AX6700S・AX6600S・AX6300S 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 Vol.2

Ver. 11.7 対応

AX63S-S010-30

AlaxalA

■対象製品

このマニュアルは AX6700S，AX6600S および AX6300S モデルを対象に記載しています。また，AX6700S，AX6600S および AX6300S のソフトウェア Ver. 11.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-SE 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

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
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 の米国及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。
Octpower は，日本電気（株）の登録商標です。
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。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
VitalQIP，VitalQIP Registration Manager は，Lucent technologies の商標です。
VLANaccessClient は，NEC ソフトの商標です。
VLANaccessController，VLANaccessAgent は，NEC の商標です。
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。
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

２０１２年　　1月 （第４版） ＡＸ６３Ｓ－Ｓ０１０－３０

■著作権

変更履歴

【Ver. 11.7 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
4　アクセスリスト	• 次に示すコマンドに policy-list パラメータを追加しました。 access-list permit（advance access-list） permit（ip access-list extended） • 次に示すコマンドに policy-switch-list パラメータを追加しました。 access-list permit（advance access-list） permit（ip access-list extended） permit（ipv6 access-list） permit（mac access-list extended） • 次に示すコマンドの注意事項を変更しました。 access-list permit（advance access-list） permit（ip access-list extended） permit（ipv6 access-list）
24　SNMP	• snmp-server host コマンドに policy-base パラメータおよび informs パラメータを追加しました。 • snmp-server informs コマンドを追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 11.5 対応版】

表　変更履歴

項目	追加・変更内容
SNMP	• snmp-server host コマンドに static-route パラメータを追加しました。

【Ver. 11.4 対応版】

表　変更履歴

項目	追加・変更内容
レイヤ 2 認証	• 本章を追加しました。
Web 認証	• web-authenticaion ip address コマンドに fqdn パラメータを追加しました。 • 次に示すコマンドを追加しました。 web-authentication redirect-mode web-authentication redirect-vlan
MAC 認証	• 次に示すコマンドを追加しました。 mac-authentication auto-logout mac-authentication dynamic-vlan max-user
DHCP snooping	• 本章を追加しました。
NIF 冗長制御	• 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	•「DHCP snooping 情報」の項を追加しました。

【Ver. 11.3 対応版】

Ver. 11.2 対応版まで「コンフィグレーションコマンドレファレンス Vol.1」に収録していた「フローモード」以降の章をこのマ

ニュアルに収録しています。
Ver. 11.2 対応版以前の変更履歴は「コンフィグレーションコマンドレファレンス Vol.1」を参照してください。

表　変更履歴

項目	追加・変更内容
アクセスリスト	• 次に示すコマンドにアクセスリストロギングの動作指定パラメータを追加しました。 access-list deny（advance access-list） deny（ip access-list extended） deny（ip access-list standard） deny（ipv6 access-list） deny（mac access-list extended）
アクセスリストロギング	• 本章を追加しました。
ログ出力機能	• 次に示すコマンドにアクセスリストロギングの記述を追加しました。 logging email-event-kind logging event-kind

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 AX6700S，AX6600S および AX6300S モデルを対象に記載しています。また，AX6700S，AX6600S および AX6300S のソフトウェア Ver. 11.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-SE 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。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。
なお，このマニュアルでは特に断らないかぎり AX6700S，AX6600S および AX6300S に共通の機能について記載しますが，機種固有の機能については以下のマークで示します。

【AX6700S】：
　AX6700S についての記述です。

【AX6600S】：
　AX6600S についての記述です。

【AX6300S】：
　AX6300S についての記述です。
また，このマニュアルでは特に断らないかぎり基本ソフトウェア OS-SE の機能について記載しますが，オプションライセンスでサポートする機能については以下のマークで示します。

【OP-BGP】：
　オプションライセンス OP-BGP についての記述です。

【OP-DH6R】：
　オプションライセンス OP-DH6R についての記述です。

【OP-MBSE】：
　オプションライセンス OP-MBSE についての記述です。

【OP-NPAR】：
　オプションライセンス OP-NPAR についての記述です。

【OP-VAA】：
　オプションライセンス OP-VAA についての記述です。

■このマニュアルの訂正について

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

■対象読者

本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。
また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。
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。

●装置の開梱から，初期導入時の基本的な設定を知りたい

AX6700S クイックスタートガイド (AX67S-Q001)	AX6600S クイックスタートガイド (AX66S-Q001)	AX6300S クイックスタートガイド (AX63S-Q001)

●ハードウェアの設備条件，取扱方法を調べる

AX6700S ハードウェア取扱説明書 (AX67S-H001)	AX6600S ハードウェア取扱説明書 (AX66S-H001)	AX6300S ハードウェア取扱説明書 (AX63S-H001)

●ソフトウェアの機能，コンフィグレーションの設定，運用コマンドを知りたい

▽まず，ガイドで使用する機能や収容条件についてご確認ください。

・収容条件 ・ログインなどの基本操作 ・VLAN，スパニングツリー	・フィルタ，QoS ・レイヤ2認証 ・高信頼化機能	・IPv4，IPv6パケット中継 ・IPv4，IPv6ルーティング プロトコル
コンフィグレーションガイド Vol.1 (AX63S-S001)	コンフィグレーションガイド Vol.2 (AX63S-S002)	コンフィグレーションガイド Vol.3 (AX63S-S003)

▽必要に応じて，レファレンスをご確認ください。

・コマンドの入力シンタックス，パラメータ詳細について

コンフィグレーション コマンドレファレンス Vol.1 (AX63S-S004)	コンフィグレーション コマンドレファレンス Vol.2 (AX63S-S010)	コンフィグレーション コマンドレファレンス Vol.3 (AX63S-S005)
運用コマンドレファレンス Vol.1 (AX63S-S006)	運用コマンドレファレンス Vol.2 (AX63S-S011)	運用コマンドレファレンス Vol.3 (AX63S-S007)

・メッセージとログについて

メッセージ・ログレファレンス (AX63S-S008)

・MIBについて

MIBレファレンス (AX63S-S009)

●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 (AX36S-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
BCU	Basic Control Unit
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
BSU	Basic Switching Unit
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
CSU	Control and Switching Unit
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
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
LLPQ	Low Latency Priority Queueing
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LLRLQ	Low Latency Rate Limited 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
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MSU	Management and Switching Unit
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
NIF	Network Interface
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
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PSP	Packet Switching Processor
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RGQ	Rate Guaranteed Queueing
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
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
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
uRPF	unicast Reverse Path Forwarding
VAA	VLAN Access Agent
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WGQ	Weighted Guaranteed 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 5

第 2 編　フィルタ・QoS 共通

2 フローモード 9
flow mac mode 10

3 VLAN リスト 13
vlan-list 14

第 3 編　フィルタ

4 アクセスリスト 17
指定できる名称および値 19
access-list 30
advance access-group 41
advance access-list 44
advance access-list resequence 46
deny（advance access-list） 47
deny（ip access-list extended） 60
deny（ip access-list standard） 68
deny（ipv6 access-list） 70
deny（mac access-list extended） 77
ip access-group 80
ip access-list extended 83
ip access-list resequence 85
ip access-list standard 87
ipv6 access-list 89
ipv6 access-list resequence 91

ipv6 traffic-filter 92
mac access-group 95
mac access-list extended 97
mac access-list resequence 99
permit（advance access-list） 100
permit（ip access-list extended） 115
permit（ip access-list standard） 124
permit（ipv6 access-list） 126
permit（mac access-list extended） 134
remark 137

5 **アクセスリストロギング** 139
access-log enable 140
access-log interval 141
access-log rate-limit 142
access-log threshold 143

6 uRPF 145
ip urpf 146
ip verify unicast source reachable-via 148
ipv6 verify unicast source reachable-via 149

第 4 編　QoS

7 QoS 151
指定できる名称および値 153
advance qos-flow-group 164
advance qos-flow-list 167
advance qos-flow-list resequence 168
ip qos-flow-group 170
ip qos-flow-list 173
ip qos-flow-list resequence 174
ipv6 qos-flow-group 175
ipv6 qos-flow-list 178
ipv6 qos-flow-list resequence 179
llrlq1-burst**【AX6700S】【AX6600S】** 180
llrlq2-burst**【AX6700S】【AX6600S】** 182
mac qos-flow-group 184
mac qos-flow-list 186

mac qos-flow-list resequence 187
mode 188
number-of-queue 191
predicted-tail-drop 193
qos（advance qos-flow-list） 194
qos（ip qos-flow-list） 210
qos（ipv6 qos-flow-list） 221
qos（mac qos-flow-list） 231
qos-queue-group 236
qos-queue-list 238
remark 241
set-default-user-priority 243
shaper auto-configuration 244
shaper default-user 246
shaper llrlq1【AX6700S】【AX6600S】 248
shaper llrlq2【AX6700S】【AX6600S】 250
shaper nif 252
shaper port buffer 253
shaper port rate-limit 255
shaper user 257
shaper user-list 260
shaper vlan-user-map 268
shaper wgq-group rate-limit【AX6700S】【AX6600S】 270
traffic-shape rate 271
upc-storm-control mode 273

第 5 編　レイヤ 2 認証

8 レイヤ 2 認証 275
コンフィグレーションコマンドと適用するレイヤ 2 認証 276
authentication ip access-group 277

9 IEEE802.1X 279
aaa accounting dot1x default 281
aaa authentication dot1x default 282
aaa authorization network default 283
dot1x force-authorized-port 284
dot1x ignore-eapol-start 285
dot1x logging enable 286
dot1x loglevel 287

dot1x max-req 289
dot1x max-supplicant 290
dot1x multiple-authentication 291
dot1x multiple-hosts 292
dot1x port-control 294
dot1x reauthentication 296
dot1x supplicant-detection 297
dot1x system-auth-control 299
dot1x timeout keep-unauth 300
dot1x timeout quiet-period 301
dot1x timeout reauth-period 302
dot1x timeout server-timeout 304
dot1x timeout supp-timeout 305
dot1x timeout tx-period 306
dot1x vlan dynamic enable 307
dot1x vlan dynamic ignore-eapol-start 308
dot1x vlan dynamic max-req 309
dot1x vlan dynamic max-supplicant 310
dot1x vlan dynamic radius-vlan 311
dot1x vlan dynamic reauthentication 313
dot1x vlan dynamic supplicant-detection 314
dot1x vlan dynamic timeout quiet-period 316
dot1x vlan dynamic timeout reauth-period 317
dot1x vlan dynamic timeout server-timeout 319
dot1x vlan dynamic timeout supp-timeout 320
dot1x vlan dynamic timeout tx-period 321
dot1x vlan enable 322
dot1x vlan ignore-eapol-start 324
dot1x vlan max-req 326
dot1x vlan max-supplicant 328
dot1x vlan reauthentication 330
dot1x vlan supplicant-detection 331
dot1x vlan timeout quiet-period 333
dot1x vlan timeout reauth-period 335
dot1x vlan timeout server-timeout 337
dot1x vlan timeout supp-timeout 338
dot1x vlan timeout tx-period 340

10 Web 認証 343

コンフィグレーションコマンドと動作モードの対応 344
aaa accounting web-authentication default start-stop group radius 345
aaa authentication web-authentication default group radius 346
web-authentication auto-logout 347

web-authentication ip address 348
web-authentication jump-url 350
web-authentication logging enable 351
web-authentication logout ping tos-windows 352
web-authentication logout ping ttl 353
web-authentication logout polling count 354
web-authentication logout polling enable 356
web-authentication logout polling interval 358
web-authentication logout polling retry-interval 360
web-authentication max-timer 362
web-authentication max-user 364
web-authentication port 365
web-authentication redirect-mode 366
web-authentication redirect-vlan 367
web-authentication static-vlan max-user 368
web-authentication system-auth-control 369
web-authentication vlan 370
web-authentication web-port 371

11 MAC 認証 373

コンフィグレーションコマンドと動作モードの対応 374
aaa accounting mac-authentication default start-stop group radius 375
aaa authentication mac-authentication default group radius 376
mac-authentication auth-interval-timer 377
mac-authentication auto-logout 378
mac-authentication dynamic-vlan max-user 379
mac-authentication logging enable 380
mac-authentication max-timer 381
mac-authentication password 382
mac-authentication port 383
mac-authentication radius-server host 384
mac-authentication static-vlan max-user 387
mac-authentication system-auth-control 388
mac-authentication vlan-check 389

12 認証 VLAN【OP-VAA】 391

fense alive-timer【OP-VAA】 392
fense retry-count【OP-VAA】 394
fense retry-timer【OP-VAA】 396
fense server【OP-VAA】 398
fense vaa-name【OP-VAA】 400
fense vaa-sync【OP-VAA】 402

fense vlan【OP-VAA】 403

第 6 編　セキュリティ

13 DHCP snooping 405
ip arp inspection limit rate 406
ip arp inspection trust 407
ip arp inspection validate 408
ip arp inspection vlan 410
ip dhcp snooping 412
ip dhcp snooping database url 413
ip dhcp snooping database write-delay 415
ip dhcp snooping information option allow-untrusted 416
ip dhcp snooping limit rate 417
ip dhcp snooping logging enable 418
ip dhcp snooping loglevel 419
ip dhcp snooping trust 421
ip dhcp snooping verify mac-address 422
ip dhcp snooping vlan 423
ip source binding 425
ip verify source 427

第 7 編　冗長化構成による高信頼化機能

14 電源機構（PS）の冗長化 429
power redundancy-mode 430

15 BSU の冗長化【AX6700S】 431
redundancy bsu-load-balancing【AX6700S】 432
redundancy bsu-mode【AX6700S】 433
redundancy max-bsu【AX6700S】 434
redundancy standby-bsu【AX6700S】 435

16 PSP の冗長化【AX6600S】 437
redundancy max-psp【AX6600S】 438
redundancy standby-psp【AX6600S】 439

17 NIF 冗長制御【AX6700S】【AX6600S】 441
redundancy nif-group max-standby-nif【AX6700S】【AX6600S】 442
redundancy nif-group nif priority【AX6700S】【AX6600S】 444

18 GSRP 447
advertise-holdtime 448
advertise-interval 449
backup-lock 450
flush-request-count 451
gsrp 452
gsrp-vlan 453
gsrp direct-link 454
gsrp exception-port 455
gsrp limit-control 456
gsrp no-flush-port 457
gsrp reset-flush-port 458
layer3-redundancy 459
no-neighbor-to-master 460
port-up-delay 462
reset-flush-time 463
selection-pattern 464
vlan-group disable 465
vlan-group priority 466
vlan-group vlan 467

19 VRRP 469
track check-reply-interface 470
track check-status-interval 471
track check-trial-times 473
track failure-detection-interval 475
track failure-detection-times 477
track interface 479
track ip route 481
track recovery-detection-interval 483
track recovery-detection-times 485
vrrp accept 487
vrrp authentication 488
vrrp follow 490
vrrp ietf-ipv6-spec-07-mode 492
vrrp ietf-unified-spec-02-mode 494
vrrp ip 496

vrrp ipv6 497
vrrp name 498
vrrp preempt 499
vrrp preempt delay 500
vrrp priority 501
vrrp timers advertise 502
vrrp timers non-preempt-swap 504
vrrp track 505
vrrp-vlan 507

第 8 編　ネットワークの障害検出による高信頼化機能

20 IEEE 802.3ah/UDLD 509
efmoam active 510
efmoam disable 511
efmoam udld-detection-count 512

21 ストームコントロール 513
storm-control（global） 514
storm-control（interface） 515

22 L2 ループ検知 519
loop-detection 520
loop-detection auto-restore-time 522
loop-detection enable 523
loop-detection hold-time 524
loop-detection interval-time 525
loop-detection threshold 526

23 CFM 527
domain name 528
ethernet cfm cc alarm-priority 530
ethernet cfm cc alarm-reset-time 532
ethernet cfm cc alarm-start-time 534
ethernet cfm cc enable 536
ethernet cfm cc interval 538
ethernet cfm domain 540
ethernet cfm enable（global） 542

ethernet cfm enable（interface） 543
ethernet cfm mep 544
ethernet cfm mip 546
ma name 547
ma vlan-group 549

第 9 編　リモートネットワーク管理

24 SNMP 551
hostname 552
rmon alarm 553
rmon collection history 556
rmon event 558
snmp-server community 561
snmp-server contact 563
snmp-server engineID local 564
snmp-server group 566
snmp-server host 569
snmp-server informs 577
snmp-server location 579
snmp-server traps 580
snmp-server user 583
snmp-server view 585
snmp trap link-status 587

25 ログ出力機能 589
logging email 590
logging email-event-kind 592
logging email-from 593
logging email-interval 594
logging email-server 595
logging event-kind 597
logging facility 598
logging host 599
logging syslog-dump 601
logging trap 602

26 sFlow 統計 605
sflow destination 606

sflow extended-information-type 607
sflow forward egress 609
sflow forward ingress 610
sflow max-header-size 611
sflow max-packet-size 612
sflow packet-information-type 613
sflow polling-interval 614
sflow sample 615
sflow source 617
sflow url-port-add 619
sflow version 620

第 10 編　隣接装置の管理

27 LLDP 621
lldp enable 622
lldp hold-count 623
lldp interval-time 624
lldp run 625

28 OADP 627
oadp cdp-listener 628
oadp enable 629
oadp hold-time 630
oadp ignore-vlan 631
oadp interval-time 632
oadp run 633

第 11 編　ポートミラーリング

29 ポートミラーリング 635
monitor option 636
monitor session 638

第 12 編　コンフィグレーションエラーメッセージ

30 コンフィグレーション編集時のエラーメッセージ 641
30.1 コンフィグレーション編集時のエラーメッセージ 642
30.1.1 共通 642
30.1.2 フローモード情報 642
30.1.3 VLAN リスト情報 642
30.1.4 アクセスリスト情報 643
30.1.5 アクセスリストロギング情報 646
30.1.6 QoS 情報 646
30.1.7 IEEE802.1X 情報 651
30.1.8 Web 認証情報 655
30.1.9 MAC 認証情報 656
30.1.10 認証 VLAN 情報【OP-VAA】 656
30.1.11 DHCP snooping 情報 657
30.1.12 BSU/PSP/NIF 冗長化情報【AX6700S】【AX6600S】 657
30.1.13 GSRP 情報 658
30.1.14 VRRP 情報 659
30.1.15 ストームコントロール情報 660
30.1.16 CFM 情報 660
30.1.17 SNMP 情報 661
30.1.18 sFlow 統計情報 662
30.1.19 OADP 情報 662
30.1.20 ポートミラーリング情報 662

索引 663

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

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記述しています。また，コンフィグレーションコマンドモード以下の各モードについては，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	コマンドモードごとのプロンプト表示	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-if)	インタフェースの設定	(config)# interface
4	(config-if-range)	インタフェースの複数設定	(config)# interface range
5	(config-vlan)	VLAN 設定	(config)# vlan
6	(config-mst)	マルチプルスパニングツリーの設定	(config)# spanning-tree mst configuration
7	(config-axrp)	Ring Protocol の設定	(config)# axrp
8	(config-gsrp)	GSRP の設定	(config)# gsrp
9	(config-adv-acl)	Advance フィルタの設定	(config)# advance access-list
10	(config-ext-nacl)	IPv4 パケットフィルタの設定	(config)# ip access-list extended
11	(config-std-nacl)	IPv4 アドレスフィルタの設定	(config)# ip access-list standard
12	(config-ipv6-acl)	IPv6 フィルタの設定	(config)# ipv6 access-list
13	(config-ext-macl)	MAC フィルタの設定	(config)# mac access-list extended
14	(config-adv-qos)	Advance QoS の設定	(config)# advance qos-flow-list
15	(config-ip-qos)	IPv4 QoS の設定	(config)# ip qos-flow-list
16	(config-ipv6-qos)	IPv6 QoS の設定	(config)# ipv6 qos-flow-list
17	(config-mac-qos)	MAC QoS の設定	(config)# mac qos-flow-list
18	(dhcp-config)	DHCP の設定	(config)# ip dhcp pool
19	(config-dhcp)	IPv6 DHCP（PD）の設定	(config)# ipv6 dhcp pool
20	(config-route-map)	ルートマップの設定	(config)# route-map
21	(config-rtr-rip)	RIPng の設定	(config)# ipv6 router rip
22	(config-router)	RIP の設定	(config)# router rip
		OSPF の設定	(config)# router ospf
		BGP4 ／ BGP4+ の設定	(config)# router bgp
23	(config-rtr)	OSPFv3 の設定	(config)# ipv6 router ospf
24	(config-router-af)	RIP の VRF 単位の設定	(config)# router rip (config-router)# address-family ipv4 vrf
		BGP4 の VRF 単位の設定 (config-router-af)(ipv4 vrf) モード	(config)# router bgp (config-router)# address-family ipv4 vrf
		BGP4+ のグローバルネットワークの設定 (config-router-af)(ipv6) モード	(config)# router bgp (config-router)# address-family ipv6
		BGP4+ の VRF 単位の設定 (config-router-af)(ipv6 vrf) モード	(config)# router bgp (config-router)# address-family ipv6 vrf

項番	コマンドモードごとのプロンプト表示	コマンドモード説明	モード移行コマンド
25	(config-auto-cf)	auto-config の設定	(config)# auto-config
26	(config-netconf)	netconf の設定	(config)# netconf
27	(config-view)	view の設定	(config)# parser view
28	(config-sh-nif)	シェーパモードの設定	(config)# shaper nif
29	(config-vrf)	config-vrf の設定	(config)# vrf definition
30	(config-ether-cfm)	ドメイン名称と MA の設定	(config)# ethernet cfm domain
31	(config-track-object)	ポリシーベースルーティングのトラッキング機能の設定	(config)# track-object
32	(config-pol)	ポリシーベースルーティングリスト情報の設定	(config)# policy-list
33	(config-pol-sw)	ポリシーベーススイッチングリスト情報の設定	(config)# policy-switch-list

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。

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
名前	1 文字目が英字で 2 文字目以降が英数字とハイフン（-），アンダースコア（_），ピリオド（.）で指定できます。	ip access-list standard inbound1
ホスト名	ホスト名は，1 文字目が英字で 2 文字目以降が英数字とハイフン（-），ピリオド（.）で指定できます。	ip host telnet-host 192.168.1.1
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
ワイルドカードマスク	IPv4 アドレスと同様の入力形式です。IPv4 アドレスの中でビットを立てた個所は任意を意味します。	255.255.0.0
IPv6 アドレス	2 バイトずつ 16 進数で表し，この間をコロン（:）で区切ります。	3ffe:501:811:ff03::87ff:fed0:c7e0
インタフェース複数指定	複数のインタフェースに関する情報を設定します。 指定できるインタフェースは，gigabitethernet，tengigabitethernet，vlan，port-channel です。 gigabitethernet と tengigabitethernet を混在して指定することはできますが，それ以外の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 <nif no.>/<port no.> [- <port no.>] • tengigabitethernet の場合 interface range tengigabitethernet <nif no.>/<port no.> [- <port no.>] • vlan の場合 interface range vlan <vlan id> [- <vlan id>] • port-channel の場合 interface range port-channel <channel group number> [- <channel group number>] また，上記入力形式をコンマ（,）で区切って最大 16 個指定できます。	interface range gigabitethernet 1/1-3 interface range gigabitethernet 1/1-3, tengigabitethernet 3/1 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。	switchport trunk allowed vlan add 100,200-210 switchport trunk allowed vlan remove 100,200-210

■任意の文字列

英数字および特殊文字で設定できます。ただし，特殊文字は一部設定できない文字があります。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 1-3 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	0	0x30	@	0x40	P	0x50	`	0x60	p	0x70

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
!	0x21	1	0x31	A	0x41	Q	0x51	a	0x61	q	0x71
"	0x22	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	O	0x4F	_	0x5F	o	0x6F	---	---

［注意事項］

- 疑問符（?）（0x3F）を入力するには［Ctrl］+［V］を入力後［?］を入力してください。また，疑問符を含む設定をコピー・ペーストで流し込むことはできません。

［設定できない特殊文字］

表 1-4　設定できない特殊文字

文字の名称	文字	コード
ダブルクォート	"	0x22
ドル	$	0x24
シングルクォート	'	0x27
セミコロン	;	0x3B
バックスラッシュ	¥	0x5C
逆シングルクォート	`	0x60
大カッコ始め	{	0x7B
大カッコ終わり	}	0x7D

［設定の例］

access-list 10 remark "mail:xx@xx %tokyo"

■ <nif no.> および <port no.> の範囲

パラメータ <nif no.> および <port no.> の値の範囲を次の表に示します。

表 1-5　<nif no.> の値の範囲

項番	モデル	<nif no.> の値の範囲
1	AX6708S	1 ～ 8

項番	モデル	<nif no.> の値の範囲
2	AX6604S	1 ～ 4
3	AX6608S	1 ～ 8
4	AX6304S	1 ～ 4
5	AX6308S	1 ～ 8

表 1-6 <port no.> の値の範囲【AX6700S】【AX6600S】

項番	NIF 型名略称	<port no.> の値の範囲
1	NK1G-24T	1 ～ 24
2	NK1G-24S	1 ～ 24
3	NK1GS-8M	1 ～ 8
4	NK10G-4RX	1 ～ 4
5	NK10G-8RX	1 ～ 8

表 1-7 <port no.> の値の範囲【AX6300S】

項番	NIF 型名略称	<port no.> の値の範囲
1	NH1G-16S	1 ～ 16
2	NH1G-24T	1 ～ 24
3	NH1G-24S	1 ～ 24
4	NH1G-48T	1 ～ 48
5	NH1GS-6M	1 ～ 6
6	NH10G-1RX	1
7	NH10G-4RX	1 ～ 4
8	NH10G-8RX	1 ～ 8

■ <channel group number> の設定値の範囲

<channel group number> の値の範囲を次の表に示します。

表 1-8 <channel group number> の値の範囲

項番	モデル	値の範囲
1	AX6304S/AX6604S	1 ～ 48
2	AX6308S/AX6608S/AX6708S	1 ～ 63

■ <vlan id> の設定値の範囲

<vlan id> の値の範囲を次の表に示します。

表 1-9 <vlan id> の値の範囲

項番	値の範囲
1	1 ～ 4095

■ <vlan id list> の指定方法と設定値の範囲

パラメータの入力形式に <vlan id list> と記載されている場合，ハイフン（-），コンマ（,）を使用して複数の VLAN ID を設定できます。また，<vlan id> と記載されている場合と同様に一つの VLAN ID を設定できます。設定値の範囲は，前述の <vlan id> の範囲に従います。<vlan id list> の設定内容が多くなった場合，<vlan id list> の設定内容を分割し，複数行のコンフィグレーションとして表示することがあります。また，add/remove 指定による VLAN の追加や削除で，<vlan id list> の設定内容が少なくなった場合，複数行のコンフィグレーションを統合して表示することがあります。

［ハイフンまたはコンマによる範囲設定の例］
1-3,5,10

［複数行表示の例］
switchport trunk allowed vlan 100,200,300・・・
switchport trunk allowed vlan add 400,500・・・

■ <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 インタフェースおよび tengigabitethernet インタフェースを設定できます。gigabitethernet インタフェースまたは tengigabitethernet インタフェース一つを設定することもできます。gigabitethernet インタフェースおよび tengigabitethernet インタフェースの入力形式は次のとおりです。

- gigabitethernet の場合
  gigabitethernet <nif no.>/<port no.> [- <port no.>]
- tengigabitethernet の場合
  tengigabitethernet <nif no.>/<port no.> [- <port no.>]

<nif no.>/<port no.> [- <port no.>] の指定範囲は，前述の <nif no.> および <port no.> の範囲に従います。

［ハイフンまたはコンマによる範囲設定の例］
gigabitethernet 1/1-2,gigabitethernet 1/5,tengigabitethernet 3/1

■ <vrf id> の設定値の範囲【OP-NPAR】

<vrf id> の値の範囲を次の表に示します。

表 1-10 <vrf id> の値の範囲

項番	VRF 動作モード	値の範囲
1	指定なし	設定不可
2	axrp-enable axrp-enable-ipv4-ipv6	2 ～ 64
3	l2protocol-disable l2protocol-disable-ipv4-ipv6	2 ～ 250
4	gsrp-enable-ipv4-ipv6	2 ～ 125

2 フローモード

flow mac mode

flow mac mode

VLAN インタフェースに対してフィルタ・QoS 機能の MAC モードを設定します。本コマンドは，MAC アクセスリストおよび MAC QoS フローリストでレイヤ 2 中継の IP パケットをフロー検出できるようにします。

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，変更する場合は該当する VLAN インタフェースに次に示すコマンドが設定されている場合は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

したがって，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，コマンド省略時の動作になります。

[入力形式]

情報の設定
　flow mac mode

情報の削除
　no flow mac mode

[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 アクセスリストおよび MAC QoS フローリストは非 IP パケットだけフロー検出します。

[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]

1. フロー配分パターンが，defaut standard，default extended，filter-only extended，qos-only extended，filter extended または qos extended の場合に設定できます。

[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

3 VLAN リスト

vlan-list

vlan-list

アクセスリストおよびQoSフローリストで使用するVLANリストを作成します。

装置当たりVLANリストを最大1024リスト作成できます。

[入力形式]

情報の設定・変更
　vlan-list <vlan id list name> <vlan id list>

情報の削除
　no vlan-list <vlan id list name>

[入力モード]

(config)

[パラメータ]

<vlan id list name>

VLAN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
   31文字以内の任意の文字列（先頭文字は英字）を指定します。
   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。ただし，スペースは指定できません。

<vlan id list>

VLAN IDを一括指定します。

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。

[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. アクセスリストまたはQoSフローリストの検出条件に指定されている場合，削除できません。該当するVLANリストの指定をアクセスリストおよびQoSフローリストから削除したあと実行してください。

[関連コマンド]

access-list

deny（advance access-list）

deny（ip access-list extended）

deny（ipv6 access-list）

deny（mac access-list extended）

permit（advance access-list）

permit（ip access-list extended）

permit（ipv6 access-list）

permit（mac access-list extended）

qos（advance qos-flow-list）

qos（ip qos-flow-list）

qos（ipv6 qos-flow-list）

qos（mac qos-flow-list）

4 アクセスリスト

指定できる名称および値
access-list
advance access-group
advance access-list
advance access-list resequence
deny（advance access-list）
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（advance access-list）
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 4-1　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

■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 4-2　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 4-3　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 4-4　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 4-5　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 4-6　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 4-7　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 4-8　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 4-9　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	
axp	0x88f3	Alaxala Protocol

イーサネットタイプ名称	Ethernet 値	備考
eapol	0x888e	
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 4-10　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
slow-protocol	0180.C200.0002	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 4-11　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

メッセージ名称	メッセージ名	タイプ	コード
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 4-12　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

メッセージ名称	メッセージ名	タイプ	コード
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

■アクセスリスト作成数

アクセスリスト作成数とは，アクセスリストの識別子として使用する名称の数です。該当するコンフィグレーションの <access list name> および <access list number> を合わせて，次に示すリスト数まで作成できます。ただし，<access list number> だけを指定する場合，最大 1599 リスト作成できます。

[AX6700S の場合]

BSU 種別によるアクセスリスト作成数を，次の表に示します。

表 4-13　BSU 種別によるアクセスリスト作成数

BSU 種別	アクセスリスト	フィルタ条件
全モデル	8574 リスト	32000 エントリ※

注※　QoS フローリストのフロー検出および動作指定のエントリも含みます。

[AX6600S の場合]

装置当たり，作成できるアクセスリスト数およびフィルタ条件数は CSU 種別によって異なります。CSU 種別によるアクセスリスト作成数を，次の表に示します。

表 4-14　CSU 種別によるアクセスリスト作成数

CSU 種別	アクセスリスト	フィルタ条件
CSU-1A	2000 リスト	4000 エントリ
CSU-1B	8574 リスト	32000 エントリ※

注※　QoS フローリストのフロー検出および動作指定のエントリも含みます。

[AX6300S の場合]

装置当たり，作成できるアクセスリスト数およびフィルタ条件数は MSU 種別によって異なります。MSU 種別によるアクセスリスト作成数を，次の表に示します。

表 4-15　MSU 種別によるアクセスリスト作成数

MSU 種別	アクセスリスト	フィルタ条件
MSU-1A，MSU-1A1	2000 リスト	4000 エントリ
MSU-1B，MSU-1B1	8574 リスト	32000 エントリ※

注※　QoS フローリストのフロー検出および動作指定のエントリも含みます。

■インタフェースへの設定数

インタフェースへの設定数とは，インタフェースに設定できるアクセスリストの延べ数です。次に示すリスト数まで作成できます。

なお，受信側と送信側や，中継種別は別に数えます。例えば，同じアクセスリスト名称を指定するかどうかに関係なく，同一インタフェースの受信側と送信側の両方に設定した場合，2 リストと数えます。同様に，同一インタフェースにレイヤ 2 中継とレイヤ 3 中継を設定した場合，2 リストと数えます。

[AX6700S の場合]

BSU 種別によるインタフェースへの設定数を，次の表に示します。

表 4-16　BSU 種別によるインタフェースへの設定数

BSU 種別	設定可能な数
全モデル	8574 リスト

[AX6600S の場合]

装置当たり，ip access-group，ipv6 traffic-filter，mac access-group，および advance access-group を設定できる数は CSU 種別によって異なります。CSU 種別によるインタフェースへの設定数を，次の表に示します。

表 4-17　CSU 種別によるインタフェースへの設定数

CSU 種別	設定可能な数
CSU-1A	2000 リスト
CSU-1B	8574 リスト

［AX6300S の場合］

装置当たり，ip access-group，ipv6 traffic-filter，mac access-group，および advance access-group を設定できる数は MSU 種別によって異なります。MSU 種別によるインタフェースへの設定数を，次の表に示します。

表 4-18　MSU 種別によるインタフェースへの設定数

MSU 種別	設定可能な数
MSU-1A，MSU-1A1	2000 リスト
MSU-1B，MSU-1B1	8574 リスト

■アクセスリスト作成数とインタフェースへの設定数の算出例

アクセスリスト作成数とインタフェースへの設定数の算出例を，次の表に示します。

表 4-19　アクセスリスト作成数とインタフェースへの設定数の算出例

設定例	使用する アクセスリスト 作成数	使用する インタフェース への設定数

アクセスリスト AAA を作成して，イーサネットインタフェース 1/1 の inbound に設定
`interface gigabitethernet 1/1`
`ip access-group AAA in layer2-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 リスト	1 リスト

アクセスリスト AAA を作成して，イーサネットインタフェース 1/1 と 1/2 の inbound に設定
`interface gigabitethernet 1/1`
`ip access-group AAA in layer2-forwarding`
 	
`interface gigabitethernet 1/2`
`ip access-group AAA in layer2-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 リスト	2 リスト

アクセスリスト AAA を作成して，イーサネットインタフェース 1/1 の inbound と outbound に設定
`interface gigabitethernet 1/1`
`ip access-group AAA in layer2-forwarding`
`ip access-group AAA out layer2-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 リスト	2 リスト

アクセスリスト AAA を作成して，VLAN 2 インタフェースの inbound に layer2-forwarding と layer3-forwarding を設定
`interface vlan 2`
`ip access-group AAA in layer2-forwarding`
`ip access-group AAA in layer3-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 リスト	2 リスト

設定例	使用する アクセスリスト 作成数	使用する インタフェース への設定数

アクセスリスト AAA を作成して，イーサネットインタフェース 1/1 の inbound に設定
アクセスリスト BBB を作成して，イーサネットインタフェース 1/2 の inbound に設定
`interface gigabitethernet 1/1`
`ip access-group AAA in layer2-forwarding`
 	
`interface gigabitethernet 1/2`
`ip access-group BBB in layer2-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
 	
`ip access-list extended BBB`
`10 permit udp any any`
`20 deny tcp any any`
	2 リスト	2 リスト

アクセスリスト AAA を作成して，イーサネットインタフェース 1/1 の inbound に設定
アクセスリスト BBB を作成して，イーサネットインタフェース 1/1 の outbound に設定
`interface gigabitethernet 1/1`
`ip access-group AAA in layer2-forwarding`
`ip access-group BBB out layer2-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
 	
`ip access-list extended BBB`
`10 permit udp any any`
`20 deny tcp any any`
	2 リスト	2 リスト

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

access-list

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。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。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，フラグメントパケット，ToS フィールドの値，ポート番号，TCP フラグ，ICMP タイプ，ICMP コードおよび IGMP タイプに基づいてフィルタします。

フラグメントパケットを検出条件に指定する場合は入力形式が異なるので注意してください。入力形式のフラグメントパケットの場合を参照してください。

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。

装置当たり，作成できるアクセスリスト数およびフィルタ条件数については「■アクセスリスト作成数」を参照してください。

ポリシーベースルーティングのパラメータは，フィルタ動作に permit を指定した場合に指定できます。なお，該当アクセスリストを，アクセスグループコマンドでインタフェースに適用する際は，VLAN インタフェースの Inbound（受信側）を指定し，かつ中継種別にレイヤ 3 中継を指定してください。

ポリシーベーススイッチングのパラメータは，フィルタ動作に permit を指定した場合に指定できます。なお，該当アクセスリストをアクセスグループコマンドでインタフェースに適用する際は，イーサネットインタフェースの Inbound（受信側）を指定してください。

［入力形式］

情報の設定・変更

補足説明の設定

access-list <access list number> remark <remark>

IPv4 アドレスフィルタの設定

access-list <access list number> [<sequence>] permit {<ipv4> [<ipv4 wildcard>] | host <ipv4> | any}

access-list <access list number> [<sequence>] deny {<ipv4> [<ipv4 wildcard>] | host <ipv4> | any} [動作指定]

動作指定

action log

IPv4 パケットフィルタの設定

access-list <access list number> [<sequence>] permit { フィルタ条件 } [動作指定]

access-list <access list number> [<sequence>] deny { フィルタ条件 } [動作指定]

フィルタ条件

- 上位プロトコルが TCP，UDP，ICMP および IGMP 以外の場合
  {deny | permit} {ip | <protocol>} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 上位プロトコルが TCP の場合
  {deny | permit} tcp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source

ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

- 上位プロトコルが UDP の場合
  {deny | permit} udp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 上位プロトコルが ICMP の場合
  {deny | permit} icmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 上位プロトコルが IGMP の場合
  {deny | permit} igmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [<igmp type>][{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- フラグメントパケット指定の場合
  {deny | permit} {ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [fragments] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

動作指定

- permit { フィルタ条件 } の場合
  action {policy interface vlan <vlan id> next-hop <next hop ipv4> | policy-list <policy list no.> | policy-switch-list <policy switch list no.>}
- deny { フィルタ条件 } の場合
  action log

情報の削除

no access-list <access list number>

[入力モード]

(config)

[パラメータ]

<access list number>

アクセスリストを識別するための識別子を指定します。
本識別子はアクセスリスト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 ～ 199 または 1300 ～ 2699（10 進数）を指定します。
   1 ～ 99 または 1300 ～ 1999（10 進数）は，IPv4 アドレスフィルタ専用の識別子です。
   100 ～ 199 または 2000 ～ 2699（10 進数）は，IPv4 パケットフィルタ専用の識別子です。

remark <remark>

アクセスリストの補足説明を設定します。
一つの ID 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。

<sequence>

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。

フィルタ条件パラメータ

{deny | permit}

フィルタ条件に一致した場合のフィルタ動作を指定します。
deny を指定した場合，アクセスを拒否します。
permit を指定した場合，アクセスを許可します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   deny または permit 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>] または，host <ipv4>，any を指定します。

<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マスクを 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> を入力した場合は <ipv4> の完全一致をフィルタ条件とします。
any を指定すると，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

{ip | <protocol> | icmp | igmp | tcp | udp}

IPv4 パケットの上位プロトコル条件を指定します。
ただし，すべてのプロトコルを対象とする場合は ip を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   0 ～ 255（10 進数）またはプロトコル名称を指定します。
   指定可能なプロトコル名称は「表 4-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>}

