AX260A 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.4.21 対応

AX26A-S003-60

AlaxalA

■対象製品

このマニュアルは AX260A モデルを対象に記載しています。
また，AX260A のソフトウェア Ver.4.21 の機能について記載しています。ソフトウェア機能は，ソフトウェア OS-L2F，およびオプションライセンスによってサポートする機能について記載します。

■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。
Internet Explorer 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。
IPX は，Novell,Inc. の商標です。
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。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
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。
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

２０２０年　１１月　（第７版）　ＡＸ２６Ａ－Ｓ００３－６０

■著作権

All Rights Reserved, Copyright(C), 2016, 2020, ALAXALA Networks, Corp.

変更履歴

【Ver.4.21（第 7 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
2　運用端末接続	・ speedコマンドの注意事項を変更しました。
5　ログインセキュリティとRADIUS	・ aaa authentication loginコマンドを変更しました。 ・ 下記コマンドを追加しました。 aaa authentication enable aaa authentication enable end-by-reject
8　装置の管理	・ system logging format-addコマンドを追加しました。
9　ゼロタッチプロビジョンニング機能	・ 本章を追加しました。
13　MACアドレステーブル	・ mac-address-table learningコマンドの注意事項を変更しました。
24　QoS	・ limit-queue-lengthコマンドの注意事項を変更しました。
30　DHCP snooping	・ 下記のコマンドを追加しました。 ip dhcp snooping information no-check ip dhcp snooping information option format remote-id ip dhcp snooping information option-insert ip dhcp snooping vlan information option format-type circuit-id
31　ホワイトリスト機能【OP-WL】	・ white-list dataコマンドの説明を変更しました。
33　アップリンク・リダンダント	・ switchport-backup startup-active-port-selectionコマンドの注意事項を変更しました。
38　SNMP	・ 下記コマンドの説明を変更しました。 snmp-server host snmp-server user
41　LLDP	・ lldp management-addressコマンドを追加しました。
44　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。 スタック情報 DHCP snooping情報 特定端末へのWeb通信不可表示機能情報

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver.4.12（第 6 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	・ スタックに関する記述を追加しました。
運用端末接続	・ line vty コマンドの説明を変更しました。
スタック【OP-WLE】	・ 本章を追加しました。
イーサネット	・ 下記のコマンドを変更しました。 interface gigabitethernet link-relay source
MAC アドレステーブル	・ mac-address-table static コマンドにパラメータを追加しました。
VLAN	・ switchport mode コマンドにパラメータを追加しました。
IGMP snooping	・ ip igmp snooping mrouter コマンドにパラメータを追加しました。
IPv4・ARP・ICMP	・ ip route コマンドの説明を変更しました。

章・節・項・タイトル	追加・変更内容
アクセスリスト	・指定できる名称のアクセスリスト数に関する記述を変更しました。
QoS	・指定できる名称および値の QoS フローリスト数に関する記述を変更しました。 ・下記のコマンドを変更しました。 limit-queue-length qos（ip qos-flow-list） qos（ipv6 qos-flow-list） qos（mac qos-flow-list）
レイヤ 2 認証共通	・下記のコマンドを変更しました。 authentication max-user（global） authentication max-user（interface）
MAC 認証	・mac-authentication timeout quiet-period コマンドの説明を変更しました。
DHCP snooping	・ip source binding コマンドにパラメータを追加しました。
ホワイトリスト機能【OP-WL】	・white-list data コマンドを変更しました。
SNMP	・snmp-server traps コマンドを変更しました。
ポートミラーリング	・monitor session source コマンドを変更しました。
ポリシーベースミラーリング	・monitor session filter コマンドを変更しました。
コンフィグレーション編集時のエラーメッセージ	・スタック情報のエラーメッセージを追加しました。 ・下記情報のエラーメッセージを変更しました。 共通 VLAN 情報 IPv4・ARP・ICMP 情報 ホワイトリスト情報 ポートミラーリング情報

【Ver.4.10（第 5 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	• save コマンドに注意事項を追加しました。
イーサネット	• link-relay source コマンドを追加しました。
IGMP snooping	• ip igmp snooping query-interval コマンドを追加しました。
IEEE802.1X	• dot1x ignore-eapol-start コマンドの注意事項を変更しました。 • dot1x supplicant-detection コマンドに passive パラメータを追加しました。
ホワイトリスト機能【OP-WL】	• 下記のコマンドを追加しました。 white-list address permit white-list logging format-add white-list packet mode • white-list data コマンドの説明を変更しました。 • white-list enable コマンドに注意事項を追加しました。
コンフィグレーション編集時のエラーメッセージ	• イーサネット情報にリンク状態中継機能のエラーメッセージを追加しました。 • 下記情報のエラーメッセージを変更しました。 共通 IEEE802.1X 情報 ホワイトリスト情報

【Ver.4.7（第 4 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
装置の管理	• system recovery コマンドの説明を変更しました。
MAC アドレステーブル	• mac-address-table learning コマンドを追加しました。
IEEE802.1X	• dot1x supplicant-detection コマンドの説明を変更しました。
DHCP snooping	• 下記コマンドの説明を変更しました。 ip dhcp snooping information option allow-untrusted ip dhcp snooping vlan
ホワイトリスト機能【OP-WL】	• white-list monitor destination interface コマンドを変更しました。
特定端末への Web 通信不可表示機能	• 本章を追加しました。
ポートミラーリング	• switchport monitor dot1q tag コマンドを追加しました。 • 下記コマンドの説明を変更しました。 ip icmp monitor destination interface monitor session source
コンフィグレーション編集時のエラーメッセージ	• 特定端末への Web 通信不可表示機能情報のエラーメッセージを追加しました。 • 下記情報のエラーメッセージを変更しました。 共通 VLAN 情報 フロー検出モード情報 ポートミラーリング情報

【Ver.4.6（第 3 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	• 下記コマンドの記述を変更しました。 duplex speed
IGMP snooping	• 下記のコマンドを追加しました。 ip igmp snooping mrouter discovery ip igmp snooping mrouter discovery extension ip igmp snooping mrouter logging
フロー検出モード	• flow detection mode コマンドにパラメータを追加しました。
ポートミラーリング	• monitor session source コマンドの入力形式を変更しました。
ポートミラーリング	• 本章を追加しました。
コンフィグレーション編集時のエラーメッセージ	• ポリシーベースミラーリング情報のエラーメッセージを追加しました。 • 下記情報のエラーメッセージを変更しました。 共通 装置の管理情報 IGMP snooping 情報 フロー検出モード情報 アクセスリスト情報 QoS 情報 ポートミラーリング情報

【Ver.4.5（第 2 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
はじめに	• 「本バージョンでご使用時の注意事項」の記述を変更しました。
装置の管理	• system receive control コマンドを追加しました。
フロー検出モード	• flow detection mode コマンドの説明を変更しました。
IEEE802.1X	• 下記コマンドの説明を変更しました dot1x port-control dot1x supplicant-detection
Web 認証	• web-authentication redirect ignore-https コマンドを追加しました。 • http-server initial-timeout コマンドの説明を変更しました。
MAC 認証	• 下記コマンドの説明を変更しました mac-authentication access-group mac-authentication port mac-authentication system-auth-control
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。 共通 装置の管理情報

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AX260Aモデルを対象に記載しています。また，AX260Aのソフトウェア Ver.4.21の機能について記載しています。ソフトウェア機能は，ソフトウェア OS-L2F，およびオプションライセンスによってサポートする機能について記載します。
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。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 AX260Aに共通の機能について記載しますが，モデル固有の機能については以下のマークで示します。

【08TF】:
AX260A-08TFについての記述です。

【08T】:
AX260A-08Tについての記述です。

また，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-WL】:
オプションライセンス OP-WLについての記述です。

【OP-WLE】:
オプションライセンス OP-WLEについての記述です。
また，当該マークの記述は，オプションライセンス OP-WL登録済が前提です。

■本バージョンでご使用時の注意事項

本バージョンは，以下の機能に制限がありますので，当該機能に関するコマンドはご使用にならないでください。

本バージョンでの制限事項（未サポート項目）

対象機能	サポート項目	制限事項（未サポート）
OAN	－	全機能

■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。
http://www.alaxala.com

■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。

●初期導入時の基本的な設定について知りたい，ハードウェアの設備条件，取扱方法を調べる

AX260A
ハードウェア取扱説明書
(AX26A-H001)

●ラック搭載の手順について知りたい

MNTKIT-01
ハードウェア取扱説明書
(AXMK-H001)

●ソフトウェアの機能，コンフィグレーションの設定，運用コマンドについて知りたい

コンフィグレーションガイド
Vol.1
(AX26A-S001)

Vol.2
(AX26A-S002)

●コンフィグレーションコマンドの入力シンタックス，パラメータ詳細について知りたい

コンフィグレーション
コマンドレファレンス
(AX26A-S003)

●運用コマンドの入力シンタックス，パラメータ詳細について知りたい

運用コマンドレファレンス
(AX26A-S004)

●メッセージとログについて調べる

メッセージ・ログレファレンス
(AX26A-S005)

●MIBについて調べる

MIBレファレンス
(AX26A-S006)

●トラブル発生時の対処方法について知りたい

トラブルシューティングガイド
(AX26A-T001)

■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
SFP+	Enhanced Small Form factor Pluggable
SML	Split Multi Link
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

1 このマニュアルの読み方 1

コマンドの記述形式 2

コマンドモード一覧 3

パラメータに指定できる値 4

文字コード一覧 7

第 2 編　運用管理

2 運用端末接続 9

ftp-server 10

line console 11

line vty 12

speed 14

transport input 15

3 コンフィグレーションの編集と操作 17

end 18

exit 19

save(write) 20

show 21

top 22

4 スタック【OP-WLE】 23

switch【OP-WLE】 24

switch priority【OP-WLE】 25

switch provision【OP-WLE】 26

switchport stack cost【OP-WLE】 28

system mac-address【OP-WLE】 29

5 ログインセキュリティと RADIUS 31

aaa authentication enable 32

aaa authentication enable end-by-reject 34

aaa authentication login 35

aaa authentication login console 37
aaa authentication login end-by-reject 38
aaa group server radius 39
banner 41
ip access-group 43
ipv6 access-class 45
radius-server attribute station-id capitalize 47
radius-server dead-interval 48
radius-server host 50
radius-server key 53
radius-server retransmit 55
radius-server timeout 56
server 57

6 時刻の設定と NTP 59

コンフィグレーションコマンドと動作モードの対応 60
clock timezone 61
ntp authenticate 63
ntp authentication-key 64
ntp broadcast 66
ntp broadcast client（global） 68
ntp broadcast client（interface） 69
ntp broadcastdelay 70
ntp interval 71
ntp master 72
ntp peer 73
ntp server 75
ntp trusted-key 77
sntp client 78

7 ホスト名と DNS 81

ip domain lookup 82
ip domain name 83
ip domain reverse-lookup 84
ip host 85
ip name-server 86
ipv6 host 87

8 装置の管理 89

system l2-table mode 90
system logging format-add 91

system memory-soft-error 92
system receive alarm logging 93
system receive alarm parameters 94
system receive control 96
system receive rate-limit 97
system recovery 98
system temperature-warning-level 99
system temperature-warning-level average 100

9 ゼロタッチプロビジョンニング機能 103
system zero-touch-provisioning 104
system zero-touch-provisioning vlan 105

10 省電力機能 107
power-control port cool-standby 108
schedule-power-control port cool-standby 109
schedule-power-control port-led 110
schedule-power-control shutdown 112
schedule-power-control system-sleep 114
schedule-power-control time-range 115
system port-led 120
system port-led trigger console 122
system port-led trigger interface 123
system port-led trigger mc 124

第 3 編　ネットワークインタフェース

11 イーサネット 125
bandwidth 126
description 127
duplex 128
flowcontrol 130
interface gigabitethernet 132
link debounce 133
link up-debounce 134
link-relay source 135
mdix auto 136
mtu 137
shutdown 139
speed 140

system mtu 142

12 リンクアグリゲーション 145

channel-group lacp system-priority 146
channel-group max-active-port 147
channel-group mode 149
channel-group periodic-timer 151
description 152
interface port-channel 153
lacp port-priority 154
lacp system-priority 155
shutdown 156

第 4 編　レイヤ 2 スイッチング

13 MAC アドレステーブル 157

mac-address-table aging-time 158
mac-address-table learning 159
mac-address-table static 160

14 VLAN 163

interface vlan 164
l2protocol-tunnel eap 165
l2protocol-tunnel stp 166
mac-address 167
name 168
protocol 169
state 170
switchport access 171
switchport dot1q ethertype 172
switchport isolation 173
switchport mac 175
switchport mac auto-vlan 178
switchport mode 179
switchport protocol 181
switchport trunk 183
switchport vlan mapping 185
switchport vlan mapping enable 187
vlan 188
vlan-dot1q-ethertype 191

vlan-protocol 192

15 スパニングツリー 195

instance 197
name 199
revision 200
spanning-tree bpdufilter 201
spanning-tree bpduguard 202
spanning-tree cost 203
spanning-tree disable 205
spanning-tree guard 206
spanning-tree link-type 208
spanning-tree loopguard default 209
spanning-tree mode 210
spanning-tree mst configuration 211
spanning-tree mst cost 212
spanning-tree mst forward-time 213
spanning-tree mst hello-time 214
spanning-tree mst max-age 215
spanning-tree mst max-hops 216
spanning-tree mst port-priority 217
spanning-tree mst root priority 218
spanning-tree mst transmission-limit 219
spanning-tree pathcost method 220
spanning-tree port-priority 222
spanning-tree portfast 223
spanning-tree portfast bpduguard default 224
spanning-tree portfast default 225
spanning-tree single 226
spanning-tree single cost 227
spanning-tree single forward-time 228
spanning-tree single hello-time 229
spanning-tree single max-age 230
spanning-tree single mode 231
spanning-tree single pathcost method 232
spanning-tree single port-priority 234
spanning-tree single priority 235
spanning-tree single transmission-limit 236
spanning-tree vlan 237
spanning-tree vlan cost 238
spanning-tree vlan forward-time 240
spanning-tree vlan hello-time 242
spanning-tree vlan max-age 243

spanning-tree vlan mode 244
spanning-tree vlan pathcost method 245
spanning-tree vlan port-priority 247
spanning-tree vlan priority 248
spanning-tree vlan transmission-limit 249

16 Ring Protocol 251

axrp 252
axrp virtual-link 253
axrp vlan-mapping 254
axrp-primary-port 256
axrp-ring-port 258
control-vlan 260
disable 262
flush-request-count 263
flush-request-transmit vlan 264
forwarding-shift-time 265
health-check holdtime 266
health-check interval 267
mode 268
multi-fault-detection holdtime 270
multi-fault-detection interval 271
multi-fault-detection mode 272
multi-fault-detection vlan 274
name 275
preempt-delay 276
vlan-group 277

17 IGMP snooping 279

ip igmp snooping（global） 280
ip igmp snooping（interface） 281
ip igmp snooping fast-leave 282
ip igmp snooping mrouter 283
ip igmp snooping mrouter discovery 284
ip igmp snooping mrouter discovery extension 285
ip igmp snooping mrouter logging 286
ip igmp snooping querier 287
ip igmp snooping query-interval 288

18 MLD snooping 289

ipv6 mld snooping（global） 290

ipv6 mld snooping（interface） 291
ipv6 mld snooping source 292
ipv6 mld snooping mrouter 293
ipv6 mld snooping querier 294

第 5 編　IP インタフェース

19 IPv4・ARP・ICMP 295
arp 296
ip address 298
ip mtu 300
ip route 302

20 IPv6・NDP・ICMPv6 305
ipv6 address 306
ipv6 default-gateway 308
ipv6 enable 310
ipv6 nd accept-ra 311
ipv6 neighbor 312

21 DHCP サーバ機能 315
default-router 316
dns-server 317
hardware-address 318
host 319
ip dhcp excluded-address 321
ip dhcp pool 322
lease 323
max-lease 325
network 327
service dhcp 329

第 6 編　フィルタ・QoS

22 フロー検出モード 331
flow detection mode 332
flow detection out mode 335

23 アクセスリスト 337

指定できる名称 338
deny（ip access-list extended） 349
deny（ip access-list standard） 355
deny（ipv6 access-list） 357
deny（mac access-list extended） 363
ip access-group 366
ip access-list extended 368
ip access-list resequence 370
ip access-list standard 372
ipv6 access-list 374
ipv6 access-list resequence 376
ipv6 traffic-filter 377
mac access-group 379
mac access-list extended 381
mac access-list resequence 383
permit（ip access-list extended） 384
permit（ip access-list standard） 390
permit（ipv6 access-list） 392
permit（mac access-list extended） 398
remark 401

24 QoS 403

指定できる名称および値 404
ip qos-flow-group 414
ip qos-flow-list 416
ip qos-flow-list resequence 417
ipv6 qos-flow-group 418
ipv6 qos-flow-list 420
ipv6 qos-flow-list resequence 421
limit-queue-length 422
mac qos-flow-group 424
mac qos-flow-list 426
mac qos-flow-list resequence 427
qos（ip qos-flow-list） 428
qos（ipv6 qos-flow-list） 437
qos（mac qos-flow-list） 445
qos-queue-group 450
qos-queue-list 451
remark 454

traffic-shape rate 455
control-packet user-priority 457

第 7 編　レイヤ 2 認証

25 レイヤ 2 認証共通 459
authentication arp-relay 460
authentication auto-logout strayer 461
authentication force-authorized enable 462
authentication force-authorized vlan 464
authentication ip access-group 465
authentication logout linkdown 467
authentication max-user（global） 468
authentication max-user（interface） 470

26 IEEE802.1X 473
コンフィグレーションコマンドと認証モードの対応 474
aaa accounting dot1x 476
aaa authentication dot1x 478
dot1x authentication 480
dot1x auto-logout 481
dot1x force-authorized eapol 482
dot1x ignore-eapol-start 483
dot1x logging enable 484
dot1x max-req 485
dot1x multiple-authentication 486
dot1x port-control 488
dot1x radius-server dead-interval 490
dot1x radius-server host 492
dot1x reauthentication 495
dot1x supplicant-detection 496
dot1x system-auth-control 498
dot1x timeout keep-unauth 499
dot1x timeout quiet-period 500
dot1x timeout reauth-period 501
dot1x timeout server-timeout 503
dot1x timeout supp-timeout 504
dot1x timeout tx-period 505

27 Web 認証 507

コンフィグレーションコマンドと認証モードの対応 509
aaa accounting web-authentication 511
aaa authentication web-authentication 513
aaa authentication web-authentication end-by-reject 515
http-server initial-timeout 516
web-authentication authentication 518
web-authentication auto-logout 519
web-authentication html-fileset 520
web-authentication ip address 521
web-authentication jump-url 523
web-authentication logging enable 525
web-authentication logout ping tos-windows 526
web-authentication logout ping ttl 527
web-authentication logout polling count 528
web-authentication logout polling enable 530
web-authentication logout polling interval 532
web-authentication logout polling retry-interval 534
web-authentication max-timer 536
web-authentication port 538
web-authentication prefilter 539
web-authentication radius-server dead-interval 540
web-authentication radius-server host 542
web-authentication redirect-mode 545
web-authentication redirect enable 546
web-authentication redirect ignore-https 547
web-authentication redirect polling 548
web-authentication redirect queries 550
web-authentication redirect target 552
web-authentication roaming 554
web-authentication static-vlan roaming 556
web-authentication system-auth-control 558
web-authentication user-group 559
web-authentication user replacement 560
web-authentication web-port 561

28 MAC 認証 563

コンフィグレーションコマンドと認証モードの対応 564
aaa accounting mac-authentication 565
aaa authentication mac-authentication 567
aaa authentication mac-authentication end-by-reject 569

mac-authentication access-group 570
mac-authentication authentication 572
mac-authentication auto-logout 573
mac-authentication id-format 575
mac-authentication logging enable 577
mac-authentication max-timer 578
mac-authentication password 579
mac-authentication port 581
mac-authentication radius-server dead-interval 582
mac-authentication radius-server host 584
mac-authentication roaming 587
mac-authentication static-vlan roaming 589
mac-authentication system-auth-control 591
mac-authentication timeout quiet-period 592
mac-authentication timeout reauth-period 593
mac-authentication vlan-check 594

29 マルチステップ認証 597
authentication multi-step 598

第 8 編　セキュリティ

30 DHCP snooping 599
ip arp inspection limit rate 600
ip arp inspection trust 601
ip arp inspection validate 602
ip arp inspection vlan 604
ip dhcp snooping 606
ip dhcp snooping database url 607
ip dhcp snooping database write-delay 609
ip dhcp snooping information no-check 610
ip dhcp snooping information option allow-untrusted 611
ip dhcp snooping information option format remote-id 612
ip dhcp snooping information option-insert 613
ip dhcp snooping limit rate 614
ip dhcp snooping trust 615
ip dhcp snooping verify mac-address 616
ip dhcp snooping vlan 617
ip dhcp snooping vlan information option format-type circuit-id 618
ip source binding 620

ip verify source 622

31 ホワイトリスト機能【OP-WL】 625

white-list action discard【OP-WL】 626
white-list action log【OP-WL】 627
white-list action monitor【OP-WL】 628
white-list address permit【OP-WL】 629
white-list address trust【OP-WL】 630
white-list data【OP-WL】 631
white-list enable【OP-WL】 634
white-list learning【OP-WL】 635
white-list logging filter【OP-WL】 636
white-list logging format-add【OP-WL】 638
white-list monitor destination interface【OP-WL】 639
white-list packet mode【OP-WL】 640
white-list packet tcp【OP-WL】 641
white-list packet trust-mode【OP-WL】 643
white-list packet udp【OP-WL】 645
white-list trust【OP-WL】 647

32 特定端末への Web 通信不可表示機能 649

access-redirect http port 650
access-redirect http target 651
access-redirect timeout 652

第 9 編　冗長化構成による高信頼化機能

33 アップリンク・リダンダント 653

switchport backup interface 654
switchport backup flush-request transmit 656
switchport backup mac-address-table update exclude-vlan 657
switchport backup mac-address-table update retransmit 658
switchport backup mac-address-table update transmit 659
switchport-backup startup-active-port-selection 660

第 10 編　ネットワークの障害検出による高信頼化機能

34 IEEE 802.3ah/UDLD 661

efmoam active 662
efmoam disable 663
efmoam udld-detection-count 664

35 ストームコントロール 665

storm-control 666

36 L2 ループ検知 671

loop-detection 672
loop-detection auto-restore-time 674
loop-detection enable 675
loop-detection hold-time 676
loop-detection interval-time 677
loop-detection threshold 678

37 CFM 679

domain name 680
ethernet cfm cc alarm-priority 682
ethernet cfm cc alarm-reset-time 684
ethernet cfm cc alarm-start-time 686
ethernet cfm cc enable 688
ethernet cfm cc interval 690
ethernet cfm domain 692
ethernet cfm enable（global） 694
ethernet cfm enable（interface） 695
ethernet cfm mep 696
ethernet cfm mip 698
ma name 699
ma vlan-group 701

第 11 編　リモートネットワーク管理

38 SNMP 703

hostname 704

rmon alarm 705
rmon collection history 709
rmon event 711
snmp-server community 713
snmp-server contact 715
snmp-server engineID local 716
snmp-server group 718
snmp-server host 721
snmp-server location 726
snmp-server traps 727
snmp-server user 730
snmp-server view 732
snmp trap link-status 734

39 ログ出力機能 735

logging event-kind 736
logging facility 737
logging host 738
logging syslog-dump 740
logging tcp connect delay 741
logging tcp notify open 742
logging tcp notify resume 743
logging tcp reconnect delay 744
logging tcp trailer 745
logging trap 746

40 sFlow 統計 749

sflow destination 750
sflow extended-information-type 751
sflow forward egress 753
sflow forward ingress 754
sflow max-header-size 755
sflow max-packet-size 756
sflow packet-information-type 757
sflow polling-interval 758
sflow sample 759
sflow source 761
sflow url-port-add 762
sflow version 763

第 12 編　隣接装置の管理

41 LLDP 765

lldp enable 766
lldp hold-count 767
lldp interval-time 768
lldp management-address 769
lldp run 770
lldp version 771

第 13 編　ポートミラーリング

42 ポートミラーリング 773

ip icmp monitor destination interface 774
monitor session source 776
switchport monitor dot1q tag 779

43 ポリシーベースミラーリング 781

monitor session filter 782

第 14 編　コンフィグレーションエラーメッセージ

44 コンフィグレーション編集時のエラーメッセージ 785

44.1　コンフィグレーション編集時のエラーメッセージ 786
44.1.1　共通 786
44.1.2　スタック情報 789
44.1.3　ログインセキュリティと RADIUS 情報 790
44.1.4　時刻の設定と NTP 情報 790
44.1.5　装置の管理情報 791
44.1.6　省電力機能情報 791
44.1.7　イーサネット情報 791
44.1.8　リンクアグリゲーション情報 792
44.1.9　MAC アドレステーブル情報 793
44.1.10　VLAN 情報 793
44.1.11　スパニングツリー情報 797
44.1.12　Ring Protocol 情報 797

44.1.13 IGMP snooping 情報 799
44.1.14 MLD snooping 情報 800
44.1.15 IPv4・ARP・ICMP 情報 800
44.1.16 IPv6・NDP・ICMPv6 情報 801
44.1.17 DHCP サーバ機能情報 802
44.1.18 フロー検出モード情報 803
44.1.19 アクセスリスト情報 803
44.1.20 QoS 情報 805
44.1.21 レイヤ 2 認証共通情報 807
44.1.22 IEEE802.1X 情報 807
44.1.23 Web 認証情報 809
44.1.24 MAC 認証情報 810
44.1.25 マルチステップ認証情報 811
44.1.26 DHCP snooping 情報 811
44.1.27 ホワイトリスト情報 812
44.1.28 特定端末への Web 通信不可表示機能情報 813
44.1.29 アップリンク・リダンダント情報 813
44.1.30 ストームコントロール情報 814
44.1.31 L2 ループ検知情報 814
44.1.32 CFM 情報 814
44.1.33 SNMP 情報 815
44.1.34 ログ出力情報 816
44.1.35 sFlow 統計情報 816
44.1.36 ポートミラーリング情報 817
44.1.37 ポリシーベースミラーリング情報 818

索引 819

1 このマニュアルの読み方

コマンドの記述形式
コマンドモード一覧
パラメータに指定できる値
文字コード一覧

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)	リモートログインやコンソールの設定	(config)# line vty (config)# line console
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-ipv6-acl)	IPv6 フィルタの設定	(config)# ipv6 access-list
12	(config-ext-macl)	MAC フィルタの設定	(config)# mac access-list extended
13	(config-ip-qos)	IPv4 QoS の設定	(config)# ip qos-flow-list
14	(config-ipv6-qos)	IPv6 QoS の設定	(config)# ipv6 qos-flow-list
15	(config-mac-qos)	MAC QoS の設定	(config)# mac qos-flow-list
16	(dhcp-config)	DHCP サーバの設定	(config)# ip dhcp pool
17	(config-auto-cf)	AUTOCONF の設定	(config)# auto-config
18	(config-netconf)	NETCONF の設定	(config)# netconf
19	(config-ether-cfm)	ドメイン名称と MA の設定	(config)# ethernet cfm domain
20	(config-sw)	スタックを構成する装置ごとの設定	(config)# switch

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できません。	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	英数字とハイフン（-），ピリオド（.）が指定できます。 ただし，以下の指定はできません。 • 先頭 1 文字目がピリオド（.） • 連続ピリオド（.） • 数字とピリオド（.）だけ また，ピリオド（.）と次のピリオド（.）の間は最大 63 文字です。	ip host telnet-host 192.168.1.1
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

パラメータ種別	説明	入力例
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，gigabitethernet，vlan，port-channel です。インタフェースは混在することはできません。 入力形式は次のとおりです。 • gigabitethernet の場合 interface range gigabitethernet <interface id list> • vlan の場合 interface range vlan <VLAN ID list> • port-channel の場合 interface range port-channel <Channel group# list> また，上記入力形式をコンマ（,）で区切って最大 8 個指定できます。	interface range gigabitethernet 1/0/1-3（スタック動作時） interface range gigabitethernet 0/1-3（スタンドアロン動作時） interface range vlan 1-100
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 gigabitethernet 0/1-3 switchport isolation interface remove gigabitethernet 0/1-3

■ <switch no.> の設定値の範囲

<switch no.> の値の範囲を次の表に示します。

表 1-3　<switch no.> の値の範囲

項番	モデル	値の範囲
1	AX260A-08TF	1 ～ 2

■ <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 1-4　<IF#> の値の範囲

項番	モデル	イーサネット種別	値の範囲
1	AX260A-08TF AX260A-08T	gigabitethernet	0/1 ～ 0/10

■ <interface 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，<interface 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 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 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]
　スタック動作時　　：gigabitethernet 1/0/1-2, gigabitethernet 1/0/5
　スタンドアロン動作時：gigabitethernet 0/1-2, gigabitethernet 0/5

■ <VLAN ID> および <vlan id> の設定値の範囲

<VLAN ID> および <vlan id> の値の範囲を次の表に示します。

表 1-5　<VLAN ID> および <vlan id> の値の範囲

項番	値の範囲
1	1 ～ 4094

■ <VLAN ID list> および <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> および <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> および <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> および <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#> および <channel group> の設定値の範囲

<Channel group#> および <channel group> の値の範囲を次の表に示します。

表 1-6　<Channel group#> および <channel group> の値の範囲

項番	モデル	値の範囲
1	AX260A-08TF（スタック全体）	1 ～ 120
2	全モデル共通（スタンドアロン）	1 ～ 64

■ <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#> および <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#> および <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 1-7　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
line console
line vty
speed
transport input

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 アドレスまたは IPv6 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 アドレスまたは IPv6 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

ipv6 access-class

line console

本コマンドを入力すると，config-line モードに移行し，CONSOLE（RS232C）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
　line console 0

情報の削除
　no line console

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

CONSOLE（RS232C）ポートにコンソールを接続できます。

［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］

なし

［関連コマンド］

speed

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
   【スタック動作時】0 ～ 3（ログインできるユーザ数を 1 ～ 4 に設定できます。）
   【スタンドアロン動作時】0 ～ 15（ログインできるユーザ数を 1 ～ 16 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，「コンフィグレーションガイド Vol.1 10.1.7 リモート運用端末からのログインを許可する IP アドレスの設定」を参照し，ip access-group，ipv6 access-class や，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。
3. リモートログイン数は本コマンドで制限されますが，スタック動作時はマスタ以外のメンバスイッチの

コンソールログイン数も含めてスタック全体で最大 4 までとなります。

［関連コマンド］

transport input

ip access-group

ipv6 access-class

speed

CONSOLE（RS232C）の通信速度を設定するために使用します。

［入力形式］

情報の設定・変更
　speed <number>

情報の削除
　no speed

［入力モード］

(config-line)

［パラメータ］

<number>

CONSOLE（RS232C）の通信速度を bit/s 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
   1200，2400，4800，9600，19200

［コマンド省略時の動作］

CONSOLE（RS232C）の通信速度は 9600bit/s です。

［通信への影響］

なし

［設定値の反映契機］

CONSOLE（RS232C）からユーザがログインしている場合，設定値変更後，ユーザがログアウトした後，通信速度が変更されます。

［注意事項］

1. 設定変更時に CONSOLE（RS232C）からユーザがログインしている場合，ユーザがログアウトした後，通信速度が変更されます。CONSOLE（RS232C）からユーザがログイン認証中に，リモート運用端末で通信速度を変更した場合は，認証に失敗することがあります。

［関連コマンド］

line console

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

ipv6 access-class

3 コンフィグレーションの編集と操作

end
exit
save(write)
show
top

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。第ニ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。

［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と banner 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 スタック【OP-WLE】

switch【OP-WLE】

switch priority【OP-WLE】

switch provision【OP-WLE】

switchport stack cost【OP-WLE】

system mac-address【OP-WLE】

switch【OP-WLE】

スタックを構成する装置ごとの項目を設定します。本コマンドを入力すると，config-sw モードに移行します。

［入力形式］

情報の設定
　switch <switch no.>

情報の削除
　no switch <switch no.>

［入力モード］

(config)

［パラメータ］

<switch no.>

スイッチ番号を指定します。

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
   「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. switch provision コマンドが未設定のスイッチ番号は指定できません。
2. switch provision コマンドを削除した場合は，該当スイッチ番号の switch コマンドおよび switch コマンド配下の設定も削除されます。
3. 本コマンドは AX260A-08T では設定できません。

［関連コマンド］

switch provision

switch priority【OP-WLE】

スタックで動作時，メンバスイッチのマスタ選出優先度を設定します。

［入力形式］

情報の設定・変更
　switch <switch no.> priority <priority>

情報の削除
　no switch <switch no.> priority

［入力モード］

(config)

［パラメータ］

<switch no.>

スイッチ番号を指定します。

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
   「パラメータに指定できる値」を参照してください。

<priority>

メンバスイッチのマスタ選出優先度を指定します。
値が大きいほど優先度が高くなります。
一つの <switch no.> 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
   省略できません。
2. 値の設定範囲
   2 ～ 31（10 進数）を指定します。

［コマンド省略時の動作］

メンバスイッチのマスタ選出優先度は 15 で動作します。

［通信への影響］

詳しくは，「コンフィグレーションガイド Vol.1　7　スタックの解説【OP-WLE】」を参照してください。

［設定値の反映契機］

設定値変更後，次回のマスタの選出を契機に反映されます。

［注意事項］

本コマンドは AX260A-08T では設定できません。

［関連コマンド］

set stack

switch provision【OP-WLE】

装置のモデルを設定します。

本コマンドは，スタックで動作させる場合に自メンバスイッチ以外のメンバスイッチに対してモデルを設定します。自メンバスイッチの情報は自動で設定されます。自メンバスイッチの情報は設定および削除できません。

［入力形式］

情報の設定
　switch <switch no.> provision 260a-08tf

情報の削除
　no switch <switch no.> provision

［入力モード］

(config)

［パラメータ］

<switch no.>

スイッチ番号を指定します。

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
   「パラメータに指定できる値」を参照してください。

260a-08tf

AX260A-08TF のモデルを設定します。

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
   260a-08tf

［コマンド省略時の動作］

自動で設定された情報に従い，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. 接続されているメンバスイッチ（自メンバスイッチを含む）の情報を変更または削除することはできません。
2. 本コマンドで存在しないメンバスイッチを設定するとイーサネットインタフェース (interface gigabitethernet) が自動的に作成されます。また，あらかじめ設定したメンバスイッチを削除するとイーサネットインタフェースが自動的に削除されます。削除されたイーサネットインタフェース内の設定もすべて削除されます。

3. 自メンバスイッチ以外の情報を変更する場合は，いったん削除してから，再設定してください。
4. 事前に登録した情報と自動認識したメンバスイッチの情報が異なる場合は，自動認識した情報で上書きされます。スイッチ番号が異なる場合は別のメンバスイッチとして新規に自動生成されます。
5. no switch <switch no.> provision を実行すると，以下のコマンドに影響があります。
   - switch
     削除したメンバスイッチのスイッチ番号の switch コマンドおよび switch コマンド配下の設定は削除されます。
   - switchport isolation コマンド
     削除したメンバスイッチのポート番号が interface パラメータ指定に含まれていた場合，当該ポートは削除されます。
     interface パラメータ指定のポート番号がすべて削除対象となった場合は，当該 switchport isolation コマンドも削除します。
   - monitor session source コマンド
     削除したメンバスイッチのポート番号が source interface パラメータ，destination interface パラメータに含まれていた場合は，monitor session source コマンドを削除します。
   - mac-address-table static コマンド
     削除したメンバスイッチのポート番号が interface パラメータで指定されていた場合，当該 mac-address-table static コマンドを削除します。
6. 本コマンドは AX260A-08T では設定できません。

［関連コマンド］

interface gigabitethernet

set stack

switchport stack cost【OP-WLE】

スタック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
　switchport stack cost <cost>

情報の削除
　no switchport stack 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
   1 ～ 128

［コマンド省略時の動作］

パスコストは 32 で動作します。

［通信への影響］

設定値の変更によってトポロジ変更する場合は通信に影響します。

詳しくは，「コンフィグレーションガイド Vol.1　7　スタックの解説【OP-WLE】」を参照してください。

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

本コマンドは AX260A-08T では設定できません。

［関連コマンド］

set stack

system mac-address【OP-WLE】

スタックの装置 MAC アドレスを設定します。

［入力形式］

情報の設定・変更
　system mac-address <mac>

情報の削除
　no system mac-address

［入力モード］

(config)

［パラメータ］

<mac>

装置 MAC アドレス（キャノニカル・フォーマット）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
   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。
   他の装置と重複しないようローカル MAC アドレス（2 桁目が 2，6，A，E）の使用を推奨します。

［コマンド省略時の動作］

最初のマスタスイッチの装置 MAC アドレスを使用します。

［通信への影響］

設定値の変更によって，自発パケットの送信元 MAC アドレスが変更されます。

詳しくは，「コンフィグレーションガイド Vol.1　7　スタックの解説【OP-WLE】」を参照してください。

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

本コマンドは AX260A-08T では設定できません。

［関連コマンド］

set stack

5 ログインセキュリティと RADIUS

aaa authentication enable

aaa authentication enable end-by-reject

aaa authentication login

aaa authentication login console

aaa authentication login end-by-reject

aaa group server radius

banner

ip access-group

ipv6 access-class

radius-server attribute station-id capitalize

radius-server dead-interval

radius-server host

radius-server key

radius-server retransmit

radius-server timeout

server

aaa authentication enable

装置管理者モードへの変更（enable コマンド）時の認証で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 enable 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 enable default <method> [<method>]

情報の削除

no aaa authentication enable

［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。

enable

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。

- グループ名に "radius" を指定した場合は，"group radius" として動作します。
- グループ名に "tacacs+"，または "tacacs+" の短縮入力と一致する文字列（"taca" 等）は設定できません。

［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したとき，装置管理者モードへ変更できなくなります。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］

aaa authentication enable end-by-reject

aaa group server radius

radius-server

aaa authentication enable end-by-reject

装置管理者モードへの変更（enable コマンド）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 enable 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 enable end-by-reject

情報の削除
　no aaa authentication enable 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 enable 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 enable 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 enable

aaa authentication login

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。

- グループ名に "radius" を指定した場合は，"group radius" として動作します。
- グループ名に "tacacs+"，または "tacacs+" の短縮入力と一致する文字列（"taca" 等）は設定できません。

［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したとき，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 console

コンソール（RS-232C）からのログイン時に aaa authentication login コマンドで指定した認証方式を使用します。

［入力形式］

情報の設定
　aaa authentication login console

情報の削除
　no aaa authentication login 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）からのログイン時は，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. RADIUS 認証を行うためには，aaa authentication login コマンドも設定してください。
2. aaa authentication login コマンドで認証方式に local パラメータを指定していない場合，本設定を行うと，RADIUS サーバと通信不可または RADIUS サーバでの認証に失敗したとき，コンソール（RS-232C）からログインできなくなります。

［関連コマンド］

aaa authentication login

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

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

banner

各接続（telnet ／ console ／ ftp）のログイン前に表示するメッセージを設定します。

［入力形式］

情報の設定・変更

banner login { encode "<encoded message>" | plain-text "<text message>" }

情報の削除

no banner login

［入力モード］

(config)

［パラメータ］

login

各接続（telnet ／ console ／ ftp）のログイン前に表示するメッセージを設定します。

plain-text "<text message>"

ログインメッセージをテキスト形式の文字列として入力します。複数行の場合は改行を入れます。改行は「¥n」と入力します。「¥」は「¥¥」と入力します。

入力内容は，自動的に encode パラメータのコンフィグレーションとして設定されます。また，以前設定されていたものは削除されます。なお，入力後，テキスト形式でのスクリーンイメージを確認したい場合は，show banner login plain-text を使用してください。

1. 本パラメータ省略時の初期値
   ログインメッセージを表示しない
2. 値の設定範囲
   任意の文字列を " " で囲んで入力する（720 文字以内）

表 5-1　エスケープシーケンス入力範囲

書式	ASCII コード	意味	備考
¥a	0x07	警報音	
¥b	0x08	バックスペース	
¥t	0x09	水平タブ	
¥n	0x0a	復帰 / 改行	
¥v	0x0b	垂直タブ	
¥f	0x0c	改ページ	
¥r	0x0d	復帰	
¥¥	0x5c	¥	
¥?	0x3f	?	「?」は「¥?」も「?」も入力可
¥'	0x27	'	「'」は「¥'」も「'」も入力可
¥ooo		ASCII コードの 8 進数表記 (3 桁)	ooo：000 ～ 377（3 桁以外はエラー）
¥xhh		ASCII コードの 16 進数表記 (2 桁)	hh：00 ～ ff　(2 桁以外はエラー)

encode "<encoded message>"

