiscards.x	1.3.6.1.2.1.2.2.1.19.x
ifOutErrors.x	1.3.6.1.2.1.2.2.1.20.x
etherStatsDropEvents.x	1.3.6.1.2.1.16.1.1.1.3.x
etherStatsOctets.x	1.3.6.1.2.1.16.1.1.1.4.x
etherStatsPkts.x	1.3.6.1.2.1.16.1.1.1.5.x
etherStatsBroadcastPkts.x	1.3.6.1.2.1.16.1.1.1.6.x
etherStatsMulticastPkts.x	1.3.6.1.2.1.16.1.1.1.7.x
etherStatsCRCAlignErrors.x	1.3.6.1.2.1.16.1.1.1.8.x
etherStatsUndersizePkts.x	1.3.6.1.2.1.16.1.1.1.9.x
etherStatsOversizePkts.x	1.3.6.1.2.1.16.1.1.1.10.x
etherStatsFragments.x	1.3.6.1.2.1.16.1.1.1.11.x
etherStatsJabbers.x	1.3.6.1.2.1.16.1.1.1.12.x
etherStatsCollisions.x	1.3.6.1.2.1.16.1.1.1.13.x
etherStatsPkts64Octets.x	1.3.6.1.2.1.16.1.1.1.14.x
etherStatsPkts65to127Octets.x	1.3.6.1.2.1.16.1.1.1.15.x
etherStatsPkts128to255Octets.x	1.3.6.1.2.1.16.1.1.1.16.x
etherStatsPkts256to511Octets.x	1.3.6.1.2.1.16.1.1.1.17.x
etherStatsPkts512to1023Octets.x	1.3.6.1.2.1.16.1.1.1.18.x
etherStatsPkts1024to1518Octets.x	1.3.6.1.2.1.16.1.1.1.19.x
ifInMulticastPkts.x	1.3.6.1.2.1.31.1.1.1.2.x
ifInBroadcastPkts.x	1.3.6.1.2.1.31.1.1.1.3.x
ifOutMulticastPkts.x	1.3.6.1.2.1.31.1.1.1.4.x
ifOutBroadcastPkts.x	1.3.6.1.2.1.31.1.1.1.5.x

x: インスタンス番号

<Interval>

閾値チェックを行う時間間隔（秒）を設定します。本パラメータは RFC1757 の alarmInterval に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 4294967295（秒）

{ delta | absolute }

閾値チェック方式を設定します。delta の場合，現在値と前回のサンプリング時の値の差分を閾値と

比較します。absolute の場合，現在値を直接閾値と比較します。本パラメータは RFC1757 の alarmSampleType に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   delta または absolute

rising-threshold <Value>

上方閾値の値を設定します。本パラメータは RFC1757 の alarmRisingThreshold に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   -2147483648 ～ 2147483647

rising-event-index <Event#>

上方閾値を超えたときのイベント方法の識別番号を設定します。イベント方法は，rmon event コマンドで設定した制御情報の情報識別番号です。本パラメータは RFC1757 の alarmRisigEventIndex に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Event#> に rmon event コマンドで設定した制御情報の情報識別番号（1 ～ 65535）

falling-threshold <Value>

下方閾値の値を設定します。本パラメータは RFC1757 の alarmFallingThreshold に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   -2147483648 ～ 2147483647

falling-event-index <Event#>

下方閾値を割ったときのイベント方法の識別番号を設定します。イベント方法は，rmon event コマンドで設定した制御情報の情報識別番号です。本パラメータは RFC1757 の alarmFallingEventIndex に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Event#> に rmon event コマンドで設定した制御情報の情報識別番号（1 ～ 65535）

owner <Owner string>

本設定の設定者の識別情報を設定します。本設定を誰が行ったかを識別するための情報です。本パラメータは RFC1757 の alarmOwner に対応します。

1. 本パラメータ省略時の初期値
   Null
2. 値の設定範囲
   24 文字以内の文字列で 設定します。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

startup-alarm { rising-falling | rising | falling }

最初のサンプリングで閾値チェックを行うタイミングを設定します。rising を設定した場合，最初の

サンプリングで上方閾値を超えた場合にアラームを出します。falling を設定した場合，最初のサンプリングで下方閾値を超えた場合にアラームを出します。rising-falling の場合，最初のサンプリングで上方閾値または下方閾値を超えた場合にアラームを出します。本パラメータは RFC1757 の alarmstartUpAlarm に対応します。

1. 本パラメータ省略時の初期値
   rising-falling
2. 値の設定範囲
   rising，falling または rising-falling

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. SNMP マネージャからアラームグループにアクセスするときは，snmp-server community コマンドで SNMP マネージャの登録が必要です。
2. アラームグループの rising-event-index，falling-event-index の値はイベントグループで設定した情報識別番号を設定してください。
3. コンソールから設定する場合は，必ず「オブジェクト名」で設定してください。また，SNMP マネージャから「オブジェクト ID」で設定した場合，コンソールで運用コマンド show running-config を実行すると「オブジェクト名」で表示します。

[関連コマンド]

snmp-server host

rmon event

rmon collection history

RMON（RFC1757）イーサネットの統計来歴の制御情報を設定します。本コマンドでは最大 32 エントリを設定できます。

[入力形式]

情報の設定・変更

rmon collection history controlEntry <Integer> [owner <Owner name>] [buckets <Bucket number>] [interval <Seconds>]

情報の削除

no rmon collection history controlEntry <Integer>

[入力モード]

(config-if)

[パラメータ]

<Integer>

統計来歴の制御情報の情報識別番号を設定します。本パラメータは RFC1757 の historyControlIndex に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 〜 65535

owner <Owner name>

本設定の設定者の識別情報を設定します。本設定を誰が行ったかを識別するための情報です。本パラメータは RFC1757 の historyControlOwner に対応します。

1. 本パラメータ省略時の初期値
   空白
2. 値の設定範囲
   24 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

buckets <Bucket number>

統計情報を格納する来歴エントリ数を設定します。本パラメータは RFC1757 の historyControlBucketsRequested に対応します。

1. 本パラメータ省略時の初期値
   50
2. 値の設定範囲
   1 〜 65535
   注　<Bucket number> に 51 〜 65535 を設定した場合，50 を設定したときと同じ動作になります。

interval <Seconds>

統計情報を収集する時間間隔（秒）を設定します。本パラメータは RFC1757 の historyControlInterval に対応します。

1. 本パラメータ省略時の初期値
   1800（秒）

2. 値の設定範囲
   1 ～ 3600（秒）

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. SNMP マネージャからイーサネットヒストリグループにアクセスするときは snmp-server community コマンドで SNMP マネージャの登録が必要です。
2. 本コマンドでエントリを追加または削除すると SNMP マネージャ等で取得する EthernetHistory グループの情報が一時的に不定な値になる場合があります。

[関連コマンド]

interface

snmp-server community

rmon event

RMON（RFC1757）イベントグループの制御情報を設定します。本コマンドでは最大 16 エントリを設定できます。

[入力形式]

情報の設定・変更

rmon event <Event#> [log] [trap <Community>] [description <Description string>] [owner <Owner string>]

情報の削除

no rmon event <Event#>

[入力モード]

(config)

[パラメータ]

<Event#>

RMON イベントグループの制御情報の情報識別番号を設定します。本パラメータは RFC1757 の eventIndex に対応します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1 ～ 65535

log

アラーム（イベント）の方法を指定するパラメータで，アラームのログを残します。本パラメータは RFC1757 の eventType に対応します。

1. 本パラメータ省略時の初期値
   アラームのログを残しません。
2. 値の設定範囲
   なし

trap <Community>

アラーム（イベント）の方法を指定するパラメータで，<Community> で指定したコミュニティに対して SNMP のトラップを送信します。本パラメータは RFC1757 の eventCommunity に対応します。

1. 本パラメータ省略時の初期値
   トラップを発行しません。
2. 値の設定範囲
   trap およびコミュニティ名を設定します。
   60 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

description <Description string>

イベントの内容を文字列で設定します。イベント内容に関するメモとして使用してください。本パラメータは RFC1757 の eventDescription に対応します。

1. 本パラメータ省略時の初期値
   空白
2. 値の設定範囲

79 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

owner <Owner string>

本設定の設定者の識別情報を設定します。本設定を誰が行ったかを識別するための情報です。本パラメータは RFC1757 の eventOwner に対応します。

1. 本パラメータ省略時の初期値
   空白
2. 値の設定範囲
   24 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. SNMP マネージャからイベントグループにアクセスするとき，および SNMP マネージャにトラップを送信するときは，snmp-server community コマンドおよび snmp-server host コマンドで SNMP マネージャの登録が必要です。
2. SNMP マネージャにトラップを送信するためには，snmp-server host コマンドで送信先の SNMP マネージャの IP アドレスおよび”rmon”を設定してください。
3. SNMP マネージャ登録時のコミュニティ名とイベントグループのコミュニティ名が一致したときだけトラップを送信します。
4. アラームグループの rising-event-index，falling-event-index の値はイベントグループで設定した情報識別番号を設定してください。値が異なっていれば，アラームが発生したときにイベントは実行されません。

[関連コマンド]

snmp-server host

rmon alarm

snmp-server community

SNMP コミュニティに対するアクセスリストを設定します。本コマンドでは最大 4 エントリの設定ができます。

[入力形式]

情報の設定・変更
snmp-server community <String> [{ro|rw}] [<ACL ID>]

情報の削除
no snmp-server community <String>

[入力モード]

(config)

[パラメータ]

<String>

SNMP マネージャのコミュニティ名称を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   60 文字以内の文字列をダブルクォート（"）で囲んで設定します。入力可能な文字は，英数字と特殊文字です。入力文字列にスペースなどの特殊文字を含まない場合，文字列をダブルクォート（"）で囲まなくても設定できます。詳細は，「パラメータに指定できる値」の「任意の文字列」を参照してください。

{ro | rw}

設定したコミュニティ名称に属する設定した IP アドレスのマネージャに対する MIB 操作の動作モードを設定します。ro を設定した場合，Get Request，GetNext Request を許可し，rw を設定した場合，Get Request，GetNext Request，Set Request を許可します。

1. 本パラメータ省略時の初期値
   ro
2. 値の設定範囲
   ro または rw

<ACL ID>

本コミュニティに対する許可を設定した IPv4 アドレスフィルタを名前で設定します。<ACL ID> が省略された場合は，すべてのアクセスを許可します。また，指定した <ACL ID> が設定されていない場合は，すべてのアクセスを許可します。
1 コミュニティに対して 1 アクセスリストになります。

1. 本パラメータ省略時の初期値
   なし（すべてのアクセスを許可します。）
2. 値の設定範囲
   3 ～ 31 文字以内のアクセスリスト名称を指定します。指定可能な文字については「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

ip access-list standard

snmp-server contact

本装置の連絡先などを設定します。

[入力形式]

情報の設定・変更

snmp-server contact <Text>

情報の削除

no snmp-server contact

[入力モード]

(config)

[パラメータ]

<Text>

本装置障害時の連絡先などを設定します。この情報は，SNMP マネージャから System グループの [sysContact] の名称で問い合わせることで参照できます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   60 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

初期値は Null の文字列です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. SNMP マネージャから name，contact，location の情報を参照する場合，snmp-server community コマンドで SNMP マネージャの登録が必要です。

[関連コマンド]

なし

snmp-server host

トラップを送信するネットワーク管理装置（SNMP マネージャ）を登録します。本コマンドでは最大 4 エントリを設定できます。

[入力形式]

情報の設定・変更

snmp-server host <Manager address> traps <Community string> [version { 1 | 2c }] [snmp] [rmon] [air-fan] [login] [system-msg] [temperature] [storm-control] [efmoam] [poe] [dot1x] [web-authentication] [mac-authentication] [loop-detection] [switchport-backup] [cfm]

情報の削除

no snmp-server host <Manager address>

[入力モード]

(config)

[パラメータ]

<Manager address>

SNMP マネージャの IP アドレスを設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <Manager address> に IPv4 アドレス（ドット記法）を設定します。
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

<Community string>

SNMPv1 および SNMPv2C の場合は，SNMP マネージャのコミュニティ名称を設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   60 文字以内の文字列で設定してください。設定可能な文字については「パラメータに指定できる値」の「任意の文字列」を参照してください。

version { 1 | 2c }

指定したコミュニティ名称に属する設定した IP アドレスのマネージャに対するトラップ送信バージョンを設定します。1 を指定した場合，SNMPv1 バージョンのトラップを，2c を指定した場合，SNMPv2C バージョンのトラップを発行します。