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>，any，own-address <source ipv4 wildcard>，host own-address，own または range-address <source ipv4 start> <source ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <source ipv4> を入力した場合は <source ipv4> の完全一致をフィルタ条件とします。
   any を指定すると，送信元 IPv4 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
   range-address は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の access-group コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを送信元 IPv4 アドレスとしてフィルタ条件にします。
   own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
   なお，own-address および own を指定したインタフェースがマルチホームの場合は，プライマリ IPv4 アドレスが対象になります。
   range-address を指定した場合は，<source ipv4 start> から <source ipv4 end> の範囲をフィルタ条件とします。
   <source ipv4 end> は <source ipv4 start> より大きい IPv4 アドレスを指定してください。
   IPv4 アドレス (nnn.nnn.nnn.nnn)：0.0.0.0 ～ 255.255.255.255

{{eq | neq} <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 4-3　TCP で指定可能なポート名称」および「表 4-4　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。
   neq を指定した場合は，<source port> 以外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> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>}

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>，any，own-address <destination ipv4 wildcard>，host own-address，own または range-address <destination ipv4 start> <destination ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <destination ipv4> を入力した場合は，<destination ipv4> の完全一致をフィルタ条件とします。
   any を指定すると，宛先 IPv4 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
   range-address は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の access-group コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを宛先 IPv4 アドレスとしてフィルタ条件にします。
   own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
   なお，own-address および own を指定したインタフェースがマルチホームの場合はプライマリ IPv4 アドレスが対象になります。
   range-address を指定した場合は <destination ipv4 start> から <destination ipv4 end> の範囲をフィルタ条件とします。
   <destination ipv4 end> は <destination ipv4 start> より大きい IPv4 アドレスを指定してください。
   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

{{eq | neq} <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 4-3　TCP で指定可能なポート名称」および「表 4-4　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。
   neq を指定した場合は，<destination port> 以外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 4-6　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 4-7　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 4-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。

ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。

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
   なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。

fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。

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
   なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。

psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。

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
   なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。

rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。

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
   なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。

syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。

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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。
urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。

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
   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 4-11　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

<igmp type>

IGMP タイプを指定します。
プロトコルが IGMP 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。

fragments

2 番目以降のフラグメントパケットを指定します。

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
   なし

vlan {<vlan id> | <vlan id list name>}

VLAN ID または VLAN リスト名称を指定します。
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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は，必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

policy interface vlan <vlan id> next-hop <next hop ipv4>

ポリシーベースルーティングの出力先を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベースルーティングを使用しません）
2. 値の設定範囲
   <vlan id>
   VLAN ID 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。
   <next hop ipv4>
   ネクストホップ IPv4 アドレスを指定します。
   指定した送信先インタフェースに接続するネットワーク内のアドレスを指定してください。ただし，指定した送信先インタフェースに接続するネットワークへのダイレクトブロードキャスト，および指定した送信先インタフェースに設定しているアドレスは指定できません。

policy-list <policy list no.>

ポリシーベースルーティングのリスト番号を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベースルーティングを使用しません）
2. 値の設定範囲
   policy-list コマンドで設定済みのポリシーベースルーティングのリスト番号を指定します。

policy-switch-list <policy switch list no.>

ポリシーベーススイッチングのリスト番号を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベーススイッチングを使用しません）
2. 値の設定範囲
   policy-switch-list コマンドで設定済みのポリシーベーススイッチングのリスト番号を指定します。

log

指定したアクセスリストで廃棄したパケットをアクセスリストロギングの対象とします。

1. 本パラメータ省略時の初期値
   なし（アクセスリストロギングを使用しません）
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]

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. IPv4 アドレスフィルタでは，対応する IP ホストアドレスを指定するときにマスクを省略すると，0.0.0.0 がマスクとして使用されます。
2. ip access-list standard で指定した 1-99 または 1300-1999 の <access list number> と同じリストを操作できます。
3. ip access-list extended で指定した 100-199 または 2000-2699 の <access list number> と同じリストを操作できます。
4. IPv4 アドレスワイルドカードマスク，送信元アドレスワイルドカードマスクおよび宛先アドレスワイルドカードマスクに 255.255.255.255 と入力したときは any と表示します。
5. IPv4 アドレス，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。
6. 動作パラメータにポリシーベースルーティングを指定する場合，フィルタ条件に設定する送信元 IPv4 アドレスおよび宛先 IPv4 アドレスに次のアドレスは指定できません。

   送信元 IPv4 アドレス
   　マルチキャストアドレス，内部ループバックアドレス

   宛先 IPv4 アドレス
   　マルチキャストアドレス，制限付きブロードキャストアドレス，内部ループバックアドレス
7. 動作パラメータにポリシーベーススイッチングを指定する場合，指定したポリシーベーススイッチングのリストで設定している VLAN ID をフィルタ条件パラメータの vlan に指定してください。このとき，VLAN リスト名称では指定できません。
8. 動作指定に log を指定したアクセスリストを設定する場合，system hardware-mode の access-log を設定してください。

［関連コマンド］

ip access-group

ip access-list resequence

vlan-list

policy-list

policy-switch-list

advance 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Advanceアクセスリストを適用し，Advanceフィルタ機能を有効にします。

装置当たり，指定できるインタフェースへの設定数については「■インタフェースへの設定数」を参照してください。

ポリシーベースルーティングのパラメータ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際は，VLANインタフェースのInbound（受信側）を指定してください。

ポリシーベーススイッチングのパラメータ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際は，イーサネットインタフェースのInbound（受信側）を指定してください。

［入力形式］

情報の設定

- イーサネットインタフェース
  advance access-group <access list name> {in | out} layer2-forwarding
- VLANインタフェース
  advance access-group <access list name> {in | out} layer2-and-layer3-forwarding

情報の削除

- イーサネットインタフェース
  no advance access-group <access list name> {in | out} layer2-forwarding
- VLANインタフェース
  no advance access-group <access list name> {in | out} layer2-and-layer3-forwarding

［入力モード］

```
(config-if)
```

［パラメータ］

<access list name>

設定するAdvance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
   31文字以内の名前を指定します。
   詳細は，「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

layer2-forwarding

フロー検出する中継種別を指定します。

layer2-forwarding はレイヤ 2 中継する IP パケットをフロー検出します。
本パラメータはイーサネットインタフェースに適用する場合だけ有効です。

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
   なし

layer2-and-layer3-forwarding

フロー検出する中継種別を指定します。
layer2-and-layer3-forwarding はレイヤ 2 中継するパケットおよびレイヤ 3 中継するパケットをフロー検出します。
本パラメータは VLAN インタフェースに適用する場合だけ有効です。

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
   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 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. 同一のイーサネットインタフェースに対しては，Inbound と Outbound にそれぞれ一つ設定できます。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してください。
2. 実在しない Advance フィルタを設定した場合は何も動作しません。Advance フィルタの識別子は登録されます。
3. フロー配分パターンが default standard-advance，default extended-advance，filter-only extended-advance，filter extended-advance または qos extended-advance の場合に設定できます。
4. フロー検出条件種別に mac-ip を指定し，フロー検出条件に own-address または own パラメータがある場合は，対象インタフェースに IPv4 アドレスが設定されているときに設定できます。
5. フロー検出条件種別に mac-ipv6 を指定し，フロー検出条件に own-address または own パラメータがある場合は，対象インタフェースに一つだけ IPv6 グローバルアドレスが設定されているときに設定できます。
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 パラメータのすべての 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 パラメータがないときに設定できます。
8. 経路系テーブルエントリ配分パターンが ipv4-uni standard，ipv4-uni extended の場合，IPv6 ポリシーベースルーティングの設定がある IPv6 フィルタは設定できません。上記以外の経路系テーブルエントリ配分パターンのときに設定できます。

9. 動作指定に log を指定したアクセスリストを設定する場合，system hardware-mode の access-log を設定してください。

［関連コマンド］

advance access-list

advance access-list

Advance フィルタとして動作するアクセスリストを設定します。

アクセスリストの一つの ID で複数個のフィルタ条件を指定できます。

装置当たり，作成できるアクセスリスト数およびフィルタ条件数については「■アクセスリスト作成数」を参照してください。

ポリシーベースルーティングのパラメータは，フィルタ動作に permit を指定した場合に指定できます。なお，該当アクセスリストを，アクセスグループコマンドでインタフェースに適用する際は，VLAN インタフェースの Inbound（受信側）を指定してください。

ポリシーベーススイッチングのパラメータは，フィルタ動作に permit を指定した場合に指定できます。なお，該当アクセスリストを，アクセスグループコマンドでインタフェースに適用する際は，イーサネットインタフェースの Inbound（受信側）を指定してください。

[入力形式]

情報の設定

advance access-list <access list name>

情報の削除

no advance access-list <access list name>

[入力モード]

(config)

[パラメータ]

<access list name>

設定する Advance フィルタの識別子を指定します。

config-adv-acl モードへ移行します。

IPv4 アドレスフィルタ，IPv4 パケットフィルタ，および MAC フィルタですでに使用されている名称は指定できません。

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
   31 文字以内の名前を指定します。
   詳細は，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

advance access-group

advance access-list resequence

deny（advance access-list）

permit（advance access-list）

remark

advance access-list resequence

Advance 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

advance 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 Advance 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
   31 文字以内の名前を指定します。
   詳細は,「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]

advance access-list extended

deny（advance access-list）

Advance 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

[<sequence>] deny mac { フィルタ条件 } [動作指定]

[<sequence>] deny mac-ip { フィルタ条件 } [動作指定]

[<sequence>] deny mac-ipv6 { フィルタ条件 } [動作指定]

フィルタ条件

mac { フィルタ条件 } の場合

MAC ヘッダ条件でフロー検出する場合のフィルタ条件です。

mac {<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 | slow-protocol} [<ethernet type>][vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

mac-ip { フィルタ条件 } の場合

MAC ヘッダ条件，IPv4 ヘッダ条件および Layer4 ヘッダ条件でフロー検出する場合のフィルタ条件です。

- フラグメントパケットなしで，上位プロトコルが TCP，UDP，ICMP および IGMP 以外の場合

  mac-ip {<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 | slow-protocol} {ip | <protocol>} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- フラグメントパケットなしで，上位プロトコルが TCP の場合

  mac-ip {<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 | slow-protocol} tcp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- フラグメントパケットなしで，上位プロトコルが UDP の場合

  mac-ip {<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 | slow-protocol} udp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

- フラグメントパケットなしで，上位プロトコルが ICMP の場合
  mac-ip {<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 | slow-protocol} icmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- フラグメントパケットなしで，上位プロトコルが IGMP の場合
  mac-ip {<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 | slow-protocol} igmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [<igmp type>] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- フラグメントパケットありの場合
  mac-ip {<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 | slow-protocol} {ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [fragments] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

mac-ipv6 { フィルタ条件 } の場合

MAC ヘッダ条件，IPv6 ヘッダ条件および Layer4 ヘッダ条件でフロー検出する場合のフィルタ条件です。

- 上位プロトコルが TCP，UDP および ICMP 以外の場合
  mac-ipv6 {<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 | slow-protocol} {ipv6 | <protocol>} {<source ipv6>/<length>| host {<source

ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

- 上位プロトコルが TCP の場合
  mac-ipv6 {<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 | slow-protocol} tcp {<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- 上位プロトコルが UDP の場合
  mac-ipv6 {<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 | slow-protocol} udp {<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- 上位プロトコルが ICMP の場合
  mac-ipv6 {<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 | slow-protocol} icmp {<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

動作指定
　action log

情報の削除
　no <sequence>

[入力モード]

(config-adv-acl)

［パラメータ］

<sequence>

フィルタ条件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
   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> 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> を入力した場合は <source mac> の完全一致をフィルタ条件とします。
   any を指定すると，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 | slow-protocol}

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，pvst-plus-bpdu または slow-protocol を指定します。
   <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> を入力した場合は <destination mac> の完全一致をフィルタ条件とします。
   any を指定すると，宛先 MAC アドレスをフィルタ条件とはしません。
   bpdu を指定すると，BPDU 制御パケットをフィルタ条件とします。
   cdp を指定すると，CDP 制御パケットをフィルタ条件とします。
   lacp または slow-protocol を指定すると，slow プロトコルパケットをフィルタ条件とします。
   本装置では LACP と IEEE802.3ah/UDLD 機能で slow プロトコルパケットを使用しています。
   lacp を指定すると，LACP 制御パケットをフィルタ条件とします。
   lldp を指定すると，LLDP 制御パケットをフィルタ条件とします。
   oadp を指定すると，OADP 制御パケットをフィルタ条件とします。
   pvst-plus-bpdu を指定すると，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 4-9　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 list name>}

VLAN ID または VLAN リスト名称を指定します。
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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

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。

ctag-untagged

カスタマ Tag がないパケットの検出を指定します。

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
   なし

ctag-user-priority <priority>

カスタマ 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
   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。

ctag-vlan <vlan id>

カスタマ Tag の VLAN ID 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 ～ 4095（10 進数）を指定します。

{ip | <protocol> | icmp | igmp | tcp | udp}

フロー検出条件指定に mac-ip を指定した場合に選択できます。
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
   0 ～ 255（10 進数）またはプロトコル名称を指定します。
   指定可能なプロトコル名称は「表 4-1　指定可能なプロトコル名称（IPv4）」を参照してください。

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

フロー検出条件指定に mac-ipv6 を指定した場合に選択できます。
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。
   指定可能なプロトコル名称は「表 4-2　指定可能なプロトコル名称（IPv6）」を参照してください。

{{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>}

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>，any，own-address <source ipv4 wildcard>，host own-address，own または range-address <source ipv4 start> <source ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <source ipv4> を入力した場合は <source ipv4> の完全一致をフィルタ条件とします。
   any を指定すると，送信元 IPv4 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
   range-address は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の access-group コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを送信元 IPv4 アドレスとしてフィルタ条件にします。
   own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
   なお，own-address および own を指定したインタフェースがマルチホームの場合はプライマリ IPv4 アドレスが対象になります。
   range-address を指定した場合は，<source ipv4 start> から <source ipv4 end> の範囲をフィルタ条件とします。
   <source ipv4 end> は <source ipv4 start> より大きい IPv4 アドレスを指定してください。
   IPv4 アドレス (nnn.nnn.nnn.nnn)：0.0.0.0 ～ 255.255.255.255

{<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address

length> | own | range-address <source ipv6 start> <source ipv6 end>}

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>，own-address <own address length>，host <source ipv6>，host own-address，any，own または range-address <source ipv6 start> <source ipv6 end> を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は <source ipv6> の完全一致をフィルタ条件とします。
   any を指定すると，送信元 IPv6 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての traffic-filter コマンドだけ有効になります。
   range-address は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の traffic-filter コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを送信元 IPv6 アドレスとしてフィルタ条件とします。
   own を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを送信元 IPv6 アドレス，IPv6 グローバルアドレスのプレフィックス長を <length> としてフィルタ条件にします。
   range-address を指定した場合は <source ipv6 start> から <source ipv6 end> の範囲をフィルタ条件とします。
   <source ipv6 end> は <source ipv6 start> より大きい IPv6 アドレスを指定してください。
   <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 | neq} <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 4-3　TCP で指定可能なポート名称」,「表 4-4　UDP で指定可能なポート名称（IPv4)」および「表 4-5　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。
   neq を指定した場合は，<source port> 以外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> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>}

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>，any，own-address <destination ipv4 wildcard>，host own-address，own または range-address <destination ipv4 start> <destination ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <destination ipv4> を入力した場合は <destination ipv4> の完全一致をフィルタ条件とします。
   any を指定すると，宛先 IPv4 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
   range-address は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の access-group コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを宛先 IPv4 アドレスとしてフィルタ条件にします。
   own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
   なお，own-address および own を指定したインタフェースがマルチホームの場合はプライマリ IPv4 アドレスが対象になります。
   range-address を指定した場合は，<destination ipv4 start> から <destination ipv4 end> の範囲をフィルタ検出条件とします。
   <destination ipv4 end> は <destination ipv4 start> より大きい IPv4 アドレスを指定してください。
   IPv4 アドレス (nnn.nnn.nnn.nnn)：0.0.0.0 ～ 255.255.255.255

{<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>}

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>，own-address <own address length>，host <destination ipv6>，host own-address，any，own または range-address <destination ipv6 start> <destination ipv6 end> を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は <destination ipv6> の完全一致をフィルタ条件とします。
any を指定すると，宛先 IPv6 アドレスをフィルタ条件とはしません。
own-address および own は，VLAN インタフェースに対しての traffic-filter コマンドだけ有効になります。
range-address は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の traffic-filter コマンドだけ有効になります。
own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレスとしてフィルタ条件とします。
own を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレス，IPv6 グローバルアドレスのプレフィックス長を <length> としてフィルタ条件にします。
range-address を指定した場合は，<destination ipv6 start> から <destination ipv6 end> の範囲をフィルタ条件とします。
<destination ipv6 end> は <destination ipv6 start> より大きい IPv6 アドレスを指定してください。
<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

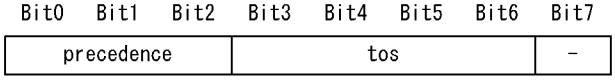
{{eq | neq} <destination port> | range <destination port start> <destination port end>}

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 4-3　TCP で指定可能なポート名称」,「表 4-4　UDP で指定可能なポート名称（IPv4)」および「表 4-5　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。
   neq を指定した場合は，<destination port> 以外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>

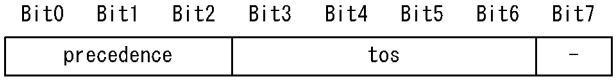
本パラメータは，ToS フィールドのビット 3 ～ 6 の 4 ビットである tos 値を指定します。
受信パケットの ToS フィールドのビット 3 ～ 6 の 4 ビットと比較します。



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 4-6　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。



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 4-7　指定可能な precedence 名称」を参照してください。

traffic-class <traffic class>

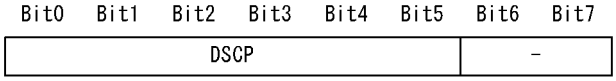
本パラメータは，トラフィッククラスフィールド値を指定します。
受信パケットのトラフィッククラスフィールドと比較します。

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>

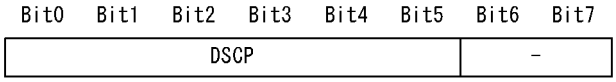
フロー検出条件種別が mac-ip の場合

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。



フロー検出条件種別が mac-ipv6 の場合

本パラメータは，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の上位 6 ビットと比較します。



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 ～ 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 4-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。

ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。

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
   なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。

fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。

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
   なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。

psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。

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
   なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。

rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。

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
   なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。

syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。

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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。

urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。

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
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 4-11　ICMP で指定可能なメッセージ名称（IPv4）」および「表 4-12　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

<igmp type>

IGMP タイプを指定します。
プロトコルが IGMP 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。

fragments

2 番目以降のフラグメントパケットを指定します。
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
なし

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

log

指定したアクセスリストで廃棄したパケットをアクセスリストロギングの対象とします。
1. 本パラメータ省略時の初期値
なし（アクセスリストロギングを使用しません）
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]

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 MAC アドレスおよび宛先 MAC 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 MAC 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 MAC アドレスに指定できるプロトコル名称のアドレスは「表 4-10　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 MAC アドレスおよび宛先 MAC 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. 送信元 IPv4 アドレスワイルドカードマスクおよび宛先 IPv4 アドレスワイルドカードマスクに 255.255.255.255 と入力したときは any と表示します。
4. 送信元 IPv4 アドレスおよび宛先 IPv4 アドレスを 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。
5. 送信元 IPv6 アドレスおよび宛先 IPv6 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。
6. 送信元 IPv6 アドレスおよび宛先 IPv6 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。

[関連コマンド]

advance access-group

advance access-list resequence

permit（advance access-list）

remark

vlan-list

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。

フラグメントパケットを検出条件に指定する場合は入力形式が異なるので注意してください。入力形式のフラグメントパケットの場合を参照してください。

［入力形式］

情報の設定・変更

[<sequence>] deny { フィルタ条件 } [動作指定]

フィルタ条件

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

| own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [<igmp type>] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

- フラグメントパケットの場合
  {ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [fragments] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

動作指定
action log

情報の削除
no <sequence>

[入力モード]

```
(config-ext-nacl)
```

[パラメータ]

<sequence>

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 | igmp | tcp | udp}

IPv4 パケットの上位プロトコル条件を指定します。
ただし，すべてのプロトコルを対象とする場合は ip を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   0 ～ 255（10 進数）またはプロトコル名称を指定します。
   指定可能なプロトコル名称は「表 4-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>}

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>，any，own-address <source ipv4 wildcard>，host own-address，own または range-address <source ipv4 start> <source ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
host <source ipv4> を入力した場合は <source ipv4> の完全一致をフィルタ条件とします。
any を指定すると，送信元 IPv4 アドレスをフィルタ条件とはしません。
own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
range-address は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の access-group コマンドだけ有効になります。
own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを送信元 IPv4 アドレスとしてフィルタ条件にします。
own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
なお，own-address および own を指定したインタフェースがマルチホームの場合はプライマリ IPv4 アドレスが対象になります。
range-address を指定した場合は，<source ipv4 start> から <source ipv4 end> の範囲をフィルタ条件とします。
<source ipv4 end> は <source ipv4 start> より大きい IPv4 アドレスを指定してください。
IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

{{eq | neq} <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 4-3　TCP で指定可能なポート名称」および「表 4-4　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。
   neq を指定した場合は，<source port> 以外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> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>}

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>，any，own-address <destination ipv4 wildcard>，host own-address，own または range-address <destination ipv4 start> <destination ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <destination ipv4> を入力した場合は <destination ipv4> の完全一致をフィルタ条件とします

す。
any を指定すると，宛先 IPv4 アドレスをフィルタ条件とはしません。
own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
range-address は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の access-group コマンドだけ有効になります。
own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを宛先 IPv4 アドレスとしてフィルタ条件にします。
own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
なお，own-address および own を指定したインタフェースがマルチホームの場合はプライマリ IPv4 アドレスが対象になります。
range-address を指定した場合は <destination ipv4 start> から <destination ipv4 end> の範囲をフィルタ条件とします。
<destination ipv4 end> は <destination ipv4 start> より大きい IPv4 アドレスを指定してください。
IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

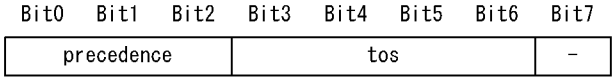
{{eq | neq} <destination port> | range <destination port start> <destination port end>}

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 4-3　TCP で指定可能なポート名称」および「表 4-4　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。
   neq を指定した場合は，<destination port> 以外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>

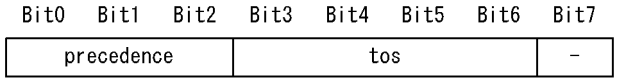
本パラメータは，ToS フィールドのビット 3 ～ 6 の 4 ビットである tos 値を指定します。
受信パケットの ToS フィールドのビット 3 ～ 6 の 4 ビットと比較します。



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 4-6　指定可能な tos 名称」を参照してください。

precedence <precedence>

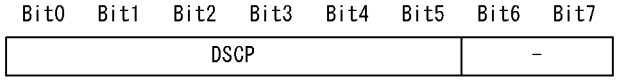
本パラメータは，ToS フィールドの上位 3 ビットである precedence 値を指定します。
受信パケットの ToS フィールド上位 3 ビットと比較します。



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 4-7　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。



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 4-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。
ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。

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
   なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。
fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。

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
   なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。

psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。

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
   なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。

rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。

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
   なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。

syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。

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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。

urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。

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
   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 4-11　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

<igmp type>

IGMP タイプを指定します。

プロトコルが IGMP 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。

fragments

2 番目以降のフラグメントパケットを指定します。

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
   なし

vlan {<vlan id> | <vlan id list name>}

VLAN ID または VLAN リスト名称を指定します。

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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は，必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

log

指定したアクセスリストで廃棄したパケットをアクセスリストロギングの対象とします。

1. 本パラメータ省略時の初期値
   なし（アクセスリストロギングを使用しません）
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]

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. 送信元アドレスワイルドカードマスクおよび宛先アドレスワイルドカードマスクに 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。

[関連コマンド]

access-list

ip access-group

ip access-list resequence

permit（ip access-list extended）

remark

vlan-list

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

[<sequence>] deny {<ipv4> [<ipv4 wildcard>] | host <ipv4> | any} [動作指定]

動作指定

action log

情報の削除

no <sequence>

［入力モード］

```
(config-std-nacl)
```

［パラメータ］

<sequence>

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> 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マスクを 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> を入力した場合は <ipv4> の完全一致をフィルタ条件とします。
   any を指定すると，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

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

log

指定したアクセスリストで廃棄したパケットをアクセスリストロギングの対象とします。

1. 本パラメータ省略時の初期値
   なし（アクセスリストロギングを使用しません）
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]

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. アドレスワイルドカードマスクに 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]

access-list

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

[<sequence>] deny { フィルタ条件 } [動作指定]

フィルタ条件

- 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 | own-address <own address length>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 上位プロトコルが TCP の場合
  tcp {<source ipv6>/<length> | host <source ipv6> | any | own-address <own address length>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}][{[established] | [{ack|+ack|-ack}] [{fin|+fin|-fin}] [{psh|+psh|-psh}] [{rst|+rst|-rst}] [{syn|+syn|-syn}] [{urg|+urg|-urg}]}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 上位プロトコルが UDP の場合
  udp {<source ipv6>/<length> | host <source ipv6> | any | own-address <own address length>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 上位プロトコルが ICMP の場合
  icmp {<source ipv6>/<length> | host <source ipv6> | any | own-address <own address length>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

動作指定

action log

情報の削除

no <sequence>

［入力モード］

```
(config-ipv6-acl)
```

［パラメータ］

<sequence>

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。
   指定可能なプロトコル名称は「表 4-2　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 | own-address <own address length>}

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>，own-address <own address length> または any を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は <source ipv6> の完全一致をフィルタ条件とします。
   any を指定すると，送信元 IPv6 アドレスをフィルタ条件とはしません。
   own-address は VLAN インタフェースに対しての traffic-filter コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを送信元 IPv6 アドレスとしてフィルタ条件とします。
   <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 | neq} <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 4-3　TCP で指定可能なポート名称」および「表 4-5　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。
neq を指定した場合は，<source port> 以外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> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>}

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>，own-address <own address length>，host <destination ipv6>，host own-address，any，own または range-address <destination ipv6 start> <destination ipv6 end> を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は <destination ipv6> の完全一致をフィルタ条件とします。
   any を指定すると，宛先 IPv6 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての traffic-filter コマンドだけ有効になります。
   range-address は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の traffic-filter コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレスとしてフィルタ条件とします。
   own を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレス，IPv6 グローバルアドレスのプレフィックス長を <length> としてフィルタ条件にします。
   range-address を指定した場合は，<destination ipv6 start> から <destination ipv6 end> の範囲をフィルタ条件とします。
   <destination ipv6 end> は <destination ipv6 start> より大きい IPv6 アドレスを指定してください。
   <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 | neq} <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 4-3　TCP で指定可能なポート名称」および「表 4-5　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。

neq を指定した場合は，<destination port> 以外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）

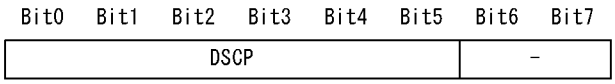
2. 値の設定範囲

0 ～ 255（10 進数）を指定します。

dscp <dscp>

本パラメータは，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。



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 4-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。

ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。

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

なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。
fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。
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
   なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。
psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。
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
   なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。
rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。
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
   なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。
syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。
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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。
urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。
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
   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 4-12　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 list name>}

VLAN ID または VLAN リスト名称を指定します。

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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は，必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

log

指定したアクセスリストで廃棄したパケットをアクセスリストロギングの対象とします。

1. 本パラメータ省略時の初期値
   なし（アクセスリストロギングを使用しません）
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]

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。

[関連コマンド]

ipv6 traffic-filter

ipv6 access-list resequence

permit（ipv6 access-list）

remark

vlan-list

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

[<sequence>] deny { フィルタ条件 } [動作指定]

フィルタ条件

{<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 | slow-protocol } [<ethernet type>] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

動作指定

action log

情報の削除

no <sequence>

［入力モード］

```
(config-ext-macl)
```

［パラメータ］

<sequence>

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> 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> を入力した場合は <source mac> の完全一致をフィルタ条件とします。
   any を指定すると，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 | slow-protocol}

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，pvst-plus-bpdu または slow-protocol を指定します。
   <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> を入力した場合は <destination mac> の完全一致をフィルタ条件とします。
   any を指定すると，宛先 MAC アドレスをフィルタ条件とはしません。
   bpdu を指定すると，BPDU 制御パケットをフィルタ条件とします。
   cdp を指定すると，CDP 制御パケットをフィルタ条件とします。
   lacp または slow-protocol を指定すると，slow プロトコルパケットをフィルタ条件とします。
   本装置では LACP と IEEE802.3ah/UDLD 機能で slow プロトコルパケットを使用しています。
   lldp を指定すると，LLDP 制御パケットをフィルタ条件とします。
   oadp を指定すると，OADP 制御パケットをフィルタ条件とします。
   pvst-plus-bpdu を指定すると，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 4-9　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 list name>}

VLAN ID または VLAN リスト名称を指定します。
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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は，必ず本パラメータを動作パラメータ全体の先頭に設定して

ください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

log

指定したアクセスリストで廃棄したパケットをアクセスリストロギングの対象とします。

1. 本パラメータ省略時の初期値
   なし（アクセスリストロギングを使用しません）
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]

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 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 4-10　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

vlan-list

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。

装置当たり，指定できるインタフェースへの設定数については「■インタフェースへの設定数」を参照してください。

ポリシーベースルーティングのパラメータ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際は，VLANインタフェースのInbound（受信側）を指定し，かつ中継種別にレイヤ3中継を指定してください。

ポリシーベーススイッチングのパラメータ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際は，イーサネットインタフェースのInbound（受信側）を指定してください。

[入力形式]

情報の設定

- イーサネットインタフェース
  ip access-group {<access list number> | <access list name>} {in | out} layer2-forwarding
- VLANインタフェース
  ip access-group {<access list number> | <access list name>} {in | out} {layer2-forwarding | layer3-forwarding}

情報の削除

- イーサネットインタフェース
  no ip access-group {<access list number> | <access list name>} {in | out} layer2-forwarding
- VLANインタフェース
  no ip access-group {<access list number> | <access list name>} {in | out} {layer2-forwarding | layer3-forwarding}

[入力モード]

(config-if)

[パラメータ]

{<access list number> | <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
   <access list number>の場合は，1～199，1300～2699（10進数）を指定します。
   <access list name>の場合は，31文字以内の名前を指定します。
   詳細は，「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

layer2-forwarding

フロー検出する中継種別を指定します。
layer2-forwarding はレイヤ 2 中継する IP パケットをフロー検出します。
本パラメータはイーサネットインタフェースに適用する場合だけ有効です。

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
   なし

{layer2-forwarding | layer3-forwarding}

フロー検出する中継種別を指定します。
layer2-forwarding はレイヤ 2 中継する IP パケットをフロー検出します。
layer3-forwarding はレイヤ 3 中継する IP パケットをフロー検出します。
本パラメータは VLAN インタフェースに適用する場合だけ有効です。

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
   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 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. 同一のイーサネットインタフェースに対しては，Inbound と Outbound にそれぞれ一つ設定できます。
   同一の VLAN インタフェースに対しては，Inbound のレイヤ 2 中継とレイヤ 3 中継，Outbound のレイヤ 2 中継とレイヤ 3 中継にそれぞれ一つ設定できます。
   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してください。
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. フロー配分パターンが default standard，default standard-advance，default extended，default extended-advance，filter-only extended，filter-only extended-advance，filter extended，filter extended-advance，qos extended または qos extended-advance の場合に設定できます。
4. フロー検出条件に own-address または own パラメータがある場合は，対象インタフェースに IPv4 アドレスが設定されているときに設定できます。
5. 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 パラメータのすべての 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. イーサネットインタフェースおよびVLANインタフェースのレイヤ2中継に対して適用する場合は，フロー検出条件にTCPフラグおよびtosパラメータがないときに設定できます。
8. VLANインタフェースのレイヤ2中継に対して適用する場合は，MACモードが設定されていないときに設定できます。
9. 動作指定にlogを指定したアクセスリストを設定する場合，system hardware-modeのaccess-logを設定してください。

［関連コマンド］

access-list

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，フラグメントパケット，ToS フィールドの値，ポート番号，TCP フラグ，ICMP タイプ，ICMP コードおよび IGMP タイプ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。

装置当たり，作成できるアクセスリスト数およびフィルタ条件数については「■アクセスリスト作成数」を参照してください。

ポリシーベースルーティングのパラメータは，フィルタ動作に permit を指定した場合に指定できます。なお，該当アクセスリストをアクセスグループコマンドでインタフェースに適用する際は，VLAN インタフェースの Inbound（受信側）を指定し，かつ中継種別にレイヤ 3 中継を指定してください。

ポリシーベーススイッチングのパラメータは，フィルタ動作に permit を指定した場合に指定できます。なお，該当アクセスリストをアクセスグループコマンドでインタフェースに適用する際は，イーサネットインタフェースの Inbound（受信側）を指定してください。

［入力形式］

情報の設定

ip access-list extended {<access list number> | <access list name>}

情報の削除

no ip access-list extended {<access list number> | <access list name>}

［入力モード］

(config)

［パラメータ］

{<access list number> | <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。

IPv4 アドレスフィルタ，IPv6 フィルタ，MAC フィルタおよび Advance フィルタですでに使用されている名称は指定できません。

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
   <access list number> の場合は，100 ～ 199，2000 ～ 2699（10 進数）を指定します。
   <access list name> の場合は，31 文字以内の名前を指定します。
   詳細は，「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. access-list で指定した 100-199 または 2000-2699 の <access list number> と同じリストを操作できます。
2. 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]

access-list

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 number> | <access list name>} [<starting sequence> [<increment sequence>]]

[入力モード]

(config)

[パラメータ]

{<access list number> | <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
   <access list number> の場合は，1 ～ 199 または 1300 ～ 2699（10 進数）を指定します。
   <access list name> の場合は，31 文字以内の名前を指定します。
   詳細は，「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］

access-list

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。

装置当たり，作成できるアクセスリスト数およびフィルタ条件数については「■アクセスリスト作成数」を参照してください。

[入力形式]

情報の設定

ip access-list standard {<access list number> | <access list name>}

情報の削除

no ip access-list standard {<access list number> | <access list name>}

[入力モード]

(config)

[パラメータ]

{<access list number> | <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。

IPv4 パケットフィルタ，IPv6 フィルタ，MAC フィルタおよび Advance フィルタですでに使用されている名称は指定できません。

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
   <access list number> の場合は，1 ～ 99，1300 ～ 1999（10 進数）を指定します。
   <access list name> の場合は，31 文字以内の名前を指定します。
   詳細は，「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. access-list で指定した 1-99 または 1300-1999 の <access list number> と同じリストを操作できます。
2. 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］

access-list

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。

装置当たり，作成できるアクセスリスト数およびフィルタ条件数については「■アクセスリスト作成数」を参照してください。

ポリシーベースルーティングのパラメータは，フィルタ動作に permit を指定した場合に指定できます。なお，該当アクセスリストをアクセスグループコマンドでインタフェースに適用する際は，VLAN インタフェースの Inbound（受信側）を指定し，かつ中継種別にレイヤ 3 中継を指定してください。

ポリシーベーススイッチングのパラメータは，フィルタ動作に permit を指定した場合に指定できます。なお，該当アクセスリストをアクセスグループコマンドでインタフェースに適用する際は，イーサネットインタフェースの Inbound（受信側）を指定してください。

[入力形式]

情報の設定

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。

IPv4 アドレスフィルタ，IPv4 パケットフィルタ，MAC フィルタおよび Advance フィルタですでに使用されている名称は指定できません。

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
   31 文字以内の名前を指定します。
   詳細は，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. 作成済みの IPv4 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
   31 文字以内の名前を指定します。
   詳細は,「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。

装置当たり，指定できるインタフェースへの設定数については「■インタフェースへの設定数」を参照してください。

ポリシーベースルーティングのパラメータ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際は，VLANインタフェースのInbound（受信側）を指定し，かつ中継種別にレイヤ3中継を指定してください。

ポリシーベーススイッチングのパラメータ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際は，イーサネットインタフェースのInbound（受信側）を指定してください。

［入力形式］

情報の設定

- イーサネットインタフェース
  ipv6 traffic-filter <access list name> {in | out} layer2-forwarding
- VLANインタフェース
  ipv6 traffic-filter <access list name> {in | out} {layer2-forwarding | layer3-forwarding}

情報の削除

- イーサネットインタフェース
  no ipv6 traffic-filter <access list name> {in | out} layer2-forwarding
- VLANインタフェース
  no ipv6 traffic-filter <access list name> {in | out} {layer2-forwarding | layer3-forwarding}

［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
   31文字以内の名前を指定します。
   詳細は，「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

layer2-forwarding

フロー検出する中継種別を指定します。
layer2-forwarding はレイヤ 2 中継する IP パケットをフロー検出します。
本パラメータはイーサネットインタフェースに適用する場合だけ有効です。
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
   なし

{layer2-forwarding | layer3-forwarding}

フロー検出する中継種別を指定します。
layer2-forwarding はレイヤ 2 中継する IP パケットをフロー検出します。
layer3-forwarding はレイヤ 3 中継する IP パケットをフロー検出します。
本パラメータは VLAN インタフェースに適用する場合だけ有効です。
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
   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. 同一のイーサネットインタフェースに対しては，Inbound と Outbound にそれぞれ一つ設定できます。
   同一の VLAN インタフェースに対しては，Inbound のレイヤ 2 中継とレイヤ 3 中継，Outbound のレイヤ 2 中継とレイヤ 3 中継にそれぞれ一つ設定できます。
   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してください。
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. フロー配分パターンが default standard，default standard-advance，default extended，default extended-advance，filter-only extended，filter-only extended-advance，filter extended，filter extended-advance，qos extended または qos extended-advance の場合に設定できます。
4. 経路系テーブルエントリ配分パターンが ipv4-uni standard，ipv4-uni extended の場合，IPv6 ポリシーベースルーティングの設定がある IPv6 アクセスリストは設定できません。
   上記以外の経路系テーブルエントリ配分パターンの場合に設定できます。
5. フロー検出条件に own-address または own パラメータがある場合は，対象インタフェースに一つだけ IPv6 グローバルアドレスが設定されているときに設定できます。
6. フロー検出条件パラメータの送信元アドレスに any または Len が 64 以下に指定されているときに設定できます。
7. 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 パラメータのすべての VLAN ID が含

まれていれば設定できます。

8. 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 パラメータがないときに設定できます。
9. イーサネットインタフェースおよび VLAN インタフェースのレイヤ 2 中継に対して適用する場合は，フロー検出条件に TCP フラグおよびトラフィッククラスフィールドパラメータがないときに設定できます。
10. VLAN インタフェースのレイヤ 2 中継に対して適用する場合は，MAC モードが設定されていないときに設定できます。
11. 動作指定に log を指定したアクセスリストを設定する場合，system hardware-mode の access-log を設定してください。

［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。

装置当たり，指定できるインタフェースへの設定数については「■インタフェースへの設定数」を参照してください。

ポリシーベーススイッチングのパラメータ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際は，イーサネットインタフェースの Inbound（受信側）を指定してください。

［入力形式］

情報の設定

mac access-group <access list name> {in | out} layer2-forwarding

情報の削除

no mac access-group <access list name> {in | out} layer2-forwarding

［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
   31 文字以内の名前を指定します。
   詳細は，「パラメータに指定できる値」の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

layer2-forwarding

フロー検出する中継種別を指定します。

layer2-forwarding はレイヤ 2 中継する非 IP パケットをフロー検出します。

1. 本パラ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. 同一のインタフェースに対して MAC フィルタを Inbound と Outbound にそれぞれ一つ設定できます。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. フロー配分パターンが default standard，default standard-advance，default extended，default extended-advance，filter-only extended，filter-only extended-advance，filter extended，filter extended-advance，qos extended または qos extended-advance の場合に設定できます。
4. 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 パラメータのすべての VLAN ID が含まれていれば設定できます。
5. 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 パラメータがないときに設定できます。
6. 動作指定に log を指定したアクセスリストを設定する場合，system hardware-mode の access-log を設定してください。