ログインメッセージとして BASE64 エンコードをした文字列を入力します。

また，以前設定されていたものは削除されます。テキスト形式でのスクリーンイメージを確認したい場合は，show banner login plain-text を使用してください。

1. 本パラメータ省略時の初期値
   ログインメッセージを表示しない
2. 値の設定範囲
   BASE64 エンコードした文字列を " " で囲んで入力する（960 文字以内）

［コマンド省略時の動作］

ログインメッセージを表示しません。

［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. ログインメッセージの設定時に，クライアントへの問い合わせプロンプトが不要なログインをした場合（クライアント側が自動的にユーザ名を渡す場合でパスワードが不要なときなど）には，ログインメッセージと認証後の画面が続けて表示されます。
2. ログインメッセージを入力するときには，クライアントの画面設定を確認して，表示できない文字を入力しないでください。show banner login plain-text の実行時や，クライアント接続時に画面やプロンプトの表示が崩れて操作できなくなるおそれがあります。

［関連コマンド］

なし

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。

ip access-group，ipv6 access-class で指定されているアクセスリストを合わせて，128 リスト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 <access list name> in

情報の削除
　no ip access-group <access list name>

［入力モード］

(config-line)

［パラメータ］

<access list name>

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
   4 ～ 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 IPv4 アドレスを使用した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 IPv4 アドレスを使用した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

ipv6 access-class

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 IPv6 アドレスを指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。

ip access-group，ipv6 access-class で指定されているアクセスリストを合わせて，128 リストになるまで複数行設定できます。

［入力形式］

情報の設定
　ipv6 access-class <access list name> in

情報の削除
　no ipv6 access-class <access list name>

［入力モード］

(config-line)

［パラメータ］

<access list name>

IPv6 フィルタの識別子（ipv6 access-list 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
   4 ～ 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 IPv6 アドレスを使用した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. ipv6 access-class 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 IPv6 アドレスを使用した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］

line vty

ftp-server

transport input

ipv6 access-list

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，監視タイマ 10 分（デフォルトコンフィグレーション）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 {<ipv4 address> | <ipv6 address>} [auth-port <port>] [acct-port <port>] [timeout <seconds>] [retransmit <retries>] [key <string>]

情報の削除

no radius-server host {<ipv4 address> | <ipv6 address>}

［入力モード］

(config)

［パラメータ］

{<ipv4 address> | <ipv6 address>}

<ipv4 address>

RADIUS サーバの IPv4 アドレスをドット記法で指定します。

<ipv6 address>

RADIUS サーバの IPv6 アドレスをコロン記法で指定します。

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
   <ipv4 address> : IPv4 ユニキャストアドレス
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   <ipv6 address> : IPv6 グローバルユニキャストアドレス
   ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff，fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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 {<ipv4 address> | <ipv6 address>} [auth-port <port>] [acct-port <port>]

情報の削除

no server {<ipv4 address> | <ipv6 address>}

［入力モード］

(config-group)

［パラメータ］

{<ipv4 address> | <ipv6 address>}

<ipv4 address>

RADIUS サーバの IPv4 アドレスをドット記法で指定します。

<ipv6 address>

RADIUS サーバの IPv6 アドレスをコロン記法で指定します。

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
   <ipv4 address> : IPv4 ユニキャストアドレス
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   <ipv6 address> : IPv6 グローバルユニキャストアドレス
   ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff，fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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

6 時刻の設定と NTP

コンフィグレーションコマンドと動作モードの対応
clock timezone
ntp authenticate
ntp authentication-key
ntp broadcast
ntp broadcast client（global）
ntp broadcast client（interface）
ntp broadcastdelay
ntp interval
ntp master
ntp peer
ntp server
ntp trusted-key
sntp client

コンフィグレーションコマンドと動作モードの対応

時刻設定および NTP に関するコンフィグレーションコマンドと動作モードの対応を次の表に示します。
SNTP 動作モードと NTP 動作モードの切り替えは，sntp client コマンドで設定します。

表 6-1　コンフィグレーションコマンドと動作モードの対応

コマンド名	SNTP 動作モード	NTP 動作モード
clock timezone	○	○
ntp authenticate	×	○
ntp authentication-key	×	○
ntp broadcast	×	○
ntp broadcast client (global)	○	○
ntp broadcast client (interface)	×	○
ntp broadcastdelay	×	○
ntp interval	○	×
ntp master	×	○
ntp peer	×	○
ntp server	○	○
ntp trusted-key	×	○
sntp client	○	○

（凡例）　○：使用可能　×：使用不可

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］

1. 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。
2. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

set clock

ntp authenticate

NTP 認証機能を有効にします。

［入力形式］

情報の設定
　ntp authenticate

情報の削除
　no ntp authenticate

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

NTP 認証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］

1. NTP 認証機能を有効にした場合，ntp authentication-key コマンドおよび ntp trusted-key コマンドが設定されていなければ，NTP メッセージの送受信が不可能になります。
2. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp authentication-key

ntp trusted-key

ntp authentication-key

認証鍵を設定します。本コマンドでは，認証鍵を最大 10 エントリまで設定できます。

［入力形式］

情報の設定・変更

ntp authentication-key <key id> md5 <value>

情報の削除

no ntp authentication-key <key id>

［入力モード］

(config)

［パラメータ］

<key id>

鍵の番号（10 進数）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 ～ 65535

md5 <value>

認証鍵に割り当てる値を指定します。

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
   30 文字以内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］

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. 認証鍵は，ntp authenticate コマンドおよび ntp trusted-key コマンドが設定されるまで有効になりません。
2. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp authenticate

ntp broadcast client

ntp master

ntp peer

ntp server

ntp trusted-key

ntp broadcast

ブロードキャストで NTP メッセージを送信し，ほかの装置が本装置に同期するように設定します。

本コマンドは，最大 10 エントリまで設定できます。

［入力形式］

情報の設定・変更

ntp broadcast [version <number>] [key <key id>]

情報の削除

no ntp broadcast

［入力モード］

(config-if)

［パラメータ］

version <number>

本装置が送信する NTP メッセージのバージョン番号を指定します。

1. 本パラメータ省略時の初期値
   バージョン 4 が指定されます。
2. 値の設定範囲
   1 ～ 4

key <key id>

アクセスするための認証鍵を指定します。この認証鍵は ntp authentication-key コマンドで設定した番号（10 進数）を指定します。

1. 本パラメータ省略時の初期値
   認証鍵の指定はなし
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］

1. 当該インタフェースに IPv4 アドレスが設定されていない場合は，本コマンドは無効です。
2. ntp authenticate コマンド未設定のときに本コマンドの key パラメータを指定すると，NTP メッセージが送信不能になります。また，key パラメータで指定された認証鍵が ntp trusted-key コマンドで有効になっていない場合も NTP メッセージが送信不能になります。
3. version パラメータに 1 を指定してもメッセージ形式は version2 以降と同じになります。（3 ビットのバージョン番号だけが 1 になります。）

4. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp authentication-key

ntp broadcast client

ntp broadcast client（global）

NTP ブロードキャストメッセージを受け付ける設定を行います。これによって，ほかの装置からの NTP ブロードキャストを受信して，本装置の時刻をほかの装置に同期させることができます。

［入力形式］

情報の設定
　ntp broadcast client

情報の削除
　no ntp broadcast client

［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。**【SNTP 動作モード時】**

ntp broadcast client(interface) コマンド設定に従います。**【NTP 動作モード時】**

［通信への影響］

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. 本コマンドと ntp server コマンドを同時に設定した場合，ntp server コマンドの設定が有効となります。**【SNTP 動作モード時】**
2. 本装置の NTP は IPv6 をサポートしていません。本コマンドは IPv4 専用です。
3. IP アドレスを持たない VLAN インタフェースにおいては，NTP ブロードキャストメッセージを受信しません。
4. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp server

ntp broadcast

ntp broadcast client（interface）

ntp broadcast client（interface）

本コマンドを設定したVLANインタフェースにおいて，NTPブロードキャストメッセージを受け付ける設定を行います。これによって，ほかの装置からのNTPブロードキャストを受信して，本装置の時刻をほかの装置に同期させることができます。本装置に最大10個まで設定できます。

［入力形式］

情報の設定
　ntp broadcast client

情報の削除
　no ntp broadcast client

［入力モード］

(config-if)

［パラメータ］

なし

［コマンド省略時の動作］

ntp broadcast client （global）コマンド設定に従います。

［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］

1. 本装置のNTPはIPv6をサポートしていません。本コマンドはIPv4専用です。
2. IPアドレスを持たないVLANインタフェースにおいては，NTPブロードキャストメッセージを受信しません。
3. 本コマンドが設定可能な動作モードは，「表6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp broadcast

ntp broadcastdelay

NTP ブロードキャストサーバと本装置間で予測される遅延時間を指定します。

［入力形式］

情報の設定・変更
　ntp broadcastdelay <micro seconds>

情報の削除
　no ntp broadcastdelay

［入力モード］

(config)

［パラメータ］

<micro seconds>

予測される片道遅延時間の倍の値をマイクロ秒単位で指定してください。

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 ～ 999999

［コマンド省略時の動作］

NTP ブロードキャストサーバの遅延時間は 4000 マイクロ秒になります。

［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. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp broadcast client

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 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］

1. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp server

ntp master

上位 NTP サーバが存在しない場合に，本装置がローカルタイムサーバとして機能し，本装置の時刻を NTP クライアントに提供します。

［入力形式］

情報の設定・変更
　ntp master [<stratum>]

情報の削除
　no ntp master

［入力モード］

(config)

［パラメータ］

<stratum>
　ストラタム値（10 進数）を指定します。本装置が NTP クライアントに送信するメッセージのストラタム値は本パラメータの値に 1 を加えたものになります。
1. 本パラメータ省略時の初期値
   8
2. 値の設定範囲
   1 ～ 15

［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. 上位 NTP サーバが存在しない間に本装置が NTP クライアントに提供する時刻は，一般に NTP プロトコルで要求される精度を満たしません。
2. システム内に複数のローカルタイムサーバが存在する場合の運用については，「コンフィグレーションガイド Vol.1　11　時刻の設定と NTP」を参照してください。
3. <stratum> パラメータの値を 15 にした場合，本装置がクライアントに送信するメッセージは，ストラタム値が 16 になり，一般の NTP クライアントによって無効と判断されます。
4. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp peer

ntp server

ntp peer

シンメトリック NTP サーバのアドレスを指定します。本装置は NTP シンメトリック・アクティブモードで動作します。

本コマンドは，ntp server コマンドと合わせて，最大 10 エントリまで設定できます。

［入力形式］

情報の設定・変更

ntp peer <ip address> [version <number>] [key <key id>] [prefer]

情報の削除

no ntp peer <ip address>

［入力モード］

(config)

［パラメータ］

<ip address>

シンメトリック NTP 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
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255

version <number>

本装置が送信する NTP メッセージのバージョン番号を指定します。

1. 本パラメータ省略時の初期値
   バージョン 4 が指定されます。
2. 値の設定範囲
   1 ～ 4

key <key id>

アクセスするための認証鍵を指定します。この認証鍵は ntp authentication-key コマンドで設定した番号（10 進数）を指定します。

1. 本パラメータ省略時の初期値
   認証鍵の指定はなし
2. 値の設定範囲
   1 ～ 65535

prefer

複数の装置を指定した場合は，prefer 指定をした装置を優先します。

1. 本パラメータ省略時の初期値
   優先指定はなし
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. ntp server コマンドと ntp peer コマンドで同じアドレスを指定することはできません。
2. <ip address> パラメータにはユニキャストアドレスを指定してください。本装置の VLAN インタフェースのプライマリ IP アドレスのブロードキャストアドレスが指定された場合は，本コマンドが無効になります。
3. prefer パラメータを指定した場合，同期先を選択する基準は RFC 非準拠になります。prefer パラメータが指定された NTP サーバは，インターセクションアルゴリズムによって棄却されません。
4. ntp authenticate コマンド未設定のときに本コマンドの key パラメータを指定すると NTP メッセージが送信不能になります。また，key パラメータで指定された鍵が ntp trusted-key コマンドで有効になっていない場合も NTP メッセージが送信不能になります。
5. version パラメータに 1 を指定してもメッセージ形式は version2 以降と同じになります。（3 ビットのバージョン番号だけが 1 になります。）
6. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp server

ntp authentication-key

ntp server

NTP サーバのアドレスを指定します。本装置は NTP クライアントとして動作します。

SNTP 動作モード時は，最大 2 エントリまで設定できます。

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。

NTP 動作モード時は，ntp peer コマンドと合わせて，最大 10 エントリまで設定できます。

［入力形式］

情報の設定・変更

ntp server <ip address>【SNTP 動作モード時】

ntp server <ip address> [version <number>] [key <key id>] [prefer]【NTP 動作モード時】

情報の削除

no ntp server <ip address>

［入力モード］

(config)

［パラメータ］

<ip address>

時刻情報を取得する NTP サーバの 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

version <number>

本装置が送信する NTP メッセージのバージョン番号を指定します。

1. 本パラメータ省略時の初期値
   バージョン 4 が指定されます。
2. 値の設定範囲
   1 ～ 4

key <key id>

アクセスするための認証鍵を指定します。この認証鍵は ntp authentication-key コマンドで設定した番号（10 進数）を指定します。

1. 本パラメータ省略時の初期値
   認証鍵の指定はなし
2. 値の設定範囲
   1 ～ 65535

prefer

複数の装置を指定した場合は，prefer を指定した装置を優先します。

1. 本パラメータ省略時の初期値
   優先指定はなし

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. SNTP 動作モード時は，ntp broadcast client コマンドを同時に設定した場合，本コマンドの設定が有効となります。
2. IPv4 アドレスとして 127.*.*.* を設定できません。
3. NTP 動作モード時は，ntp server コマンドと ntp peer コマンドで同じアドレスを指定することはできません。
4. <ip address> パラメータにはユニキャストアドレスを指定してください。本装置の VLAN インタフェースのプライマリ IP アドレスのブロードキャストアドレスが指定された場合は，本コマンドが無効になります。
5. prefer パラメータを指定した場合，同期先を選択する基準は RFC 非準拠になります。prefer パラメータが指定された NTP サーバは，インターセクションアルゴリズムによって棄却されません。
6. ntp authenticate コマンド未設定のときに本コマンドの key パラメータを指定すると，NTP メッセージが送信不能になります。また，key パラメータで指定された認証鍵が ntp trusted-key コマンドで有効になっていない場合も NTP メッセージが送信不能になります。
7. version パラメータに 1 を指定してもメッセージ形式は version2 以降と同じになります。（3 ビットのバージョン番号だけが 1 になります。）
8. sntp client コマンドで NTP 動作モードを SNTP 動作モードに変更したときは，　変更後 3 秒以上経過してから本コマンドを設定してください。動作モード変更後すぐに本コマンドを設定すると，NTP サーバに対する最初の時刻取得を失敗する場合があります。なお，SNTP 動作モードを NTP 動作モードに変更する場合は問題ありません。
9. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

[関連コマンド]

ntp authentication-key

ntp broadcast client

ntp interval

ntp peer

ntp trusted-key

ほかの装置と同期する場合に，セキュリティ目的の認証を行うように鍵番号を設定します。デフォルトコンフィグレーションでは，認証に使用される鍵は設定されていません。本コマンドでは，鍵番号を最大 10 エントリまで設定できます。

［入力形式］

情報の設定

ntp trusted-key <key id>

情報の削除

no ntp trusted-key <key id>

［入力モード］

(config)

［パラメータ］

<key id>

認証に使用する鍵番号を指定します。この認証鍵は ntp authentication-key コマンドで設定した番号（10 進数）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 ～ 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］

1. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp authenticate

ntp authentication-key

sntp client

no sntp client コマンドを設定すると，SNTP クライアントを停止し，標準 NTP のコンフィグレーションを可能にします。デフォルトコンフィグレーションでは，SNTP クライアントで動作します。本コマンドを設定すると標準 NTP で動作します。

［入力形式］

情報の設定
　no sntp client

情報の削除
　sntp client

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

コンフィグレーションに従い，SNTP クライアントが動作します。

［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］

1. 本コマンドを設定または削除する場合は，下記のコンフィグレーションをすべて削除したあとに切り替えてください。

   ＜ no sntp client 設定時＞
   - ntp interval
   - ntp broadcast client(global)
   - ntp server

   ＜ sntp client で削除時＞
   - ntp authenticate
   - ntp authentication-key
   - ntp broadcast
   - ntp broadcast client(global)
   - ntp broadcast client(interface)
   - ntp broadcastdelay
   - ntp master
   - ntp peer
   - ntp server
   - ntp trusted-key

2. 本コマンドが設定可能な動作モードは，「表 6-1　コンフィグレーションコマンドと動作モードの対応」を参照してください。

［関連コマンド］

ntp authenticate

ntp authentication-key

ntp broadcast

ntp broadcast client(global)

ntp broadcast client(interface)

ntp broadcastdelay

ntp interval

ntp master

ntp peer

ntp server

ntp trusted-key

7 ホスト名と DNS

ip domain lookup

ip domain name

ip domain reverse-lookup

ip host

ip name-server

ipv6 host

ip domain lookup

no ip domain lookup コマンドを設定すると，DNS リゾルバ機能が無効になります。

［入力形式］

情報の設定
　no ip domain lookup

情報の削除
　ip domain lookup

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

DNS リゾルバ機能が有効になります。

［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。ただし，実行中のコマンド（運用コマンド traceroute など）の動作には反映されない場合があります。

［注意事項］

なし

［関連コマンド］

ip name-server

ip domain name

DNS リゾルバで使用するドメイン名を設定します。

［入力形式］

情報の設定・変更
　ip domain name <domain name>

情報の削除
　no ip domain name

［入力モード］

(config)

［パラメータ］

<domain name>

本装置のドメイン名を指定します。

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
   1 ～ 255 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「ホスト名」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。ただし，実行中のコマンドの動作には反映されない場合があります。

［注意事項］

なし

［関連コマンド］

ip name-server

ip domain lookup

ip domain reverse-lookup

no ip domain reverse-lookup コマンドを設定すると，DNS リゾルバ機能の逆引き機能（IP アドレスからホスト名を検索する機能）が無効になります。

［入力形式］

情報の設定
　no ip domain reverse-lookup

情報の削除
　ip domain reverse-lookup

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

DNS リゾルバ機能が有効の場合は，逆引き機能は有効化されています。

［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。ただし，実行中のコマンド（運用コマンド traceroute など）の動作には反映されない場合があります。

［注意事項］

1. DNS リゾルバ機能が無効の場合は，本設定にかかわらず DNS リゾルバ機能は動作しません。

［関連コマンド］

ip domain lookup

ip name-server

ip host

IPv4 アドレスに付与するホスト名情報を設定します。本コマンドでは最大 20 エントリを設定できます。

［入力形式］

情報の設定・変更
　ip host <name> <ip address>

情報の削除
　no ip host <name>

［入力モード］

(config)

［パラメータ］

<name>

IPv4 アドレスに付与するホ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
   1 ～ 63 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。

<ip address>

ホスト名を設定する装置の IPv4 アドレスをドット記法で指定します。

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
   IPv4 ユニキャストアドレスを指定します。

［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. ホスト名として localhost を設定できません。
2. ホスト名は大文字と小文字を区別しません。
3. ip host コマンドと ipv6 host コマンドで同一のホスト名を設定している場合，明示的に IPv6 が選択（運用コマンド ping ipv6 など）されない限り ip host コマンドが優先されます。

［関連コマンド］

なし

ip name-server

DNS リゾルバが参照するネームサーバを設定します。ネームサーバは，3 台まで指定できます。複数のネームサーバを指定した場合は，設定した順番にネームサーバへの問い合わせが行われます。DNS リゾルバ機能は，デフォルトコンフィグレーションで有効化されているので，ネームサーバが設定された時点から機能します。

［入力形式］

情報の設定

ip name-server <ip address>

情報の削除

no ip name-server <ip address>

［入力モード］

(config)

［パラメータ］

<ip address>

ネームサーバの IPv4 アドレスをドット記法で指定します。

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
   IPv4 ユニキャストアドレスを指定します。

［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。ただし，実行中のコマンド（運用コマンド traceroute など）の動作には反映されない場合があります。

［注意事項］

1. DNS サーバの IP アドレス（ip name-server）を正しく設定してください。DNS サーバの IP アドレスが正しく設定されていない場合，ホスト名の参照時に DNS サーバとの通信不可を検知するまでに時間がかかり，運用に支障をきたすことがあります（例：traceroute の結果表示に時間がかかります）。
2. IPv6 を使用して AAAA クエリ情報を参照できません。IPv4 で AAAA クエリ情報を参照します。

［関連コマンド］

ip domain lookup

ipv6 host

IPv6 アドレスに付与するホスト名情報を設定します。本コマンドでは最大 20 エントリを設定できます。

［入力形式］

情報の設定・変更

ipv6 host <name> <ipv6 address>

情報の削除

no ipv6 host <name>

［入力モード］

(config)

［パラメータ］

<name>

IPv6 アドレスに付与するホ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
   1 ～ 63 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。

<ipv6 address>

ホスト名を設定する装置の IPv6 アドレスをコロン記法で指定します。

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
   IPv6 グローバルユニキャストアドレスを指定します。

［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. ホスト名として localhost を設定できません。
2. ホスト名は大文字と小文字を区別しません。
3. ipv6 host コマンドと ip host コマンドで同一のホスト名を設定している場合，明示的に IPv6 が選択（運用コマンド ping ipv6 など）されない限り ip host コマンドが優先されます。

［関連コマンド］

なし

8 装置の管理

system l2-table mode

system logging format-add

system memory-soft-error

system receive alarm logging

system receive alarm parameters

system receive control

system receive rate-limit

system recovery

system temperature-warning-level

system temperature-warning-level average

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。

[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。

[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 logging format-add

ログ出力する追加情報を指定します。

対象機能については，「コンフィグレーションガイド Vol.1　13　装置の管理」を参照してください。

［入力形式］

情報の設定
　system logging format-add year

情報の削除
　no system logging format-add year

［入力モード］

(config)

［パラメータ］

year

　ログ出力時に西暦（年号）情報を追加します。

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
   year

［コマンド省略時の動作］

ログ出力する情報に追加情報は表示しません。

［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

system memory-soft-error

Switch processor 内または FPGA 内メモリのソフトエラー発生時にログメッセージの出力を設定します。（FPGA は【08TF】のみです。）

［入力形式］

情報の設定
　system memory-soft-error log

情報の削除
　no system memory-soft-error log

［入力モード］

(config)

［パラメータ］

log

Switch processor 内または FPGA 内メモリのソフトエラー発生時にログメッセージを出力します。

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

［コマンド省略時の動作］

Switch processor 内および FPGA 内メモリのソフトエラー発生時にログ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］

なし

［関連コマンド］

なし

system receive alarm logging

no system receive alarm logging 設定時，本装置の CPU が大量のパケットを受信したと判断したときに出力する運用ログを抑止します。次の運用ログが対象です。

- E3 KERNEL 01f10001 Receiving many packets for CPU.
  （CPU 宛に大量のパケットを受信しています。）
- E3 KERNEL 01f10002 No longer receiving many packets for CPU.
  （CPU 宛に大量のパケットを受信しなくなりました。）

［入力形式］

情報の設定
　no system receive alarm logging

情報の削除
　system receive alarm logging

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

本装置の CPU が大量のパケットを受信したと判断したときに出力する運用ログを抑止しません。

［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］

なし

system receive alarm parameters

本装置の CPU が大量のパケットを受信したと見なす基準となる閾値を指定します。

［入力形式］

情報の設定・変更

system receive alarm parameters <upper limit> <lower limit> <upper period> <lower period>

情報の削除

no system receive alarm parameters

［入力モード］

(config)

［パラメータ］

<upper limit>

大量と見なす閾値を [パケット / 秒] 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 ～ 600（パケット / 秒）

<lower limit>

大量ではなくなったと見なす閾値を [パケット / 秒] 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 ～ <upper limit>（パケット / 秒）

<upper period>

大量と見なすまでの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 ～ 10（秒）

<lower period>

大量ではなくなったと見なすまでの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 ～ 10（秒）

［コマンド省略時の動作］

以下で動作します。

- 大量と見なす閾値：540 パケット / 秒
- 大量ではなくなったと見なす閾値：360 パケット / 秒
- 大量と見なすまでの時間：5 秒

- 大量ではなくなったと見なすまでの時間：5 秒

［通信への影響］

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，最大 10 秒程度の遅延を生じる場合があります。

［注意事項］

なし

［関連コマンド］

なし

system receive control

装置のパケット受信モードを切り替えます。

［入力形式］

情報の設定・変更

system receive control {coarse | fine}

情報の削除

no system receive control

［入力モード］

(config)

［パラメータ］

{coarse | fine}

coarse

収容条件重視モードで動作します。

fine

受信条件重視モードで動作します。

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
   coarse，fine

［コマンド省略時の動作］

収容条件重視モードで動作します。

［通信への影響］

運用中に変更した場合，全ポートが一時的に通信断となります。

［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

system receive rate-limit

no system receive rate-limit 設定時，装置全体の受信レート制限を解除します。

［入力形式］

情報の設定
　no system receive rate-limit

情報の削除
　system receive rate-limit

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

装置全体の受信レートが制限されています。

［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. VLAN 内に流入するブロードキャストトラフィックが多い環境の場合，装置の受信負荷に伴い CPU 使用率が高騰する要因となるため，本コマンドを設定しないでください。

［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　13　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）は自動復旧は停止状態となり，致命的障害（E9 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　13　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
   【08T】: 25 ～ 45（℃）
   上記以外 : 25 ～ 50（℃）

［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
   38（℃）
2. 値の設定範囲
   【08T】：25 ～ 45（℃）
   上記以外：25 ～ 50（℃）

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

9 ゼロタッチプロビジョンニング機能

system zero-touch-provisioning

system zero-touch-provisioning vlan

system zero-touch-provisioning

ゼロタッチプロビジョニング機能を有効にします。

［入力形式］

情報の設定
　system zero-touch-provisioning

情報の削除
　no system zero-touch-provisioning

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

ゼロタッチプロビジョニング機能は有効です。

本機能サポート前のソフトウェアからアップデートする場合の動作は，「コンフィグレーションガイド Vol.1　15.1.1　概要　表 15-1　本機能サポート前の装置を有効にする操作」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，コンフィグレーションを保存してください。次回の装置起動時に適用されます。

［注意事項］

本機能を使用しない場合は，"no system zero-touch-provisioning" で削除してください。

［関連コマンド］

system zero-touch-provisioning vlan

system zero-touch-provisioning vlan

ゼロタッチプロビジョニング機能で使用する VLAN インタフェースを設定します。

装置で，1 つの VLAN インタフェースだけに設定可能です。

［入力形式］

情報の設定・変更

system zero-touch-provisioning vlan <vlan id>

情報の削除

no system zero-touch-provisioning vlan

［入力モード］

(config)

［パラメータ］

vlan <vlan id>

ゼロタッチプロビジョニング機能で使用する VLAN 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
   「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］

VLAN インタフェース 1 が有効です。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，コンフィグレーションを保存してください。次回の装置起動時に適用されます。

［注意事項］

なし

［関連コマンド］

system zero-touch-provisioning

10 省電力機能

power-control port cool-standby

schedule-power-control port cool-standby

schedule-power-control port-led

schedule-power-control shutdown

schedule-power-control system-sleep

schedule-power-control time-range

system port-led

system port-led trigger console

system port-led trigger interface

system port-led trigger mc

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]

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. SFP ポートは，リンクダウンポートの省電力機能未サポートのため，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］

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. SFP ポートは，リンクダウンポートの省電力機能未サポートのため，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 | economy | disable }

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。

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

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，economy，disable

[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，ST2，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

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 <interface id list>

情報の変更

schedule-power-control shutdown interface {<interface id list> | add <interface id list> | remove <interface id list> }

情報の削除

no schedule-power-control shutdown interface

［入力モード］

(config)

［パラメータ］

interface <interface id 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
   <interface id 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 <interface id 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
   <interface id 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 <interface id 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
   <interface id 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

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（日付指定，曜日指定，毎日指定）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。
   - 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：60 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 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 | economy | disable }

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。

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

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，economy，disable

[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，ST2，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 <interface id list>

情報の削除

no system port-led trigger interface

［入力モード］

(config)

［パラメータ］

<interface id 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

11 イーサネット

bandwidth

description

duplex

flowcontrol

interface gigabitethernet

link debounce

link up-debounce

link-relay source

mdix auto

mtu

shutdown

speed

system mtu

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 ～ 10000000（kbit/s）
   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

回線速度が最大 1000Mbit/s のイーサネットインタフェースでポートの 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。
ポート，回線種別で設定可能なパラメータが異なります。設定可能なパラメータの組み合わせを「表 11-1　設定可能なパラメータ（ポート別）」「表 11-2　設定可能なパラメータ（回線種別）」に示します。

表 11-1　設定可能なパラメータ（ポート別）

モデル名	ポート	設定可能なパラメータ
AX260A-08TF	0/1 ～ 0/10	full，auto
AX260A-08T	0/1 ～ 0/8	half，full，auto
	0/9 ～ 0/10	full，auto

表 11-2　設定可能なパラメータ（回線種別）

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

注 ※　half を指定できません。【08TF】

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 11-1　設定可能なパラメータ（ポート別）」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。

また，回線テストを実行している場合，回線テストを中断します。

［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. UTP ポートを固定設定で使用する場合には MDI-X となります。
4. 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。【08T】
5. half パラメータは指定できません。【08TF】

［関連コマンド］

speed

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］

受信動作は off，送信動作は desired 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。

また，回線テストを実行している場合，回線テストを中断します。

［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. 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。

［関連コマンド］

なし

interface gigabitethernet

回線速度が最大 1000Mbit/s のイーサネット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，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 <switch no.>/<IF#>**【スタック動作時】**

interface gigabitethernet <IF#>**【スタンドアロン動作時】**

［入力モード］

(config)

［パラメータ］

<switch no.>/<IF#>【スタック動作時】

<IF# >【スタンドアロン動作時】

スイッチ番号，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
   <switch no.>，および <IF#> 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］

なし

［注意事項］

1. ポートの名称は，'geth'+' スイッチ番号 / インタフェースポート番号 ' となります。**【スタック動作時】**
   例　スイッチ番号 1，0/1 のポートの名称は geth1/0/1 となります。
   ポートの名称は，'geth'+' インタフェースポート番号 ' となります。**【スタンドアロン動作時】**
   例　0/1 のポートの名称は geth0/1 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

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］

回線テストを実行している場合，回線テストを中断します。

［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. 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。
3. 本装置はリンク障害の発生から検出まで約 200 ミリ秒かかります。本コマンドはリンク障害検出後のタイマ値を設定するものであるため，本コマンドで 0 ミリ秒を設定した場合でも，リンク障害発生からリンクダウン検出まで約 200 ミリ秒かかります。

［関連コマンド］

なし

link up-debounce

リンク障害回復を検出してからリンクアップするまでのリンクアップ検出時間を設定します。本設定値を大きくすると，一時的なリンクアップを検出しなくなるため，ネットワーク状態が不安定になることを防げます。

［入力形式］

情報の設定・変更
　link up-debounce time <milli seconds>

情報の削除
　no link up-debounce

［入力モード］

(config-if)

［パラメータ］

time <milli seconds>

　リンクアップ時の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
   省略できません。
2. 値の設定範囲
   0 ～ 10000 の値で 100 の倍数

［コマンド省略時の動作］

回線速度を固定設定している場合には 1000 ミリ秒，回線速度をオートネゴシエーション設定している場合には 0 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. リンクアップ検出タイマを長く設定すると，リンク障害回復後，通信できるまでの時間が長くなります。リンク障害回復から通信可能になるまでの時間を短くしたい場合は，リンクアップ検出タイマを設定しないでください。
2. コマンド省略時の値未満にすると，リンクが不安定になることがあります。
3. 本装置はリンク障害の復旧から検出まで約 200 ミリ秒かかります。本コマンドはリンク障害復旧検出後のタイマ値を設定するものであるため，本コマンドで 0 ミリ秒を設定した場合（コマンド省略時含む）でも，リンク障害復旧からリンクアップ検出まで，約 200 ミリ秒かかります。

［関連コマンド］

link debounce

speed

duplex

link-relay source

リンク状態中継先ポートに，リンク状態中継元ポートを設定します。

［入力形式］

情報の設定・変更
　link-relay source interface <interface id list>

情報の削除
　no link-relay source

［入力モード］

(config-if)

［パラメータ］

interface <interface id list>
　リンク状態中継元ポートをリスト形式で指定します。指定できるポートは 4 ポートまでです。
　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。

［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. リンク状態中継元ポートおよびリンク状態中継先ポートは，物理ポートを指定可能です。ポートチャネルインタフェースは指定できません。
2. 同一ポートをリンク状態中継元ポートとリンク状態中継先ポートの両方には設定できません。
3. スタック動作時に使用する場合は，リンク状態中継元ポートとリンク状態中継先ポートの組み合わせを，同一メンバスイッチ内で指定してください。

［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。

また，回線テストを実行している場合，回線テストを中断します。

［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. SFP ポートでは本コマンドは無効です。【08TF】
3. SFP ポートでは本コマンドは無効です。（SFP-T 実装時を除く）【08T】

［関連コマンド］

なし

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 17.1.3 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 11-3　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］

回線テストを実行している場合，回線テストを中断します。

［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. 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 17.1.3 MAC および LLC 副層制御」を参照してください。

表 11-4　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。
3. VLAN トンネリングで Tag が 2 段になる場合は，フレーム長が「IP パケット長＋ 22 オクテット」となります。1500 オクテットの IP パケットを，Tag が 2 段になるポートで送信する場合，mtu に 1504 より大きい値を設定してください。

［関連コマンド］

なし

shutdown

ポートをシャットダウン状態にします。

［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］

回線テストを実行している場合，回線テストを中断します。

［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. 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 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 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

回線速度が最大 1000Mbit/s のイーサネットインタフェースで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。

ポート，回線種別で設定可能なパラメータが異なります。設定可能なパラメータの組み合わせを「表 11-5　設定可能なパラメータ（ポート別）」「表 11-6　設定可能なパラメータ（回線種別）」に示します。

表 11-5　設定可能なパラメータ（ポート別）

モデル名	ポート	設定可能なパラメータ
AX260A-08TF AX260A-08T	0/1 ～ 0/8	10 100 1000 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
	0/9 ～ 0/10	1000 auto auto 1000

表 11-6　設定可能なパラメータ（回線種別）

回線種別	設定可能なパラメータ
10BASE-T/ 100BASE-TX/ 1000BASE-T	10 100 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
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，回線使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 11-5　設定可能なパラメータ（ポート別）」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。

また，回線テストを実行している場合，回線テストを中断します。

［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. UTP ポートを固定設定で使用する場合には MDI-X となります。

［関連コマンド］

duplex

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 17.1.3 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］

回線テストを実行している場合，回線テストを中断します。

［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. 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 17.1.3 MACおよびLLC副層制御」を参照してください。

表 11-7　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 トンネリングで Tag が 2 段になる場合は，フレーム長が「IP パケット長＋ 22 オクテット」となります。1500 オクテットの IP パケットを，Tag が 2 段になるポートで送信する場合，mtu に 1504 より大きい値になるように system mtu を設定するか，ポートで mtu を設定してください。

［関連コマンド］

なし

12 リンクアグリゲーション

channel-group lacp system-priority

channel-group max-active-port

channel-group mode

channel-group periodic-timer

description

interface port-channel

lacp port-priority

lacp system-priority

shutdown

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運用可能な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

ポートをチャネルグループに追加し，また，リンクアグリゲーションのモードを設定します。本コマンドを設定すると，ポートチャネルインタフェースが自動的に作成されます。

［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　18.2.4　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 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。

［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 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 gigabitethernet

channel-group mode

channel-group max-active-port

lacp system-priority

channel-group lacp system-priority コマンドの設定がない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
　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 コマンドの設定がないチャネルグループの LACP システム優先度は 128 になります。

［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

13 MAC アドレステーブル

mac-address-table aging-time

mac-address-table learning

mac-address-table static

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。

- dot1x auto-logout 有効
- web-authentication auto-logout 有効
- mac-authentication auto-logout 有効

[関連コマンド]

なし

mac-address-table learning

ダイナミックな MAC アドレス学習を抑止します。MAC アドレス学習を抑止すると，自装置宛てのフレームおよびスタティックエントリが設定されたフレーム以外はフラッディングします。

［入力形式］

情報の設定・変更

no mac-address-table learning vlan <vlan id list>

情報の削除

mac-address-table learning

［入力モード］

(config)

［パラメータ］

vlan <vlan id list>

学習抑止の対象となる VLAN の VLAN ID を指定します。指定できる VLAN は 4 個までです。

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。

［コマンド省略時の動作］

MAC アドレス学習を抑止しません。

［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］

1. 本コマンド設定時，当該 VLAN のダイナミック学習の MAC アドレスを自動的に消去します。
2. スタック動作時，通信中に MAC アドレス学習の抑止を設定した場合は，必ず運用コマンド clear mac-address-table を実行してください。

［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 <switch no.>/<IF#> | port-channel <channel group>}【スタック動作時】

mac-address-table static <mac> vlan <vlan id> interface {gigabitethernet <IF#> | port-channel <channel group>}【スタンドアロン動作時】

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 <switch no.>/<IF#> | port-channel <channel group>}【スタック動作時】

interface {gigabitethernet <IF#> | port-channel <channel group>}【スタンドアロン動作時】

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
   <switch no.>，<IF#> および <channel group> 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］

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

14 VLAN

interface vlan

l2protocol-tunnel eap

l2protocol-tunnel stp

mac-address

name

protocol

state

switchport access

switchport dot1q ethertype

switchport isolation

switchport mac

switchport mac auto-vlan

switchport mode

switchport protocol

switchport trunk

switchport vlan mapping

switchport vlan mapping enable

vlan

vlan-dot1q-ethertype

vlan-protocol

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，VLAN 全体で 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。vlan コマンドで <VLAN ID list> を設定した場合は設定できません。

[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。設定した情報はトンネリングポートのアクセス VLAN にも反映されます。

［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。トンネリングポートのアクセス VLAN も指定された VLAN 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
   「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］

非 VLAN トンネリングモードのとき，デフォルト VLAN（VLAN ID=1）のアクセスポートになります。VLAN トンネリングモードのときは，どの VLAN にも所属せず，通信に使用できません。

［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. 非 VLAN トンネリングモードでは，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。
2. VLAN トンネリングモードでは，フレームに Tag が付いているかどうかによらず，ポート VLAN でフレームを扱います。

［関連コマンド］

switchport mode

vlan

switchport dot1q ethertype

ポートでVLANフレームを識別するTPID（Tag Protocol IDentifier）値を設定します。標準以外のTPID値を使用しているネットワークと接続する場合に設定します。

［入力形式］

情報の設定・変更
　switchport dot1q ethertype <hex>

情報の削除
　no switchport dot1q ethertype

［入力モード］

(config-if)

［パラメータ］

<hex>

本装置が付けるVLAN Tagの TPID値を設定します。本コマンドでポートのデフォルト値を設定します。

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
   4けたの16進数

［コマンド省略時の動作］

vlan-dot1q-ethertypeコマンドが設定されている場合は，その設定値をTPID値とします。
vlan-dot1q-ethertypeコマンドが設定されていない場合は，TPID値を0x8100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. 本コマンドを指定したポートでは，vlan-dot1q-ethertypeの指定値は適用されません。
2. TPIDの値は装置で4種類（vlan-dot1q-ethertypeを含む）まで指定できます。

［関連コマンド］

なし

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 <interface id list>

情報の変更

switchport isolation interface { <interface id list> | add <interface id list> | remove <interface id list>}

情報の削除

no switchport isolation

［入力モード］

(config-if)

［パラメータ］

interface <interface id list>

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
   <interface 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。

interface add <interface id list>

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
   <interface 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。

interface remove <interface id list>

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
   <interface 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。

［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。
2. 本コマンドで 1 行に指定できる <interface id list> は最大 26 個です。27 個以上指定する場合は，add <interface id list> パラメータで追加設定してください。

［関連コマンド］

なし

switchport mac

MAC VLAN 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，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。