1. 本パラメータ省略時の初期値
   1
2. 値の設定範囲
   1，または 2c のどちらかを設定します。

[snmp] [rmon] [air-fan] [login] [system-msg] [temperature] [storm-control] [efmoam] [poe] [dot1x] [web-authentication] [mac-authentication] [loop-detection] [switchport-backup] [cfm]

各パラメータを設定することによって，送信するトラップを選択します。各パラメータを設定した際に送信するトラップを次の表に示します。

表 33-2　パラメータとトラップの対応

パラメータ	トラップ
snmp	coldStart
	warmStart
	linkUp
	linkDown
	authenticationFailure
rmon	risingAlarm
	fallingAlarm
temperature	ax2230sTemperatureTrap【S2200】 ax2130sTemperatureTrap【S2100】 ax1250sTemperatureTrap【SS1250】 ax1240sTemperatureTrap【SS1240】
air-fan	ax2230sAirFanStopTrap【S2200】 ax2130sAirFanStopTrap【S2100】 ax1240sAirFanStopTrap【SS1240】
login	ax2230sLoginSuccessTrap【S2200】 ax2130sLoginSuccessTrap【S2100】 ax1250sLoginSuccessTrap【SS1250】 ax1240sLoginSuccessTrap【SS1240】
	ax2230sLoginFailureTrap【S2200】 ax2130sLoginFailureTrap【S2100】 ax1250sLoginFailureTrap【SS1250】 ax1240sLoginFailureTrap【SS1240】
	ax2230sLogoutTrap【S2200】 ax2130sLogoutTrap【S2100】 ax1250sLogoutTrap【SS1250】 ax1240sLogoutTrap【SS1240】
system-msg	ax2230sSystemMsgTrap【S2200】 ax2130sSystemMsgTrap【S2100】 ax1250sSystemMsgTrap【SS1250】 ax1240sSystemMsgTrap【SS1240】
storm-control	ax2230sBroadcastStormDetectTrap【S2200】 ax2130sBroadcastStormDetectTrap【S2100】 ax1250sBroadcastStormDetectTrap【SS1250】 ax1240sBroadcastStormDetectTrap【SS1240】
	ax2230sMulticastStormDetectTrap【S2200】 ax2130sMulticastStormDetectTrap【S2100】 ax1250sMulticastStormDetectTrap【SS1250】 ax1240sMulticastStormDetectTrap【SS1240】
	ax2230sUnicastStormDetectTrap【S2200】 ax2130sUnicastStormDetectTrap【S2100】 ax1250sUnicastStormDetectTrap【SS1250】 ax1240sUnicastStormDetectTrap【SS1240】
	ax2230sBroadcastStormPortInactivateTrap【S2200】 ax2130sBroadcastStormPortInactivateTrap【S2100】 ax1250sBroadcastStormPortInactivateTrap【SS1250】 ax1240sBroadcastStormPortInactivateTrap【SS1240】

パラメータ	トラップ
	ax2230sMulticastStormPortInactivateTrap【S2200】 ax2130sMulticastStormPortInactivateTrap【S2100】 ax1250sMulticastStormPortInactivateTrap【SS1250】 ax1240sMulticastStormPortInactivateTrap【SS1240】
	ax2230sUnicastStormPortInactivateTrap【S2200】 ax2130sUnicastStormPortInactivateTrap【S2100】 ax1250sUnicastStormPortInactivateTrap【SS1250】 ax1240sUnicastStormPortInactivateTrap【SS1240】
	ax2230sBroadcastStormRecoverTrap【S2200】 ax2130sBroadcastStormRecoverTrap【S2100】 ax1250sBroadcastStormRecoverTrap【SS1250】 ax1240sBroadcastStormRecoverTrap【SS1240】
	ax2230sMulticastStormRecoverTrap【S2200】 ax2130sMulticastStormRecoverTrap【S2100】 ax1250sMulticastStormRecoverTrap【SS1250】 ax1240sMulticastStormRecoverTrap【SS1240】
	ax2230sUnicastStormRecoverTrap【S2200】 ax2130sUnicastStormRecoverTrap【S2100】 ax1250sUnicastStormRecoverTrap【SS1250】 ax1240sUnicastStormRecoverTrap【SS1240】
efmoam	ax2230sEfmoamUdldPortInactivateTrap【S2200】 ax2130sEfmoamUdldPortInactivateTrap【S2100】 ax1250sEfmoamUdldPortInactivateTrap【SS1250】 ax1240sEfmoamUdldPortInactivateTrap【SS1240】
poe	pethPsePortOnOffNotification【S2200】【S2100】【SS1240】
	pethMainPowerUsageOnNotification【S2200】【S2100】【SS1240】
	pethMainPowerUsageOffNotification【S2200】【S2100】【SS1240】
dot1x	ax2230sDot1xFailureTrap【S2200】 ax2130sDot1xFailureTrap【S2100】 ax1250sDot1xFailureTrap【SS1250】 ax1240sDot1xFailureTrap【SS1240】
	ax2230sDot1xEventTrap【S2200】 ax2130sDot1xEventTrap【S2100】 ax1250sDot1xEventTrap【SS1250】 ax1240sDot1xEventTrap【SS1240】
	ax2230sDot1xSystemTrap【S2200】 ax2130sDot1xSystemTrap【S2100】 ax1250sDot1xSystemTrap【SS1250】 ax1240sDot1xSystemTrap【SS1240】
web-authentication	ax2230sWauthFailureTrap【S2200】 ax1250sWauthFailureTrap【SS1250】 ax1240sWauthFailureTrap【SS1240】
	ax2230sWauthEventTrap【S2200】 ax1250sWauthEventTrap【SS1250】 ax1240sWauthEventTrap【SS1240】
	ax2230sWauthSystemTrap【S2200】 ax1250sWauthSystemTrap【SS1250】 ax1240sWauthSystemTrap【SS1240】

パラメータ	トラップ
mac-authentication	ax2230sMauthFailureTrap【S2200】 ax2130sMauthFailureTrap【S2100】 ax1250sMauthFailureTrap【SS1250】 ax1240sMauthFailureTrap【SS1240】
	ax2230sMauthEventTrap【S2200】 ax2130sMauthEventTrap【S2100】 ax1250sMauthEventTrap【SS1250】 ax1240sMauthEventTrap【SS1240】
	ax2230sMauthSystemTrap【S2200】 ax2130sMauthSystemTrap【S2100】 ax1250sMauthSystemTrap【SS1250】 ax1240sMauthSystemTrap【SS1240】
loop-detection	ax2230sL2ldLinkDown【S2200】 ax2130sL2ldLinkDown【S2100】 ax1250sL2ldLinkDown【SS1250】 ax1240sL2ldLinkDown【SS1240】
	ax2230sL2ldLinkUp【S2200】 ax2130sL2ldLinkUp【S2100】 ax1250sL2ldLinkUp【SS1250】 ax1240sL2ldLinkUp【SS1240】
	ax2230sL2ldLoopDetection【S2200】 ax2130sL2ldLoopDetection【S2100】 ax1250sL2ldLoopDetection【SS1250】 ax1240sL2ldLoopDetection【SS1240】
switchport-backup	ax2230sUlrChangeSecondary【S2200】 ax2130sUlrChangeSecondary【S2100】 ax1250sUlrChangeSecondary【SS1250】 ax1240sUlrChangeSecondary【SS1240】
	ax2230sUlrChangePrimary【S2200】 ax2130sUlrChangePrimary【S2100】 ax1250sUlrChangePrimary【SS1250】 ax1240sUlrChangePrimary【SS1240】
cfm	dot1agCfmFaultAlarm

snmp

coldStart，warmStart，linkDown，linkUp，authenticationFailure トラップを送信します。

rmon

rmon のアラームの上方閾値を超えたときおよび下方閾値を下回ったときのトラップを送信します。

air-fan

FAN がストップしたときにトラップを送信します。

login

ログインの成功，失敗，ログアウトの発生時にトラップを送信します。

system-msg

システムメッセージを出力したときのトラップを送信します。

temperature

温度状態の変化のトラップを送信します。

storm-control

ストームコントロール機能によって，ストームの発生を検出した場合，またはストームから回復した場合にトラップを送信します。

efmoam

片方向リンク障害検出時のトラップを送信します。

poe

電源供給状態が変化した場合，または装置の合計消費電力が閾値を超えた場合にトラップを送信します。

dot1x

IEEE802.1X 認証で，特定の認証アカウントログに対するトラップを送信します。

web-authentication

Web 認証で，特定の認証アカウントログに対するトラップを送信します。

mac-authentication

MAC 認証で，特定の認証アカウントログに対するトラップを送信します。

loop-detection

L2 ループ検知時のトラップを送信します。

switchport-backup

アップリンク・リダンダントで，回線切替発生時にトラップを送信します。

cfm

CC で障害検出のトラップを送信します。

1. 本パラメータ省略時の初期値
   パラメータに対応するトラップを発行しません。
2. 値の設定範囲
   snmp，rmon，air-fan，login，system-msg，temperature，storm-control，efmoam，poe，dot1x，web-authentication，mac-authentication，loop-detection，switchport-backup，cfm

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. サポート MIB およびサポートトラップの一覧は「MIB レファレンス」を参照してください。
2. 特定の認証アカウントログと各認証機能（IEEE802.1X，Web 認証，MAC 認証）のプライベート Trap 発行条件については，「コンフィグレーションガイド Vol.2」の各認証の「アカウント機能」を参照してください。
3. air-fan は FAN 搭載モデルだけ，poe は PoE 機能サポートモデルだけ設定可能です。
4. <Manager address> には，IPv4 アドレスとして 127.*.*.* を設定できません。
5. 連続して大量のトラップが発生した場合，SNMP マネージャに対してトラップの送達抜けが発生することがあります。

[関連コマンド]

なし

snmp-server location

本装置を設置する場所の名称を設定します。

[入力形式]

情報の設定・変更

snmp-server location <Text>

情報の削除

no snmp-server location

[入力モード]

(config)

[パラメータ]

<Text>

本装置を設置する場所の名称を設定します。この情報は，SNMP マネージャから System グループの [sysLocation] の名称で問い合わせることで参照できます。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   60 文字以内の文字列をダブルクォート（"）で囲んで設定します。入力可能な文字は，英数字と特殊文字です。入力文字列にスペースなどの特殊文字を含まない場合，文字列をダブルクォート（"）で囲まなくても設定できます。詳細は，「パラメータに指定できる値」の「任意の文字列」を参照してください。

[コマンド省略時の動作]

初期値は Null の文字列です。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. SNMP マネージャから name，contact，location の情報を参照する場合，snmp-server community コマンドで SNMP マネージャの登録が必要です。

[関連コマンド]

なし

snmp-server traps

トラップの発行契機を設定します。

[入力形式]

情報の設定・変更

snmp-server traps [{ limited-coldstart-trap | unlimited-coldstart-trap }] [link-trap-bind-info {private | standard}] [system-msg-trap-level <Level>] [agent-address <Agent address>] [dot1x-trap {failure | all}] [web-authentication-trap {failure | all}] [mac-authentication-trap {failure | all}]

情報の削除

no snmp-server traps

[入力モード]

(config)

[パラメータ]

{ limited-coldstart-trap | unlimited-coldstart-trap }

coldStart Trap を発行する契機を限定します。本パラメータの設定による coldStart Trap の発行契機の概要を次の表に示します。

表 33-3　パラメータごとの coldStart Trap 発行契機

パラメータ	coldStart Trap 発行契機
limited-coldstart-trap	• 装置を起動したとき（装置電源オン）
unlimited-coldstart-trap	• 装置を起動したとき（装置電源オン） • IP のコンフィグレーションを追加または削除したとき • set clock コマンドで時間を変更したとき

1. 本パラメータ省略時の初期値
   limited-coldstart-trap
2. 値の設定範囲
   limited-coldstart-trap または unlimited-coldstart-trap

link-trap-bind-info {private | standard}

link up/down Trap を発行する際に付加する MIB を，選択するための設定をします。
本パラメータの設定による link up/down Trap の発行の際，付加する MIB を次の表に示します。

表 33-4　パラメータごとの link up/down Trap 発行時に付加する MIB

パラメータ	link up/down Trap 発行時に付加する MIB
private	• SNMPv1/SNMPv2C トラップ共通) ifIndex，ifDescr，ifType
standard	• (SNMPv1 トラップの場合) ifIndex • (SNMPv2C トラップの場合) ifIndex，ifAdminStatus，ifOperStatus

1. 本パラメータ省略時の初期値
   standard
2. 値の設定範囲
   private または standard

system-msg-trap-level <Level>}

システムメッセージトラップの送信レベル（10 進数）を指定します。指定したレベルより重大（数値が小さい）なイベントが発生した場合に，トラップが発行されます。本パラメータで指定したレベルによって発行するシステムメッセージトラップの概要を次の表に示します。