[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。

装置当たり，作成できるアクセスリスト数およびフィルタ条件数については「■アクセスリスト作成数」を参照してください。

ポリシーベーススイッチングのパラメータは，フィルタ動作に permit を指定した場合に指定できます。なお，該当アクセスリストをアクセスグループコマンドでインタフェースに適用する際は，イーサネットインタフェースの Inbound（受信側）を指定してください。

[入力形式]

情報の設定

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。

IPv4 アドレスフィルタ，IPv4 パケットフィルタ，IPv6 フィルタおよび Advance フィルタですでに使用されている名称は指定できません。

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
   31 文字以内の名前を指定します。
   詳細は，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 作成済みの IPv4 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
   31 文字以内の名前を指定します。
   詳細は,「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（advance access-list）

Advance 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

[<sequence>] permit mac { フィルタ条件 } [動作指定]

[<sequence>] permit mac-ip { フィルタ条件 } [動作指定]

[<sequence>] permit mac-ipv6 { フィルタ条件 } [動作指定]

フィルタ条件

mac { フィルタ条件 } の場合

MAC ヘッダ条件でフロー検出する場合のフィルタ条件です。

mac {<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 | slow-protocol} [<ethernet type>][vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

mac-ip { フィルタ条件 } の場合

MAC ヘッダ条件，IPv4 ヘッダ条件および Layer4 ヘッダ条件でフロー検出する場合のフィルタ条件です。

- フラグメントパケットなしで，上位プロトコルが TCP，UDP，ICMP および IGMP 以外の場合

  mac-ip {<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 | slow-protocol} {ip | <protocol>} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- フラグメントパケットなしで，上位プロトコルが TCP の場合

  mac-ip {<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 | slow-protocol} tcp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- フラグメントパケットなしで，上位プロトコルが UDP の場合

  mac-ip {<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 | slow-protocol} udp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

- フラグメントパケットなしで，上位プロトコルが ICMP の場合
  mac-ip {<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 | slow-protocol} icmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- フラグメントパケットなしで，上位プロトコルが IGMP の場合
  mac-ip {<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 | slow-protocol} igmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [<igmp type>] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- フラグメントパケットありの場合
  mac-ip {<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 | slow-protocol} {ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [fragments] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

mac-ipv6 { フィルタ条件 } の場合

MAC ヘッダ条件，IPv6 ヘッダ条件および Layer4 ヘッダ条件でフロー検出する場合のフィルタ条件です。

- 上位プロトコルが TCP，UDP および ICMP 以外の場合
  mac-ipv6 {<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 | slow-protocol} {ipv6 | <protocol>} {<source ipv6>/<length>| host {<source

ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

- 上位プロトコルが TCP の場合
  mac-ipv6 {<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 | slow-protocol} tcp {<source ipv6>/<length>| host {<source ipv6> | own-address} | any| own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- 上位プロトコルが UDP の場合
  mac-ipv6 {<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 | slow-protocol} udp {<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]
- 上位プロトコルが ICMP の場合
  mac-ipv6 {<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 | slow-protocol} icmp {<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

動作指定

mac { フィルタ条件 } の場合

action policy-switch-list <policy switch list no.>

mac-ip { フィルタ条件 } の場合

action {policy interface vlan <vlan id> next-hop <next hop ipv4> | policy-list <policy list no.> | policy-switch-list <policy switch list no.>}

mac-ipv6 { フィルタ条件 } の場合
action {policy interface vlan <vlan id> next-hop <next hop ipv6> | policy-switch-list <policy switch list no.>}

情報の削除
no <sequence>

[入力モード]

```
(config-adv-acl)
```

[パラメータ]

<sequence>

フィルタ条件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
   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。

フィルタ条件パラメータ

{<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> 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> を入力した場合は <source mac> の完全一致をフィルタ条件とします。
   any を指定すると，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 | slow-protocol}

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，pvst-plus-bpdu または slow-protocol を指定します。
   <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> を入力した場合は <destination mac> の完全一致をフィルタ条件とします。

any を指定すると，宛先 MAC アドレスをフィルタ条件とはしません。
bpdu を指定すると，BPDU 制御パケットをフィルタ条件とします。
cdp を指定すると，CDP 制御パケットをフィルタ条件とします。
lacp または slow-protocol を指定すると，slow プロトコルパケットをフィルタ条件とします。
本装置では LACP と IEEE802.3ah/UDLD 機能で slow プロトコルパケットを使用しています。
lacp を指定すると，LACP 制御パケットをフィルタ条件とします。
lldp を指定すると，LLDP 制御パケットをフィルタ条件とします。
oadp を指定すると，OADP 制御パケットをフィルタ条件とします。
pvst-plus-bpdu を指定すると，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 4-9　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 list name>}

VLAN ID または VLAN リスト名称を指定します。
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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

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。

ctag-untagged

カスタマ Tag がないパケットの検出を指定します。

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
   なし

ctag-user-priority <priority>

カスタマ 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
   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。

ctag-vlan <vlan id>

カスタマ Tag の VLAN ID 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 ～ 4095（10 進数）を指定します。

{ip | <protocol> | icmp | igmp | tcp | udp}

フロー検出条件指定に mac-ip を指定した場合に選択できます。

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
   0 ～ 255（10 進数）またはプロトコル名称を指定します。
   指定可能なプロトコル名称は「表 4-1　指定可能なプロトコル名称（IPv4）」を参照してください。

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

フロー検出条件指定に mac-ipv6 を指定した場合に選択できます。

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。
   指定可能なプロトコル名称は「表 4-2　指定可能なプロトコル名称（IPv6）」を参照してください。

{{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>}

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>，any，own-address <source ipv4 wildcard>，host own-address，own または range-address <source ipv4 start> <source ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <source ipv4> を入力した場合は <source ipv4> の完全一致をフィルタ条件とします。
   any を指定すると，送信元 IPv4 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
   range-address は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の access-group コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを送信元 IPv4 アドレスとしてフィルタ条件にします。

own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
なお，own-address および own を指定したインタフェースがマルチホームの場合はプライマリ IPv4 アドレスが対象になります。
range-address を指定した場合は，<source ipv4 start> から <source ipv4 end> の範囲をフィルタ条件とします。
<source ipv4 end> は <source ipv4 start> より大きい IPv4 アドレスを指定してください。
IPv4 アドレス (nnn.nnn.nnn.nnn)：0.0.0.0 ～ 255.255.255.255

{<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>}

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>，own-address <own address length>，host <source ipv6>，host own-address，any，own または range-address <source ipv6 start> <source ipv6 end> を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は <source ipv6> の完全一致をフィルタ条件とします。
   any を指定すると，送信元 IPv6 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての traffic-filter コマンドだけ有効になります。
   range-address は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の traffic-filter コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを送信元 IPv6 アドレスとしてフィルタ条件とします。
   own を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを送信元 IPv6 アドレス，IPv6 グローバルアドレスのプレフィックス長を <length> としてフィルタ条件にします。
   range-address を指定した場合は <source ipv6 start> から <source ipv6 end> の範囲をフィルタ条件とします。
   <source ipv6 end> は <source ipv6 start> より大きい IPv6 アドレスを指定してください。
   <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 | neq} <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 4-3　TCP で指定可能なポート名称」,「表 4-4　UDP で指定可能なポート名称（IPv4）」および「表 4-5　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。
neq を指定した場合は，<source port> 以外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> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>}

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>，any，own-address <destination ipv4 wildcard>，host own-address，own または range-address <destination ipv4 start> <destination ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <destination ipv4> を入力した場合は <destination ipv4> の完全一致をフィルタ条件とします。
   any を指定すると，宛先 IPv4 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
   range-address は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の access-group コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを宛先 IPv4 アドレスとしてフィルタ条件にします。
   own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
   なお，own-address および own を指定したインタフェースがマルチホームの場合はプライマリ IPv4 アドレスが対象になります。
   range-address を指定した場合は，<destination ipv4 start> から <destination ipv4 end> の範囲をフィルタ検出条件とします。
   <destination ipv4 end> は <destination ipv4 start> より大きい IPv4 アドレスを指定してください。
   IPv4 アドレス (nnn.nnn.nnn.nnn)：0.0.0.0 ～ 255.255.255.255

{<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>}

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>，own-address <own address length>，host <destination ipv6>，host own-address，any，own または range-address <destination ipv6 start> <destination ipv6 end> を指定します。
<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。
<own address length> には own-address 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> を入力した場合は <destination ipv6> の完全一致をフィルタ条件とします。
any を指定すると，宛先 IPv6 アドレスをフィルタ条件とはしません。
own-address および own は，VLAN インタフェースに対しての traffic-filter コマンドだけ有効になります。
range-address は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の traffic-filter コマンドだけ有効になります。
own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレスとしてフィルタ条件とします。
own を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレス，IPv6 グローバルアドレスのプレフィックス長を <length> としてフィルタ条件にします。
range-address を指定した場合は，<destination ipv6 start> から <destination ipv6 end> の範囲をフィルタ条件とします。
<destination ipv6 end> は <destination ipv6 start> より大きい IPv6 アドレスを指定してください。
<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

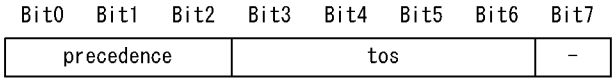
{{eq | neq} <destination port> | range <destination port start> <destination port end>}

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 4-3　TCP で指定可能なポート名称」,「表 4-4　UDP で指定可能なポート名称（IPv4)」および「表 4-5　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。
neq を指定した場合は，<destination port> 以外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>

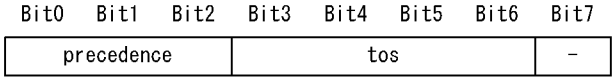
本パラメータは，ToS フィールドのビット 3 ～ 6 の 4 ビットである tos 値を指定します。
受信パケットの ToS フィールドのビット 3 ～ 6 の 4 ビットと比較します。



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 4-6　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。



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 4-7　指定可能な precedence 名称」を参照してください。

traffic-class <traffic class>

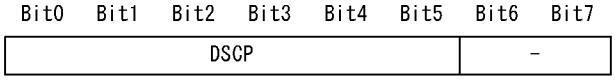
本パラメータは，トラフィッククラスフィールド値を指定します。
受信パケットのトラフィッククラスフィールドと比較します。

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>

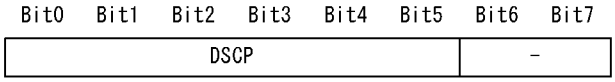
フロー検出条件種別が mac-ip の場合

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。



フロー検出条件種別が mac-ipv6 の場合

本パラメータは，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の上位 6 ビットと比較します。



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 ～ 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 4-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。

ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。

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
   なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。

fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。

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
   なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。

psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。

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
   なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。

rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。

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
   なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。

syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。

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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。
urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。

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
   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 4-11　ICMP で指定可能なメッセージ名称（IPv4）」および「表 4-12　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

<igmp type>

IGMP タイプを指定します。
プロトコルが IGMP 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。

fragments

2 番目以降のフラグメントパケットを指定します。

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
   なし

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

policy interface vlan <vlan id> next-hop <next hop ipv4>

ポリシーベースルーティングの出力先を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベースルーティングを使用しません）
2. 値の設定範囲
   <vlan id>
   VLAN ID 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。
   <next hop ipv4>
   ネクストホップ IPv4 アドレスを指定します。
   指定した送信先インタフェースに接続するネットワーク内のアドレスを指定してください。ただし，指定した送信先インタフェースに接続するネットワークへのダイレクトブロードキャスト，および指定した送信先インタフェースに設定しているアドレスは指定できません。

policy interface vlan <vlan id> next-hop <next hop ipv6>

ポリシーベースルーティングの出力先を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベースルーティングを使用しません）
2. 値の設定範囲
   <vlan id>
   VLAN ID 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 ID で指定した VLAN インタフェースは，ipv6 enable を設定し，IPv6 機能が有効である必要があります。
   <next hop ipv6>
   ネクストホップ IPv6 アドレスを指定します。
   指定した送信先インタフェースに接続するネットワークのアドレスを指定してください。ただし，指定した送信先インタフェースに設定しているアドレスは指定できません。

policy-list <policy list no.>

ポリシーベースルーティングのリスト番号を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベースルーティングを使用しません）
2. 値の設定範囲
   policy-list コマンドで設定済みのポリシーベースルーティングのリスト番号を指定します。

policy-switch-list <policy switch list no.>

ポリシーベーススイッチングのリスト番号を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベーススイッチングを使用しません）
2. 値の設定範囲
   policy-switch-list コマンドで設定済みのポリシーベーススイッチングのリスト番号を指定します。

［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 MAC アドレスおよび宛先 MAC 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 MAC 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 MAC アドレスに指定できるプロトコル名称のアドレスは「表 4-10　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 MAC アドレスおよび宛先 MAC 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. 送信元 IPv4 アドレスワイルドカードマスクおよび宛先 IPv4 アドレスワイルドカードマスクに 255.255.255.255 と入力したときは any と表示します。
4. 送信元 IPv4 アドレスおよび宛先 IPv4 アドレスを 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。
5. 動作パラメータにポリシーベースルーティングを指定する場合，フィルタ条件に設定する送信元 IPv4 アドレス，宛先 IPv4 アドレスに次のアドレスは指定できません。

   送信元 IPv4 アドレス
   　マルチキャストアドレス，内部ループバックアドレス

   宛先 IPv4 アドレス
   　マルチキャストアドレス，制限付きブロードキャストアドレス，内部ループバックアドレス
6. 送信元 IPv6 アドレスおよび宛先 IPv6 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。
7. 送信元 IPv6 アドレスおよび宛先 IPv6 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。
8. 動作パラメータにポリシーベースルーティングを指定する場合，フィルタ条件に設定する送信元 IPv6 アドレスおよび宛先 IPv6 アドレスにマルチキャストアドレス，リンクローカルアドレスは指定できません。
9. 動作パラメータにポリシーベーススイッチングを指定する場合，指定したポリシーベーススイッチングのリストで設定している VLAN ID をフィルタ条件パラメータの vlan に指定してください。このとき，VLAN リスト名称では指定できません。

［関連コマンド］

advance access-group

advance access-list resequence

deny（advance access-list）

remark

vlan-list

policy-list

policy-switch-list

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。

フラグメントパケットを検出条件に指定する場合は，入力形式が異なるので注意してください。入力形式のフラグメントパケットの場合を参照してください。

［入力形式］

情報の設定・変更

[<sequence>] permit { フィルタ条件 } [動作指定]

フィルタ条件

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

[precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

- フラグメントパケットの場合
  {ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [fragments] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

動作指定
action {policy interface vlan <vlan id> next-hop <next hop ipv4> | policy-list <policy list no.> | policy-switch-list <policy switch list no.>}

情報の削除
no <sequence>

[入力モード]

(config-ext-nacl)

[パラメータ]

<sequence>

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。

フィルタ条件パラメータ

{ip | <protocol> | icmp | igmp | tcp | udp}

IPv4 パケットの上位プロトコル条件を指定します。
ただし，すべてのプロトコルを対象とする場合は ip を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   0 ～ 255（10 進数）またはプロトコル名称を指定します。
   指定可能なプロトコル名称は「表 4-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>}

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>，any，own-address <source ipv4 wildcard>，host own-address，own または range-address <source ipv4 start> <source ipv4 end> を指定します。

<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マスクを IPv4 アドレス形式で指定します。
host <source ipv4> を入力した場合は <source ipv4> の完全一致をフィルタ条件とします。
any を指定すると，送信元 IPv4 アドレスをフィルタ条件とはしません。
own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
range-address は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の access-group コマンドだけ有効になります。
own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを送信元 IPv4 アドレスとしてフィルタ条件にします。
own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
なお，own-address および own を指定したインタフェースがマルチホームの場合は，プライマリ IPv4 アドレスが対象になります。
range-address を指定した場合は，<source ipv4 start> から <source ipv4 end> の範囲をフィルタ条件とします。
<source ipv4 end> は <source ipv4 start> より大きい IPv4 アドレスを指定してください。
IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

{{eq | neq} <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 4-3　TCP で指定可能なポート名称」および「表 4-4　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。
   neq を指定した場合は，<source port> 以外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> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>}

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>，any，own-address <destination ipv4 wildcard>，host own-address，own または range-address <destination ipv4 start> <destination ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。

host <destination ipv4> を入力した場合は <destination ipv4> の完全一致をフィルタ条件とします。
any を指定すると，宛先 IPv4 アドレスをフィルタ条件とはしません。
own-address および own は，VLAN インタフェースに対しての access-group コマンドだけ有効になります。
range-address は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の access-group コマンドだけ有効になります。
own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを宛先 IPv4 アドレスとしてフィルタ条件にします。
own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフィルタ条件にします。ホストアドレス部は任意としてフィルタ条件にします。
なお，own-address および own を指定したインタフェースがマルチホームの場合はプライマリ IPv4 アドレスが対象になります。
range-address を指定した場合は <destination ipv4 start> から <destination ipv4 end> の範囲をフィルタ条件とします。
<destination ipv4 end> は <destination ipv4 start> より大きい IPv4 アドレスを指定してください。
IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

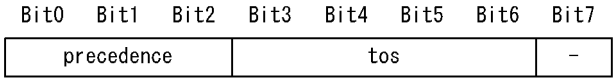
{{eq | neq} <destination port> | range <destination port start> <destination port end>}

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 4-3　TCP で指定可能なポート名称」および「表 4-4　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。
   neq を指定した場合は，<destination port> 以外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。

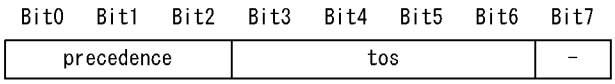


1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 15（10 進数）または tos 名称を指定します。
   指定可能な tos 名称は「表 4-6　指定可能な tos 名称」を参照してください。

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。

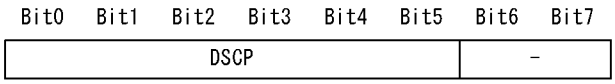
受信パケットの ToS フィールド上位 3 ビットと比較します。



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 4-7　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。



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 4-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。
ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。

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
   なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。
fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。

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
   なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。
psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。
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
   なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。
rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。
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
   なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。
syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。
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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。
urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。
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
   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 4-11　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

<igmp type>

IGMP タイプを指定します。

プロトコルが IGMP 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。

fragments

2 番目以降のフラグメントパケットを指定します。

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
   なし

vlan {<vlan id> | <vlan id list name>}

VLAN ID または VLAN リスト名称を指定します。

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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は，必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

policy interface vlan <vlan id> next-hop <next hop ipv4>

ポリシーベースルーティングの出力先を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベースルーティングを使用しません）
2. 値の設定範囲
   <vlan id>
   VLAN ID 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。
   <next hop ipv4>
   ネクストホップ IPv4 アドレスを指定します。
   指定した送信先インタフェースに接続するネットワーク内のアドレスを指定してください。ただし，指定した送信先インタフェースに接続するネットワークへのダイレクトブロードキャスト，および指定した送信先インタフェースに設定しているアドレスは指定できません。

policy-list <policy list no.>

ポリシーベースルーティングのリスト番号を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベースルーティングを使用しません）
2. 値の設定範囲
   policy-list コマンドで設定済みのポリシーベースルーティングのリスト番号を指定します。

policy-switch-list <policy switch list no.>

ポリシーベーススイッチングのリスト番号を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベーススイッチングを使用しません）
2. 値の設定範囲
   policy-switch-list コマンドで設定済みのポリシーベーススイッチングのリスト番号を指定します。

[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. 送信元アドレスワイルドカードマスクおよび宛先アドレスワイルドカードマスクに 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. 動作パラメータにポリシーベースルーティングを指定する場合，フィルタ条件に設定する送信元 IPv4 アドレスおよび宛先 IPv4 アドレスに次のアドレスは指定できません。

   送信元 IPv4 アドレス
   　マルチキャストアドレス，内部ループバックアドレス

   宛先 IPv4 アドレス

マルチキャストアドレス，制限付きブロードキャストアドレス，内部ループバックアドレス

4. 動作パラメータにポリシーベーススイッチングを指定する場合，指定したポリシーベーススイッチングのリストで設定している VLAN ID をフィルタ条件パラメータの vlan に指定してください。このとき，VLAN リスト名称では指定できません。

［関連コマンド］

access-list

ip access-group

ip access-list resequence

deny（ip access-list extended）

remark

vlan-list

policy-list

policy-switch-list

permit（ip access-list standard）

IPv4 アドレスフィルタでのアクセスを許可する条件を指定します。

［入力形式］

情報の設定・変更

[<sequence>] permit {<ipv4> [<ipv4 wildcard>] | host <ipv4> | any}

情報の削除

no <sequence>

［入力モード］

(config-std-nacl)

［パラメータ］

<sequence>

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> 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マスクを 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> を入力した場合は <ipv4> の完全一致をフィルタ条件とします。
   any を指定すると，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］

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. アドレスワイルドカードマスクに 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］

access-list

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

[<sequence>] permit { フィルタ条件 } [動作指定]

フィルタ条件

- 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 | own-address <own address length>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 上位プロトコルが TCP の場合
  tcp {<source ipv6>/<length> | host <source ipv6> | any | own-address <own address length>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 上位プロトコルが UDP の場合
  udp {<source ipv6>/<length> | host <source ipv6> | any | own-address <own address length>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq}<destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 上位プロトコルが ICMP の場合
  icmp {<source ipv6>/<length> | host <source ipv6> | any | own-address <own address length>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

動作指定

action {policy interface vlan <vlan id> next-hop <next hop ipv6>| policy-switch-list <policy switch list no.>}

情報の削除

no <sequence>

［入力モード］

(config-ipv6-acl)

［パラメータ］

<sequence>

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。

フィルタ条件パラメータ

{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。
   指定可能なプロトコル名称は「表 4-2　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 | own-address <own address length>}

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>，own-address <own address length> または any を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は <source ipv6> の完全一致をフィルタ条件とします。
   any を指定すると，送信元 IPv6 アドレスをフィルタ条件とはしません。
   own-address は VLAN インタフェースに対しての traffic-filter コマンドだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを送信元 IPv6 アドレスとしてフィルタ条件とします。
   <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 | neq} <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 4-3　TCP で指定可能なポート名称」および「表 4-5　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。
   neq を指定した場合は，<source port> 以外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> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>}

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>，own-address <own address length>，host <destination ipv6>，host own-address，any，own または range-address <destination ipv6 start> <destination ipv6 end> を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は <destination ipv6> の完全一致をフィルタ条件とします。
   any を指定すると，宛先 IPv6 アドレスをフィルタ条件とはしません。
   own-address および own は，VLAN インタフェースに対しての traffic-filter コマンドだけ有効になります。
   range-address はイーサネットインタフェースおよび VLAN インタフェースに対しての traffic-filter コマンドだけ有効なります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレスとしてフィルタ条件とします。
   own を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレス，IPv6 グローバルアドレスのプレフィックス長を <length> としてフィルタ条件にします。
   range-address を指定した場合は <destination ipv6 start> から <destination ipv6 end> の範囲をフィルタ条件とします。
   <destination ipv6 end> は <destination ipv6 start> より大きい IPv6 アドレスを指定してください。
   <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 | neq} <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 4-3　TCP で指定可能なポート名称」および「表 4-5　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。
   neq を指定した場合は，<destination port> 以外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。

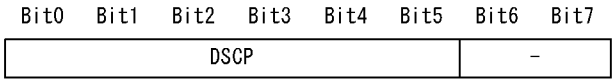
traffic-class <traffic class>

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，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。



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 4-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。
ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。

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
   なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。

fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。

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
   なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。

psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。

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
   なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。

rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。

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
   なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。

syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。

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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。

urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。

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
   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 4-12　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 list name>}

VLAN ID または VLAN リスト名称を指定します。
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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。
1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は，必ず本パラメータを動作パラメータ全体の先頭に設定してください。
1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

policy interface vlan <vlan id> next-hop <next hop ipv6>

ポリシーベースルーティングの出力先を指定します。
1. 本パラメータ省略時の初期値
   なし（ポリシーベースルーティングを使用しません）

2. 値の設定範囲
   <vlan id>
   VLAN ID 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 ID で指定した VLAN インタフェースは，ipv6 enable を設定し，IPv6 機能が有効である必要があります。
   <next hop ipv6>
   ネクストホップ IPv6 アドレスを指定します。
   指定した送信先インタフェースに接続するネットワークのアドレスを指定してください。ただし，指定した送信先インタフェースに設定しているアドレスは指定できません。

policy-switch-list <policy switch list no.>

ポリシーベーススイッチングのリスト番号を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベーススイッチングを使用しません）
2. 値の設定範囲
   policy-switch-list コマンドで設定済みのポリシーベーススイッチングのリスト番号を指定します。

[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. 動作パラメータにポリシーベースルーティングを指定する場合，フィルタ条件に設定する送信元 IPv6 アドレスおよび宛先 IPv6 アドレスに，マルチキャストアドレス，リンクローカルアドレスは指定できません。
4. 動作パラメータにポリシーベーススイッチングを指定する場合，指定したポリシーベーススイッチングのリストで設定している VLAN ID をフィルタ条件パラメータの vlan に指定してください。このとき，VLAN リスト名称では指定できません。

[関連コマンド]

ipv6 traffic-filter

ipv6 access-list resequence

deny（ipv6 access-list）

remark

vlan-list

policy-switch-list

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

[<sequence>] permit { フィルタ条件 } [動作指定]

フィルタ条件

{<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 | slow-protocol } [<ethernet type>] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

動作指定

action policy-switch-list <policy switch list no.>

情報の削除

no <sequence>

［入力モード］

```
(config-ext-macl)
```

［パラメータ］

<sequence>

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。

フィルタ条件パラメータ

{<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> 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> を入力した場合は <source mac> の完全一致をフィルタ条件とします。
   any を指定すると，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 | slow-protocol }

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，pvst-plus-bpdu または slow-protocol を指定します。
   <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> を入力した場合は <destination mac> の完全一致をフィルタ条件とします。
   bpdu を指定すると，BPDU 制御パケットをフィルタ条件とします。
   cdp を指定すると，CDP 制御パケットをフィルタ条件とします。
   lacp または slow-protocol を指定すると，slow プロトコルパケットをフィルタ条件とします。
   本装置では LACP と IEEE802.3ah/UDLD 機能で slow プロトコルパケットを使用しています。
   lldp を指定すると，LLDP 制御パケットをフィルタ条件とします。
   oadp を指定すると，OADP 制御パケットをフィルタ条件とします。
   pvst-plus-bpdu を指定すると，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 4-9　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 list name>}

VLAN ID または VLAN リスト名称を指定します。

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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は，必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

policy-switch-list <policy switch list no.>

ポリシーベーススイッチングのリスト番号を指定します。

1. 本パラメータ省略時の初期値
   なし（ポリシーベーススイッチングを使用しません）
2. 値の設定範囲
   policy-switch-list コマンドで設定済みのポリシーベーススイッチングのリスト番号を指定します。

［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 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 4-10　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. 動作パラメータにポリシーベーススイッチングを指定する場合，指定したポリシーベーススイッチングのリストで設定している VLAN ID をフィルタ条件パラメータの vlan に指定してください。このとき，VLAN リスト名称では指定できません。

［関連コマンド］

mac access-group

mac access-list resequence

deny（mac access-list extended）

remark

vlan-list

policy-switch-list

remark

アクセスリストの補足説明を指定します。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，Advance 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)
(config-adv-acl)
```

[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]

advance access-list

ip access-list standard

ip access-list extended

ipv6 access-list

mac access-list extended

5 アクセスリストロギング

access-log enable
access-log interval
access-log rate-limit
access-log threshold

access-log enable

アクセスリストロギングを有効にします。

[入力形式]

情報の設定
　access-log enable

情報の削除
　no access-log enable

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

アクセスリストロギングを無効にします。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映します。

[注意事項]

1. 本コンフィグレーションを設定する場合，system hardware-mode の access-log を設定してください。

[関連コマンド]

access-list

deny（advance access-list）

deny（ip access-list extended）

deny（ip access-list standard）

deny（ipv6 access-list）

deny（mac access-list extended）

system hardware-mode

access-log interval

アクセスリストロギングでのアクセスリストログ出力の時間間隔を指定します。

［入力形式］

情報の設定

access-log interval {<minutes> | unlimit}

情報の削除

no access-log interval

［入力モード］

(config)

［パラメータ］

{<minutes> | unlimit}

アクセスリストログを出力する時間間隔を指定します。

<minutes>

時間間隔を分単位で指定します。

unlimit

時間間隔を契機としたアクセスリストログの出力はしません。管理しているアクセスリストログ情報を確認するためには，運用コマンド show access-log flow を使用してください。

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
   5 ～ 1440（24 時間），unlimit

［コマンド省略時の動作］

5 分間隔でアクセスリストログを出力します。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映します。

［注意事項］

1. 本コマンド入力時，アクセスリストロギングが管理しているすべてのアクセスリストログ情報をクリアします。

［関連コマンド］

access-log enable

access-log rate-limit

BSU，CSU または MSU 当たり，1 秒間に CPU へ転送するパケット数の上限値を指定します。上限値を超えた場合，パケットは廃棄します。

［入力形式］

情報の設定

access-log rate-limit <number>

情報の削除

no access-log rate-limit

［入力モード］

(config)

［パラメータ］

<number>

1 秒間に CPU へ転送するパケット数の上限値を指定します。0 を指定した場合は転送しません。

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
   0 または 10 ～ 250

［コマンド省略時の動作］

1 秒間に CPU へ転送するパケット数の上限値は 100 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，すぐに運用に反映します。

［注意事項］

1. 本コマンドで指定する値は CPU へ転送するパケット数です。指定値までの転送を保証するものではありません。

［関連コマンド］

access-log enable

access-log threshold

指定したスレッシュホールドのＮ倍（Ｎは１から）のパケット数に達した時点でアクセスリストログを出力します。

［入力形式］

情報の設定
　access-log threshold <packet count>

情報の削除
　no access-log threshold

［入力モード］

(config)

［パラメータ］

<packet count>
　アクセスリストログの出力契機とするパケット数を指定します。
　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 ～ 4294967295

［コマンド省略時の動作］

スレッシュホールドによるアクセスリスト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，すぐに運用に反映します。

［注意事項］

1. 一つ目のフロー受信時にアクセスリストログを出力します。その後，同一フローのパケット数が，指定したスレッシュホールドのＮ倍（Ｎは１から）に達した時点で出力します。
2. スレッシュホールドに小さい値を設定し，アクセスリストロギング対象のパケットが大量に発生した場合，短い時間で多量のアクセスリストログが出力します。その場合，一部のアクセスリストログを出力できないことがあります。

［関連コマンド］

access-log enable

6 uRPF

ip urpf
ip verify unicast source reachable-via
ipv6 verify unicast source reachable-via

ip urpf

uRPF 機能を使用する場合に設定します。

[入力形式]

情報の設定
　ip urpf [allow-default]

情報の削除
　no ip urpf

[入力モード]

(config)

[パラメータ]

allow-default

　デフォルト経路を uRPF のチェック対象とします。
　全インタフェースでの Strict モードおよび Loose モードの両方で有効となります。

1. 本パラメータ省略時の初期値
　デフォルト経路を uRPF のチェック対象としません。
2. 値の設定範囲
　なし

[コマンド省略時の動作]

uRPF 機能を使用できません。uRPF 機能を使用する場合には，ip urpf を設定してください。

[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]

1. 本設定は IPv6 でも有効となります。
2. maximum-paths コマンドでマルチパス数に 9 以上を設定している場合は，本コマンドを設定できません。本コマンドを設定する前に，マルチパス数を 8 以下に変更してください。
　マルチパス数を 9 以上から 8 以下に変更した場合，経路情報をハードウェアに反映させるまでにある程度の時間が必要となり，この間は uRPF が誤動作するおそれがあります。そのため，マルチパス数を 9 以上から 8 以下に変更した場合は，装置再起動を実施してから本コマンドを設定することを推奨します。

[関連コマンド]

ip verify unicast source reachable-via

ipv6 verify unicast source reachable-via

ip route static maximum-paths

maximum-paths(OSPF)

maximum-paths(BGP4)

ipv6 route static maximum-paths

maximum-paths(OSPFv3)

maximum-paths(BGP4+)

ip verify unicast source reachable-via

IPv4 の uRPF を行います。

［入力形式］

情報の設定
　ip verify unicast source reachable-via { rx | any }

情報の削除
　no ip verify unicast source reachable-via

［入力モード］

(config-if)

［パラメータ］

{rx | any}
　uRPF の動作モードを設定します。

　rx
　　Strict モード

　any
　　Loose モード

1. 本パラ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］

IPv4 の uRPF 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］

1. ip urpf コマンドを設定していない場合，本コマンドは有効となりません。
2. 同一インタフェースで ipv6 verify unicast source reachable-via コマンドをすでに設定している場合，異なる動作モードは設定できません。

［関連コマンド］

ip urpf

ipv6 verify unicast source reachable-via

ipv6 verify unicast source reachable-via

IPv6 の uRPF を行います。

［入力形式］

情報の設定

ipv6 verify unicast source reachable-via { rx | any }

情報の削除

no ipv6 verify unicast source reachable-via

［入力モード］

(config-if)

［パラメータ］

{ rx | any }

uRPF の動作モードを設定します。

rx

Strict モード

any

Loose モード

1. 本パラ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］

IPv6 の uRPF 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］

1. ip urpf コマンドを設定していない場合，本コマンドは有効となりません。
2. 同一インタフェースで ip verify unicast source reachable-via コマンドをすでに設定している場合，異なる動作モードは設定できません。

［関連コマンド］

ip urpf

ip verify unicast source reachable-via

7 QoS

指定できる名称および値
advance qos-flow-group
advance qos-flow-list
advance qos-flow-list resequence
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
llrlq1-burst【AX6700S】【AX6600S】
llrlq2-burst【AX6700S】【AX6600S】
mac qos-flow-group
mac qos-flow-list
mac qos-flow-list resequence
mode
number-of-queue
predicted-tail-drop
qos（advance qos-flow-list）
qos（ip qos-flow-list）
qos（ipv6 qos-flow-list）
qos（mac qos-flow-list）
qos-queue-group

qos-queue-list
remark
set-default-user-priority
shaper auto-configuration
shaper default-user
shaper llrlq1【AX6700S】【AX6600S】
shaper llrlq2【AX6700S】【AX6600S】
shaper nif
shaper port buffer
shaper port rate-limit
shaper user
shaper user-list
shaper vlan-user-map
shaper wgq-group rate-limit【AX6700S】【AX6600S】
traffic-shape rate
upc-storm-control mode

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 7-1　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

■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 7-2　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 7-3　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 7-4　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 7-5　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 7-6　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 7-7　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 7-8　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 7-9　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	
axp	0x88f3	Alaxala Protocol

イーサネットタイプ名称	Ethernet 値	備考
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 7-10　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
slow-protocol	0180.C200.0002	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 7-11　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

メッセージ名称	メッセージ名	タイプ	コード
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 7-12　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

メッセージ名称	メッセージ名	タイプ	コード
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，次の表に示します。

表 7-13　帯域監視の値の設定範囲

設定範囲		刻み値
G 単位	1G ～ 10G	1G ※
M 単位	1M ～ 10000M	1M ※
k 単位	5 ～ 10000000	－

（凡例）－：該当しない
注※　1G，1M は，それぞれ 1000000k，1000k として扱います。

■ QoS フローリスト作成数

QoS フローリスト作成数とは，QoS フローリストの識別子として使用する名称の数です。該当するコンフィグレーションの <qos flow list name> を次に示すリスト数まで作成できます。

[AX6700S の場合]

BSU 種別による QoS フローリスト作成数を，次の表に示します。

表 7-14　BSU 種別による QoS フローリスト作成数

BSU 種別	QoS フローリスト	フロー検出および動作指定
全モデル	8574 リスト	32000 エントリ※

注※　アクセスリストのフィルタ条件のエントリも含みます。

[AX6600S の場合]

装置当たり，作成できる QoS フローリスト数とフロー検出および動作指定数は CSU 種別によって異なります。CSU 種別による QoS フローリスト作成数を，次の表に示します。

表 7-15　CSU 種別による QoS フローリスト作成数

CSU 種別	QoS フローリスト	フロー検出および動作指定
CSU-1A	4000 リスト	4000 エントリ
CSU-1B	8574 リスト	32000 エントリ※

注※　アクセスリストのフィルタ条件のエントリも含みます。

[AX6300S の場合]

装置当たり，作成できる QoS フローリスト数とフロー検出および動作指定数は MSU 種別によって異なります。MSU 種別による QoS フローリスト作成数を，次の表に示します。

表 7-16　MSU 種別による QoS フローリスト作成数

MSU 種別	QoS フローリスト	フロー検出および動作指定
MSU-1A，MSU-1A1	4000 リスト	4000 エントリ
MSU-1B，MSU-1B1	8574 リスト	32000 エントリ※

注※　アクセスリストのフィルタ条件のエントリも含みます。

■インタフェースへの設定数

インタフェースへの設定数とは，インタフェースに設定できる QoS フローリストの延べ数です。次に示すリスト数まで作成できます。

なお，受信側と送信側や，中継種別は別に数えます。例えば，同じ QoS フローリスト名称を指定するかどうかに関係なく，同一インタフェースの受信側と送信側の両方に設定した場合，2 リストと数えます。同様に，同一インタフェースにレイヤ 2 中継とレイヤ 3 中継を設定した場合，2 リストと数えます。

[AX6700S の場合]

BSU 種別によるインタフェースへの設定数を，次の表に示します。

表 7-17　BSU 種別によるインタフェースへの設定数

BSU 種別	設定可能な数
全モデル	8574 リスト

［AX6600S の場合］

装置当たり，ip qos-flow-group，ipv6 qos-flow-group，mac qos-flow-group および advance qos-flow-group を設定できる数は CSU 種別によって異なります。CSU 種別によるインタフェースへの設定数を，次の表に示します。

表 7-18　CSU 種別によるインタフェースへの設定数

CSU 種別	設定可能な数
CSU-1A	4000 リスト
CSU-1B	8574 リスト

［AX6300S の場合］

装置当たり，ip qos-flow-group，ipv6 qos-flow-group，mac qos-flow-group および advance qos-flow-group を設定できる数は MSU 種別によって異なります。MSU 種別によるインタフェースへの設定数を，次の表に示します。

表 7-19　MSU 種別によるインタフェースへの設定数

MSU 種別	設定可能な数
MSU-1A，MSU-1A1	4000 リスト
MSU-1B，MSU-1B1	8574 リスト

■ QoS フローリスト作成数とインタフェースへの設定数の算出例

QoS フローリスト作成数とインタフェースへの設定数の算出例を，次の表に示します。

表 7-20　QoS フローリスト作成数とインタフェースへの設定数の算出例

設定例	使用する QoS フローリスト作成数	使用するインタフェースへの設定数

QoS フローリスト AAA を作成して，イーサネットインタフェース 2/1 の inbound に設定
`interface gigabitethernet 2/1`
`ip qos-flow-group AAA in layer2-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action min-rate 10M`
	1 リスト	1 リスト

QoS フローリスト AAA を作成して，イーサネットインタフェース 2/1 と 2/2 の inbound に設定
`interface gigabitethernet 2/1`
`ip qos-flow-group AAA in layer2-forwarding`
 	
`interface gigabitethernet 2/2`
`ip qos-flow-group AAA in layer2-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action min-rate 10M`
	1 リスト	2 リスト

設定例	使用する QoS フローリスト作成数	使用するインタフェースへの設定数

QoS フローリスト AAA を作成して，イーサネットインタフェース 2/1 の inbound と outbound に設定
`interface gigabitethernet 2/1`
`ip qos-flow-group AAA in layer2-forwarding`
`ip qos-flow-group AAA out layer2-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action max-rate 10M`
	1 リスト	2 リスト

QoS フローリスト AAA を作成して，VLAN 2 インタフェースの inbound に layer2-forwarding と layer3-forwarding を設定
`interface vlan 2`
`ip qos-flow-group AAA in layer2-forwarding`
`ip qos-flow-group AAA in layer3-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action max-rate 10M`
	1 リスト	2 リスト

QoS フローリスト AAA を作成して，イーサネットインタフェース 2/1 の inbound に設定
QoS フローリスト BBB を作成して，イーサネットインタフェース 2/2 の inbound に設定
`interface gigabitethernet 2/1`
`ip qos-flow-group AAA in layer2-forwarding`
 	
`interface gigabitethernet 2/2`
`ip qos-flow-group BBB in layer2-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action max-rate 10M`
 	
`ip qos-flow-list BBB`
`10 qos udp any any action max-rate 10M`
`20 qos tcp any any action min-rate 10M`
	2 リスト	2 リスト

QoS フローリスト AAA を作成して，イーサネットインタフェース 2/1 の inbound に設定
QoS フローリスト BBB を作成して，イーサネットインタフェース 2/1 の outbound に設定
`interface gigabitethernet 2/1`
`ip qos-flow-group AAA in layer2-forwarding`
`ip qos-flow-group BBB out layer2-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action max-rate 10M`
 	
`ip qos-flow-list BBB`
`10 qos udp any any action max-rate 10M`
`20 qos tcp any any action min-rate 10M`
	2 リスト	2 リスト

QoS フローリスト AAA を作成して，インタフェースに適用しない
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
	1 リスト	0 リスト

advance 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，Advance QoSフローリストを適用し，QoS機能を有効にします。

装置当たり，指定できるインタフェースへの設定数については「■インタフェースへの設定数」を参照してください。

[入力形式]

情報の設定

- イーサネットインタフェース
  advance qos-flow-group <qos flow list name> {in | out} layer2-forwarding
- VLANインタフェース
  advance qos-flow-group <qos flow list name> {in | out} layer2-and-layer3-forwarding

情報の削除

- イーサネットインタフェース
  no advance qos-flow-group <qos flow list name> {in | out} layer2-forwarding
- VLANインタフェース
  no advance qos-flow-group <qos flow list name> {in | out} layer2-and-layer3-forwarding

[入力モード]