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，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>

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，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 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，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。

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，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。

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，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］

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。

ただし，認証機能との連動によって，認証後 VLAN に指定された MAC VLAN では通信できます。

［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. 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
2. switchport mac dot1q vlan コマンドで指定した VLAN がすでにダイナミック VLAN 認証の認証後 VLAN に指定されていても，当該ダイナミック VLAN 認証は自動的に解除されません。

［関連コマンド］

switchport mode

vlan mac-based

switchport mac auto-vlan

no switchport mac auto-vlan コマンドで，認証機能による認証後 VLAN が switchport mac vlan コマンドで指定された VLAN と一致するときだけ通信できるようにします。

［入力形式］

情報の設定
　no switchport mac auto-vlan

情報の削除
　switchport mac auto-vlan

［入力モード］

(config-if)

［パラメータ］

なし

［コマンド省略時の動作］

認証機能による認証後 VLAN と switchport mac vlan コマンドで指定された VLAN との突合せをしません。

［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. 本コマンドを設定すると，switchport mac vlan コマンドで指定されていない VLAN を認証後 VLAN とする端末のダイナミック VLAN 認証が解除されます。

［関連コマンド］

switchport mac vlan

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 | dot1q-tunnel | stack}

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 | dot1q-tunnel | stack}

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。非 VLAN トンネリング時は，Untagged フレームを送信します。VLAN トンネリング時は，Tagged フレーム，Untagged フレームによらず送受信します。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。

dot1q-tunnel

当該インタフェースをトンネリングポートに設定します。トンネリングポートでは，Tagged フレーム，Untagged フレームによらず送受信します。

stack

インタフェースをスタックポートモードに設定します。

本パラメータはポートチャネルインタフェースには指定できません。

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

   【08T】：access，trunk，protocol-vlan，mac-vlan，または dot1q-tunnel

   上記以外：access，trunk，protocol-vlan，mac-vlan，dot1q-tunnel または stack

［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
4. 当該インタフェースをトンネリングポートに設定した場合，VLAN は switchport access コマンドで設定します。トンネリングポートは，デフォルト VLAN に自動加入しません。デフォルト VLAN を使用する場合は，明示的に switchport access コマンドで VLAN を設定してください。VLAN が設定されていない場合，トンネリングポートでは通信できません。
5. 装置内に一つでもトンネリングポートが設定されている場合は，装置全体が VLAN トンネリングモードになり，アクセスポートもトンネリングポートと同じ動作となります。
6. スタックで動作時にスタックポートモードに設定した場合，またはスタックポートモードからそのほかのモードに設定した場合，リンクが一度ダウンします。
7. スタックポートモードに設定した場合に設定できるコンフィグレーションについては，「コンフィグレーションガイド Vol.1　7.3.2　スタックポートとスタックリンク」を参照してください。
8. スタックポートに設定可能なポートは，以下のとおりです。
   【08TF】0/9 ～ 0/10　最大 2 ポートまで設定可能

［関連コマンド］

set stack

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，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。

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，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 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，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］

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 と MAC 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，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>

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，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>

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，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］

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

switchport vlan mapping

Tag 変換情報エントリを設定します。

［入力形式］

情報の設定・変更
　switchport vlan mapping <vlan tag> <vlan id>

情報の削除
　no switchport vlan mapping <vlan tag> <vlan id>

［入力モード］

(config-if)

［パラメータ］

<vlan tag>

LAN 上で使用する VLAN Tag の値を指定します。

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 ～ 4094

<vlan id>

フレームを扱う VLAN 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。

［コマンド省略時の動作］

Tag 変換しません。

［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. Tag 変換を有効にするためには，switchport vlan mapping enable を指定する必要があります。
2. Tag 変換は，該当ポートがトランクポートのときだけ有効です。
3. ネイティブ VLAN では，送受信するフレームに Tag が付かないため，Tag 変換を指定しても実際には変換されません。VLAN Tag，VLAN ID に，ネイティブ VLAN の VLAN ID を指定しないでください。
4. Tag 変換が有効なポートでは，switchport vlan mapping が設定された VLAN Tag だけが送受信できます。Tag 変換を設定するポートでは，送受信する VLAN Tag と VLAN ID が一致する場合でも switchport vlan mapping を設定してください。

［関連コマンド］

switchport mode trunk

switchport trunk

switchport vlan mapping enable

switchport vlan mapping enable

Tag 変換を有効にします。

［入力形式］

情報の設定
　switchport vlan mapping enable

情報の削除
　no switchport vlan mapping 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］

Tag 変換は無効です。

［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. Tag を変換するためには，switchport vlan mapping を指定する必要があります。
2. Tag 変換は，該当ポートがトランクポートのときだけ有効です。
3. Tag 変換が有効なポートでは，switchport vlan mapping が設定された VLAN Tag だけが送受信できます。Tag 変換を設定するポートでは，送受信する VLAN Tag と VLAN ID が一致する場合でも switchport vlan mapping を設定してください。

［関連コマンド］

switchport mode

switchport trunk

switchport vlan mapping

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。
   ・VLAN トンネリング機能と同時に利用できません。

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。
   ・VLAN トンネリング機能と同時に利用できません。

［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-dot1q-ethertype

VLAN Tag の TPID を設定します。

［入力形式］

情報の設定・変更
　vlan-dot1q-ethertype <hex>

情報の削除
　no vlan-dot1q-ethertype

［入力モード］

(config)

［パラメータ］

<hex>

本装置が付ける VLAN Tag の TPID 値を設定します。本コマンドで全ポートのデフォルト値を設定します。

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
   4 けたの 16 進数

［コマンド省略時の動作］

TPID 値として 0x8100 を使用します。ただし，switchport dot1q ethertype が設定されている回線は，その設定値を TPID 値として使用します。

［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］

なし

［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」の「任意の文字列」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

15 スパニングツリー

instance

name

revision

spanning-tree bpdufilter

spanning-tree bpduguard

spanning-tree cost

spanning-tree disable

spanning-tree guard

spanning-tree link-type

spanning-tree loopguard default

spanning-tree mode

spanning-tree mst configuration

spanning-tree mst cost

spanning-tree mst forward-time

spanning-tree mst hello-time

spanning-tree mst max-age

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst root priority

spanning-tree mst transmission-limit

spanning-tree pathcost method

spanning-tree port-priority

spanning-tree portfast

spanning-tree portfast bpduguard default

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

16 Ring Protocol

axrp

axrp virtual-link

axrp vlan-mapping

axrp-primary-port

axrp-ring-port

control-vlan

disable

flush-request-count

flush-request-transmit vlan

forwarding-shift-time

health-check holdtime

health-check interval

mode

multi-fault-detection holdtime

multi-fault-detection interval

multi-fault-detection mode

multi-fault-detection vlan

name

preempt-delay

vlan-group

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 51 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］

1. Ring Protocol とスパニングツリーの併用，または多重障害監視機能を使用する場合は，リング ID は 8 個までとなります。

［関連コマンド］

なし

axrp virtual-link

スパニングツリーと併用している拠点を識別するための仮想リンク ID を設定します。本装置に設定可能な仮想リンク ID は一つだけです。

［入力形式］

情報の設定・変更

axrp virtual-link <link id> vlan <vlan id>

情報の削除

no axrp virtual-link <link id>

［入力モード］

(config)

［パラメータ］

<link id>

仮想リンク 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 ～ 250

<vlan id>

仮想リンクに使用する 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。

［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. 制御 VLAN に使用している VLAN は指定できません。
2. 同一装置内での多重障害監視機能と，仮想リンクを用いたスパニングツリーとの併用は，同時使用できません。
3. 同一のスパニングツリートポロジを構成するノードは本装置を含め 2 台までです。2 台に設定する仮想リンク ID は同一の ID を指定してください。

［関連コマンド］

vlan

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。
4. Ring Protocol と PVST+ を併用する際は，VLAN マッピングに指定できる VLAN ID は一つだけとなります。Ring Protocol で複数の VLAN を制御したい場合は，別の VLAN マッピング ID に残りの VLAN ID を設定し，該当リング ID の VLAN グループに割り当ててください。
5. Ring Protocol とマルチプルスパニングツリー併用時には，本コマンドで指定する VLAN ID と MST インスタンスに所属する VLAN を一致させる必要があります。不一致となった VLAN はブロッキング状態となります。

［関連コマンド］

vlan

axrp-primary-port

マスタノードでのプライマリポートを設定します。

本コマンドを設定した場合，マスタノードで，プライマリポートは自動で割り当てられず，本コマンドで指定したインタフェースがプライマリポートとして動作します。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-primary-port <ring id> vlan-group <group id>

情報の削除

no axrp-primary-port <ring id> vlan-group <group 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

vlan-group <group id>

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

［コマンド省略時の動作］

プライマリポートは自動で割り当てられます。

［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. リングポートを設定していないインタフェースに対して，本コマンドを入力しても動作しません。
2. Ring Protocol 動作中にプライマリポートの変更または削除をすると，本機能が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。
3. 本装置が次のノードである場合，本コマンドを入力しても動作しません。

- トランジットノード
- 共有リンク非監視リングの最終端となっているマスタノード

4. プライマリポートは，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設定できません。また，プライマリ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。プライマリポートは，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。
5. 一つのリング ID，かつ同一 VLAN グループとなるプライマリポートは一つです。

［関連コマンド］

mode

axrp-ring-port

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・変更

axrp-ring-port <ring id> [{shared-edge | 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-edge | shared}

共有リンクとなるリングポートを指定します。

shared-edge

本装置が共有リンク非監視リングの最終端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 1 ポートだけ指定できます。

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
   shared-edge または shared

［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. 共有リンクありのマルチリング構成の構築で，本装置が隣接するリングですでにマスタノードとして動作している場合，プライマリポートとして使用されているポートに対して，shared-edge 指定のリングポートを設定または削除すると，本機能が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。
3. 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設定できません。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。
4. 本装置がマスタノードに指定されている場合は，登録済みのリングポートに対して VLAN グループごとにプライマリポートが自動で割り当てられます。ただし，axrp-primary-port コマンドで指定されたインタフェースが優先されプライマリポートとして動作します。
5. 共有ノードで共有ポートを指定しなかった場合，Ring Protocol 機能が正常に動作しません。

［関連コマンド］

mode

axrp-primary-port

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。

トランジットノードに対して，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・変更

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. 制御 VLAN に指定した VLAN とスパニングツリーとの併用はできません。
6. 仮想リンクに使用している VLAN を制御 VLAN に指定できません。
7. forwarding-delay-time は，動作モードがトランジットノードの場合だけ有効です。
8. 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

flush-request-count

リングの障害発生／復旧時に，マスタノードがリング内のトランジットノードに対して MAC アドレステーブルのクリアを行うフラッシュ制御フレームを送信する回数を指定します。

［入力形式］

情報の設定・変更
　flush-request-count <count>

情報の削除
　no flush-request-count

［入力モード］

（config-axrp）

［パラメータ］

<count>

フラッシュ制御フレームの送信回数を指定します。

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］

フラッシュ制御フレームの送信回数は 3 回になります。

［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. トランジットノードでの MAC アドレステーブルのエントリのクリア動作は，最初に受信したフラッシュ制御フレームについて実施します。エントリクリア中に受信したフラッシュ制御フレームについては，エントリのクリアは実施しません。

［関連コマンド］

なし

flush-request-transmit vlan

リングの障害発生／復旧時に，隣接するリング構成の装置の MAC アドレステーブルをクリアするため，隣接リング用フラッシュ制御フレームを送信する設定をします。

本設定を行う場合は，「コンフィグレーションガイド Vol.1 25.1.11 隣接リング用フラッシュ制御フレームの送信設定」を参照してください。

［入力形式］

情報の設定・変更
　flush-request-transmit vlan <vlan id>

情報の削除
　no flush-request-transmit vlan

［入力モード］

（config-axrp）

［パラメータ］

<vlan id>

隣接リング用フラッシュ制御フレームを送信する VLAN 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。

［コマンド省略時の動作］

隣接するリング構成の装置に対して，隣接リング用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. 本コマンドはマスタノードに設定してください。トランジットノードに指定しても本機能は有効になりません。
2. VLAN ID には VLAN マッピングで指定した VLAN ID を設定してください。また，この VLAN ID は，隣接リング用フラッシュ制御フレームの送信専用として，データ転送には使用しないでください。

［関連コマンド］

vlan

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・変更
　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

health-check holdtime

マスタノード自身および共有リンク非監視リングの最終端共有ノードが送信したヘルスチェックフレームを，マスタノードが受信しないで障害発生と判断するまでの保護時間を設定します。

［入力形式］

情報の設定・変更
　health-check holdtime <milli seconds>

情報の削除
　no health-check holdtime

［入力モード］

（config-axrp）

［パラメータ］

<milli seconds>

ヘルスチェックフレーム受信までの保護時間を 50 ミリ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
   500 ～ 300000（ミリ秒）

［コマンド省略時の動作］

ヘルスチェックフレームの受信待ち保護時間は 3000 ミリ秒となります。

［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. 本コマンドでは，health-check interval コマンドの設定値よりも大きい値を設定してください。
   health-check interval コマンドの設定値以下の値を本コマンドで設定した場合，ヘルスチェックタイムアウトを検出します。
2. 保護時間を経過した場合，マスタノードは障害発生と判断し，障害処理を行い復旧監視状態へ移行します。
3. リング ID を 9 個以上に設定した場合は，ヘルスチェックフレーム受信待ち保護時間を 3000 ミリ秒以上に設定してください。

［関連コマンド］

なし

health-check interval

マスタノード，または共有リンク非監視リングの最終端共有ノードが送信するヘルスチェック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
　health-check interval <milli seconds>

情報の削除
　no health-check interval

［入力モード］

（config-axrp）

［パラメータ］

<milli seconds>

ヘルスチェックフレームの送信間隔を 50 ミリ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
   200 ～ 60000（ミリ秒）

［コマンド省略時の動作］

ヘルスチェックフレームの送信間隔は 1000 ミリ秒となります。

［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. health-check holdtime コマンドでは，本コマンドの設定値よりも大きい値を設定してください。本コマンドの設定値以下の値を health-check holdtime コマンドで設定した場合，ヘルスチェックタイムアウトを検出します。
2. 同一リングのマスタノードと共有リンク非監視リングの最終端共有ノードでのヘルスチェック送信間隔は同じ値を設定してください。設定値が異なる場合，障害検出処理が正常に行われません。
3. リング ID を 9 個以上に設定した場合は，ヘルスチェックフレームの送信間隔を 1000 ミリ秒以上に設定してください。

［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。

また，リング構成として，共有リンクありのマルチリング構成である場合，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを設定します。

［入力形式］

情報の設定・変更
　mode {master | transit} [ring-attribute {rift-ring | rift-ring-edge <edge node id>}]

情報の削除
　no mode

［入力モード］

（config-axrp）

［パラメータ］

{master | transit}

動作モードを指定します。

master

マスタノードとして動作します。

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
   master または transit

ring-attribute {rift-ring | rift-ring-edge <edge node id>}

共有リンクありのマルチリング構成でのリングの属性として，共有リンク非監視リング（共有リンクを監視しないリング）を指定し，またそのリングでの本装置の位置づけを指定します。
なお，rift-ring-edge を指定した場合は，axrp-ring-port コマンドに shared-edge パラメータを指定する必要があります。

rift-ring

共有リンク非監視リングを構成するノード（ただし，最終端ノードは除く）として動作します。
本パラメータは，マスタノードの場合だけ指定できます。

rift-ring-edge <edge node id>

共有リンク非監視リングの最終端となるノード（共有ノード）として動作します。二つある最終端ノードを区別するために，装置単位でエッジノード ID（1 または 2）を指定します。

1. 本パラメータ省略時の初期値
   マスタノードの場合，共有リンク監視リング（共有リンクを監視するリング）のマスタノードとして動作します。
   トランジットノードの場合，共有リンク監視リング，または共有リンク非監視リングのトランジットノードとして動作します。
2. 値の設定範囲
   rift-ring，rift-ring-edge1，または rift-ring-edge 2

［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. マスタノードはリング内に一装置だけ設定してください。複数設定した場合，Ring Protocol 機能が正常に動作しません。
2. Ring Protocol 動作中にモード変更，または削除を行うと，本機能が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。
3. ring-attribute パラメータに rift-ring-edge を指定した場合は，axrp-ring-port コマンドに shared-edge パラメータを指定してください。
4. 同一リングの共有リンク非監視リングの最終端ノードには，それぞれ異なるエッジノード ID を指定してください。正しく設定されていない場合，リング機能が正常に動作しません。

［関連コマンド］

なし

multi-fault-detection holdtime

共有リンクありのマルチリング構成の共有リンクの両端に位置する共有ノードが，共有リンク監視リングに送信した多重障害監視フレームを受信しないで多重障害発生と判断するまでの保護時間を設定します。

［入力形式］

情報の設定・変更

multi-fault-detection holdtime <milli seconds>

情報の削除

no multi-fault-detection holdtime

［入力モード］

(config-axrp)

［パラメータ］

<milli seconds>

多重障害監視フレーム受信までの保護時間を 50 ミリ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
   1000 ～ 300000（ミリ秒）

［コマンド省略時の動作］

多重障害監視フレームの受信待ち保護時間は 6000 ミリ秒となります。

［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. 同一装置内での多重障害監視機能と，仮想リンクを用いたスパニングツリーとの併用は，同時使用できません。
2. multi-fault-detection holdtime には対向共有ノードの multi-fault-detection interval より大きな値を設定してください。対向共有ノードの multi-fault-detection interval 以下の値を設定した場合，多重障害を検出します。
3. 保護時間を経過した場合，共有ノードは共有リンク監視リングに多重障害が発生したと判断し，障害処理を行います。

［関連コマンド］

なし

multi-fault-detection interval

共有リンクありのマルチリング構成の共有リンクの両端に位置する共有ノードが，共有リンク監視リングに送信する多重障害監視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

multi-fault-detection interval <milli seconds>

情報の削除

no multi-fault-detection interval

［入力モード］

(config-axrp)

［パラメータ］

<milli seconds>

多重障害監視フレームの送信間隔を 50 ミリ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
   500 ～ 60000（ミリ秒）

［コマンド省略時の動作］

多重障害監視フレームの送信間隔は 2000 ミリ秒となります。

［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. 同一装置内での多重障害監視機能と，仮想リンクを用いたスパニングツリーとの併用は，同時使用できません。
2. multi-fault-detection interval には対向共有ノードの multi-fault-detection holdtime より小さい値を設定してください。multi-fault-detection holdtime 以上の値を設定した場合，対向共有ノードが多重障害を検出します。

［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と，多重障害検出時にリング経路を切り替えるためのバックアップリングに使用する共有リンク非監視リングのリング ID を設定します。

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・変更

multi-fault-detection mode {monitor-enable backup-ring <ring id> | transport-only}

情報の削除

no multi-fault-detection mode

［入力モード］

(config-axrp)

［パラメータ］

{monitor-enable backup-ring <ring id> | transport-only}

多重障害監視機能の監視モードを指定します。

monitor-enable backup-ring <ring id>

多重障害監視フレームの送信および受信監視を行います。本パラメータは最終端共有ノードの共有リンク監視リングに設定します。また，多重障害検出時にリング経路を切り替えるためのバックアップリングに使用する共有リンク非監視リングのリング ID を指定します。

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
   monitor-enable backup-ring <ring id> または transport-only。
   <ring id> には，次の値を指定できます。
   1 ～ 65535

［コマンド省略時の動作］

共有リンク監視リングの多重障害監視を行いません。

［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. 同一装置内での多重障害監視機能と，仮想リンクを用いたスパニングツリーとの併用は，同時使用できません。
2. 多重障害の監視を行う装置は，共有リンクの両端に位置する共有ノードとなります。共有ノード以外の装置で監視機能（monitor-enable パラメータ）を有効にすると，多重障害の監視を正常に行えません。

[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送受信を実施します。

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・変更
　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 <vlan id>

多重障害監視に使用する 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］

共有リンク監視リングの多重障害監視を行いません。

［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. 同一装置内での多重障害監視機能と，仮想リンクを用いたスパニングツリーとの併用は，同時使用できません。
2. 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。
3. 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。
4. 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・変更
　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

preempt-delay

マスタノードで，障害復旧検出後，経路切り戻し動作を実施するまでの抑止時間を設定します。

本コマンドを設定した場合，マスタノードは障害復旧を検出しても，経路切り戻し抑止時間が経過するまで，復旧動作を実施しません。

［入力形式］

情報の設定・変更
　preempt-delay { <seconds> | infinity }

情報の削除
　no preempt-delay

［入力モード］

（config-axrp）

［パラメータ］

{ <seconds> | infinity }

<seconds>
　経路切り戻し抑止時間を秒単位で指定します。

infinity
　抑止時間が無限となり，運用コマンド clear axrp preempt-delay を実行するまで，マスタノードは復旧動作を実施しません。

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 ～ 3600（秒）または infinity

［コマンド省略時の動作］

経路切り戻し動作を抑止しません。

［通信への影響］

なし

［設定値の反映契機］

本コマンドの設定または変更時，リング状態が正常の場合は，すぐに運用に反映されます。リング状態が障害発生中の場合は，次回に反映されます。

本コマンドの削除時，すぐに運用に反映されます。

［注意事項］

1. 本機能を設定する場合は，リングを構成するすべてのトランジットノードの forwarding-shift-time に infinity を設定するか，経路切り戻し抑止時間よりも大きな値を設定してください。経路切り戻し抑止時間よりも小さな値を設定した場合，ループが発生するおそれがあります。

［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。また，VLAN グループを二つ作成することによって，VLAN ごとに負荷分散を行えます。

［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/shared-edge 設定のリングポート）の場合は指定できます。

2. 本装置がマスタノードに指定されている場合は，登録済みのリングポートに対して VLAN グループごとにプライマリポートが自動で割り当てられます。ただし，axrp-primary-port コマンドが入力済みの場合は，指定されたインタフェースが優先されてプライマリポートに設定されます。

［関連コマンド］

axrp vlan-mapping

17 IGMP snooping

ip igmp snooping（global）

ip igmp snooping（interface）

ip igmp snooping fast-leave

ip igmp snooping mrouter

ip igmp snooping mrouter discovery

ip igmp snooping mrouter discovery extension

ip igmp snooping mrouter logging

ip igmp snooping querier

ip igmp snooping query-interval

ip igmp snooping（global）

no ip igmp snooping 設定時，本装置の 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］

なし

［関連コマンド］

なし

ip igmp snooping fast-leave

VLAN インタフェースで，IGMP Leave および IGMPv3 Report（離脱要求）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 および IGMPv3 Report（離脱要求）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 および IGMPv3 Report（離脱要求）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］

1. 本コマンドを設定して IGMP Leave および IGMPv3 Report（離脱要求）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静的に設定します。

［入力形式］

情報の設定・変更

ip igmp snooping mrouter interface {gigabitethernet <switch no.>/<IF#> | port-channel <channel group>}【スタック動作時】

ip igmp snooping mrouter interface {gigabitethernet <IF#> | port-channel <channel group>}【スタンドアロン動作時】

情報の削除

no ip igmp snooping mrouter interface {gigabitethernet <switch no.>/<IF#> | port-channel <channel group>}【スタック動作時】

no ip igmp snooping mrouter interface {gigabitethernet <IF#> | port-channel <channel group>}【スタンドアロン動作時】

［入力モード］

(config-if)

［パラメータ］

{gigabitethernet <switch no.>/<IF#> | port-channel <channel group>}【スタック動作時】

{gigabitethernet <IF#> | port-channel <channel group>}【スタンドアロン動作時】

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
   <switch no.>，<IF#> および <channel group> 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 mrouter discovery

VLAN インタフェースで，マルチキャストルータを検知する監視パケット種別を設定します。マルチキャストルータを検知した場合，当該 VLAN の属するポートをマルチキャストルータポートとして動的に設定します。

［入力形式］

情報の設定

ip igmp snooping mrouter discovery igmp
ip igmp snooping mrouter discovery pim

情報の削除

no ip igmp snooping mrouter discovery igmp
no ip igmp snooping mrouter discovery pim

［入力モード］

(config-if)

［パラメータ］

igmp

IGMP パケットを監視対象にします。

pim

PIM パケットを監視対象にします。

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

［コマンド省略時の動作］

IGMP パケット，PIM パケットともに監視対象としません。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに反映されます。

［注意事項］

1. ip igmp snooping mrouter discovery igmp を設定する場合は，当該 VLAN に ip igmp snooping を設定してください。
2. 本コマンドを削除した場合は，当該 VLAN が属するポートで検知したマルチキャストルータ情報をクリアします。なお，当該 VLAN の ip igmp snooping を削除してもマルチキャストルータ情報はクリアせず，保持時間満了時にクリアします。

［関連コマンド］

ip igmp snooping（interface）

ip igmp snooping mrouter discovery extension

VLAN インタフェースで検知したマルチキャストルータ情報の保持時間の加算値を設定します。

［入力形式］

情報の設定・変更

ip igmp snooping mrouter discovery extension <seconds>

情報の削除

no ip igmp snooping mrouter discovery extension

［入力モード］

(config)

［パラメータ］

<seconds>

検知したマルチキャストルータ情報の保持時間の加算値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］

保持時間の加算値が 0 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，すぐに反映されます。

［注意事項］

なし

［関連コマンド］

なし

ip igmp snooping mrouter logging

VLAN インタフェースで no ip igmp snooping mrouter logging 設定時，マルチキャストルータ検知に関する運用ログの出力を抑止します。次の運用ログが対象です。

- E3 SNOOP 02e30000 Multicast router discovery table overflow.
  （検知したマルチキャストルータ数が収容条件を超過したので学習できません。）
- E3 SNOOP 02e31100 Found <Type> router <IPv4 address> on VLAN <VLAN ID> <IF#>.
  （マルチキャストルータを検知しました。）
- E3 SNOOP 02e31200 Lost <Type> router <IPv4 address> on VLAN <VLAN ID> <IF#>.
  （マルチキャストルータを削除しました。）

［入力形式］

情報の設定

no ip igmp snooping mrouter logging

情報の削除

ip igmp snooping mrouter logging

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

マルチキャストルータ検知に関する運用ログを採取します。

［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］

なし

［関連コマンド］

なし

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］

1. 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

ip igmp snooping query-interval

VLAN インタフェースで，装置から定期的に送信する IGMP Query メッセージの送信間隔を設定します。

［入力形式］

情報の設定・変更

ip igmp snooping query-interval <seconds>

情報の削除

no ip igmp snooping query-interval

［入力モード］

(config-if)

［パラメータ］

<seconds>

Query メッセージの送信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 ～ 300（秒）

［コマンド省略時の動作］

125 秒で動作します。

［通信への影響］

IGMP クエリア機能運用中に本コマンドを変更すると，グループ情報が一時的にタイムアウトする場合があります。

［設定値の反映契機］

設定値変更後，すぐに反映されます。

［注意事項］

IGMPv3 で運用している VLAN で本装置が代表クエリアの場合，または IGMPv2 で運用している場合，他装置を含む当該 VLAN 内では，IGMP Query メッセージ送信間隔を本コマンドで同じ値に設定してください。

［関連コマンド］

ip igmp snooping

ip igmp snooping querier

ip address

18 MLD snooping

ipv6 mld snooping（global）

ipv6 mld snooping（interface）

ipv6 mld snooping source

ipv6 mld snooping mrouter

ipv6 mld snooping querier

ipv6 mld snooping（global）

no ipv6 mld snooping 設定時，本装置の 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］

なし

［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。
4. IPv6 アドレスは省略形で表示します。

［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>}

情報の削除

no ipv6 mld snooping mrouter interface {gigabitethernet <IF#> | port-channel <channel group>}

［入力モード］

(config-if)

［パラメータ］

{gigabitethernet <IF#> | port-channel <channel group>}

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#> および <channel group> 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

19 IPv4・ARP・ICMP

arp
ip address
ip mtu
ip route

arp

スタティック ARP テーブルを作成します。ARP をサポートしていない製品が接続されている場合，IPv4 アドレスと物理アドレスの変換ができないため，あらかじめスタティック ARP テーブルを作成しておく必要があります。

［入力形式］

情報の設定・変更

arp <ip address> interface vlan <vlan id> <mac address>

情報の削除

no arp <ip address>

［入力モード］

(config)

［パラメータ］

<ip address>

ネクストホップ 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 ユニキャストアドレスを指定します。

interface vlan <vlan id>

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
   <vlan id> には interface vlan コマンドで設定した VLAN ID を指定します。

<mac address>

接続先 MAC アドレス（キャノニカル・フォーマット）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
   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。

［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

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> ［secondary］

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）

secondary

マルチホームの場合にセカンダリ設定を指定します。

1. 本パラメータ省略時の初期値
   プライマリ設定となります。マルチホームの場合でも，プライマリ設定を一つ必ず指定してください。
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］

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，show ipv6 interface，または show ip-dual 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］

RA 受信した MTU とポート MTU 情報で設定された MTU を比較し，小さい方の値を IP MTU 長として使用します。

RA 受信していない場合は，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。
2. Web 認証と DHCP サーバ機能を使用する場合は，IP MTU 長をデフォルトコンフィグレーションで運用してください。
   デフォルトコンフィグレーションより短くすると，Web 認証や DHCP サーバ機能で正常に動作しない場合があります。

3. 本設定はIPv6でも有効となります。IPv6ではMTU長を1280以上とすることがプロトコル仕様として決められています。よって，IPv6を使用する場合は，MTU長に1280未満を指定しないでください。
4. 本設定を省略した場合，RA受信したMTUがIPv4にも適用されます。

［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
   【スタック動作時】0.0.0.0
   【スタンドアロン動作時】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
   【スタック動作時】0.0.0.0
   【スタンドアロン動作時】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]

スタック動作時，デフォルトゲートウェイ以外の設定はできません。

[関連コマンド]

なし

20 IPv6・NDP・ICMPv6

ipv6 address
ipv6 default-gateway
ipv6 enable
ipv6 nd accept-ra
ipv6 neighbor

ipv6 address

自 IPv6 アドレスを指定します。

[入力形式]

情報の設定・変更

ipv6 address { <ipv6 address>[/<prefixlen>] | <ipv6 prefix>[/<prefixlen>] }

情報の削除

no ipv6 address { <ipv6 address>[/<prefixlen>] | <ipv6 prefix>[/<prefixlen>] }

[入力モード]

(config-if)

[パラメータ]

<ipv6 address>

自 IPv6 アドレスを指定します。

1. 値の設定範囲
   IPv6 グローバルユニキャストアドレスを指定します。
   ただし，<ipv6 address>/<prefixlen> が 0::/64，または fe80::/10 に重なる指定はできません。

<ipv6 prefix>

IPv6 プレフィックスを指定します。インタフェース -ID 部を自動設定とする場合に指定します。自動設定する場合は，必ずプレフィックス長に 64 を設定してください。

1. 値の設定範囲
   IPv6 アドレスのインタフェースー ID 部が 0 の IPv6 グローバルユニキャストアドレスを指定します。ただし，0::/64 は指定できません。

/<prefixlen>

プレフィックス長を指定します。

1. 本パラメータ省略時の初期値
   64
2. 値の設定範囲
   1 ～ 64

[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］

interface vlan

ipv6 enable

ipv6 default-gateway

デフォルト経路の IPv6 アドレスを指定します。

［入力形式］

情報の設定

グローバルアドレスの場合

ipv6 default-gateway <ipv6 address>

リンクローカルアドレスの場合

ipv6 default-gateway interface vlan <vlan id> <ipv6 address>

情報の削除

no ipv6 default-gateway

［入力モード］

(config)

［パラメータ］

<ipv6 address>

デフォルト経路のゲートウェイである IPv6 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
   interface vlan <vlan id> を指定しない場合
   IPv6 グローバルユニキャストアドレスを指定します。
   interface vlan <vlan id> を指定する場合
   IPv6 リンクローカルユニキャストアドレス（fe80::/64 だけ）を指定します。

interface vlan <vlan id>

VLAN ID を指定します。

1. 本パラメータ省略時の初期値
   IPv6 リンクローカルユニキャストアドレスを設定する場合，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］

interface vlan

ipv6 address

ipv6 enable

ipv6 enable

IPv6 アドレスを使用する場合に指定します。

本コマンドを指定すると自動生成リンクアドレスが生成されます。

［入力形式］

情報の設定
　ipv6 enable

情報の削除
　no ipv6 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］

IPv6 アドレスを使用できません。

IPv6 アドレスを使用する場合に，ipv6 enable を指定してください。

［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］

なし

［関連コマンド］

interface vlan

ipv6 nd accept-ra

RA を受信して IPv6 アドレスやデフォルトゲートウェイを自動設定します。

［入力形式］

情報の設定
　ipv6 nd accept-ra

情報の削除
　no ipv6 nd accept-ra

［入力モード］

(config-if)

［パラメータ］

なし

［コマンド省略時の動作］

RA を受信しても破棄します。RS 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. 本コマンドの設定および削除は，ipv6 enable コマンド未設定の状態で行ってください。
2. コンフィグレーションガイド Vol.1 3.2.5 IP インタフェース「(1) IP アドレスを設定できる最大インタフェース数」と「(2) VLAN ごとの受信制御ができる最大インタフェース数」に関して，本コマンドが設定された VLAN インタフェースは IPv6 アドレスが設定されているものとみなされます。

［関連コマンド］

ipv6 enable

ipv6 neighbor

スタティック NDP テーブルを作成します。NDP をサポートしていない製品が接続されている場合，IPv6 アドレスと物理アドレスの変換ができないため，あらかじめスタティック NDP テーブルを作成しておく必要があります。

［入力形式］

情報の設定・変更

ipv6 neighbor <ipv6 address> interface vlan <vlan id> <mac address>

情報の削除

no ipv6 neighbor <ipv6 address>

［入力モード］

(config)

［パラメータ］

<ipv6 address>

ネクストホップ IPv6 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
   IPv6 グローバルユニキャストアドレス（0::/64 以外），または IPv6 リンクローカルユニキャストアドレス（fe80::/64 だけ）を指定します。

interface vlan <vlan id>

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
   <vlan id> には interface vlan コマンドで設定した VLAN ID を指定します。

<mac address>

接続先 MAC アドレス（キャノニカル・フォーマット）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
   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。

［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］

ipv6 enable

21 DHCP サーバ機能

default-router

dns-server

hardware-address

host

ip dhcp excluded-address

ip dhcp pool

lease

max-lease

network

service dhcp

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

hardware-address

クライアント装置に固定の IP アドレスを配布する際に，対象となる装置の MAC アドレスを指定します。本コマンドは host コマンドとセットで使用します。

［入力形式］

情報の設定・変更
　hardware-address <MAC address> <protocol>

情報の削除
　no hardware-address

［入力モード］

(dhcp-config)

［パラメータ］

<MAC address>

DHCP アドレスプール情報に対する MAC 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
   1 バイトずつの 16 進で表す
   （入力例）0211.2233.4455

<protocol>

DHCP アドレスプール情報に対するプロトコルを指定します。指定方法はシンボルまたは数値で指定できます。

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
   ethernet（数値指定の場合は 1）だけ

［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. network コマンドと同時に入力することはできません。
2. 本コマンドは，host コマンドを設定することで有効となります。

［関連コマンド］

host

host

クライアント装置に固定の IP アドレスを配布する際に，割り当てる IP アドレスを指定します。本コマンドは hardware-address コマンドとセットで使用します。

［入力形式］

情報の設定・変更
　host {<ip address>/<masklen> | <ip address> [<mask>]}

情報の削除
　no host

［入力モード］

(dhcp-config)

［パラメータ］

{<ip address>/<masklen> | <ip address> [<mask>]}

DHCP アドレスプール情報に対する IP 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 21-1　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 1 のアドレス
   ・「表 21-1　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 21-1　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

<mask>

1. 本パラメータ省略時の初期値
   「表 21-1　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
   255.0.0.0 ～ 255.255.255.255

［コマンド省略時の動作］

なし

［通信への影響］

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. 同一プール設定内で network 設定とは同時に設定できません。
2. host 設定時に同じサブネットの network および host 設定が存在しない場合，そのサブネットも network 設定数と同様に扱われます。そのため，最大管理サブネット数を超えるサブネットに対する固定アドレスプールを用意することはできません。
3. host 設定を行った場合，クライアントに配布するオプション情報（default-router，dns-server）は設定された IP アドレスと同じサブネットの network 設定を行った DHCP アドレスプールのオプション情報を継承します。
4. 本コマンドは，hardware-address コマンドを設定することで有効となります。
5. 直収サブネット（本装置の VLAN インタフェースサブネット）にアドレスを配布するときは，ip address コマンドと同じマスク長にしてください。
6. 本コマンドで指定したマスクはクライアントに通知されます。

［関連コマンド］

hardware-address

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 1024 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 文字以内の名前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］

1. 本コマンドは最大管理サブネット数と最大固定 IP アドレス数の合計値まで設定できます。

［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 1 日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 1 日となります。

［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. 固定 IP アドレス設定を行った場合は，クライアントは標準で 24 時間のリース時間を持ちます（ただし，固定 IP アドレスで配布を行った場合は show ip dhcp binding コマンドでリース期限を表示しません）。また，その固定 IP アドレスと同じサブネットの network 設定を行った DHCP アドレスプールが在る場合は，そのプールのリース時間が優先されます。
3. 固定 IP アドレス設定を行っている DHCP アドレスプール情報では lease コマンドは無視されます。
4. 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。
5. 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. 固定 IP アドレス設定を行った場合は，クライアントは標準で 24 時間のリース時間を持ちます。また，その固定 IP アドレスと同じサブネットの network 設定を行った DHCP アドレスプールが在る場合は，そのプールの最大リース時間が優先されます。
2. 固定 IP アドレス設定を行っている DHCP アドレスプール情報では max-lease コマンドは無視されます。
3. 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。
4. 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> | <ip address> [<mask>]}

情報の削除

no network

［入力モード］

(dhcp-config)

［パラメータ］

{<ip address>/<masklen> | <ip address> [<mask>]}

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 21-2　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 0 以外のアドレス
   ・「表 21-2　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 21-2　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

<mask>

1. 本パラメータ省略時の初期値
   「表 21-2　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
   255.0.0.0 ～ 255.255.255.255

［コマンド省略時の動作］

なし

［通信への影響］

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. 同一プール設定内で，host および hardware-address 設定とは同時に設定できません。
3. network 設定を含むプールは，最大管理サブネット数まで作成できます。また，host 設定時に同一のサブネットを持つ network/host 設定が存在しない場合，そのサブネットについても network 設定数と同様に扱われます。
4. 直収サブネット（本装置の VLAN インタフェースサブネット）にアドレスを配布するときは，ip address コマンドと同じマスク長にしてください。

［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 64 です。

［関連コマンド］

interface vlan

22 フロー検出モード

flow detection mode

flow detection out mode

flow detection mode

受信側インタフェースに対し，フィルタ・QoS 機能，およびポリシーベースミラーリング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
- ipv6 traffic-filter
- mac access-group
- ip qos-flow-group
- ipv6 qos-flow-group
- mac qos-flow-group

また，以下の機能を未サポートのモードに変更する場合も，各コマンドを削除する必要があります。

- ホワイトリスト機能：white-list enable
- 特定端末への Web 通信不可機能：access-redirect http port
- ポリシーベースミラーリング：monitor session filter

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（デフォルトコンフィグレーション）になります。

［入力形式］

情報の設定・変更
　flow detection mode {layer2-1 | layer2-2 | layer2-3 | layer2-1-mirror | layer2-2-mirror}

情報の削除
　no flow detection mode

［入力モード］

(config)

［パラメータ］

{layer2-1 | layer2-2 | layer2-3 | layer2-1-mirror | layer2-2-mirror}

受信側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

受信側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 22-1　受信側フロー検出モードによる適用コマンド（フィルタ，ポリシーベースミラーリング）

受信側フロー検出モード	適用コマンド		
	mac access-group	ip access-group	ipv6 traffic-filter
layer2-1	○	×	×
layer2-2	×	○	×
layer2-3	×	○	○
layer2-1-mirror	○	×	×
layer2-2-mirror	×	○	×

（凡例）　○：設定可能　×：設定不可

表 22-2　受信側フロー検出モードによる適用コマンド（QoS）

受信側フロー検出モード	適用コマンド		
	mac qos-flow-group	ip qos-flow-group	ipv6 qos-flow-group
layer2-1	○	×	×
layer2-2	×	○	×
layer2-3	×	○	○
layer2-1-mirror	×	×	×
layer2-2-mirror	×	×	×