表 33-5　システムメッセージトラップのレベルと意味 MIB

レベル	意味
1	致命的障害の運用に関するシステムメッセージトラップを送信します。
2	重度障害以上のシステムメッセージトラップを送信します。
3	ソフトウェア部障害以上のシステムメッセージトラップを送信します。
4 ～ 5	警告レベル以上のシステムメッセージトラップを送信します。
6	運用に関するイベント情報以上のシステムメッセージトラップを送信します。

1. 本パラメータ省略時の初期値
   1
2. 値の設定範囲
   1 ～ 6

agent-address <Agent address>

SNMPv1 形式のトラップ通知フレーム内の agent address に使用する IPv4 アドレスを設定します。Trap-PDU 内に agent-address フィールドを持つのは SNMPv1 形式だけのため，本コマンドで設定したアドレスは SNMPv1 のトラップに適用されます。

1. 本パラメータ省略時の初期値
   本パラメータが設定されていない場合，トラップ通知フレーム内の agent address の値として最も小さい VLAN ID の IPv4 アドレスが使用されます。
2. 値の設定範囲
   <Agent address> に IPv4 アドレス（0.0.0.0 ～ 255.255.255.255）を設定します。

dot1x-trap {failure | all}

IEEE802.1X 認証のトラップ種別を設定します。

failure

認証失敗のトラップだけを発行します。

all

認証成功，認証失敗および認証解除のトラップを発行します。

1. 本パラメータ省略時の初期値
   failure
2. 値の設定範囲
   failure または all

web-authentication-trap {failure | all}

Web 認証のトラップ種別を設定します。

failure

認証失敗のトラップだけを発行します。

all

認証成功，認証失敗および認証解除のトラップを発行します。

1. 本パラメータ省略時の初期値

failure

2. 値の設定範囲
   failure または all

mac-authentication-trap {failure | all}

MAC 認証のトラップ種別を設定します。

failure

認証失敗のトラップだけを発行します。

all

認証成功，認証失敗および認証解除のトラップを発行します。

1. 本パラメータ省略時の初期値
   failure
2. 値の設定範囲
   failure または all

[コマンド省略時の動作]

本コマンドのパラメータがすべて初期値で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. サポート MIB およびサポートトラップの一覧は「MIB レファレンス」を参照してください。
2. 本コマンド入力時，全パラメータを省略することはできません。いずれか 1 つ以上設定してください。

[関連コマンド]

なし

snmp trap link-status

no snmp trap link-status 設定時，回線がリンクアップまたはダウンした場合に，トラップ（linkDown トラップおよび linkUp トラップ）の送信を抑止します。

[入力形式]

情報の設定
　no snmp trap link-status

情報の削除
　snmp trap link-status

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

トラップ（linkDown トラップおよび linkUp トラップ）の抑止を行いません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

34 ログ出力機能

logging event-kind

syslog サーバに送信対象とするログ情報のイベント種別を設定します。イベント種別は複数設定できます。

[入力形式]

情報の設定・変更
    logging event-kind <Event kind>

情報の削除
    no logging event-kind <Event kind>

[入力モード]

(config)

[パラメータ]

<Event kind>

出力するログのイベント種別を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   key，rsp，err，evt の中から指定します。

[コマンド省略時の動作]

イベント種別は「evt」および「err」となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドで設定したイベント種別は，logging host コマンドで指定されたすべての出力先に対して適用されます。
2. 本コマンドでイベント種別を設定した場合，デフォルトのイベント種別（evt，err）は無効になり，設定したイベント種別だけが有効になります。

[関連コマンド]

logging host

logging facility

ログ情報を syslog インタフェースで出力するためのファシリティを設定します。

[入力形式]

情報の設定・変更

logging facility <Facility>

情報の削除

no logging facility

[入力モード]

(config)

[パラメータ]

<Facility>

syslog のファシリティを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   local0，local1，local2，local3，local4，local5，local6，local7 のどれか一つを指定します。

[コマンド省略時の動作]

ファシリティは「local0」となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドで設定したファシリティは，logging host コマンドで指定されたすべての出力先に対して適用されます。

[関連コマンド]

logging host

logging host

ログ情報の出力先を設定します。本コマンドでは最大 4 エントリの設定ができます。

[入力形式]

情報の設定・変更

logging host <IP address>

情報の削除

no logging host <IP address>

[入力モード]

(config)

[パラメータ]

<IP address>

ログ出力先の IPv4 アドレスを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IP address>
   IPv4 アドレスをドット記法で指定します。
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. syslog 機能を使用するためには，出力先ホスト側で syslog デーモンプログラムが動作していて，かつ本装置からの syslog 情報を受け取れるように設定されている必要があります。
2. IPv4 アドレスとして 127.*.*.* を設定できません。
3. 一度に大量のログ情報が発生した場合，syslog 情報に抜けが発生することがあります。

[関連コマンド]

なし

logging syslog-header

syslog サーバに送信するメッセージに HOSTNAME，TIMESTAMP，および機能番号を付加します。

以下のコマンドでの出力には影響しません。

- show dot1x logging
- show logging
- show web-authentication logging
- show mac-authentication logging

[入力形式]

情報の設定
　logging syslog-header

情報の削除
　no logging syslog-header

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

従来どおりです。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 機能番号は上位機種が出力する syslog メッセージの形式に合わせるために付加しています。

[関連コマンド]

なし

logging trap

syslog サーバに送信対象とするログ情報の重要度を設定します。

[入力形式]

情報の設定・変更

logging trap { <Level> | <Keyword> }

情報の削除

no logging trap

[入力モード]

(config)

[パラメータ]

{ <Level> | <Keyword> }

syslog メッセージの重要度をレベルまたはキーワードの内，どれか一つを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   設定できる重要度は次の表を参照してください。なお，レベル指定で設定した場合も，キーワードで情報が表示されます。

レベル（Level）	キーワード（Keyword）	説明
1	fatal	即時対応が必要
2	critical	クリティカル状態
3	error	エラー状態
4	warning	警告状態
6	information	通知目的だけのメッセージ
7	debugging	デバッグ中にだけ表示されるメッセージ

[コマンド省略時の動作]

重要度はレベル 6 の「information」となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドで設定した重要度は，logging host コマンドで指定されたすべての出力先に対して適用されます。

[関連コマンド]

logging host

35 LLDP

lldp enable

ポートで LLDP の運用を開始します。

[入力形式]

情報の設定
　lldp enable

情報の削除
　no lldp enable

[入力モード]

(config-if)

[パラメータ]

なし

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

lldp run

lldp hold-count

本装置が送信する LLDP フレームに対して隣接装置が保持する時間を設定します。

[入力形式]

情報の設定・変更

lldp hold-count <Count>

情報の削除

no lldp hold-count

[入力モード]

(config)

[パラメータ]

<Count>

本装置が送信する LLDP フレームに対して，隣接装置が保持する時間を lldp interval-time コマンドで設定した値に対する倍率で設定します。保持時間が 65535 を超える場合は，最大値である 65535 で動作します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   2 ～ 10

[コマンド省略時の動作]

本装置が送信する LLDP フレームに対する隣接装置が，保持する時間は 4 となります。

[通信への影響]

なし

[設定値の反映契機]

設定値更新後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

lldp run

lldp interval-time

本装置が送信する LLDP フレームの送信間隔を設定します。

[入力形式]

情報の設定・変更
　lldp interval-time <Seconds>

情報の削除
　no lldp interval-time

[入力モード]

(config)

[パラメータ]

<Seconds>

本装置が送信する LLDP フレームの送信間隔を秒単位で設定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   5 ～ 32768（秒）

[コマンド省略時の動作]

本装置が送信する LLDP フレームの送信間隔は 30 秒となります。

[通信への影響]

なし

[設定値の反映契機]

設定値更新後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

lldp run

lldp run

LLDP 機能を有効にします。

[入力形式]

情報の設定

lldp run

情報の削除

no lldp run

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

LLDP 機能は無効となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

36 ポートミラーリング

monitor session

ポートミラーリング機能を設定します。

[入力形式]

情報の設定・変更

monitor session <Session#> source interface <IF# list> [{rx | tx | both}] destination interface gigabitethernet <IF#>【S2200】

monitor session <Session#> source interface <IF# list> [{rx | tx | both}] destination interface {gigabitethernet <IF#> | port-channel <Channel group#>}【S2100】

monitor session <Session#> source interface <IF# list> [{rx | tx | both}] destination interface {fastethernet <IF#>| gigabitethernet <IF#>}【SS1250】【SS1240】

情報の削除

no monitor session <Session#>

[入力モード]

(config)

[パラメータ]

<Session#>

ポートミラーリングセッションの番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   1

source interface <IF# list>

ポートミラーリングのモニターポートを指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

{rx | tx | both}

ポートミラーリングするトラフィックの方向を指定します。

rx

受信フレームをミラーリングします。

tx

送信フレームをミラーリングします。

both

送受信フレームをミラーリングします。

1. 本パラメータ省略時の初期値
   both
2. 値の設定範囲
   なし

destination interface gigabitethernet <IF#>【S2200】

destination interface {gigabitethernet <IF#> | port-channel <Channel group#>}【S2100】

destination interface {fastethernet <IF#>| gigabitethernet <IF#>}【SS1250】【SS1240】

ポートミラーリングのミラーポートを指定します。

設定できるインタフェースは物理ポートまたはポートチャネルインタフェースです。【S2100】

レイヤ 2 情報を設定したポートは指定できません。【S2200】【SS1250】【SS1240】

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   <IF#> :「パラメータに指定できる値」を参照してください。
   <Channel Group#> :「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

運用中の回線をミラーポートに設定した場合，その回線で通信できなくなります。モニターポートに設定した場合は通信に影響しません。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 同時に設定できるモニターポートとミラーポートの組み合わせは 1 です。
2. すでにモニターポートとして設定しているポートをミラーポートに設定できません。
3. 複数のモニターポートに対して一つのミラーポートを設定できます。一つのモニターポートに対して複数のミラーポートを設定できません。
4. ポートミラーリングでコピーしたフレームの量が回線帯域を超えた場合，そのフレームは廃棄されます。
5. ミラーポートに設定したポートでは，通常のフレーム送受信はできません。
6. レイヤ 2 情報を設定したポートをミラーポートに設定することはできません。詳細は「コンフィグレーションガイド Vol.2　26. ポートミラーリング」を参照してください。

[関連コマンド]

なし

switchport monitor dot1q tag【S2100】

ポートミラーリング機能で該当ポートがミラーポートに指定された場合，ミラーリング対象フレームに指定した 802.1Q Tag を付与して送信します。

[入力形式]

情報の設定・変更

switchport monitor dot1q tag <VLAN ID> [priority <Priority>]

情報の削除

no switchport monitor dot1q tag

[入力モード]

(config-if)

[パラメータ]

<VLAN ID>

付与する Tag の VLAN ID を指定します。

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   「パラメータに指定できる値」を参照してください。

priority <Priority>

付与する Tag のユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   3
2. 値の設定範囲
   0 ～ 7

[コマンド省略時の動作]

ミラーリング対象フレームに 802.1Q Tag を付与しません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドでは，vlan，interface vlan で設定していない VLANID を 1 つ指定してください。
2. 本コマンドで指定するユーザ優先度は 802.1Q Tag 内だけに記録されるものであり，本装置の送信キュー選択には影響しません。

[関連コマンド]

monitor session

37 コンフィグレーション編集時のエラーメッセージ

37.1 コンフィグレーション編集時のエラーメッセージ

37.1.1 共通

表 37-1 共通のエラーメッセージ

メッセージ	内容
Access denied.	アクセスが拒否されました。
Ambiguous command.	何通りかに解釈できるコマンドなので一意に特定できません。
Ambiguous data.	何通りかに解釈できるデータなので一意に特定できません。
Ambiguous parameter.	何通りかに解釈できるパラメータなので一意に特定できません。
Authorization error.	認証エラーです。
Bad command.	コマンド入力が正しくありません。
Bad value.	値が正しくありません。
Cannot execute.	実行できません。
Cannot register this command in a range mode.	このコマンドはレンジモードでは登録できません。
Command chaining not allowed.	２つのコマンドを続けて入力できません。
Don't specify a <MSTI ID list>.	<MSTI ID list> の入力は不要です。
Event not found.	イベントが見つかりませんでした。
File not found.	ファイルが見つかりませんでした。
Incomplete command.	コマンドが不完全です。
Inconsistent name.	名前が矛盾しています。
Inconsistent value.	値が矛盾しています。
interface: Invalid IPv4 address.	インタフェース：IPv4 アドレスが不正です。
interface: Invalid Mask.	インタフェース：マスクが不正です。
Invalid parameter order.	パラメータ指定が不正です。
Invalid parameter.	入力されたパラメータは無効です。
Invalid value.	入力された値は無効です。
It will be logged out if it remains idle for another <min> minutes.	IDLE 状態があと <min> 分続いたらログアウトします。
Log out by the system.	システムによりログアウトしました。
Login incorrect.	指定したホストへのログインが認められません。
Missing parameter.	パラメータが欠けています。
Missing parameter data.	パラメータのデータが欠けています。
No Access.	アクセスがありません。
No help available.	ヘルプが無効です。
'no' is not applicable.	'no' は使えません。
No such name.	そのような名前はありません。
Not found:	見つかりませんでした。
Not writable.	書けません。
Out of range. Valid range is: <range>	入力範囲外です。有効な入力範囲は <range> です。
Please set parameter more than one.	パラメータが 1 個も指定されていません。