```
(config-if)
```

[パラメータ]

<qos flow list name>

Advance 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
   31文字以内の名前を指定します。
   詳細は，「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

layer2-forwarding

フロー検出する中継種別を指定します。

layer2-forwardingはレイヤ2中継するパケットをフロー検出します。

本パラメータはイーサネットインタフェースに適用する場合だけ有効です。

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

なし

layer2-and-layer3-forwarding

フロー検出する中継種別を指定します。
layer2-and-layer3-forwarding はレイヤ 2 中継するパケットおよびレイヤ 3 中継するパケットをフロー検出します。
本パラメータは VLAN インタフェースに適用する場合だけ有効です。

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
   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. 同一のインタフェースに対して Inbound と Outbound にそれぞれ一つ設定できます。
   すでに設定されている場合，いったん削除してから設定してください。
2. 実在しない Advance QoS フローリストを設定した場合は何も動作しません。Advance QoS フローリストの識別子は登録されます。
3. フロー配分パターンが default standard-advance，default extended-advance，qos-only extended-advance，filter extended-advance または qos extended-advance の場合に設定できます。
4. フロー検出条件種別に mac-ip を指定し，フロー検出条件に own-address または own パラメータがある場合は，対象インタフェースに IPv4 アドレスが設定されているときに設定できます。
5. フロー検出条件種別に mac-ipv6 を指定し，フロー検出条件に own-address パラメータがある場合は，対象インタフェースに一つだけ IPv6 グローバルアドレスが設定されているときに設定できます。
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 パラメータのすべての 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 パラメータがないときに設定できます。
8. 帯域監視をフロー検出条件に対して最大帯域制御および最低帯域監視の同時設定する場合は，Inbound で帯域監視ストームコントロールモードが upc-in-in のときに設定できます。
9. 帯域監視はイーサネットインタフェースの Inbound に設定できます。**【AX6700S】**
10. 帯域監視を Outbound に設定する場合，帯域監視ストームコントロールモードが upc-in-out のときに設定できます。**【AX6600S】【AX6300S】**
11. 帯域監視を VLAN インタフェースの Inbound に設定する場合，次のコマンドで指定する稼働 PSP 数にすべて 1 を指定してください。**【AX6600S】**
    - redundancy max-psp
    - schedule-power-control max-psp
    - adaptive-power-control max-psp

［関連コマンド］

advance qos-flow-list

advance 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 Advance QoS フローリストを作成します。

装置当たり，作成できる QoS フローリスト数とフロー検出および動作指定数については「■ QoS フローリスト作成数」を参照してください。

[入力形式]

情報の設定

advance qos-flow-list <qos flow list name>

情報の削除

no advance qos-flow-list <qos flow list name>

[入力モード]

(config)

[パラメータ]

<qos flow list name>

Advance 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
   31 文字以内の名前を指定します。
   詳細は，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 作成済みの IPv4 QoS フローリスト名称，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]

advance qos-flow-group

advance qos-flow-list resequence

qos（advance qos-flow-list）

remark

advance qos-flow-list resequence

Advance 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

advance 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 Advance 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
   31 文字以内の名前を指定します。
   詳細は,「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]

advance qos-flow-list

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。

装置当たり，指定できるインタフェースへの設定数については「■インタフェースへの設定数」を参照してください。

[入力形式]

情報の設定

- イーサネットインタフェース
  ip qos-flow-group <qos flow list name> {in | out} layer2-forwarding
- VLANインタフェース
  ip qos-flow-group <qos flow list name> {in | out} {layer2-forwarding | layer3-forwarding}

情報の削除

- イーサネットインタフェース
  no ip qos-flow-group <qos flow list name> {in | out} layer2-forwarding
- VLANインタフェース
  no ip qos-flow-group <qos flow list name> {in | out} {layer2-forwarding | layer3-forwarding}

[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
   31文字以内の名前を指定します。
   詳細は，「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

layer2-forwarding

フロー検出する中継種別を指定します。

layer2-forwardingはレイヤ2中継するIPパケットをフロー検出します。

本パラメータはイーサネットインタフェースに適用する場合だけ有効です。

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

なし

{layer2-forwarding | layer3-forwarding}

フロー検出する中継種別を指定します。

layer2-forwarding はレイヤ 2 中継する IP パケットをフロー検出します。

layer3-forwarding はレイヤ 3 中継する IP パケットをフロー検出します。

本パラメータは VLAN インタフェースに適用する場合だけ有効です。

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
   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. 同一のイーサネットインタフェースに対しては，Inbound と Outbound にそれぞれ一つ設定できます。同一の VLAN インタフェースに対しては，Inbound のレイヤ 2 中継とレイヤ 3 中継，Outbound のレイヤ 2 中継とレイヤ 3 中継にそれぞれ一つ設定できます。
   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してください。
2. 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。
3. フロー配分パターンが default standard，default standard-advance，default extended，default extended-advance，qos-only extended，qos-only extended-advance，filter extended，filter extended-advance，qos extended または qos extended-advance の場合に設定できます。
4. フロー検出条件に own-address または own パラメータがある場合は，対象インタフェースに IPv4 アドレスが設定されているときに設定できます。
5. イーサネットインタフェースおよび VLAN インタフェースのレイヤ 2 中継に対して適用する場合は，MAC モードが設定されていないときに設定できます。
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 パラメータのすべての 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 パラメータがないときに設定できます。
8. イーサネットインタフェースおよび VLAN インタフェースのレイヤ 2 中継に対して適用する場合は，フロー検出条件に TCP フラグ，tos パラメータ，動作指定に DSCP 書き換えおよび最低帯域違反時の DSCP 書き替えパラメータがないときに設定できます。
9. 帯域監視をフロー検出条件に対して最大帯域制御および最低帯域監視の同時設定をする場合は，Inbound で帯域監視ストームコントロールモードが upc-in-in のときに設定できます。
10. 帯域監視はイーサネットインタフェースの Inbound に設定できます。**【AX6700S】**
11. 帯域監視を Outbound に設定する場合，帯域監視ストームコントロールモードが upc-in-out のときに

設定できます。**【AX6600S】【AX6300S】**

12. 帯域監視を VLAN インタフェースの Inbound に設定する場合，次のコマンドで指定する稼働 PSP 数にすべて 1 を指定してください。**【AX6600S】**
    - redundancy max-psp
    - schedule-power-control max-psp
    - adaptive-power-control max-psp

［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。

装置当たり，作成できる QoS フローリスト数とフロー検出および動作指定数については「■ QoS フローリスト作成数」を参照してください。

[入力形式]

情報の設定

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
   31 文字以内の名前を指定します。
   詳細は，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 作成済みの IPv6 QoS フローリスト名称，MAC QoS フローリスト名称および Advance 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
   31 文字以内の名前を指定します。
   詳細は,「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IPv6 QoSフローリストを適用し，QoS機能を有効にします。

装置当たり，指定できるインタフェースへの設定数については「■インタフェースへの設定数」を参照してください。

［入力形式］

情報の設定

- イーサネットインタフェース
  ipv6 qos-flow-group <qos flow list name> {in | out} layer2-forwarding
- VLANインタフェース
  ipv6 qos-flow-group <qos flow list name> {in | out} {layer2-forwarding | layer3-forwarding}

情報の削除

- イーサネットインタフェース
  no ipv6 qos-flow-group <qos flow list name> {in | out} layer2-forwarding
- VLANインタフェース
  no ipv6 qos-flow-group <qos flow list name> {in | out} {layer2-forwarding | layer3-forwarding}

［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
   31文字以内の名前を指定します。
   詳細は，「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

layer2-forwarding

フロー検出する中継種別を指定します。

layer2-forwardingはレイヤ2中継するIPパケットをフロー検出します。

本パラメータはイーサネットインタフェースに適用する場合だけ有効です。

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

なし

{layer2-forwarding | layer3-forwarding}

フロー検出する中継種別を指定します。

layer2-forwarding はレイヤ 2 中継する IP パケットをフロー検出します。

layer3-forwarding はレイヤ 3 中継する IP パケットをフロー検出します。

本パラメータは VLAN インタフェースに適用する場合だけ有効です。

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
   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. 同一のイーサネットインタフェースに対しては，Inbound と Outbound にそれぞれ一つ設定できます。同一の VLAN インタフェースに対しては，Inbound のレイヤ 2 中継とレイヤ 3 中継，Outbound のレイヤ 2 中継とレイヤ 3 中継にそれぞれ一つ設定できます。
   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してください。
2. 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。
3. フロー配分パターンが default standard，default standard-advance，default extended，default extended-advance，qos-only extended，qos-only extended-advance，filter extended，filter extended-advance，qos extended または qos extended-advance の場合に設定できます。
4. フロー検出条件に own-address パラメータがある場合は，対象インタフェースに一つだけ IPv6 グローバルアドレスが設定されているときに設定できます。
5. フロー検出条件パラメータの送信元アドレスに any または Len が 64 以下に指定されているときに設定できます。
6. イーサネットインタフェースおよび VLAN インタフェースのレイヤ 2 中継に対して適用する場合は，MAC モードが設定されていないときに設定できます。
7. 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 パラメータのすべての VLAN ID が含まれていれば設定できます。
8. 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 パラメータがないときに設定できます。
9. イーサネットインタフェースおよび VLAN インタフェースのレイヤ 2 中継に対して適用する場合は，フロー検出条件に TCP フラグ，トラフィッククラスフィールドパラメータ，動作指定に DSCP 書き換えおよび最低帯域違反時の DSCP 書き替えパラメータがないときに設定できます。
10. 帯域監視をフロー検出条件に対して最大帯域制御および最低帯域監視の同時設定をする場合は，Inbound で帯域監視ストームコントロールモードが upc-in-in のときに設定できます。

11. 帯域監視はイーサネットインタフェースの Inbound に設定できます。**【AX6700S】**
12. 帯域監視を Outbound に設定する場合，帯域監視ストームコントロールモードが upc-in-out のときに設定できます。**【AX6600S】【AX6300S】**
13. 帯域監視を VLAN インタフェースの Inbound に設定する場合，次のコマンドで指定する稼働 PSP 数にすべて 1 を指定してください。**【AX6600S】**
    - redundancy max-psp
    - schedule-power-control max-psp
    - adaptive-power-control max-psp

［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。

装置当たり，作成できる QoS フローリスト数とフロー検出および動作指定数については「■ QoS フローリスト作成数」を参照してください。

[入力形式]

情報の設定

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
   31 文字以内の名前を指定します。
   詳細は，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 作成済みの IPv4 QoS フローリスト名称，MAC QoS フローリスト名称および Advance 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
   31 文字以内の名前を指定します。
   詳細は,「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

llrlq1-burst【AX6700S】【AX6600S】

該当シェーパモード
[rgq llrlq] [wgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]

LLRLQ1 に対してバーストサイズを設定します。

指定した NIF の LLRLQ1 に対して，基準となる送信帯域とバーストサイズを設定します。

該当 NIF の各インタフェースの LLRLQ1 には，設定した基準となる送信帯域とバーストサイズの比率に基づき，最大帯域値からバーストサイズが設定されます。

本パラメータの送信帯域：本パラメータのバーストサイズ =

各 LLRLQ1 の最大帯域：各 LLRLQ1 のバーストサイズ

[入力形式]

情報の設定・変更
llrlq1-burst <Mbit/s>M <byte>

情報の削除
no llrlq1-burst

[入力モード]

```
(config-sh-nif)
```

[パラメータ]

<Mbit/s>M
基準となる送信帯域を設定します。
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 ～ 1000 を指定します。

<byte>
基準となるバーストサイズを設定します。
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 ～ 32000 を指定します。

[コマンド省略時の動作]

LLRLQ1 にバーストサイズを設定しません。

[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. 本コマンドを設定する際は，llrlq1 に設定してあるユーザリストの最大帯域を 1M ～ 100M の値で設定してください。

［関連コマンド］

なし

llrlq2-burst【AX6700S】【AX6600S】

該当シェーパモード
[rgq llrlq] [wgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]

LLRLQ2 に対してバーストサイズを設定します。

指定した NIF の LLRLQ2 に対して，基準となる送信帯域とバーストサイズを設定します。

該当 NIF の各インタフェースの LLRLQ2 には，設定した基準となる送信帯域とバーストサイズの比率に基づき，最大帯域値からバーストサイズが設定されます。

本パラメータの送信帯域：本パラメータのバーストサイズ =

各 LLRLQ2 の最大帯域：各 LLRLQ2 のバーストサイズ

[入力形式]

情報の設定・変更
llrlq2-burst <Mbit/s>M <byte>

情報の削除
no llrlq2-burst

[入力モード]

```
(config-sh-nif)
```

[パラメータ]

<Mbit/s>M
基準となる送信帯域を設定します。
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 ～ 1000 を指定します。

<byte>
基準となるバーストサイズを設定します。
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 ～ 32000 を指定します。

[コマンド省略時の動作]

LLRLQ2 にバーストサイズを設定しません。

[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. 本コマンドを設定する際は，llrlq2 に設定してあるユーザリストの最大帯域を 1M ～ 100M の値で設定してください。

[関連コマンド]

なし

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。

装置当たり，指定できるインタフェースへの設定数については「■インタフェースへの設定数」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 | out} layer2-forwarding

情報の削除

no mac qos-flow-group <qos flow list name> {in | out} layer2-forwarding

[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
   31文字以内の名前を指定します。
   詳細は，「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

layer2-forwarding

フロー検出する中継種別を指定します。

layer2-forwardingはレイヤ2中継するパケットをフロー検出します。

1. 本パラ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. 同一のインタフェースに対して Inbound と Outbound にそれぞれ一つ設定できます。すでに設定されている場合，いったん削除してから設定してください。
2. 実在しない MAC QoS フローリストを設定した場合は何も動作しません。MAC QoS フローリストの識別子は登録されます。
3. フロー配分パターンが default standard，default standard-advance，default extended，default extended-advance，qos-only extended，qos-only extended-advance，filter extended，filter extended-advance，qos extended または qos extended-advance の場合に設定できます。
4. 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 パラメータのすべての VLAN ID が含まれていれば設定できます。
5. 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 パラメータがないときに設定できます。
6. 帯域監視をフロー検出条件に対して最大帯域制御および最低帯域監視の同時設定する場合は，Inbound で帯域監視ストームコントロールモードが upc-in-in のときに設定できます。
7. 帯域監視はイーサネットインタフェースの Inbound に設定できます。**【AX6700S】**
8. 帯域監視を Outbound に設定する場合，帯域監視ストームコントロールモードが upc-in-out のときに設定できます。**【AX6600S】【AX6300S】**
9. 帯域監視を VLAN インタフェースの Inbound に設定する場合，次のコマンドで指定する稼働 PSP 数にすべて 1 を指定してください。**【AX6600S】**
   - redundancy max-psp
   - schedule-power-control max-psp
   - adaptive-power-control max-psp

[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。

装置当たり，作成できる QoS フローリスト数とフロー検出および動作指定数については「■ QoS フローリスト作成数」を参照してください。

[入力形式]

情報の設定

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
   31 文字以内の名前を指定します。
   詳細は，「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 作成済みの IPv4 QoS フローリスト名称，IPv6 QoS フローリスト名称および Advance 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
   31 文字以内の名前を指定します。
   詳細は,「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

mode

シェーパモードを設定します。本コマンドは該当 NIF の階層化シェーパの帯域制御方式を決定します。本コマンドを設定した NIF のインタフェースに対してシェーパコンフィグレーションを設定している場合，変更できません。また，シェーパ自動設定機能を使用している場合，設定できません。

［入力形式］

情報の設定・変更

mode { rgq | wgq | llpq1 | llpq2 | llpq4 }[llrlq]**【AX6700S】【AX6600S】**

情報の設定

mode rgq**【AX6300S】**

情報の削除

no mode

［入力モード］

(config-sh-nif)

［パラメータ］

{ rgq | wgq | llpq1 | llpq2 | llpq4 }【AX6700S】【AX6600S】

rgq

帯域制御方式を RGQ に設定します。RGQ はユーザごとに最低帯域を保証する方式です。出力優先度はユーザ間で均等です。

wgq

帯域制御方式を WGQ に設定します。WGQ はユーザごとの重みの比率で帯域を分配します。出力優先度はユーザ間で均等です。

llpq1

シェーパモードを LLPQ1 に設定し，帯域制御方式を LLPQ に決定します。LLPQ1 はユーザごとに最低帯域を保証しながら，ユーザの一つのキューを低遅延で送信する方式です。出力優先度は，全ユーザの通常キューより，全ユーザの低遅延キューが高くなります。ユーザ間は均等です。

llpq2

シェーパモードを LLPQ2 に設定し，帯域制御方式を LLPQ に決定します。LLPQ2 はユーザごとに最低帯域を保証しながら，ユーザ内の二つのキューを低遅延で送信する方式です。出力優先度は，全ユーザの通常キューより，全ユーザの低遅延キューが高くなります。ユーザ間は均等です。

llpq4

シェーパモードを LLPQ4 に設定し，帯域制御方式を LLPQ に決定します。LLPQ4 はユーザごとに最低帯域を保証しながら，ユーザ内の四つのキューを低遅延で送信する方式です。出力優先度は，全ユーザの通常キューより，全ユーザの低遅延キューが高くなります。ユーザ間は均等です。

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
   rgq，wgq，llpq1，llpq2，llpq4 を指定します。
3. 本パラメータ使用時の注意事項

llpq1 パラメータは，キュー数が 4 の場合，4 番キューが低遅延キューとなります。キュー数が 8 の場合，8 番キューが低遅延キューとなります。
llpq2 パラメータは，キュー数が 4 の場合，3 番，4 番のキューが低遅延キューとなります。
キュー数が 8 の場合，7 番，8 番のキューが低遅延キューとなります。
llpq4 パラメータは，キュー数が 8 の場合，5 ～ 8 番のキューが低遅延キューとなります。キュー数 4 は選択できません。

llrlq【AX6700S】【AX6600S】

シェーパモードで指定したユーザとは独立した二つの低遅延優先のユーザ（llrlq1，llrlq2）の設定を可能にします。出力優先度は次のようになります。
llrlq1 ＞ llrlq2 ＞全ユーザ

1. 本パラメータ省略時の初期値
   llrlq1，llrlq2 の設定はできません。
2. 値の設定範囲
   なし
3. 本パラメータ使用時の注意事項
   本パラメータを設定した場合，指定したシェーパモードのユーザ数が二つ減ります。

rgq【AX6300S】

帯域制御方式を RGQ に設定します。RGQ はユーザごとに最低帯域を保証する方式です。出力優先度はユーザ間で均等です。

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
   rgq を指定します。

［コマンド省略時の動作］

シェーパモードを設定しません。

［通信への影響］

設定内容を変更，削除した場合，NIF がリセットされて通信が一時的に切断されます。

［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. 装置の受信側インタフェース（イーサネット，VLAN）に，階層化シェーパ機能のユーザ，llrlq1，llrlq2 のどれかを動作パラメータに指定した QoS フローリストが設定されている場合，次の条件に注意してください。**【AX6700S】【AX6600S】**
   - シェーパモードを設定する場合，シェーパモード設定済みの NIF で，シェーパモード，キュー数が一致するように設定してください。
   - シェーパモードは変更できません。
   - 設定済みシェーパモードをすべて削除することはできません。装置に設定が一つ以上残る状態にしてください。
2. 装置の受信側インタフェース（イーサネット，VLAN）に，階層化シェーパ機能のユーザを動作パラメータに指定した QoS フローリストが設定されている場合，次の条件に注意してください。
   【AX6300S】

- シェーパモードを設定する場合，シェーパモード設定済みの NIF で，キュー数が一致するように設定してください。
- 設定済みシェーパモードをすべて削除することはできません。装置に設定が一つ以上残る状態にしてください。

3. 該当 NIF の送信側インタフェース（イーサネット）に，階層化シェーパ機能のユーザ，llrlq1，llrlq2 のどれかを動作パラメータに指定した QoS フローリストが設定されている場合，シェーパモードの変更および削除はできません。**【AX6700S】【AX6600S】**
4. 該当 NIF の送信側インタフェース（イーサネット）に，階層化シェーパ機能のユーザを動作パラメータに指定した QoS フローリストが設定されている場合，シェーパモードの削除はできません。
   【AX6300S】
5. 該当 NIF のポートが属する送信側インタフェース（VLAN）に，階層化シェーパ機能のユーザ，llrlq1，llrlq2 のどれかを動作パラメータに指定した QoS フローリストが設定されている場合，次の条件に注意してください。**【AX6700S】【AX6600S】**
   - シェーパモードを設定する場合，該当 VLAN に属するポートを持つシェーパモード設定済みの NIF で，シェーパモード，キュー数が一致するように設定してください。
   - 該当 VLAN に属するポートを持つ NIF に対して設定してあるシェーパモードは変更できません。
   - シェーパモードを削除することで，該当 VLAN に属するポートを持つすべての NIF でシェーパモードの設定がなくなる場合は，削除できません。
6. 該当 NIF のポートが属する送信側インタフェース（VLAN）に，階層化シェーパ機能のユーザを動作パラメータに指定した QoS フローリストが設定されている場合，次の条件に注意してください。
   【AX6300S】
   - シェーパモードを設定する場合，該当 VLAN に属するポートを持つすべてのシェーパモード設定済みの NIF で，キュー数が一致するように設定してください。
   - シェーパモードを削除することで，該当 VLAN に属するポートを持つすべての NIF でシェーパモードの設定がなくなる場合は，削除できません。

［関連コマンド］

なし

number-of-queue

該当シェーパモード

[rgq] [rgq llrlq] [wgq] [wgq llrlq] [llpq1] [llpq1 llrlq] [llpq2] [llpq2 llrlq]

指定したシェーパ NIF に対して，ユーザ当たりのキュー数を設定します。本コマンドを設定した NIF のインタフェースに対して，シェーパコンフィグレーションを設定している場合，設定，削除はできません。

[入力形式]

情報の設定

number-of-queue 4

情報の削除

no number-of-queue

[入力モード]

(config-sh-nif)

[パラメータ]

4

ユーザ当たりのキュー数を 4 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
   なし

[コマンド省略時の動作]

ユーザ当たりのキュー数を 8 に設定します。

[通信への影響]

設定内容を変更，削除した場合，NIF がリセットされて通信が一時的に切断されます。

[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. シェーパモードが反映されていない NIF に対しては，反映されません。
2. 装置の受信側インタフェース（イーサネット，VLAN）に，階層化シェーパ機能のユーザ，llrlq1，llrlq2 のどれかを動作パラメータに指定した QoS フローリストが設定されている場合，シェーパモード設定済みの NIF に対して，キュー数の変更はできません。**【AX6700S】【AX6600S】**
3. 装置の受信側インタフェース（イーサネット，VLAN）に，階層化シェーパ機能のユーザを動作パラメータに指定した QoS フローリストが設定されている場合，シェーパモード設定済みの NIF に対して，キュー数の変更はできません。**【AX6300S】**
4. 該当 NIF の送信側インタフェース（イーサネット）に，階層化シェーパ機能のユーザ，llrlq1，llrlq2 のどれかを動作パラメータに指定した QoS フローリストが設定されている場合，シェーパモード設定済みの NIF に対して，キュー数の変更はできません。**【AX6700S】【AX6600S】**
5. 該当 NIF の送信側インタフェース（イーサネット）に，階層化シェーパ機能のユーザを動作パラメー

タに指定した QoS フローリストが設定されている場合，シェーパモード設定済みの NIF に対して，キュー数の変更はできません。**【AX6300S】**

6. 該当 NIF のポートが属する送信側インタフェース（VLAN）に，階層化シェーパ機能のユーザ，llrlq1，llrlq2 のどれかを動作パラメータに指定した QoS フローリストが設定されている場合，該当 VLAN に属するポートを持つシェーパモードが設定してある NIF に対して，キュー数の変更はできません。**【AX6700S】【AX6600S】**
7. 該当 NIF のポートが属する送信側インタフェース（VLAN）に，階層化シェーパ機能のユーザを動作パラメータに指定した QoS フローリストが設定されている場合，該当 VLAN に属するポートを持つシェーパモードが設定してある NIF に対して，キュー数の変更はできません。**【AX6300S】**

［関連コマンド］

shaper nif

predicted-tail-drop

該当シェーパモード

すべて

指定した NIF または装置に搭載されているすべての NIF に対して，早期検出テールドロップ機能を無効にします。

本機能は，ポートごとに割り当てた各 QoS のバッファが 7/8 まで溜まった場合，該当ポートのインタフェースに設定している全ユーザに対して，溜まった QoS 番号と等しいキュー番号のキュー長を半分にする機能です。

［入力形式］

情報の設定

predicted-tail-drop disable

情報の削除

no predicted-tail-drop

［入力モード］

(config-sh-nif)

［パラメータ］

なし

［コマンド省略時の動作］

早期検出テールドロップ機能を有効にします。

［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］

shaper nif

qos（advance qos-flow-list）

Advance 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

[<sequence>] qos mac { フロー検出条件 }[動作指定]

[<sequence>] qos mac-ip { フロー検出条件 }[動作指定]

[<sequence>] qos mac-ipv6 { フロー検出条件 }[動作指定]

- mac { フロー検出条件 } の場合

MAC ヘッダ条件でフロー検出する場合のフロー検出条件です。

mac {<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 | slow-protocol} [<ethernet type>][vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

- mac-ip { フロー検出条件 } の場合

MAC ヘッダ条件，IPv4 ヘッダ条件および Layer4 ヘッダ条件でフロー検出する場合のフロー検出条件です。

フラグメントパケットなしで，上位プロトコルが TCP，UDP，ICMP および IGMP 以外の場合

mac-ip {<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 | slow-protocol} {ip | <protocol>} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

フラグメントパケットなしで，上位プロトコルが TCP の場合

mac-ip {<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 | slow-protocol} tcp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

フラグメントパケットなしで，上位プロトコルが UDP の場合

mac-ip {<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 | slow-protocol} udp {{<source ipv4> | own-address} <source ipv4 wildcard> |

host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

フラグメントパケットなしで，上位プロトコルが ICMP の場合

mac-ip {<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 | slow-protocol} icmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

フラグメントパケットなしで，上位プロトコルが IGMP の場合

mac-ip {<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 | slow-protocol} igmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [<igmp type>] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

フラグメントパケットありの場合

mac-ip {<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 | slow-protocol} {ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [fragments] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

- mac-ipv6 { フロー検出条件 } の場合

MAC ヘッダ条件，IPv6 ヘッダ条件および Layer4 ヘッダ条件でフロー検出する場合のフロー検出です。

上位プロトコルが TCP，UDP および ICMP 以外の場合

mac-ipv6 {<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 | slow-protocol} {ipv6 | <protocol>} {<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address

<source ipv6 start> <source ipv6 end>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

上位プロトコルが TCP の場合

mac-ipv6 {<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 | slow-protocol} tcp {<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

上位プロトコルが UDP の場合

mac-ipv6 {<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 | slow-protocol} udp {<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

上位プロトコルが ICMP の場合

mac-ipv6 {<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 | slow-protocol} icmp {<source ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>][{ctag-untagged | [ctag-user-priority <priority>] [ctag-vlan <vlan id>]}]

- 動作指定

DSCP マッピングなしの場合

action [user <user id> | llrlq1 | llrlq2] [priority-class <class>] [discard-class <class>] [replace-dscp <dscp>] [replace-user-priority <priority>] [max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>] [min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>] [penalty-discard-class <class>] [penalty-dscp <dscp>]

[penalty-user-priority <priority>]]

DSCP マッピングありの場合

action [user <user id> | llrlq1 | llrlq2] [dscp-map] [replace-dscp <dscp>] [replace-user-priority <priority>] [max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>] [min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>] [penalty-dscp <dscp>] [penalty-user-priority <priority>]]

情報の削除

no <sequence>

［入力モード］

(config-adv-qos)

［パラメータ］

<sequence>

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 より大きい値を設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> 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> を入力した場合は <source mac> の完全一致をフロー検出条件とします。
   any を指定すると，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 | slow-protocol}

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，pvst-plus-bpdu または slow-protocol を指定します。
   <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> を入力した場合は <destination mac> の完全一致をフロー検出条件とします。
any を指定すると，宛先 MAC アドレスをフロー検出条件とはしません。
bpdu を指定すると，BPDU 制御パケットをフロー検出条件とします。
cdp を指定すると，CDP 制御パケットをフロー検出条件とします。
lacp または slow-protocol を指定すると，slow プロトコルパケットをフロー検出条件とします。
本装置では LACP と IEEE802.3ah/UDLD 機能で slow プロトコルパケットを使用しています。
lacp を指定すると，LACP 制御パケットをフロー検出条件とします。
lldp を指定すると，LLDP 制御パケットをフロー検出条件とします。
oadp を指定すると，OADP 制御パケットをフロー検出条件とします。
pvst-plus-bpdu を指定すると，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値を指定します。

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。
   指定可能なプロトコル名称は「表 7-9　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 list name>}

VLAN ID または VLAN リスト名称を指定します。
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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

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。

ctag-untagged

カスタマ Tag がないパケットの検出を指定します。

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
   なし

ctag-user-priority <priority>

カスタマ 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
   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。

ctag-vlan <vlan id>

カスタマ Tag の VLAN ID 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 ～ 4095（10 進数）を指定します。

{ip | <protocol> | icmp | igmp | tcp | udp }

フロー検出条件指定に mac-ip を指定した場合に選択できます。

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
   0 ～ 255（10 進数）またはプロトコル名称を指定します。
   指定可能なプロトコル名称は「表 7-1　指定可能なプロトコル名称（IPv4）」を参照してください。

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

フロー検出条件指定に mac-ipv6 を指定した場合に選択できます。

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。
   指定可能なプロトコル名称は「表 7-2　指定可能なプロトコル名称（IPv6）」を参照してください。

{{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>}

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>，any，own-address <source ipv4 wildcard>，host own-address，own または range-address <source ipv4 start> <source ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <source ipv4> を入力した場合は，<source ipv4> の完全一致をフロー検出条件とします。
   any を指定すると，送信元 IPv4 アドレスをフロー検出条件とはしません。
   own-address および own は，VLAN インタフェースに対して有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを送信元 IPv4 アドレスとしてフロー検出条件にします。
   own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフロー検出条件にします。ホストアドレス部は任意としてフロー検出条件にします。

なお，own-address および own を指定したインタフェースがマルチホームの場合は，プライマリ IPv4 アドレスが対象になります。
range-address を指定した場合は，<source ipv4 start> から <source ipv4 end> の範囲をフロー検出条件とします。
<source ipv4 end> は <source ipv4 start> より大きい IPv4 アドレスを指定してください。
IPv4 アドレス (nnn.nnn.nnn.nnn)：0.0.0.0 ～ 255.255.255.255

{<source ipv6>/<length> | host {<source ipv6> | own-address} | any | own-address <own address length> | own | range-address <source ipv6 start> <source ipv6 end>}

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>，own-address <own address length>，host <source ipv6>，host own-address，any，own または range-address <source ipv6 start> <source ipv6 end> を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は，<source ipv6> の完全一致をフロー検出条件とします。
   any を指定すると，送信元 IPv6 アドレスをフロー検出条件とはしません。
   own-address および own は，VLAN インタフェースに対してだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを送信元 IPv6 アドレスとしてフロー検出条件とします。
   own を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを送信元 IPv6 アドレス，IPv6 グローバルアドレスのプレフィックス長を <length> としてフロー検出条件にします。
   range-address を指定した場合は，<source ipv6 start> から <source ipv6 end> の範囲をフロー検出条件とします。
   <source ipv6 end> は <source ipv6 start> より大きい IPv6 アドレスを指定してください。
   <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 | neq} <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 7-3　TCP で指定可能なポート名称」,「表 7-4　UDP で指定可能なポート名称（IPv4）」および「表 7-5　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。

neq を指定した場合は，<source port> 以外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> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>}

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>，any，
   own-address <destination ipv4 wildcard>，host own-address，own または range-address <destination ipv4 start> <destination ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <destination ipv4> を入力した場合は <destination ipv4> の完全一致をフロー検出条件とします。
   any を指定すると，宛先 IPv4 アドレスをフロー検出条件とはしません。
   own-address および own は，VLAN インタフェースに対して有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを宛先 IPv4 アドレスとしてフロー検出条件にします。
   own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフロー検出条件にします。ホストアドレス部は任意としてフロー検出条件にします。
   なお，own-address および own を指定したインタフェースがマルチホームの場合は，プライマリ IPv4 アドレスが対象になります。
   range-address を指定した場合は <destination ipv4 start> から <destination ipv4 end> の範囲をフロー検出条件とします。
   <destination ipv4 end> は <destination ipv4 start> より大きい IPv4 アドレスを指定してください。
   IPv4 アドレス (nnn.nnn.nnn.nnn)：0.0.0.0 ～ 255.255.255.255

{<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>}

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>，own-address <own address length>，host <destination ipv6>，host own-address，any，own または range-address <destination ipv6 start> <destination ipv6 end> を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は <destination ipv6> の完全一致をフロー検出条件とします。
any を指定すると，宛先 IPv6 アドレスをフロー検出条件とはしません。
own-address および own は，VLAN インタフェースに対してだけ有効になります。
own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレスとしてフロー検出条件とします。
own を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレス，IPv6 グローバルアドレスのプレフィックス長を <length> としてフロー検出条件にします。
range-address を指定した場合は <destination ipv6 start> から <destination ipv6 end> の範囲をフロー検出条件とします。
<destination ipv6 end> は <destination ipv6 start> より大きい IPv6 アドレスを指定してください。
<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

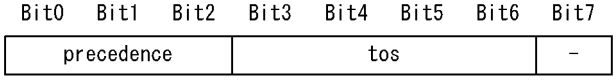
{{eq | neq} <destination port> | range <destination port start> <destination port end>}

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 7-3　TCP で指定可能なポート名称」，「表 7-4　UDP で指定可能なポート名称（IPv4）」および「表 7-5　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。
   neq を指定した場合は，<destination port> 以外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。
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。

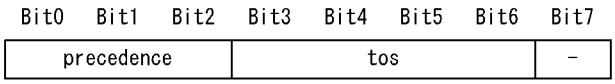


1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 15（10 進数）または tos 名称を指定します。
   指定可能な tos 名称については，「表 7-6　指定可能な tos 名称」を参照してください。

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。



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 7-7　指定可能な precedence 名称」を参照してください。

traffic-class <traffic class>

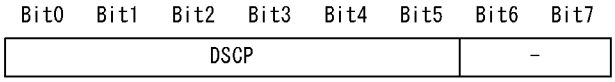
本パラメータは，トラフィッククラスフィールド値を指定します。
受信パケットのトラフィッククラスフィールドと比較します。

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>

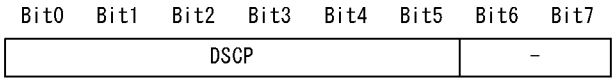
フロー検出条件種別が mac-ip の場合

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。



フロー検出条件種別が mac-ipv6 の場合

本パラメータは，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。



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 7-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。
ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。
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
   なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。
fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。
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
   なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。
psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。
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
   なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。
rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。
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
   なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。
syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。
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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。
urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。
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
   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 7-11　ICMP で指定可能なメッセージ名称（IPv4）」および「表 7-12　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

<igmp type>

IGMP タイプを指定します。
プロトコルが IGMP 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。

fragments

2 番目以降のフラグメントパケットを指定します。

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
   なし

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

{user <user id> | llrlq1 | llrlq2}【AX6700S】【AX6600S】

階層化シェーパ機能で設定したユーザ ID，llrlq1 または llrlq2 を指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   <user id>：1 ～ 1023 を指定します。

user <user id>【AX6300S】

階層化シェーパ機能で設定したユーザ ID を指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   <user id>：1 ～ 511 を指定します。

priority-class <class>

出力優先度を指定します。

1. 本パラメータ省略時の初期値
   デフォルトの出力優先度となります。デフォルトの出力優先度については「コンフィグレーションガイド Vol.2　5.10 優先度決定の解説」を参照してください。
2. 値の設定範囲
   1 ～ 8（10 進数）を指定します。

discard-class <class>

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
   デフォルトのキューイング優先度となります。デフォルト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　5.10 優先度決定の解説」を参照してください。
2. 値の設定範囲
   1 ～ 4（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 7-8　指定可能な DSCP 名称」を参照してください。

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。

dscp-map

DSCP 値によって出力優先度およびキューイング優先度を決定する DSCP マップ機能を有効にします。

DSCP 値に対応する出力優先度とキューイング優先度は「コンフィグレーションガイド Vol.2　5.10 優先度決定の解説」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（DSCP マップ機能を使用しません）
2. 値の設定範囲
   なし

max-rate

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 }

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 7-13　帯域監視の値の設定範囲」を参照してください。

max-rate-burst <byte>

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
   3000
2. 値の設定範囲
   <byte>：84 ～ 131072（10 進数）を指定します。

min-rate

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ーを科します。

ペナルティーは penalty-discard-class，penalty-dscp および penalty-user-priority を用いて指定します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}

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
   指定可能な監視帯域値については，「表 7-13　帯域監視の値の設定範囲」を参照してください。

min-rate-burst <byte>

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
   3000
2. 値の設定範囲
   <byte>：84 ～ 131072（10 進数）を指定します。

penalty-discard-class <class>

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 ～ 4（10 進数）を指定します。

penalty-dscp <dscp>

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 7-8　指定可能な DSCP 名称」を参照してください。

penalty-user-priority <priority>

最低帯域違反時のユーザ優先度の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，違反パケットのユーザ優先度を指定値 <priority> に書き換えます。
遵守パケットは replace-user-priority 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 ～ 7（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元 MAC アドレスおよび宛先 MAC 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 MAC 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 MAC アドレスに指定できるプロトコル名称のアドレスは「表 7-10　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 MAC アドレスおよび宛先 MAC 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. 送信元 IPv4 アドレスワイルドカードマスクおよび宛先 IPv4 アドレスワイルドカードマスクに 255.255.255.255 と入力したときは any と表示します。
4. 送信元 IPv4 アドレスおよび宛先 IPv4 アドレスを 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。
5. 送信元 IPv6 アドレスおよび宛先 IPv6 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。
6. 送信元アドレスおよび宛先 IPv6 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。

［関連コマンド］

advance qos-flow-list

advance qos-flow-group

advance qos-flow-list resequence

mode

remark

shaper llrlq1

shaper llrlq2

shaper user

vlan-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。

フラグメントパケットを検出条件に指定する場合は入力形式が異なるので注意してください。入力形式のフラグメントパケットの場合を参照してください。

DSCP マッピングを動作指定に指定する場合は入力形式が異なるので注意してください。入力形式のDSCP マッピングありの場合を参照してください。

［入力形式］

情報の設定・変更

[<sequence>] qos { フロー検出条件 } [動作指定]

- フロー検出条件

フラグメントパケットなしの場合

上位プロトコルが TCP，UDP，ICMP および IGMP 以外の場合

{ip | <protocol>} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id>| <vlan id list name>}] [user-priority <priority>]

上位プロトコルが TCP の場合

tcp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end> } [{{eq | neq} <destination port> | range <destination port start> <destination port end>}][{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

上位プロトコルが UDP の場合

udp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source port> | range <source port start> <source port end>}] {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end> } [{{eq | neq} <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

上位プロトコルが ICMP の場合

icmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end> } [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

上位プロトコルが IGMP の場合

igmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end> } [<igmp type>] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

フラグメントパケットの場合

{ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end> } [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [fragments] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

- 動作指定

AX6700S，AX6600S の場合

DSCP マッピングなしの場合

action
[{user <user id> | llrlq1 | llrlq2}]
[priority-class <class>] [discard-class <class>] [replace-dscp <dscp>] [replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]
[penalty-discard-class <class>] [penalty-dscp <dscp>] [penalty-user-priority <priority>]]

DSCP マッピングありの場合

action
[{user <user id> | llrlq1 | llrlq2}]
[dscp-map] [replace-dscp <dscp>] [replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]
[penalty-dscp <dscp>] [penalty-user-priority <priority>]]

AX6300S の場合

DSCP マッピングなしの場合

action
[user <user id>]
[priority-class <class>] [discard-class <class>] [replace-dscp <dscp>][replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]
[penalty-discard-class <class>] [penalty-dscp <dscp>] [penalty-user-priority <priority>]]

DSCP マッピングありの場合

action
[user <user id>]
[dscp-map] [replace-dscp <dscp>] [replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]

[penalty-dscp <dscp>] [penalty-user-priority <priority>]]

情報の削除

no <sequence>

［入力モード］

(config-ip-qos)

［パラメータ］

<sequence>

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 より大きい値を設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 | igmp | tcp | udp }

IPv4 パケットの上位プロトコル条件を指定します。

ただし，すべてのプロトコルを対象とする場合は ip を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   0 ～ 255（10 進数）またはプロトコル名称を指定します。
   指定可能なプロトコル名称は「表 7-1　指定可能なプロトコル名称（IPv4）」を参照してください。

{{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own | range-address <source ipv4 start> <source ipv4 end>}

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>，any，own-address <source ipv4 wildcard>，host own-address，own または range-address <source ipv4 start> <source ipv4 end> を指定します。
   <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マスクを IPv4 アドレス形式で指定します。
   host <source ipv4> を入力した場合は，<source ipv4> の完全一致をフロー検出条件とします。
   any を指定すると，送信元 IPv4 アドレスをフロー検出条件とはしません。
   own-address および own は，VLAN インタフェースに対して有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを送信元 IPv4 アドレスとしてフロー検出条件にします。
   own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフロー検出条件にします。ホストアドレス部は任意としてフロー検出条件にします。
   なお，own-address および own を指定したインタフェースがマルチホームの場合は，プライマリ IPv4 アドレスが対象になります。

range-address を指定した場合は，<source ipv4 start> から <source ipv4 end> の範囲をフロー検出条件とします。
<source ipv4 end> は <source ipv4 start> より大きい IPv4 アドレスを指定してください。
IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

{{eq | neq} <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 7-3　TCP で指定可能なポート名称」および「表 7-4　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。
   neq を指定した場合は，<source port> 以外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> | own-address} <destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any | own | range-address <destination ipv4 start> <destination ipv4 end>}

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>，any，own-address <destination ipv4 wildcard>，host own-address，own または range-address <destination ipv4 start> <destination ipv4 end> を指定します。<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マスクを IPv4 アドレス形式で指定します。
   host <destination ipv4> を入力した場合は <destination ipv4> の完全一致をフロー検出条件とします。
   any を指定すると，宛先 IPv4 アドレスをフロー検出条件とはしません。
   own-address および own は，VLAN インタフェースに対して有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv4 アドレスを宛先 IPv4 アドレスとしてフロー検出条件にします。
   own を指定した場合は，対象インタフェースに設定されている IPv4 アドレスのネットワークアドレス部をフロー検出条件にします。ホストアドレス部は任意としてフロー検出条件にします。
   なお，own-address および own を指定したインタフェースがマルチホームの場合は，プライマリ IPv4 アドレスが対象になります。
   range-address を指定した場合は <destination ipv4 start> から <destination ipv4 end> の範囲をフロー検出条件とします。
   <destination ipv4 end> は <destination ipv4 start> より大きい IPv4 アドレスを指定してください。
   IPv4 アドレス（nnn.nnn.nnn.nnn）：0.0.0.0 ～ 255.255.255.255

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

宛先ポート番号を指定します。

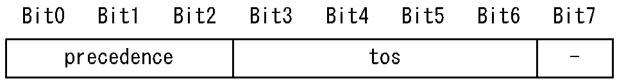
プロトコルが TCP および UDP だけのオプションです。

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 7-3　TCP で指定可能なポート名称」および「表 7-4 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。
   neq を指定した場合は，<destination port> 以外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。

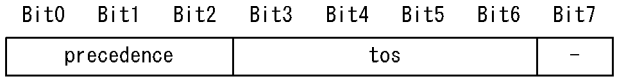


1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 15（10 進数）または tos 名称を指定します。
   指定可能な tos 名称については，「表 7-6　指定可能な tos 名称」を参照してください。

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。

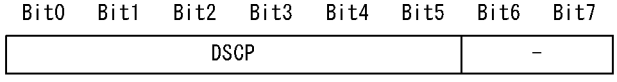


1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）または precedence 名称を指定します。
   指定可能な precedence 名称については，「表 7-7　指定可能な precedence 名称」を参照してください。

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。



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 7-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。

ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。

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

なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。

fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。

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

なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。

psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。

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

なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。

rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。

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

なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。
syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。
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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。
urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。
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
   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 7-11　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

<igmp type>

IGMP タイプを指定します。
プロトコルが IGMP 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。

fragments

2 番目以降のフラグメントパケットを指定します。

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
   なし

vlan {<vlan id> | <vlan id list name>}

VLAN ID または VLAN リスト名称を指定します。

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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

{user <user id> | llrlq1 | llrlq2}【AX6700S】【AX6600S】

階層化シェーパ機能で設定したユーザ ID，llrlq1 または llrlq2 を指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   <user id>：1 ～ 1023 を指定します。

user <user id>【AX6300S】

階層化シェーパ機能で設定したユーザ ID を指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   <user id>：1 ～ 511 を指定します。

priority-class <class>

出力優先度を指定します。

1. 本パラメータ省略時の初期値
   デフォルトの出力優先度となります。デフォルトの出力優先度については「コンフィグレーション

ガイド Vol.2　5.10 優先度決定の解説」を参照してください。

2. 値の設定範囲
   1 ～ 8（10 進数）を指定します。

discard-class <class>

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
   デフォルトのキューイング優先度となります。デフォルト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　5.10 優先度決定の解説」を参照してください。
2. 値の設定範囲
   1 ～ 4（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 7-8　指定可能な DSCP 名称」を参照してください。

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。

dscp-map

DSCP 値によって出力優先度およびキューイング優先度を決定する DSCP マップ機能を有効にします。
DSCP 値に対応する出力優先度とキューイング優先度は「コンフィグレーションガイド Vol.2　5.10 優先度決定の解説」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（DSCP マップ機能を使用しません）
2. 値の設定範囲
   なし

max-rate

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 }

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 7-13　帯域監視の値の設定範囲」を参照してください。

max-rate-burst <byte>

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
   3000
2. 値の設定範囲
   <byte>：84 ～ 131072（10 進数）を指定します。

min-rate

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ーを科します。ペナルティーは penalty-discard-class，penalty-dscp および penalty-user-priority を用いて指定します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}

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
   指定可能な監視帯域値については，「表 7-13　帯域監視の値の設定範囲」を参照してください。

min-rate-burst <byte>

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
   3000
2. 値の設定範囲
   <byte>：84 ～ 131072（10 進数）を指定します。

penalty-discard-class <class>

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 ～ 4（10 進数）を指定します。

penalty-dscp <dscp>

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 7-8　指定可能な DSCP 名称」を参照してください。

penalty-user-priority <priority>

最低帯域違反時のユーザ優先度の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，違反パケットのユーザ優先度を指定値 <priority> に書き換えます。
遵守パケットは replace-user-priority 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 ～ 7（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元アドレスワイルドカードマスクおよび宛先アドレスワイルドカードマスクに 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。

[関連コマンド]

ip qos-flow-list

ip qos-flow-group

ip qos-flow-list resequence

mode

remark

shaper llrlq1

shaper llrlq2

shaper user

vlan-list

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。

DSCP マッピングを動作指定に指定する場合は入力形式が異なるので注意してください。入力形式の DSCP マッピングありの場合を参照してください。

［入力形式］

情報の設定・変更

[<sequence>] 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 | own-address <own address length>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

  上位プロトコルが TCP の場合

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

  上位プロトコルが UDP の場合

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

  上位プロトコルが ICMP の場合

  icmp {<source ipv6>/<length> | host <source ipv6> | any | own-address <own address length>} {<destination ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]

- 動作指定

AX6700S，AX6600S の場合

DSCP マッピングなしの場合

action

[{user <user id> | llrlq1 | llrlq2}]
[priority-class <class>] [discard-class <class>] [replace-dscp <dscp>] [replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]
[penalty-discard-class <class>] [penalty-dscp <dscp>] [penalty-user-priority <priority>]]

DSCP マッピングありの場合

action
[{user <user id> | llrlq1 | llrlq2}]
[dscp-map] [replace-dscp <dscp>] [replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]
[penalty-dscp <dscp>] [penalty-user-priority <priority>]]

AX6300S の場合

DSCP マッピングなしの場合

action
[user <user id>]
[priority-class <class>] [discard-class <class>] [replace-dscp <dscp>] [replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]
[penalty-discard-class <class>] [penalty-dscp <dscp>] [penalty-user-priority <priority>]]

DSCP マッピングありの場合

action
[user <user id>]
[dscp-map] [replace-dscp <dscp>] [replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]
[penalty-dscp <dscp>] [penalty-user-priority <priority>]]

情報の削除

no <sequence>

[入力モード]