（凡例）　○：設定可能　×：設定不可
各受信側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 受信側フロー検出モード」（フィルタ）および「コンフィグレーションガイド Vol.2 3.1.1 受信側フロー検出モード」（QoS）を参照してください。

［コマンド省略時の動作］

受信側フロー検出モードは，layer2-2 で動作します。

［通信への影響］

system receive control fine 設定時に本コマンドを変更した場合，全ポートが一時的に通信断となります。

［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］

ip access-group

ipv6 traffic-filter

mac access-group

ip qos-flow-group

ipv6 qos-flow-group

mac qos-flow-group

monitor session filter

white-list enable

flow detection out mode

送信側インタフェースに対し，フィルタ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，変更する場合は送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
- ipv6 traffic-filter
- mac access-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-out（デフォルトコンフィグレーション）になります。

［入力形式］

情報の設定・変更
　flow detection out mode {layer2-1-out | layer2-2-out | layer2-3-out}

情報の削除
　no flow detection out mode

［入力モード］

(config)

［パラメータ］

{layer2-1-out | layer2-2-out | layer2-3-out}

送信側フロー検出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。
2. 値の設定範囲
   なし

送信側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 22-3　送信側フロー検出モードによる適用コマンド

送信側フロー検出モード	適用コマンド		
	mac access-group	ip access-group	ipv6 traffic-filter
layer-2-1-out	○	×	×
layer-2-2-out	×	○	×
layer-2-3-out	○	○	○

（凡例）　○：設定可能　×：設定不可
各送信側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 1.1.4 送信側フロー検出モード」を参照してください。

［コマンド省略時の動作］

送信側フロー検出モードは，layer2-2-out 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

ipv6 traffic-filter

mac access-group

23 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（ipv6 access-list）
deny（mac access-list extended）
ip access-group
ip access-list extended
ip access-list resequence
ip access-list standard
ipv6 access-list
ipv6 access-list resequence
ipv6 traffic-filter
mac access-group
mac access-list extended
mac access-list resequence
permit（ip access-list extended）
permit（ip access-list standard）
permit（ipv6 access-list）
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 23-1　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

注 ※　プロトコル名称 ah またはプロトコル番号 51 は，フィルタ条件として指定しても検出できません。

■プロトコル名称（IPv6）

IPv6 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 23-2　指定可能なプロトコル名称（IPv6）

プロトコル名称	対象プロトコル番号
gre	47
icmp	58
ipv6	すべての IP プロトコル
ospf	89
pcp	108
pim	103
sctp	132
tcp	6
tunnel	4
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 23-3　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)
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)

ポート名称	対象ポート名および番号
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 23-4　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)
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)

表 23-5　UDP で指定可能なポート名称（IPv6）

ポート名称	対象ポート名および番号
biff	Biff (512)
dhcpv6-client	DHCPv6 client (546)
dhcpv6-server	DHCPv6 server (547)
discard	Discard (9)
domain	Domain Name System (53)

ポート名称	対象ポート名および番号
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
ripng	Routing Information Protocol next generation (521)
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 23-6　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 23-7　指定可能な Precedence 名称

Precedence 名称	Precedence 値
critical	5
flash	3
flash-override	4
immediate	2

Precedence 名称	Precedence 値
internet	6
network	7
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 23-8　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 23-9　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	

イーサネットタイプ名称	Ethernet 値	備考
gsrp	― ※	GSRP 制御パケットをフィルタします
ipv4	0x0800	
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 23-10　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

■メッセージ名称（ICMP）

ICMP で指定できるメッセージ名称を，次の表に示します。

表 23-11　ICMP で指定可能なメッセージ名称（IPv4）

メッセージ名称	メッセージ名	タイプ	コード
administratively-prohibited	Administratively prohibited	3	13
alternate-address	Alternate address	6	指定なし
conversion-error	Datagram conversion	31	指定なし
dod-host-prohibited	Host prohibited	3	10
dod-net-prohibited	Network prohibited	3	9
echo	Echo (ping)	8	指定なし
echo-reply	Echo reply	0	指定なし
general-parameter-problem	Parameter problem	12	0
host-isolated	Host isolated	3	8
host-precedence-unreachable	Host unreachable for precedence	3	14
host-redirect	Host redirect	5	1
host-tos-redirect	Host redirect for TOS	5	3
host-tos-unreachable	Host unreachable for TOS	3	12
host-unknown	Host unknown	3	7
host-unreachable	Host unreachable	3	1
information-reply	Information replies	16	指定なし

メッセージ名称	メッセージ名	タイプ	コード
information-request	Information requests	15	指定なし
mask-reply	Mask replies	18	指定なし
mask-request	Mask requests	17	指定なし
mobile-redirect	Mobile host redirect	32	指定なし
net-redirect	Network redirect	5	0
net-tos-redirect	Network redirect for TOS	5	2
net-tos-unreachable	Network unreachable for TOS	3	11
net-unreachable	Network unreachable	3	0
network-unknown	Network unknown	3	6
no-room-for-option	Parameter required but no room	12	2
option-missing	Parameter required but not present	12	1
packet-too-big	Fragmentation needed and DF set	3	4
parameter-problem	All parameter problems	12	指定なし
port-unreachable	Port unreachable	3	3
precedence-unreachable	Precedence cutoff	3	15
protocol-unreachable	Protocol unreachable	3	2
reassembly-timeout	Reassembly timeout	11	1
redirect	All redirects	5	指定なし
router-advertisement	Router discovery advertisements	9	指定なし
router-solicitation	Router discovery solicitations	10	指定なし
source-quench	Source quenches	4	指定なし
source-route-failed	Source route failed	3	5
time-exceeded	All time exceeded	11	指定なし
timestamp-reply	Timestamp replies	14	指定なし
timestamp-request	Timestamp requests	13	指定なし
traceroute	Traceroute	30	指定なし
ttl-exceeded	TTL exceeded	11	0
unreachable	All unreachable	3	指定なし

表 23-12　ICMP で指定可能なメッセージ名称（IPv6）

メッセージ名称	メッセージ名	タイプ	コード
beyond-scope	Destination beyond scope	1	2
destination-unreachable	Destination address is unreachable	1	3
echo-reply	Echo reply	129	指定なし
echo-request	Echo request (ping)	128	指定なし
header	Parameter header problems	4	0
hop-limit	Hop limit exceeded in transit	3	0
mld-query	Multicast Listener Discovery Query	130	指定なし
mld-reduction	Multicast Listener Discovery Reduction	132	指定なし
mld-report	Multicast Listener Discovery Report	131	指定なし

メッセージ名称	メッセージ名	タイプ	コード
nd-na	Neighbor discovery neighbor advertisements	136	指定なし
nd-ns	Neighbor discovery neighbor solicitations	135	指定なし
next-header	Parameter next header problems	4	1
no-admin	Administration prohibited destination	1	1
no-route	No route to destination	1	0
packet-too-big	Packet too big	2	指定なし
parameter-option	Parameter option problems	4	2
parameter-problem	All parameter problems	4	指定なし
port-unreachable	Port unreachable	1	4
reassembly-timeout	Reassembly timeout	3	1
renum-command	Router renumbering command	138	0
renum-result	Router renumbering result	138	1
renum-seq-number	Router renumbering sequence number reset	138	255
router-advertisement	Neighbor discovery router advertisements	134	指定なし
router-renumbering	All router renumbering	138	指定なし
router-solicitation	Neighbor discovery router solicitations	133	指定なし
time-exceeded	All time exceeded	3	指定なし
unreachable	All unreachable	1	指定なし

■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
- ipv6 access-list
- 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 gigabitethernet/vlan 下の ip access-group
- interface gigabitethernet/vlan 下の ipv6 traffic-filter
- interface gigabitethernet/vlan 下の mac access-group

注 ※1　in と out は別件数に数えます。

注 ※2　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/ipv6 traffic-filter
・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※
- ipv6 access-list※
- 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（スタック動作時はスタック全体）で，IPv4，IPv6，MAC のアクセスリストを最大 512 エントリ

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，IPv6 フィルタ，MAC フィルタごとに，フィルタ条件を装置全体（スタック動作時はスタック全体）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 23-13　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 AAAAA を作成して，イーサネットインタフェース 1/0/1 の inbound に設定
`interface gigabitethernet 1/0/1`
`  ip access-group AAAAA in`
`ip access-list extended AAAAA`
`  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 AAAAA を作成して，イーサネットインタフェース 1/0/1 と 1/0/2 の inbound に設定
`interface gigabitethernet 1/0/1`
`  ip access-group AAAAA in`
`interface gigabitethernet 1/0/2`
`  ip access-group AAAAA in`
`ip access-list extended AAAAA`
`  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

アクセスリスト AAAAA を作成して，イーサネットインタフェース 1/0/1 の inbound と outbound に設定
`interface gigabitethernet 1/0/1`
`  ip access-group AAAAA in`
`  ip access-group AAAAA out`
`ip access-list extended AAAAA`
`  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

アクセスリスト AAAAA を作成して，イーサネットインタフェース 1/0/1 の inbound に設定
アクセスリスト BBBBB を作成して，イーサネットインタフェース 1/0/2 の inbound に設定
`interface gigabitethernet 1/0/1`
`  ip access-group AAAAA in`
`interface gigabitethernet 1/0/2`
`  ip access-group BBBBB in`
`ip access-list extended AAAAA`
`  10 permit tcp any any`
`  20 deny udp any any`
`ip access-list extended BBBBB`
`  10 permit udp any any`
`  20 deny tcp any any`
	2 リスト	2 リスト	2 リスト	6 リスト

アクセスリスト AAAAA を作成して，イーサネットインタフェース 1/0/1 の inbound に設定
アクセスリスト BBBBB を作成して，イーサネットインタフェース 1/0/1 の outbound に設定
`interface gigabitethernet 1/0/1`
`  ip access-group AAAAA in`
`  ip access-group BBBBB out`
`ip access-list extended AAAAA`
`  10 permit tcp any any`
`  20 deny udp any any`
`ip access-list extended BBBBB`
`  10 permit udp any any`
`  20 deny tcp any any`
	2 リスト	2 リスト	2 リスト	6 リスト

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 AAAAA を作成して，イーサネットインタフェース 1/0/1 の inbound に設定
アクセスリスト BBBBB を作成して，インタフェースに適用しない
`interface gigabitethernet 1/0/1`
`ip access-group AAAAA in`
 	
`ip access-list extended AAAAA`
`10 permit tcp any any`
`20 deny udp any any`
 	
`ip access-list extended BBBBB`
`10 permit udp any any`
`20 deny tcp any any`
	2 リスト	1 リスト	2 リスト	6 リスト

アクセスリスト AAAAA を作成して，インタフェースに適用しない
`ip access-list extended AAAAA`
`10 permit tcp any any`
	1 リスト	0 リスト	1 リスト	2 リスト

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 および ICMP 以外の場合
  [<seq>] deny {ip | <protocol>} {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが TCP の場合
  [<seq>] deny tcp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [ack] [fin] [psh] [rst] [syn] [urg] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが UDP の場合
  [<seq>] deny udp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが ICMP の場合
  [<seq>] deny icmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

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 4294967284 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 ～ 4294967294（10 進数）を指定します。

{ip | <protocol> | icmp | 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 23-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{<source ipv4> <source ipv4 wildcard> | host <source 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
   <source ipv4> <source ipv4 wildcard>，host <source ipv4> または any を指定します。
   - <source ipv4> <source ipv4 wildcard> 指定：
     <source ipv4> には送信元 IPv4 アドレスを指定します。
     <source 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 <source ipv4> 指定：
     <source 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 <source port> | range <source port start> <source port end>}

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 23-3　TCP で指定可能なポート名称」および「表 23-4　UDP で指定可能なポート名称（IPv4）」を参照してください。
   eq を指定した場合は，<source port> の完全一致をフィルタ条件とします。

   range を指定した場合は，<source port start> から <source port end> の範囲をフィルタ条件とします。
   <source port end> は <source port start> より大きいポート番号を指定してください。

{<destination ipv4> <destination ipv4 wildcard> | host <destination 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
   <destination ipv4> <destination ipv4 wildcard>，host <destination ipv4> または any を指定します。
   - <destination ipv4> <destination ipv4 wildcard> 指定：

<destination ipv4> には宛先 IPv4 アドレスを指定します。
<destination 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 <destination ipv4> 指定：
  <destination 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 <destination port> | range <destination port start> <destination port end>}

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 23-3　TCP で指定可能なポート名称」および「表 23-4　UDP で指定可能なポート名称（IPv4）」を参照してください。
   eq を指定した場合は，<destination port> の完全一致をフィルタ条件とします。
   range を指定した場合は，<destination port start> から <destination port end> の範囲をフィルタ条件とします。
   <destination port end> は <destination port start>> より大きいポート番号を指定してください。

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 23-6　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 23-7　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 23-8　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

<icmp type>

ICMP タイプを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp code>

ICMP コードを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp message>

ICMP メッセージ名称を指定します。

プロトコルが ICMP だけのオプションです。

指定可能な ICMP メッセージ名称は「表 23-11　ICMP で指定可能なメッセージ名称（IPv4）」を参照してください。

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。

class <class> [mask <class mask>]

ユーザクラスとクラスマスクを指定します。

<class mask> には <class> の中で比較対象にするビットを立てたクラスマスクを指定します。

<class mask> を省略した場合は全ビットが比較対象となります。

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 ～ 63（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。
4. <protocol> にプロトコル名称 ah または 51（10 進数）を検出条件としたフィルタ検出はできません。

［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 {<ipv4> [<ipv4 wildcard>] | host <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 4294967284 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 ～ 4294967294（10 進数）を指定します。

{<ipv4> [<ipv4 wildcard>] | host <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
   <ipv4> [<ipv4 wildcard>]，host <ipv4> または any を指定します。
   - <ipv4> [<ipv4 wildcard>] 指定：
     <ipv4> には IPv4 アドレスを指定します。
     [<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 <ipv4> の完全一致をフィルタ条件とします。
   - host <ipv4> 指定：
     <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（ipv6 access-list）

IPv6 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 および ICMP 以外の場合
  [<seq>] deny {ipv6 | <protocol>} {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが TCP の場合
  [<seq>] deny tcp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [ack] [fin] [psh] [rst] [syn] [urg] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが UDP の場合
  [<seq>] deny udp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが ICMP の場合
  [<seq>] deny icmp {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

情報の削除

no <seq>

［入力モード］

(config-ipv6-acl)

［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 4294967284 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 ～ 4294967294（10 進数）を指定します。

{ipv6 | <protocol> | icmp | tcp | udp}

IPv6 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 ipv6 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 ～ 42，45 ～ 49，52 ～ 59，61 ～ 255（10 進数）またはプロトコル名称を指定します。

「表 23-2　指定可能なプロトコル名称（IPv6）」を参照してください。

{<source ipv6>/<length> | host <source ipv6> | any}

送信元 IPv6 アドレスを指定します。

すべての送信元 IPv6 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

<source ipv6>/<length>，host <source ipv6> または any を指定します。

- <source ipv6>/<length> 指定：

  <source ipv6> には送信元 IPv6 アドレスを指定します。

  <length> には IPv6 アドレスの中で一致条件となる部分をアドレスの先頭からの bit 数で指定します。

- host <source ipv6> 指定：

  <source ipv6> の完全一致をフィルタ条件とします。

- any 指定：

  送信元 IPv6 アドレスをフィルタ条件とはしません。

<source ipv6>（nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn）：

0:0:0:0:0:0:0:0 ～ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<length>：0 ～ 128

{eq <source port> | range <source port start> <source port end>}

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 23-3　TCP で指定可能なポート名称」および「表 23-5　UDP で指定可能なポート名称（IPv6）」を参照してください。

eq を指定した場合は，<source port> の完全一致をフィルタ条件とします。

range を指定した場合は，<source port start> から <source port end> の範囲をフィルタ条件とします。

<source port end> は <source port start> より大きいポート番号を指定してください。

{<destination ipv6>/<length> | host <destination ipv6> | any}

宛先 IPv6 アドレスを指定します。

すべての宛先 IPv6 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

<destination ipv6>/<length>，host <destination ipv6> または any を指定します。

- <destination ipv6>/<length> 指定：

  <destination ipv6> には宛先 IPv6 アドレスを指定します。

<length> には IPv6 アドレスの中で一致条件となる部分をアドレスの先頭からの bit 数で指定します。

- host <destination ipv6> 指定：
  <destination ipv6> の完全一致をフィルタ条件とします。
- any 指定：
  宛先 IPv6 アドレスをフィルタ条件とはしません。

<destination ipv6>（nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn）：

0:0:0:0:0:0:0:0 ～ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<length>：0 ～ 128

{eq <destination port> | range <destination port start> <destination port end>}

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 23-3　TCP で指定可能なポート名称」および「表 23-5　UDP で指定可能なポート名称（IPv6）」を参照してください。
   eq を指定した場合は，<destination port> の完全一致をフィルタ条件とします。
   range を指定した場合は，<destination port start> から <destination port end> の範囲をフィルタ条件とします。
   <destination port end> は <destination port start>> より大きいポート番号を指定してください。

traffic-class <traffic class>

本パラメータは，トラフィッククラスフィールド値を指定します。

受信パケットのトラフィッククラスフィールドと比較します。

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 ～ 255（10 進数）を指定します。

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 23-8　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

<icmp type>

ICMP タイプを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp code>

ICMP コードを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp message>

ICMP メッセージ名称を指定します。

プロトコルが ICMP だけのオプションです。

指定可能な ICMP メッセージ名称は「表 23-12　ICMP で指定可能なメッセージ名称（IPv6）」を参照してください。

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。

class <class> [mask <class mask>]

ユーザクラスとクラスマスクを指定します。

<class mask> には <class> の中で比較対象にするビットを立てたクラスマスクを指定します。

<class mask> を省略した場合は全ビットが比較対象となります。

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 ～ 63（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］

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または変更すると，エントリがインタフェースに適用されるまでの間，該当インタフェースで受信したパケットが一時的に廃棄される場合があ

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. 送信元アドレスおよび宛先アドレスに nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/0 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 nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/128 と入力したときは host nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn と表示します。
3. IPv6 アドレスは省略形で表示します。

［関連コマンド］

ipv6 traffic-filter

ipv6 access-list resequence

permit（ipv6 access-list）

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 {<source mac> <source mac mask> | host <source mac> | any} {<destination mac> <destination mac mask> | host <destination mac> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu } [<ethernet type>] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

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 4294967284 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 ～ 4294967294（10 進数）を指定します。

{<source mac> <source mac mask> | host <source 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
   <source mac> <source mac mask>，host <source mac> または any を指定します。
   - <source mac> <source mac mask> 指定：
     <source mac> には送信元 MAC アドレスを指定します。
     <source 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 <source mac> 指定：
     <source 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）

{<destination mac> <destination mac mask> | host <destination 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
   <destination mac> <destination mac mask>，host <destination mac>，any，bpdu，cdp，lacp，lldp，oadp または pvst-plus-bpdu を指定します。
   - <destination mac> <destination mac mask> 指定：
     <destination mac> には宛先 MAC アドレスを指定します。
     <destination 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 <destination mac> 指定：
     <destination 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 23-9　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。

class <class> [mask <class mask>]

ユーザクラスとクラスマスクを指定します。

<class mask> には <class> の中で比較対象にするビットを立てたクラスマスクを指定します。

<class mask> を省略した場合は全ビットが比較対象となります。

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 ～ 63（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 23-10　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。

設定数については，「■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

ip access-group <access list name> {in | out}

情報の削除

no ip access-group <access list name> {in | out}

［入力モード］

(config-if)

［パラメータ］

<access list name>

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
   4～31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 | out}

Inboundまたは Outboundを指定します。

in ：Inbound（受信側の指定）

out：Outbound（送信側の指定）

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. IPv4アクセスリストは同一インタフェースのInboundとOutboundに対して，それぞれ一つ適用できます。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。

2. 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。
3. 受信側フロー検出モードによる設定の可否は，flow detection mode コマンドを参照してください。
4. 送信側フロー検出モードによる設定の可否は，flow detection out mode コマンドを参照してください。
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. フロー検出条件に VLAN パラメータがあるアクセスリストを Outbound に設定する場合は，装置のイーサネットインタフェースに対してトンネリングポートの設定が一つもないときに設定できます。
8. フロー検出条件に VLAN パラメータがあるアクセスリストを Outbound に設定する場合は，該当インタフェースに対して Tag 変換の設定がないときに設定できます。
9. アクセスリストを VLAN インタフェースの Outbound に設定する場合，装置のイーサネットインタフェースに対してトンネリングポートの設定が一つもないときに設定できます。
10. アクセスリストを VLAN インタフェースの Outbound に設定する場合，VLAN インタフェースに含まれているイーサネットインタフェースに設定されている Tag 変換の設定が一つもないときに設定できます。
11. 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，TCP フラグ，ICMP タイプおよび ICMP コード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，受信側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 255 個，送信側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 <access list name>

情報の削除

no ip access-list extended <access list name>

［入力モード］

(config)

［パラメータ］

<access list name>

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
   4 ～ 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，IPv6 アクセスリスト名称，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 <access list name> [<starting sequence> [<increment sequence>]]

［入力モード］

(config)

［パラメータ］

<access list name>

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
   4 ～ 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 sequence>

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 ～ 4294967294（10 進数）を指定します。

<increment sequence>

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，受信側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 255 個，送信側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 <access list name>

情報の削除

no ip access-list standard <access list name>

［入力モード］

(config)

［パラメータ］

<access list name>

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
   4 ～ 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，IPv6 アクセスリスト名称，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

ipv6 access-list

IPv6 フィルタとして動作するアクセスリストを設定します。IPv6 フィルタとして動作するアクセスリストでは，送信元 IPv6 アドレス，宛先 IPv6 アドレス，VLAN ID，ユーザ優先度，トラフィッククラスフィールドの値，ポート番号，TCP フラグ，ICMP タイプ，および ICMP コード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，受信側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 255 個，送信側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

ipv6 access-list <access list name>

情報の削除

no ipv6 access-list <access list name>

［入力モード］

(config)

［パラメータ］

<access list name>

設定する IPv6 フィルタの識別子を指定します。

config-ipv6-acl 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
   4 ～ 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，MAC アクセスリスト名称は指定できません。

［関連コマンド］

ipv6 traffic-filter

ipv6 access-list resequence

deny（ipv6 access-list）

permit（ipv6 access-list）

remark

ipv6 access-list resequence

IPv6 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

ipv6 access-list resequence <access list name> [<starting sequence> [<increment sequence>]]

［入力モード］

(config)

［パラメータ］

<access list name>

設定する IPv6 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
   4 ～ 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 sequence>

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 ～ 4294967294（10 進数）を指定します。

<increment sequence>

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］

ipv6 access-list

ipv6 traffic-filter

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IPv6アクセスリストを適用し，IPv6フィルタ機能を有効にします。

設定数については，「■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

ipv6 traffic-filter <access list name> {in | out}

情報の削除

no ipv6 traffic-filter <access list name> {in | out}

［入力モード］

(config-if)

［パラメータ］

<access list name>

設定するIPv6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
   4～31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 | out}

InboundまたはOutboundを指定します。

in：Inbound（受信側の指定）

out：Outbound（送信側の指定）

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，該当インタフェースで受信したIPv6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. IPv6アクセスリストは同一インタフェースのInboundとOutboundに対して，それぞれ一つ適用できます。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。

2. 実在しない IPv6 フィルタを設定した場合は何も動作しません。IPv6 フィルタの識別子は登録されます。
3. 受信側フロー検出モードによる設定の可否は，flow detection mode コマンドを参照してください。
4. 送信側フロー検出モードによる設定の可否は，flow detection out mode コマンドを参照してください。
5. イーサネットインタフェースに対して IPv6 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 IPv6 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. フロー検出条件に VLAN パラメータがあるアクセスリストを Outbound に設定する場合は，装置のイーサネットインタフェースに対してトンネリングポートの設定が一つもないときに設定できます。
8. フロー検出条件に VLAN パラメータがあるアクセスリストを Outbound に設定する場合は，該当インタフェースに対して Tag 変換の設定がないときに設定できます。
9. アクセスリストを VLAN インタフェースの Outbound に設定する場合，装置のイーサネットインタフェースに対してトンネリングポートの設定が一つもないときに設定できます。
10. アクセスリストを VLAN インタフェースの Outbound に設定する場合，VLAN インタフェースに含まれているイーサネットインタフェースに設定されている Tag 変換の設定が一つもないときに設定できます。
11. 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］

ipv6 access-list

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。

設定数については，「■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

mac access-group <access list name> {in | out}

情報の削除

no mac access-group <access list name> {in | out}

［入力モード］

(config-if)

［パラメータ］

<access list name>

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
   4～31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 | out}

InboundまたはOutboundを指定します。

in ：Inbound（受信側の指定）

out：Outbound（送信側の指定）

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. MACアクセスリストは同一インタフェースのInboundとOutboundに対して，それぞれ一つ適用できます。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。

2. 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。
3. 受信側フロー検出モードによる設定の可否は，flow detection mode コマンドを参照してください。
4. 送信側フロー検出モードによる設定の可否は，flow detection out mode コマンドを参照してください。
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. フロー検出条件に VLAN パラメータがあるアクセスリストを Outbound に設定する場合は，装置のイーサネットインタフェースに対してトンネリングポートの設定が一つもないときに設定できます。
8. フロー検出条件に VLAN パラメータがあるアクセスリストを Outbound に設定する場合は，該当インタフェースに対して Tag 変換の設定がないときに設定できます。
9. アクセスリストを VLAN インタフェースの Outbound に設定する場合，装置のイーサネットインタフェースに対してトンネリングポートの設定が一つもないときに設定できます。
10. アクセスリストを VLAN インタフェースの Outbound に設定する場合，VLAN インタフェースに含まれているイーサネットインタフェースに設定されている Tag 変換の設定が一つもないときに設定できます。
11. 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，受信側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 255 個，送信側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 <access list name>

情報の削除

no mac access-list extended <access list name>

［入力モード］

(config)

［パラメータ］

<access list name>

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
   4 ～ 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，IPv6 アクセスリスト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 <access list name> [<starting sequence> [<increment sequence>]]

[入力モード]

(config)

[パラメータ]

<access list name>

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
   4 ～ 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 sequence>

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 ～ 4294967294（10 進数）を指定します

<increment sequence>

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 および ICMP 以外の場合
  [<seq>] permit {ip | <protocol> } {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが TCP の場合
  [<seq>] permit tcp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [ack] [fin] [psh] [rst] [syn] [urg] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが UDP の場合
  [<seq>] permit udp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが ICMP の場合
  [<seq>] permit icmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

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 4294967284 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 ～ 4294967294（10 進数）を指定します。

{ip | <protocol> | icmp| 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 23-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{<source ipv4> <source ipv4 wildcard> | host <source 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
   <source ipv4> <source ipv4 wildcard>，host <source ipv4> または any を指定します。
   - <source ipv4> <source ipv4 wildcard> 指定：
     <source ipv4> には送信元 IPv4 アドレスを指定します。
     <source 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 <source ipv4> 指定：
     <source 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 <source port> | range <source port start> <source port end>}

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 23-3　TCP で指定可能なポート名称」および「表 23-4　UDP で指定可能なポート名称（IPv4）」を参照してください。
   eq を指定した場合は，<source port> の完全一致をフィルタ条件とします。
   range を指定した場合は，<source port start> から <source port end> の範囲をフィルタ条件とします。
   <source port end> は <source port start> より大きいポート番号を指定してください。

{<destination ipv4> <destination ipv4 wildcard> | host <destination 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
   <destination ipv4> <destination ipv4 wildcard>，host <destination ipv4> または any を指定します。
   - <destination ipv4> <destination ipv4 wildcard> 指定：

<destination ipv4> には宛先 IPv4 アドレスを指定します。
<destination 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 <destination ipv4> 指定：
  <destination 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 <destination port> | range <destination port start> <destination port end>}

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 23-3　TCP で指定可能なポート名称」および「表 23-4　UDP で指定可能なポート名称（IPv4）」を参照してください。
   eq を指定した場合は，<destination port> の完全一致をフィルタ条件とします。
   range を指定した場合は，<destination port start> から <destination port end> の範囲をフィルタ条件とします。
   <destination port end> は <destination port start> より大きいポート番号を指定してください。

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 23-6　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 23-7　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 23-8　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

<icmp type>

ICMP タイプを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp code>

ICMP コードを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp message>

ICMP メッセージ名称を指定します。

プロトコルが ICMP だけのオプションです。

指定可能な ICMP メッセージ名称は「表 23-11　ICMP で指定可能なメッセージ名称（IPv4）」を参照してください。

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。

class <class> [mask <class mask>]

ユーザクラスとクラスマスクを指定します。

<class mask> には <class> の中で比較対象にするビットを立てたクラスマスクを指定します。

<class mask> を省略した場合は全ビットが比較対象となります。

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 ～ 63（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 の同時指定はできません。
4. <protocol> にプロトコル名称 ah または 51（10 進数）を検出条件としたフィルタ検出はできません。

［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］

情報の指定・変更

[<seq>] permit {<ipv4> [<ipv4 wildcard>] | host <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 4294967284 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 ～ 4294967294（10 進数）を指定します。

{<ipv4> [<ipv4 wildcard>] | host <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
   <ipv4> [<ipv4 wildcard>]，host <ipv4> または any を指定します。
   - <ipv4> [<ipv4 wildcard>] 指定：
     <ipv4> には IPv4 アドレスを指定します。
     [<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 <ipv4> の完全一致をフィルタ条件とします。
   - host <ipv4> 指定：
     <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（ipv6 access-list）

IPv6 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 および ICMP 以外の場合
  [<seq>] permit {ipv6 | <protocol>} {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが TCP の場合
  [<seq>] permit tcp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [ack] [fin] [psh] [rst] [syn] [urg] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが UDP の場合
  [<seq>] permit udp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 上位プロトコルが ICMP の場合
  [<seq>] permit icmp {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

情報の削除

no <seq>

［入力モード］

(config-ipv6-acl)

［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 4294967284 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 ～ 4294967294（10 進数）を指定します。

{ipv6 | <protocol> | icmp | tcp | udp}

IPv6 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 ipv6 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 ～ 42，45 ～ 49，52 ～ 59，61 ～ 255（10 進数）またはプロトコル名称を指定します。

「表 23-2　指定可能なプロトコル名称（IPv6）」を参照してください。

{<source ipv6>/<length> | host <source ipv6> | any}

送信元 IPv6 アドレスを指定します。

すべての送信元 IPv6 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

<source ipv6>/<length>，host <source ipv6> または any を指定します。

- <source ipv6>/<length> 指定：

  <source ipv6> には送信元 IPv6 アドレスを指定します。

  <length> には IPv6 アドレスの中で一致条件となる部分をアドレスの先頭からの bit 数で指定します。

- host <source ipv6> 指定：

  <source ipv6> の完全一致をフィルタ条件とします。

- any 指定：

  送信元 IPv6 アドレスをフィルタ条件とはしません。

<source ipv6>（nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn）：

0:0:0:0:0:0:0:0 ～ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<length>：0 ～ 128

{eq <source port> | range <source port start> <source port end>}

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 23-3　TCP で指定可能なポート名称」および「表 23-5　UDP で指定可能なポート名称（IPv6）」を参照してください。

eq を指定した場合は，<source port> の完全一致をフィルタ条件とします。

range を指定した場合は，<source port start> から <source port end> の範囲をフィルタ条件とします。

<source port end> は <source port start> より大きいポート番号を指定してください。

{<destination ipv6>/<length> | host <destination ipv6> | any}

宛先 IPv6 アドレスを指定します。

すべての宛先 IPv6 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

<destination ipv6>/<length>，host <destination ipv6> または any を指定します。

- <destination ipv6>/<length> 指定：

  <destination ipv6> には宛先 IPv6 アドレスを指定します。

<length> には IPv6 アドレスの中で一致条件となる部分をアドレスの先頭からの bit 数で指定します。

- host <destination ipv6> 指定：
  <destination ipv6> の完全一致をフィルタ条件とします。
- any 指定：
  宛先 IPv6 アドレスをフィルタ条件とはしません。

<destination ipv6>（nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn）：

0:0:0:0:0:0:0:0 ～ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<length>：0 ～ 128

{eq <destination port> | range <destination port start> <destination port end>}

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 23-3　TCP で指定可能なポート名称」および「表 23-5　UDP で指定可能なポート名称（IPv6）」を参照してください。
   eq を指定した場合は，<destination port> の完全一致をフィルタ条件とします。
   range を指定した場合は，<destination port start> から <destination port end> の範囲をフィルタ条件とします。
   <destination port end> は <destination port start>> より大きいポート番号を指定してください。

traffic-class <traffic class>

本パラメータは，トラフィッククラスフィールド値を指定します。

受信パケットのトラフィッククラスフィールドと比較します。

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 ～ 255（10 進数）を指定します。

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 23-8　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

<icmp type>

ICMP タイプを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp code>

ICMP コードを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp message>

ICMP メッセージ名称を指定します。

プロトコルが ICMP だけのオプションです。

指定可能な ICMP メッセージ名称は「表 23-12　ICMP で指定可能なメッセージ名称（IPv6）」を参照してください。

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。

class <class> [mask <class mask>]

ユーザクラスとクラスマスクを指定します。

<class mask> には <class> の中で比較対象にするビットを立てたクラスマスクを指定します。

<class mask> を省略した場合は全ビットが比較対象となります。

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 ～ 63（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］

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または変更すると，エントリがインタフェースに適用されるまでの間，該当インタフェースで受信したパケットが一時的に廃棄される場合があ

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. 送信元アドレスおよび宛先アドレスに nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/0 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 nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/128 と入力したときは host nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn と表示します。
3. IPv6 アドレスは省略形で表示します。

［関連コマンド］

ipv6 traffic-filter

ipv6 access-list resequence

deny（ipv6 access-list）

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 {<source mac> <source mac mask> | host <source mac> | any} {<destination mac> <destination mac mask> | host <destination mac> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu } [<ethernet type>] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

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 4294967284 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 ～ 4294967294（10 進数）を指定します。

{<source mac> <source mac mask> | host <source 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
   <source mac> <source mac mask>，host <source mac> または any を指定します。
   - <source mac> <source mac mask> 指定：
     <source mac> には送信元 MAC アドレスを指定します。
     <source 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 <source mac> 指定：
     <source 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）

{<destination mac> <destination mac mask> | host <destination 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
   <destination mac> <destination mac mask>，host <destination mac>，any，bpdu，cdp，lacp，lldp，oadp または pvst-plus-bpdu を指定します。
   - <destination mac> <destination mac mask> 指定：
     <destination mac> には宛先 MAC アドレスを指定します。
     <destination 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 <destination mac> 指定：
     <destination 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 23-9　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。

class <class> [mask <class mask>]

ユーザクラスとクラスマスクを指定します。

<class mask> には <class> の中で比較対象にするビットを立てたクラスマスクを指定します。

<class mask> を省略した場合は全ビットが比較対象となります。

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 ～ 63（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 23-10　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，IPv6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-ipv6-acl)
(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」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］

なし

［関連コマンド］

ip access-list standard

ip access-list extended

ipv6 access-list

mac access-list extended

24 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
ipv6 qos-flow-group
ipv6 qos-flow-list
ipv6 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（ipv6 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 24-1　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

注 ※　プロトコル名称 ah またはプロトコル番号 51 は，フロー検出条件として指定しても検出できません。

■プロトコル名称（IPv6）

IPv6 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 24-2　指定可能なプロトコル名称（IPv6）

プロトコル名称	対象プロトコル番号
gre	47
icmp	58
ipv6	すべての IP プロトコル
ospf	89
pcp	108
pim	103
sctp	132
tcp	6
tunnel	4

プロトコル名称	対象プロトコル番号
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 24-3　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)
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)

ポート名称	対象ポート名および番号
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 24-4　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)
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)

表 24-5　UDP で指定可能なポート名称（IPv6）

ポート名称	対象ポート名および番号
biff	Biff (512)
dhcpv6-client	DHCPv6 client (546)
dhcpv6-server	DHCPv6 server (547)
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)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
ripng	Routing Information Protocol next generation (521)
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 24-6　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 24-7　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
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 24-8　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 24-9　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	
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 24-10　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

■メッセージ名称（ICMP）

ICMP で指定できるメッセージ名称を，次の表に示します。

表 24-11　ICMP で指定可能なメッセージ名称（IPv4）

メッセージ名称	メッセージ名	タイプ	コード
administratively-prohibited	Administratively prohibited	3	13
alternate-address	Alternate address	6	指定なし
conversion-error	Datagram conversion	31	指定なし
dod-host-prohibited	Host prohibited	3	10
dod-net-prohibited	Network prohibited	3	9
echo	Echo (ping)	8	指定なし
echo-reply	Echo reply	0	指定なし
general-parameter-problem	Parameter problem	12	0
host-isolated	Host isolated	3	8
host-precedence-unreachable	Host unreachable for precedence	3	14
host-redirect	Host redirect	5	1
host-tos-redirect	Host redirect for TOS	5	3

メッセージ名称	メッセージ名	タイプ	コード
host-tos-unreachable	Host unreachable for TOS	3	12
host-unknown	Host unknown	3	7
host-unreachable	Host unreachable	3	1
information-reply	Information replies	16	指定なし
information-request	Information requests	15	指定なし
mask-reply	Mask replies	18	指定なし
mask-request	Mask requests	17	指定なし
mobile-redirect	Mobile host redirect	32	指定なし
net-redirect	Network redirect	5	0
net-tos-redirect	Network redirect for TOS	5	2
net-tos-unreachable	Network unreachable for TOS	3	11
net-unreachable	Network unreachable	3	0
network-unknown	Network unknown	3	6
no-room-for-option	Parameter required but no room	12	2
option-missing	Parameter required but not present	12	1
packet-too-big	Fragmentation needed and DF set	3	4
parameter-problem	All parameter problems	12	指定なし
port-unreachable	Port unreachable	3	3
precedence-unreachable	Precedence cutoff	3	15
protocol-unreachable	Protocol unreachable	3	2
reassembly-timeout	Reassembly timeout	11	1
redirect	All redirects	5	指定なし
router-advertisement	Router discovery advertisements	9	指定なし
router-solicitation	Router discovery solicitations	10	指定なし
source-quench	Source quenches	4	指定なし
source-route-failed	Source route failed	3	5
time-exceeded	All time exceeded	11	指定なし
timestamp-reply	Timestamp replies	14	指定なし
timestamp-request	Timestamp requests	13	指定なし
traceroute	Traceroute	30	指定なし
ttl-exceeded	TTL exceeded	11	0
unreachable	All unreachable	3	指定なし

表 24-12　ICMP で指定可能なメッセージ名称（IPv6）

メッセージ名称	メッセージ名	タイプ	コード
beyond-scope	Destination beyond scope	1	2
destination-unreachable	Destination address is unreachable	1	3
echo-reply	Echo reply	129	指定なし
echo-request	Echo request (ping)	128	指定なし
header	Parameter header problems	4	0

メッセージ名称	メッセージ名	タイプ	コード
hop-limit	Hop limit exceeded in transit	3	0
mld-query	Multicast Listener Discovery Query	130	指定なし
mld-reduction	Multicast Listener Discovery Reduction	132	指定なし
mld-report	Multicast Listener Discovery Report	131	指定なし
nd-na	Neighbor discovery neighbor advertisements	136	指定なし
nd-ns	Neighbor discovery neighbor solicitations	135	指定なし
next-header	Parameter next header problems	4	1
no-admin	Administration prohibited destination	1	1
no-route	No route to destination	1	0
packet-too-big	Packet too big	2	指定なし
parameter-option	Parameter option problems	4	2
parameter-problem	All parameter problems	4	指定なし
port-unreachable	Port unreachable	1	4
reassembly-timeout	Reassembly timeout	3	1
renum-command	Router renumbering command	138	0
renum-result	Router renumbering result	138	1
renum-seq-number	Router renumbering sequence number reset	138	255
router-advertisement	Neighbor discovery router advertisements	134	指定なし
router-renumbering	All router renumbering	138	指定なし
router-solicitation	Neighbor discovery router solicitations	133	指定なし
time-exceeded	All time exceeded	3	指定なし
unreachable	All unreachable	1	指定なし

■帯域監視の値の設定範囲

帯域監視の値の設定範囲を，次に示します。

表 24-13　帯域監視の値の設定範囲

設定単位 ※1	設定範囲	刻み値
Gbit/s	1G	1Gbit/s
Mbit/s	1M ～ 10000M	1Mbit/s
kbit/s	1000 ～ 10000000	100kbit/s※2
	64 ～ 960	64kbit/s※3