メッセージ	内容
Read only.	読み込み専用です。
Resource unavailable.	資源が無効です。
String must be more than 0 characters.	文字列は 1 文字以上でなければばなりません。
String too long.	文字列が長すぎます。
The command execution failed, because "xxx" is executing.	他のユーザによってコマンド実行中です。しばらく経ってから実行するか，他のユーザが操作していないか確認してください。 xxx：他のユーザ情報（console，vty0，vty1 などが表示されます。）
The number of the <HEX enum> exceeds a maximum number.	コマンドの <HEX enum> のパラメータ数が最大を超えています。
This command is not supported with this model.	本コマンドはこのモデルでは未サポートです。
This command uses the "no" prefix.	このコマンドは "no" コマンドの接頭辞です。
Too big.	大きすぎます。
Too many parameters.	パラメータが多すぎます。
Unknown user.	指定したユーザ名が登録されていません。
Wrong encoding.	エンコーディングが誤っています。
Wrong length.	長さが正しくありません。
Wrong type.	型が誤っています。
Wrong value.	値が正しくありません。
Invalid parameter 'xxx'.	パラメータ 'xxx' が無効です。
Some parameters are insufficient.	パラメータが不足しています。
Cannot set TOS/Precedence and DSCP at the same time.	TOS/Precedence と DSCP を同時に設定できません。どちらか片方だけにしてください。

37.1.2　ログインセキュリティと RADIUS

表 37-2　ログインセキュリティと RADIUS のエラーメッセージ

メッセージ	内容
Can't delete it because data is not corresponding.	指定したコンフィグレーションが存在しないため削除できません。
radius-server: Cannot add new group because the maximum number is already set.	最大エントリ数登録されているため，これ以上登録できません。
radius-server: Cannot add new radius-server host because the maximum number is already set.	最大エントリ数登録されているため，これ以上登録できません。
radius-server: Port Number is duplicate between auth port and acct port.	auth-port と acct-port のポート番号が重複しています。

37.1.3　時刻の設定と NTP 情報

表 37-3　時刻の設定と NTP のエラーメッセージ

メッセージ	内容
Entry count over	これ以上 NTP サーバアドレスを設定できません。すでに設定されている NTP サーバアドレスを確認してください。

37.1.4　装置の管理情報

表 37-4　装置の管理のエラーメッセージ

メッセージ	内容
dhcp-snooping is in use.	DHCP snooping 機能が有効に設定されているため，本設定を変更できません。ip dhcp snooping 設定を削除してください。
extended-authentication is in use.	下記の機能のいずれかが有効に設定されているため，本設定を変更できません。 • 認証専用 IPv4 アクセスリスト • IEEE802.1X：ポート単位認証（動的） • Web 認証：固定 VLAN モード，ダイナミック VLAN モード，Web 認証専用 IP アドレス • MAC 認証：固定 VLAN モード，ダイナミック VLAN モード 下記の設定を削除してください。 • authentication arp-relay • authentication ip access-group • dot1x port-control • web-authentication ip address • web-authentication port • mac-authentication port
filter is in use.	フィルタ機能が有効に設定されているため，本設定を変更できません。ip access-group，mac access-group 設定を削除してください。
igmp-snooping is in use.	IGMP snooping 機能が有効に設定されているため，本設定を変更できません。ip igmp snooping 設定を削除してください。
mld-snooping is in use.	MLD snooping 機能が有効に設定されているため，本設定を変更できません。ipv6 mld snooping 設定を削除してください。
qos is in use.	QoS 機能が有効に設定されているため，本設定を変更できません。ip qos-flow-group，mac qos-flow-group 設定を削除してください。
resource unavailable	指定したリソースの合計が 7 を超えています。 7 以下となるよう設定してください。

37.1.5　省電力機能情報

表 37-5　省電力機能のエラーメッセージ

メッセージ	内容
Can't execute.	コマンドを実行できません。再度実行してください。
Invalid time-range.	日付指定で開始日より終了日が古いです。 設定内容の見直しを実施してください。

37.1.6　イーサネット情報

表 37-6　イーサネットのエラーメッセージ

メッセージ	内容
Cannot attach the interface specified as a ring-port to the channel-group.	リングポートに指定したインタフェースをポートチャネルに参加させることはできません。 指定したインタフェースをポートチャネルに参加させる場合には，リングに関する設定を削除してから実施してください。

メッセージ	内容
port:Relations between media type and <command> configuration are inconsistent.	media-type auto 設定のため，<command> 情報を変更できません。 <command>：duplex，mdix auto，speed
this command is different from this one in channel-group port.	ポートチャネルの設定内容と不一致です。 ポートチャネルの設定内容を一致させてください。

37.1.7　リンクアグリゲーション情報

表 37-7　リンクアグリゲーションのエラーメッセージ

メッセージ	内容
Can't delete port-channel configuration referred by other configuration.	他のコンフィグレーションで使用しているため削除できません。
Cannot attach the interface specified as a ring-port to the channel-group.	リングポートに指定したインタフェースをポートチャネルに参加させることはできません。 指定したインタフェースをポートチャネルに参加させる場合には，リングに関する設定を削除してから実施してください。
dot1x(link-aggregation): The specified ethernet <IF#> cannot add to the specified port-channel(<Channel group#>) because 802.1X configuration is different.	リンクアグリゲーションで一致すべき IEEE802.1X の設定が異なるため，ethernet <IF#> を指定された port-channel(<Channel group#>) に登録できません。 <IF#>：インタフェースポート番号 <Channel group#>：チャネルグループ番号
interface : Cannot attach the interface that specified cfm enable to the channel-group.	CFM の enable を設定したインタフェースをポートチャネルに参加させることはできません。 設定したインタフェースをポートチャネルに参加させる場合には，CFM の enable を削除してから実施してください。
interface : Cannot attach the interface that specified mep to the channel-group.	MEP を設定したインタフェースをポートチャネルに参加させることはできません。 設定したインタフェースをポートチャネルに参加させる場合には，MEP を削除してから実施してください。
interface : Cannot attach the interface that specified mip to the channel-group.	MIP を設定したインタフェースをポートチャネルに参加させることはできません。 設定したインタフェースをポートチャネルに参加させる場合には，MIP を削除してから実施してください。
interface : Invalid authentication arp-relay configuration.	authentication arp-relay 設定が異なるため，ポートチャネルに加入できません。
interface : Invalid authentication ip access-group configuration.	authentication ip access-group 設定が異なるため，ポートチャネルに加入できません。
interface : Relations between authentication configuration and channel-group configuration within same port.	指定ポートは認証共通コマンドで使用しているため，ポートチャネルに加入できません。
interface : Relations between the mac-authentication configuration and the channel-group configuration within same port.	指定ポートは MAC 認証設定で使用しているため，ポートチャネルに加入できません。
interface : Relations between the web-authentication configuration and the channel-group configuration within same port.	指定ポートは Web 認証設定で使用しているため，ポートチャネルに加入できません。
interface : this command is different from this one in channel-group port.	コンフィグレーションが異なるため，ポートチャネルに加入できません。
invalid data[channel-group].	ポートチャネル番号の指定が不正です。
invalid data[ethernet-if].	インターフェースポート番号の指定が不正です。

メッセージ	内容
Maximum number of channel-group port are already defined.	これ以上ポートを設定できません。 チャネルグループ単位のポート数を再確認してください。
Mirror port and port-channel are inconsistent.	ミラーポートとして使用しているためポートチャネルに加入できません。
Relations between ip dhcp snooping configuration and channel-group configuration are inconsistent.	指定したポートは ip dhcp snooping 設定で使用しているためポートチャネルに加入できません。 ip dhcp snooping 設定を削除後に再設定してください。
Relations between ip source binding configuration and channel-group configuration are inconsistent.	指定したポートは ip source binding 設定で使用しているためポートチャネルに加入できません。 ip source binding 設定を削除後に再設定してください。
	指定したポートチャネルは ip source binding 設定で使用しているため削除できません。 ip source binding 設定を削除後に再設定してください。
Relations between ip verify source configuration and channel-group configuration are inconsistent.	指定したポートは ip verify source 設定で使用しているためポートチャネルに加入できません。 ip verify source 設定を削除後に再設定してください。
Relations between vlan in mac-address-table static configuration and channel-group configuration are inconsistent.	mac-address-table static で使用しているインタフェースのためポートチャネルに加入できません。
this command is different from this one in channel-group port.	同一チャネルグループに指定したポートで設定内容の異なるものがあります。 同一チャネルグループに指定するポートは設定内容を一致させるか削除してください。
vlan : Data(port-channel) is invalid.	ポートチャネル番号の指定が不正です。
vlan : This command is different from vlan configuration in channel-group port.	VLAN コンフィグレーションが異なっているため，ポートチャネルに加入できません。

37.1.8 MAC アドレステーブル情報

表 37-8 MAC アドレステーブルのエラーメッセージ

メッセージ	内容
Can't set mac-address-table because of port-channel nothing.	ポートチャネルが存在しないため，mac-address-table が設定できません。
Relations between vlan in mac-address-table static configuration and switchport configuration are inconsistent.	mac-address-table static の vlan 指定と switchport のコンフィグレーションが不一致です。mac-address-table static で指定された vlan は，指定されたインタフェースの switchport access/switchport trunk allowed vlan/switchport mac vlan/switchport protocol vlan で指定されていなければなりません。

37.1.9　VLAN 情報

表 37-9　VLAN のエラーメッセージ

メッセージ	内容
ChGr <Channel group#>: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	IEEE802.1X 認証または switchport で使用しているためポートチャネルを削除できません。 <Channel group#>：チャネルグループ番号
Inconsistency is found between the dot1x vlan enable or dot1x vlan dynamic radius-vlan <VLAN ID> and the vlan configuration.	指定した VLAN は，IEEE802.1X　VLAN 単位認証（動的）の VLAN で使用しているため削除できません。 <VLAN ID>：VLAN ID
interface : Relations between the mac-authentication configuration and the vlan mode configuration are inconsistent.	指定したポートは MAC 認証で使用しているため設定変更できません。 mac-authentication port の設定を削除後に再設定してください。
interface : Relations between the web-authentication configuration and the vlan mode configuration are inconsistent.	指定したポートは Web 認証で使用しているため設定変更できません。 web-authentication port の設定を削除後に再設定してください。
Mirror port and switchport are inconsistent.	ミラーポートと switchport は同時に設定できません。
port <IF#>: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	指定したポートは IEEE802.1X 認証で使用しているため変更できません。 <IF#>：インタフェースポート番号
Relations between vlan in access-group configuration and switchport configuration are inconsistent.	指定した VLAN は ip access-group または mac access-group で使用しているため設定変更できません。 該当する VLAN を設定している ip access-group または mac access-group の設定を削除後に再設定してください。
Relations between vlan in dot1q configuration and mac vlan configuration are inconsistent.	switchport mac dot1q vlan と switchport mac vlan で，同じ VLAN を指定しているため設定できません。
Relations between vlan in dot1q configuration and native configuration are inconsistent.	switchport mac dot1q vlan と switchport mac native vlan で，同じ VLAN を指定しているため設定できません。
Relations between vlan in ip source binding configuration and switchport configuration are inconsistent.	ip source binding 設定で使用しているため設定変更できません。 ip source binding 設定を削除後に再設定してください。
Relations between vlan in qos-flow-group configuration and switchport configuration are inconsistent.	指定した VLAN は ip qos-flow-group または mac qos-flow-group で使用しているため設定変更できません。 該当する VLAN を設定している ip qos-flow-group または mac qos-flow-group の設定を削除後に再設定してください。
vlan : Can't change mode from {nothing | protocol-based | mac-based } to {nothing | protocol-based | mac-based }.	指定した VLAN モードの VLAN 種別が不一致です。(VLAN 範囲指定）
vlan : Can't delete vlan configuration because of default vlan.	デフォルト VLAN のため削除できません。
vlan : Can't setting port[<IF#>] because of channel-group port.	指定したポート番号はチャネルグループに所属しているためポートから設定できません。 <IF#>：インタフェースポート番号
vlan : Data(mac-address) is invalid.	指定した mac-address が範囲外のため登録できません。
vlan : maximum number which can be used is exceeded.	VLAN 数が最大エントリ数を超えたため生成できません。
vlan : Not found protocol name.	vlan-protocol が未設定のため設定できません。
vlan : Some port's setting have been failed.	Channel から Port への設定が失敗しました。