```
(config-ipv6-qos)
```

[パラメータ]

<sequence>

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 より大きい値を設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
   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。
   指定可能なプロトコル名称は「表 7-2　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 | own-address <own address length>}

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>，own-address <own address length> または any を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は，<source ipv6> の完全一致をフロー検出条件とします。
   any を指定すると，送信元 IPv6 アドレスをフロー検出条件とはしません。
   own-address は VLAN インタフェースに対してだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを送信元 IPv6 アドレスとしてフロー検出条件とします。
   <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 | neq} <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 7-3　TCP で指定可能なポート名称」および「表 7-5　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。
   neq を指定した場合は，<source port> 以外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> | own-address} | any | own-address <own address length> | own | range-address <destination ipv6 start> <destination ipv6 end>}

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>，own-address <own address length>，host <destination ipv6>，host own-address，any，own または range-address <destination ipv6 start> <destination ipv6 end> を指定します。
   <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。
   <own address length> には own-address 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> を入力した場合は <destination ipv6> の完全一致をフロー検出条件とします。
   any を指定すると，宛先 IPv6 アドレスをフロー検出条件とはしません。
   own-address および own は，VLAN インタフェースに対してだけ有効になります。
   own-address を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレスとしてフロー検出条件とします。
   own を指定した場合は，対象インタフェースに設定されている IPv6 グローバルアドレスを宛先 IPv6 アドレス，IPv6 グローバルアドレスのプレフィックス長を <length> としてフロー検出条件にします。
   range-address を指定した場合は <destination ipv6 start> から <destination ipv6 end> の範囲をフロー検出条件とします。
   <destination ipv6 end> は <destination ipv6 start> より大きい IPv6 アドレスを指定してください。
   <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 | neq} <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 7-3　TCP で指定可能なポート名称」および「表 7-5　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。
   neq を指定した場合は，<destination port> 以外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>

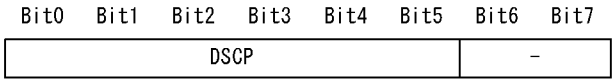
本パラメータは，トラフィッククラスフィールド値を指定します。
受信パケットのトラフィッククラスフィールドと比較します。

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，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。



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 7-8　指定可能な DSCP 名称」を参照してください。

established

TCP ヘッダの ACK フラグまたは 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

{ack | +ack | -ack}

TCP ヘッダの ACK フラグ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。
ack または +ack は ACK フラグが 1 のパケット，-ack は ACK フラグが 0 のパケットとなります。

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
   なし

{fin | +fin | -fin}

TCP ヘッダの FIN フラグ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。
fin または +fin は FIN フラグが 1 のパケット，-fin は FIN フラグが 0 のパケットとなります。

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
   なし

{psh | +psh | -psh}

TCP ヘッダの PSH フラグ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。
psh または +psh は PSH フラグが 1 のパケット，-psh は PSH フラグが 0 のパケットとなります。

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
   なし

{rst | +rst | -rst}

TCP ヘッダの RST フラグ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。

rst または +rst は RST フラグが 1 のパケット，-rst は RST フラグが 0 のパケットとなります。

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
   なし

{syn | +syn | -syn}

TCP ヘッダの SYN フラグ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。

syn または +syn は SYN フラグが 1 のパケット，-syn は SYN フラグが 0 のパケットとなります。

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
   なし

{urg | +urg | -urg}

TCP ヘッダの URG フラグ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。

urg または +urg は URG フラグが 1 のパケット，-urg は URG フラグが 0 のパケットとなります。

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
   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 7-12　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 list name>}

VLAN ID または VLAN リスト名称を指定します。

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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

{user <user id> | llrlq1 | llrlq2}【AX6700S】【AX6600S】

階層化シェーパ機能で設定したユーザ ID，llrlq1 または llrlq2 を指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   <user id>：1 ～ 1023 を指定します。

user <user id>【AX6300S】

階層化シェーパ機能で設定したユーザ ID を指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   <user id>：1 ～ 511 を指定します。

priority-class <class>

出力優先度を指定します。

1. 本パラメータ省略時の初期値
   デフォルトの出力優先度となります。デフォルトの出力優先度については「コンフィグレーションガイド Vol.2　5.10 優先度決定の解説」を参照してください。
2. 値の設定範囲
   1 ～ 8（10 進数）を指定します。

discard-class <class>

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
   デフォルトのキューイング優先度となります。デフォルト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　5.10 優先度決定の解説」を参照してください。
2. 値の設定範囲
   1 ～ 4（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 7-8　指定可能な DSCP 名称」を参照してください。

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。

dscp-map

DSCP 値によって出力優先度およびキューイング優先度を決定する DSCP マップ機能を有効にします。
DSCP 値に対応する出力優先度とキューイング優先度は「コンフィグレーションガイド Vol.2　5.10 優先度決定の解説」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（DSCP マップ機能を使用しません）
2. 値の設定範囲
   なし

max-rate

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 }

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
   指定可能な監視帯域値については，「表 7-13　帯域監視の値の設定範囲」を参照してください。

max-rate-burst <byte>

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

3000

2. 値の設定範囲
<byte>：84 ～ 131072（10 進数）を指定します。

min-rate

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ーを科します。ペナルティーは penalty-discard-class，penalty-dscp および penalty-user-priority を用いて指定します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}

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
指定可能な監視帯域値については，「表 7-13　帯域監視の値の設定範囲」を参照してください。

min-rate-burst <byte>

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
3000
2. 値の設定範囲
<byte>：84 ～ 131072（10 進数）を指定します。

penalty-discard-class <class>

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 ～ 4（10 進数）を指定します。

penalty-dscp <dscp>

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 7-8　指定可能な DSCP 名称」を参照してください。

penalty-user-priority <priority>

最低帯域違反時のユーザ優先度の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，違反パケットのユーザ優先度を指定値 <priority> に書き換えま

す。
遵守パケットは replace-user-priority 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 ～ 7（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元アドレスおよび宛先アドレスに nnnn:nnnn:nnnn: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。

[関連コマンド]

ipv6 qos-flow-list

ipv6 qos-flow-group

ipv6 qos-flow-list resequence

mode

remark

shaper llrlq1

shaper llrlq2

shaper user

vlan-list

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

[<sequence>] 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 | slow-protocol} [<ethernet type>] [vlan {<vlan id> | <vlan id list name>}] [user-priority <priority>]
- 動作指定

AX6700S，AX6600S の場合

action
[{user <user id> | llrlq1 | llrlq2}]
[priority-class <class>] [discard-class <class>] [replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]
[penalty-discard-class <class>] [penalty-user-priority <priority>]]

AX6300S の場合

action
[user <user id>]
[priority-class <class>] [discard-class <class>] [replace-user-priority <priority>]
[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst <byte>]]
[min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst <byte>]
[penalty-discard-class <class>] [penalty-user-priority <priority>]]

情報の削除

no <sequence>

［入力モード］