注 ※1　1G，1M，1k はそれぞれ 1000000000，1000000，1000 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）。

■ 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
- ipv6 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 gigabitethernet/vlan 下の ip qos-flow-group
- interface gigabitethernet/vlan 下の ipv6 qos-flow-group
- interface 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
- ipv6 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（スタック動作時はスタック全体）で IPv4，IPv6，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，IPv6 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（スタック動作時はスタック全体）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 24-14　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 AAAAA を作成して，イーサネットインタフェース 1/0/1 の inbound に設定
`interface gigabitethernet 1/0/1`
`  ip qos-flow-group AAAAA in`
`ip qos-flow-list AAAAA`
`  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 AAAAA を作成して，イーサネットインタフェース 1/0/1 と 1/0/2 の inbound に設定
`interface gigabitethernet 1/0/1`
`  ip qos-flow-group AAAAA in`
`interface gigabitethernet 1/0/2`
`  ip qos-flow-group AAAAA in`
`ip qos-flow-list AAAAA`
`  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 AAAAA を作成して，イーサネットインタフェース 1/0/1 の inbound に設定
QoS フローリスト BBBBB を作成して，イーサネットインタフェース 1/0/2 の inbound に設定
`interface gigabitethernet 1/0/1`
`  ip qos-flow-group AAAAA in`
`interface gigabitethernet 1/0/2`
`  ip qos-flow-group BBBBB in`
`ip qos-flow-list AAAAA`
`  10 qos tcp any any action cos 5`
`  20 qos udp any any action cos 4`
`ip qos-flow-list BBBBB`
`  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

QoS フローリスト AAAAA を作成して，イーサネットインタフェース 1/0/1 の inbound に設定
QoS フローリスト BBBBB を作成して，インタフェースには適用しない
`interface gigabitethernet 1/0/1`
`  ip qos-flow-group AAAAA in`
`ip qos-flow-list AAAAA`
`  10 qos tcp any any action cos 5`
`  20 qos udp any any action cos 4`
`ip qos-flow-list BBBBB`
`  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 AAAAA を作成して，インタフェースに適用しない
`ip qos-flow-list AAAAA`
`  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。

設定数については，「■ 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
　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
   4 ～ 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. IPv4 QoSフローリストは，インタフェースのInboundに一つ適用できます。
2. IPv4 QoSフローリストをInboundに適用する場合，1フローリスト当たりに指定可能なエントリ数は最大128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. 受信側フロー検出モードによる設定の可否は，flow detection mode コマンドを参照してください。
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
   4 ～ 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 IPv6 QoS フローリスト名称および MAC 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 sequence> [<increment sequence>]]

［入力モード］

(config)

［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
   4 ～ 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 sequence>

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 ～ 4294967294（10 進数）を指定します。

<increment sequence>

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

ipv6 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，IPv6QoSフローリストを適用してQoS機能を有効にします。

設定数については，「■ 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
　ipv6 qos-flow-group <qos flow list name> in

情報の削除
　no ipv6 qos-flow-group <qos flow list name> in

［入力モード］

(config-if)

［パラメータ］

<qos flow list name>

IPv6 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
   4～31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. IPv6 QoSフローリストは，インタフェースのInboundに一つ適用できます。
2. IPv6 QoSフローリストをInboundに適用する場合，1フローリスト当たりに指定可能なエントリ数は最大64です。
3. 実在しないIPv6 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。IPv6 QoSフローリスト

名称は登録されます。

4. 受信側フロー検出モードによる設定の可否は，flow detection mode コマンドを参照してください。
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］

ipv6 qos-flow-list

ipv6 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 IPv6 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
　ipv6 qos-flow-list <qos flow list name>

情報の削除
　no ipv6 qos-flow-list <qos flow list name>

［入力モード］

(config)

［パラメータ］

<qos flow list name>

IPv6 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
   4 ～ 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 IPv4 QoS フローリスト名称および MAC QoS フローリスト名称は指定できません。

［関連コマンド］

ipv6 qos-flow-group

ipv6 qos-flow-list resequence

qos（ipv6 qos-flow-list）

remark

ipv6 qos-flow-list resequence

IPv6 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

ipv6 qos-flow-list resequence <qos flow list name> [<starting sequence> [<increment sequence>]]

［入力モード］

(config)

［パラメータ］

<qos flow list name>

変更する IPv6 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
   4 ～ 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 sequence>

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 ～ 4294967294（10 進数）を指定します。

<increment sequence>

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］

ipv6 qos-flow-list

limit-queue-length

物理ポートの最大送信キュー長を設定します。

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。また，スタック動作時は，運用コマンド reload all で全メンバスイッチの一括再起動が必要です。

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，キュー長 64 で動作します。

［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
　　64，128，728 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，64 で動作します。

［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。再起動することで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。また，スタック動作時は，運用コマンド reload all で全メンバスイッチを一括再起動してください。

【スタック動作時】

```
Please execute 'reload all' command after save,
because this command becomes effective after reboot.
```

【スタンドアロン動作時】

```
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 64 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 64 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 8：64
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 2：64
   キュー 3 ～キュー 8：0

［関連コマンド］

qos-queue-list

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。

設定数については，「■ 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

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
   4～31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. MAC QoSフローリストは，インタフェースのInboundに一つ適用できます。
2. MAC QoSフローリストをInboundに適用する場合，1フローリスト当たりに指定可能なエントリ数は最大128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. 受信側フロー検出モードによる設定の可否は，flow detection mode コマンドを参照してください。
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
   4 ～ 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 IPv4 QoS フローリスト名称および IPv6 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 sequence> [<increment sequence>]]

［入力モード］

(config)

［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
   4 ～ 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 sequence>

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 ～ 4294967294（10 進数）を指定します。

<increment sequence>

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 および ICMP 以外の場合

{ip | <protocol> } {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

上位プロトコルが TCP の場合

tcp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [ack] [fin] [psh] [rst] [syn] [urg] [{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

上位プロトコルが UDP の場合

udp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

上位プロトコルが ICMP の場合

icmp{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}[{<icmp type> [<icmp code>] | <icmp message>}][{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

- 動作指定

action [cos <cos>] [replace-user-priority <priority>] [replace-dscp <dscp>]**【スタック動作時】**
action [cos <cos>] [replace-user-priority <priority>] [discard-class <class>] [replace-dscp <dscp>] [max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst {<kbyte> | <Mbyte>M}]] [min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst {<kbyte> | <Mbyte>M}] [penalty-discard-class <class>] [penalty-dscp <dscp>]]**【スタンドアロン動作時】**

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 4294967284 より大きい値を指定した場合は省略できません。
2. 値の設定範囲
   1 ～ 4294967294（10 進数）を指定します。

{ip | <protocol> | icmp | 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 24-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{<source ipv4> <source ipv4 wildcard> | host <source 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
   <source ipv4> <source ipv4 wildcard>，host <source ipv4> または any を指定します。
   - <source ipv4> <source ipv4 wildcard> 指定：
     <source ipv4> には送信元 IPv4 アドレスを指定します。
     <source 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 <source ipv4> 指定：
     <source 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 <source port> | range <source port start> <source port end>}

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 24-3　TCP で指定可能なポート名称」および「表 24-4　UDP で指定可能なポート名称（IPv4）」を参照してください。
   eq を指定した場合は，<source port> の完全一致をフロー検出条件とします。
   range を指定した場合は，<source port start> から <source port end> の範囲をフロー検出条件とします。
   <source port end> は <source port start> より大きいポート番号を指定してください。

{<destination ipv4> <destination ipv4 wildcard> | host <destination 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
   <destination ipv4> <destination ipv4 wildcard>，host <destination ipv4> または any を指定します。
   - <destination ipv4> <destination ipv4 wildcard> 指定：
     <destination ipv4> には宛先 IPv4 アドレスを指定します。
     <destination 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 <destination ipv4> 指定：
     <destination 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 <destination port> | range <destination port start> <destination port end>}

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 24-3　TCP で指定可能なポート名称」および「表 24-4　UDP で指定可能なポート名称（IPv4）」を参照してください。
   eq を指定した場合は，<destination port> の完全一致をフロー検出条件とします。
   range を指定した場合は，<destination port start> から <destination port end> の範囲をフロー検出条件とします。
   <destination port end> は <destination port start> より大きいポート番号を指定してください。

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 24-6　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 24-7　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 24-8　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

<icmp type>

ICMP タイプを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp code>

ICMP コードを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp message>

ICMP メッセージ名称を指定します。

プロトコルが ICMP だけのオプションです。

指定可能な ICMP メッセージ名称は「表 24-11　ICMP で指定可能なメッセージ名称（IPv4）」を参照してください。

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。

class <class> [mask <class mask>]

ユーザクラスとクラスマスクを指定します。

<class mask> には <class> の中で比較対象にするビットを立てたクラスマスクを指定します。

<class mask> を省略した場合は全ビットが比較対象となります。

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 ～ 63（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
   デフォルトコンフィグレーションの CoS 値となります。デフォルトコンフィグレーションの CoS 値については「コンフィグレーションガイド Vol.2 3.10.1 CoS 値・キューイング優先度」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。

discard-class <class>【スタンドアロン動作時】

キューイング優先度を指定します。

受信したパケットのキューイング優先度を指定値 <class> に変更します。

1. 本パラメータ省略時の初期値
   デフォルトコンフィグレーションのキューイング優先度となります。デフォルトコンフィグレーションのキューイング優先度については「コンフィグレーションガイド Vol.2 3.10.1 CoS 値・キューイング優先度」を参照してください。
2. 値の設定範囲
   1 ～ 3（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 24-8　指定可能な DSCP 名称」を参照してください。

max-rate【スタンドアロン動作時】

最大帯域制御を実施します。

送受信するパケットの帯域監視を行い，指定した最大帯域値を超えた違反パケットを廃棄します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}【スタンドアロン動作時】

最大帯域制御での監視帯域値を指定します。min-rate より大きい値を指定してください。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   指定可能な帯域監視値は，「表 24-13　帯域監視の値の設定範囲」を参照してください。

max-rate-burst {<kbyte> | <Mbyte>M}【スタンドアロン動作時】

最大帯域制御でのバーストサイズ（最大帯域を超えて遵守パケットと判定するパケットのバイト数）を設定します。

1. 本パラメータ省略時の初期値
   32
2. 値の設定範囲
   <kbyte>：32，64，128，256，512，1000，2000，4000，8000，16000
   <Mbyte>M：1M，2M，4M，8M，16M

min-rate【スタンドアロン動作時】

最低帯域監視を実施します。

送受信するパケットの帯域監視を実行し，指定した監視帯域値を超えた違反パケットにペナルティを科します。ペナルティは penalty-discard-class，penalty-dscp を用いて指定します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}【スタンドアロン動作時】

最低帯域監視での監視帯域値を指定します。max-rate より小さい値を指定してください。

なお，回線速度以上の帯域を指定すると，違反時の動作はできません。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   指定可能な帯域監視値は，「表 24-13　帯域監視の値の設定範囲」を参照してください。

min-rate-burst {<kbyte> | <Mbyte>M}【スタンドアロン動作時】

最低帯域監視でのバーストサイズ（最低帯域を超えて遵守パケットと判定するパケットのバイト数）

を設定します。

1. 本パラメータ省略時の初期値
   32
2. 値の設定範囲
   <kbyte>：32，64，128，256，512，1000，2000，4000，8000，16000
   <Mbyte>M：1M，2M，4M，8M，16M

penalty-discard-class <class>【スタンドアロン動作時】

最低帯域違反時のキューイング優先度を指定します。
min-rate を使用した最低帯域監視で，違反パケットのキューイング優先度を指定値 <class> に変更します。遵守パケットは discard-class の指定に従います。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   1 ～ 3（10 進数）を指定します。

penalty-dscp <dscp>【スタンドアロン動作時】

最低帯域違反時の DSCP 書き換え値を指定します。
min-rate を使用した最低帯域監視で，違反パケットの DSCP フィールドを，指定値 <dscp> に書き換えます。遵守パケットは replace-dscp の指定に従います。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   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 24-8　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. 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。
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。
5. <protocol> にプロトコル名称 ah または 51（10 進数）を検出条件としたフロー検出はできません。
6. 帯域監視値を Mbit/s 単位（<Mbit/s>M），または Gbit/s 単位（<Gbit/s>G）で設定した場合，運用コマンド show running-config/show startup-config では kbit/s 単位で表示されます。バーストサイズを Mbyte 単位（<Mbyte>M）で設定した場合，運用コマンド show running-config/show startup-config

では kbyte 単位で表示されます。**【スタンドアロン動作時】**

［関連コマンド］

ip qos-flow-list

ip qos-flow-group

ip qos-flow-list resequence

remark

qos（ipv6 qos-flow-list）

IPv6 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 および ICMP 以外の場合

{ipv6 | <protocol>} {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

上位プロトコルが TCP の場合

tcp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [ack] [fin] [psh] [rst] [syn] [urg] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

上位プロトコルが UDP の場合

udp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

上位プロトコルが ICMP の場合

icmp {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

- 動作指定

action [cos <cos>] [replace-user-priority <priority>] [replace-dscp <dscp>]**【スタック動作時】**
action [cos <cos>] [replace-user-priority <priority>] [discard-class <class>] [replace-dscp <dscp>] [max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst {<kbyte> | <Mbyte>M}]] [min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst {<kbyte> | <Mbyte>M}] [penalty-discard-class <class>] [penalty-dscp <dscp>]]**【スタンドアロン動作時】**

情報の削除

no <seq>

［入力モード］

(config-ipv6-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設定します。

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 4294967284 より大きい値を指定した場合は省略できません。

2. 値の設定範囲
   1 ～ 4294967294（10 進数）を指定します。

{ipv6 | <protocol> | icmp | tcp | udp}

IPv6 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 ipv6 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>：
     1 ～ 42，45 ～ 49，52 ～ 59，61 ～ 255（10 進数）またはプロトコル名称を指定します。
     「表 24-2　指定可能なプロトコル名称（IPv6）」を参照してください。

{<source ipv6>/<length> | host <source ipv6> | any}

送信元 IPv6 アドレスを指定します。
すべての送信元 IPv6 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
   <source ipv6>/<length>，host <source ipv6>，または any を指定します。
   - <source ipv6>/<length> 指定：
     <source ipv6> には送信元 IPv6 アドレスを指定します。
     <length> には IPv6 アドレスの中で一致条件となる部分をアドレスの先頭からの bit 数で指定します。
   - host <source ipv6> 指定：
     <source ipv6> の完全一致をフロー検出条件とします。
   - any 指定：
     送信元 IPv6 アドレスをフロー検出条件とはしません。

   <source ipv6>（nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn）：
   0:0:0:0:0:0:0:0 ～ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
   <length>：0 ～ 128

{eq <source port> | range <source port start> <source port end>}

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 24-3　TCP で指定可能なポート名称」および「表 24-5　UDP で指定可能なポート名称（IPv6）」を参照してください。
   eq を指定した場合は <source port> の完全一致をフロー検出条件とします。
   range を指定した場合は <source port start> から <source port end> の範囲をフロー検出条件とします。
   <source port end> は <source port start> より大きいポート番号を指定してください。

{<destination ipv6>/<length> | host <destination ipv6> | any}

宛先 IPv6 アドレスを指定します。
すべての宛先 IPv6 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
   <destination ipv6>/<length>，host <destination ipv6>，または any を指定します。
   - <destination ipv6>/<length> 指定：
     <destination ipv6> には宛先 IPv6 アドレスを指定します。
     <length> には IPv6 アドレスの中で一致条件となる部分をアドレスの先頭からの bit 数で指定します。
   - host <destination ipv6> 指定：
     <destination ipv6> の完全一致をフロー検出条件とします。
   - any 指定：
     宛先 IPv6 アドレスをフロー検出条件とはしません。

   <destination ipv6>（nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn）：

   0:0:0:0:0:0:0:0 ～ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
   <length>：0 ～ 128

{eq <destination port> | range <destination port start> <destination port end>}

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 24-3　TCP で指定可能なポート名称」および「表 24-5 UDP で指定可能なポート名称（IPv6）」を参照してください。
   eq を指定した場合は <destination port> の完全一致をフロー検出条件とします。
   range を指定した場合は <destination port start> から <destination port end> の範囲をフロー検出条件とします。
   <destination port end> は <destination port start> より大きいポート番号を指定してください。

traffic-class <traffic class>

トラフィッククラスフィールド値を指定します。
受信パケットのトラフィッククラスフィールドと比較します。

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 ～ 255（10 進数）を指定します。

dscp <dscp>

トラフィッククラスフィールドの上位 6 ビットである DSCP 値を指定します。
受信パケットのトラフィッククラスフィールド上位 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 24-8　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

<icmp type>

ICMP タイプを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp code>

ICMP コードを指定します。

プロトコルが ICMP 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 ～ 255（10 進数）を指定します。

<icmp message>

ICMP メッセージ名称を指定します。

プロトコルが ICMP だけのオプションです。

指定可能な ICMP メッセージ名称は「表 24-12　ICMP で指定可能なメッセージ名称（IPv6）」を参照してください。

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。

class <class> [mask <class mask>]

ユーザクラスとクラスマスクを指定します。

<class mask> には <class> の中で比較対象にするビットを立てたクラスマスクを指定します。

<class mask> を省略した場合は全ビットが比較対象となります。

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 ～ 63（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
   デフォルトコンフィグレーションの CoS 値となります。デフォルトコンフィグレーションの CoS 値については「コンフィグレーションガイド Vol.2 3.10.1 CoS 値・キューイング優先度」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。

discard-class <class>【スタンドアロン動作時】

キューイング優先度を指定します。

受信したパケットのキューイング優先度を指定値 <class> に変更します。

1. 本パラメータ省略時の初期値
   デフォルトコンフィグレーションのキューイング優先度となります。デフォルトコンフィグレーションのキューイング優先度については「コンフィグレーションガイド Vol.2 3.10.1 CoS 値・キューイング優先度」を参照してください。
2. 値の設定範囲
   1 ～ 3（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 24-8　指定可能な DSCP 名称」を参照してください。

max-rate【スタンドアロン動作時】

最大帯域制御を実施します。

送受信するパケットの帯域監視を行い，指定した最大帯域値を超えた違反パケットを廃棄します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}【スタンドアロン動作時】

最大帯域制御での監視帯域値を指定します。min-rate より大きい値を指定してください。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   指定可能な帯域監視値は，「表 24-13　帯域監視の値の設定範囲」を参照してください。

max-rate-burst {<kbyte> | <Mbyte>M}【スタンドアロン動作時】

最大帯域制御でのバーストサイズ（最大帯域を超えて遵守パケットと判定するパケットのバイト数）を設定します。

1. 本パラメータ省略時の初期値
   32
2. 値の設定範囲
   <kbyte>：32，64，128，256，512，1000，2000，4000，8000，16000
   <Mbyte>M：1M，2M，4M，8M，16M

min-rate【スタンドアロン動作時】

最低帯域監視を実施します。

送受信するパケットの帯域監視を実行し，指定した監視帯域値を超えた違反パケットにペナルティを科します。ペナルティは penalty-discard-class，penalty-dscp を用いて指定します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}【スタンドアロン動作時】

最低帯域監視での監視帯域値を指定します。max-rate より小さい値を指定してください。

なお，回線速度以上の帯域を指定すると，違反時の動作はできません。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   指定可能な帯域監視値は，「表 24-13　帯域監視の値の設定範囲」を参照してください。

min-rate-burst {<kbyte> | <Mbyte>M}【スタンドアロン動作時】

最低帯域監視でのバーストサイズ（最低帯域を超えて遵守パケットと判定するパケットのバイト数）を設定します。

1. 本パラメータ省略時の初期値
   32
2. 値の設定範囲
   <kbyte>：32，64，128，256，512，1000，2000，4000，8000，16000
   <Mbyte>M：1M，2M，4M，8M，16M

penalty-discard-class <class>【スタンドアロン動作時】

最低帯域違反時のキューイング優先度を指定します。

min-rate を使用した最低帯域監視で，違反パケットのキューイング優先度を指定値 <class> に変更します。遵守パケットは discard-class の指定に従います。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   1 ～ 3（10 進数）を指定します。

penalty-dscp <dscp>【スタンドアロン動作時】

最低帯域違反時の DSCP 書き換え値を指定します。

min-rate を使用した最低帯域監視で，違反パケットの DSCP フィールドを，指定値 <dscp> に書き換

えます。遵守パケットは replace-dscp の指定に従います。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   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 24-8　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. 送信元アドレスおよび宛先アドレスに nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/0 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 nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/128 と入力したときは host nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn と表示します。
3. traffic-class 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 を同時に指定した場合，ユーザ優先度は cos の指定値に書き換えられます。
5. 帯域監視値を Mbit/s 単位（<Mbit/s>M），または Gbit/s 単位（<Gbit/s>G）で設定した場合，運用コマンド show running-config/show startup-config では kbit/s 単位で表示されます。バーストサイズを Mbyte 単位（<Mbyte>M）で設定した場合，運用コマンド show running-config/show startup-config では kbyte 単位で表示されます。**【スタンドアロン動作時】**

［関連コマンド］

ipv6 qos-flow-list

ipv6 qos-flow-group

ipv6 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
  {<source mac> <source mac mask> | host <source mac> | any}{<destination mac> <destination mac mask> | host <destination mac> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu }[<ethernet type>] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]
- 動作指定
  action [cos <cos>] [replace-user-priority <priority>]**【スタック動作時】**
  action [cos <cos>] [replace-user-priority <priority>] [discard-class <class>] [max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst {<kbyte> | <Mbyte>M}]] [min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst {<kbyte> | <Mbyte>M}] [penalty-discard-class <class>]]**【スタンドアロン動作時】**

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 4294967284 より大きい値を指定した場合は省略できません。
2. 値の設定範囲
   1 ～ 4294967294（10 進数）を指定します。

{<source mac> <source mac mask> | host <source 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
   <source mac> <source mac mask>，host <source mac> または any を指定します。
   - <source mac> <source mac mask> 指定：
     <source mac> には送信元 MAC アドレスを指定します。
     <source 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 <source mac> 指定：
     <source 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）

{<destination mac> <destination mac mask> | host <destination 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
   <destination mac> <destination mac mask>，host <destination mac>，any，bpdu，cdp，lacp，lldp，oadp または pvst-plus-bpdu を指定します。
   - <destination mac> <destination mac mask> 指定：
     <destination mac> には宛先 MAC アドレスを指定します。
     <destination 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 <destination mac> 指定：
     <destination 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 24-9　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。

class <class> [mask <class mask>]

ユーザクラスとクラスマスクを指定します。

<class mask> には <class> の中で比較対象にするビットを立てたクラスマスクを指定します。

<class mask> を省略した場合は全ビットが比較対象となります。

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 ～ 63（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
   デフォルトコンフィグレーションの CoS 値となります。デフォルトコンフィグレーションの CoS 値については「コンフィグレーションガイド Vol.2 3.10.1 CoS 値・キューイング優先度」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。

discard-class <class>【スタンドアロン動作時】

キューイング優先度を指定します。

受信したパケットのキューイング優先度を指定値 <class> に変更します。

1. 本パラメータ省略時の初期値
   デフォルトコンフィグレーションのキューイング優先度となります。デフォルトコンフィグレーションのキューイング優先度については「コンフィグレーションガイド Vol.2 3.10.1 CoS 値・

キューイング優先度」を参照してください。

2. 値の設定範囲
   1 ～ 3（10 進数）を指定します。

max-rate【スタンドアロン動作時】

最大帯域制御を実施します。
送受信するパケットの帯域監視を行い，指定した最大帯域値を超えた違反パケットを廃棄します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}【スタンドアロン動作時】

最大帯域制御での監視帯域値を指定します。min-rate より大きい値を指定してください。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   指定可能な帯域監視値は，「表 24-13　帯域監視の値の設定範囲」を参照してください。

max-rate-burst {<kbyte> | <Mbyte>M}【スタンドアロン動作時】

最大帯域制御でのバーストサイズ（最大帯域を超えて遵守パケットと判定するパケットのバイト数）を設定します。

1. 本パラメータ省略時の初期値
   32
2. 値の設定範囲
   <kbyte>：32，64，128，256，512，1000，2000，4000，8000，16000
   <Mbyte>M：1M，2M，4M，8M，16M

min-rate【スタンドアロン動作時】

最低帯域監視を実施します。
送受信するパケットの帯域監視を実行し，指定した監視帯域値を超えた違反パケットにペナルティを科します。ペナルティは penalty-discard-class を用いて指定します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}【スタンドアロン動作時】

最低帯域監視での監視帯域値を指定します。max-rate より小さい値を指定してください。
なお，回線速度以上の帯域を指定すると，違反時の動作はできません。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   指定可能な帯域監視値は，「表 24-13　帯域監視の値の設定範囲」を参照してください。

min-rate-burst {<kbyte> | <Mbyte>M}【スタンドアロン動作時】

最低帯域監視でのバーストサイズ（最低帯域を超えて遵守パケットと判定するパケットのバイト数）を設定します。

1. 本パラメータ省略時の初期値
   32
2. 値の設定範囲
   <kbyte>：32，64，128，256，512，1000，2000，4000，8000，16000
   <Mbyte>M：1M，2M，4M，8M，16M

penalty-discard-class <class>【スタンドアロン動作時】

最低帯域違反時のキューイング優先度を指定します。
min-rate を使用した最低帯域監視で，違反パケットのキューイング優先度を指定値 <class> に変更します。遵守パケットは discard-class の指定に従います。

1. 本パラメータ省略時の初期値

なし

2. 値の設定範囲
   1 ～ 3（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 24-10　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。
5. 帯域監視値を Mbit/s 単位（<Mbit/s>M），または Gbit/s 単位（<Gbit/s>G）で設定した場合，運用コマンド show running-config/show startup-config では kbit/s 単位で表示されます。バーストサイズを Mbyte 単位（<Mbyte>M）で設定した場合，運用コマンド show running-config/show startup-config では kbyte 単位で表示されます。**【スタンドアロン動作時】**

［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
   4 ～ 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 キューリスト名を指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 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。全ポート合計で，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
   4 ～ 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，G が指定可能です。
{ <Min rate> | <Min rate>M | <Min rate>G }
<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 24-15　最低保証帯域の設定範囲

設定単位 ※1	設定範囲	刻み値
Gbit/s	1G	1Gbit/s
Mbit/s	1M ～ 10000M	1Mbit/s
kbit/s	1000 ～ 10000000	100kbit/s※2
	64 ～ 960	64kbit/s※3

注 ※1　1G，1M，1k はそれぞれ 1000000000，1000000，1000 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指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），または Gbit/s 単位（<Gbit/s>G）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 IPv6 QoS フローリスト，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-ipv6-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」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］

なし

［関連コマンド］

ip qos-flow-list

ipv6 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 | <Gbit/s>G }

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 | <Gbit/s>G }

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，G 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 24-16　ポート帯域制御の設定範囲

設定単位 ※1	設定範囲	刻み値
Gbit/s	1G	1Gbit/s
Mbit/s	1M ～ 10000M	1Mbit/s
kbit/s	1000 ～ 10000000	100kbit/s※2
	64 ～ 960	64kbit/s※3

注 ※1　1G，1M，1k はそれぞれ 1000000000，1000000，1000 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），または Gbit/s 単位（<Gbit/s>G）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 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

25 レイヤ 2 認証共通

authentication arp-relay
authentication auto-logout strayer
authentication force-authorized enable
authentication force-authorized vlan
authentication ip access-group
authentication logout linkdown
authentication max-user（global）
authentication max-user（interface）

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。

[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

[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 auto-logout strayer

Web 認証 /MAC 認証の認証済み端末が，Web 認証 /MAC 認証未設定ポートに移動したことを検出したときに，認証を解除します。

［入力形式］

情報の設定
　authentication auto-logout strayer

情報の削除
　no authentication auto-logout strayer

［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 /MAC 認証の認証済み端末が，Web 認証 /MAC 認証未設定ポートへ移動したことを検出しても，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. IEEE802.1X は本コマンドの対象外です。
2. Web 認証中（RADIUS 認証待ち状態など）に移動した端末は，認証完了後，移動を再検出したときに認証を解除します。
3. MAC 認証中（RADIUS 認証待ち状態など）または保留中に移動した場合は，認証を中止します。
4. 移動に伴って端末の VLAN が変わる場合は，移動を検出しない可能性があります。その場合，認証は解除されませんが，移動後の通信には影響しません。

［関連コマンド］

なし

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. 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。
4. 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。
5. 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。

［関連コマンド］

aaa authentication dot1x

aaa authentication mac-authentication

aaa authentication web-authentication

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. 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。
4. 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。

［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。

［入力形式］

情報の設定

authentication ip access-group <access list name>

情報の削除

no authentication ip access-group

［入力モード］

(config-if)

［パラメータ］

<access list name>

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。

1. 本パラ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 ～ 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

［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

authentication logout linkdown

no authentication logout linkdown 設定時，認証済み端末の所属ポートがリンクダウンしても認証解除しません。

［入力形式］

情報の設定
　no authentication logout linkdown

情報の削除
　authentication logout linkdown

［入力モード］

(config-if)

［パラメータ］

なし

［コマンド省略時の動作］

認証済み端末の所属ポートがリンクダウンすると認証を解除します。

［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］

dot1x port-control

dot1x system-auth-control

mac-authentication port

mac-authentication system-auth-control

shutdown

web-authentication port

web-authentication system-auth-control

authentication max-user（global）

IEEE802.1X 認証，Web 認証および MAC 認証を合わせた最大認証端末数（全ポート合計）を設定します。

［入力形式］

情報の設定・変更
　authentication max-user <count>

情報の削除
　no authentication max-user

［入力モード］

(config)

［パラメータ］

<count>

IEEE802.1X 認証，Web 認証および MAC 認証を合わせた最大認証端末数（全ポート合計）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
   【スタック動作時】1 ～ 2048
   【スタンドアロン動作時】1 ～ 1024

［コマンド省略時の動作］

【スタック動作時】認証可能な最大認証端末数は，全ポート合計で 2048 端末となります。

【スタンドアロン動作時】認証可能な最大認証端末数は，全ポート合計で 1024 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. 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。また，再認証やローミングでも認証が解除される場合があります。
2. 全ポート合計とポート単位の最大認証端末数を同時に設定できます。
   - 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，該当ポートで，以降の新規端末の認証はできません。
   - 認証済み端末数が最大認証端末数（全ポート合計）に達した場合，以降の新規端末の認証はできません。
   - Web 認証のダイナミック VLAN モード，MAC 認証のダイナミック VLAN モードおよびこれらと同時に設定してある IEEE802.1X のポート単位認証（動的）による該当ポートの最大認証数は，MAC VLAN の制限で 1000 端末が上限です。

［関連コマンド］

dot1x system-auth-control

mac-authentication system-auth-control

web-authentication system-auth-control

authentication max-user（interface）

IEEE802.1X 認証，Web 認証および MAC 認証を合わせた該当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
　authentication max-user <count>

情報の削除
　no authentication max-user

［入力モード］

(config-if)

［パラメータ］

<count>

IEEE802.1X 認証，Web 認証および MAC 認証を合わせた該当ポートの最大認証端末数を指定します。

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
   【スタック動作時】1 ～ 2048
   【スタンドアロン動作時】1 ～ 1024

［コマンド省略時の動作］

【スタック動作時】ポート単位の認証可能な最大認証端末数は，2048 端末となります。

【スタンドアロン動作時】ポート単位の認証可能な最大認証端末数は，1024 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. 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。また，再認証やローミングでも認証が解除される場合があります。
2. 全ポート合計とポート単位の最大認証端末数を同時に設定できます。
   - 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，該当ポートで，以降の新規端末の認証はできません。
   - 認証済み端末数が最大認証端末数（全ポート合計）に達した場合，以降の新規端末の認証はできません。
3. Web 認証のダイナミック VLAN モード，MAC 認証のダイナミック VLAN モードおよびこれらと同時に設定してある IEEE802.1X のポート単位認証（動的）による該当ポートの最大認証数は，MAC VLAN の制限で 1000 端末が上限です。

［関連コマンド］

dot1x port-control

mac-authentication port

web-authentication port

26 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
dot1x authentication
dot1x auto-logout
dot1x force-authorized eapol
dot1x ignore-eapol-start
dot1x logging enable
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

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 26-1　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	
	（静的）	（動的）
aaa accounting dot1x	○	○
aaa authentication dot1x	○	○
authentication arp-relay※1	○	○
authentication ip access-group※1	○	○
dot1x authentication	○	○
dot1x auto-logout	○	○
dot1x force-authorized eapol	○	○
dot1x ignore-eapol-start	○	○
dot1x logging enable	○	○
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	○	○

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，「25　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，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。

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。

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

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。

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

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。

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

［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 26-1　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。

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

<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 26-1　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 group server radius

dot1x authentication

dot1x system-auth-control

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 26-1　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. web-authentication user-group コマンドが設定されている場合は，本コマンドを設定できません。
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。

［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 26-1　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 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 26-1　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，authentication force-authorized enable 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。

［関連コマンド］

authentication force-authorized enable

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 26-1　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 passive，および 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 passive，または 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 logging enable

IEEE802.1X 認証の動作ログに出力する情報を syslog サーバに出力します。

[入力形式]

情報の設定
　dot1x logging enable

情報の削除
　no dot1x logging enable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

syslog サーバに動作ログを出力しません。

[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. 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 26-1　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 system-auth-control

logging event-kind

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 26-1　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 26-1　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］

system receive control fine 設定時に IEEE802.1X を有効にした場合，MAC アドレステーブルのダイナミックエントリ (当該ポート，または当該チャネルグループ) がクリアされ，一時的なフラッディングが発生します。

［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 26-1　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）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。
   - dot1x port-control auto
   - switchport mode access
   - switchport access
4. ポート単位認証（動的）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。
   - 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，監視タイマ 10 分（デフォルトコンフィグレーション）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 26-1　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 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 {<ipv4 address> | <ipv6 address>} [auth-port <port>] [acct-port <port>] [timeout <seconds>] [retransmit <retries>] [key <string>]

情報の削除

no dot1x radius-server host {<ipv4 address> | <ipv6 address>}

［入力モード］

(config)

［パラメータ］

{<ipv4 address> | <ipv6 address>}

<ipv4 address>

RADIUS サーバの IPv4 アドレスをドット記法で指定します。

<ipv6 address>

RADIUS サーバの IPv6 アドレスをコロン記法で指定します。

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
   <ipv4 address>：IPv4 ユニキャストアドレス
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   <ipv6 address>：IPv6 グローバルユニキャストアドレス
   ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff，fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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 26-1　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 26-1　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 {passive | disable | shortcut | auto}

情報の削除

no dot1x supplicant-detection

［入力モード］

(config-if)

［パラメータ］

{passive | 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。

passive

当該ポートの検出済み端末の存在有無に関係なく，EAP-Request/Identity をマルチキャスト送信しません。

このため，本パラメータを指定した場合，端末側から自発的に EAPOL-Start を送信しない Supplicant ソフトウェアを使用する場合，認証を開始できません。

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
   passive，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 26-1　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 コマンドを指定したインタフェースで dot1x supplicant-detection コマンドの passive，または disable を設定することはできません。
6. system receive control fine 設定時，本コマンドを auto 設定以外（または未設定）から auto 設定に変更した場合，その時点で当該端末の MAC アドレスが MAC アドレステーブルに登録済の場合は認証契機を検出しません。その場合は，運用コマンド clear mac-address-table により，装置全体，当該端末が接続されているポート，または当該端末の MAC アドレスのいずれかを指定して MAC アドレステーブルから消去してください。

［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 26-1　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 26-1　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 26-1　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 26-1　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 26-1　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 26-1　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 26-1　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

27 Web 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 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 html-fileset
web-authentication ip address
web-authentication jump-url
web-authentication logging enable
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 port
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 polling
web-authentication redirect queries
web-authentication redirect target
web-authentication roaming
web-authentication static-vlan roaming
web-authentication system-auth-control
web-authentication user-group
web-authentication user replacement
web-authentication web-port

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 27-1　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	
	固定 VLAN モード	ダイナミック VLAN モード
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 html-fileset	○	○
web-authentication ip address	○	○
web-authentication jump-url	○	○
web-authentication logging enable	○	○
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 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 polling	○	○
web-authentication redirect queries	○	○
web-authentication redirect target	○	○
web-authentication roaming	－	○
web-authentication static-vlan roaming	○	－
web-authentication system-auth-control	○	○

コマンド名	Web 認証の認証モード ※3	
	固定 VLAN モード	ダイナミック VLAN モード
web-authentication user-group	○	○
web-authentication user replacement	○	○
web-authentication web-port	○	○

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，「25　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。

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

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。

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

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。

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

［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 27-1　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。

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

<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 27-1　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 27-1　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/HTTPS リクエストは初期タイムアウト 36 秒，他の HTTP/HTTPS リクエストは初期タイムアウト 8 秒で動作します。

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
   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 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 27-1　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. web-authentication user-group コマンドが設定されている場合は，本コマンドを設定できません。
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。

［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 27-1　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

mac-address-table aging-time

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 27-1　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。

[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 27-1　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。
4. 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。
5. 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

ログイン成功画面表示後，自動的に表示する URL と URL 移動までの時間を指定します。

［入力形式］

情報の設定・変更

web-authentication jump-url { <url> | original } [delay <seconds>]

情報の削除

no web-authentication jump-url

［入力モード］

(config)

［パラメータ］

{ <url> | original }

<url>

ログイン成功画面表示後，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。）

original

URL リダイレクトで認証を開始した場合は，ログイン成功画面表示後，リダイレクト前の URL 画面を表示します。

Web 認証専用 IP アドレスまたは本装置の IP アドレスをダイレクトに指定して認証を開始した場合は，認証成功後にログイン成功画面を表示するだけとなります。

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
   <url> には，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。
   （URL を指定した場合の設定例）
   (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］

認証成功後の表示画面は，ログイン成功画面を表示するだけとなります。

［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 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 27-1　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 でログイン成功画面を入れ替える際，入れ替えるログイン成功画面ファイル（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. パスワード入力ミスなどによってログイン失敗画面が表示され，「login page」ボタンをクリックしログイン画面に戻った場合は，original が無効となり，認証成功後にログイン成功画面が表示されたままとなります。
5. 外部 Web サーバへのリダイレクト機能を使用する場合は，外部 Web サーバに依存します。詳細については，「コンフィグレーションガイド Vol.2 8 Web 認証の解説」を参照してください。
6. original 指定時，リダイレクト前の URL の文字数や文字コードの制限については，「コンフィグレーションガイド Vol.2 8 Web 認証の解説」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 logging enable

Web 認証の動作ログに出力する情報を syslog サーバへ出力します。

［入力形式］

情報の設定
　web-authentication logging enable

情報の削除
　no web-authentication logging enable

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

syslog サーバへ動作ログを出力しません。

［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. 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 27-1　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

logging event-kind

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 27-1　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 27-1　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 27-1　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コンフィグレーションでの使用を推奨します。
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 27-1　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コンフィグレーションでの使用を推奨します。
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 27-1　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コンフィグレーションでの使用を推奨します。
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 27-1　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コンフィグレーションでの使用を推奨します。
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 27-1　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 auto-logout

web-authentication port

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]

当該ポートで Web 認証は動作しません。

[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]

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 27-1　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 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］

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。

［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，監視タイマ 10 分（デフォルトコンフィグレーション）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 27-1　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 {<ipv4 address> | <ipv6 address>} [auth-port <port>] [acct-port <port>] [timeout <seconds>] [retransmit <retries>] [key <string>]

情報の削除

no web-authentication radius-server host {<ipv4 address> | <ipv6 address>}

［入力モード］

(config)

［パラメータ］

{<ipv4 address> | <ipv6 address>}

<ipv4 address>

RADIUS サーバの IPv4 アドレスをドット記法で指定します。

<ipv6 address>

RADIUS サーバの IPv6 アドレスをコロン記法で指定します。

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
   <ipv4 address>：IPv4 ユニキャストアドレス
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   <ipv6 address>：IPv6 グローバルユニキャストアドレス
   ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff，fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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 27-1　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 27-1　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 27-1　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 polling

外部 Web サーバの生死監視を実施し，障害時には本装置の Web サーバにリダイレクトします。

［入力形式］

情報の設定

web-authentication redirect polling tcp [interval <seconds>] [dead-count <count>] [alive-count <count>]

情報の削除

no web-authentication redirect polling

［入力モード］

(config)

［パラメータ］

tcp

tcp パケットで監視します。

1. 本パラメータ省略時の初期値
   省略できません。

interval <seconds>

監視間隔時間を設定します。

1. 本パラメータ省略時の初期値
   60（秒）
2. 値の設定範囲
   10 ～ 3600（秒）

dead-count <count>

「無応答」を検出したときに，障害と判断する回数を設定します。

1. 本パラメータ省略時の初期値
   1（回）
2. 値の設定範囲
   1 ～ 5（回）

alive-count <count>

「応答」を検出したときに，正常と判断する回数を設定します。

1. 本パラメータ省略時の初期値
   1（回）
2. 値の設定範囲
   1 ～ 5（回）

［コマンド省略時の動作］

外部サーバにリダイレクトします。

［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 27-1　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。
4. DNS 解決できない場合，監視失敗となります。
5. プロキシ経由の監視は未サポートです。

［関連コマンド］

web-authentication system-auth-control

web-authentication port

authentication ip access-group

authentication arp-relay

web-authentication redirect enable

web-authentication redirect queries

web-authentication redirect target

web-authentication redirect queries

本装置や認証端末に関するパラメータをリダイレクト先（外部 Web サーバ）の URL にクエリとして付加します。

［入力形式］

情報の設定

web-authentication redirect queries [switch-hostname] [switch-mac] [switch-ip] [client-mac] [client-vlan] [client-ip] [port] [original-url]

情報の削除

no web-authentication redirect queries

［入力モード］

(config)

［パラメータ］

[switch-hostname] [switch-mac] [switch-ip] [client-mac] [client-vlan] [client-ip] [port] [original-url]

各パラメータを設定することによって，付加するクエリを選択します。本コマンド入力時，すべての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。

switch-hostname

本装置のホスト名（hostname コマンド）を付加します。

switch-mac

本装置のシステム MAC アドレスを付加します。

switch-ip

本装置の実 IP アドレスを付加します。

client-mac

認証端末の MAC アドレスを付加します。

client-vlan

認証端末の VLAN 番号を付加します。

client-ip

認証端末の IP アドレスを付加します。

port

認証端末が接続されているポートを付加します。

original-url

リダイレクト前の URL を付加します。

1. 本パラメータ省略時の初期値
   指定しないパラメータのクエリは付加しません。
2. 値の設定範囲
   switch-hostname，switch-mac，switch-ip，client-mac，client-vlan，client-ip，port，original-url

［コマンド省略時の動作］

外部 Web サーバへリダイレクトするとき，URL にクエリを付加しません。

［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 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 27-1　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。
4. original-url 指定時，リダイレクト前の URL の文字数や文字コードの制限については，「コンフィグレーションガイド Vol.2 8 Web 認証の解説」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 enable

web-authentication redirect polling

web-authentication redirect target

web-authentication redirect target

URL リダイレクト機能におけるリダイレクト先を，指定された外部 Web サーバに変更します。

［入力形式］

情報の設定
　web-authentication redirect target <url>

情報の削除
　no web-authentication redirect target

［入力モード］

(config)

［パラメータ］

<url>

外部 Web サーバのリダイレクト先 URL を指定します。
URL の入力は先頭文字（例えば，"http:// ～ "）から指定してください。（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」を参照してください。
   以下の書式に従って入力してください。
   書式："<scheme>://<host>[:<port>][/<path>][?<query>]"
   <scheme> ："http" もしくは "https" を小文字で入力してください。
   <host>：「パラメータに指定できる値」の「ホスト名」または「IPv4 アドレス」を設定してください。
   <port>：1 ～ 65535 までの数字が設定できます。省略可能です。
   <path>：「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，セミコロン (;)，クエスチョン (?) を除く）。省略可能です。
   <query>：「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，スラッシュ (/)，セミコロン (;)，クエスチョン (?) を除く）。省略可能です。
   （設定例）
   (config)# web-authentication redirect target "http://www.example.com:80/login.html?value=3"

［コマンド省略時の動作］

本装置の Web サーバにリダイレクトします。

［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 27-1　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。
4. パスワード入力ミスなどによってログイン失敗画面が表示され，そこで login page ボタンをクリックした場合は，本装置の内蔵 Web サーバのログイン画面が表示されます。

［関連コマンド］

web-authentication system-auth-control

web-authentication port

authentication ip access-group

authentication arp-relay

web-authentication redirect enable

web-authentication redirect polling

web-authentication redirect queries

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 27-1　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 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 27-1　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 27-1　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 27-1　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
   - mac-authentication authentication
   - web-authentication authentication
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 27-1　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 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 27-1　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。

［関連コマンド］

authentication ip access-group

authentication arp-relay

web-authentication port

web-authentication system-auth-control

28 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 id-format
mac-authentication logging enable
mac-authentication max-timer
mac-authentication password
mac-authentication port
mac-authentication radius-server dead-interval
mac-authentication radius-server host
mac-authentication roaming
mac-authentication static-vlan roaming
mac-authentication system-auth-control
mac-authentication timeout quiet-period
mac-authentication timeout reauth-period
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 28-1　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	
	固定 VLAN モ モード	ダイナミック VLAN モ モード
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 id-format	○	○
mac-authentication logging enable	○	○
mac-authentication max-timer	○	○
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 roaming	○	－
mac-authentication system-auth-control	○	○
mac-authentication timeout quiet-period	○	○
mac-authentication timeout reauth-period	○	○
mac-authentication vlan-check	○	－

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，「25　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。

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

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。

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

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。

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

［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 28-1　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。

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

<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 28-1　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 28-1　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 <access list name>

情報の削除

no mac-authentication access-group

［入力モード］

(config)

［パラメータ］

<access list name>

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
   4 ～ 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 28-1　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。
5. system receive control fine 設定時，本コマンド，または本コマンドから参照しているアクセスリストの変更によって，MAC 認証対象外の端末が MAC 認証対象に変化したとき，当該端末の MAC アドレスが MAC アドレステーブルに登録済の場合は MAC 認証が開始されません。
   その場合は，運用コマンド clear mac-address-table により，装置全体，当該端末が接続されているポート，または当該端末の MAC アドレスのいずれかを指定して MAC アドレステーブルから消去して

ください。

［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 28-1　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. web-authentication user-group コマンドが設定されている場合は，本コマンドを設定できません。
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。

[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。

［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>

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 3600 秒（デフォルトコンフィグレーション）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（秒）

［コマンド省略時の動作］

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。

［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 28-1　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 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 28-1　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 logging enable

MAC 認証の動作ログに出力する情報を syslog サーバへ出力します。

［入力形式］

情報の設定
　mac-authentication logging enable

情報の削除
　no mac-authentication logging enable

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

syslog サーバへ動作ログを出力しません。

［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］

なし

［関連コマンド］

mac-authentication system-auth-control

logging event-kind

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 28-1　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 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 28-1　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]

当該ポートで MAC 認証は動作しません。

[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。
- system receive control fine 設定時に本コマンドを設定した場合，MAC アドレステーブルのダイナミックエントリ (当該ポート，または当該チャネルグループ) がクリアされ，一時的なフラッディングが発生します。

[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 28-1　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

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，監視タイマ 10 分（デフォルトコンフィグレーション）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 28-1　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 {<ipv4 address> | <ipv6 address>} [auth-port <port>] [acct-port <port>] [timeout <seconds>] [retransmit <retries>] [key <string>]

情報の削除

no mac-authentication radius-server host {<ipv4 address> | <ipv6 address>}

［入力モード］

(config)

［パラメータ］

{<ipv4 address> | <ipv6 address>}

<ipv4 address>

RADIUS サーバの IPv4 アドレスをドット記法で指定します。

<ipv6 address>

RADIUS サーバの IPv6 アドレスをコロン記法で指定します。

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
   <ipv4 address> : IPv4 ユニキャストアドレス
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   <ipv6 address> : IPv6 グローバルユニキャストアドレス
   ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff，fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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 28-1　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 28-1　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 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 28-1　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。
- system receive control fine 設定時に本コマンドを設定した場合，MAC アドレステーブルのダイナミックエントリ (全ポート，全チャネルグループ) がクリアされ，一時的なフラッディングが発生します。

［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 28-1　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 28-1　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。
4. スタック動作時，認証保留中の端末はポート移動しても検知しません。認証再開猶予タイマがタイムアウトするまで待つか，または運用コマンド clear mac-authentication auth-state を実行し，認証を中止してください。

［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28-1　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-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28-1　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

29 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 認証を許可します。1 段目の MAC 認証または IEEE802.1X 認証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 認証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］

なし

［関連コマンド］

なし

30 DHCP snooping

ip arp inspection limit rate
ip arp inspection trust
ip arp inspection validate
ip arp inspection vlan
ip dhcp snooping
ip dhcp snooping database url
ip dhcp snooping database write-delay
ip dhcp snooping information no-check
ip dhcp snooping information option allow-untrusted
ip dhcp snooping information option format remote-id
ip dhcp snooping information option-insert
ip dhcp snooping limit rate
ip dhcp snooping trust
ip dhcp snooping verify mac-address
ip dhcp snooping vlan
ip dhcp snooping vlan information option format-type circuit-id
ip source binding
ip verify source

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]

なし

[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 no-check

DHCP Reply パケットからリレーエージェント情報オプション（DHCP Option82）を削除する際に，DHCP Option82 をチェックせずに転送します。

［入力形式］

情報の設定
　ip dhcp snooping information no-check

情報の削除
　no ip dhcp snooping information no-check

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

DHCP Option82 が無効である DHCP Reply パケットは廃棄します。

［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 dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping information option-insert

ip dhcp snooping information option allow-untrusted

信頼されていないポート（untrust ポート）でリレーエージェント情報オプション [Option 82] を持った DHCP パケットの受信を許可します。

［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］

リレーエージェント情報オプションを持った DHCP パケットを廃棄します。

［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 dhcp snooping

ip dhcp snooping information option format remote-id

DHCP Option82 サブオプションのリモート ID を設定します。

[入力形式]

情報の設定・変更

ip dhcp snooping information option format remote-id str <string>

情報の削除

no ip dhcp snooping information option format remote-id

[入力モード]

(config)

[パラメータ]

str <string>

リモート ID の値を設定します。

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
   63 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]

リモート ID に装置 MAC アドレスを設定します。

[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]

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping information option-insert

ip dhcp snooping information option-insert

リレーエージェント情報オプション（DHCP Option82）の付加を有効にします。

［入力形式］

情報の設定
　ip dhcp snooping information option-insert

情報の削除
　no ip dhcp snooping information option-insert

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

DHCP Option82 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］

なし

［関連コマンド］

ip dhcp snooping

ip dhcp snooping vlan

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］

1. 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「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。

［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］

1. 本コマンドを設定しない VLAN では，DHCP snooping は無効です。
2. 設定済の VLAN ID と異なる VLAN ID を指定したときは追加となります。

［関連コマンド］

ip dhcp snooping

ip dhcp snooping vlan information option format-type circuit-id

DHCP Option82 サブオプションのサーキット ID を設定します。

［入力形式］

情報の設定・変更

ip dhcp snooping vlan <vlan id > information option format-type circuit-id {type <circuit-id-type> | str <circuit-id-string>}

情報の削除

no ip dhcp snooping vlan <vlan id> information option format-type circuit-id

［入力モード］

(config-if)

［パラメータ］

<vlan id>

VLAN ID 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
   「パラメータに指定できる値」を参照してください。

{type <circuit-id-type> | str <circuit-id-string>}

サーキット ID をタイプまたは文字列で設定します。

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
   <circuit-id-type>：0，または 2 を設定してください。
   <circuit-id-string>：63 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］

circuit-id-type 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］

1. 本コマンドは，ポート毎に入力可能です。
   スタンドアロン動作時は最大 64 件，スタック動作時は最大 8 件です。
2. 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。

［関連コマンド］

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping information option-insert

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 <switch no.>/<IF#> | port-channel <channel group>}【スタック動作時】

ip source binding <mac> vlan <vlan id> <ip address> interface {gigabitethernet <IF#> | port-channel <channel group>}【スタンドアロン動作時】

情報の削除

no ip source binding <mac> vlan <vlan id> <ip address> interface {gigabitethernet <switch no.>/<IF#> | port-channel <channel group>}【スタック動作時】

no ip source binding <mac> vlan <vlan id> <ip address> interface {gigabitethernet <IF#> | port-channel <channel group>}【スタンドアロン動作時】

［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 <switch no.>/<IF#> | port-channel <channel group>}【スタック動作時】

interface { gigabitethernet <IF#> | port-channel <channel group> }【スタンドアロン動作時】

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
   <switch no.>，<IF#> および <channel group> 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 128 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。
3. 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。

［関連コマンド］

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping trust

ip source binding

31 ホワイトリスト機能【OP-WL】

white-list action discard【OP-WL】

white-list action log【OP-WL】

white-list action monitor【OP-WL】

white-list address permit【OP-WL】

white-list address trust【OP-WL】

white-list data【OP-WL】

white-list enable【OP-WL】

white-list learning【OP-WL】

white-list logging filter【OP-WL】

white-list logging format-add【OP-WL】

white-list monitor destination interface【OP-WL】

white-list packet mode【OP-WL】

white-list packet tcp【OP-WL】

white-list packet trust-mode【OP-WL】

white-list packet udp【OP-WL】

white-list trust【OP-WL】

white-list action discard【OP-WL】

ホワイトリスト運用状態で，当該ポートで受信したホワイトリスト未学習パケットを廃棄します。

［入力形式］

情報の設定
　white-list action discard

情報の削除
　no white-list action discard

［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］

当該ポートで受信する未学習パケットを廃棄します。

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. 本コマンドを設定したポートがチャネルグループに属している場合は，同じチャネルグループの全ポートに本コマンドを設定してください。
3. ホワイトリスト学習状態では，本コマンドは無効です。
4. ホワイトリスト機能とフィルタ機能の併用時の動作については，「コンフィグレーションガイド Vol.2 14　ホワイトリスト機能」を参照してください。

［関連コマンド］

white-list enable

white-list action log【OP-WL】

ホワイトリスト運用状態で，当該ポートで受信したホワイトリスト未学習パケットのパケット情報をsyslogサーバへ出力します。

syslogサーバ送信先は，logging hostコマンドで設定してください。また，syslogサーバにホワイトリスト情報だけを出力する場合は，logging event-kindコマンドで設定してください。

［入力形式］

情報の設定
　white-list action log

情報の削除
　no white-list action log

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. ホワイトリスト学習状態では，本コマンドは無効です。

［関連コマンド］

logging event-kind

logging host

white-list enable

white-list action monitor【OP-WL】

ホワイトリストのミラーリング機能を有効化します。

本コマンドは，ホワイトリスト運用状態で，当該ポートで受信したホワイトリスト未学習パケットをミラーリング対象に設定します。

ホワイトリストのミラーリング出力先ポートは，white-list monitor destination interface コマンドで指定してください。

［入力形式］

情報の設定
　white-list action monitor

情報の削除
　no white-list action monitor

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. ホワイトリスト学習状態では，本コマンドは無効です。
3. white-list monitor destination interface コマンドが未設定の場合は，本コマンドは無効です。

［関連コマンド］

white-list enable

white-list monitor destination interface

white-list address permit【OP-WL】

指定機能の制御フレームを，ホワイトアドレスリスト対象外にします。

［入力形式］

情報の設定
　white-list address permit loop-detection

情報の削除
　no white-list address permit loop-detection

［入力モード］

(config)

［パラメータ］

loop-detection

L2 ループ検知の制御フレームを，ホワイトアドレスリスト対象外にします。

1. 本パラ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-detection

［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］

white-list enable

white-list address trust【OP-WL】

ホワイトアドレスリスト機能を無効に設定します。

［入力形式］

情報の設定
　white-list address trust

情報の削除
　no white-list address trust

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

ホワイトアドレスリスト機能は有効です。

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. 本コマンド削除時，MAC アドレステーブルのダイナミックエントリはすべて削除されます。

［関連コマンド］

white-list enable

white-list data【OP-WL】

ホワイトリスト機能で学習したリストをコンフィグレーションとして保持するためのコマンドです。

本コマンドはホワイトリスト機能の学習状態で自動的に設定されます。本コマンドは手動設定を想定したものではありませんが，手動による設定変更も可能です。本コマンドの使用については，「コンフィグレーションガイド Vol.2 14 ホワイトリスト機能」を参照してください。

［入力形式］

情報の設定・変更
　white-list data <list entry>

情報の削除
　no white-list data <list entry>

［入力モード］

(config)

［パラメータ］

<list entry>

追加または削除するホワイトリストエントリを，ダブルクォート（"）で囲んだ文字列で設定します。

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
   文字列の範囲は最大 255 文字です。

＜指定可能な文字列の形式＞

① ホワイトアドレスリスト