メッセージ	内容
vlan : Some setting can't have been done because of vlan unmatch.	存在しない VLAN が 1 つ以上含まれているため，設定できない VLAN がありました。
vlan[<VLAN ID>] : Can't change mode from {nothing | protocol-based | mac-based} to {nothing | protocol-based | mac-based}.	指定した VLAN モードの VLAN 種別が不一致です。(VLAN 単独指定) <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : Can't delete it because data is not corresponding.	指定した VLAN が存在しないため削除できません。 指定した mac-address は登録されていないため削除できません。 指定した mac-address-table は存在しないため削除できません。 <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : Can't delete port-channel configuration referred by other configuration.	他のコンフィグレーションで使用しているため削除できません。 <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : Can't delete vlan configuration referred by other configuration.	他のコンフィグレーションで使用しているため削除できません。 <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : Can't set access-vlan which is not configured to use vlan.	VLAN が存在しないためアクセス VLAN が設定できません。 <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : Can't set mac-address-table static which is not configured to use vlan.	VLAN が存在しないため mac-address-table を設定できません。 <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : Can't set native-vlan which is not configured to use vlan.	VLAN が存在しないためネイティブ VLAN を設定できません。 <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : Data can't be set because of not mac-based.	指定した VLAN は MAC VLAN でないため，mac-address を登録できません。 <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : Data can't be set because of not protocol-based.	指定した VLAN はプロトコル VLAN でないため protocol を登録できません。 <VLAN ID>：VLAN ID
VLAN <VLAN ID> is already in use for mirroring.	指定した VLAN は switchport monitor dot1q tag で使用しているため設定することはできません。
vlan[<VLAN ID>] : mac-address has already been set to other VLAN[<VLAN ID>].	他の VLAN で既に指定 mac-address は登録されているので登録できません。 <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : maximum number which can be used is exceeded.	VLAN 数が最大エントリ数を超えたため生成できません。 登録 mac-address 数が最大エントリ数を超えたため登録できません。 登録 mac-address-table 数が最大エントリ数を超えたため登録できません。 <VLAN ID>：VLAN ID
vlan[<VLAN ID>] : Protocol {ethertype | llc | snap-ethertype} <HEX> duplicate at ChGr[<Channel group#>].	同じポートチャネル上には同じプロトコル値で識別する VLAN は一つしか設定できません。 <VLAN ID>：VLAN ID <HEX>：プロトコル値 <Channel group#>：チャネルグループ番号
vlan[<VLAN ID>] : Protocol {ethertype | llc | snap-ethertype} <HEX> duplicate at port[<IF#>].	同じポート上には同じプロトコル値で識別する VLAN は一つしか設定できません。 <VLAN ID>：VLAN ID <HEX>：プロトコル値 <IF#>：イーサネットポート番号
vlan-protocol : Cannot delete protocol referred by VLAN configuration.	protocol で使用しているため削除できません。
vlan-protocol : maximum number which can be used is exceeded.	装置全体で使用するプロトコル値（ethertype 値，llc 値，snap-ethertype 値）は最大 16 個です。16 個を超えて設定できません。

37.1.10　スパニングツリー情報

表 37-10　スパニングツリーのエラーメッセージ

メッセージ	内容
Can not configure spanning-tree when Ring Protocol is configured.	Ring Protocol 機能が設定されているため，スパニングツリーを設定できません。
Cost is over 65535, please set up in 1 to 65535 or set pathcost method to long.	cost の値が 65535 以上です。cost の値を 1 から 65535 の範囲で設定するか，pathcost method を long にしてください。
Maximum number of entries are already defined. <STP_VLAN>	最大エントリ数以上のエントリを追加しようとしています。不要なエントリを削除してから追加してください。
Maximum number of MST instance are already defined.	MST インスタンス数がすでに最大数設定されています。設定できる MST インスタンスは最大 16 です。
Pathcost method is short, please set up in 1 to 65535 or set pathcost method to long.	pathcost method が short です。cost の値を 1 から 65535 の範囲で設定するか，pathcost method を long にしてください。
Relations between l2protocol-tunnel stp and spanning-tree configuration are inconsistent.	BPDU フォワーディングコンフィグレーションとスパニングツリーコンフィグレーションとの関係が不一致です。BPDU フォワーディングコンフィグレーションを設定する際は，スパニングツリーを停止する必要があります。
Relations between PVST+ and the protocol-vlan or mac-vlan configuration are inconsistent.	PVST+ と，プロトコル VLAN または MAC VLAN は同時に設定できません。
Too many parameters (VLAN-range of MST Instance <MSTI ID>).	入力パラメータ数が最大数（200）を超えています。最大数以内で設定してください。 <MSTI ID>：MST インスタンス ID

37.1.11　Ring Protocol 情報

表 37-11　Ring Protocol のエラーメッセージ

メッセージ	内容
axrp-<Ring ID>: cannot configure this command to channel-group port.	ポートチャネルに参加しているインタフェースに，リングポートは設定できません。 <Ring ID>：リング ID
axrp-<Ring ID>: Can't delete axrp configuration referred by other.	指定したリング ID は，axrp-ring-port コマンドで使用しているため削除できません。 <Ring ID>：リング ID
axrp-<Ring ID>: maximum number of ring-id are already defined.	装置全体で使用できるリング ID は最大 4 個です。4 個を超えて設定できません。 リング ID を追加する場合は，登録済みのリング ID を削除してください。 <Ring ID>：リング ID
axrp-<Ring ID>: maximum number of ring-port are already defined.	リングポートは，一つのリング ID に対して二つ設定します。 別のポートをリングポートに設定する場合は，設定済みのリングポートを削除してください。 <Ring ID>：リング ID
axrp-<Ring ID>: Relations between uplink redundant and ring protocol are inconsistent.	指定されたインタフェースは，アップリンク・リダンダント機能がすでに設定されています。 アップリンク・リダンダント機能を削除するか，または別のインタフェースを指定してください。 <Ring ID>：リング ID

メッセージ	内容
axrp-<Ring ID>: this interface is already defined as a ring port of other ring configured the same vlan-mapping.	指定されたインタフェースは，本コマンドで指定したリングに適用されている VLAN マッピングと同じ VLAN マッピングを適用しているほかのリングのリングポートとして，すでに設定されています。 当該インタフェースを共有リンク指定するか，または別のインタフェースを指定してください。 <Ring ID>：リング ID
axrp-<Ring ID>: vlan <VLAN ID> is already configured in control-vlan.	指定された VLAN は，すでに制御 VLAN に設定されています。 制御 VLAN から該当 VLAN を削除するか，別の VLAN を使用してください。 <Ring ID>：リング ID <VLAN ID>：VLAN ID
axrp-<Ring ID>: vlan <VLAN ID> is already configured in control-vlan of other ring.	指定された VLAN は，すでにほかのリングの制御 VLAN に設定されています。 ほかのリングの制御 VLAN から該当 VLAN を削除するか，別の VLAN を使用してください。 <Ring ID>：リング ID <VLAN ID>：VLAN ID
axrp-<Ring ID>: vlan <VLAN ID> is already configured in multi-fault-detection-vlan.	指定された VLAN は，すでに多重障害監視 VLAN に設定されています。 多重障害監視 VLAN から該当 VLAN を削除するか，別の VLAN を使用してください。 <Ring ID>：リング ID <VLAN ID>：VLAN ID
axrp-<Ring ID>: vlan <VLAN ID> is already configured in multi-fault-detection-vlan of other ring.	指定された VLAN は，すでにほかのリングの多重障害監視 VLAN に設定されています。 ほかのリングの多重障害監視 VLAN から該当 VLAN を削除するか，別の VLAN を使用してください。 <Ring ID>：リング ID <VLAN ID>：VLAN ID
axrp-<Ring ID>: vlan <VLAN ID> is already configured in vlan-mapping.	指定された VLAN は，すでに VLAN マッピングに設定されています。 VLAN マッピングから該当 VLAN を削除するか，別の VLAN を使用してください。 <Ring ID>：リング ID <VLAN ID>：VLAN ID
axrp-<Ring ID>: vlan-mapping <Mapping ID> is already configured in vlan-group of other ring.	指定された VLAN マッピングは，すでにほかのリングの VLAN グループに設定されています。 ほかの VLAN グループから削除するか，別の VLAN グループを使用してください。 <Ring ID>：リング ID <Mapping ID>：VLAN マッピング ID
axrp-<Ring ID>-<Group ID>: vlan-mapping <Mapping ID> is already configured in another vlan-group.	指定された VLAN マッピングはすでに同一リングの別の VLAN グループに設定されています。 ほかの VLAN グループから削除するか，別の VLAN マッピングを使用してください。 <Ring ID>：リング ID <Group ID>：VLAN グループ ID <Mapping ID>：VLAN マッピング ID
axrp-vlan-mapping-<Mapping ID>: vlan <VLAN ID> is already configured in control-vlan.	指定された VLAN は，すでに制御 VLAN に設定されています。 制御 VLAN から該当 VLAN を削除するか，別の VLAN を使用してください。

メッセージ	内容
	<Mapping ID>：VLAN マッピング ID <VLAN ID>：VLAN ID
axrp-vlan-mapping-<Mapping ID>: vlan <VLAN ID> is already configured in multi-fault-detection-vlan.	指定された VLAN は，すでに多重障害監視 VLAN に設定されています。 多重障害監視 VLAN から該当 VLAN を削除するか，別の VLAN を使用してください。 <Mapping ID>：VLAN マッピング ID <VLAN ID>：VLAN ID
axrp-vlan-mapping-<Mapping ID>: vlan <VLAN ID> is already configured in other vlan-mapping.	指定された VLAN は，すでにほかのマッピングに設定されています。 ほかの VLAN マッピングから該当 VLAN を削除するか，別の VLAN を使用してください。 <Mapping ID>：VLAN マッピング ID <VLAN ID>：VLAN ID
Cannot configure Ring Protocol when spanning-tree is configured.	スパニングツリーが設定されているため，Ring Protocol 機能を設定できません。

37.1.12　IGMP snooping 情報

表 37-12　IGMP snooping のエラーメッセージ

メッセージ	内容
Maximum number of VLAN are already defined, <VLAN ID> igmp snooping can not enable.	IGMP snooping と MLD snooping で指定できる vlan の合計は最大 32 個です。32 を超えて設定できません。 <VLAN ID> : VLAN ID
system function isn't set.	system function 設定がないため設定できません。 system function で igmp-snooping を設定してください。

37.1.13　MLD snooping 情報

表 37-13　MLD snooping のエラーメッセージ

メッセージ	内容
Duplicate mld query message source address.	同じ MLD Query メッセージの送信元 IP アドレスが定義されているため設定できません。
Maximum number of VLAN are already defined, <VLAN ID> mld snooping can not enable.	IGMP snooping と MLD snooping で指定できる vlan の合計は最大 32 個です。32 を超えて設定できません。 <VLAN ID> : VLAN ID
system function isn't set.	system function 設定がないため設定できません。 system function で mld-snooping を設定してください。

37.1.14　IPv4・ARP・ICMP 情報

表 37-14　IPv4・ARP・ICMP のエラーメッセージ

メッセージ	内容
ip : Inconsistency has occurred in a setting of IP address and route.	IP 情報で設定したアドレスとルート情報で設定した nexthop のネットワークアドレスに矛盾が生じています。 nexthop を正しく設定してください。
ip : IP address is duplicate between interface and nexthop.	IP 情報で設定したアドレスとルート情報で設定した nexthop のアドレスが重複しています。 アドレスが重複しないように設定してください。
ip : maximum number of route are already defined.	これ以上ルート情報を設定できません。 ネットワーク構成を見直してください。
ip[<VLAN ID>] : Can't delete IP configuration with route configuration.	ルート情報が存在しています。 ルート情報を削除した後，IP 情報を削除してください。 <VLAN ID> : VLAN ID
ip[<VLAN ID>] : Duplicate network address.	他の VLAN に，同じネットワークアドレスの IP アドレスが定義されています。 すべてのネットワークアドレスがユニークになるように IP アドレスを設定してください。 <VLAN ID> : VLAN ID
	Web 認証専用 IP アドレスに，同じネットワークアドレスの IP アドレスが定義されています。 Web 認証専用 IP アドレスのネットワークアドレスと重複しないように，IP アドレスを設定してください。 <VLAN ID> : VLAN ID
ip[<VLAN ID>] : maximum number of IP configuration are already defined.	これ以上 IP アドレスを設定できません。 ネットワーク構成を見直してください。 <VLAN ID> : VLAN ID