```
(config-mac-qos)
```

［パラメータ］

<sequence>

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 より大きい値を設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> または，host <source mac>，any を指定します。<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> を入力した場合は <source mac> の完全一致をフロー検出条件とします。any を指定すると，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 | slow-protocol}

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> または，host <destination mac>，any，bpdu，cdp，lacp，lldp，oadp，pvst-plus-bpdu，または slow-protocol を指定します。
   <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> を入力した場合は <destination mac> の完全一致をフロー検出条件とします。
   any を指定すると，宛先 MAC アドレスをフロー検出条件とはしません。
   bpdu を指定すると，BPDU 制御パケットをフロー検出条件とします。
   cdp を指定すると，CDP 制御パケットをフロー検出条件とします。
   lacp または slow-protocol を指定すると，slow プロトコルパケットをフロー検出条件とします。
   本装置では LACP と IEEE802.3ah/UDLD 機能で slow プロトコルパケットを使用しています。
   lldp を指定すると，LLDP 制御パケットをフロー検出条件とします。
   oadp を指定すると，OADP 制御パケットをフロー検出条件とします。
   pvst-plus-bpdu を指定すると，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値を指定します。

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。指定可能なプロトコル名称は「表 7-9　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 list name>}

VLAN ID または VLAN リスト名称を指定します。
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
   VLAN ID または VLAN リスト名称を指定します。
   VLAN ID 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。

user-priority <priority>

ユーザ優先度を指定します。

1. 本パラメータ省略時の初期値
   なし（検出条件としません）
2. 値の設定範囲
   0 ～ 7（10 進数）を指定します。

動作パラメータ

action

動作パラメータを設定，変更する場合は必ず本パラメータを動作パラメータ全体の先頭に設定してください。

1. 本パラメータ省略時の初期値
   なし（動作指定をする場合は省略できません）
2. 値の設定範囲
   なし

{user <user id> | llrlq1 | llrlq2}【AX6700S】【AX6600S】

階層化シェーパ機能で設定したユーザ ID，llrlq1 または llrlq2 を指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   <user id>：1 ～ 1023 を指定します。

user <user id>【AX6300S】

階層化シェーパ機能で設定したユーザ ID を指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   <user id>：1 ～ 511 を指定します。

priority-class <class>

出力優先度を指定します。

1. 本パラメータ省略時の初期値
   デフォルトの出力優先度となります。デフォルトの出力優先度については「コンフィグレーションガイド Vol.2　5.10 優先度決定の解説」を参照してください。
2. 値の設定範囲
   1 ～ 8（10 進数）を指定します。

discard-class <class>

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
   デフォルトのキューイング優先度となります。デフォルト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　5.10 優先度決定の解説」を参照してください。
2. 値の設定範囲
   1 ～ 4（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。

max-rate

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 }

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
   指定可能な監視帯域値については，「表 7-13　帯域監視の値の設定範囲」を参照してください。

max-rate-burst <byte>

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
   3000
2. 値の設定範囲
   <byte>：84 ～ 131072（10 進数）を指定します。

min-rate

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ーを科します。ペナルティーは penalty-discard-class および penalty-user-priority を用いて指定します。

{<kbit/s> | <Mbit/s>M | <Gbit/s>G}

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
   指定可能な監視帯域値については，「表 7-13　帯域監視の値の設定範囲」を参照してください。

min-rate-burst <byte>

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
   3000
2. 値の設定範囲
   <byte>：84 ～ 131072（10 進数）を指定します。

penalty-discard-class <class>

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 ～ 4（10 進数）を指定します。

penalty-user-priority <priority>

最低帯域違反時のユーザ優先度の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，違反パケットのユーザ優先度を指定値 <priority> に書き換えます。
遵守パケットは replace-user-priority 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 ～ 7（10 進数）を指定します。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 送信元アドレスおよび宛先アドレスに nnnn.nnnn.nnnn ffff.ffff.ffff と入力したときは any と表示します。
2. 宛先アドレスにプロトコル名称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 7-10　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 qos-flow-list

mac qos-flow-group

mac qos-flow-list resequence

mode

remark

shaper llrlq1

shaper llrlq2

shaper user

vlan-list

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
   使用可能な文字列は先頭が英字の 31 文字以内の英数字です。

[コマンド省略時の動作]

スケジューリングモードは PQ，キュー数は 8 で動作します。

[通信への影響]

QoS キューリスト名を指定してキュー数を変更した場合，当該回線が再起動するため，当該回線を使用した通信が一時的に途切れます。

[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. QoS キューリスト名を指定してキュー数を変更した場合，変更したインタフェース（物理ポート）が再起動します。変更したときに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，すべて吐き出す処理を行います。パケットの吐き出し処理中は，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 キューリスト名を指定してキュー数設定を行わなかった場合，キュー数は 8 で動作します。
4. 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。
5. 当該回線で設定した QoS キューリスト情報が使用できない場合，運用ログメッセージが表示されます。使用可能な QoS キューリスト情報については，「コンフィグレーションガイド Vol.2　6.10 NIF 種別と送信制御機能との対応」を参照してください。
6. レガシーシェーパ機能をサポートしていない NIF のインタフェースに対して，本コマンドは設定できません。

7. 階層化シェーパ機能が設定してある NIF のインタフェースに対して，本コマンドは設定できません。

［関連コマンド］

qos-queue-list

interface gigabitethernet

interface tengigabitethernet

qos-queue-list

QoS キューリスト情報にスケジューリングモードおよびキュー数を設定します。装置当たり最大 384 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 [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }] | rr [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }] | 4pq+4wfq <rate1>% <rate2>% <rate3>% <rate4>% | 2pq+4wfq+2beq <rate3>% <rate4>% <rate5>% <rate6>% | 4wfq+4beq <rate5>% <rate6>% <rate7>% <rate8>% }

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
   使用可能な文字列は先頭が英字の 31 文字以内の英数字です。

{ pq [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }] | rr [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }] | 4pq+4wfq <rate1>% <rate2>% <rate3>% <rate4>% | 2pq+4wfq+2beq <rate3>% <rate4>% <rate5>% <rate6>% | 4wfq+4beq <rate5>% <rate6>% <rate7>% <rate8>% }

スケジューリングモードを指定します。キュー数はスケジューリングモードによって 8 キュー固定または 1，2，4，8 キューが選択可能となります。PQ の動作をするキューの優先度は，キュー番号が大きいほどキューの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

pq [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }]

PQ で動作します。また，物理ポート当たりのキュー数を設定します。

キュー数は物理ポート当たり 1，2，4 キューを選択可能であり，選択しない場合は 8 キューとなります。複数のキューにパケットが在る場合，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。

number_of_queue_1：キュー数は 1

number_of_queue_2：キュー数は 2

number_of_queue_4：キュー数は 4

1. 本パラメータ省略時の初期値
   pq だけを指定した場合，キュー数は 8 です。

rr [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }]

RR で動作します。また，物理ポート当たりのキュー数を設定します。キュー数は物理ポート当

たり 1，2，4 キューを選択可能であり，選択しない場合は 8 キューとなります。複数のキューにパケットが在る場合，順番にキューを見ながらパケットを送信します。パケット長に関係なく，パケット数が均等になるように制御します。

number_of_queue_1：キュー数は 1

number_of_queue_2：キュー数は 2

number_of_queue_4：キュー数は 4

1. 本パラメータ省略時の初期値
   rr だけを指定した場合，キュー数は 8 です。

4pq+4wfq <rate1>% <rate2>% <rate3>% <rate4>%

4PQ ＋ 4WFQ で動作します。キュー数は物理ポート当たり 8 キュー固定です。4pq（8 ～ 5 番キュー）にパケットが在る場合，該当パケットを最優先で送信します。4wfq（4 ～ 1 番キュー）は 4pq にパケットがない場合，設定した重みの比率 <rate> に応じてパケットを送信します。なお，<rate> の後ろに付く番号は，キュー番号を意味します。

1. パラメータ省略時の初期値
   <rate>：省略できません
2. 値の設定範囲
   <rate>：1 ～ 97
   注　次の二つの式を満たすように設定してください。
   - <rate1> + <rate2> + <rate3> + <rate4> ＝ 100
   - <rate1> ≦ <rate2> ≦ <rate3> ≦ <rate4>

2pq+4wfq+2beq <rate3>% <rate4>% <rate5>% <rate6>%

2PQ ＋ 4WFQ ＋ 2BEQ で動作します。キュー数は物理ポート当たり 8 キュー固定です。2pq（8 ～ 7 番キュー）にパケットが在る場合，該当パケットを最優先で送信します。4wfq（6 ～ 3 番キュー）は 2pq にパケットがない場合，重みの比率 <rate> に応じてパケットを送信します。2beq（2 ～ 1 番キュー）は 2pq および 4wfq にパケットがない場合，PQ 動作でパケットを送信します。なお，<rate> の後ろに付く番号は，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
   <rate>：省略できません
2. 値の設定範囲
   <rate>：1 ～ 97
   注　次の二つの式を満たすように設定してください。
   - <rate3> + <rate4> + <rate5> + <rate6> ＝ 100
   - <rate3> ≦ <rate4> ≦ <rate5> ≦ <rate6>

4wfq+4beq <rate5>% <rate6>% <rate7>% <rate8>%

4WFQ ＋ 4BEQ で動作します。キュー数は物理ポート当たり 8 キュー固定です。4wfq（8 ～ 5 番キュー）は重みの比率 <rate> に応じてパケットを送信します。4beq（4 ～ 1 番キュー）は 4wfq にパケットがない場合，PQ 動作でパケットを送信します。なお，<rate> の後ろに付く番号は，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
   <rate>：省略できません
2. 値の設定範囲
   <rate>：1 ～ 97
   注　次の二つの式を満たすように設定してください。
   - <rate5> + <rate6> + <rate7> + <rate8> ＝ 100
   - <rate5> ≦ <rate6> ≦ <rate7> ≦ <rate8>

[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指定してキュー数を変更した場合，当該回線が再起動するため，当該回線を使用した通信が一時的に途切れます。

[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. qos-queue-group コマンドに QoS キューリスト名称を指定してキュー数を変更した場合，変更したインタフェース（物理ポート）が再起動します。変更したときに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，すべて吐き出す処理を行います。パケットの吐き出し処理中は，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 キューインタフェース情報で使用している QoS キューリスト情報の「キュー数」のパラメータを追加，変更，削除した場合，当該インタフェースが一度ダウンして再度アップします。
3. 当該回線で設定した QoS キューリスト情報が使用できない場合，運用ログメッセージが表示されます。使用可能な QoS キューリスト情報については，「コンフィグレーションガイド Vol.2　6.10 NIF 種別と送信制御機能との対応」を参照してください。

[関連コマンド]

qos-queue-group

remark

QoS フローリストの補足説明を指定します。

QoS フローリストには IPv4 QoS フローリスト，IPv6 QoS フローリスト，MAC QoS フローリストまたは Advance 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)
(config-adv-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]

advance qos-flow-list

ip qos-flow-list

ipv6 qos-flow-list

mac qos-flow-list

set-default-user-priority

該当シェーパモード
すべて

指定した NIF から出力されるすべてのフレームに対して，ユーザ優先度を 0 に書き換えます。

［入力形式］

情報の設定
set-default-user-priority

情報の削除
no set-default-user-priority

［入力モード］

(config-sh-nif)

［パラメータ］

なし

［コマンド省略時の動作］

ユーザ優先度の書き換えをしません。

［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. 本機能は，VLAN Tag の TPID に 0x8100 または 0x9100 の値が設定してあるパケットを対象にします。

［関連コマンド］

shaper nif

shaper auto-configuration

装置にシェーパ自動設定機能を使用します。本コマンドは，シェーパ NIF 情報を設定している場合，設定できません。

［入力形式］

情報の設定・変更

shaper auto-configuration { rgq | wgq | llpq } number-of-user <user number>**【AX6700S】【AX6600S】**

shaper auto-configuration rgq number-of-user <user number>**【AX6300S】**

情報の削除

no shaper auto-configuration

［入力モード］

(config)

［パラメータ］

{ rgq | wgq | llpq }【AX6700S】【AX6600S】

シェーパ自動設定機能のシェーパモードを指定します。

rgq

帯域制御方式を RGQ に設定します。RGQ はユーザごとに最低帯域を保証する方式です。出力優先度はユーザ間で均等です。

wgq

帯域制御方式を WGQ に設定します。WGQ はユーザごとの重みの比率で帯域を分配します。出力優先度はユーザ間で均等です。

llpq

シェーパモードを LLPQ1 に設定し，帯域制御方式を LLPQ に決定します。LLPQ1 はユーザごとに最低帯域を保証しながら，ユーザの一つのキューを低遅延で送信する方式です。出力優先度は，全ユーザの通常キューより，全ユーザの低遅延キューが高くなります。ユーザ間は均等です。

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
   rgq，wgq，llpq を指定します。
3. 本パラメータ使用時の注意事項
   llpq パラメータは，8 番キューが低遅延キューとなります。

rgq【AX6300S】

シェーパ自動設定機能の帯域制御方式を RGQ に設定します。RGQ はユーザごとに最低帯域を保証する方式です。出力優先度はユーザ間で均等です。

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
   rgq を指定します。

number-of-user <user number>

インタフェース当たりのユーザ数を指定します。

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
   <user number>：1 ～ 512 を指定します。**【AX6700S】【AX6600S】**
   <user number>：1 ～ 256 を指定します。**【AX6300S】**
3. 本パラメータ使用時の注意事項**【AX6700S】【AX6600S】**
   本コマンドのパラメータで llpq を選択した場合，ユーザ数は 1 ～ 256 の範囲となります。

［コマンド省略時の動作］

シェーパ自動設定機能を使用しません。

［通信への影響］

設定内容を変更，削除した場合，NIF がリセットされて通信が一時的に切断されます。

［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. 本機能は，階層化シェーパ機能をサポートしていない NIF に対しては反映されません。
2. インタフェース（イーサネット，VLAN）に，階層化シェーパ機能のユーザ，llrlq1，llrlq2 のどれかを動作パラメータに指定した QoS フローリストが設定されている場合，本機能の変更，削除はできません。**【AX6700S】【AX6600S】**
3. インタフェース（イーサネット，VLAN）に，階層化シェーパ機能のユーザを動作パラメータに指定した QoS フローリストが設定されている場合，本機能の変更，削除はできません。**【AX6300S】**

［関連コマンド］

shaper nif

shaper vlan-user-map

shaper default-user

該当シェーパモード

すべて

イーサネットインタフェースに対して，ユーザリストを適用して，デフォルトユーザを有効にします。

本コマンドは，該当インタフェースの NIF に対してシェーパモードの設定がない場合，設定できません。また，シェーパ自動設定機能を使用している場合や，シェーパ機能を使用できるポート数の上限を超える場合，本コマンドは設定できません。

[入力形式]

情報の設定・変更

shaper default-user list <user list name>

情報の削除

no shaper default-user

[入力モード]

(config-if)

[パラメータ]

list <user list name>

デフォルトユーザに使用するユーザ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
   ・<user list name>：31 文字以内（先頭文字は数字以外）の名前を指定します。
   ・shaper user-list コマンドで作成済みのユーザリスト名称を指定します。
3. 本パラメータ使用時の注意事項
   ・該当インタフェースに設定しているすべてのユーザとデフォルトユーザの最低帯域の合計値がポート帯域制御値を超える場合は設定できません（該当シェーパモード：[rgq] [llpq1] [llpq2] [llpq4]）。
   ・該当インタフェースに設定しているすべてのユーザとデフォルトユーザの最低帯域と，llrlq1，llrlq2 の最大帯域との合計値がポート帯域制御値を超える場合は設定できません（該当シェーパモード：[rgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]）。**【AX6700S】【AX6600S】**
   ・指定したユーザリストが，該当インタフェースの NIF に設定されているシェーパモードに適した設定内容になっていない場合，設定できません。詳しい設定内容の制限はユーザリストのコマンドを参照してください。

[コマンド省略時の動作]

該当インタフェースに対してデフォルトユーザを設定しません。

[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. 階層化シェーパ機能をサポートしていない NIF のインタフェースに対して，本コマンドは設定できません。

[関連コマンド]

shaper nif

shaper user-list

shaper llrlq1【AX6700S】【AX6600S】

該当シェーパモード

[rgq llrlq] [wgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]

イーサネットインタフェースに対して，ユーザリストを適用して llrlq1 を有効にします。本コマンドは，該当インタフェースの NIF に対して該当シェーパモードの設定がない場合，設定できません。また，シェーパ自動設定機能を使用している場合や，シェーパ機能を使用できるポート数の上限を超える場合，本コマンドは設定できません。

［入力形式］

情報の設定・変更

shaper llrlq1 list <user list name>

情報の削除

no shaper llrlq1

［入力モード］

(config-if)

［パラメータ］

list <user list name>

ユーザ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
   ・<user list name>：31 文字以内（先頭文字は数字以外）の名前を指定します。
   ・shaper user-list コマンドで作成済みのユーザリスト名称を指定します。
3. 本パラメータ使用時の注意事項
   ・指定したユーザリストの最大帯域と該当インタフェースに設定されている llrlq2 の最大帯域，すべてのユーザ，デフォルトユーザの最低帯域の合計値がポート帯域制御値を超える場合は指定できません（該当シェーパモード：[rgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]）。
   ・指定したユーザリストの最大帯域と該当インタフェースに設定されている llrlq2 の最大帯域の合計値がポート帯域制御値を超える場合は指定できません（該当シェーパモード：[wgq llrlq]）。
   ・指定したユーザリストが，該当インタフェースの NIF に設定されているシェーパモードに適した設定内容になっていない場合，設定できません。詳しい設定内容の制限はユーザリストのコマンドを参照してください。

［コマンド省略時の動作］

該当インタフェースに対して llrlq1 を設定しません。

［通信への影響］

設定内容を変更，削除した場合，llrlq1 の通信が一時的に切断されます。

［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. 階層化シェーパ機能をサポートしていない NIF のインタフェースに対して，本コマンドは設定できません。

［関連コマンド］

shaper nif

shaper user-list

shaper llrlq2【AX6700S】【AX6600S】

該当シェーパモード

[rgq llrlq] [wgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]

イーサネットインタフェースに対して，ユーザリストを適用して llrlq2 を有効にします。本コマンドは該当インタフェースの NIF に対して該当シェーパモードの設定がない場合，設定できません。また，シェーパ自動設定機能を使用している場合や，シェーパ機能を使用できるポート数の上限を超える場合，本コマンドは設定できません。

[入力形式]

情報の設定・変更

shaper llrlq2 list <user list name>

情報の削除

no shaper llrlq2

[入力モード]

(config-if)

[パラメータ]

list <user list name>

ユーザ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
   ・<user list name>：31 文字以内（先頭文字は数字以外）の名前を指定します。
   ・shaper user-list コマンドで作成済みのユーザリスト名称を指定します。
3. 本パラメータ使用時の注意事項
   ・指定したユーザリストの最大帯域と該当インタフェースに設定されている llrlq1 の最大帯域，すべてのユーザ，デフォルトユーザの最低帯域の合計値がポート帯域制御値を超える場合は指定できません（該当シェーパモード：[rgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]）。
   ・指定したユーザリストの最大帯域と該当インタフェースに設定されている llrlq2 の最大帯域の合計値がポート帯域制御値を超える場合は指定できません（該当シェーパモード：[wgq llrlq]）。
   ・指定したユーザリストが，該当インタフェースの NIF に設定されているシェーパモードに適した設定内容になっていない場合，設定できません。詳しい設定内容の制限はユーザリストのコマンドを参照してください。

[コマンド省略時の動作]

該当インタフェースに対して llrlq2 を設定しません。

[通信への影響]

設定内容を変更，削除した場合，llrlq2 の通信が一時的に切断されます。

[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. 階層化シェーパ機能をサポートしていない NIF のインタフェースに対して，本コマンドは設定できません。

［関連コマンド］

shaper nif

shaper user-list

shaper nif

シェーパ NIF 情報を設定します。なお，シェーパ自動設定機能を使用している場合，設定できません。本コマンドを入力すると，config-sh-nif モードに移行し，対象シェーパ NIF に関する情報を設定できます。

[入力形式]

情報の設定・変更
　shaper nif <nif list>

情報の削除
　no shaper nif <nif list>

[入力モード]

(config)

[パラメータ]

<nif list>

NIF 番号を指定します。ハイフン（-）およびコンマ（,）を使用して複数の NIF 番号を指定できます。また，<nif no.> と記載されている場合と同様に，一つの NIF 番号を指定することもできます。

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
   「パラメータに指定できる値」の <nif no.> の範囲を参照してください。

[コマンド省略時の動作]

シェーパ NIF 情報を設定しません。

[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. 本コマンドは，階層化シェーパ機能をサポートしていない NIF に対しては設定できません。また，レガシーシェーパ機能を設定している NIF に対しても設定できません。

[関連コマンド]

なし

shaper port buffer

該当シェーパモード

すべて

イーサネットインタフェースに対して，ポート帯域制御で使用するキューごとのバッファ容量を設定します。

本コマンドは，該当インタフェースの NIF に対してシェーパモードの設定がない場合，設定できません。また，シェーパ自動設定機能を使用している場合や，シェーパ機能を使用できるポート数の上限を超える場合，本コマンドは設定できません。

[入力形式]

情報の設定・変更

shaper port buffer <qos1> <qos2> <qos3> <qos4> [<qos5> <qos6> <qos7> <qos8>]

情報の削除

no shaper port buffer

[入力モード]

(config-if)

[パラメータ]

<qos1> <qos2> <qos3> <qos4> [<qos5> <qos6> <qos7> <qos8>]

バッファ容量を指定します。

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
   - <qos>：0 ～ 96000 を指定します。**【AX6700S】【AX6600S】**
   - <qos>：0 ～ 48000 を指定します。**【AX6300S】**
   - 4 キューモード時は <qos1> ～ <qos4> が設定できます。
   - 8 キューモード時は <qos1> ～ <qos8> が設定できます。

[コマンド省略時の動作]

ポート帯域制御で使用するキューごとのバッファの値を，デフォルト値に従って設定します。デフォルト値は，「コンフィグレーションガイド Vol.2　6.7.2 バッファ管理」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. 階層化シェーパ機能をサポートしていない NIF のインタフェースに対して，本コマンドは設定できません。
2. NIF 当たりのバッファ容量の上限値を超えて <qos> に設定した場合，上限値を装置に反映します。**【AX6300S】**

3. 4 キューモード時に，<qos1> ～ <qos8> に値を設定した場合，<qos1> ～ <qos4> に設定した値は反映され，<qos5> ～ <qos8> に設定した値は無視されます。
4. 8 キューモード時に，<qos5> ～ <qos8> に値を設定しなかった場合，<qos1> ～ <qos4> に指定した値は無視され，初期値が反映されます。

［関連コマンド］

shaper nif

shaper port rate-limit

該当シェーパモード

すべて

イーサネットインタフェースに対して，ポート帯域制御を設定します。

本コマンドは，該当インタフェースの NIF に対してシェーパモードの設定がない場合，設定できません。また，シェーパ自動設定機能を使用している場合や，シェーパ機能を使用できるポート数の上限を超える場合，該当インタフェースに対して，本コマンドは設定できません。

［入力形式］

情報の設定・変更

shaper port rate-limit { <kbit/s> | <Mbit/s>M }

情報の削除

no shaper port rate-limit

［入力モード］

(config-if)

［パラメータ］

{ <kbit/s> | <Mbit/s>M }

ポート帯域制御値を指定します。本機能を使用すれば，回線の送信帯域を指定した帯域に制限できます。

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
   次の表に示します。
   値の単位には M が指定できます。
   帯域は回線速度以下になるように設定してください。

表 7-21　ポート帯域制御値の設定範囲

回線速度（オートネゴシエーション結果も含む）	設定範囲		刻み値
1000Mbit/s	M 単位	1M ～ 1000M	1Mbit/s
	k 単位	64 ～ 1000000	1kbit/s
100Mbit/s	M 単位	1M ～ 100M	1Mbit/s
	k 単位	64 ～ 100000	1kbit/s
10Mbit/s	M 単位	1M ～ 10M	1Mbit/s
	k 単位	64 ～ 10000	1kbit/s

3. 本パラメータ使用時の注意事項
   ・該当インタフェースに設定してある，すべてのユーザとデフォルトユーザの最低帯域の合計値より小さい値は設定できません（該当シェーパモード：[rgq] [llpq1] [llpq2] [llpq4]）。
   ・インタフェースに対して llrlq1 または llrlq2 を設定している場合，該当インタフェースに設定されている llrlq1 および llrlq2 の最大帯域，ならびにすべてのユーザおよびデフォルトユーザの最低帯域の合計値より小さい値は設定できません（該当シェーパモード：[rgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]）。**【AX6700S】【AX6600S】**

・インタフェースに対して llrlq1 または llrlq2 を設定している場合，該当インタフェースに設定されている llrlq1 と llrlq2 の最大帯域の合計値より小さい値は設定できません（該当シェーパモード：[wgq llrlq]）。**【AX6700S】【AX6600S】**
・インタフェースに対して shaper wgq-group rate-limit を設定している場合，該当インタフェースに設定してある shaper wgq-group rate-limit より小さい値は設定できません。**【AX6700S】【AX6600S】**

[コマンド省略時の動作]

ポート帯域制御値を 1000M に設定します。

[通信への影響]

設定内容を変更，削除した場合，ポートの inactivate 処理が行われ，通信が一時的に切断されます。

[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. 階層化シェーパ機能をサポートしていない NIF のインタフェースに対して，本コマンドは設定できません。

[関連コマンド]

shaper nif

shaper user

該当シェーパモード

すべて

イーサネットインタフェースに対して，ユーザリストを適用して，ユーザを有効にします。

本コマンドは，該当インタフェースの NIF に対してシェーパモードの設定がない場合，設定できません。また，シェーパ自動設定機能を使用している場合や，シェーパ機能を使用できるポート数の上限を超える場合，本コマンドは設定できません。

［入力形式］

情報の設定

shaper user <user id list> list <user list name>

情報の変更

shaper user { <user id list> | add <user id list> } list <user list name>

shaper user remove <user id list>

情報の削除

no shaper user

［入力モード］

(config-if)

［パラメータ］

<user id list>

ユーザ 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 ～ 1023 を指定します。設定できるユーザ ID の範囲は，シェーパモード，キュー数によって異なります。設定範囲外のユーザ ID を指定した場合，装置に反映されません。**【AX6700S】** **【AX6600S】**
   ・1 ～ 511 を指定します。設定できるユーザ ID の範囲は，キュー数によって異なります。設定範囲外のユーザ ID を指定した場合，装置に反映されません。**【AX6300S】**
   ・指定する値はインタフェース内で重複できません。

list <user list name>

ユーザ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
   ・<user list name>：31 文字以内（先頭文字は数字以外）の名前を指定します。
   ・shaper user-list コマンドで作成済みのユーザリスト名称を指定します。
3. 本パラメータ使用時の注意事項
   ・該当インタフェースに設定している，すべてのユーザとデフォルトユーザの最低帯域の合計値がポート帯域制御値を超える場合は設定できません（該当シェーパモード：[rgq] [llpq1] [llpq2] [llpq4]）。
   ・該当インタフェースに設定しているすべてのユーザおよびデフォルトユーザの最低帯域，ならび

に llrlq1 および llrlq2 の最大帯域との合計がポート帯域制御値を超える場合は設定できません（該当シェーパモード：[rgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]）。**【AX6700S】【AX6600S】**
・指定したユーザリストが，該当インタフェースの NIF に設定されているシェーパモードに適した設定内容になっていない場合，設定できません。詳しい設定内容の制限はユーザリストのコマンドを参照してください。

add <user id list>

指定済みユーザリストにユーザ ID 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
   ・1 ～ 1023 を指定します。設定するユーザ ID の範囲は，シェーパモード，キュー数によって異なります。設定範囲外のユーザ ID を指定した場合，装置に反映されません。**【AX6700S】【AX6600S】**
   ・1 ～ 511 を指定します。設定するユーザ ID の範囲は，キュー数によって異なります。設定範囲外のユーザ ID を指定した場合，装置に反映されません。**【AX6300S】**
   ・指定する値はインタフェース内で重複できません。
3. 変更後の <user id list> の扱い
   ユーザ ID の追加でユーザリストの長さが長くなった場合，ユーザリストを分割して複数行の ” shaper user ” 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，ユーザ ID の追加後にユーザリストの長さが短くなった場合，複数行の ” shaper user ” コマンドのユーザ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。

remove <user id list>

指定済みユーザリストからユーザ ID 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
   ・1 ～ 1023 を指定します。ただし，該当ユーザリストに指定済みのユーザ ID だけが対象です。複数のユーザリストを削除できます。**【AX6700S】【AX6600S】**
   ・1 ～ 511 を指定します。ただし，該当ユーザリストに指定済みのユーザ ID だけが対象です。複数のユーザリストを削除できます。**【AX6300S】**
3. 変更後の <user id list> の扱い
   ユーザ ID の削除でユーザリストの長さが長くなった場合，ユーザリストを分割して複数行の ” shaper user ” 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，ユーザ ID の削除後にユーザリストの長さが短くなった場合，複数行の ” shaper user ” コマンドのユーザ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］

該当インタフェースに対してユーザを設定しません。

［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. 階層化シェーパ機能をサポートしていない NIF のインタフェースに対して，本コマンドは設定できません。

[関連コマンド]

shaper nif

shaper user-list

shaper user-list

該当シェーパモード

すべて

ユーザリストを作成します。装置当たり最大 8192 リスト作成できます。

[入力形式]

情報の設定・変更

shaper user-list <user list name> [peak-rate {<kbit/s> | <Mbit/s>M} [min-rate {<kbit/s> | <Mbit/s>M} [llpq-peak-rate {<kbit/s> | <Mbit/s>M}]]] [weight <weight>] [{
pq |
llq+3wfq <rate1>% <rate2>% <rate3>% <rate4>% |
4wfq <rate1>% <rate2>% <rate3>% <rate4>% |
pq+llq+2wfq <rate1>% <rate2>% <rate3>% |
2pq+llq+4wfq+beq <rate2>% <rate3>% <rate4>% <rate5>% <rate6>% |
4pq+4wfq <rate1>% <rate2>% <rate3>% <rate4>% |
2pq+4wfq+2beq <rate3>% <rate4>% <rate5>% <rate6>% }]
[queue-length <length1> <length2> <length3> <length4> [<length5> <length6> <length7> <length8>]] [discard <queue1> <queue2> <queue3> <queue4> [<queue5> <queue6> <queue7> <queue8>]]**【AX6700S】【AX6600S】**

shaper user-list <user list name> [peak-rate {<kbit/s> | <Mbit/s>M} [min-rate {<kbit/s> | <Mbit/s>M}]] [weight <weight>] [{
pq |
llq+3wfq <rate1>% <rate2>% <rate3>% <rate4>% |
4wfq <rate1>% <rate2>% <rate3>% <rate4>% |
pq+llq+2wfq <rate1>% <rate2>% <rate3>% |
2pq+llq+4wfq+beq <rate2>% <rate3>% <rate4>% <rate5>% <rate6>% |
4pq+4wfq <rate1>% <rate2>% <rate3>% <rate4>% |
2pq+4wfq+2beq <rate3>% <rate4>% <rate5>% <rate6>% }]
[queue-length <length1> <length2> <length3> <length4> [<length5> <length6> <length7> <length8>]] [discard <queue1> <queue2> <queue3> <queue4> [<queue5> <queue6> <queue7> <queue8>]]**【AX6300S】**

情報の削除

no shaper user-list <user list name>

[入力モード]

(config)

[パラメータ]

<user list name>

ユーザ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
   <user list name>：31 文字以内（先頭文字は数字以外）の名前を指定します。
3. 本パラメータ使用時の注意事項

なし

peak-rate {<kbit/s> | <Mbit/s>M}

最大帯域を指定します。

1. 本パラメータ省略時の初期値
   最大帯域を設定しません。
2. 値の設定範囲
   ・<kbit/s>：64 ～ 1000000 を指定します。
   ・<Mbit/s>：1M ～ 1000M を指定します。
3. 本パラメータ使用時の注意事項
   ・該当シェーパモードのインタフェースのユーザまたはデフォルトユーザには，最大帯域を指定してください。指定していない場合は，該当ユーザリストは装置に反映されません（該当シェーパモード：[rgq] [rgq llrlq] [llpq1] [llpq1 llrlq] [llpq2] [llpq2 llrlq] [llpq4] [llpq4 llrlq]）。
   ・llrlq1 または llrlq2 に設定するユーザリストに最大帯域を指定していない場合は，該当ユーザリストは装置に反映されません。**【AX6700S】【AX6600S】**
   ・該当ユーザリストの最低帯域値より小さい値は設定できません。
   ・該当ユーザリストの LLPQ 帯域制御値より小さい値は設定できません。
   ・インタフェースのユーザまたはデフォルトユーザに設定するユーザリストの最大帯域値は，インタフェースに設定しているポート帯域制御値以下の値を設定してください。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに設定するユーザリストに最大帯域を設定した場合，最大帯域は装置に反映されません（該当シェーパモード：[wgq] [wgq llrlq]）。**【AX6700S】【AX6600S】**
   ・該当シェーパモードのインタフェースの llrlq1，llrlq2 の最大帯域の合計が，インタフェースに設定しているポート帯域制御値を超える値は設定できません（該当シェーパモード：[wgq llrlq]）。**【AX6700S】【AX6600S】**
   ・該当シェーパモードのインタフェースの llrlq1，llrlq2 の最大帯域とすべてのユーザ，デフォルトユーザの最低帯域の合計値が，インタフェースに設定しているポート帯域制御値を超える値は設定できません（該当シェーパモード：[rgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]）。**【AX6700S】【AX6600S】**

min-rate {<kbit/s> | <Mbit/s>M}

最低帯域を指定します。

1. 本パラメータ省略時の初期値
   最低帯域を設定しません。
2. 値の設定範囲
   ・<kbit/s>：64 ～ 1000000 を指定します。
   ・<Mbit/s>：1M ～ 1000M を指定します。
3. 本パラメータ使用時の注意事項
   ・該当シェーパモードのインタフェースのユーザまたはデフォルトユーザには，最低帯域を指定してください。指定していない場合は，該当ユーザリストは装置に反映されません（該当シェーパモード：[rgq] [rgq llrlq] [llpq1] [llpq1 llrlq] [llpq2] [llpq2 llrlq] [llpq4] [llpq4 llrlq]）。
   ・該当ユーザリストの最大帯域を超える値は設定できません。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに設定するユーザリストに最低帯域を設定した場合，最低帯域は装置に反映されません（該当シェーパモード：[wgq] [wgq llrlq]）。**【AX6700S】【AX6600S】**
   ・llrlq1 または llrlq2 に設定するユーザリストに最低帯域を設定した場合，最低帯域は装置に反映されません。**【AX6700S】【AX6600S】**
   ・インタフェースに対して，該当ユーザリストが設定されいる場合，該当インタフェースに設定し

ているユーザ，デフォルトユーザの最低帯域の合計値がポート帯域制御値を超える場合は設定できません（該当シェーパモード：[rgq] [llpq1] [llpq2] [llpq4]）。
・インタフェースに対して，該当ユーザリストが設定されいる場合，該当インタフェースに設定しているユーザ，デフォルトユーザの最低帯域と llrlq1，llrlq2 の最大帯域の合計値がポート帯域制御値を超える場合は設定できません（該当シェーパモード：[rgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]）。**【AX6700S】【AX6600S】**

llpq-peak-rate {<kbit/s> | <Mbit/s>M}【AX6700S】【AX6600S】

LLPQ 帯域制御を指定します。

1. 本パラメータ省略時の初期値
   低遅延キューの最大帯域値は，ユーザリストの最低帯域値となります。
2. 値の設定範囲
   ・<kbit/s>：64 ～ 1000000 を指定します。
   ・<Mbit/s>：1M ～ 1000M を指定します。
3. 本パラメータ使用時の注意事項
   ・該当ユーザリストに最低帯域の設定がない場合は設定できません。
   ・該当ユーザリストの最大帯域値を超える値は設定できません。
   ・llrlq1 または llrlq2 に設定するユーザリストに LLPQ 帯域制御を指定した場合，LLPQ 帯域制御は装置に反映されません。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに設定するユーザリストに LLPQ 帯域制御を指定した場合，LLPQ 帯域制御は装置に反映されません（該当シェーパモード：[rgq] [rgq llrlq] [wgq] [wgq llrlq]）。

weight <weight>

帯域分配の重みを指定します。

1. 本パラメータ省略時の初期値
   帯域分配の重みを 1 に設定します。
2. 値の設定範囲
   1 ～ 50 を指定します。
3. 本パラメータ使用時の注意事項
   ・該当シェーパモードのインタフェースの llrlq1 または llrlq2 に設定したユーザリストに weight 値を指定した場合，weight 値は装置に反映されません。**【AX6700S】【AX6600S】**
   ・該当シェーパモードのインタフェースのユーザまたはデフォルトユーザに設定したユーザリストに weight 値 11 以上を指定した場合，weight 値は 10 で装置に反映されます（該当シェーパモード：[wgq] [wgq llrlq]）。**【AX6700S】【AX6600S】**
   ・該当シェーパモードのインタフェースのユーザまたはデフォルトユーザに設定したユーザリストに，peak-rate と min-rate が同じ値で設定してある場合，weight 値は装置に反映されません（該当シェーパモード：[rgq] [rgq llrlq] [llpq1] [llpq1 llrlq] [llpq2] [llpq2 llrlq] [llpq4] [llpq4 llrlq]）。

{ pq |

llq+3wfq <rate1>% <rate2>% <rate3>% <rate4>% |

4wfq <rate1>% <rate2>% <rate3>% <rate4>% |

pq+llq+2wfq <rate1>% <rate2>% <rate3>% |

2pq+llq+4wfq+beq <rate2>% <rate3>% <rate4>% <rate5>% <rate6>% |

4pq+4wfq <rate1>% <rate2>% <rate3>% <rate4>% |

2pq+4wfq+2beq <rate3>% <rate4>% <rate5>% <rate6>%}

スケジューリングモードを指定します。NIF に設定しているユーザのキュー数によって，設定できるスケジューリングモードが変わります。

4 キューモード：pq,llq+3wfq,4wfq,pq+llq+2wfq

8 キューモード：pq,2pq+llq+4wfq+beq,4pq+4wfq,2pq+4wfq+2beq

pq

完全優先制御でパケットを送信します。

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
   なし
3. 本パラメータ使用時の注意事項**【AX6700S】【AX6600S】**
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，最優先のキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq1] [llpq1 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，優先度の高い二つのキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq2] [llpq2 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，優先度の高い四つのキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq4] [llpq4 llrlq]）。

llq+3wfq <rate1>% <rate2>% <rate3>% <rate4>%

4 番キュー（llq）を設定比率分だけ最優先で出力します。3 ～ 1 番キュー（3wfq）は，ユーザの送信帯域から 4 番キューの使用帯域（設定帯域ではない）を引いた残りの帯域を，重みに従って分配する重み付き均等保障キューです。

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
   ・<rate1> ～ <rate3>：1 ～ 100 を指定します。ただし，「<rate1> ≦ <rate2> ≦ <rate3>」かつ各 <rate> の合計値が 100 以下になるように指定してください。
   ・<rate4>：5 ～ 100 を指定します。ただし，数値は 5 刻みです。100 を指定した場合，4 番キューは完全優先として動作します。
3. 本パラメータ使用時の注意事項**【AX6700S】【AX6600S】**
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，<rate4> に 100 を設定したときだけ，最優先のキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります。<rate4> に 100 以外の値が設定されていた場合，pq として動作します（該当シェーパモード：[llpq1] [llpq1 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，pq として動作します（該当シェーパモード：[llpq2] [llpq2 llrlq] [llpq4] [llpq4 llrlq]）。

4wfq <rate1>% <rate2>% <rate3>% <rate4>%

重みに従って分配する重み付き均等保障キューです。

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
   <rate1> ～ <rate4>：1 ～ 100 を指定します。ただし，「<rate1> ≦ <rate2> ≦ <rate3> ≦ <rate4>」かつ各 <rate> の合計値が 100 以下になるように指定してください。

3. 本パラメータ使用時の注意事項【AX6700S】【AX6600S】
   該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，pq として動作します（該当シェーパモード：[llpq1] [llpq1 llrlq] [llpq2] [llpq2 llrlq] [llpq4] [llpq4 llrlq]）。

pq+llq+2wfq <rate1>% <rate2>% <rate3>%

4 番キュー（pq）は，最優先でパケットを出力する完全優先キューです。3 番キュー（llq）は，ユーザの送信帯域から 4 番キューの使用帯域を引いた残りの帯域を，設定比率分だけ優先的にパケット出力します。残りの帯域を 2 ～ 1 番キュー（2wfq）で重み付けによる分配をします。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   ・<rate1> ～ <rate2>：1 ～ 100 を指定します。ただし，「<rate1> ≦ <rate2>」かつ各 <rate> の合計値が 100 以下になるように指定してください。
   ・<rate3>：5 ～ 100 を指定します。ただし，数値は 5 刻みです。100 を指定した場合，3 番キューは完全優先として動作します。
3. 本パラメータ使用時の注意事項【AX6700S】【AX6600S】
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，最優先のキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq1] [llpq1 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，<rate3> に 100 を設定した場合だけ，優先度の高い二つのキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります。<rate3> に 100 以外の値が設定されていた場合，pq として動作します（該当シェーパモード：[llpq2] [llpq2 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，pq として動作します（該当シェーパモード：[llpq4] [llpq4 llrlq]）。

2pq+llq+4wfq+beq <rate2>% <rate3>% <rate4>% <rate5>% <rate6>%

8 ～ 7 番キュー（2pq）は，最優先でパケットを出力する完全優先キューです。6 番キュー（llq）は，ユーザの送信帯域から 8 ～ 7 番キューの使用帯域を引いた残りの帯域を，設定比率分だけ優先的にパケット出力をします。残りの帯域を 5 ～ 2 番キュー（4wfq）で重み付けによる分配をします。残り帯域を 1 番キュー（beq）が使用します。

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
   ・<rate2> ～ <rate5>：1 ～ 100 を指定します。ただし，「<rate2> ≦ <rate3> ≦ <rate4> ≦ <rate5>」かつ各 <rate> の合計値が 100 以下になるように指定してください。
   ・<rate6>：5 ～ 100 を指定します。ただし，数値は 5 刻みです。100 を指定した場合，6 番キューは完全優先として動作します。
3. 本パラメータ使用時の注意事項【AX6700S】【AX6600S】
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，最優先のキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq1] [llpq1 llrlq] [llpq2] [llpq2 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，優先度の高い二つのキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq2] [llpq2 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，pq として動作します（該当シェーパモード：[llpq4] [llpq4 llrlq]）。

4pq+4wfq <rate1>% <rate2>% <rate3>% <rate4>%

8 ～ 5 番キュー（4pq）は，最優先でパケットを出力する完全優先キューです。4 ～ 1 番キュー（4wfq）は，ユーザの送信帯域から 8 ～ 5 番キューの使用帯域（設定帯域ではない）を引いた残りの帯域を，重みに従って分配する重み付き均等保障キューです。

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
   <rate1> ～ <rate4>：1 ～ 100 を指定します。ただし，「<rate1> ≦ <rate2> ≦ <rate3> ≦ <rate4>」かつ各 <rate> の合計値が 100 以下になるように指定してください。
3. 本パラメータ使用時の注意事項**【AX6700S】【AX6600S】**
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，最優先のキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq1] [llpq1 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，優先度の高い二つのキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq2] [llpq2 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，優先度の高い四つのキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq4] [llpq4 llrlq]）。

2pq+4wfq+2beq <rate3>% <rate4>% <rate5>% <rate6>%

8 ～ 7 番キュー（2pq）は，最優先でパケットを出力する完全優先キューです。6 ～ 3 番キュー（4wfq）は，ユーザの送信帯域から 8 ～ 7 番キューの使用帯域（設定帯域ではない）を引いた残りの帯域を，重みに従って分配する重み付き均等保障キューです。残りの帯域を 2 ～ 1 番キュー（2beq）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
   <rate3> ～ <rate6>：1 ～ 100 を指定します。ただし，「<rate3> ≦ <rate4> ≦ <rate5> ≦ <rate6>」かつ各 <rate> の合計値が 100 以下になるように指定してください。ユーザリストの最大帯域値を設定します。
3. 本パラメータ使用時の注意事項**【AX6700S】【AX6600S】**
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，最優先のキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq1] [llpq1 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，優先度の高い二つのキューが，LLPQ 帯域制御を最大帯域とした低遅延キューとなります（該当シェーパモード：[llpq2] [llpq2 llrlq]）。
   ・該当シェーパモードのインタフェースのユーザおよびデフォルトユーザに指定した場合，pq として動作します（該当シェーパモード：[llpq4] [llpq4 llrlq]）。

1. 本パラメータ省略時の初期値
   スケジューリングモードは pq になります。
2. 値の設定範囲
   pq，llq+3wfq，4wfq，pq+llq+2wfq，2pq+llq+4wfq+beq，4pq+4wfq，2pq+4wfq+2beq
3. 本パラメータ使用時の注意事項
   キューモードと一致しないスケジューリングモードを指定した場合，pq で動作します。

queue-length <length1> <length2> <length3> <length4> [<length5> <length6> <length7> <length8>]

各キューに対するキュー長を指定します。

1. 本パラメータ省略時の初期値
   各キューのキュー長をデフォルト値に従って設定します。デフォルト値は，「コンフィグレーションガイド Vol.2　6.7.2 バッファ管理」を参照してください。
2. 値の設定範囲
   ・<length>：0 ～ 4000 を指定します。
   ・4 キューモード時は <length1> ～ <length4> が設定できます。
   ・8 キューモード時は <length1> ～ <length8> が設定できます。
3. 本パラメータ使用時の注意事項
   ・4 キューモード時に，<length1> ～ <length8> に値を設定した場合，<length1> ～ <length4> に設定した値は反映され，<length5> ～ <length8> に設定した値は無視されます。
   ・8 キューモード時に，<length5> ～ <length8> に値を設定しなかった場合，<length1> ～ <length4> に指定した値は無視され，初期値が反映されます。

discard <queue1> <queue2> <queue3> <queue4> [<queue5> <queue6> <queue7> <queue8>]

各キューの廃棄制御モードを指定します。

1. 本パラメータ省略時の初期値
   各キューは tail-drop2 で動作します。
2. 値の設定範囲
   ・<queue>：tail-drop1，tail-drop2，tail-drop3 を指定します。
   ・4 キューモード時は <queue1> ～ <queue4> が設定できます。
   ・8 キューモード時は <queue1> ～ <queue8> が設定できます。
   次の表に各廃棄モードに対する廃棄閾値を示します。

表 7-22　廃棄モードに対する破棄閾値

廃棄モード	キューイング優先度	
	1 ～ 2	3 ～ 4
tail-drop1	1/4	4/4
tail-drop2	2/4	4/4
tail-drop3	3/4	4/4

3. 本パラメータ使用時の注意事項
   ・4 キューモード時に，<queue1> ～ <queue8> に値を設定した場合，<queue1> ～ <queue4> に設定した値は反映され，<queue5> ～ <queue8> に設定した値は無視されます。
   ・8 キューモード時に，<queue5> ～ <queue8> に値を設定しなかった場合，<queue1> ～ <queue4> に指定した値は無視され，初期値が反映されます。

[コマンド省略時の動作]

ユーザリストを作成しません。

[通信への影響]

インタフェースに設定済みのユーザリストの設定内容を変更した場合，該当ユーザの通信が一時的に切断されます。

[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]

なし

[関連コマンド]

shaper nif

shaper vlan-user-map

装置に VLAN ユーザマッピングを使用します。本コマンドを設定した場合，VLAN Tag のヘッダ情報に基づいたキューイングをします。QoS フローリストの優先度決定によるキューイングはしません。

［入力形式］

情報の設定・変更

shaper vlan-user-map [user-priority-queue-map <priority0> <priority1> <priority2> <priority3> <priority4> <priority5> <priority6> <priority7>]

情報の削除

no shaper vlan-user-map

［入力モード］

(config)

［パラメータ］

user-priority-queue-map <priority0> <priority1> <priority2> <priority3> <priority4> <priority5> <priority6> <priority7>

ユーザ優先度キューマッピングの設定をします。ユーザ優先度 0 ～ 7 に対応する <priority0> ～ <priority7> にキュー番号を指定してください。

1. 本パラメータ省略時の初期値
   <priority0>：3
   <priority1>：1
   <priority2>：2
   <priority3>：4
   <priority4>：5
   <priority5>：6
   <priority6>：7
   <priority7>：8
2. 値の設定範囲
   <priority0> ～ <priority7>：1 ～ 8 を指定します。
3. 本パラメータ使用時の注意事項
   シェーパ NIF で動作しているキュー数によって，キューイングされるキュー番号が異なります。キューイングされるキュー番号を次の表に示します。

表 7-23　キューイングされるキュー番号

本パラメータで指定したキュー番号	8 キュー動作（デフォルト）時のキューイングされるキュー番号	4 キュー動作時のキューイングされるキュー番号
1	1	1
2	2	
3	3	2
4	4	
5	5	3
6	6	
7	7	4

本パラメータで指定したキュー番号	8 キュー動作（デフォルト）時のキューイングされるキュー番号	4 キュー動作時のキューイングされるキュー番号
8	8	

［コマンド省略時の動作］

VLAN ユーザマッピングを使用しません。

［通信への影響］

設定内容を変更，削除した場合，NIF がリセットされて通信が一時的に切断されます。

［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. 本機能は，階層化シェーパ機能をサポートしていない NIF に対しては反映されません。
2. 本機能は，VLAN Tag の TPID に 0x8100 または 0x9100 の値が設定してあるパケットを対象にします。
3. 本機能は，シェーパ自動設定機能またはシェーパモードが反映されていない NIF に対しては反映されません。

［関連コマンド］

shaper nif

shaper auto-configuration

shaper wgq-group rate-limit【AX6700S】【AX6600S】

該当シェーパモード
[wgq llrlq]

イーサネットインタフェースに対して，該当インタフェース内のすべてのユーザで使用する合計帯域に，WGQ 帯域制御を設定します。本コマンドは，該当インタフェースの NIF に対してシェーパモードの設定がない場合，設定できません。

[入力形式]

情報の設定・変更
shaper wgq-group rate-limit { <kbit/s> | <Mbit/s>M }

情報の削除
no shaper wgq-group rate-limit

[入力モード]

```
(config-if)
```

[パラメータ]

rate-limit { <kbit/s> | <Mbit/s>M }
WGQ 帯域制御値を指定します。
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
   ・<kbit/s>：64 ～ 1000000 を指定します。
   ・<Mbit/s>：1M ～ 1000M を指定します。
3. 本パラメータ使用時の注意事項
   ポート帯域制御値を超える値は設定できません。

[コマンド省略時の動作]

該当インタフェースに対して，WGQ 帯域制御を設定しません。

[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. 階層化シェーパ機能をサポートしていない NIF のインタフェースに対して，本コマンドは設定できません。
2. 該当シェーパモード以外のシェーパモードで動作しているインタフェースに対して本コマンドを設定した場合，装置に反映されません。

[関連コマンド]

shaper nif

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 7-24　ポート帯域制御の設定範囲

項番	回線速度（オートネゴシエーション結果も含む）	設定範囲		刻み値
1	10Gbit/s	G 単位	1G ～ 10G	1Gbit/s
		M 単位	100M ～ 10000M	100Mbit/s
		k 単位	指定不可	－
2	1Gbit/s	G 単位	1G	－
		M 単位	10M ～ 1000M	10Mbit/s
		k 単位	指定不可	－
3	100Mbit/s ※	G 単位	指定不可	－
		M 単位	1M ～ 100M	1Mbit/s
		k 単位	指定不可	－
4	10Mbit/s ※	G 単位	指定不可	－
		M 単位	1M ～ 10M	1Mbit/s
		k 単位	300 ～ 10000	100kbit/s

（凡例）　－：該当しない

注※　全二重モードの場合だけポート帯域制御が動作します

［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. 回線状態が半二重の場合，ポート帯域制御は動作しません。
2. 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。
3. あらかじめポート帯域制御を設定しているポートで，オートネゴシエーションで決定した回線速度では，設定した帯域幅でポート帯域制御が動作できないことがあります。このような場合，運用ログメッセージが出力されます。
   ポート帯域制御が動作しない場合の例を次に示します。
   - ポート帯域制御の設定帯域が，オートネゴシエーションで決定した回線速度を超えている場合
     （例：ポート帯域設定 50Mbit/s　決定した回線速度 10Mbit/s など）
   - ポート帯域制御の設定帯域が，オートネゴシエーションで決定した回線速度の設定単位と異なる場合
     （例：ポート帯域設定 50Mbit/s　決定した回線速度 1000Mbit/s など）
4. レガシーシェーパ機能をサポートしていない NIF のインタフェースに対して，本コマンドは設定できません。
5. 階層化シェーパ機能が設定してある NIF のインタフェースに対して，本コマンドは設定できません。

[関連コマンド]

interface gigabitethernet

interface tengigabitethernet

upc-storm-control mode

QoS 機能の帯域監視およびストームコントロールのモードを設定します。本コマンドは，装置当たりのハードウェアテーブルでの QoS 機能の帯域監視およびストームコントロールの最大エントリ数を変更します。運用形態に応じたモードに変更することで，ハードウェアリソースを必要な機能に集中させて使用できるようになります。

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，変更する場合に QoS 機能の帯域監視を削除する必要があります。また，変更するモードによってはストームコントロールを削除する必要があります。したがって，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。

［入力形式］

情報の設定・変更

upc-storm-control mode {upc-in-and-storm-control | upc-in-in}**【AX6700S】**

upc-storm-control mode {upc-in-and-storm-control | upc-in-in | upc-in-out}**【AX6600S】** **【AX6300S】**

［入力モード］

(config)

［パラメータ］

{upc-in-and-storm-control | upc-in-in}【AX6700S】

{upc-in-and-storm-control | upc-in-in | upc-in-out}【AX6600S】【AX6300S】

帯域監視ストームコントロールモードを指定します。

upc-in-and-storm-control は，帯域監視を受信側にフロー検出条件に対して最大帯域制御または最低帯域監視とストームコントロールが使用できるモードに設定します。

upc-in-in は，帯域監視を受信側にフロー検出条件に対して最大帯域制御および最低帯域監視が使用できるモードに設定します。

AX6300S の場合，upc-in-out は帯域監視を受信側および送信側にフロー検出条件に対して最大帯域制御または最低帯域監視が使用できるモードに設定します。

帯域監視ストームコントロールモードの詳細については，「コンフィグレーションガイド Vol.2」を参照してください。

1. 本パラ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］

初期起動時に upc-in-and-storm-control 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]

1. AX6700S では，ストームコントロールが設定されている場合，upc-in-in は設定できません。
2. AX6600S，AX6300S では，ストームコントロールが設定されている場合，upc-in-in または upc-in-out は設定できません。
3. 帯域監視ストームコントロールモードに upc-in-out を設定する場合，次のコマンドで指定する稼働 PSP 数にすべて 1 を指定してください。**【AX6600S】**
   - redundancy max-psp
   - schedule-power-control max-psp
   - adaptive-power-control max-psp

[関連コマンド]

ip qos-flow-group

ipv6 qos-flow-group

mac qos-flow-group

storm-control（global）

storm-control（interface）

8 レイヤ 2 認証

コンフィグレーションコマンドと適用するレイヤ 2 認証

authentication ip access-group

コンフィグレーションコマンドと適用するレイヤ 2 認証

レイヤ 2 認証で共通に使用するコンフィグレーションコマンドと適用するレイヤ 2 認証を次の表に示します。

表 8-1　コンフィグレーションコマンドと適用するレイヤ 2 認証

コマンド名	適用するレイヤ 2 認証		
	IEEE802.1X※1	Web 認証※2	MAC 認証
authentication ip access-group	○	○	○

（凡例）
○：コマンドが設定できます。
注※ 1　IEEE802.1X はポート単位認証のシングルモードとマルチモードでは適用できません。
注※ 2　Web 認証は固定 VLAN モードおよびダイナミック VLAN モードで適用します。

authentication ip access-group

認証前の端末から送信される他宛ての IP パケットを，IPv4 アクセスリストを適用して指定されたパケットだけ認証対象外のポートへ出力させます。

[入力形式]

情報の設定・変更

authentication ip access-group {<access list number> | <access list name>}

情報の削除

no authentication ip access-group {<access list number> | <access list name>}

[入力モード]

(config)

[パラメータ]

{<access list number> | <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。

本パラメータで設定できる IPv4 パケットフィルタの識別子は装置で一つです。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   <access list number> の場合は，100 ～ 199，2000 ～ 2699（10 進数）を指定します。
   <access list name> の場合は，31 文字以内の名前を指定します。
   詳細は，「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. 認証用 IPv4 アクセスリストで適用できるアクションは permit だけで，フィルタ条件も下記に限定されます。
   - プロトコル名称が tcp または udp
   - 宛先 IPv4 アドレスおよびマスク
   - 宛先ポート番号
2. 認証用 IPv4 アクセスリストに一致したパケットは，装置内の処理優先度が低くなります。例えば，ルーティングプロトコルの制御パケットが認証用 IPv4 アクセスリストに一致した場合，装置内で処理する優先度が低いためにパケットが失われ，ルーティングテーブル上から経路がなくなるおそれがあります。
   このため，適用する認証用 IPv4 アクセスリストは，認証前に通信が必要なホストを指定するなど，必要最低限の条件を設定してください。

［関連コマンド］

dot1x system-auth-control

mac-authentication system-auth-control

web-authentication system-auth-control

9 IEEE802.1X

aaa accounting dot1x default

aaa authentication dot1x default

aaa authorization network default

dot1x force-authorized-port

dot1x ignore-eapol-start

dot1x logging enable

dot1x loglevel

dot1x max-req

dot1x max-supplicant

dot1x multiple-authentication

dot1x multiple-hosts

dot1x port-control

dot1x reauthentication

dot1x supplicant-detection

dot1x system-auth-control

dot1x timeout keep-unauth

dot1x timeout quiet-period

dot1x timeout reauth-period

dot1x timeout server-timeout

dot1x timeout supp-timeout

dot1x timeout tx-period

dot1x vlan dynamic enable

dot1x vlan dynamic ignore-eapol-start

dot1x vlan dynamic max-req

dot1x vlan dynamic max-supplicant

dot1x vlan dynamic radius-vlan
dot1x vlan dynamic reauthentication
dot1x vlan dynamic supplicant-detection
dot1x vlan dynamic timeout quiet-period
dot1x vlan dynamic timeout reauth-period
dot1x vlan dynamic timeout server-timeout
dot1x vlan dynamic timeout supp-timeout
dot1x vlan dynamic timeout tx-period
dot1x vlan enable
dot1x vlan ignore-eapol-start
dot1x vlan max-req
dot1x vlan max-supplicant
dot1x vlan reauthentication
dot1x vlan supplicant-detection
dot1x vlan timeout quiet-period
dot1x vlan timeout reauth-period
dot1x vlan timeout server-timeout
dot1x vlan timeout supp-timeout
dot1x vlan timeout tx-period

aaa accounting dot1x default

指定された認証方式のアカウンティング集計を行う場合に設定します。IEEE802.1X の認証のアカウンティング情報だけが集計されます。

[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]

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

RADIUS サーバ承認によるアカウンティング要求を行います。

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
   group radius

[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]

dot1x system-auth-control

radius-server host

aaa authentication dot1x default

IEEE802.1X のユーザ認証方式を指定します。

［入力形式］

情報の設定

aaa authentication dot1x default group radius

情報の削除

no aaa authentication dot1x default

［入力モード］

(config)

［パラメータ］

group radius

RADIUS サーバによる IEEE802.1X 認証を行います。

1. 本パラ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］

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. 本設定が行われていないと，IEEE802.1X の認証時に RADIUS サーバを使用できません。

［関連コマンド］

aaa authorization network

dot1x system-auth-control

radius-server host

aaa authorization network default

認証方式によって指定された VLAN 情報に従って，VLAN 単位認証（動的）を行う場合に指定します。

［入力形式］

情報の設定

aaa authorization network default group radius

情報の削除

no aaa authorization network default

［入力モード］

(config)

［パラメータ］

group radius

RADIUS サーバによる IEEE802.1X 認証を行います。

1. 本パラ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］

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. 本設定が行われていないと，VLAN 単位認証（動的）を使用できません。

［関連コマンド］

dot1x vlan dynamic enable

aaa authentication dot1x

radius-server host

dot1x force-authorized-port

VLAN 単位認証（静的）を設定した VLAN 内に，認証不要で疎通を許可する特定のポートまたはチャネルグループを設定します。

［入力形式］

情報の設定
　dot1x force-authorized-port

情報の削除
　no dot1x force-authorized-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］

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 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. Web 認証および MAC 認証の認証ポートには設定しないでください。

［関連コマンド］

dot1x system-auth-control

dot1x vlan 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 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. 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。
3. 本コマンドは dot1x reauthentication コマンドが設定されていて，かつ dot1x supplicant-detection コマンドの disable の指定がないインタフェースにだけ設定できます。
4. dot1x supplicant-detection コマンドの disable を指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。
5. 本コマンドを指定したインタフェースでは，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］

なし

［関連コマンド］

dot1x loglevel

dot1x system-auth-control

logging email-event-kind

logging event-kind

dot1x loglevel

IEEE802.1X の動作ログメッセージで記録するメッセージレベルを指定します。記録されたログメッセージは運用コマンド show dot1x logging で表示されます。

[入力形式]

情報の設定・変更

dot1x loglevel {error | warning | notice | info}

情報の削除

no dot1x loglevel

[入力モード]

(config)

[パラメータ]

{error | warning | notice | info}

error

error レベルのログメッセージだけを記録します。ソフトウェアエラーだけ記録します。

warning

error レベルと warning レベルのログメッセージを記録します。不正フレーム情報などの異常検出情報が記録されます。

notice

error，warning，notice および normal レベルのログメッセージを記録します。認証可否情報やサーバ接続情報が記録されます。

info

error，warning，notice，normal および info レベルのログメッセージを記録します。動作追跡情報が記録されます。

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
   error，warning，notice，または info

[コマンド省略時の動作]

動作ログメッセージで記録するメッセージレベルは info 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 IEEE802.1X は，dot1x 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］

dot1x system-auth-control

dot1x max-req

supp-timeout 値を超えた際の EAP-Request 再送の最大回数を指定します。再送回数が本値を超えた場合，認証失敗と判定します。

[入力形式]

情報の設定・変更
　dot1x max-req <count>

情報の削除
　no dot1x max-req

[入力モード]

(config-if)

[パラメータ]

<count>

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

[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 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. 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 max-supplicant

認証サブモードを端末認証モードに指定したときの指定インタフェースに接続可能な最大端末数を指定します。本値を超えて端末を接続しようとした場合，認証を行わないで端末接続数を制限できます。

[入力形式]

情報の設定・変更
dot1x max-supplicant <clients>

情報の削除
no dot1x max-supplicant

[入力モード]

(config-if)

[パラメータ]

<clients>

指定インタフェースに接続可能な最大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
   1 ～ 256

[コマンド省略時の動作]

接続可能な最大端末数は 256 です。

[通信への影響]

現在指定インタフェースで認証されている端末数よりも小さい値を指定した場合，指定インタフェースで認証されているすべての Supplicant の認証状態が解除されます。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 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. 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。
3. 現在指定インタフェースで認証されている端末数よりも小さい値を指定した場合，指定インタフェースで認証されているすべての Supplicant の認証状態がいったん解除されます。

[関連コマンド]

dot1x system-auth-control

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。mac-address-table static コマンドで設定された端末は，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。

認証サブモードにマルチモードまたは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，指定インタフェースが非認証状態へ移行します。mac-address-table static コマンドで設定された端末についても，認証対象の端末が認証に成功しなければ疎通しません。

[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，指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 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. 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。
3. 認証サブモードを変更した場合，指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。
4. dot1x multiple-hosts コマンドまたは dot1x multiple-authentication コマンドを設定しない場合は，認証サブモードにシングルモードが適用されます。

[関連コマンド]

dot1x system-auth-control

dot1x port-control

dot1x multiple-hosts

dot1x multiple-hosts

IEEE802.1X の認証サブモードをマルチモードに設定します。認証対象の端末は最初に認証を開始した 1 端末だけですが，この認証が成功すれば，そのほかの端末が認証不要で疎通可能になります。複数端末の接続が可能になります。mac-address-table static コマンドで設定された端末についても，認証対象の端末が認証に成功しなければ疎通しません。

認証サブモードにマルチモードまたは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，指定インタフェースが非認証状態へ移行します。mac-address-table static コマンドで設定された端末についても，認証対象の端末が認証に成功しなければ疎通しません。

[入力形式]

情報の設定
　dot1x multiple-hosts

情報の削除
　no dot1x multiple-hosts

[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，指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 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. 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。
3. 認証サブモードを変更した場合，指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。
4. dot1x multiple-hosts コマンドまたは dot1x multiple-authentication コマンドを設定しない場合は，認証サブモードにシングルモードが適用されます。
5. Web 認証および MAC 認証の認証ポートには設定しないでください。

[関連コマンド]

dot1x system-auth-control

dot1x port-control

dot1x multiple-authentication

dot1x port-control

指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 認証を行って，認証結果に応じて指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，指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。

force-unauthorized

IEEE802.1X 認証を行わないで，指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。

1. 本パラ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］

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 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. dot1x multiple-hosts コマンドまたは 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。
3. インタフェースが所属している VLAN に VLAN 単位認証が設定されているインタフェースには設定できません。

4. アクセスモードが設定されていないインタフェースには設定できません。
5. トンネリングポートには設定できません。
6. MAC アドレス学習抑止が設定されている VLAN に所属しているインタフェースには設定できません。
7. MAC アドレス学習数制限が設定されているインタフェースには設定できません。
8. MAC アドレス学習数制限が設定されている VLAN に所属しているインタフェースには設定できません。
9. EAPOL フォワーディング機能が設定されている VLAN に所属しているインタフェースには設定できません。
10. Web 認証および MAC 認証の認証ポートには，dot1x port-control force-authorized および dot1x port-control force-unauthorized を設定しないでください。
11. Web 認証および MAC 認証の認証ポートに設定する場合は，認証サブモードの端末認証モードを設定してください。

[関連コマンド]

dot1x system-auth-control

dot1x multiple-hosts

dot1x multiple-authentication

dot1x vlan enable

switchport mode

switchport access

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 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. 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。
3. dot1x ignore-eapol-start コマンドを指定したインタフェースでは，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指定した時の新規端末検出の動作を指定します。

[入力形式]

情報の設定・変更

dot1x supplicant-detection {disable | shortcut}

情報の削除

dot1x supplicant-detection

[入力モード]

(config-if)

[パラメータ]

{disable | shortcut}

認証サブモードに端末認証モード設定時の新規端末検出の動作を指定します。

disable

認証サブモードを端末認証モードに設定した場合に認証済み端末が存在するときは，新規端末検出用 EAP-Request/Identity 送信処理を抑止します。装置負荷低減のための認証シーケンスの省略によって異常動作となる Supplicant を使用している場合に指定してください。

本パラメータを指定した場合，端末側から認証を開始できないタイプの Supplicant でもデータフレームを検出した端末に対しては EAP-Request/Identity を送信して認証開始を促します。

shortcut

認証サブモードを端末認証モードに設定したときの新規端末検出用 EAP-Request/Identity 送信処理で，負荷低減のために認証済端末の認証シーケンスを省略します。端末側から認証を開始できないタイプの Supplicant を使用している場合に指定してください。

本パラメータを指定した場合，一部の Supplicant が正常に動作しないで，通信が一時的に停止します。

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
   disable または shortcut

[コマンド省略時の動作]

新規端末検出動作は 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 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. 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。

3. 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。
4. 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 disable を設定することはできません。

［関連コマンド］

dot1x ignore-eapol-start

dot1x multiple-authentication

dot1x system-auth-control

dot1x port-control

dot1x system-auth-control

IEEE802.1X を有効にします。

［入力形式］

情報の設定
　dot1x system-auth-control

情報の削除
　no dot1x system-auth-control

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. すべての IEEE802.1X 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. 認証 VLAN のコンフィグレーション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. GSRP 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。
4. aaa authentication dot1x default group radius 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］

aaa authentication dot1x default

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指定します。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]

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 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. 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。
3. 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-hosts

dot1x multiple-authentication

dot1x timeout quiet-period

IEEE802.1X の認証失敗後の該当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

［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 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. 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

［コマンド省略時の動作］

Supplicant の再認証を行う周期は 3600 秒です。

［通信への影響］

なし

［設定値の反映契機］

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき
- 認証済端末が存在しない状態の認証単位で認証端末の認証が成功したとき

［注意事項］

1. すべての IEEE802.1X 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. 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。
3. 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。
4. 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

[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 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. 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

［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 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. 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

［コマンド省略時の動作］

EAP-Request/Identity の送出間隔は 30 秒です。

［通信への影響］

なし

［設定値の反映契機］

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき

［注意事項］

1. すべての IEEE802.1X 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. 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。
3. パラメータの設定値は，dot1x timeout reauth-period コマンドで設定した値より小さな値を設定してください。

［関連コマンド］

dot1x timeout reauth-period

dot1x system-auth-control

dot1x port-control

dot1x vlan dynamic enable

IEEE802.1X VLAN 単位認証（動的）を有効にします。

［入力形式］

情報の設定
　dot1x vlan dynamic enable

情報の削除
　no dot1x vlan dynamic enable

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. すべての IEEE802.1X 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. dot1x vlan dynamic enable コマンドを設定する場合, aaa authorization network default group radius コマンドの設定を行わないと有効になりません。
3. 本コマンドが設定されていないと，すべての VLAN 単位認証（動的）機能は，有効になりません。

［関連コマンド］

dot1x system-auth-control

aaa authorization network default

dot1x vlan dynamic ignore-eapol-start

Supplicant からの EAPOL-Start 受信時に，EAP-Request/Identity を発行しないよう指定します。

［入力形式］

情報の設定
　dot1x vlan dynamic ignore-eapol-start

情報の削除
　no dot1x vlan dynamic ignore-eapol-start

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. すべての IEEE802.1X 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
3. 本コマンドは dot1x vlan dynamic reauthentication コマンドが設定されていて，かつ dot1x vlan dynamic supplicant-detection コマンドの disable の指定がないインタフェースにだけ設定できます。
4. dot1x vlan dynamic supplicant-detection コマンドを disable に指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。
5. 本コマンドを指定したインタフェースでは no dot1x vlan dynamic reauthentication コマンドで再認証を実施しないように設定することはできません。

［関連コマンド］

dot1x vlan dynamic reauthentication

dot1x vlan dynamic supplicant-detection

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic max-req

supp-timeout 値を超えた際の EAP-Request 再送の最大回数を指定します。再送回数が本値を超えた場合，認証失敗と判定します。

［入力形式］

情報の設定・変更

dot1x vlan dynamic max-req <count>

情報の削除

no dot1x vlan dynamic max-req

［入力モード］

(config)

［パラメータ］

<count>

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

［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 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。

［関連コマンド］

dot1x system-auth-control

dot1x vlan dynamic timeout supp-timeout

dot1x vlan dynamic enable

dot1x vlan dynamic max-supplicant

VLAN 単位認証（動的）で接続可能な最大端末数を指定します。本値を超えて端末を接続しようとした場合，認証を行わないで端末接続数を制限できます。

[入力形式]

情報の設定・変更

dot1x vlan dynamic max-supplicant <clients>

情報の削除

no dot1x vlan dynamic max-supplicant

[入力モード]

(config)

[パラメータ]

<clients>

VLAN 単位認証（動的）で接続可能な最大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
   1 ～ 4096

[コマンド省略時の動作]

最大端末数は 4096 です。

[通信への影響]

現在指定インタフェースで認証されている端末数よりも小さい値を指定した場合，指定インタフェースで認証されているすべての Supplicant の認証状態が解除されます。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 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
3. 現在 VLAN 単位認証（動的）で認証されている端末数よりも小さい値を指定した場合，VLAN 単位認証（動的）で認証されているすべての Supplicant の認証状態がいったん解除されます。

[関連コマンド]

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic radius-vlan

IEEE802.1X の認証時に RADIUS サーバから送信される VLAN 情報によって，動的な VLAN 割り当てを許可する VLAN を指定します。

［入力形式］

情報の設定

dot1x vlan dynamic radius-vlan <vlan id list>

情報の変更

dot1x vlan dynamic radius-vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

情報の削除

no dot1x vlan dynamic radius-vlan

［入力モード］

(config)

［パラメータ］

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。変更時は設定済みの VLAN を指定された VLAN に置き換えます。指定できる VLAN は MAC VLAN 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
   <vlan id list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。ただし，このコマンドでデフォルト VLAN（VLAN ID=1）は指定できません。

add <vlan id list>

IEEE802.1X 認証設定を適用する VLAN に追加する VLAN を指定します。指定できる VLAN は MAC VLAN 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
   <vlan id list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。ただし，このコマンドでデフォルト VLAN（VLAN ID=1）は指定できません。

remove <vlan id list>

IEEE802.1X 認証設定を適用する VLAN から削除する VLAN を指定します。指定できる VLAN は MAC VLAN 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
   <vlan id list> の指定方法，また，値の設定範囲については「パラメータに指定できる値」を参照してください。ただし，このコマンドでデフォルト VLAN（VLAN ID=1）は指定できません。

［コマンド省略時の動作］

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. すべての IEEE802.1X 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
3. VLAN 単位認証（動的）と VLAN 単位認証（静的）で設定できる最大 VLAN 数は合わせて 1024 です。
4. すべての VLAN 単位認証を設定した VLAN に所属するポートとチャネルグループの合計の最大数は VLAN 単位認証（動的）と VLAN 単位認証（静的）を合わせて 1024 までです。最大数を超える場合，VLAN は設定できません。
5. VLAN が範囲指定の場合，すべての VLAN が設定可能でなければエラーになります。
6. MAC アドレス学習抑止が設定されている VLAN は指定できません。
7. MAC アドレス学習数制限が設定されている VLAN は指定できません。
8. MAC アドレス学習数制限が設定されているインタフェースが所属している VLAN は指定できません。
9. EAPOL フォワーディング機能が設定されている VLAN は指定できません。

[関連コマンド]

vlan

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan enable

switchport mac

dot1x vlan dynamic reauthentication

IEEE802.1X の認証成功後，Supplicant の再認証を有効にするかどうかを設定します。本設定が有効になると，dot1x vlan dynamic timeout reauth-period コマンドで設定する値の周期で再認証用 EAP-Request/Identity を Supplicant に対して送出し，Supplicant の再認証を促します。

［入力形式］

情報の設定
　dot1x vlan dynamic reauthentication

情報の削除
　no dot1x vlan dynamic reauthentication

［入力モード］