```
"a <mac> v <vlan id> {p <IF#> | c <channel group>}"
```

② ホワイトパケットリスト：IPv4 の場合（white-list packet mode 1：受信パケット種別モード）

```
"p {<IF#> | c <channel group>} v <vlan id> ip {<src ip> | <src ip>/<masklen>}
{<dest ip> | <dest ip>/<masklen>} [<protocol> [s <src port>] [d <dest port>]]"
```

③ ホワイトパケットリスト：IPv4 の場合（white-list packet mode 2：送信元抽出モード）

```
"p {<IF#> | c <channel group>} v <vlan id> ip <src mac> <src ip>"
```

④ ホワイトパケットリスト：ARP の場合

```
"p {<IF#> | c <channel group>} v <vlan id> arp <src mac> <src ip>"
```

⑤ ホワイトパケットリスト：上記以外の場合（white-list packet mode 1：受信パケット種別モード）

```
"p {<IF#> | c <channel group>} v <vlan id> <src mac> <dest mac>"
```

⑥ ホワイトパケットリスト：上記以外の場合（white-list packet mode 2：送信元抽出モード）

```
"p {<IF#> | c <channel group>} v <vlan id> <src mac>"
```

<masklen> は，受信パケット種別モードでホワイトパケットリスト IPv4 の場合だけ指定できます。

表 31-1　①の指定範囲

キーワード / パラメータ ※1	内容	範囲
a	ホワイトアドレスリスト	―
<mac>	MAC ヘッダの 送信元 MAC アドレス	0000.0000.0001 ～ feff.ffff.ffff※2
v <vlan id>	VLAN ID	1 ～ 4094
p <IF#>	ポート番号	【スタック動作時】 <switch no.>/0/1～<switch no.>/0/10 【スタンドアロン動作時】 0/1～0/10
c <channel group>	チャネルグループ番号	【スタック動作時】 1～120 【スタンドアロン動作時】 1～64

注 ※1　キーワード：アルファベットだけの表記，パラメータ：< >表記

注 ※2　以下は学習対象外となるため，指定できません。

- 非ユニキャスト（先頭バイトの最下位ビットが 1）
- すべてのビットが 0
- 自装置 MAC アドレス

表 31-2　②～⑥の指定範囲

キーワード / パラメータ ※1	内容	範囲
p	ホワイトパケットリスト	―
<IF#>	ポート番号	【スタック動作時】 <switch no.>/0/1～<switch no.>/0/10 【スタンドアロン動作時】 0/1～0/10
c <channel group>	チャネルグループ番号	【スタック動作時】 1～120 【スタンドアロン動作時】 1～64
v <vlan id>	VLAN ID	1 ～ 4094
ip <src ip> または <src ip>/<masklen> <dest ip> または <dest ip>/<masklen>	送信元 IP アドレス	0.0.0.0 ～ 223.255.255.255 クラスD～E（224.0.0.0～255.255.255.255）は指定不可※2
	送信元IPアドレスマスク	0～32
	宛先 IP アドレス	0.0.0.0 ～ 255.255.255.255 ブロードキャストを除くクラス E（240.0.0.0 ～ 255.255.255.254）は指定不可
	宛先IPアドレスマスク	0～32
ip <src mac> <src ip>	MAC ヘッダ内の 送信元 MAC アドレス	0000.0000.0001～feff.ffff.ffff※3
	送信元 IP アドレス	0.0.0.0 ～ 223.255.255.255 クラス D ～ E（224.0.0.0 ～ 255.255.255.255）は指定不可
<protocol>	L4 プロトコル番号	0 ～ 50，52 ～ 255 51（認証）は指定不可

キーワード / パラメータ ※1	内容	範囲
s <src port> d <dest port>	送信元ポート番号 宛先ポート番号	0 ～ 65535 <protocol> で 6（tcp）または 17(udp) 指定時にポート番号指定可
arp <src mac> <src ip>	ARP ヘッダ内の Sender Hardware Address	0000.0000.0001 ～ feff.ffff.ffff※3
	ARP ヘッダ内の Sender Protocol Address	0.0.0.0 ～ 223.255.255.255 クラス D ～ E（224.0.0.0 ～ 255.255.255.255）は指定不可
<src mac> <dest mac>	MAC ヘッダ内の 送信元 MAC アドレス	0000.0000.0001 ～ feff.ffff.ffff※3
	MAC ヘッダ内の 宛先 MAC アドレス	0000.0000.0000 ～ ffff.ffff.ffff

注 ※1　キーワード：アルファベットだけの表記，パラメータ：＜ ＞表記

注 ※2　IP アドレスマスクの指定有無に関わらず，<src ip> および <dest ip> の指定値でクラス D ～ E を判定します。

注 ※3　以下は学習対象外となるため，指定できません。

- 非ユニキャスト（先頭バイトの最下位ビットが 1）
- すべてのビットが 0
- 自装置 MAC アドレス

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. ポート番号またはチャネルグループ番号が異なる場合は，当該エントリが上書きされます。
3. <list entry> のシンタックスチェック，補完機能，ヘルプ機能は実施されません。
4. ダブルクォート内の書式は，上記のいずれかの形式で入力されることを前提とします。
5. キーワードや設定値の入力順が不正な場合は，装置に正しく反映されない場合があります。
6. キーワードを含む設定値はすべて小文字で入力してください。
7. キーワードと設定値の間はスペース 1 文字を入力してください。

［関連コマンド］

white-list enable

white-list enable【OP-WL】

本装置でホワイトリスト機能を有効にします。

［入力形式］

情報の設定
　white-list enable

情報の削除
　no white-list 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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. 本コマンド設定時，MAC アドレステーブルのダイナミックエントリはすべて削除されます。
3. ホワイトリスト機能有効時，併用できない機能があります。詳細は「コンフィグレーションガイド Vol.2　14　ホワイトリスト機能」を参照してください。
4. ホワイトリスト機能は，制御フレーム全般（L2 ループ検知フレームを含む）がホワイトリスト対象となります。このため，L2 ループ検知を併用する場合は，white-list address permit コマンドで loop-detection を設定してください。

［関連コマンド］

no ip igmp snooping

no ipv6 mld snooping

white-list learning【OP-WL】

本装置でホワイトリスト機能の学習（ホワイトリスト生成）を開始します。

［入力形式］

情報の設定
　white-list learning

情報の削除
　no white-list learning

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

ホワイトリスト機能有効時，ホワイトリスト機能の運用状態となります。

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。

［関連コマンド］

white-list enable

white-list logging filter【OP-WL】

white-list action log コマンドを設定時に，ホワイトリスト未学習パケットを syslog サーバへ出力する際のパケット種別を制限します。

パケット種別の制限は，ポートごとに設定可能です。

また，未学習パケットの syslog サーバ出力制限は，ホワイトアドレスリスト，ホワイトパケットリストそれぞれで設定可能です。

ホワイトパケットリストで syslog サーバへの出力を制限するパケット種別は，複数選択可能です。

［入力形式］

情報の設定・変更

white-list logging filter address
white-list logging filter packet [arp] [ipv4] [ipv6] [other]

情報の削除

no white-list logging filter address
no white-list logging filter packet

［入力モード］

(config-if)

［パラメータ］

address

ホワイトアドレスリストの未学習パケットは，syslog サーバへの出力を抑止します。

packet [arp] [ipv4] [ipv6] [other]

各パラメータを設定することによって，syslog サーバへの出力を抑止する未学習パケット種別を選択します。
arp，ipv4，ipv6，other のすべての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。

arp

ARP パケットの未学習パケットは，syslog サーバへの出力を抑止します。

ipv4

IPv4 の未学習パケットは，syslog サーバへの出力を抑止します。

ipv6

IPv6 の未学習パケットは，syslog サーバへの出力を抑止します。

other

上記以外の未学習パケットは，syslog サーバへの出力を抑止します。

1. 本パラメータ省略時の初期値
   指定しない未学習パケット種別は，syslog サーバへの出力を抑止しません。
2. 値の設定範囲
   address，packet，arp，ipv4，ipv6，other

［コマンド省略時の動作］

未学習パケットの syslog サーバへの出力を抑止しません。

［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］

1. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. パラメータ address 指定で 1 行，packet 指定で 1 行だけ設定できます。それぞれを再度入力した場合は，上書きされます。

［関連コマンド］

white-list enable

white-list logging format-add【OP-WL】

ホワイトリスト未学習パケットを syslog サーバへ出力する際の情報を追加します。

［入力形式］

情報の設定
　white-list logging format-add address src-ip

情報の削除
　no white-list logging format-add address

［入力モード］

(config-if)

［パラメータ］

address src-ip

ホワイトアドレスリストの未学習の ARP パケットまたは IPv4 パケット受信時，syslog サーバへ出力する際に送信元 IP アドレスを追加します。

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
   address src-ip

［コマンド省略時の動作］

ホワイトリスト未学習パケットを syslog サーバへ出力する際の情報を追加しません。

［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］

なし

［関連コマンド］

white-list enable

white-list action log

white-list monitor destination interface【OP-WL】

white-list action monitor コマンドを設定したポートで受信した，ホワイトリスト未学習パケットのミラーポートを設定します。

［入力形式］

情報の設定・変更

white-list monitor destination interface {<interface id list> | port-channel <channel group>}

情報の削除

no white-list monitor destination interface

［入力モード］

(config)

［パラメータ］

{<interface id list> | port-channel <channel group>}

ミラーポートを指定します。ミラーポートは最大 2 件の物理ポート，または最大 1 件のポートチャネルインタフェースを指定できます。

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
   <interface id list> :「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。

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. monitor session source コマンドの注意事項を参照してください。

［関連コマンド］

white-list enable

white-list action monitor

white-list packet mode【OP-WL】

ホワイトパケットリスト機能の動作モードを設定します。

［入力形式］

情報の設定・変更
　white-list packet mode {1 | 2}

情報の削除
　no white-list packet mode

［入力モード］

(config)

［パラメータ］

{1 | 2}
　動作モードを指定します。

　1
　　受信パケット種別モードで動作します。

　2
　　送信元抽出モードで動作します。

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
   1，2

［コマンド省略時の動作］

受信パケット種別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. ホワイトパケットリスト動作モードを変更する前に，必ず white-list enable コマンドを削除し，運用コマンド erase white-list packet all を実行してください。

［関連コマンド］

white-list enable

white-list packet tcp【OP-WL】

ホワイトパケットリストのフロー条件に TCP のポート番号を含めます。

本コマンドの設定により，すべての IPv4 パケットに対して L4 プロトコル条件がホワイトパケットリストのフロー条件に追加されます。

［入力形式］

情報の設定・変更
　white-list packet tcp {source | destination | both | server}

情報の削除
　no white-list packet tcp

［入力モード］

(config-if)

［パラメータ］

{source | destination | both | server}
　TCP ポート番号の条件を指定します。

　source
　　送信元 TCP ポート番号をホワイトパケットリストに含めます。

　destination
　　宛先 TCP ポート番号をホワイトパケットリストに含めます。

　both
　　送信元および宛先 TCP ポート番号をホワイトパケットリストに含めます。

　server
　　サーバ側の TCP ポート番号をホワイトパケットリストに含めます。

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

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。

2. 本コマンドを設定したポートがチャネルグループに属している場合は，同じチャネルグループの全ポートに本コマンドを設定してください。
3. 生成済みのホワイトパケットリストエントリには，本コマンドの指定は反映されません。
4. 本コマンドの設定変更後，新規エントリが既存エントリを包含している場合，既存エントリを削除しません。また，既存エントリに包含されるエントリは新規に生成しません。
5. 認証ヘッダ（protocol=51）が付与されている IP パケットは未サポートです。
6. IP トンネリング（protocol=4）が付与されているパケットは，外側の IP ヘッダをホワイトパケットリスト生成の対象とします。内側の IP ヘッダ，および内側の IP ヘッダの L4 プロトコル情報は認識しません。

［関連コマンド］

white-list enable

white-list learning

white-list packet trust-mode【OP-WL】

ホワイトパケットリスト機能の trust モードを設定します。

本コマンドを設定したポートから受信したパケットは，次に示すホワイトリスト機能の影響を受けません。

- ホワイトリスト機能の white-list action discard が当該ポートに設定済でも廃棄されません。
- ホワイトリスト機能の white-list action monitor が当該ポートに設定済でもミラーリング対象になりません。
- ホワイトリスト機能の white-list action log が当該ポートに設定済でも syslog サーバへパケット情報を出力しません。
- ホワイトリスト学習状態でも，ホワイトパケットリストエントリを生成しません。

［入力形式］

情報の設定・変更
　white-list packet trust-mode { 1 | 2 | 3 | 4 }

情報の削除
　no white-list packet trust-mode

［入力モード］

(config-if)

［パラメータ］

{ 1 | 2 | 3 | 4 }
　trust モードを指定します。

1
　IPv6 パケットは，ホワイトパケットリスト機能の影響を受けません。

2
　IPv4(ARP を含む) パケット以外は，ホワイトパケットリスト機能の影響を受けません。

3
　ホワイトアドレスリスト機能だけが動作します。
　全パケットがホワイトパケットリスト機能の影響を受けません。

4
　IPv4 パケット以外はホワイトパケットリスト機能の影響を受けません。

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, 2, 3, 4

［コマンド省略時の動作］

ホワイトリスト機能有効時，当該ポートで受信した全パケットをホワイトパケットリスト機能の対象とします。

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. 本コマンドを設定したポートがチャネルグループに属している場合は，同じチャネルグループの全ポートに本コマンドを設定してください。

［関連コマンド］

white-list enable

white-list packet udp【OP-WL】

ホワイトパケットリストのフロー条件に UDP ポート番号を含めます。

本コマンドの設定により，すべての IPv4 パケットに対して L4 プロトコル条件がホワイトパケットリストのフロー条件に追加されます。

［入力形式］

情報の設定・変更

white-list packet udp {source | destination | both}

情報の削除

no white-list packet udp

［入力モード］

(config-if)

［パラメータ］

{source | destination | both}

UDP ポート番号の条件を指定します。

source

送信元 UDP ポート番号をホワイトパケットリストに含めます。

destination

宛先 UDP ポート番号をホワイトパケットリストに含めます。

both

送信元および宛先 UDP ポート番号をホワイトパケットリストに含めます。

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

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. 本コマンドを設定したポートがチャネルグループに属している場合は，同じチャネルグループの全ポートに本コマンドを設定してください。
3. 生成済みのホワイトパケットリストエントリには，本コマンドの指定は反映されません。

4. 本コマンドの設定変更後，新規エントリが既存エントリを包含している場合，既存エントリを削除しません。また，既存エントリに包含されるエントリは新規に生成しません。
5. 認証ヘッダ（protocol=51）が付与されている IP パケットは未サポートです。
6. IP トンネリング（protocol=4）が付与されているパケットは，外側の IP ヘッダをホワイトパケットリスト生成の対象とします。内側の IP ヘッダ，および内側の IP ヘッダの L4 プロトコル情報は認識しません。

［関連コマンド］

white-list enable

white-list learning

white-list trust【OP-WL】

ホワイトリスト機能の trust ポートを設定します。

本コマンドを設定したポートから受信したパケットは，次に示すホワイトリスト機能の影響を受けません。

- ホワイトリスト機能の white-list action discard が当該ポートに設定済でも廃棄されません。
- ホワイトリスト機能の white-list action monitor が当該ポートに設定済でもミラーリング対象になりません。
- ホワイトリスト機能の white-list action log が当該ポートに設定済でも syslog サーバへパケット情報を出力しません。
- ホワイトリスト学習状態でも，ホワイトアドレスリストエントリ，ホワイトパケットリストエントリを生成しません。

［入力形式］

情報の設定
　white-list trust

情報の削除
　no white-list 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］

ホワイトリスト機能有効時，当該ポートで受信した全パケットをホワイトリスト機能の対象とします。

［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. オプションライセンス【OP-WL】については以下のとおりです。
   【08TF】登録が必要です。
   【08T】登録不要です。
2. 本コマンドを設定したポートがチャネルグループに属している場合は，同じチャネルグループの全ポートに本コマンドを設定してください。
3. 本コマンド削除時，MAC アドレステーブルのダイナミックエントリはすべて削除されます。

［関連コマンド］

white-list enable

32 特定端末への Web 通信不可表示機能

access-redirect http port

access-redirect http target

access-redirect timeout

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

33 アップリンク・リダンダント

switchport backup interface
switchport backup flush-request transmit
switchport backup mac-address-table update exclude-vlan
switchport backup mac-address-table update retransmit
switchport backup mac-address-table update transmit
switchport-backup startup-active-port-selection

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>]

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>}

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#> および <channel group> 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。

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 set 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. 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。
   - プライマリポートがリンクアップした場合
   - 運用コマンド set switchport-backup active の実行によって，セカンダリポートがアクティブポートに遷移した場合
   - スタック動作時，マスタスイッチの切り替えが発生した場合

[関連コマンド]

なし

34 IEEE 802.3ah/UDLD

efmoam active

efmoam disable

efmoam udld-detection-count

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

35 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
   次の表に示します。

表 35-1　閾値の設定範囲と刻み値

設定範囲（単位：pps）	刻み値（単位：pps）
0 ～ 1,500,000	10
1,500,000 ～ 10,000,000	100

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

表 35-2　閾値の設定範囲と刻み値

設定範囲（単位：pps）	刻み値（単位：pps）
0 ～ 1,500,000	10
1,500,000 ～ 10,000,000	100

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

表 35-3　閾値の設定範囲と刻み値

設定範囲（単位：pps）	刻み値（単位：pps）
0 ～ 1,500,000	10
1,500,000 ～ 10,000,000	100

filter-unicast <packet/s>

ユニキャストフラッディン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ン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ングフレームをすべて廃棄します。
2. 値の設定範囲

表 35-4　閾値の設定範囲と刻み値

設定範囲（単位：pps）	刻み値（単位：pps）
0 ～ 1,500,000	10
1,500,000 ～ 10,000,000	100

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

36 L2 ループ検知

loop-detection

loop-detection auto-restore-time

loop-detection enable

loop-detection hold-time

loop-detection interval-time

loop-detection threshold

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

37 CFM

domain name
ethernet cfm cc alarm-priority
ethernet cfm cc alarm-reset-time
ethernet cfm cc alarm-start-time
ethernet cfm cc enable
ethernet cfm cc interval
ethernet cfm domain
ethernet cfm enable（global）
ethernet cfm enable（interface）
ethernet cfm mep
ethernet cfm mip
ma name
ma vlan-group

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。設定可能な文字は先頭 1 文字目が英字，他は英数字とハイフン（-），ピリオド（.）です。
   <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 37-1　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コンフィグレーション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

38 SNMP

hostname
rmon alarm
rmon collection history
rmon event
snmp-server community
snmp-server contact
snmp-server engineID local
snmp-server group
snmp-server host
snmp-server location
snmp-server traps
snmp-server user
snmp-server view
snmp trap link-status

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 38-1　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 38-1　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 38-1　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または SNMPv3 ユーザに対して 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 50 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}] [<access list name>]

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，GetBulkRequest を許可し，rw を設定した場合，Get Request，GetNext Request，GetBulkRequest，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

<access list name>

本コミュニティに対する許可を設定した IPv4 アドレスフィルタまたは IPv6 フィルタを名前で設定します。<access list name> 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 <access list name> 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
   4 ～ 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］

1. IPv4 アドレスフィルタを設定した場合は，IPv6 によるアクセスは許可されません。
2. IPv6 フィルタを設定した場合は，IPv4 によるアクセスは許可されません。

［関連コマンド］

ip access-list standard

ipv6 access-list

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 engineID local

SNMP エンジン ID 情報の設定をします。

［入力形式］

情報の設定・変更

snmp-server engineID local <engineid string>

情報の削除

no snmp-server engineID local

［入力モード］

(config)

［パラメータ］

<engineid string>

SNMP エンジン ID を設定します。

装置に設定される SNMP エンジン ID の値は，次のようになります。

1 ～ 4 オクテット：0x8000554F

5 オクテット：0x04

6 ～ 32 オクテット以降：<engineid string> 設定値

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   27 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］

装置に設定される SNMP エンジン ID の値は，次のようになります。

1 ～ 4 オクテット：0x8000554F

5 オクテット：0x80

6 ～ 9 オクテット：擬似乱数

10 ～ 13 オクテット：自動生成時の時刻（1970 年からの積算秒数）

［通信への影響］

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 エンジン ID 設定状態は運用コマンド show snmp engineID local で確認できます。
2. SNMP エンジン ID を変更したときにコンフィグレーションを保存せずに再起動すると，起動回数だけ

リセットされ SNMPv3 の認証が機能しなくなる可能性があります。その場合，SNMP エンジン ID を再設定し，保存した後に再起動をしてください。

3. 意図しない不慮の再起動が発生した場合，SNMP エンジン ID や SNMP エンジン ID 変更後の起動回数をビット単位で壊す可能性があります。その場合，運用コマンド set snmp-server engineID local で復旧できます。
4. 複数のユーザを登録している場合，SNMP エンジン ID の変更に数十秒かかります。

［関連コマンド］

snmp-server view

snmp-server user

snmp-server group

snmp-server host

snmp-server group

SNMP セキュリティグループ情報の設定をします。本コマンドでは最大 50 個のグループ名称を設定できます。

［入力形式］

情報の設定・変更

snmp-server group <group name> v3 { noauth | auth | priv } [read <view name>] [write <view name>] [notify <view name>]

情報の削除

no snmp-server group <group name> v3 { noauth | auth | priv }

［入力モード］

(config)

［パラメータ］

<group name>

SNMP セキュリティ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。

{ noauth | auth | priv }

Read ビュー，Write ビュー，Notify ビューパラメータで指定した MIB ビューへのアクセス権を与えるために要求するセキュリティレベルです。

送受信メッセージが本パラメータで設定したセキュリティレベルとより低い場合は，アクセス権を与えません。

同じ SNMP セキュリティグループ名で複数のセキュリティレベルを設定している場合は，送受信メッセージのセキュリティレベルと同じもしくは低いセキュリティレベルのうち，最も高いセキュリティレベルの MIB ビューでアクセス制御を行います。

noauth：認証なし，暗号化なし
auth：認証あり，暗号化なし
priv：認証あり，暗号化あり

1. 本パラメータ省略時の初期値
   省略できません。
2. 値の設定範囲
   noauth，auth，または priv のどれか

read <view name>

次の PDU タイプの SNMP パケットを受信したときにアクセス制御に使用する MIB ビュー名を設定します。

・GetRequest-PDU
・GetNextRequest-PDU
・GetBulkRequest-PDU

1. 本パラメータ省略時の初期値
   Read のアクセス権が与えられません。
2. 値の設定範囲
   32 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。

write <view name>

SetRequest-PDU の SNMP パケットを受信したときにアクセス制御に使用する MIB ビュー名を設定します。

1. 本パラメータ省略時の初期値
   Write のアクセス権が与えられません。
2. 値の設定範囲
   32 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。

notify <view name>

トラップを送信するときにアクセス制御に使用する MIB ビュー名を設定します。
トラップ自体のオブジェクト識別子とトラップに含まれる各オブジェクト識別子がすべてアクセス可能でなければ，トラップを送信しません。

1. 本パラメータ省略時の初期値
   Notify のアクセス権が与えられません。
2. 値の設定範囲
   32 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］

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-server view コマンドで設定されていない MIB ビュー名を本コマンドの Read ビュー名，Write ビュー名，Notify ビュー名に設定した場合，本コマンドに設定したビュー名の情報は空となりますので，ご注意ください。
2. トラップを生成するときは本コマンドの notify ビュー名の情報と snmp-server host コマンドの設定が必要です。

［関連コマンド］

snmp-server engineID local

snmp-server view

snmp-server user

snmp-server host

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 50 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 <string> [version { 1 | 2c | 3 { noauth | auth | priv } }] [snmp] [rmon] [air-fan] [power] [login] [system-msg] [temperature] [axrp] [storm-control] [efmoam] [dot1x] [web-authentication] [mac-authentication] [loop-detection] [switchport-backup] [cfm] [lldp]

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）を指定するか，または <manager address> に IPv6 アドレス（コロン記法）を指定します。
   IPv4 ユニキャストアドレス
   1.0.0.0 ～ 126.255.255.255，128.0.0.0 ～ 223.255.255.255
   IPv6 グローバルユニキャストアドレス
   ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff，fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<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。
SNMPv3 の場合はセキュリティユーザ名を設定します。
セキュリティユーザ名にアットマーク (@) を使用しないでください。

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
   SNMPv1 および SNMPv2C は 60 文字以内，SNMPv3 は 32 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。

version { 1 | 2c | 3 { noauth | auth | priv }}

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トラップ送信バージョンを設定します。1 を設定した場合，SNMPv1 バージョンのトラップを，2c を設定した場合，SNMPv2C バージョンのトラップを，3 を設定した場合，SNMPv3 バージョンのトラップを発行します。
3 を指定した場合は，さらにトラップ送信のセキュリティレベルを設定します。

- noauth を設定した場合，認証なし，暗号化なしでトラップが送信されます。
- auth を設定した場合，認証あり，暗号化なしでトラップが送信されます。
- priv を設定した場合，認証あり，暗号化ありでトラップが送信されます。

1. 本パラメータ省略時の初期値
   1
2. 値の設定範囲
   1，2c，または 3 のどれかを設定します。
   3 を設定した場合，さらに noauth，auth，または priv のどれかを設定します。

[snmp] [rmon] [air-fan] [power] [login] [system-msg] [temperature] [axrp] [storm-control] [efmoam] [dot1x] [web-authentication] [mac-authentication] [loop-detection] [switchport-backup] [cfm] [lldp]

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 38-2　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	ax260aTemperatureTrap
air-fan	ax260aAirFanStopTrap
power	ax260aAX260APowerSupplyFailureTrap
login	ax260aLoginSuccessTrap
	ax260aLoginFailureTrap
	ax260aLogoutTrap
system-msg	ax260aSystemMsgTrap
axrp	ax260aAxrpStateTransitionTrap
	ax260aAxrpMultiFaultDetectionStartTrap
	ax260aAxrpMultiFaultDetectionStateTransitionTrap
storm-control	ax260aBroadcastStormDetectTrap
	ax260aMulticastStormDetectTrap
	ax260aUnicastStormDetectTrap
	ax260aBroadcastStormPortInactivateTrap
	ax260aMulticastStormPortInactivateTrap
	ax260aUnicastStormPortInactivateTrap
	ax260aBroadcastStormRecoverTrap
	ax260aMulticastStormRecoverTrap
	ax260aUnicastStormRecoverTrap
efmoam	ax260aEfmoamUdldPortInactivateTrap

パラメータ	トラップ
dot1x	ax260aDot1xFailureTrap
	ax260aDot1xEventTrap
	ax260aDot1xSystemTrap
web-authentication	ax260aWauthFailureTrap
	ax260aWauthEventTrap
	ax260aWauthSystemTrap
mac-authentication	ax260aMauthFailureTrap
	ax260aMauthEventTrap
	ax260aMauthSystemTrap
loop-detection	ax260aL2ldLinkDown
	ax260aL2ldLinkUp
	ax260aL2ldLoopDetection
switchport-backup	ax260aUlrChangeSecondary
	ax260aUlrChangePrimary
cfm	dot1agCfmFaultAlarm
lldp	lldpV2RemTablesChange
指定不要	ax260aDeviceErrorTrap

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

ファンがストップしたときにトラップを送信します。

power

一つの電源に障害発生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。

axrp

リングの障害監視状態が変化したときに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。

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。

lldp

LLDP の隣接装置に関する情報が更新されたときに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，power，login，system-msg，temperature，axrp，storm-control，efmoam，dot1x，web-authentication，mac-authentication，loop-detection，switchport-backup，cfm，lldp

［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 はファン搭載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］

snmp-server engineID local

snmp-server view

snmp-server user

snmp-server group

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 38-3　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） ・ スタックとして動作中にマスタに切り替ったとき
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 ・ スタックとして動作中にマスタに切り替ったとき

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 38-4　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/SNMPv3 トラップ共通) ifIndex，ifDescr，ifType
standard	• (SNMPv1 トラップの場合) ifIndex • (SNMPv2C/SNMPv3 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。指定したレベル以上の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 38-5　システムメッセージトラップのレベルと意味

レベル	意味
9	致命的障害のシステムメッセージトラップを送信します。
8	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。
5 ～ 7	温度異常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	ネットワーク系障害以上のシステムメッセージトラップを送信します。
1 ～ 3	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。

1. 本パラメータ省略時の初期値
   9
2. 値の設定範囲
   1 ～ 9

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-server user

SNMP セキュリティユーザ情報の設定をします。本コマンドで作成したユーザ情報は，snmp-server group コマンドおよび snmp-server host コマンドで使用します。本コマンドでは最大 50 エントリを設定できます。

本コマンドでは，認証プロトコルとプライバシープロトコルを設定します。プライバシープロトコルは，認証プロトコルを設定していないと設定できません。認証プロトコルとプライバシープロトコルの組み合わせを次の表に示します。

表 38-6　認証プロトコルとプライバシープロトコルの設定可能な組み合わせ

項番	認証プロトコル	プライバシープロトコル
1	なし	なし
2	HMAC-MD5，HMAC-SHA1，HMAC-SHA-256，または HMAC-SHA-512	なし
3	HMAC-MD5，HMAC-SHA1，HMAC-SHA-256，または HMAC-SHA-512	CBC-DES または CFB128-AES-128DES

［入力形式］

情報の設定・変更

snmp-server user <user name> <group name> v3 [auth { md5 | sha | sha256 | sha512 } <authentication password> [priv { des | aes128 } <privacy password>]]

情報の削除

no snmp-server user <user name>

［入力モード］

(config)

［パラメータ］

<user name>

SNMP セキュリティユーザ名を設定します。

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。

<group name>

SNMP セキュリティユーザが所属する SNMP セキュリティ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。

v3 [auth { md5 | sha | sha256 | sha512 } <authentication password> [priv { des | aes128 } <privacy password>]]

auth { md5 | sha | sha256 | sha512 } <authentication password>

認証プロトコルおよび認証パスワードを設定します。

md5：認証プロトコルに HMAC-MD5 を使用します。

sha：認証プロトコルに HMAC-SHA1 を使用します。

sha256：認証プロトコルに HMAC-SHA-256 を使用します。

sha512：認証プロトコルに HMAC-SHA-512 を使用します。

priv { des | aes128 } <privacy password>

プライバシープロトコルおよびプライバシーパスワードを設定します。

des：プライバシープロトコルに CBC-DES を使用します。

aes128：プライバシープロトコルに CFB-128-AES-128 を使用します。

1. 本パラメータ省略時の初期値
   auth 以降を省略した場合，認証されている受信メッセージと認証するべき送信メッセージは破棄されます。
   priv 以降を省略した場合，暗号化されている受信メッセージと暗号化するべき送信メッセージは破棄されます。
2. 値の設定範囲
   <authentication password> および <privacy password> は，どちらも 8 文字以上 32 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］

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］

snmp-server engineID local

snmp-server view

snmp-server group

snmp-server host

snmp-server view

MIB ビュー情報の設定をします。

本コマンドで設定可能なパラメータごとのエントリ数を次の表に示します。

表 38-7　パラメータごとのエントリ数

項番	パラメータ	最大エントリ数
1	MIB ビュー	50 エントリ
2	サブツリー	MIB ビュー当たり 30 エントリ
3		全体で 500 エントリ

［入力形式］

情報の設定・変更

snmp-server view <view name> <oid tree> { included | excluded }

情報の削除

no snmp-server view <view name> <oid tree>

［入力モード］

(config)

［パラメータ］

<view name>

MIB ビュー名を設定します。

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。

<oid tree>

サブツリーを表すオブジェクト 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
   オブジェクト ID をドット記法で設定します。最大 64 文字です。サブ識別（ドットで区切られた数字）ごとにワイルドカード（*）を設定することもできます。

{ included | excluded }

サブツリーの包含または除外を設定します。サブツリーを MIB ビューに含む場合は included を設定します。サブツリーを MIB ビューから除く場合は excluded 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
   included または excluded のどちらかを設定します。

［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. 情報の変更および削除の際，<oid tree> のサブ識別にワイルドカード（*）を設定すると，同じ位置のサブ識別が 0 であるエントリと同一とみなされます。また，0 を設定すると，同じ位置のサブ識別が * であるエントリと同一とみなされます。
   これによって，別のエントリであるにもかかわらず，情報の変更では上書きされ，情報の削除では削除されます。

［関連コマンド］

snmp-server engineID local

snmp-server user

snmp-server group

snmp-server host

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

39 ログ出力機能

logging event-kind

logging facility

logging host

logging syslog-dump

logging tcp connect delay

logging tcp notify open

logging tcp notify resume

logging tcp reconnect delay

logging tcp trailer

logging trap

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
　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，aut，wht の中から指定します。

［コマンド省略時の動作］

ホワイトリスト機能有効時：イベント種別は「evt」「err」「wht」となります。

ホワイトリスト機能無効時：イベント種別は「evt」「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，デフォルトコンフィグレーションのイベント種別（evt，err，wht）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

white-list enable

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。

また，ログ情報の送信プロトコルと宛先ポート番号を出力先ごとに設定できます。

［入力形式］

情報の設定・変更

logging host <ipv4 address > [{tcp | udp}] [port <number>] [no-date-info]
logging host <ipv6 address> [udp] [port <number>] [no-date-info]

情報の削除

no logging host <ipv4 address > [{tcp | udp}] [port <number>]
no logging host <ipv6 address> [udp] [port <number>]

［入力モード］

(config)

［パラメータ］

<ipv4 address>

ログ情報出力先の 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
   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

<ipv6 address>

ログ情報出力先の IPv6 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
   IPv6 アドレスをコロン記法で指定します。
   ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff，fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

{tcp | udp}

ログ情報出力時の送信プロトコルを設定します。
tcp は IPv4 アドレス指定時だけ設定可能です。

1. 本パラメータ省略時の初期値
   udp で動作します。
2. 値の設定範囲
   tcp，udp

port <number>

ログ情報出力時の宛先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
   514 で動作します。
2. 値の設定範囲
   1 ～ 65535

no-date-info

ログ情報から時刻を除いた部分を送信します。ログ種別が EVT または ERR の場合は，時刻，メッセージ識別子を除いた部分を送信します。
ログ情報のフォーマットについては，「メッセージ・ログレファレンス　1.2.3　運用ログのフォーマット」を参照してください。

1. 本パラメータ省略時の初期値
   すべてのログ情報を送信します。
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. 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. ログ情報出力先として本装置の IP アドレスを指定しないでください。指定した場合は本装置の他機能に影響する可能性があります。（一例として，ログ情報出力先として本装置の TCP ポート 21 を指定すると本装置の FTP サーバが使用不能になる可能性があります。）
3. ログ情報をブロードキャスト宛（例：192.168.0.255）に送信することはできません。
4. 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。
5. no-date-info を指定した場合でも，装置内に保存されるログ情報には時刻情報は残ります。
6. no-date-info を指定すると，ログ出力先に送信するメッセージ内の時刻は除かれますが，ログ出力機能自体が時刻をヘッダとして追加するため，ログ出力先ではログ情報の送信日時がメッセージとして表示されます。
7. 本コマンド設定時，同一の「IP アドレス・プロトコル（省略時は "udp" 指定と同じ）・ポート番号（省略時は "port 514" 指定と同じ）」を指定したときは，上書きされます。
   なお，運用コマンド show running-config では，入力した書式で表示されます（プロトコルやポート番号を省略した場合は，表示されません）。
8. 本コマンド削除時，「IP アドレス・プロトコル（省略時は "udp" 指定と同じ）・ポート番号（省略時は "port 514" 指定と同じ）」が，すべて一致したエントリが削除されます。
9. "tcp" を指定した出力先アドレスのコマンド削除処理は，TCP コネクションの切断（通信障害時は 10 秒でタイムアウト）が完了するまで待機します。
10. "tcp" を指定した出力先アドレスを設定している場合，装置再起動処理（運用コマンド reload など）は，syslog 送信キューが空になって TCP コネクションが切断されるまで待機します。

［関連コマンド］

なし

logging syslog-dump

no logging syslog-dump 設定時，装置で発生したログを内蔵フラッシュメモリに格納しません。

［入力形式］

情報の設定
　no logging syslog-dump

情報の削除
　logging syslog-dump

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

ログは内蔵フラッシュメモリに格納されます。

［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. ログとは，運用ログ，種別ログを指します。
2. 本設定を行うとログが本装置に保存されませんので，syslog インタフェースによるログ送信を行うことを推奨します。
3. 運用コマンド clear logging を実行すると，内蔵フラッシュメモリにアクセスを行いログの消去を行います。

［関連コマンド］

logging host

logging tcp connect delay

装置起動時，コンフィグレーション展開から TCP で接続開始するまでの時間を指定します。

［入力形式］

情報の設定・変更
　logging tcp connect delay <seconds>

情報の削除
　no logging tcp connect delay

［入力モード］

(config)

［パラメータ］

<seconds>
　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 ～ 60（秒）

［コマンド省略時の動作］

5 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。

ただし，本コマンドの設定値は装置起動直後だけに使用されるため，装置起動後（60 秒以内，かつ TCP 接続開始以前）に変更した場合を除き，変更後の値は次回以降の装置起動時に使用されます。

［注意事項］

なし

［関連コマンド］

logging host

logging tcp notify open

TCP 接続したとき，開始メッセージを送信します。

［入力形式］

情報の設定
　logging tcp notify open

情報の削除
　no logging tcp notify open

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

開始メッセージを送信しません。

［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］

なし

［関連コマンド］

logging host

logging tcp notify resume

TCP 送信バッファ溢れが解消したときに再開メッセージを送信します。

［入力形式］

情報の設定
　logging tcp notify resume

情報の削除
　no logging tcp notify resume

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

送信バッファ溢れが解消したときも再開メッセージを送信しません。

［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］

なし

［関連コマンド］

logging host

logging tcp reconnect delay

TCP の接続開始までの時間を指定します。

［入力形式］

情報の設定・変更
　logging tcp reconnect delay <seconds>

情報の削除
　no logging tcp reconnect delay

［入力モード］

(config)

［パラメータ］

<seconds>
　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 ～ 60（秒）

［コマンド省略時の動作］

5 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］

logging host

logging tcp trailer

TCP 送信の syslog メッセージの区切り文字を指定します。

［入力形式］

情報の設定・変更

logging tcp trailer {<code> | crlf}

情報の削除

no logging tcp trailer

［入力モード］

(config)

［パラメータ］

{<code> | crlf}

区切り文字を 10 進数のコードで指定します。

「crlf」を指定した場合は，CR+LF の 2 バイトを区切り文字とします。

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
   0 ～ 255 または crlf

［コマンド省略時の動作］

メッセージ長を付加し，区切り文字を使用しません。

［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］

logging host

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。

表 39-1　指定できる重要度

レベル（level）	キーワード（keyword）	説明
0	emergencies	システムは使用不能
1	alerts	即時対応が必要
2	critical	クリティカル状態
3	errors	エラー状態
4	warnings	警告状態
5	notifications	正常だが注意を要する状態
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

40 sFlow 統計

sflow destination

sflow extended-information-type

sflow forward egress

sflow forward ingress

sflow max-header-size

sflow max-packet-size

sflow packet-information-type

sflow polling-interval