37.1.15　フロー検出モード情報

表 37-15　フローモードのエラーメッセージ

メッセージ	内容
Cannot change the flow detection mode.	以下が設定されているため，フロー検出モードを変更できません。 ・インタフェースにアクセスリスト適用 ・インタフェースに QoS フローリスト適用 ・access-redirect http port フロー検出モードを変更したい場合は，上記の設定をすべて削除してください。

37.1.16　アクセスリスト情報

表 37-16　アクセスリストのエラーメッセージ

メッセージ	内容
Cannot attach this list because flow detection mode Layer2-1.	フロー検出モードが Layer2-1 の場合には，このアクセスリストは適用できません。 フロー検出モードが Layer2-1 のとき，MAC アクセスリストが適用できます。 次のコマンドが使用できます。 mac access-group コマンド
Cannot attach this list because flow detection mode Layer2-2.	フロー検出モードが Layer2-2 の場合には，このアクセスリストは適用できません。 フロー検出モードが Layer2-2 のとき，IPv4 アクセスリストが適用できます。 次のコマンドが使用できます。 ip access-group コマンド
Maximum number of entries are already defined. <value1>	最大エントリ数以上のエントリを追加しようとしています。不要なエントリを削除してから追加してください。
Over two entry as an address family cannot be set.	ほかのアクセスリストがすでに適用済みです。 アクセスリストを適用したい場合には，適用されているアクセスリストの適用を削除してから，行ってください。
system function isn't set.	system function 設定がないため設定できません。 system function で filter を指定してください。
The sequence number exceeded the maximum value. Try "resequence" Command.	自動シーケンス番号が最大値を超えました。 resequence を実行してください。
This list cannot be set to this port.	このアクセスリストはこのイーサネットインタフェースには適用できません。 イーサネットインタフェースにアクセスリストを適用する場合には，アクセスリスト内のフロー検出条件の VLAN ID が適用するイーサネットインタフェースの設定内容に含まれている必要があります。
This list cannot be set to VLAN.	このアクセスリストは VLAN インタフェースには適用できません。 アクセスリスト内のフロー検出条件に VLAN ID が指定されている場合には，そのアクセスリストは VLAN インタフェースには適用できません。 イーサネットインタフェースに適用するか，検出条件から VLAN ID を削除してください。
This list name is being used as other protocol type by other definition.	その識別子はほかのアクセスリストで使用済みの名称のため指定できません。 ほかのアクセスリストで使用していない名称を指定してください。
The maximum number of entries are exceeded.	設定可能なエントリ数を超えました。不要なエントリを削除してから実行してください。

37.1.17 QoS 情報

表 37-17 QoS のエラーメッセージ

メッセージ	内容
Can not set command, because limit-queue-length command is set.	limit-queue-length コマンドが設定されているため，PQ 以外のスケジューリングモードは設定できません。
Can not set command, because scheduling modes is not PQ.	PQ 以外のスケジューリングモードが設定されているため，limit-queue-length コマンドは設定できません。
Can not set half duplex because traffic-shape rate is specified for the port.	回線にポート帯域制御が指定されているため，duplex に設定できません。
Can not set half duplex because WFQ min-rate is specified for the port.	回線に WFQ モードの最低保証帯域が指定されているため，duplex に設定できません。
Can not set traffic-shape rate because of the port is half duplex.	回線が半二重のため，ポート帯域制御を指定できません。
Can not set WFQ min-rate because of the port is half duplex.	回線が半二重のため，WFQ モードの最低保証帯域を指定できません。
Cannot attach this list because flow detection mode Layer2-1.	フロー検出モードが Layer2-1 の場合には，この QoS フローリストは適用できません。 フロー検出モードが Layer2-1 のとき，MAC QoS フローリストが適用できます。 次のコマンドが使用できます。 mac qos-flow-group コマンド
Cannot attach this list because flow detection mode Layer2-2.	フロー検出モードが Layer2-2 の場合には，この QoS フローリストは適用できません。 フロー検出モードが Layer2-2 のとき，IPv4 QoS フローリストが適用できます。 次のコマンドが使用できます。 ip qos-flow-group コマンド
Maximum number of entries are already defined. <value1>	最大エントリ数以上のエントリを追加しようとしています。不要なエントリを削除してから追加してください。
Over two entry as an address family cannot be set.	ほかの QoS フローリストがすでに適用済みです。 QoS フローリストを適用したい場合には，適用されている QoS フローリストの適用を削除してから，行ってください。
system function isn't set.	system function 設定がないため設定できません。 system function で qos を指定してください。
The different name is already defined.	既に queue-group が設定されている I/F にエントリ追加しようとした場合
The Maximum number of entries are already defined. <QOSFLOW_GROUP>	QoS フローリストの I/F への最大適用数を超えています。
The Maximum number of entries are already defined. <QOSFLOW_LIST>	QoS フローリスト remark の最大設定数を超えています。
The Maximum number of entries are already defined. <QOSFLOW_MAC>	MAC-QoS フローリストのエントリ数が収容条件を超えています。
The maximum number of entries are exceeded.	QoS エントリ数が収容条件を超えています。 なお，このコンフィグレーションでの使用エントリ数および空きエントリ数は show system コマンドで確認できます。
The sequence number exceeded the maximum value. Try "resequence" Command.	自動シーケンス番号が最大値を超過しました。resequence コマンドを実行してください。
The total of min-rate exceeded bandwidth of port.	指定した最低保証帯域の総和が回線帯域を超えています。 回線帯域以下になるように設定してください。

メッセージ	内容
This list cannot be set to this port.	この QoS フローリストはこのイーサネットインタフェースには適用できません。 イーサネットインタフェースに QoS フローリストを適用する場合には，QoS フローリスト内のフロー検出条件の VLAN ID が適用するイーサネットインタフェースの設定内容に含まれている必要があります。
This list cannot be set to VLAN.	この QoS フローリストは VLAN インタフェースには適用できません。 QoS フローリスト内のフロー検出条件に VLAN ID が指定されている場合には，その QoS フローリストは VLAN インタフェースには適用できません。イーサネットインタフェースに適用するか，検出条件から VLAN ID を削除してください。
This list name is being used as other protocol type by other definition.	ほかの QoS フローリストで使用済みの名称です。 ほかの QoS フローリストで使用していない名称または対象となる QoS フローリストを指定してください。

37.1.18 レイヤ 2 認証共通情報

表 37-18 レイヤ 2 認証共通のエラーメッセージ

メッセージ	内容
interface : Invalid access-list ID for authentication.	authentication ip access-group で適用済みのアクセスリストと異なります。(適用可能リスト名称は 1 つだけです。) 既に設定済みのアクセスリストを設定してください。または，他のインタフェースで適用済みのアクセスリストをすべて削除後，再設定してください。
interface : Invalid authentication arp-relay configuration.	該当ポートに下記コマンドがどれも設定されていないため，authentication arp-relay を設定できません。 • dot1x port-control • web-authentication port • mac-authentication port いずれかを該当ポートに設定後，再設定してください。
interface : Invalid authentication ip access-group configuration.	該当ポートに下記コマンドがどれも設定されていないため，authentication arp-relay を設定できません。 • dot1x port-control • web-authentication port • mac-authentication port いずれかを該当ポートに設定後，再設定してください。
interface : Over two entry as an address family cannot be set.	ほかのアクセスリストがすでに適用済みです。 適用されているアクセスリストの適用を削除後，再設定してください。
interface : Relations between the switchport mac vlan and authentication force-authorized vlan are inconsistent.	指定した VLAN は MAC VLAN でないため，authentication force-authorized vlan を設定できません。

メッセージ	内容
interface : Relations between individual force-authorized and common force-authorized are inconsistent.	各認証機能の強制認証が設定されているため，指定ポートに authentication force-authorized vlan コマンドを設定できません。下記の設定を削除してください。 • dot1x force-authorized • dot1x force-authorized vlan • web-authentication force-authorized vlan • web-authentication static-vlan force-authorized • mac-authentication force-authorized vlan • mac-authentication static-vlan force-authorized
Relations between individual force-authorized and common force-authorized are inconsistent.	各認証機能の強制認証が設定されているため，authentication force-authorized enable コマンドを設定できません。下記の設定を削除してください。 • dot1x force-authorized • dot1x force-authorized vlan • web-authentication force-authorized vlan • web-authentication static-vlan force-authorized • mac-authentication force-authorized vlan • mac-authentication static-vlan force-authorized

37.1.19 IEEE802.1X 情報

表 37-19 IEEE802.1X のエラーメッセージ

メッセージ	内容
dot1x(xxxxx): Cannot set "dot1x port-control" because monitor session mode is set now.	interface xxxxx のポートミラーが有効になっているため，ポート単位認証を設定できません。 xxxxx : ethernet <IF#> : イーサネット インタフェースポート番号
dot1x(xxxxx): Cannot set " dot1x authentication " command because user-group or legacy mode configuration(s) is set now.	interface xxxxx にユーザ ID 別認証方式，またはレガシーモードが有効になっているため，dot1x authentication コマンドを設定できません。 下記の設定を削除してください。 • dot1x vlan dynamic enable • dot1x vlan dynamic radius-vlan • web-authentication user-group • web-authentication vlan • mac-authentication interface • mac-authentication vlan
dot1x(link-aggregation): Cannot set the configuration because the ethernet <IF#> belongs to the port-channel	指定の ethernet <IF#> はポートチャネルに属しているため，IEEE802.1X の設定できません。 <IF#> : インタフェースポート番号
dot1x(vlan dynamic): Cannot set "dot1x vlan dynamic ignore-eapol-start" because supplicant-detection is disable-method.	VLAN 単位認証（動的）の端末検出動作が disable であるため，端末要求再認証抑止機能を設定できません。
dot1x(vlan dynamic): Cannot set "dot1x vlan dynamic ignore-eapol-start" because reauthentication mode is invalid.	VLAN 単位認証 (動的) の再認証要求機能が有効になっていないため，端末要求再認証抑止機能を設定できません。
dot1x(vlan dynamic): Cannot set "dot1x vlan dynamic radius-vlan" because the specified vlan <VLAN ID> is not found.	指定された VLAN <VLAN ID> は装置に登録されていないため，radius-vlan として登録できません。 <VLAN ID> : VLAN ID
dot1x(vlan dynamic): Cannot set "dot1x vlan dynamic radius-vlan" because the specified vlan <VLAN ID> is not mac-vlan.	指定された VLAN <VLAN ID> は MAC VLAN ではないため，radius-vlan として登録できません。 <VLAN ID> : VLAN ID

メッセージ	内容
dot1x(vlan dynamic): Cannot set "dot1x vlan dynamic supplicant-detection disable" because ignore-eapol-start is set now.	VLAN 単位認証（動的）の端末要求認証抑止機能が設定されているため，端末検出動作を disable にできません。
dot1x(vlan dynamic): Cannot set "no dot1x vlan dynamic reauthentication" because ignore-eapol-start is set now.	VLAN 単位認証 (動的) の端末要求再認証抑止機能が設定されているため，再認証要求機能を無効にできません。
dot1x(xxxx): Cannot delete "dot1x port-control"　because authentication ip access-group/arp-relay is set.	interface xxxxx に，authentication arp-relay，authentication ip access-group が設定されているため，dot1x port-control を削除できません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(xxxx): Cannot delete "dot1x port-control"　because dot1x force-authorized is set.	interface xxxxx に，dot1x force-authorized コマンドが設定されているため，dot1x port-control を削除できません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(xxxx): Cannot set "dot1x force-authorized" because authentication force-authorized is set.	interface xxxxx の authentication force-authorized コマンドが設定されているため，dot1x force-authorized コマンドを設定できません。 ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(xxxx): Cannot set "dot1x force-authorized" because 802.1X auth mode is unmatch.	interface xxxxx の認証モードが異なるため，dot1x force-authorized コマンドを設定できません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(xxxxx): Cannot set "dot1x ignore-eapol-start" because reauthentication mode is invalid.	interface xxxxx の再認証要求機能が有効になっていないため，端末要求再認証抑止機能を設定できません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(xxxxx): Cannot set "dot1x ignore-eapol-start" because supplicant-detection is disable-method.	interface xxxxx の端末検出動作が disable であるため，端末要求再認証抑止機能を設定できません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x: Cannot set "aaa authentication dot1x" because the maximum number is already set.	認証方式リストは最大エントリ数登録されているため，これ以上登録できません。
dot1x(xxxxx): Cannot set "dot1x multiple-authentication" because force-mode is set now.	interface xxxxx が force-unauthorized または force-authorized モードになっているため，端末認証モードを設定できません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(xxxxx): Cannot set "dot1x port-control force" command because sub-mode is multiple-authentication.	interface xxxxx が端末認証モードになっているため。force-unauthorized または force-authorized モードを設定できません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号