```
(config)
```

［パラメータ］

なし

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. すべての IEEE802.1X 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
3. dot1x vlan dynamic ignore-eapol-start コマンドを指定したインタフェースでは no dot1x vlan dynamic reauthentication コマンドで再認証を実施しない設定にすることはできません。

［関連コマンド］

dot1x system-auth-control

dot1x vlan dynamic ignore-eapol-start

dot1x vlan dynamic timeout reauth-period

dot1x vlan dynamic enable

dot1x vlan dynamic supplicant-detection

新規端末検出の動作を指定します。

［入力形式］

情報の設定・変更
dot1x vlan dynamic supplicant-detection {disable | shortcut}

情報の削除
no dot1x vlan dynamic supplicant-detection

［入力モード］

(config)

［パラメータ］

{disable | shortcut}

新規端末検出の動作を指定します。

disable

認証サブモードを端末認証モードに設定した場合に認証済み端末が存在するときは，新規端末検出用 EAP-Request/Identity 送信処理を抑止します。装置負荷低減のための認証シーケンスの省略によって異常動作となる Supplicant を使用している場合に指定してください。
本パラメータを指定した場合，端末側から認証を開始できないタイプの Supplicant でもデータフレームを検出した端末に対しては EAP-Request/Identity を送信して認証開始を促します。

shortcut

新規端末検出用 EAP-Request/Identity 送信処理で，負荷低減のために認証済端末の認証シーケンスを省略します。端末側から認証を開始できないタイプの Supplicant を使用している場合に指定してください。
本パラメータを指定した場合，一部の Supplicant は正常に動作しないで，通信が一時的に停止します。

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
   disable または shortcut

［コマンド省略時の動作］

新規端末検出動作は shortcut 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 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。

3. dot1x vlan dynamic ignore-eapol-start コマンドを指定したインタフェースで dot1x vlan dynamic supplicant-detection コマンドの disable を設定することはできません。

［関連コマンド］

dot1x vlan dynamic ignore-eapol-start

dot1x vlan dynamic enable

dot1x system-auth-control

dot1x vlan dynamic timeout quiet-period

IEEE802.1X の認証失敗後の該当インタフェースの非認証状態保持時間を秒単位で指定します。本時間内は，EAPOL パケットの送出は行わず，かつ，受信 EAPOL パケットを無視し，認証処理は行いません。

［入力形式］

情報の設定・変更

dot1x vlan dynamic timeout quiet-period <seconds>

情報の削除

no dot1x vlan dynamic timeout quiet-period

［入力モード］

(config)

［パラメータ］

<seconds>

非認証状態保持時間を秒単位で指定します。

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

［コマンド省略時の動作］

非認証状態保持時間は 60 秒です。

［通信への影響］

なし

［設定値の反映契機］

認証失敗による非認証状態になったとき

［注意事項］

1. すべての IEEE802.1X 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。

［関連コマンド］

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic timeout reauth-period

IEEE802.1X の認証成功後，Supplicant の再認証を行う周期を秒単位で指定します。本値の周期で再認証用 EAP-Request/Identity を Supplicant に対して送出し，Supplicant の再認証を促します。

［入力形式］

情報の設定・変更

dot1x vlan dynamic timeout reauth-period <seconds>

情報の削除

no dot1x vlan dynamic timeout reauth-period

［入力モード］

(config)

［パラメータ］

<seconds>

Supplicant の再認証を行う周期を秒単位で指定します。

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］

Supplicant の再認証を行う周期は 3600 秒です。

［通信への影響］

なし

［設定値の反映契機］

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき
- 認証済端末が存在しない状態の認証単位で認証端末の認証が成功したとき

［注意事項］

1. すべての IEEE802.1X 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
3. 本コマンドは，dot1x vlan dynamic reauthentication コマンドによって再認証を行う設定にならないと有効になりません。
4. パラメータの設定値は dot1x vlan dynamic timeout tx-period コマンドで設定した値より大きな値を設定してください。

［関連コマンド］

dot1x vlan dynamic timeout tx-period

dot1x vlan dynamic reauthentication

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic timeout server-timeout

認証サーバとの再送を含めた全体の応答待ち時間を秒単位で指定します。

［入力形式］

情報の設定・変更

dot1x vlan dynamic timeout server-timeout <seconds>

情報の削除

no dot1x vlan dynamic timeout server-timeout

［入力モード］

(config)

［パラメータ］

<seconds>

応答待ち時間を秒単位で指定します。

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

［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 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。

［関連コマンド］

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic timeout supp-timeout

Supplicant へ送出する EAP-Request に対して，Supplicant からの応答待ち時間を秒単位で指定します。指定秒応答がない場合，EAP-Request の再送を行います。

［入力形式］

情報の設定・変更

dot1x vlan dynamic timeout supp-timeout <seconds>

情報の削除

no dot1x vlan dynamic timeout supp-timeout

［入力モード］

(config)

［パラメータ］

<seconds>

Supplicant からの応答待ち時間を秒単位で指定します。

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

［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 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。

［関連コマンド］

dot1x system-auth-control

dot1x vlan dynamic max-req

dot1x vlan dynamic enable

dot1x vlan dynamic timeout tx-period

IEEE802.1X の認証有効時の，EAP-Request/Identity の送出間隔を秒単位で指定します。

［入力形式］

情報の設定・変更

dot1x vlan dynamic timeout tx-period <seconds>

情報の削除

no dot1x vlan dynamic timeout tx-period

［入力モード］

(config)

［パラメータ］

<seconds>

EAP-Request/Identity の送出間隔を秒単位で指定します。

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

［コマンド省略時の動作］

EAP-Request/Identity の送出間隔は 30 秒です。

［通信への影響］

なし

［設定値の反映契機］

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき

［注意事項］

1. すべての IEEE802.1X 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. dot1x vlan dynamic enable コマンドが設定されていないと本コマンドは有効になりません。
3. パラメータの設定値は，dot1x vlan dynamic timeout reauth-period コマンドで設定した値より小さな値を設定してください。

［関連コマンド］

dot1x system-auth-control

dot1x vlan dynamic timeout reauth-period

dot1x vlan dynamic enable

dot1x vlan enable

IEEE802.1X VLAN 単位認証（静的）を有効にします。

［入力形式］

情報の設定
　dot1x vlan <vlan id list> enable

情報の削除
　no dot1x vlan <vlan id list> enable

［入力モード］

(config)

［パラメータ］

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. すべての IEEE802.1X 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. 本コマンドが設定されていないと，VLAN 単位認証（静的）を使用できません。
3. VLAN が範囲指定の場合，すべての VLAN が設定可能でなければエラーになります。
4. VLAN に所属しているポートまたはチャネルグループにポート単位認証が設定されている VLAN は指定できません。
5. VLAN 単位認証（動的）と VLAN 単位認証（静的）で設定できる最大 VLAN 数は合わせて 1024 までです。
6. すべての VLAN 単位認証を設定した VLAN に所属するポートとチャネルグループの合計の最大数は VLAN 単位認証（動的）と VLAN 単位認証（静的）を合わせて 1024 までです。最大数を超える場合，VLAN は設定できません。
7. MAC ポートまたはプロトコルポートのネイティブ VLAN に設定されている VLAN は指定できません。
8. トンネリングポートが所属している VLAN は指定できません。
9. MAC アドレス学習抑止が設定されている VLAN は指定できません。

10. MAC アドレス学習数制限が設定されている VLAN は指定できません。
11. MAC アドレス学習数制限が設定されているインタフェースが所属している VLAN は指定できません。
12. EAPOL フォワーディング機能が設定されている VLAN は指定できません。

［関連コマンド］

vlan

dot1x system-auth-control

dot1x port-control

dot1x vlan dynamic radius-vlan

switchport mode

switchport access

dot1x vlan ignore-eapol-start

Supplicant からの EAPOL-Start 受信時に，EAP-Request/Identity を発行しないよう指定します。

［入力形式］

情報の設定

dot1x vlan <vlan id list> ignore-eapol-start

情報の削除

no dot1x vlan <vlan id list> ignore-eapol-start

［入力モード］

(config)

［パラメータ］

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. すべての IEEE802.1X 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。
3. 本コマンドは dot1x vlan <vlan id list> reauthentication コマンドが設定されていて，かつ dot1x vlan <vlan id list> supplicant-detection コマンドの disable の指定がないインタフェースにだけ設定できます。
4. dot1x vlan<vlan id list> supplicant-detection コマンドの disable を指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。
5. 本コマンドを指定したインタフェースでは，no dot1x vlan <vlan id list> reauthentication コマンドで再認証を実施しないように設定することはできません。

［関連コマンド］

dot1x vlan reauthentication

dot1x vlan supplicant-detection

dot1x system-auth-control

dot1x vlan enable

dot1x vlan max-req

supp-timeout 値を超えた際の EAP-Request 再送の最大回数を指定します。再送回数が本値を超えた場合，認証失敗と判定します。

[入力形式]

情報の設定・変更

dot1x vlan <vlan id list> max-req <count>

情報の削除

no dot1x vlan <vlan id list> max-req

[入力モード]

(config)

[パラメータ]

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

<count>

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

[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 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan timeout supp-timeout

dot1x vlan enable

dot1x vlan max-supplicant

指定 VLAN インタフェースに接続可能な最大端末数を指定します。本値を超えて端末を接続しようとした場合，認証を行わないで端末接続数を制限できます。

[入力形式]

情報の設定・変更

dot1x vlan <vlan id list> max-supplicant <clients>

情報の削除

no dot1x vlan <vlan id list> max-supplicant

[入力モード]

(config)

[パラメータ]

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

<clients>

指定 VLAN インタフェースに接続可能な最大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
   1 ～ 256

[コマンド省略時の動作]

端末接続数は 256 です。

[通信への影響]

現在指定インタフェースで認証されている端末数よりも小さい値を指定した場合，指定インタフェースで認証されているすべての Supplicant の認証状態が解除されます。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 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。
3. 現在 VLAN 単位認証（静的）で認証されている端末数よりも小さい値を指定した場合，VLAN 単位認証（静的）で認証されているすべての Supplicant の認証状態がいったん解除されます。

［関連コマンド］

dot1x system-auth-control

dot1x vlan enable

dot1x vlan reauthentication

IEEE802.1X の認証成功後，Supplicant の再認証を有効にするかどうかを設定します。本設定が有効になると，dot1x vlan <vlan id list> timeout reauth-period コマンドで設定する値の周期で再認証用 EAP-Request/Identity を Supplicant に対して送出し，Supplicant の再認証を促します。

［入力形式］

情報の設定

dot1x vlan <vlan id list> reauthentication

情報の削除

no dot1x vlan <vlan id list> reauthentication

［入力モード］

(config)

［パラメータ］

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

［コマンド省略時の動作］

なし

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. すべての IEEE802.1X 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。
3. dot1x vlan <vlan id list> ignore-eapol-start コマンドを指定した VLAN インタフェースでは no dot1x vlan <vlan id list> reauthentication コマンドで再認証を実施しない設定にすることはできません。

［関連コマンド］

dot1x system-auth-control

dot1x vlan ignore-eapol-start

dot1x vlan timeout reauth-period

dot1x vlan enable

dot1x vlan supplicant-detection

新規端末検出の動作を指定します。

［入力形式］

情報の設定・変更

dot1x vlan <vlan id list> supplicant-detection {disable | shortcut}

情報の削除

no dot1x vlan <vlan id list> supplicant-detection

［入力モード］

(config)

［パラメータ］

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

{disable | shortcut}

新規端末検出の動作を指定します。

disable

認証サブモードを端末認証モードに設定した場合に認証済み端末が存在するときは，新規端末検出用 EAP-Request/Identity 送信処理を抑止します。装置負荷低減のための認証シーケンスの省略によって異常動作となる Supplicant を使用している場合に指定してください。

本パラメータを指定した場合，端末側から認証を開始できないタイプの Supplicant でもデータフレームを検出した端末に対しては EAP-Request/Identity を送信して認証開始を促します。

shortcut

新規端末検出用 EAP-Request/Identity 送信処理で，負荷低減のために認証済端末の認証シーケンスを省略します。端末側から認証を開始できないタイプの Supplicant を使用している場合に指定してください。

本パラメータを指定した場合，一部の Supplicant は正常に動作しないで，通信が一時的に停止します。

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
   disable または shortcut

［コマンド省略時の動作］

新規端末検出動作は shortcut 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 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。
3. dot1x vlan <vlan id list> ignore-eapol-start コマンドを指定したインタフェースで dot1x vlan <vlan id list> supplicant-detection コマンドの disable を設定することはできません。

[関連コマンド]

dot1x vlan ignore-eapol-start

dot1x system-auth-control

dot1x vlan enable

dot1x vlan timeout quiet-period

IEEE802.1X の認証失敗後の該当 VLAN インタフェースの非認証状態保持時間を秒単位で指定します。本時間内は，EAPOL パケットの送出は行わず，かつ，受信 EAPOL パケットを無視し，認証処理は行いません。

[入力形式]

情報の設定・変更

dot1x vlan <vlan id list> timeout quiet-period <seconds>

情報の削除

no dot1x vlan <vlan id list> timeout quiet-period

[入力モード]

(config)

[パラメータ]

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

<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

[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 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan enable

dot1x vlan timeout reauth-period

IEEE802.1X の認証成功後，Supplicant の再認証を行う周期を秒単位で指定します。本値の周期で再認証用 EAP-Request/Identity を Supplicant に対して送出し，Supplicant の再認証を促します。

[入力形式]

情報の設定・変更

dot1x vlan <vlan id list> timeout reauth-period <seconds>

情報の削除

no dot1x vlan <vlan id list> timeout reauth-period

[入力モード]

(config)

[パラメータ]

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

<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

[コマンド省略時の動作]

Supplicant の再認証を行う周期は 3600 秒になります。

[通信への影響]

なし

[設定値の反映契機]

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき
- 認証済端末が存在しない状態の認証単位で認証端末の認証が成功したとき

[注意事項]

1. すべての IEEE802.1X 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。
3. 本コマンドは，dot1x vlan <vlan id list> 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。

4. パラメータの設定値は dot1x vlan <vlan id list> timeout tx-period コマンドで設定した値より大きな値を設定してください。

［関連コマンド］

dot1x vlan timeout tx-period

dot1x vlan reauthentication

dot1x system-auth-control

dot1x vlan enable

dot1x vlan timeout server-timeout

認証サーバとの再送を含めた全体の応答待ち時間を秒単位で指定します。

[入力形式]

情報の設定・変更

dot1x vlan <vlan id list> timeout server-timeout <seconds>

情報の削除

no dot1x vlan <vlan id list> timeout server-timeout

[入力モード]

(config)

[パラメータ]

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

<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

[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 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan enable

dot1x vlan timeout supp-timeout

Supplicant へ送出する EAP-Request に対して，Supplicant からの応答待ち時間を秒単位で指定します。指定秒応答がない場合，EAP-Request の再送を行います。

[入力形式]

情報の設定・変更

dot1x vlan <vlan id list> timeout supp-timeout <seconds>

情報の削除

no dot1x vlan <vlan id list> timeout supp-timeout

[入力モード]

(config)

[パラメータ]

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

<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

[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 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。

[関連コマンド]

dot1x system-auth-control

dot1x vlan max-req

dot1x vlan enable

dot1x vlan 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 vlan <vlan id list> timeout tx-period <seconds>

情報の削除

no dot1x vlan <vlan id list> timeout tx-period

［入力モード］

(config)

［パラメータ］

<vlan id list>

IEEE802.1X 認証設定を適用する VLAN の VLAN ID を指定します。本装置に未設定の VLAN は指定できません。

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

<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

［コマンド省略時の動作］

EAP-Request/Identity の送出間隔は 30 秒です。

［通信への影響］

なし

［設定値の反映契機］

- 現在動作中のタイマがタイムアウトし，タイマ値が 0 になったとき
- 運用コマンド clear dot1x auth-state を実行し，認証単位または装置単位での認証解除を実施したとき

［注意事項］

1. すべての IEEE802.1X 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. dot1x vlan <vlan id list> enable コマンドが設定されていないと本コマンドは有効になりません。
3. パラメータの設定値は，dot1x vlan <vlan id list> 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 vlan timeout reauth-period

dot1x system-auth-control

dot1x vlan enable

10 Web 認証

コンフィグレーションコマンドと動作モードの対応
aaa accounting web-authentication default start-stop group radius
aaa authentication web-authentication default group radius
web-authentication auto-logout
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 max-user
web-authentication port
web-authentication redirect-mode
web-authentication redirect-vlan
web-authentication static-vlan max-user
web-authentication system-auth-control
web-authentication vlan
web-authentication web-port

コンフィグレーションコマンドと動作モードの対応

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 認証の動作モードを次の表に示します。

表 10-1　コンフィグレーションコマンドと Web 認証の動作モード

コマンド名	Web 認証の動作モード		
	固定 VLAN モード	ダイナミック VLAN モード	レガシーモード
aaa accounting web-authentication default start-stop group radius	○	○	○
aaa authentication web-authentication default group radius	○	○	○
authentication ip access-group	○	○	－
web-authentication auto-logout	－	○	○
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 max-user	－	○	○
web-authentication port	○	○	×
web-authentication redirect-mode	－	○	－
web-authentication redirect-vlan	－	○	－
web-authentication static-vlan max-user	○	－	－
web-authentication system-auth-control	○	○	○
web-authentication vlan	×	×	○
web-authentication web-port	○	○	○

（凡例）
○：コマンドが設定でき，設定内容が反映されます。
－：コマンドは設定できますが，設定内容は反映されません。
×：コマンドが設定できません。

aaa accounting web-authentication default start-stop group radius

Web 認証での認証結果をアカウンティングサーバに通知します。

[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]

なし

[コマンド省略時の動作]

本設定が行われないと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]

なし

[関連コマンド]

web-authentication system-auth-control

web-authentication max-timer

web-authentication max-user

web-authentication vlan

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa authentication web-authentication default group radius

Web 認証機能での RADIUS サーバの使用有無を設定します。

[入力形式]

情報の設定
　aaa authentication web-authentication default group radius

情報の削除
　no aaa authentication web-authentication default

[入力モード]