sflow sample

sflow source

sflow url-port-add

sflow version

sflow destination

sFlow パケットの宛先であるコレクタの IP アドレスを指定します。

[入力形式]

情報の設定

sflow destination { <ip address> | <ipv6 address> } [<udp port>]

情報の削除

no sflow destination { <ip address> | <ipv6 address> } [<udp port>]

[入力モード]

(config)

[パラメータ]

{ <ip address> | <ipv6 address> }

sFlow パケットの宛先であるコレクタの IP アドレスを指定します。IP アドレスと UDP ポート番号の組み合わせで最大 4 組を指定できます。

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
   IPv4 形式または IPv6 形式の IP アドレスを指定します。

<udp port>

sFlow パケットの宛先であるコレクタの UDP 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
   6343
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]

1. 本パラメータは変更ができません。一度削除したあとに追加してください。
2. 同一の IP アドレスに対して，複数の UDP ポート番号の設定もできます。
3. コレクタの IPv4，IPv6 アドレスとしてブロードキャストアドレス，マルチキャストアドレス，およびリンクローカルアドレスは設定できません。

[関連コマンド]

なし

sflow extended-information-type

フローサンプルの各拡張データ形式の送信有無を指定します。

［入力形式］

情報の設定・変更

sflow extended-information-type { [switch] [router] [gateway] [user] [url] | none }

情報の削除

no sflow extended-information-type

［入力モード］

(config)

［パラメータ］

{ [switch] [router] [gateway] [user] [url] | none }

フローサンプルの各拡張データ形式の送信有無を指定します。
ここで指定する拡張データ形式とは，パケット情報から判断できるスイッチやルータなどに関するネットワーク情報のまとまりを指します。詳細については，「コンフィグレーションガイド Vol.2 24.1.3　sFlow パケットフォーマット (c) 拡張データ形式」を参照してください。
本パラメータは複数指定が可能です。複数指定する場合には，パラメータとパラメータの間に空白の区切りを入れて設定してください。ただし，none パラメータはほかのパラメータと同時に指定できません。

switch

スイッチ情報（VLAN 情報など）の送信を許容します。

router

ルータ情報の送信を許容します。

gateway

ゲートウェイ情報の送信を許容します。

user

ユーザ情報の送信を許容します。

url

URL 情報の送信を許容します。

none

すべての拡張データ形式をコレクタに送信しません。

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
   switch，router，gateway，user，url，none

［コマンド省略時の動作］

すべての拡張データ形式をコレクタに送信します。

［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. 本コマンドによる設定は上書きされます。パラメータを変更したい場合は，必要なパラメータ値をすべて入力してください。
2. 本装置はレイヤ 2 スイッチであるため，ルータ情報およびゲートウェイ情報の送信は未サポートです。

［関連コマンド］

なし

sflow forward egress

指定したポートの送信トラフィックを sFlow 統計の監視対象にします。

［入力形式］

情報の設定
　sflow forward egress

情報の削除
　no sflow forward egress

［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. 装置として sflow forward egress または sflow forward ingress のどちらかしか指定できません。送信トラフィックを監視対象にする場合は，他ポートに設定した sflow forward ingress をすべて削除してから，監視ポートに sflow forward egress を設定してください。

［関連コマンド］

sflow forward ingress

sflow forward ingress

指定したポートの受信トラフィックを sFlow 統計の監視対象にします。

[入力形式]

情報の設定
　sflow forward ingress

情報の削除
　no sflow forward ingress

[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. 装置として sflow forward ingress または sflow forward egress のどちらかしか指定できません。受信トラフィックを監視対象にする場合は，他ポートに設定した sflow forward egress をすべて削除してから，監視ポートに sflow forward ingress を設定してください。

[関連コマンド]

sflow forward egress

sflow max-header-size

基本データ形式（sflow packet-information-type コマンド参照）にヘッダ型を使用している場合，サンプルパケットの先頭からコピーされる最大サイズを指定します。

［入力形式］

情報の設定・変更
　sflow max-header-size <bytes>

情報の削除
　no sflow max-header-size

［入力モード］

(config)

［パラメータ］

<bytes>

基本データ形式にヘッダ型を使用している場合，サンプルパケットの先頭からコピーされる最大サイズ（バイト）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
   0 ～ 256

［コマンド省略時の動作］

サンプルパケットの先頭からコピーされる最大サイズは 128 バイトになります。

［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］

なし

［関連コマンド］

なし

sflow max-packet-size

sFlow パケットの最大サイズを指定します。

［入力形式］

情報の設定・変更

sflow max-packet-size <bytes>

情報の削除

no sflow max-packet-size

［入力モード］

(config)

［パラメータ］

<bytes>

sFlow パケットの最大サイズ（バイト）を指定します。本値はコレクタへの送信元インタフェースに付いている MTU 長（バイト）以下の値を指定します。

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
   1400 ～ 9216

［コマンド省略時の動作］

sFlow パケットの最大サイズは 1400 バイトになります。

［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］

なし

［関連コマンド］

なし

sflow packet-information-type

フローサンプルの基本データ形式を指定します。

［入力形式］

情報の設定
　sflow packet-information-type ip

情報の削除
　no sflow packet-information-type

［入力モード］

(config)

［パラメータ］

ip

フローサンプルの基本データ形式を指定します。
ip 指定時は，対象パケットが IPv4 パケットの場合は IPv4 型で，IPv6 パケットの場合は IPv6 型でコレクタに送信します。ここで指定する基本データ形式の詳細については，「コンフィグレーションガイド Vol.2　24.1.3　sFlow パケットフォーマット (b) 基本データ形式」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
   ip

［コマンド省略時の動作］

ヘッダ型を用いてコレクタに送信します。

［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］

なし

［関連コマンド］

なし

sflow polling-interval

カウンタサンプルをコレクタへ送信する間隔を指定します。

[入力形式]

情報の設定・変更
　sflow polling-interval <seconds>

情報の削除
　no sflow polling-interval

[入力モード]

(config)

[パラメータ]

<seconds>

カウンタサンプルをコレクタへ送信する間隔を秒単位で指定します。0 秒を指定すると，カウンタサンプルはコレクタに送信されません。

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
   0 ～ 2147483647（=2 ^ 31 － 1）

[コマンド省略時の動作]

カウンタサンプルをコレクタへ 20 秒間隔で送信します。

[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. 20 ポート以上を監視する場合，本装置に負荷が掛かることがあります。その場合は，監視対象の物理ポートの総数を目安秒として指定してください。

   （例）監視対象の物理ポートが 40 ポートの場合，40 秒以上を指定します。

[関連コマンド]

なし

sflow sample

本装置に適用するサンプリング間隔を指定します。

［入力形式］

情報の設定・変更

sflow sample <sample count>

情報の削除

no sflow sample

［入力モード］

(config)

［パラメータ］

<sample count>

本装置に適用するサンプリング間隔を指定します（単位：パケット）。設定したサンプリング間隔ごとに 1 個パケットを確率に従ってサンプリングします（例えば，サンプリング間隔を 512 に設定した場合は，パケットごとに 1/512 の確率でサンプリングします）。運用コマンド show interfaces で，sFlow 統計を有効にするポートの稼働状態の受信または送信の PPS（パケット数／秒）をすべて調べてください。「表 40-1　稼働環境でのサンプリング間隔の目安」の，合計した PPS に対応する「目安となるサンプリング間隔」が推奨値になります。サンプリング間隔に推奨値よりも小さな値を設定すると，CPU 負荷が高くなるおそれがあります。

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
   256，512，1024，2048，4096，8192，16384，32768，65536，131072，262144，524288，1048576，2097152
   式（2 ^ n）の n に 8 ～ 21 を入れた値を指定してください。これら以外の値が入力された場合，入力値に応じて自動的にこれらの値を設定し動作します。その場合の具体的な入力値と設定値の関係を「表 40-2　サンプリング間隔繰り上げ表」に示します。

表 40-1　稼働環境でのサンプリング間隔の目安

合計した PPS の数	目安となるサンプリング間隔	目安となる実装例
25kpps 以下	256	
50kpps 以下	512	100Mbit/s イーサネット ×1 本
100kpps 以下	1024	
200kpps 以下	2048	
400kpps 以下	4096	1Gbit/s イーサネット ×1 本
800kpps 以下	8192	
1.6Mpps 以下	16384	
3.2Mpps 以下	32768	
6.4Mpps 以下	65536	10Gbit/s イーサネット ×1 本
13Mpps 以下	131072	
26Mpps 以下	262144	1Gbit/s イーサネット ×48 本

合計した PPS の数	目安となるサンプリング間隔	目安となる実装例
52Mpps 以下	524288	
100Mpps 以下	1048576	
200Mpps 以下	2097152	

表 40-2　サンプリング間隔繰り上げ表

コマンド入力されたサンプリング間隔	実際に動作するサンプリング間隔
256	256
257 ～ 512	512
513 ～ 1024	1024
1025 ～ 2048	2048
2049 ～ 4096	4096
4097 ～ 8192	8192
8193 ～ 16384	16384
16385 ～ 32768	32768
32769 ～ 65536	65536
65537 ～ 131072	131072
131073 ～ 262144	262144
262145 ～ 524288	524288
524289 ～ 1048576	1048576
1048577 ～ 2097152	2097152
2097153 以上	2097152

（例）

<sample count> に 1000 が指定された場合は，1024（=2 ^ 10）で動作します。

［コマンド省略時の動作］

本装置に適用するサンプリング間隔は 2097152（=2 ^ 21）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

sflow source

sFlow パケットの送信元（エージェント）に設定される IP アドレスを指定します。

［入力形式］

情報の設定・変更

sflow source { <ip address> | <ipv6 address> }

情報の削除

no sflow source { <ip address> | <ipv6 address> }

［入力モード］

(config)

［パラメータ］

{ <ip address> | <ipv6 address> }

sFlow パケットの送信元（エージェント）の IP アドレスとして使用する IP アドレスを指定します。IPv4 アドレスと IPv6 アドレスはそれぞれ一つずつ指定できます。

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
   IPv4 形式または IPv6 形式の IP アドレスを指定します。

［コマンド省略時の動作］

本装置が選択した送信元 IP アドレスが使用されます。

［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. sFlow パケットのエージェント IP アドレスとしてブロードキャストアドレス，マルチキャストアドレス，およびリンクローカルアドレスは設定できません。
2. エージェント IP アドレスとして使用する IP アドレスは，本装置の VLAN に割り付けられている IP アドレスを指定してください。本装置以外の IP アドレスを指定した場合，sFlow パケットは送信できません。

［関連コマンド］

なし

sflow url-port-add

拡張データ形式でURL情報を使用する場合に，HTTPパケットと判断するポート番号を80以外に追加指定します。

［入力形式］

情報の設定・変更
　sflow url-port-add <url port>

情報の削除
　no sflow url-port-add

［入力モード］

(config)

［パラメータ］

<url port>

拡張データ形式でURL情報を使用する場合に，HTTPパケットと判断するポート番号を80以外に追加指定します。

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

［コマンド省略時の動作］

HTTPパケットと判断するポート番号は80番だけになります。

［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

sflow version

送信する sFlow パケットのバージョンを設定します。

［入力形式］

情報の設定
　sflow version <version no.>

情報の削除
　no sflow version

［入力モード］

(config)

［パラメータ］

<version no.>

送信する sFlow パケットのバージョンを設定します。指定されたバージョンの sFlow パケットを用いてコレクタに送信します。

1. 本パラ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

［コマンド省略時の動作］

sFlow パケットバージョンは 4 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

41 LLDP

lldp enable
lldp hold-count
lldp interval-time
lldp management-address
lldp run
lldp version

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 management-address

LLDP の管理アドレスを設定します。

［入力形式］

情報の設定・変更

lldp management-address {ip <ip address> | ipv6 <ipv6 address>}

情報の削除

no lldp management-address

［入力モード］

(config)

［パラメータ］

{ip <ip address> | ipv6 <ipv6 address>}

管理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 アドレスまたは IPv6 アドレスを指定します。

［コマンド省略時の動作］

隣接装置へ管理アドレスを通知しません。

［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

lldp version

本装置の LLDP のバージョンを設定します。

［入力形式］

情報の設定
　lldp version { auto | draft | 2005 }

情報の削除
　no lldp version

［入力モード］

(config-if)

［パラメータ］

{ auto | draft | 2005 }
　本装置の LLDP のバージョンを設定します。

　auto
　　自動で判別します。

　draft
　　IEEE802.1AB/D6.0（2003 年 10 月）に設定します。

　2005
　　IEEE802.1AB-2005 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
   auto，draft，または 2005

［コマンド省略時の動作］

auto 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］

lldp run

42 ポートミラーリング

ip icmp monitor destination interface
monitor session source
switchport monitor dot1q tag

ip icmp monitor destination interface

ICMP パケットに限定したポートミラーリング機能を設定します。

本コマンドを設定したポートは，モニターポートになります。当該ポートで受信した ICMP パケットをミラーリングします。

［入力形式］

情報の設定・変更

ip icmp monitor destination interface {<interface id list> | port-channel <channel group>}

情報の削除

no ip icmp monitor destination interface

［入力モード］

(config-if)

［パラメータ］

{<interface id list> | port-channel <channel group>}

ICMP 限定ミラーリングのミラーポートを指定します。最大 2 件の物理ポート，または最大 1 件のポートチャネルインタフェースを指定できます。

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
   <interface id list> :「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. 本機能を使用する場合は，フロー検出モードをデフォルトコンフィグレーション（コマンド未設定）のままにしてください。
   フロー検出モード変更後に本機能を使用する場合は，フロー検出モードをデフォルトコンフィグレーションに戻した後，装置再起動が必要です。
   本機能を使用後にフロー検出モードを変更する場合は，本機能のコンフィグレーションを削除した後，装置再起動が必要です。
2. 本機能と QoS フローリストを併用することはできません。
   QoS フローリスト使用後に本機能を使用する場合は，QoS フローリストのコンフィグレーションを削除した後，装置再起動が必要です。
   本機能を使用した後に QoS フローリストを使用する場合は，本機能のコンフィグレーションを削除し

た後，装置再起動が必要です。

3. 本機能と他のミラーリング機能を併用する場合の収容条件やミラーポートの注意事項など，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］

flow detection mode

monitor session source

white-list monitor destination interface

monitor session source

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 no.> source interface <interface id list> [{rx | tx | both}] destination interface <interface id list>【スタック動作時】

monitor session <session no.> source interface <interface id list> [{rx | tx | both}] destination interface {<interface id list> | port-channel <channel group>}【スタンドアロン動作時】

情報の変更

monitor session <session no.> source {interface add <interface id list> | interface remove <interface id list>}【スタンドアロン動作時】

情報の削除

no monitor session <session no.> source

［入力モード］

(config)

［パラメータ］

<session no.>

ポートミラーリングのセッション番号を指定します。

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
   【スタック動作時】1
   【スタンドアロン動作時】1 ～ 4

interface <interface id 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。

interface add <interface id list>【スタンドアロン動作時】

ポートミラーリングのモニター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
   「パラメータに指定できる値」を参照してください。

interface remove <interface id list>【スタンドアロン動作時】

ポートミラーリングのモニター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
   「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 <interface id list>【スタック動作時】

destination interface {<interface id list> | port-channel <channel group>}【スタンドアロン動作時】

ポートミラーリングのミラーポートを指定します。

スタック動作時は，最大 2 件の物理ポートを指定できます。

スタンドアロン動作時は，最大 2 件の物理ポート，または最大 1 件のポートチャネルインタフェースを指定できます。

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
   <interface id list> :「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. 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。
2. スタンドアロン動作時は，ミラーポートについて次の制限があります。
   - 受信フレーム（rx/both）に対するミラーポートの合計：4（装置全体）
   - 1 つのモニターポートの受信フレーム（rx/both）に対するミラーポート：最大 2 ポート
   - 送信フレーム（tx/both）に対するミラーポートの合計：2（装置全体）
   - ポートチャネルインタフェースのミラーポート：ポートチャネルインタフェース全体を 1 件として数えます。ポートチャネルインタフェースに属するポートは，ミラーポートの収容条件に影響しません。

   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。
3. 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

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に，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］

ip icmp monitor destination

monitor session source

white-list monitor destination

43 ポリシーベースミラーリング

monitor session filter

monitor session filter

モニターポートに適用するポリシーベースミラーリングのフロー検出条件（アクセスリスト）を設定します。

［入力形式］

情報の設定・変更

monitor session <session no.> filter {mac | ip} access-group <access list name>

情報の削除

no monitor session <session no.> filter

［入力モード］

(config)

［パラメータ］

<session no.>

ポリシーベースミラーリングに適用する monitor session source コマンドのセッション番号を指定します。最大 2 セッションまで指定できます。

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
   【スタック動作時】 1
   【スタンドアロン動作時】 1 ～ 4

{mac | ip}

設定するアクセスリストの種別を指定します。

mac

MAC フィルタを設定する場合に指定します。

ip

IPv4 アドレスフィルタまたは IPv4 パケットフィルタを設定する場合に指定します。

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
   mac，ip

<access list name>

設定する MAC フィルタ，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
   4 ～ 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］

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. 本コマンドを設定する前に，flow detection mode コマンドで layer2-1-mirror または layer2-2-mirror を設定してください。
2. 本コマンドと同じセッション番号で使用する monitor session source コマンドのトラフィック方向は，"rx"（受信フレームをミラーする）を指定してください。"tx" や "both" は使用できません。

［関連コマンド］

flow detection mode

ip access-list extended

ip access-list standard

mac access-list extended

monitor session source

44 コンフィグレーション編集時のエラーメッセージ

44.1　コンフィグレーション編集時のエラーメッセージ

44.1　コンフィグレーション編集時のエラーメッセージ

スタック動作時，<IF#> は，スイッチ番号，インタフェースポート番号 <switch no.>/<IF#> を表示します。

44.1.1　共通

表 44-1　共通のエラーメッセージ

メッセージ	内容
<function 1> and <function 2> are mutually exclusive, unless receive control is set to fine.	system receive control fine 未設定のとき，white-list enable と ip igmp snooping (global) は排他です。
	white-list enable と ip igmp snooping (global) がともに設定されているとき，system receive control coarse，または no system receive control は設定できません。
<function 1> and <function 2> are mutually exclusive.	機能 1 と機能 2 は排他です。 <function 1> と <function 2> には以下が表示されます。 White-list IGMP snooping MLD snooping Dot1x Web-authentication MAC-authentication DHCP snooping Flow detection mode layer2-3 syslog TCP NETCONF querier mrouter discovery no mac-address-table learning Mirroring to a port-channel Tagged mirroring Access-redirect CFM White-list packet mode 2 White-list packet tcp/udp on port <IF#>
<Start allocation> can set only 0.	<Start allocation> は 0 だけ設定可能です。
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。
Can not change it because data is not corresponding.	該当するデータがないため，変更できません。 変更対象データがあるか確認してください。
Cannot change mdix.	SFP ポートで自動 MDIX 機能の設定はできません。
Cannot execute.	実行できません。
Can't execute.	
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。

メッセージ	内容
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。
Cannot set Traffic-class and DSCP at the same time.	Traffic-class 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。
Can not delete it because data is not corresponding.	一致するデータがない，または重複して指定しているので，削除できません。 削除対象データがあるか，または重複して指定していないか確認してください。
Can't execute command it because data is not corresponding.	一致するデータがないため，コマンドを実行できません。
Command chaining not allowed.	２つのコマンドを続けて入力できません。
Command process stopped because master has changed.	スタックのマスタスイッチ交替が発生したため，コマンド処理を中断しました。
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。
Illegal combination 'xxx' and 'yyy'.	パラメータ 'xxx' とパラメータ 'yyy' は同時指定できません。
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 'xxxx', because stack is disabled.	スタックが無効なため，指定したパラメータは設定できません。
Invalid parameter 'xxxx', because stack is enabled.	スタックが有効なため，指定したパラメータは設定できません。
Invalid parameter 'xxx'.	パラメータ 'xxx' が無効です。
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。
License key is not installed.	ライセンスキーが未設定です。
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。
Maximum number of entries are already defined.	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。
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。

メッセージ	内容
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。
Prohibited by the prior use of a competing feature.	過去に排他機能が使用されたため，本機能を使用するには装置再起動が必要です。 なお，startup-config に排他機能のコマンドが登録されている場合は，排他機能のコマンドを削除してから装置を再起動してください。
Read only.	読み込み専用です。
Resource unavailable.	資源が無効です。
Some parameters are insufficient.	パラメータが不足しています。
Specified parameter 'xxxx' is not supported with this model.	パラメータ 'xxxx' はこのモデルでは未サポートです。
String must be more than 0 characters.	文字列は 1 文字以上でなければなりません。
String too long.	文字列が長すぎます。
The command execution failed, because "xxx" is executing.	xxx によってコマンドまたは機能実行中です。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。 運用コマンド show config-lock-status，who コマンドで確認してください。
The different name is already defined.	異なる名前がすでに設定されています。
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。
The sequence number exceeded the maximum value. Try "resequence" Command.	シーケンス番号が最大値を超えました。 エントリの指定を行うには，resequence コマンドを実行してから，再度このエントリの指定を行ってください。
This command cannot configure in this port.	本コマンドはこのポートには設定できません。
This command cannot configure, because stack is enabled.	このコマンドはスタック有効のため設定できません。
This command is not supported with this model.	このコマンドはこのモデルでは未サポートです。
This command not execute, because it is the command-limited state.	このコマンドはコマンド限定状態のため実行できません。
This command not execute, because stack is enabled.	このコマンドはスタック有効のため実行できません。
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。

44.1.2　スタック情報

表 44-2　スタックのエラーメッセージ

メッセージ	内容
Cannot configure switch <switch no.> because switch provision is not configured.	指定したスイッチ番号は switch provision で設定していないため，設定できません。 <switch no.>：スイッチ番号
Cannot configure switch <switch no.> provision configuration because stack is active.	指定したスイッチ番号はスタック動作中のため実行できません。 スイッチ番号を確認してください。 <switch no.>：スイッチ番号
Can't delete switch <switch no.> provision configuration because the other user is editing in the interface [ten]gigabitethernet mode configuration of the switch <switch no.>.	switch <switch no.> provision 設定は，当該装置のインタフェースモードを編集中のため削除できません。 <switch no.>：スイッチ番号
Relations between switchport mode stack and <Configuration> are inconsistent.	下記以外のコマンドは，switchport mode stack と同じポートに設定できません。 • description • no snmp trap link-status • shutdown • switchport mode • switchport stack cost • speed • duplex
Relations between switchport mode stack and mac-address-table static interface are inconsistent.	switchport mode stack で指定したポートは，mac-address-table static の interface に指定できません。
Relations between switchport mode stack and monitor session are inconsistent.	switchport mode stack で指定したポートは，ポートミラーリングのポートに指定できません。
Relations between switchport mode stack and switchport backup interface are inconsistent.	switchport mode stack で指定したポートは switchport backup のインタフェースに指定できません。
Relations between switchport mode stack and switchport isolation interface are inconsistent.	switchport mode stack で指定したポートは switchport isolation の interface に指定できません。
Relations between switchport mode stack and white-list data interface are inconsistent.	switchport mode stack で指定したポートは white-list data の interface に指定できません。
set stack enable is necessary for switchport mode stack.	switchport mode stack 設定にはスタック機能を有効にする必要があります。
stack enable is necessary for this command.	このコマンドの設定には，スタック機能を有効にする必要があります。
switchport mode stack cannot be set on this interface.	switchport mode stack はこのインタフェースには設定できません。
This command cannot configure, because stack is enabled.	スタック動作中のため，指定したコマンドを設定できません。

44.1.3　ログインセキュリティと RADIUS 情報

表 44-3　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
<Group name> is not available.	指定した RADIUS サーバグループ名を設定できません。 <Group name> : RADIUS サーバグループ名
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。

44.1.4　時刻の設定と NTP 情報

表 44-4　時刻の設定と NTP のエラーメッセージ

メッセージ	内容
Can't set this command, because NTP-related command is set.	本コマンドを設定または削除する場合は，下記のコンフィグレーションをすべて削除したあとに切り替えてください。 <no sntp client 設定時 > • ntp interval • ntp broadcast client(global) • ntp server <sntp client で削除時 > • ntp authenticate • ntp authentication-key • ntp broadcast • ntp broadcast client(global) • ntp broadcast client(interface) • ntp broadcastdelay • ntp master • ntp peer • ntp server • ntp trusted-key
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。
This command cannot configure, because SNTP client is effective.	SNTP クライアントが有効なのでこのコマンドの設定はできません。
This command is SNTP client device dependent command.	このコマンドは SNTP クライアント専用コマンドです。
This command not configure, because specified an invalid parameter.	NTP 動作モードでは，指定できないパラメータが設定されています。

44.1.5　装置の管理情報

表 44-5　装置の管理情報のエラーメッセージ

メッセージ	内容
IGMP snooping requires 'system receive control fine'.	system receive control が fine でないため設定できません。
The lower limit must not be greater than the upper limit.	<lower limit> が <upper limit> より大きくなっています。 <lower limit> は，<upper limit> 以下の値を設定してください。
Too many ARP insepction VLANs for the fine mode.	ダイナミック ARP 検査の設定 VLAN 数が収容条件を超過しているため，system receive control fine に変更できません。
Too many authentication access-list entries for the fine mode.	認証専用 IPv4 アクセスリストに指定できるフィルタ条件数が収容条件を超過しているため，system receive control fine に変更できません。
Too many DHCP snooping VLANs for the fine mode.	DHCP snooping の設定 VLAN 数が収容条件を超過しているため，system receive control fine に変更できません。
Too many IGMP or MLD snooping VLANs for the fine mode.	IGMP snooping または MLD snooping の設定 VLAN 数が収容条件を超過しているため，system receive control fine に変更できません。
Too many IP addresses for the fine mode.	IP アドレスの設定数が収容条件を超過しているため，system receive control fine に変更できません。

44.1.6　省電力機能情報

表 44-6　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。

44.1.7　イーサネット情報

表 44-7　イーサネット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。
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。
Port <IF#> cannot be simultaneously a link-relay and a source.	同じポートがリンク状態中継先ポートとリンク状態中継元ポートに設定されています。
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。

44.1.8　リンクアグリゲーション情報

表 44-8　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：This command is different from authentication configuration in channel-group port.	認証共通の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。
interface：This command is different from the mac-authentication configuration in the channel-group port.	MAC 認証の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。
interface：This command is different from the web-authentication configuration in the channel-group port.	Web 認証の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。
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].	インタフェースポート番号の指定が不正です。
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。

メッセージ	内容
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。
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。

44.1.9　MAC アドレステーブル情報

表 44-9　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。

44.1.10　VLAN 情報

表 44-10　VLAN のエラーメッセージ

メッセージ	内容
<Configuration>：maximum number which can be used is exceeded.	<Configuration>が最大エントリ数を超えたため生成できません。 ・ vlan ・ vlan (protocol-based)【スタック動作時】 ・ switchport protocol vlan【スタック動作時】
Cannot change vlan configuration referred by flow configuration.	指定 vlan コンフィグレーションはフィルタまたは QoS コンフィグレーションで指定されているため，変更できません。 指定 vlan コンフィグレーションを変更するには，指定 vlan コンフィグレーションに設定されているフィルタまたは QoS コンフィグレーションを削除してください。

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
Duplicate translated id.	指定した VLAN Tag の値は，他の VLAN で使用中です。
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。
interface：VLAN is not Port VLAN.	指定した VLAN はポート VLAN ではありません。 ポート VLAN を指定してください。
interface：VLAN is not Port VLAN or MAC VLAN.	指定した VLAN はポート VLAN または MAC VLAN ではありません。 ポート VLAN または MAC VLAN を指定してください。
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。
Not found <VLAN ID>.	指定した VLAN ID は設定できません。 <VLAN ID>：VLAN ID
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 access-list and dot1q-tunnel are inconsistent.	VLAN トンネリングを設定している場合，VLAN インタフェースの送信側へアクセスリストを適用できません。 また，イーサネットインタフェースの送信側へ適用するアクセスリストのフィルタ条件には，VLAN 条件を指定できません。
Relations between access-list and vlan mapping are inconsistent.	Tag 変換を設定している場合，VLAN インタフェースの送信側へアクセスリストを適用できません。 また，イーサネットインタフェースの送信側へ適用するアクセスリストのフィルタ条件には，VLAN 条件を指定できません。
Relations between igmp snooping and vlan mapping are inconsistent.	IGMP snooping を設定している VLAN でトランクポートに vlan mapping を指定できません。
Relations between igmp snooping and vlan-tunneling are inconsistent.	IGMP snooping と VLAN トンネリングを同時に指定できません。
Relations between ip dhcp snooping configuration and vlan mapping configuration are inconsistent.	ip dhcp snooping vlan を設定している VLAN でトランクポートに vlan mapping を設定できません。
Relations between ip dhcp snooping configuration and vlan-tunneling configuration are inconsistent.	ip dhcp snooping vlan と VLAN トンネリングを同時に設定できません。
Relations between mac-based and vlan-tunneling-enable are inconsistent.	MAC VLAN と VLAN トンネリングは同時に設定できません。
Relations between mld snooping and vlan mapping are inconsistent.	MLD snooping を設定している VLAN でトランクポートに vlan mapping を指定できません。
Relations between mld snooping and vlan-tunneling are inconsistent.	MLD snooping と VLAN トンネリングを同時に指定できません。
Relations between protocol-based and vlan-tunneling-enable are inconsistent.	プロトコル VLAN と VLAN トンネリングは同時に設定できません。
Relations between the dot1x configuration and the VLAN mode configuration are inconsistent.	VLAN モードがトンネリングモードのポートに対してポート単位認証の設定はできません。

メッセージ	内容
Relations between the mac-authentication configuration and the VLAN mode configuration are inconsistent.	VLAN モードがトンネリングモードまたはプロトコル VLAN モードのポートに対して，MAC 認証の設定はできません。
Relations between the web-authentication configuration and the VLAN mode configuration are inconsistent.	VLAN モードがトンネリングモードまたはプロトコル VLAN モードのポートに対して Web 認証の設定はできません。
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。
Relations between vlan-mapping and dot1q ethertype configuration are inconsistent.	Tag 変換と TPID は同時に指定できません。
Relations between vlan-tunneling and spanning-tree configuration are inconsistent.	VLAN トンネリ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。 VLAN トンネリ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。
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。
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

メッセージ	内容
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。

44.1.11　スパニングツリー情報

表 44-11　スパニングツリーのエラーメッセージ

メッセージ	内容
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。
Relations between vlan-tunneling and spanning-tree configuration are inconsistent.	VLAN トンネリ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。 VLAN トンネリ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。
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

44.1.12　Ring Protocol 情報

表 44-12　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.	最大設定数を超えています。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>: shared-edge port is already defined in another ring-port.	共有ポートは，すでに他方のリングポートに対して shared-edge 設定されています。 別のポートを shared-edge 共有ポートに設定する場合は，設定済みの共有ポートを削除してください。 <Ring ID>：リング ID
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 virtual-link.	指定された VLAN はすでに仮想リンクに設定されています。 仮想リンクから該当 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

メッセージ	内容
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-virtual-link-<Link 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。 <Link ID>：仮想リンク ID <VLAN ID>：VLAN 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。 <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 axrp-virtual-link when multi-fault-detection is configured.	多重障害監視機能の設定があるため，仮想リンクが設定できません。
Cannot configure multi-fault-detection when axrp-virtual-link is configured.	仮想リンクの設定があるため，多重障害監視機能が設定できません。
Cannot configure when forwarding-delay-time is running.	forwarding-delay-time が動作中のため，コンフィグレーションを設定できません。

44.1.13　IGMP snooping 情報

表 44-13　IGMP snooping のエラーメッセージ

メッセージ	内容
IGMP snooping requires 'system receive control fine'.	system receive control が fine でないため設定できません。
Maximum number of VLAN are already defined, <VLAN ID> igmp snooping can not enable.【Ver.4.5 未満】	IGMP snooping で指定できる vlan は最大 32 個です。32 を超えて設定できません。【Ver.4.5 未満】 <VLAN ID>：VLAN ID
Relations between igmp snooping and vlan-tunneling are inconsistent.	IGMP snooping と VLAN トンネリングを同時に設定できません。
Relations between igmp snooping and vlan mapping are inconsistent.	IGMP snooping を設定している VLAN でトランクポートに vlan mapping を設定できません。

44.1.14　MLD snooping 情報

表 44-14　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.【Ver.4.5 未満】	MLD snooping で指定できる vlan は最大 32 個です。32 を超えて設定できません。【Ver.4.5 未満】 <VLAN ID> : VLAN ID
Relations between ip address and mld snooping source address are inconsistent.	同一の VLAN に IPv6 機能有効設定と MLD snooping の送信元 IPv6 アドレス設定を同時指定できません。
Relations between mld snooping and vlan-tunneling are inconsistent.	MLD snooping と VLAN トンネリングを同時に設定できません。
Relations between mld snooping and vlan mapping are inconsistent.	MLD snooping を設定している VLAN でトランクポートに vlan mapping を設定できません。

44.1.15　IPv4・ARP・ICMP 情報

表 44-15　IPv4・ARP・ICMP のエラーメッセージ

メッセージ	内容
ip : Can't change ARP entry.	ARP の設定は変更できません。削除してから再設定してください。
ip : Inconsistency has occurred in a setting of IP address and ARP.	IP 情報で設定したアドレスと ARP 情報で設定したアドレスのネットワークアドレスに矛盾が生じています。 ネットワークアドレスを正しく指定してください。
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 ARP entry.	IP 情報で設定したアドレスと ARP 情報で設定した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指定してください。
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指定してください。
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 : Only default-gateways are supported.	スタック機能が有効です。 デフォルトゲートウェイを指定してください。
ip : The number of pieces of the ARP entry exceeds the capacity of this system.	ARP テーブルのエントリが装置の最大エントリ数を超えています。
ip[<VLAN ID>] : Can't delete a primary IP address when a secondary IP address is existing.	セカンダリ IP アドレスが存在しています。 セカンダリ IP アドレスを削除したあと，プライマリ IP アドレスを削除してください。 <VLAN ID> : VLAN ID
ip[<VLAN ID>] : Can't delete IP configuration with arp configuration.	ARP の情報が存在しています。 ARP 情報を削除したあと，IP 情報を削除してください。 <VLAN ID> : VLAN ID
ip[<VLAN ID>] : Can't delete IP configuration with dhcp configuration.	DHCP サーバ設定が存在しています。 DHCP サーバ設定を削除したあと，IP 情報を削除してください。 <VLAN ID> : VLAN ID

メッセージ	内容
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あと，IP 情報を削除してください。 <VLAN ID> : VLAN ID
ip[<VLAN ID>]：Can't set a secondary IP address on a interface which does not have a primary IP address.	プライマリ IP アドレスの設定のないインタフェースに，セカンダリ IP アドレスを設定しようとしています。 先にプライマリ IP アドレスを設定してください。 <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>]：Interface not found.	指定したインタフェースが見つかりません。 インタフェースの設定を確認してください。 <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

44.1.16　IPv6・NDP・ICMPv6 情報

表 44-16　IPv6・NDP・ICMPv6 情報のエラーメッセージ

メッセージ	内容
ip：Can't change NDP entry.	NDP 情報の設定は変更できません。削除してから再設定してください。
ip：IPv6 address is duplicate between interface and default gateway entry.	IP 情報で設定したアドレスとデフォルトゲートウェイ情報で設定した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指定してください。
ip：IPv6 address is duplicate between interface and NDP entry.	IP 情報で設定したアドレスと NDP 情報で設定した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指定してください。