メッセージ	内容
dot1x(xxxxx): Cannot set "dot1x port-control" because switchport mode is not access-mode.	interface xxxxx の switchport mode が access でないため，ポート単位認証を設定できません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(xxxxx):Cannot set "dot1x port-control force" because switchport mode is mac-vlan mode.	interface xxxxx(ethernet <IF#> または port-channel <Channel group#>) の switchport mode が MAC VLAN になっているため， force-unauthorized または force-authorized モードを設定できません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(xxxxx): Cannot set "dot1x supplicant-detection disable" because ignore-eapol-start is set now.	interface xxxxx の端末要求認証抑止機能が設定されているため，端末検出動作を disable にできません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(xxxxx): Cannot set "no dot1x reauthentication" because ignore-eapol-start is set now.	interface xxxxx の端末要求再認証抑止機能が設定されているため，再認証要求機能を無効にできません。 xxxxx： ethernet <IF#>：イーサネット インタフェースポート番号 port-channel <Channel group#>：ポートチャネル番号
dot1x(vlan dynamic): Cannot set "dot1x vlan dynamic enable" because authentication list or user-group is set.	ユーザ ID 別認証方式，またはポート別認証方式が設定されているため， dot1x vlan dynamic enable コマンドを設定できません。 下記の設定を削除してください。 • dot1x authentication • mac-authentication authentication • web-authentication authentication • web-authentication user-group
dot1x(vlan dynamic): Cannot set "dot1x vlan dynamic enable" because authentication multi-step is set.	マルチステップ認証が設定されているため，dot1x vlan dynamic enable コマンドを設定できません。 authentication multi-step コマンド設定を削除してください。
dot1x(vlan dynamic): Cannot set "dot1x vlan dynamic radius-vlan" because authentication list or user-group is set.	ユーザ ID 別認証方式，またはポート別認証方式が設定されているため， dot1x vlan dynamic radius-vlan コマンドを設定できません。 下記の設定を削除してください。 • dot1x authentication • mac-authentication authentication • web-authentication authentication • web-authentication user-group
dot1x(vlan dynamic): Cannot set "dot1x vlan dynamic radius-vlan" because the authentication multi-step is set.	マルチステップ認証が設定されているため，dot1x vlan dynamic radius-vlan コマンドを設定できません。 authentication multi-step コマンド設定を削除してください。
dot1x: Cannot set "dot1x system-auth-control" because l2protocol-tunnel eap configuration is valid now.	EAPOL フォワーディング機能が有効であるため，IEEE802.1X を設定できません。
l2protocol-tunnel: Cannot set "l2protocol-tunnel eap" because 802.1X configuration is valid now.	IEEE802.1X が有効であるため，EAPOL フォワーディング機能を設定できません。
radius-server: Cannot add new radius-server host because the maximum number is already set.	最大エントリ数登録されているため，これ以上登録できません。
radius-server: Port Number is duplicate between auth port and acct port.	auth-port と acct-port のポート番号が重複しています。

メッセージ	内容
system function isn't set.	system function 設定がないため，下記コマンドを設定できません。 • dot1x port-control auto • authentication arp-relay • authentication ip access-group
xxxxx: Cannot set the command because of internal error. (code=y)	内部エラーが発生し，コマンドを設定できませんでした。 xxxxx：dot1x / radius-server / l2protocol-tunnel / multi-step， y : 1, 2, 3, 4

37.1.20　Web 認証情報 (DHCP サーバ情報含む)

表 37-20　Web 認証のエラーメッセージ

メッセージ	内容
Conflicting port number.	Web 認証用ポート番号が重複しています。Web 認証用ポート番号が重複しないようにしてください。
Duplicate network address.	他の VLAN に, 同じネットワークアドレスの IP アドレスが定義されています。 VLAN のネットワークアドレスと重複しないように, Web 認証専用 IP アドレスを設定してください。
interface : Invalid web-authentication html-fileset configuration.	該当ポートに web-authentication port コマンドが設定されていないため，web-authentication html-fileset コマンドを設定できません。
interface : Invalid web-authentication port configuration.	該当ポートに下記コマンドが設定されているため，web-authentication port コマンドを削除できません。 • authentication ip access-group • authentication arp-relay • web-authentication html-fileset
interface : Relations between the web-authentication configuration and the channel-group configuration within same port.	指定ポートは Web 認証設定で使用しているため，ポートチャネルに加入できません。
interface : Relations between the web-authentication configuration and the vlan mode configuration are inconsistent.	指定ポートはプロトコルポート設定のため，Web 認証を設定できません。
interface : Relations between the web-authentication configuration and the mirror configuration are inconsistent.	指定ポートはミラーポート設定のため，Web 認証を設定できません。
interface : Relations between user-group or legacy mode configuration(s) and authentication list configuration(s) are inconsistent.	ユーザ ID 別認証方式，またはレガシーモードが設定されているため，web-authentication authentication コマンドを設定できません。 下記の設定を削除してください。 • dot1x vlan dynamic enable • dot1x vlan dynamic radius-vlan • web-authentication user-group • web-authentication vlan • mac-authentication interface • mac-authentication vlan
interface : Cannot set the command because the specified vlan <VLAN ID> is not found.	指定した VLAN が MAC VLAN ではないため，設定できません。 <VLAN ID>:VLAN ID

メッセージ	内容
interface : Relations between individual force-authorized and common force-authorized are inconsistent.	認証機能共通の強制認証が設定されているため，指定ポートに下記のコマンドを設定できません。 • web-authentication force-authorized vlan • web-authentication static-vlan force-authorized 下記の設定を削除してください。 • authentication force-authorized enable • authentication force-authorized vlan
radius-server: Cannot add new radius-server host because the maximum number is already set.	最大エントリ数登録されているため，これ以上登録できません。
radius-server: Port Number is duplicate between auth port and acct port.	auth-port と acct-port のポート番号が重複しています。
system function isn't set.	system function コマンド設定がないため，下記コマンドを設定できません。 • web-authentication ip address • web-authentication port system function で extended-authentication を設定してください。
web-auth : Cannot set the command because the specified vlan <VLAN ID> is not found.	指定した VLAN が MAC VLAN ではないため，設定できません。 <VLAN ID> : VLAN ID
web-auth : Cannot set the command because of internal error. (code=x)	内部エラーが発生し，コマンドを設定できません。
web-auth : Maximum number of entries are already defined. <LIST-NAME>	認証方式リストの最大エントリ数を超えました。
web-auth : Relations between multi-step configuration and web-authentication vlan configuration are inconsistent.	マルチステップ認証が設定されているため，web-authentication vlan コマンドを設定できません。 authentication multi-step コマンド設定を削除してください。
web-auth : Relations between authentication list or legacy mode configuration(s) and user-group configuration are inconsistent.	ポート別認証方式，またはレガシーモードが設定されているため，web-authentication user-group コマンドを設定できません。 下記の設定を削除してください。 • dot1x authentication • dot1x vlan dynamic enable • dot1x vlan dynamic radius-vlan • web-authentication authentication • web-authentication vlan • mac-authentication authentication • mac-authentication interface • mac-authentication vlan
web-auth : Relations between user-group or authentication list configuration(s) and legacy mode configuration(s) are inconsistent.	ユーザ ID 別認証方式，またはポート別認証方式が設定されているため，web-authentication vlan コマンドを設定できません。 下記の設定を削除してください。 • dot1x authentication • web-authentication authentication • web-authentication user-group • mac-authentication authentication

表 37-21　Web 認証のエラーメッセージ（内蔵 DHCP サーバ設定）

メッセージ	内容
Can not delete it because data is not corresponding.	指定された設定が存在しないため削除できません。
Interface not found.	VLAN または IP アドレスが設定されていません。VLAN と IP の設定を見直してください。

メッセージ	内容
Invalid network.	ネットワークの設定が不正です。
ip [<VLAN ID>]: Can't delete IP configuration with dhcp configuration.	DHCP サーバ設定で使用しているため IP を削除または変更できません。 <VLAN ID> : VLAN ID
It exceeded maximum number of IP-address pool.	IP アドレスプールの最大値を超えました。network と除外アドレス設定を見直してください。
Maximum number of entries are already defined. <DHCP-EXCLUDED-ADDRESS>	設定可能な除外アドレス数の最大値を超えました。
Maximum number of entries are already defined. <DHCP-IF>	設定可能なインタフェース数の最大値を超えました。
Maximum number of entries are already defined. <DHCP-POOL>	設定可能なプール数の最大値を超えました。
network conflicts.	ネットワークの設定が重複しています。
vlan [<VLAN ID>]: Can't delete vlan configuration referred by other configuration.	DHCP サーバ設定で使用しているため VLAN を削除できません。 <VLAN ID> : VLAN ID

37.1.21 MAC 認証情報

表 37-22 MAC 認証のエラーメッセージ

メッセージ	内容
interface : Invalid mac-authentication port configuration.	該当ポートに authentication ip access-group，または authentication arp-relay 設定があるため削除できません。
interface : Relations between the mac-authentication configuration and the vlan mode configuration are inconsistent.	指定ポートはプロトコルポート設定のため，MAC 認証を設定できません。
interface : Relations between the mac-authentication configuration and the mirror configuration are inconsistent.	指定ポートはミラーポート設定のため，MAC 認証を設定できません。
interface : Relations between the mac-authentication configuration and the channel-group configuration within same port.	指定ポートは MAC 認証設定で使用しているため，ポートチャネルに加入できません。
interface : Cannot set the command because the specified vlan <VLAN ID> is not found.	指定した VLAN が MAC VLAN ではないため，設定できません。 <VLAN ID>:VLAN ID
interface : Relations between individual force-authorized and common force-authorized are inconsistent.	認証機能共通の強制認証が設定されているため，指定ポートに下記のコマンドを設定できません。 • mac-authentication force-authorized vlan • mac-authentication static-vlan force-authorized 下記の設定を削除してください。 • authentication force-authorized enable • authentication force-authorized vlan
interface : Relations between user-group or legacy mode configuration(s) and authentication list configuration(s) are inconsistent.	ユーザ ID 別認証方式，またはレガシーモードが設定されているため，mac-authentication authentication コマンドを設定できません。 下記の設定を削除してください。 • dot1x vlan dynamic enable • dot1x vlan dynamic radius-vlan • web-authentication user-group • web-authentication vlan • mac-authentication interface • mac-authentication vlan

メッセージ	内容
mac-auth : Cannot set the command because the specified vlan ＜ VLAN ID> is not found.	指定した VLAN が MAC VLAN ではないため，設定できません。 <VLAN ID>:VLAN ID
mac-auth : Cannot set the command because of internal error. (code=x)	内部エラーが発生し，コマンド設定をできません。
mac-auth : Maximum number of entries are already defined. <LIST-NAME>	認証方式リストの最大エントリ数を超えました。
mac-auth : Relations between multi-step configuration and mac-authentication interface configuration are inconsistent.	マルチステップ認証が設定されているため，mac-authentication interface コマンドを設定できません。 authentication multi-step コマンド設定を削除してください。
mac-auth : Relations between multi-step configuration and mac-authentication vlan configuration are inconsistent.	マルチステップ認証が設定されているため，mac-authentication vlan コマンドを設定できません。 authentication multi-step コマンド設定を削除してください。
mac-auth : Relations between user-group or authentication list configuration(s) and legacy mode configuration(s) are inconsistent.	ユーザ ID 別認証方式，またはポート別認証方式が設定されているため，下記のコマンドを設定できません。 • mac-authentication interface • mac-authentication vlan 下記の設定を削除してください。 • dot1x authentication • web-authentication authentication • web-authentication user-group • mac-authentication authentication
radius-server: Cannot add new radius-server host because the maximum number is already set.	最大エントリ数登録されているため，これ以上登録できません。
radius-server: Port Number is duplicate between auth port and acct port.	auth-port と acct-port のポート番号が重複しています。
system function isn't set.	system function 設定がないため，mac-authentication port を設定できません。 system function extended-authentication を設定してください。