ip：The number of pieces of the NDP entry exceeds the capacity of this system.	NDP テーブルのエントリが装置の最大エントリ数を超えています。
ip[<VLAN ID>]：Duplicate prefix.	同一プレフィックスの IP アドレスが設定されています。 プレフィックスがユニークになるように設定してください。 <VLAN ID> : VLAN ID
ip[<VLAN ID>]：Interface not found.	指定したインタフェースが見つかりません。 インタフェースの設定を確認してください。 <VLAN ID> : VLAN ID
ip[<VLAN ID>]：Invalid IPv6 address -- <value1>	IPv6 アドレスまたは IPv6 リンクローカルアドレスが不正です。 正しい IPv6 アドレスを設定してください。 <value1>：不正な値
Relations between ip address and mld snooping source address are inconsistent.	同一の VLAN に IPv6 機能有効設定と MLD snooping の送信元 IPv6 アドレス設定を同時指定できません。

44.1.17　DHCP サーバ機能情報

表 44-17　DHCP サーバ機能のエラーメッセージ

メッセージ	内容
<Pool name> overlaps with other entries.	同一 pool 内で network と host ／ hardware-address を同時に設定することはできません。どちらか一方を削除後，設定してください。
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。
Exceeded the number of maximums that it was managed with IP dhcp pool.	最大管理サブネット数を超えました。network と host 設定を見直してください。
Host is already used.	同一 IP アドレスの host がすでに使用されています。 異なる IP アドレスを指定してください。
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。
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-HOST>	設定可能な固定 IP 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。
Maximum number of entries are already defined. <DHCP_SUBNET>	設定可能なサブネット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。
This configuration has already been set.	このコンフィグレーションはすでに設定済みです。
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

44.1.18　フロー検出モード情報

表 44-18　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，受信側フロー検出モードを変更できません。 ・受信側インタフェースにアクセスリスト適用 ・受信側インタフェースに QoS フローリスト適用 ・access-redirect http port ・monitor session filter ・white-list enable 受信側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。
Cannot change the flow detection out mode.	アクセスリストまたは QoS フローリストが送信側インタフェースに適用されているため，送信側フロー検出モードを変更できません。 送信側フロー検出モードを変更したい場合は，適用されているリストをすべて削除してください。

44.1.19　アクセスリスト情報

表 44-19　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.	受信側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。 受信側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.	受信側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。 受信側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
Cannot attach this list because flow detection mode layer2-3.	受信側フロー検出モードが layer2-3 の場合には，このアクセスリストは適用できません。 受信側フロー検出モードが layer2-3 のとき，IPv4 アクセスリストおよび IPv6 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 ipv6 traffic-filter コマンド
Cannot attach this list because flow detection mode layer2-1-mirror.	受信側フロー検出モードが layer2-1-mirror の場合には，このアクセスリストは適用できません。 受信側フロー検出モードが layer2-1-mirror 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-mirror.	受信側フロー検出モードが layer2-2-mirror の場合には，このアクセスリストは適用できません。 受信側フロー検出モードが layer2-2-mirror 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

メッセージ	内容
Cannot attach this list because flow detection out mode layer2-1-out.	送信側フロー検出モードが layer2-1-out の場合には，このアクセスリストは適用できません。 送信側フロー検出モードが layer2-1-out 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 out mode layer2-2-out.	送信側フロー検出モードが layer2-2-out の場合には，このアクセスリストは適用できません。 送信側フロー検出モードが layer2-2-out 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。
Range-Start must be less than Range-End.	範囲指定の開始値が終了値以上になっています。 範囲指定では，開始値は終了値より小さい値を設定してください。
Relations between access-list and dot1q-tunnel are inconsistent.	VLAN トンネリングを設定している場合，VLAN インタフェースの送信側へアクセスリストを適用できません。 また，イーサネットインタフェースの送信側へ適用するアクセスリストのフィルタ条件には，VLAN 条件を指定できません。
Relations between access-list and vlan mapping are inconsistent.	Tag 変換を設定している場合，VLAN インタフェースの送信側へアクセスリストを適用できません。 また，イーサネットインタフェースの送信側へ適用するアクセスリストのフィルタ条件には，VLAN 条件を指定できません。
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。
The maximum number of TCP/UDP port entries are exceeded.	TCP/UDP ポート番号の範囲指定のエントリが最大数を超えています。 TCP/UDP ポート番号の範囲指定のエントリは，最大 16 パターンです。 なお，このコンフィグレーションファイルでの使用エントリ数および空きエントリ数は，運用コマンド show system で確認できます。
This list cannot be set for out.	このアクセスリストは送信側フロー検出モード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 Class が指定されている場合には，そのアクセスリストは送信側フロー検出モードには適用できません。
This list cannot be set to the outbound because the list includes TCP/UDP port range entry.	このアクセスリストのフロー検出条件はこのインタフェースへの適用はできません。 検出条件に送信元ポート番号範囲指定または宛先ポート番号範囲指定を含まないリストが送信側インタフェースに適用できます。 次のコマンドが使用できます。 ip access-group コマンド ipv6 traffic-filter コマンド
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。

メッセージ	内容
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。

44.1.20　QoS 情報

表 44-20　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.	受信側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。 受信側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.	受信側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。 受信側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
Cannot attach this list because flow detection mode layer2-3.	受信側フロー検出モードが layer2-3 の場合には，この QoS フローリストは適用できません。 受信側フロー検出モードが layer2-3 のとき，IPv4 QoS フローリストおよび IPv6 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 ipv6 qos-flow-group コマンド
Cannot attach this list because flow detection mode layer2-1-mirror. Cannot attach this list because flow detection mode layer2-2-mirror.	受信側フロー検出モードが layer2-1-mirror，layer2-2-mirror の場合には，QoS フローリストを適用できません。 QoS フローリストを適用する場合は，受信側フロー検出モードを layer2-1，layer2-2，layer2-3 のいずれかで設定してください。
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。

メッセージ	内容
Min-burst must be less than max-burst.	最低帯域バーストサイズが最大帯域バーストサイズ以上になっています。 最低帯域バーストサイズは，最大帯域バーストサイズより小さい値を設定してください。
Minrate must be less than maxrate.	最低帯域値が最大帯域値以上になっています。 最低帯域値は，最大帯域値より小さい値を設定してください。
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。
Range-Start must be less than Range-End.	範囲指定の開始値が終了値以上になっています。 範囲指定では，開始値は終了値より小さい値を設定してください。
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 maximum number of TCP/UDP port entries are exceeded.	TCP/UDP ポート番号の範囲指定のエントリが最大数を超えています。 TCP/UDP ポート番号の範囲指定のエントリは最大 16 パターンです。 なお，このコンフィグレーションファイルでの使用エントリ数および空きエントリ数は，運用コマンド show system で確認できます。
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。
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。

44.1.21　レイヤ 2 認証共通情報

表 44-21　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 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。
	該当ポートはチャネルグループに属しているため設定（あるいは削除）できません。ポートチャネルインタフェースに設定（あるいは削除）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 ip access-group 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。
	該当ポートはチャネルグループに属しているため設定（あるいは削除）できません。ポートチャネルインタフェースに設定（あるいは削除）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 authentication 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。
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。
max-user: 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

44.1.22　IEEE802.1X 情報

表 44-22　IEEE802.1X のエラーメッセージ

メッセージ	内容
dot1x(xxxxx): Cannot set " dot1x authentication " command because user-group configuration is set now.	interface xxxxx にユーザ ID 別認証方式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。 web-authentication user-group コマンド設定を削除してください。 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(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

メッセージ	内容
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(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/ passive-method.	interface xxxxx の端末検出動作が disable または passive 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
dot1x(xxxxx): Cannot set "dot1x port-control" because switchport mode is not access-mode.	interface xxxxx の switchport mode が access または MAC VLAN のどちらでもないため，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 port-control" because of a wrong "switchport mode".	interface xxxxx(ethernet <IF#> または port-channel <Channel group#>) の switchport mode が不適切なため，IEEE802.1X 認証の設定はできません。 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/passive" 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 または passive 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

メッセージ	内容
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: 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。
Relations between the dot1x configuration and the mirror configuration are inconsistent.	ミラーポートに対して IEEE802.1X は設定できません。
Relations between the dot1x configuration and the VLAN mode configuration are inconsistent.	VLAN モードがトンネリングモードのポートに対してポート単位認証の設定はできません。
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，y：1, 2, 3, 4

44.1.23　Web 認証情報

表 44-23　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 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
interface：Relations between the web-authentication configuration and the 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。
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 the web-authentication configuration and the vlan mode configuration are inconsistent.	指定ポートはトンネリングポートまた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。

メッセージ	内容
interface : Relations between user-group configuration and authentication list configuration(s) are inconsistent.	ユーザ ID 別認証方式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。 web-authentication user-group コマンド設定を削除してください。
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。
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 authentication list configuration(s) and user-group configuration are inconsistent.	ポート別認証方式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 • web-authentication authentication • mac-authentication authentication

44.1.24　MAC 認証情報

表 44-24　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 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。
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 vlan mode configuration are inconsistent.	指定ポートはトンネリングポートまた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 user-group configuration and authentication list configuration(s) are inconsistent.	ユーザ ID 別認証方式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。 web-authentication user-group コマンド設定を削除してください。
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。
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。

44.1.25　マルチステップ認証情報

表 44-25　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 authentication 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。
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

44.1.26　DHCP snooping 情報

表 44-26　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 there are a lot of entries in mac-vlan.	MAC VLAN の端末数が 500 端末より多く登録されているため，DHCP snooping を設定できません。 MAC VLAN の端末数を 500 端末以下にしてから設定してください。
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。
	ip dhcp snooping vlan information option format-type circuit-id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 dhcp snooping configuration and vlan mapping configuration are inconsistent.	ip dhcp snooping vlan を設定している VLAN でトランクポートに vlan mapping を設定できません。
Relations between ip dhcp snooping configuration and vlan-tunneling configuration are inconsistent.	ip dhcp snooping vlan と VLAN トンネリングを同時に設定できません。

メッセージ	内容
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。

44.1.27　ホワイトリスト情報

表 44-27　ホワイトリストのエラーメッセージ

メッセージ	内容
Cannot change the white-list packet mode.	以下が設定されているため，ホワイトパケットリスト動作モードを変更できません。 • white-list enable ・ white-list data "p～" ※ ホワイトパケットリスト動作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。 注 ※　ホワイトパケットリストだけが対象です。ホワイトアドレスリストは影響ありません。
Confliction between port mirroring and white-list mirroring.	destination interface をポートミラーリングで使用しているためミラーポートに設定できません。
Invalid white-list data.	white-list data コマンドの入力内容が不正です。
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-address-table are inconsistent.	destination interface を mac-address-table 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 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。
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。
Port <IF#> cannot be simultaneously a source and a destination.	指定されたミラーポートは，ポートミラーリング (ICMP 限定ミラーリングを含む) のモニターポートとして設定されています。
Too many destinations for port <IF#>.	ポートミラーリングの受信フレーム（rx/both) のミラーポートと ICMP 限定ミラーリングのミラーポート，およびホワイトリストのミラーポートの合計が，ポートごとの収容条件を超えているため設定できません。
Too many destinations.	ポートミラーリングの受信フレーム（rx/both) のミラーポートと ICMP 限定ミラーリングのミラーポート，およびホワイトリストのミラーポートの合計が，装置全体のミラーポートの収容条件を超えているため設定できません。

44.1.28　特定端末への Web 通信不可表示機能情報

表 44-28　特定端末への 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
Access-redirect requires 'system receive control fine'.	system receive control が fine でないため設定できません。
Cannot change access-redirect because access-group is set.	ip access-group in が設定されているため，access-redirect を変更できません。
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.	この受信側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，受信側フロー検出モードに layer2-2，layer2-3，または layer2-2-mirror を設定してください。

44.1.29　アップリンク・リダンダント情報

表 44-29　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
Relations between flush-request transmit and mac-address-table update transmit are inconsistent.	フラッシュ制御フレーム送信と MAC アドレスアップデートフレーム送信は同時に設定できません。
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。

44.1.30　ストームコントロール情報

表 44-30　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。

44.1.31　L2 ループ検知情報

表 44-31　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。

44.1.32　CFM 情報

表 44-32　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

メッセージ	内容
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。
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

44.1.33　SNMP 情報

表 44-33　SNMP 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。
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。
Maximum number of entries are already defined.	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。

メッセージ	内容
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 : 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。
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。

44.1.34　ログ出力情報

表 44-34　ログ出力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。
logging : Can not delete it because data is not corresponding.	イベント種別が設定されていないため，削除できません。
Relations between IPv6 address and tcp are inconsistent.	IPv6 アドレスと TCP は同時に指定できません。
too much number of the host.	出力先の最大エントリを超えたため，設定できません。

44.1.35　sFlow 統計情報

表 44-35　sFlow 統計のエラーメッセージ

メッセージ	内容
Can not delete it because data is not corresponding.	一致するデータがない，または重複して指定しているので，削除できません。 削除対象データがあるか，または重複して指定していないか確認してください。
Maximum number of entries are already defined.	コレクタの設定数が最大値を超えています。 コレクタの設定数を 4 台以下にして利用してください。

メッセージ	内容
Only either of the following commands "sflow forward egress" or "sflow forward ingress" can be configured at a time on this device.	装置として sflow forward egress か sflow forward ingress のどちらかだけを指定できます。 送信トラフィックを監視対象にしたい場合は，他ポートの sflow forward ingress 指定をすべて削除してから，監視ポートに再度設定してください。 受信トラフィックを監視対象にしたい場合は，他ポートの sflow forward egress 指定をすべて削除してから，監視ポートに再度設定してください。
This system doesn't support "sflow forward egress" the command.	本装置では sflow forward egress コマンドはサポートしていないため，使用できません。

44.1.36　ポートミラーリング情報

表 44-36　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
Confliction between port mirroring and white-list mirroring.	destination interface をホワイトリストのミラーポートで使用しているためミラーポートに設定できません。
Duplicated policy based mirroring destinations.	複数のセッションでポリシーベースミラーリングのミラーポートが完全同一となる設定はできません。 ただし，セッション間でポリシーベースミラーリングのモニターポートが完全に分離しているときは可能です。
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 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。
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。
Port <IF#> cannot be simultaneously a source and a destination.	同じポートがモニターポートとミラーポートに設定されています。 なお，セッション 1 内のモニターポートとミラーポートが競合する場合は本メッセージが表示されませんので，競合しないように注意してください。
Port <IF#> is a present source.	add で指定したポートは，当該セッションですでにモニターポートとして設定されています。
Port <IF#> is not a present source.	remove で指定したポートは，当該セッションのモニターポートに設定されていません。
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。
Relations between the direction and policy based mirroring are inconsistent.	同じセッション番号の monitor session filter が設定されているため，rx 以外の方向は設定できません。
The specified VLAN ID is already in use.	指定された VLAN 番号は既に使用中です。
Too many destinations for port <IF#> rx.	受信フレーム（rx/both）のミラーポートがモニターポートごとの収容条件を超えているため設定できません。
Too many destinations for port <IF#>.	ICMP 限定ミラーリングのミラーポートと受信フレーム（monitor session source rx/both）のミラーポート，およびホワイトリストのミラーポートの合計が，モニターポートごとのミラーポートの収容条件を超えるため設定できません。

メッセージ	内容
Too many destinations for rx.	受信フレーム（rx/both）のミラーポートが収容条件を超えているため設定できません。
Too many destinations for tx.	送信フレーム（tx/both）のミラーポートが収容条件を超えているため設定できません。
Too many destinations.	ICMP 限定ミラーリングのミラーポートと受信フレーム（monitor session source rx/both）のミラーポート，およびホワイトリストのミラーポートの合計が，装置全体のミラーポートの収容条件を超えるため設定できません。

44.1.37　ポリシーベースミラーリング情報

表 44-37　ポリシーベースミラーリング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. Cannot attach this list because flow detection mode layer2-2. Cannot attach this list because flow detection mode layer2-3.	受信側フロー検出モードが layer2-1，layer2-2，layer2-3 の場合は，monitor session filter コマンドを設定できません。 monitor session filter コマンドを設定する場合は，受信側フロー検出モードを layer2-1-mirror，または layer2-2-mirror で設定してください。
Cannot attach this list because flow detection mode layer2-1-mirror.	受信側フロー検出モードが layer2-1-mirror の場合には，このアクセスリストは適用できません。 受信側フロー検出モードが layer2-1-mirror のとき，MAC アクセスリストを適用できます。 次のコマンドが使用できます。 monitor session filter コマンド（mac access-group 指定）
Cannot attach this list because flow detection mode layer2-2-mirror.	受信側フロー検出モードが layer2-2-mirror の場合には，このアクセスリストは適用できません。 受信側フロー検出モードが layer2-2-mirror のとき，IPv4 アクセスリストを適用できます。 次のコマンドが使用できます。 monitor session filter コマンド（ip access-group 指定）
Duplicated policy based mirroring destinations.	複数のセッションでポリシーベースミラーリングのミラーポートが完全同一となる設定はできません。 ただし，セッション間でポリシーベースミラーリングのモニターポートが完全に分離しているときは可能です。
Relations between the direction and policy based mirroring are inconsistent.	同じセッション番号の monitor session source コマンドに rx 以外が指定されているため，ポリシーベースミラーリングに適用できません。
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。
The maximum number of TCP/UDP port entries are exceeded.	TCP/UDP ポート番号の範囲指定のエントリが最大数を超えています。 TCP/UDP ポート番号の範囲指定のエントリは，最大 16 パターンです。 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，運用コマンド show system で確認できます。

索引

A

aaa accounting dot1x 476
aaa accounting mac-authentication 565
aaa accounting web-authentication 511
aaa authentication dot1x 478
aaa authentication enable 32
aaa authentication enable end-by-reject 34
aaa authentication login 35
aaa authentication login console 37
aaa authentication login end-by-reject 38
aaa authentication mac-authentication 567
aaa authentication mac-authentication end-by-reject 569
aaa authentication web-authentication 513
aaa authentication web-authentication end-by-reject 515
aaa group server radius 39
access-redirect http port 650
access-redirect http target 651
access-redirect timeout 652
arp 296
authentication arp-relay 460
authentication auto-logout strayer 461
authentication force-authorized enable 462
authentication force-authorized vlan 464
authentication ip access-group 465
authentication logout linkdown 467
authentication max-user（global） 468
authentication max-user（interface） 470
authentication multi-step 598
axrp 252
axrp-primary-port 256
axrp-ring-port 258
axrp virtual-link 253
axrp vlan-mapping 254

B

bandwidth 126
banner 41

C

channel-group lacp system-priority 146
channel-group max-active-port 147
channel-group mode 149
channel-group periodic-timer 151
clock timezone 61
control-packet user-priority 457
control-vlan 260

D

default-router 316
deny（ip access-list extended） 349
deny（ip access-list standard） 355
deny（ipv6 access-list） 357
deny（mac access-list extended） 363
description（イーサネット） 127
description（リンクアグリゲーション） 152
disable 262
dns-server 317
domain name 680
dot1x authentication 480
dot1x auto-logout 481
dot1x force-authorized eapol 482
dot1x ignore-eapol-start 483
dot1x logging enable 484
dot1x max-req 485
dot1x multiple-authentication 486
dot1x port-control 488
dot1x radius-server dead-interval 490
dot1x radius-server host 492
dot1x reauthentication 495
dot1x supplicant-detection 496
dot1x system-auth-control 498
dot1x timeout keep-unauth 499
dot1x timeout quiet-period 500
dot1x timeout reauth-period 501
dot1x timeout server-timeout 503
dot1x timeout supp-timeout 504
dot1x timeout tx-period 505
duplex 128

E

efmoam active 662
efmoam disable 663
efmoam udld-detection-count 664
end 18
ethernet cfm cc alarm-priority 682
ethernet cfm cc alarm-reset-time 684
ethernet cfm cc alarm-start-time 686
ethernet cfm cc enable 688
ethernet cfm cc interval 690

ethernet cfm domain 692
ethernet cfm enable（global） 694
ethernet cfm enable（interface） 695
ethernet cfm mep 696
ethernet cfm mip 698
exit 19

F

flowcontrol 130
flow detection mode 332
flow detection out mode 335
flush-request-count 263
flush-request-transmit vlan 264
forwarding-shift-time 265
ftp-server 10

H

hardware-address 318
health-check holdtime 266
health-check interval 267
host 319
hostname 704
http-server initial-timeout 516

I

instance 197
interface gigabitethernet 132
interface port-channel 153
interface vlan 164
ip access-group（アクセスリスト） 366
ip access-group（ログインセキュリティと RADIUS） 43
ip access-list extended 368
ip access-list resequence 370
ip access-list standard 372
ip address 298
ip arp inspection limit rate 600
ip arp inspection trust 601
ip arp inspection validate 602
ip arp inspection vlan 604
ip dhcp excluded-address 321
ip dhcp pool 322
ip dhcp snooping 606
ip dhcp snooping database url 607
ip dhcp snooping database write-delay 609
ip dhcp snooping information no-check 610
ip dhcp snooping information option allow-untrusted 611
ip dhcp snooping information option format remote-id 612
ip dhcp snooping information option-insert 613
ip dhcp snooping limit rate 614
ip dhcp snooping trust 615
ip dhcp snooping verify mac-address 616
ip dhcp snooping vlan 617
ip dhcp snooping vlan information option format-type circuit-id 618
ip domain lookup 82
ip domain name 83
ip domain reverse-lookup 84
ip host 85
ip icmp monitor destination interface 774
ip igmp snooping（global） 280
ip igmp snooping（interface） 281
ip igmp snooping fast-leave 282
ip igmp snooping mrouter 283
ip igmp snooping mrouter discovery 284
ip igmp snooping mrouter discovery extension 285
ip igmp snooping mrouter logging 286
ip igmp snooping querier 287
ip igmp snooping query-interval 288
ip mtu 300
ip name-server 86
ip qos-flow-group 414
ip qos-flow-list 416
ip qos-flow-list resequence 417
ip route 302
ip source binding 620
ipv6 access-class 45
ipv6 access-list 374
ipv6 access-list resequence 376
ipv6 address 306
ipv6 default-gateway 308
ipv6 enable 310
ipv6 host 87
ipv6 mld snooping（global） 290
ipv6 mld snooping（interface） 291
ipv6 mld snooping mrouter 293
ipv6 mld snooping querier 294
ipv6 mld snooping source 292
ipv6 nd accept-ra 311
ipv6 neighbor 312
ipv6 qos-flow-group 418
ipv6 qos-flow-list 420
ipv6 qos-flow-list resequence 421
ipv6 traffic-filter 377
ip verify source 622

L

l2protocol-tunnel eap 165
l2protocol-tunnel stp 166
lacp port-priority 154
lacp system-priority 155
lease 323
limit-queue-length 422
line console 11
line vty 12
link debounce 133
link up-debounce 134
link-relay source 135
lldp enable 766
lldp hold-count 767
lldp interval-time 768
lldp management-address 769
lldp run 770
lldp version 771
logging event-kind 736
logging facility 737
logging host 738
logging syslog-dump 740
logging tcp connect delay 741
logging tcp notify open 742
logging tcp notify resume 743
logging tcp reconnect delay 744
logging tcp trailer 745
logging trap 746
loop-detection 672
loop-detection auto-restore-time 674
loop-detection enable 675
loop-detection hold-time 676
loop-detection interval-time 677
loop-detection threshold 678

M

mac-address 167
mac-address-table aging-time 158
mac-address-table learning 159
mac-address-table static 160
mac-authentication access-group 570
mac-authentication authentication 572
mac-authentication auto-logout 573
mac-authentication id-format 575
mac-authentication logging enable 577
mac-authentication max-timer 578
mac-authentication password 579
mac-authentication port 581
mac-authentication radius-server dead-interval 582
mac-authentication radius-server host 584
mac-authentication roaming 587
mac-authentication static-vlan roaming 589
mac-authentication system-auth-control 591
mac-authentication timeout quiet-period 592
mac-authentication timeout reauth-period 593
mac-authentication vlan-check 594
mac access-group 379
mac access-list extended 381
mac access-list resequence 383
mac qos-flow-group 424
mac qos-flow-list 426
mac qos-flow-list resequence 427
ma name 699
ma vlan-group 701
max-lease 325
mdix auto 136
mode 268
monitor session filter 782
monitor session source 776
mtu 137
multi-fault-detection holdtime 270
multi-fault-detection interval 271
multi-fault-detection mode 272
multi-fault-detection vlan 274

N

name（Ring Protocol） 275
name（VLAN） 168
name（スパニングツリー） 199
network 327
ntp authenticate 63
ntp authentication-key 64
ntp broadcast 66
ntp broadcast client(global) 68
ntp broadcast client(interface) 69
ntp broadcastdelay 70
ntp interval 71
ntp master 72
ntp peer 73
ntp server 75
ntp trusted-key 77

P

permit（ip access-list extended） 384
permit（ip access-list standard） 390
permit（ipv6 access-list） 392
permit（mac access-list extended） 398
power-control port cool-standby 108

preempt-delay 276
protocol 169

Q

qos-queue-group 450
qos-queue-list 451
qos（ip qos-flow-list）428
qos（ipv6 qos-flow-list） 437
qos（mac qos-flow-list） 445

R

radius-server attribute station-id capitalize 47
radius-server dead-interval 48
radius-server host 50
radius-server key 53
radius-server retransmit 55
radius-server timeout 56
remark（QoS） 454
remark（アクセスリスト） 401
revision 200
rmon alarm 705
rmon collection history 709
rmon event 711

S

save(write) 20
schedule-power-control port-led 110
schedule-power-control port cool-standby 109
schedule-power-control shutdown 112
schedule-power-control system-sleep 114
schedule-power-control time-range 115
server 57
service dhcp 329
sflow destination 750
sflow extended-information-type 751
sflow forward egress 753
sflow forward ingress 754
sflow max-header-size 755
sflow max-packet-size 756
sflow packet-information-type 757
sflow polling-interval 758
sflow sample 759
sflow source 761
sflow url-port-add 762
sflow version 763
show 21
shutdown（イーサネット） 139
shutdown（リンクアグリゲーション） 156
snmp-server community 713
snmp-server contact 715
snmp-server engineID local 716
snmp-server group 718
snmp-server host 721
snmp-server location 726
snmp-server traps 727
snmp-server user 730
snmp-server view 732
snmp trap link-status 734
sntp client 78
spanning-tree bpdufilter 201
spanning-tree bpduguard 202
spanning-tree cost 203
spanning-tree disable 205
spanning-tree guard 206
spanning-tree link-type 208
spanning-tree loopguard default 209
spanning-tree mode 210
spanning-tree mst configuration 211
spanning-tree mst cost 212
spanning-tree mst forward-time 213
spanning-tree mst hello-time 214
spanning-tree mst max-age 215
spanning-tree mst max-hops 216
spanning-tree mst port-priority 217
spanning-tree mst root priority 218
spanning-tree mst transmission-limit 219
spanning-tree pathcost method 220
spanning-tree port-priority 222
spanning-tree portfast 223
spanning-tree portfast bpduguard default 224
spanning-tree portfast default 225
spanning-tree single 226
spanning-tree single cost 227
spanning-tree single forward-time 228
spanning-tree single hello-time 229
spanning-tree single max-age 230
spanning-tree single mode 231
spanning-tree single pathcost method 232
spanning-tree single port-priority 234
spanning-tree single priority 235
spanning-tree single transmission-limit 236
spanning-tree vlan 237
spanning-tree vlan cost 238
spanning-tree vlan forward-time 240
spanning-tree vlan hello-time 242
spanning-tree vlan max-age 243
spanning-tree vlan mode 244
spanning-tree vlan pathcost method 245

spanning-tree vlan port-priority 247
spanning-tree vlan priority 248
spanning-tree vlan transmission-limit 249
speed（イーサネット） 140
speed（運用端末接続） 14
state 170
storm-control 666
switch 24
switch priority 25
switch provision 26
switchport access 171
switchport backup flush-request transmit 656
switchport backup interface 654
switchport backup mac-address-table update exclude-vlan 657
switchport backup mac-address-table update retransmit 658
switchport backup mac-address-table update transmit 659
switchport-backup startup-active-port-selection 660
switchport dot1q ethertype 172
switchport isolation 173
switchport mac 175
switchport mac auto-vlan 178
switchport mode 179
switchport monitor dot1q tag 779
switchport protocol 181
switchport stack cost 28
switchport trunk 183
switchport vlan mapping 185
switchport vlan mapping enable 187
system l2-table mode 90
system logging format-add 91
system mac-address 29
system memory-soft-error 92
system mtu 142
system port-led 120
system port-led trigger console 122
system port-led trigger interface 123
system port-led trigger mc 124
system receive alarm logging 93
system receive alarm parameters 94
system receive control 96
system receive rate-limit 97
system recovery 98
system temperature-warning-level 99
system temperature-warning-level average 100
system zero-touch-provisioning 104
system zero-touch-provisioning vlan 105

T

top 22
traffic-shape rate 455
transport input 15

V

vlan 188
vlan-dot1q-ethertype 191
vlan-group 277
vlan-protocol 192

W

web-authentication authentication 518
web-authentication auto-logout 519
web-authentication html-fileset 520
web-authentication ip address 521
web-authentication jump-url 523
web-authentication logging enable 525
web-authentication logout ping tos-windows 526
web-authentication logout ping ttl 527
web-authentication logout polling count 528
web-authentication logout polling enable 530
web-authentication logout polling interval 532
web-authentication logout polling retry-interval 534
web-authentication max-timer 536
web-authentication port 538
web-authentication prefilter 539
web-authentication radius-server dead-interval 540
web-authentication radius-server host 542
web-authentication redirect-mode 545
web-authentication redirect enable 546
web-authentication redirect ignore-https 547
web-authentication redirect polling 548
web-authentication redirect queries 550
web-authentication redirect target 552
web-authentication roaming 554
web-authentication static-vlan roaming 556
web-authentication system-auth-control 558
web-authentication user-group 559
web-authentication user replacement 560
web-authentication web-port 561
white-list action log 627
white-list action monitor 628
white-list address permit 629
white-list address trust 630
white-list data 631
white-list enable 634
white-list learning 635

white-list logging filter 636
white-list logging format-add 638
white-list monitor destination interface 639
white-list packet mode 640
white-list packet tcp 641
white-list packet trust-mode 643
white-list packet udp 645
white-list trust 647

こ

コマンドの記述形式 2