37.1.22　マルチステップ認証情報

表 37-23　マルチステップ認証のエラーメッセージ

メッセージ	内容
interface : Relations between multi-step configuration and legacy mode configuration(s) are inconsistent.	レガシーモードが有効になっているため，authentication multi-step コマンドを設定できません。 下記の設定を削除してください。 • dot1x vlan dynamic enable • dot1x vlan dynamic radius-vlan • mac-authentication interface • mac-authentication vlan • web-authentication vlan
multi-step: Cannot set the command because of internal error. (code=x)	内部エラーが発生し，コマンドを設定できませんでした。 x : 1, 2

37.1.23 DHCP snooping 情報

表 37-24 DHCP snooping のエラーメッセージ

メッセージ	内容
Can't delete it because data is not corresponding.	指定 VLAN の DHCP snooping が有効になっていない，または指定したコンフィグレーションが存在しないため削除できません。
Can't delete it vlan configuration referred by other configuration.	ip source binding 設定で VLAN を使用しているため削除できません。 削除対象 VLAN を指定している ip source binding 設定を先に削除してください。
Can't set it because snooping is disable.	指定した VLAN は DHCP snooping が有効になっていないため指定できません。 DHCP snooping を有効にした VLAN を指定してください。
Can't set it because vlan doesn't exist.	ip dhcp snooping vlan で指定した VLAN が存在しないため設定できません。
	ip arp inspection vlan で指定した VLAN が存在しないため設定できません。
Duplicate entry.	設定が重複しているため設定できません。 重複している設定を削除した後，再設定してください。
Maximum number of entries are already defined.	ip dhcp snooping vlan で指定した VLAN の設定が設定可能上限数を超えています。
	ip source binding での Config 設定，および dynamic 学習の総数がバインディングデータベースエントリの上限を超えたため設定できません。不要な Config 設定や dynamic 学習を削除した後，再設定してください。
	ip arp inspection vlan で設定した VLAN 数が設定可能上限数を超えています。
Relations between ip dhcp snooping configuration and channel-group configuration are inconsistent.	該当ポートはチャネルグループに属しているため設定できません。 ポートチャネルインタフェースに設定してください。
Relations between ip source binding configuration and channel-group configuration are inconsistent.	指定したポートはチャネルグループに属している，または指定したポートチャネルは存在しないため設定できません。
Relations between ip source binding configuration and switchport configuration are inconsistent.	指定したインタフェースは VLAN に属していないため設定できません。
Relations between ip verify source configuration and channel-group configuration are inconsistent.	該当ポートはチャネルグループに属しているため設定できません。 ポートチャネルインタフェースに設定してください。
system function isn't set.	system function 設定がないため設定できません。 system function で dhcp-snooping を設定してください。

37.1.24 特定端末の Web 通信不可表示機能情報

表 37-25 特定端末の Web 通信不可表示機能のエラーメッセージ

メッセージ	内容
Cannot change access-redirect because access-group is set.	ip access-group が設定されているため，access-redirect を変更できません。

メッセージ	内容
Duplicated port numbers.	ポート番号が重複しています。 ポート番号が重複しないようにしてください。
Incompatible flow detection mode.	このフロー検出モードでは設定できません。 access-redirect を設定・変更・削除する場合は，フロー検出モードに layer2-2 を設定してください。

37.1.25　アップリンク・リダンダント情報

表 37-26　アップリンク・リダンダントのエラーメッセージ

メッセージ	内容
Can't set ethernet <IF#> because it is a channel-group port.	指定されたインタフェースは，チャネルグループに所属しているため，インタフェースの設定変更ができません。 <IF#>：インタフェースポート番号
Ethernet <IF#> is already an uplink redundant interface.	指定されたインタフェースは，アップリンク・リダンダント機能がすでに設定されています。 <IF#>：インタフェースポート番号
Ethernet <IF#> Relations between uplink redundant and ring protocol are inconsistent.	指定されたインタフェースは，Ring Protocol 機能がすでに設定されています。Ring Protocol 機能を削除するか，または別のインタフェースを設定してください。 <IF#>：インタフェースポート番号
Port-channel <Channel group#> is already an uplink redundant interface.	指定されたインタフェースは，アップリンク・リダンダント機能がすでに設定されています。 <Channel group#>：ポートチャネル番号
Port-channel <Channel group#> Relations between uplink redundant and ring protocol are inconsistent.	指定されたインタフェースは，Ring Protocol 機能がすでに設定されています。Ring Protocol 機能を削除するか，または別のインタフェースを設定してください。 <Channel group#>：ポートチャネル番号
Secondary interface is same as primary interface.	プライマリとセカンダリを同一ポートに設定しています。
this command is different from this one in channel-group port.	コンフィグレーションが異なるため，ポートチャネルに加入できません。
Too many parameters (exclude-VLAN).	入力パラメータ数が最大数（200）を超えています。最大数以内で設定してください。

37.1.26　ストームコントロール情報

表 37-27　ストームコントロールのエラーメッセージ

メッセージ	内容
Please lower the recovery threshold than the detection threshold.	ストーム検出閾値よりもストーム回復閾値を大きい値に指定しました。ストーム回復閾値はストーム検出閾値以下の値に設定してください。

37.1.27 L2 ループ検知情報

表 37-28 L2 ループ検知のエラーメッセージ

メッセージ	内容
L2LD : Can't setting port[<IF#>] because of channel-group port.	指定したポート番号はチャネルグループに所属しているため，loop-detection コマンドの設定を変更できません。 <IF#>：インタフェースポート番号
this command is different from this one in channel-group port.	loop-detection 設定が異なるため，チャネルグループに加入できません。

37.1.28 CFM 情報

表 37-29 CFM のエラーメッセージ

メッセージ	内容
ethernet : Can not delete it because data is not corresponding.	指定したコンフィグレーションが存在しない，またはデータが重複しているため，削除できません。
ethernet : Cannot change cfm domain direction.	ドメインで設定する MEP の方向は変更できません。 いったん該当コマンドを削除してから再設定してください。
ethernet : Can't delete this configuration referred by other configuration.	ほかのコンフィグレーションで参照しているため，本設定を変更できません。 参照しているコンフィグレーションを削除してから再設定してください。
ethernet : MA <No.> is already configured in cfm domain.	指定された MA 識別番号はすでにほかのドメインに設定されています。 <No.>：MA 識別番号
ethernet : MA name <Name> is already configured in cfm domain.	指定された MA 名称はすでに同一のドメインに設定されています。 <Name>：MA 名称
ethernet : Maximum number of entries are already defined. <CFM_MA>	収容条件以上のコンフィグレーションを設定しようとしているか，収容条件最大の環境でコンフィグレーションを変更しようとしています。 使用しないコンフィグレーションを削除してから再度設定してください。
ethernet : Not found <Level>.	指定したドメインレベルが見つかりません。ドメインレベルが設定されているか確認してください。 <Level>：ドメインレベル
ethernet : Not found <No.>.	指定した MA 識別番号が見つかりません。MA 識別番号が設定されているか確認してください。 <No.>：MA 識別番号
ethernet : Not found VLAN ID <VLAN ID> in MA.	プライマリで指定した VLAN ID が VLAN ID list に存在しません。MA で設定済みの VLAN ID を指定してください。 <VLAN ID>：VLAN ID
ethernet : Too many parameters (CFM_VLAN).	入力パラメータ数が最大数（256）を超えています。最大数以内で設定してください。
ethernet : VLAN ID <VLAN ID> is already configured in MA name.	指定された VLAN ID はすでにほかの MA 名称に設定されています。 < VLAN ID >：VLAN ID
interface : Can not delete it because data is not corresponding.	指定したコンフィグレーションが存在しない，またはデータが重複しているため，削除できません。
interface : Cannot change cfm mep direction.	MEP の方向は変更できません。 いったん該当コマンドを削除してから再設定してください。
interface : Cannot configure cfm enable to channel-group port.	ポートチャネルに参加しているインタフェースに CFM の enable を設定できません。
interface : Cannot configure cfm mep to channel-group port.	ポートチャネルに参加しているインタフェースに，MEP を設定できません。

メッセージ	内容
interface : Cannot configure cfm mip to channel-group port.	ポートチャネルに参加しているインタフェースに，MIP を設定できません。
interface : Domain level <Level> is set with a value less than cfm mep.	指定したドメインレベルが MEP の設定値以下の値で設定されています。 <Level>：ドメインレベル
interface : Domain level <Level> is set with values more than cfm mip.	指定したドメインレベルが MIP の設定値以上の値で設定されています。 <Level>：ドメインレベル
interface : Exceeded the number of the maximum port.	MEP と MIP を設定できるポート数を超えました。
interface : Maximum number of entries are already defined. <CFM_MEP>	収容条件以上のコンフィグレーションを設定しようとしているか，収容条件最大の環境でコンフィグレーションを変更しようとしています。 使用しないコンフィグレーションを削除してから再度設定してください。
interface : Maximum number of entries are already defined. <CFM_MIP>	収容条件以上のコンフィグレーションを設定しようとしているか，収容条件最大の環境でコンフィグレーションを変更しようとしています。 使用しないコンフィグレーションを削除してから再度設定してください。
interface : MEP ID <MEPID> is already configured in cfm mep.	指定された MEP ID はすでにほかの MEP に設定されています。 < MEPID >：MEP ID
interface : Not found <Level>.	指定したドメインレベルが見つかりません。ドメインレベルが設定されているか確認してください。 <Level>：ドメインレベル
interface : Not found <No.>.	指定した MA 識別番号が見つかりません。 MA 識別番号が設定されているか確認してください。 <No.>：MA 識別番号

37.1.29 SNMP 情報

表 37-30 SNMP のエラーメッセージ

メッセージ	内容
interface : Can not delete it because data is not corresponding.	存在しない識別番号を削除しようとしました。識別番号を再確認してください。
interface : Maximum number of entries are already defined. <RMON_HISTRY_CTR>	最大設定数を超えています。不要なエントリを削除してください。
interface : This configuration has already been set.	rmon collection history 設定時，識別番号が他インタフェースで使われています。 別の識別番号を指定するか，他インタフェースの同識別番号番号を削除してから再設定してください。
rmon : Can not delete it because data is not corresponding.	存在しない識別番号を削除しようとしました。識別番号を再確認してください。
rmon : Can't delete this configuration referred by other configuration.	削除指定した event エントリは，alarm エントリと関連付けがあるため削除できません。
rmon : Maximum number of entries are already defined. <RMON_ALARM>	最大設定数を超えています。不要なエントリを削除してください。
rmon : Maximum number of entries are already defined. <RMON_EVENT>	最大設定数を超えています。不要なエントリを削除してください。
rmon : Can not delete it because data is not corresponding.	存在しない識別番号を削除しようとしました。識別番号を再確認してください。
rmon : Not found <event_no>.	rising-event-index または falling-event-index に存在しないイベント識別番号を指定しました。 rising-event-index または falling-event-index を再確認してください。または該当イベント識別番号の設定後に再設定してください。

メッセージ	内容
rmon : Not supported <variable>.	variable にサポートしないオブジェクトまたは範囲外のインスタンス番号を指定しました。 オブジェクトおよびインスタンス番号を再確認してください。
rmon : RMON alarm rising threshold is less than falling threshold.	下方閾値が上方閾値より上回っています。下方閾値を上方閾値以下としてください。
snmp-server: Maximum number of entries are already defined. <SNMP_TRAP>	SNMP トラップ送信先情報の登録が最大数を超えました。不要なトラップ送信先情報を削除してから追加してください。
snmp-server: Maximum number of entries are already defined. <SNMP_VIEW>	SNMP コミュニティ情報の登録が最大数を超えました。不要なコミュニティ情報を削除してから追加してください。

37.1.30　ポートミラーリング情報

表 37-31　ポートミラーリングのエラーメッセージ

メッセージ	内容
Mirror port and dot1x are inconsistent.	destination interface を dot1x で使用しているためミラーポートに設定できません。
Mirror port and mac-authentication are inconsistent.	destination interface を MAC 認証で使用しているためミラーポートに設定できません。
Mirror port and web-authentication are inconsistent.	destination interface を Web 認証で使用しているためミラーポートに設定できません。
Mirror port and port-channel are inconsistent.	destination interface をポートチャネルで使用しているためミラーポートに設定できません。
Mirror port and switchport are inconsistent.	ミラーポートと switchport は同時に設定できません。
Port-channel <Channel group#> is not configured.	ミラーポートに指定されたポートチャネル番号は，ポートチャネルインタフェースが設定されていません。
The specified VLAN ID is already in use.	指定された VLAN 番号は既に使用中です。

索引

A

B

C

D

E

N

P

Q

R

S

T

V

W

こ