```
(config)
```

[パラメータ]

なし

[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]

全ユーザの認証が解除されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを入力する場合には，RADIUS サーバの認証設定が別途必要になります。

[関連コマンド]

web-authentication system-auth-control

web-authentication max-timer

web-authentication max-user

web-authentication vlan

web-authentication auto-logout

aaa accounting web-authentication default start-stop group radius

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が一定時間使用されていない状態を検出して認証解除を行う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］

MAC アドレステーブルから Web 認証で認証中の MAC アドレスが一定時間使用されていない状態が検出された場合に，認証が解除されます。

［通信への影響］

本コマンド実行時は，MAC アドレステーブルから Web 認証で認証中の MAC アドレスが一定時間使用されていない状態が検出された場合でも，認証を解除しません。

［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］

なし

［関連コマンド］

web-authentication system-auth-control

mac-address-table aging-time

web-authentication ip address

Web 認証専用の IP アドレスを設定します。

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。

なお，レガシーモード以外では必ず設定してください。

また，Web 認証専用の IP アドレスに対応する FQDN（Fully Qualified Domain Name）を設定します。

[入力形式]

情報の設定・変更

web-authentication ip address <authentication address> [fqdn <fqdn>]

情報の削除

no web-authentication ip address

[入力モード]

(config)

[パラメータ]

<authentication 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
   <authentication address> に IPv4 アドレス（ドット記法）を指定します。
   次に示す値は設定できません。
   ・ループバックインタフェースに設定した IP アドレス
   ・各インタフェースに設定したサブネットに含まれる IP アドレス

fqdn <fqdn>

Web 認証専用 IP アドレスに対応する FQDN を指定します。

1. 本パラメータ省略時の初期値
   FQDN が設定されていないものとします。
2. 値の設定範囲
   1 ～ 255 文字の文字列をダブルクォート（"）で囲んで指定します。入力可能な文字は，英数字，ピリオド（.）およびハイフン（-）です。だたし，先頭文字は英数字だけ使用できます。なお，文字列をダブルクォート（"）で囲まなくても設定できます。

[コマンド省略時の動作]

Web 認証専用の IP アドレスは設定されません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，運用コマンド restart web-authentication web-server による Web サーバの再起動後に反

映されます。

[注意事項]

1. 本コマンドで設定した IP アドレスは，装置内での Web 認証アクセス専用として使用されるため，装置外には送出されません。
2. 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。
3. 本コマンドで設定および削除を行った場合は，直ちに運用コマンド restart web-authentication web-server で Web サーバの再起動を行ってください。
4. レガシーモードの状態（web-authentication port コマンドが一つも設定されていない状態）で，本コマンド設定後に web-authentication port コマンドを設定した場合は，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。
   また，本コマンドの削除前にレガシーモードの状態（web-authentication port コマンドをすべて削除した状態）だった場合も，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。

[関連コマンド]

web-authentication system-auth-control

web-authentication port

web-authentication jump-url

認証成功画面表示後に自動的に表示する URL を指定します。

[入力形式]

情報の設定・変更
　web-authentication jump-url <url>

情報の削除
　no web-authentication jump-url

[入力モード]

(config)

[パラメータ]

<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:// ～ ”）から指定してください（下記設定例参照）。

1. 本パラ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，スペースを除く英数字と特殊文字です。入力文字列に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。
   （設定例）
   (config)# web-authentication jump-url "http://www.example.com/"

[コマンド省略時の動作]

認証成功後の表示画面は，認証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. 運用コマンド set web-authentication html-files で認証成功画面を入れ替える際，入れ替える認証成功画面ファイル（loginOK.html）上に認証成功後のジャンプ先 URL のタグ（<!--Redirect_URL-->）を記載すると，認証成功後に設定した URL へ自動的にアクセスされます。

[関連コマンド]

web-authentication system-auth-control

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]

なし

[関連コマンド]

web-authentication system-auth-control

logging event-kind

logging email-event-kind

web-authentication logout ping tos-windows

Web 認証で固定 VLAN モードによる運用を行う場合，認証済み端末から特殊パケット（ping）を受信したときに該当する MAC アドレスの認証状態を解除する特殊パケットの 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>

Web 認証用の特殊パケットの 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］

特殊パケットの TOS 値は 1 で設定されます。

［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］

なし

［関連コマンド］

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout ping ttl

web-authentication logout ping ttl

Web 認証で固定 VLAN モードによる運用を行う場合，認証済み端末から特殊パケット（ping）を受信したときに該当する MAC アドレスの認証状態を解除する特殊パケットの 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>

Web 認証用の特殊パケットの 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］

特殊パケットの TTL 値は 1 で設定されます。

［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］

なし

［関連コマンド］

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout ping tos-windows

web-authentication logout polling count

Web 認証で固定 VLAN モードによる運用を行う場合，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パケットの応答で，無応答を検出時に再送する送信回数の設定を行います。

[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>

監視用パケット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]

監視用パケットの再送が最大 3 回実施されます。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，次の送出間隔から運用に反映されます。

[注意事項]

1. 本コマンドは，固定 VLAN モード設定時に有効です。
2. ログアウト監視機能による周期監視より先に，対象ポートのリングダウンを検出した場合は，周期監視は停止されログアウトが実施されます。
3. 認証最大時間の設定時間に達したら，該当 VLAN の監視は停止されます。
4. 無応答検出時の再送回数を最大に設定した場合に，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パケットの送信が多くなるため，装置に負荷をかけることになります。
   ポーリング間隔の目安として，以下の条件で設定願います。

   ＜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

   無応答検出時の再送処理が，全体のポーリング間隔時間を超えない値で設定してください（1 回のポーリング間隔内で再送処理を完結させるため）。

   (1)：web-authentication logout polling interval

   (2)：web-authentication logout polling retry-interval

   (3)：web-authentication logout polling count

- 認証端末数が約 2000 台を超える場合，監視用パケットの送出間隔に 300 秒より小さい値を設定しないでください。
- 認証端末数が約 2000 台以下の場合で，監視用パケットの送出間隔に 300 秒より小さい値を設定する場合は，再送間隔と再送回数はデフォルト値を使用してください。

［関連コマンド］

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout polling enable

web-authentication logout polling interval

web-authentication logout polling retry-interval

web-authentication logout polling enable

Web 認証で固定 VLAN モードによる運用を行う場合に，認証済みの端末が接続されているか周期的にチェックし，未接続を検出したときに強制ログアウトの動作をする設定を行います。

no web-authentication logout polling enable コマンドで，周期チェックによる強制ログアウト設定を無効にした場合は，一定周期による監視は行いません。

[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，次に示す一定周期での監視を行います。

ポーリング間隔：
　web-authentication logout polling interval コマンドで設定した間隔。省略時は 300 秒。

再送間隔：
　web-authentication logout polling retry-interval コマンドで設定した間隔。省略時は 1 秒。

再送回数：
　web-authentication logout polling count コマンドで設定した回数。省略時は 3 回。

[通信への影響]

なし

[設定値の反映契機]

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，固定 VLAN モード設定時に有効です。
2. 該当端末のポートがリンクダウンした場合は，対象端末の監視は停止され，ポートリンクダウンによるログアウトが実施されます。
3. 認証最大時間の設定時間（web-authentication max-timer コマンド）に達したら，該当端末の監視は停止して，ログアウトが実施されます。
4. 送出間隔の時間（web-authentication logout polling interval コマンド）を最小に設定した場合，認証済みユーザ数に比例して監視用パケットの送出が多くなるため，装置に負荷をかけることになります。また，無応答検出時の再送回数（web-authentication logout polling count コマンド）を最大値，再送間隔時間（web-authentication logout polling retry-interval コマンド）を最小値に設定すると，同様

に装置に負荷がかかります。
ポーリング間隔の目安として，次に示す条件で設定願います。

＜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
無応答検出時の再送処理が，全体のポーリング間隔時間を超えない値で設定してください（1 回のポーリング間隔内で再送処理を完結させるためです）。
(1)：web-authentication logout polling interval
(2)：web-authentication logout polling retry-interval
(3)：web-authentication logout polling count

- 認証端末数が約 2000 台を超える場合，監視用パケットの送出間隔に 300 秒より小さい値を設定しないでください。
- 認証端末数が約 2000 台以下の場合で，監視用パケットの送出間隔に 300 秒より小さい値を設定する場合は，再送間隔と再送回数はデフォルト値を使用してください。

[関連コマンド]

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout polling interval

web-authentication logout polling retry-interval

web-authentication logout polling count

web-authentication logout polling interval

Web 認証で固定 VLAN モードによる運用を行う場合，認証済みの端末が接続されているか周期的にチェックする監視用パケットの送出間隔の設定を行います。

[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>

監視用パケットの送出間隔を設定します。
設定は装置単位となります。

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
   60 ～ 86400（秒）

[コマンド省略時の動作]

ログアウト監視コマンド（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，監視用パケットが 300 秒周期で送出されます。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，次の送出間隔から運用に反映されます。

[注意事項]

1. 本コマンドは，固定 VLAN モード設定時に有効です。
2. ログアウト監視機能による周期監視より先に，対象ポートのリングダウンを検出した場合は，周期監視は停止されログアウトが実施されます。
3. 認証最大時間の設定時間に達したら，該当端末の監視は停止されます。
4. 送信間隔の時間を最小に設定した場合，認証済みユーザ数に比例して監視用パケットの送出が多くなるため，装置に負荷をか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願います。

   ＜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
   無応答検出時の再送処理が，全体のポーリング間隔時間を超えない値で設定してください（1 回のポーリング間隔内で再送処理を完結させるためです）。
   (1)：web-authentication logout polling interval

(2)：web-authentication logout polling retry-interval
(3)：web-authentication logout polling count

- 認証端末数が約 2000 台を超える場合，監視用パケットの送出間隔に 300 秒より小さい値を設定しないでください。
- 認証端末数が約 2000 台以下の場合で，監視用パケットの送出間隔に 300 秒より小さい値を設定する場合は，再送間隔と再送回数はデフォルト値を使用してください。

［関連コマンド］

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout polling enable

web-authentication logout polling retry-interval

web-authentication logout polling count

web-authentication logout polling retry-interval

Web 認証で固定 VLAN モードによる運用を行う場合，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パケットの応答で，無応答検出時に再送する送信間隔の設定を行います。

[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>

監視用パケットの再送送出間隔を設定します。

設定は装置単位となります。

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

[コマンド省略時の動作]

監視用パケットの再送は 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，次の送出間隔から運用に反映されます。

[注意事項]

1. 本コマンドは，固定 VLAN モード設定時に有効です。
2. ログアウト監視機能による周期監視より先に，対象ポートのリングダウンを検出した場合は，周期監視は停止されログアウトが実施されます。
3. 認証最大時間の設定時間に達したら，該当端末の監視は停止されます。
4. 再送送信間隔の時間を最小に設定した場合，認証済みユーザ数に比例して監視用パケットの送出が多くなるため，装置に負荷をか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願います。

   ＜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

   無応答検出時の再送処理が，全体のポーリング間隔時間を超えない値で設定してください（1 回のポーリング間隔内で再送処理を完結させるためです）。

   (1)：web-authentication logout polling interval

   (2)：web-authentication logout polling retry-interval

(3)：web-authentication logout polling count

- 認証端末数が約 2000 台を超える場合，監視用パケットの送出間隔に 300 秒より小さい値を設定しないでください。
- 認証端末数が約 2000 台以下の場合で，監視用パケットの送出間隔に 300 秒より小さい値を設定する場合は，再送間隔と再送回数はデフォルト値を使用してください。

［関連コマンド］

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout polling enable

web-authentication logout polling interval

web-authentication logout polling count

web-authentication max-timer

Web 認証での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>

情報の削除

no web-authentication max-timer

[入力モード]

(config)

[パラメータ]

<minutes>

Web 認証システムで，ユーザが認証を行う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，自動的に認証が解除されます。なお，設定された時間が経過してから 1 分以内で認証解除を行います。

「infinity」と指定した場合は，最大接続時間を無限とし，最大接続時間による認証解除を行いません。

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
   10 ～ 1440，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. 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コンフィグレーション設定が有効になります。
2. Web 認証での接続時間は，装置の時刻を用いて管理しています。そのため，運用コマンド set clock で日時を変更した場合，接続時間に影響が出ます。

   （例）

   3 時間後の時刻に値を変更した場合，接続時間が 3 時間経過した状態になってしまいます。また，逆に 3 時間前の時刻に値を変更した場合，接続時間が 3 時間延長されてしまいます。

[関連コマンド]

web-authentication system-auth-control

web-authentication max-user

web-authentication vlan

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa accounting web-authentication default start-stop group radius

web-authentication max-user

Web 認証機能のダイナミック VLAN モードおよびレガシーモードで認証できる最大ユーザ数を設定します。

[入力形式]

情報の設定・変更

web-authentication max-user <count>

情報の削除

no web-authentication max-user

[入力モード]

(config)

[パラメータ]

<count>

Web 認証で，ユーザ認証を行う最大数を設定します。設定した数を超えてのユーザ認証はできません。

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
   1 ～ 4096

[コマンド省略時の動作]

認証可能な最大ユーザ数は，4096 ユーザになります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本設定を行った場合，現在認証中のユーザはそのままですが，次回ログイン時からコンフィグレーション設定が有効となります。

[関連コマンド]

web-authentication system-auth-control

web-authentication max-timer

web-authentication vlan

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa accounting web-authentication default start-stop group radius

web-authentication port

指定されたポートに対して，Web 認証を設定します。

アクセスポートおよびトランクポートに設定された場合は，固定 VLAN モードとなります。また，MAC VLAN が設定されたポートの場合は，ダイナミック VLAN モードとなります。

[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]

本コマンドが一つも設定されていない場合は，通常の動作となります。

[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. 本コマンドは web-authentication vlan コマンドが設定されている状態では設定できません。
2. 本コマンドで，他の認証対象ポートに固定 VLAN モードが設定されている状態では，該当ポートにダイナミック VLAN モードの設定はできません。また，他の認証ポートにダイナミック VLAN モードが設定されている状態では，該当ポートに固定 VLAN モードの設定はできません。
3. レガシーモードの状態で，本コマンドを設定する前に web-authentication ip address コマンドを設定した場合は，本コマンド設定後に運用コマンド restart web-authentication web-server で Web サーバを再起動してください。
   また，本コマンドを削除し，レガシーモードの状態（一つも本コマンドの設定がなくなった状態）で，web-authentication ip address コマンドが設定されている場合は，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。

[関連コマンド]

web-authentication ip address

web-authentication system-auth-control

web-authentication redirect-mode

Web 認証での URL リダイレクト機能動作時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}

http

URL リダイレクト機能有効時，http によるログイン画面が表示されます。

https

URL リダイレクト機能有効時，https によるログイン画面が表示されます。

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
   http または https

［コマンド省略時の動作］

本コマンド省略時は，https でログイン画面を表示します。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，運用コマンド restart web-authentication web-server による Web サーバの再起動後に反映されます。

［注意事項］

1. web-authentication redirect-vlan コマンドで URL リダイレクト実施 VLAN の設定がないと，本設定は有効になりません。

［関連コマンド］

web-authentication port

web-authentication redirect-vlan

web-authentication system-auth-control

web-authentication redirect-vlan

ダイナミック VLAN モードを設定する MAC ポートのネイティブ VLAN を指定します。URL リダイレクト機能を使用する際には本設定が必要です。

[入力形式]

情報の設定・変更

web-authentication redirect-vlan <vlan id list>

情報の削除

no web-authentication redirect-vlan

[入力モード]

(config)

[パラメータ]

<vlan id list>

ダイナミック VLAN モードで使用する認証前 VLAN を指定します。変更時は，設定済みの VLAN を指定された VLAN に置き換えます。MAC VLAN は指定できません。

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

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，運用コマンド restart web-authentication web-server で Web サーバを再起動したあとに反映されます。

[注意事項]

1. 本コマンドで指定した認証前 VLAN では，http/https ポートの通信が制限されます。
2. 本コマンドで指定した認証前 VLAN を，ダイナミック VLAN モードを設定した MAC ポートのネイティブ VLAN に設定してください。

[関連コマンド]

switchport mac native vlan

web-authentication static-vlan max-user

Web 認証機能を固定 VLAN モードで認証できる，最大ユーザ数を設定します。

［入力形式］

情報の設定・変更

web-authentication static-vlan max-user <count>

情報の削除

no web-authentication static-vlan max-user

［入力モード］

(config)

［パラメータ］

<count>

Web 認証で，固定 VLAN モードでユーザ認証を行う最大数を設定します。

設定した数を超えてのユーザ認証はできません。

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
   1 ～ 4096

［コマンド省略時の動作］

認証可能な最大ユーザ数：4096 ユーザ

［通信への影響］

なし

［設定値の反映契機］

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，現在認証中のユーザはそのままですが，次回ログイン時からコンフィグレーションの設定が有効となります。

［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 count

web-authentication system-auth-control

Web 認証デーモンの起動を行い，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 認証デーモンを停止します。

［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，認証済みユーザの認証が解除されます。

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. 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。
2. 認証 VLAN が設定されている場合，本コマンドは設定できません。
3. no web-authentication system-auth-control で Web 認証を停止したあと，すぐに web-authentication system-auth-control で Web 認証を起動する場合は，10 秒以上の時間間隔をおいてから実行してください。

［関連コマンド］

web-authentication max-timer

web-authentication max-user

web-authentication vlan

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa accounting web-authentication default start-stop group radius

web-authentication vlan

Web 認証のレガシーモードで VLAN 切り替えを許可する VLAN ID を指定します。

本コマンドで VLAN ID が設定されていない場合は，認証後の VLAN 切り替えが行われません。

[入力形式]

情報の設定・変更
　web-authentication vlan <vlan id list>

情報の削除
　no web-authentication vlan <vlan id list>

[入力モード]

(config)

[パラメータ]

<vlan id list>

Web 認証でユーザ認証後に切り替える MAC VLAN の VLAN リストを指定します。

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
   <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，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]

認証後の VLAN 切り替えが行われません。

[通信への影響]

本コマンドで VLAN を削除した場合，削除した VLAN で登録をしていたユーザの認証が解除されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 指定されたすべての VLAN ID は，MAC VLAN で設定されている必要があります。
2. 本コマンドは web-authentication port コマンドが設定されている状態では設定できません。

[関連コマンド]

web-authentication system-auth-control

web-authentication max-timer

web-authentication max-user

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa accounting web-authentication default start-stop group radius

web-authentication web-port

Web 認証用の TCP ポート番号を任意のポート番号に追加します。

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追加指定できます。レガシーモード，ダイナミック VLAN モード，固定 VLAN モードのどのモードでも使用できます。

なお，固定 VLAN モードおよびダイナミック VLAN モードで，認証対象ポートに AX-Config-Master を接続する場合は，OAN が使用するポート番号（https の 832 と 9698）を指定してください。

［入力形式］

情報の設定・変更

web-authentication web-port {http | https} <port> [<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 | https}

http

http 用の TCP ポート番号を追加します。

https

https 用の TCP ポート番号を追加します。

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
   http または https

<port>

追加する 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
   832，1024 ～ 65535

［コマンド省略時の動作］

次に示す初期値のポート番号によって通信されます。

- 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，運用コマンド restart web-authentication web-server による Web サーバの再起動後に反映されます。

[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。
2. OAN と共存する場合，OAN が使用するポート番号（832 と 9698）は，Web 認証のログイン操作およびログアウト操作に使用できません。
3. 本コマンドで設定および削除を行った場合は，直ちに運用コマンド restart web-authentication web-server で Web サーバの再起動を行ってください。

[関連コマンド]

web-authentication system-auth-control

web-authentication vlan

web-authentication port

restart web-authentication

11 MAC 認証

コンフィグレーションコマンドと動作モードの対応
aaa accounting mac-authentication default start-stop group radius
aaa authentication mac-authentication default group radius
mac-authentication auth-interval-timer
mac-authentication auto-logout
mac-authentication dynamic-vlan max-user
mac-authentication logging enable
mac-authentication max-timer
mac-authentication password
mac-authentication port
mac-authentication radius-server host
mac-authentication static-vlan max-user
mac-authentication system-auth-control
mac-authentication vlan-check

コンフィグレーションコマンドと動作モードの対応

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 認証の動作モードを次の表に示します。

表 11-1　コンフィグレーションコマンドと MAC 認証の動作モード

コマンド名	MAC 認証の動作モード	
	固定 VLAN モード	ダイナミック VLAN モード
aaa accounting mac-authentication default start-stop group radius	○	○
aaa authentication mac-authentication default group radius	○	○
authentication ip access-group	○	○
mac-authentication auth-interval-timer	○	○
mac-authentication auto-logout	○	○
mac-authentication dynamic-vlan max-user	―	○
mac-authentication logging enable	○	○
mac-authentication max-timer	○	○
mac-authentication password	○	○
mac-authentication port	○	○
mac-authentication radius-server host	○	○
mac-authentication static-vlan max-user	○	―
mac-authentication system-auth-control	○	○
mac-authentication vlan-check	○	―

（凡例）
○：コマンドが設定でき，設定内容が反映されます。
―：コマンドは設定できますが，設定内容は反映されません。

aaa accounting mac-authentication default start-stop group radius

MAC 認証での認証結果をアカウンティングサーバに通知します。

[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]

なし

[コマンド省略時の動作]

本設定が行われないと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]

なし

[関連コマンド]

mac-authentication system-auth-control

mac-authentication port

mac-authentication radius-server host

aaa authentication mac-authentication default group radius

radius-server host

aaa authentication mac-authentication default group radius

MAC 認証機能で RADIUS サーバの使用有無を設定します。

[入力形式]

情報の設定
　aaa authentication mac-authentication default group radius

情報の削除
　no aaa authentication mac-authentication default

[入力モード]

```
(config)
```

[パラメータ]

なし

[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]

すべての認証が解除されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定する場合は，RADIUS サーバの認証設定が別途必要になります。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication port

mac-authentication radius-server host

radius-server host

mac-authentication auth-interval-timer

MAC 認証で認証失敗後の MAC アドレスに対し，次の認証処理が行われるまでの時間間隔を設定します。

［入力形式］

情報の設定・変更

mac-authentication auth-interval-timer <minutes>

情報の削除

no mac-authentication auth-interval-timer

［入力モード］

(config)

［パラメータ］

<minutes>

認証失敗後に次の認証が行われるまでの時間間隔の設定を分単位で行います。
なお，設定された時間が経過してから 1 分以内で次の認証処理を開始します。

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
   1 ～ 1440

［コマンド省略時の動作］

次に認証処理されるまでの時間間隔がデフォルトの 5 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. 時間の設定・変更を行った場合，現在認証中のものに対しては前設定を有効とし，次の認証処理からコンフィグレーションの設定が有効になります。
2. MAC 認証での接続時間は，装置の時刻を用いて管理しています。そのため，運用コマンド set clock で日時を変更した場合，設定した時間に影響が出ます。

   （例）

   3 時間後の時刻に値を変更した場合，設定した時間から 3 時間経過した状態になってしまいます。
   また，逆に 3 時間前の時刻に値を変更した場合，設定した時間から 3 時間延長されてしまいます。

［関連コマンド］

mac-authentication system-auth-control

mac-authentication port

mac-authentication auto-logout

no mac-authentication auto-logout コマンドで，MAC 認証の MAC アドレスが一定時間使用されていない状態を検出して認証解除を行う設定を無効にします。

自動認証解除を無効にした場合は，MAC アドレステーブルから MAC 認証で認証中の MAC アドレスが使用されていないことが検出されたときでも，自動的に認証が解除されません。

［入力形式］

情報の設定
　no mac-authentication auto-logout

情報の削除
　mac-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］

MAC アドレステーブルから MAC 認証で認証中の MAC アドレスが一定時間使用されていない状態が検出された場合，認証が解除されます。

［通信への影響］

本コマンド実行時は，MAC アドレステーブルから MAC 認証で認証中の MAC アドレスが一定時間使用されていない状態が検出された場合でも，認証状態が解除されません。

［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. MAC 認証で認証中の MAC アドレスで，未アクセス状態検出での認証解除の設定が有効な場合（デフォルト時，または本コマンド削除時），MAC アドレステーブルのエージング時間経過後に認証が解除されます。

［関連コマンド］

max-authentication system-auth-control

mac-address-table aging-time

mac-authentication dynamic-vlan max-user

MAC 認証のダイナミック VLAN モードで認証できる最大 MAC アドレス数を設定します。

［入力形式］

情報の設定・変更

mac-authentication dynamic-vlan max-user <count>

情報の削除

no mac-authentication dynamic-vlan max-user

［入力モード］

(config)

［パラメータ］

<count>

MAC 認証のダイナミック VLAN モードで，認証を行う最大数の設定を行います。設定した数を超えての認証はできません。

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
   1 ～ 4096

［コマンド省略時の動作］

認証可能な最大認証数：

4096

［通信への影響］

なし

［設定値の反映契機］

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，現在認証中のものはそのままで，次回ログイン時からコンフィグレーションの設定が有効となります。

［関連コマンド］

mac-authentication system-auth-control

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

logging email-event-kind

mac-authentication max-timer

MAC 認証での最大接続時間の設定を行います。

[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}

MAC 認証が認証を行う最大接続時間の設定を分単位で行います。認証成功後から，本コマンドの設定時間が経過した場合，自動的に認証が解除されます。なお，設定された時間が経過してから 1 分以内で認証解除を行います。

「infinity」と指定した場合は，最大接続時間を無限とし，最大接続時間による認証解除を行いません。

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
   10 ～ 1440，または infinity

[コマンド省略時の動作]

最大接続時間による認証解除を行いません。

[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]

1. 最大接続時間の短縮，延長を行った場合には，現在認証中のものは前設定を有効とし，次回ログイン時からコンフィグレーションの設定が有効になります。
2. MAC 認証での接続時間は，装置の時刻を用いて管理しています。そのため，運用コマンド set clock で日時を変更した場合，接続時間に影響が出ます。

   （例）

   3 時間後の時刻に値を変更した場合，接続時間が 3 時間経過した状態になってしまいます。また，逆に 3 時間前の時刻に値を変更した場合，接続時間が 3 時間延長されてしまいます。

[関連コマンド]

mac-authentication system-auth-control

mac-authentication port

mac-authentication password

MAC 認証で，RADIUS サーバに認証要求を出すときの端末ユーザで使用する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>

MAC 認証で，RADIUS サーバに認証要求を出すときのユーザ情報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]

本設定が行われないと，ユーザ情報パスワードとして，認証対象端末の MAC 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]

なし

[関連コマンド]

mac-authentication system-auth-control

mac-authentication port

aaa authentication mac-authentication default group radius

mac-authentication port

MAC 認証を動作させるポートを指定します。

本コマンドを設定していないポートでは MAC 認証が動作しません。

アクセスポートおよびトランクポートに設定された場合は，固定 VLAN モードとなります。また，MAC VLAN が設定されたポートの場合は，ダイナミック VLAN モードとなります。

[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]

該当ポートで MAC 認証による認証が行われません。

[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，該当ポートでの認証が解除されます。

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

mac-authentication system-auth-control

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

mac-authentication radius-server host {<ipv4 address> | <ipv6 address> [interface <interface type> <interface number>] | <host name>} [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> [interface <interface type> <interface number>] | <host name>}

［入力モード］

(config)

［パラメータ］

{<ipv4 address> | <ipv6 address> [interface <interface type> <interface number>] | <host name>}

<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> [interface <interface type> <interface number>]

RADIUS サーバの IPv6 アドレスをコロン記法で指定します。

リンクローカルアドレス指定時だけ interface パラメータを設定します。

<interface type> <interface number> には，次を指定できます。

- vlan <vlan id>
  <vlan id> は interface vlan コマンドで設定した VLAN ID を指定します。
- mgmt 0

<host name>

RADIUS サーバのホスト名称を 64 文字以内で指定します。

ホスト名称として使用できる文字については，「パラメータに指定できる値」を参照してください。

1. 本パラ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，IPv6 アドレス，またはホスト名称を指定します。
   IPv6 リンクローカルアドレス指定時はインタフェースも指定します。

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
   5
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
   3
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 サーバ上と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，該当する RADIUS サーバは無効になります。
2. 値の設定範囲
   １～ 64 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，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]

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. 本コマンドが実行されている場合，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。
2. 本コマンドで設定可能な RADIUS サーバ数は装置当たり最大 4 です。
3. 本コマンドで複数の RADIUS サーバが設定されている場合，コンフィグレーションの表示結果で最も上にくる RADIUS サーバが最初の認証に使用されます。

［関連コマンド］

mac-authentication system-auth-control

mac-authentication port

aaa authentication mac-authentication default group radius

aaa accounting mac-authentication default start-stop group radius

radius-server host

mac-authentication static-vlan max-user

MAC 認証の固定 VLAN モードで認証できる最大 MAC アドレス数を設定します。

［入力形式］

情報の設定・変更

mac-authentication static-vlan max-user <count>

情報の削除

no mac-authentication static-vlan max-user

［入力モード］

(config)

［パラメータ］

<count>

MAC 認証の固定 VLAN モードで，認証を行う最大数を設定します。設定した数を超えての認証はできません。

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
   1 ～ 4096

［コマンド省略時の動作］

認証可能な最大認証数：4096

［通信への影響］

なし

［設定値の反映契機］

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，現在認証中のものはそのままで，次回ログイン時からコンフィグレーションの設定が有効となります。

［関連コマンド］

mac-authentication system-auth-control

mac-authentication port

mac-authentication system-auth-control

MAC 認証デーモンの起動を行い，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 認証デーモンを停止します。

［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，すべての認証が解除されます。

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

1. 認証 VLAN が設定されている場合，本コマンドは設定できません。

［関連コマンド］

mac-authentication port

mac-authentication vlan-check

MAC 認証の固定 VLAN モードの認証処理で MAC アドレスを照合する際，VLAN ID も照合を行います。

［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>

MAC 認証の固定 VLAN モードで，RADIUS サーバに問い合わせる際のアカウントに付加する文字列を設定します。本装置が MAC 認証機能で RADIUS サーバに問い合わせる際のアカウントは，MAC アドレス文字列と本コマンドで設定した文字列と，VLAN ID 文字列を結合したものを使用します。

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。
   （例）” @vlan ” を設定した場合，mac アドレス 0012.e201.23ab,vlan id 10 のユーザ情報を RADIUS サーバへ送信するときのユーザ情報は 0012e20123ab@vlan10 となる。

［コマンド省略時の動作］

認証処理で VLAN ID のチェックを行いません。

［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］

mac-authentication system-auth-control

mac-authentication port

aaa authentication mac-authentication default group radius

12 認証 VLAN【OP-VAA】

fense alive-timer【OP-VAA】

fense retry-count【OP-VAA】

fense retry-timer【OP-VAA】

fense server【OP-VAA】

fense vaa-name【OP-VAA】

fense vaa-sync【OP-VAA】

fense vlan【OP-VAA】

fense alive-timer【OP-VAA】

VLANaccessController からの Keep Alive パケットが本コマンドで指定した秒単位の時間間隔以内に到着しない場合，認証サーバへの再接続処理を実行します。

［入力形式］

情報の設定・変更

fense <vaa id> alive-timer <seconds>

情報の削除

no fense <vaa id> alive-timer

［入力モード］

(config)

［パラメータ］

<vaa id>

認証 VLAN システムで，本装置が VLANaccessController への接続を一意に識別するための番号を指定します。

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

<seconds>

VLANaccessController からの Keep Alive パケット監視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
   20 ～ 7200

［コマンド省略時の動作］

<seconds> は 20 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. IEEE802.1X の dot1x system-auth-control コマンドが設定されている場合，本コマンドは設定できません。

［関連コマンド］

fense vaa-name

fense server

fense vlan

fense retry-count【OP-VAA】

VLANaccessAgent が VLANaccessController に対する接続に失敗した時，fense retry-timer コマンドで指定した間隔で接続を試みます。このリトライは no fense server コマンドを実行しないかぎり実行しますが，本装置内に起動しているすべての VLANaccessAgent の接続リトライ失敗回数が本コマンドで設定したリトライ失敗回数を上回れば，本装置内の，すべての認証 VLAN の動的 MAC アドレスを削除します。

［入力形式］

情報の設定・変更

fense <vaa id> retry-count { <count> | infinity }

情報の削除

no fense <vaa id> retry-count

［入力モード］

(config)

［パラメータ］

<vaa id>

認証 VLAN システムで，本装置が VLANaccessController への接続を一意に識別するための番号を指定します。

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

{ <count> | infinity }

infinity を一つ以上の VLANaccessAgent に対して指定した場合，認証 VLAN の動的 MAC アドレスの全削除は行わないで，接続リトライ処理を無限に行います。
コマンドの引数として 0 を指定すると，リトライ失敗ごとに認証 VLAN の動的 MAC アドレスの削除を試みます。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   infinity または 0 ～ 32767

［コマンド省略時の動作］

<count> は 25920 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. IEEE802.1X の dot1x system-auth-control コマンドが設定されている場合，本コマンドは設定できま

せん。

［関連コマンド］

fense vaa-name

fense server

fense vlan

fense retry-timer【OP-VAA】

VLANaccessController との通信に失敗した際に，本コマンドで設定した秒単位の時間間隔で接続を試みます。

［入力形式］

情報の設定・変更
　fense <vaa id> retry-timer <seconds>

情報の削除
　no fense <vaa id> retry-timer

［入力モード］

(config)

［パラメータ］

<vaa id>

認証 VLAN システムで，本装置が VLANaccessController への接続を一意に識別するための番号を指定します。

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

<seconds>

リトライ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

［コマンド省略時の動作］

<seconds> は 10 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. IEEE802.1X の dot1x system-auth-control コマンドが設定されている場合，本コマンドは設定できません。

［関連コマンド］

fense vaa-name

fense server

fense vlan

fense server【OP-VAA】

認証サーバ（VLANaccessController）の IP アドレス，TCP ポート番号を指定します。

［入力形式］

情報の設定・変更

fense <vaa id> server <server address> [<port>]

情報の削除

no fense <vaa id> server

［入力モード］

(config)

［パラメータ］

<vaa id>

認証 VLAN システムで，本装置が VLANaccessController への接続を一意に識別するための番号を指定します。

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

<server address>

VLANaccessController 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
   VLANaccessController の IPv4 アドレスをドット記法で指定します。

<port>

VLANaccessController の TCP 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
   52153
2. 値の設定範囲
   1024 ～ 65535

［コマンド省略時の動作］

なし

［通信への影響］

本コマンドによって認証サーバを変更した場合，変更前のサーバとは通信断，変更後のサーバとの通信となります。認証済みクライアントの通信には影響はありません。

［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。

ただし，次の条件を満たす場合，VLANaccessAgent を起動し認証サーバへの接続を開始します。

- fense vaa-name コマンドによって装置名称が設定されている。
- fense server コマンドによって認証サーバの設定がされている。
- fense vlan コマンドでエントリが一つ以上設定されている。

[注意事項]

1. IEEE802.1X の dot1x system-auth-control コマンドが設定されている場合，本コマンドは設定できません。
2. fense vlan コマンドで認証 VLAN システムのネットワーク構成を変更した場合，必ず認証サーバの各機能の再起動を行い，さらに，本装置の認証 VLAN の再起動を行ってください。
3. 本コマンドで複数の <vaa id> にわたって同じ <server address> を設定した場合，認証サーバとの接続が不安定になる可能性があります。その場合，ネットワーク構成を見直し認証 VLAN のコンフィグレーションを再設定したあと，本装置の認証 VLAN を再起動してください。
4. fense server コマンドで登録したものと同じ <vaa id> を持つ fense vlan コマンドが設定されている場合，no fense server コマンドで削除できません。あらかじめ no fense vlan コマンドで削除したあとに，no fense server コマンドを実行してください。

[関連コマンド]

fense vaa-name

fense vlan

fense vaa-name【OP-VAA】

VLANaccessController に送信する VLANaccessAgent の名称を設定します。この名称は装置に一つだけ設定します。認証サーバ配下に複数の VLANaccessAgent が稼働する装置を接続する場合は，装置ごとに異なる名称を設定してください。

［入力形式］

情報の設定・変更
　fense vaa-name <name>

情報の削除
　no fense vaa-name

［入力モード］

(config)

［パラメータ］

<name>
　VLANaccessController に送信する VLANaccessAgent の名称を指定します。この名称は装置に一つだけ設定します。
　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
　　指定できる文字数は 1 ～ 64 文字です。また，使用できる文字は，英数字および「/」，「-」，「_」，「.」だけです。さらに次の文字列は指定できません。
　　.（先頭 1 文字がドット「.」だけの場合）
　　ID
　　DPCI
　　VLAN
　　MAC
　　-ERR

［コマンド省略時の動作］

なし

［通信への影響］

本コマンドによって vaa-name を変更または削除した場合，VLANaccessAgent と認証サーバとの接続がいったん切断され再度接続されますが，認証済みクライアントの通信には影響はありません。

［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。

ただし，次の条件を満たす場合，VLANaccessAgent を起動し認証サーバへの接続を開始します。

- fense vaa-name コマンドによって装置名称が設定されている。
- fense server コマンドによって認証サーバの設定がされている。
- fense vlan コマンドでエントリが一つ以上設定されている。

[注意事項]

1. IEEE802.1X の dot1x system-auth-control コマンドが設定されている場合，本コマンドは設定できません。
2. 本コマンドで認証 VLAN システムのネットワーク構成を変更した場合，必ず認証サーバの各機能の再起動を行い，さらに，本装置の認証 VLAN の再起動を行ってください。

[関連コマンド]

fense server

fense vlan

fense vaa-sync【OP-VAA】

認証サーバからの MAC VLAN の MAC アドレス登録要求に対し，通常モードでの動作を行ないます。なお，no fense vaa-sync が設定された場合は，スイッチ間非同期モードとなります。

［入力形式］

情報の設定
　no fense vaa-sync

情報の削除
　fense vaa-sync

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

通常モードでの動作となります。

［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］

fense vaa-name

fense vlan【OP-VAA】

認証済み VLAN の VLAN ID およびサブネットを指定します。

［入力形式］

情報の設定・変更

fense <vaa id> vlan <vlan id> <subnet address> <subnet mask>

情報の削除

no fense <vaa id> vlan <vlan id> <subnet address> <subnet mask>

［入力モード］

(config)

［パラメータ］

<vaa id>

認証 VLAN システムで，本装置が VLANAccessController への接続を一意にするための番号を指定します。

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

<vlan id>

認証済み 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
   MAC VLAN で設定した VLAN ID を指定してください。

<subnet address>

認証済み VLAN のサブネット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
   認証済み VLAN のサブネットアドレスをドット記法で指定します。

<subnet mask>

認証済み VLAN のサブネットマスクを指定します。

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
   128.0.0.0 ～ 255.255.255.255

［コマンド省略時の動作］

なし

［通信への影響］

本コマンドによって認証済み VLAN を追加または削除した場合，VLANaccessAgent と認証サーバとの接

続がいったん切断され再度接続されますが，認証済みクライアントの通信には影響はありません。

［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。

ただし，次の条件を満たす場合，VLANaccessAgent を起動し認証サーバへの接続を開始します。

- fense vaa-name コマンドによって装置名称が設定されている。
- fense server コマンドによって認証サーバの設定がされている。
- fense vlan コマンドでエントリが一つ以上設定されている。

［注意事項］

1. VLAN ID に対応する VLAN に対して MAC VLAN が設定されている必要があります。
2. <vaa id> を通して，VLAN ID に対して設定されているサブネットと異なるサブネットを同一の VLAN ID に対して設定することはできません。
3. <vaa id> を通して装置内に fense vlan コマンドとして設定できる上限は 4094 個です。なお，複数の <vaa id> に同一の VLAN ID を設定した場合，それぞれを 1 個とカウントします。
4. IEEE802.1X の dot1x system-auth-control コマンドが設定されている場合，本コマンドは設定できません。
5. 本コマンドで認証 VLAN システムのネットワーク構成を変更した場合，必ず認証サーバの各機能の再起動を行い，さらに，本装置の認証 VLAN の再起動を行ってください。

［関連コマンド］

fense vaa-name

fense server

13 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 option allow-untrusted
ip dhcp snooping limit rate
ip dhcp snooping logging enable
ip dhcp snooping loglevel
ip dhcp snooping trust
ip dhcp snooping verify mac-address
ip dhcp snooping vlan
ip source binding
ip verify source

ip arp inspection limit rate

本装置での DHCP snooping の有効時に，装置当たりの 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。なお，実際の受信レートは本コマンドと ip dhcp snooping limit rate コマンドの合計受信レートが使用され，受信可能なパケット数も DHCP パケットと ARP パケットの合計になります。

[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)

[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
   10 ～ 125（packet/s）

[コマンド省略時の動作]

受信レートを制限しません。

[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

本装置での DHCP snooping の有効時に，該当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. 本コマンドを設定したインタフェースでは，ダイナミック ARP 検査が有効になっている VLAN に収容されていても，ARP 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 vlan

ip arp inspection validate

本装置でのダイナミック ARP 検査の有効時，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 [src-mac] [dst-mac] [ip]

情報の削除

no ip arp inspection validate

［入力モード］

(config)

［パラメータ］

src-mac

受信 ARP パケットのレイヤ 2 ヘッダに含まれる送信元 MAC アドレス（Source MAC）と，ARP ヘッダに含まれる送信元 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。

1. 本パラメータ省略時の初期値
   受信 ARP パケットのレイヤ 2 ヘッダに含まれる送信元 MAC アドレス（Source MAC）と，ARP ヘッダに含まれる送信元 MAC アドレス（Sender MAC Address）が同一であるかを検査しません。
2. 値の設定範囲
   なし

dst-mac

受信 ARP パケットのレイヤ 2 ヘッダに含まれる宛先 MAC アドレス（Destination MAC）と，ARP ヘッダに含まれる宛先 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。

1. 本パラメータ省略時の初期値
   受信 ARP パケットのレイヤ 2 ヘッダに含まれる宛先 MAC アドレス（Destination MAC）と，ARP ヘッダに含まれる宛先 MAC アドレス（Target MAC Address）が同一であるかを検査しません。
2. 値の設定範囲
   なし

ip

受信 ARP パケットの ARP ヘッダに含まれる宛先 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 に対してだけ実施します。

1. 本パラメータ省略時の初期値
   受信 ARP パケットの ARP ヘッダに含まれる宛先 IP アドレス（Target IP Address）を検査しません。
2. 値の設定範囲

なし

[コマンド省略時の動作]

ダイナミック ARP 検査の追加検査を行いません。

[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]

ip arp inspection vlan

ip dhcp snooping

ip dhcp snooping vlan

ip arp inspection vlan

本装置での DHCP snooping の有効時に，ダイナミック ARP 検査の検査対象 VLAN を設定します。

［入力形式］

情報の設定
ip arp inspection vlan <vlan id list>

情報の変更
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. 本コマンドには DHCP snooping を有効にしている VLAN ID を設定する必要があります。

［関連コマンド］

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping

本装置での DHCP snooping 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]

DHCP snooping 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. fldm prefer コマンドのフロー配分パターンに qos-only が設定されている場合，本コマンドは設定できません。同様に，フロー検出拡張モードに standard または extended が設定されている場合も，本コマンドは設定できません。

[関連コマンド]

fldm prefer

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 | mc <file name>}
保存先を指定します。

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 文字が設定できます。
   MC 上のファイル名称を指定します。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 64 文字まで設定できます。

[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待ち時間は，次のどれかを保存契機としてタイマをスタートし，タイマの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，または削除時
   - 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

タイマが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最大書き込み待ち時間を設定します。

[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最大書き込み待ち時間を設定します。

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]

最大書き込み待ち時間が 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待ち時間は，次のどれかを保存契機としてタイマをスタートし，タイマの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，または削除時
   - 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

   タイマが満了する前に装置電源断などが発生した場合は，バインディングデータベースを保存できません。
2. no ip dhcp snooping database url コマンドを入力した場合は，本コマンドで設定した時間のタイマがスタートしていても，バインディングデータベースを保存しません。

[関連コマンド]

ip dhcp snooping

ip dhcp snooping database url

ip dhcp snooping vlan

ip dhcp snooping information option allow-untrusted

信頼されていないポート（untrust ポート）でリレーエージェント情報オプション（Option82）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 limit rate

装置当たりの，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。なお，実際の受信レートは本コマンドと ip arp inspection limit rate コマンドの合計受信レートが使用され，受信可能なパケット数も DHCP パケットと ARP パケットの合計になります。

［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)

［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
   10 ～ 125（packet/s）

［コマンド省略時の動作］

受信レートを制限しません。

［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 logging enable

DHCP snooping 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
　ip dhcp snooping logging enable

情報の削除
　no ip dhcp snooping 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］

なし

［関連コマンド］

ip dhcp snooping

ip dhcp snooping loglevel

DHCP snooping の動作ログメッセージで記録するメッセージレベルを指定します。記録されたログメッセージは，運用コマンド show ip dhcp snooping logging で表示されます。

[入力形式]

情報の設定・変更

ip dhcp snooping loglevel {error | warning | notice | info}

情報の削除

no ip dhcp snooping loglevel

[入力モード]

(config)

[パラメータ]

{error | warning | notice | info}

error

error レベルのログメッセージだけを記録します。ソフトウェアエラーだけ記録します。

warning

error および warning レベルのログメッセージを記録します。不正パケットなどの異常検出情報が記録されます。

notice

error，warning および notice レベルのログメッセージを記録します。不正サーバ検出情報が記録されます。

info

error，warning，notice および info レベルのログメッセージを記録します。動作追跡情報が記録されます。

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
   error，warning，notice，info

[コマンド省略時の動作]

動作ログメッセージで記録するメッセージレベルは notice 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. ログメッセージの記録は ip dhcp snooping コマンドを設定している間だけ有効になります。

［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］

該当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しないかを設定します。

［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］

1. 本コマンドが未設定の場合，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。

[入力形式]

情報の設定
ip dhcp snooping vlan <vlan id list>

情報の変更
ip dhcp snooping vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

情報の削除
no ip dhcp snooping vlan

[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
   <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>

DHCP snooping を有効にする 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>

DHCP snooping を有効にする 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]

DHCP snooping を無効にします。

[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ない VLAN では，DHCP snooping は無効です。

[関連コマンド]

ip dhcp snooping

ip source binding

バインディングデータベースにスタティックエントリを設定します。

［入力形式］

情報の設定

ip source binding <mac address> vlan <vlan id> <ip address> interface <interface type> <interface number>

情報の削除

no ip source binding <mac address> vlan <vlan id> <ip address> interface <interface type> <interface number>

［入力モード］

(config)

［パラメータ］

<mac address>

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 <interface type> <interface number>

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
   <interface type> <interface number> には，次の値を設定できます。
   ・gigabitethernet <nif no.>/<port no.>
   ・tengigabitethernet <nif no.>/<port no.>
   ・port-channel <channel group number>
   <nif no.>/<port no.> および <channel group number> 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]

1. 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，バインディングデータベースに登録されません。

[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。

端末フィルタとは，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です。

［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
   port-security，mac-only

［コマンド省略時の動作］

端末フィルタを行いません。

［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. 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は無効です。
2. DHCP snooping の有効時に本設定を行う場合，DHCP snooping が無効な VLAN でも端末フィルタが有効になります。

［関連コマンド］

ip dhcp snooping

ip dhcp snooping trust

ip dhcp snooping vlan

ip source binding

14 電源機構（PS）の冗長化

power redundancy-mode

power redundancy-mode

冗長電源が実装されていない場合に，それを知らせるログを表示するかどうかの設定ができます。

［入力形式］

情報の設定
　power redundancy-mode redundancy-check

情報の削除
　no power redundancy-mode

［入力モード］

(config)

［パラメータ］

redundancy-check

　このパラメータは冗長電源の実装状態をチェックします。
　冗長電源が未実装の場合は，電源が冗長実装でないことを知らせるログを表示します。

1. 本パラ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］

冗長電源の実装状態のチェックをしません。

冗長電源が未実装の場合でも，電源が冗長実装でないことを知らせるログを表示しません。

［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］

なし

［関連コマンド］

なし

15 BSU の冗長化【AX6700S】

redundancy bsu-load-balancing【AX6700S】

redundancy bsu-mode【AX6700S】

redundancy max-bsu【AX6700S】

redundancy standby-bsu【AX6700S】

redundancy bsu-load-balancing【AX6700S】

パケット転送の負荷分散方式を設定します。

[入力形式]

情報の設定
　redundancy bsu-load-balancing smac

情報の削除
　no redundancy bsu-load-balancing

[入力モード]

(config)

[パラメータ]

smac
　受信パケットの送信元 MAC アドレスごとに振り分け先 BSU を選択します。中継するパケットの送信元 MAC アドレスが多数ある環境で効果があります。詳細については,「コンフィグレーションガイド Vol.2　18. BSU の冗長化【AX6700S】」を参照してください。

[コマンド省略時の動作]

パケットを受信したポートごとに振り分け先 BSU を選択します。

[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]

本パラメータを設定した場合は，コンフィグレーションを保存したあとに，必ず本装置を再起動してください。再起動しないと設定値が運用に反映されません。

[注意事項]

1. 本設定を変更後，本装置の再起動をする前に，BSU および NIF の再起動をしないでください。
2. 本コマンドは，redundancy bsu-mode fixed および no system recovery コマンドと同時に設定して使用します。
3. 本コマンドは，power-control，schedule-power-control mode，schedule-power-control max-bsu，schedule-power-control standby-bsu，schedule-power-control time-range および adaptive-power-control enable コマンドが設定されていないときに設定できます。
4. 本コマンド使用時は，QoS の帯域監視機能およびストームコントロール機能を使用しないでください。

[関連コマンド]

redundancy bsu-mode

no system recovery

redundancy bsu-mode【AX6700S】

BSU 運転モードを設定します。

［入力形式］

情報の設定
　redundancy bsu-mode fixed

情報の削除
　no redundancy bsu-mode

［入力モード］

(config)

［パラメータ］

fixed
　固定モードを設定します。本モードは，正常な BSU を使用している通信には一切影響を与えず，障害の BSU だけ停止する機能です。障害の BSU を使用していた通信は通信障害とします。詳細については，「コンフィグレーションガイド Vol.2　18. BSU の冗長化【AX6700S】」を参照してください。

［コマンド省略時の動作］

BSU の閉塞や障害が発生しても，正常な BSU を使用して通信を継続します。

［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］

本パラメータを設定した場合は，コンフィグレーションを保存したあとに，必ず本装置を再起動してください。再起動しないと設定値が運用に反映されません。

［注意事項］

1. 本設定を変更後，本装置の再起動をする前に，BSU および NIF の再起動をしないでください。
2. 本コマンドは，redundancy bsu-load-balancing smac および no system recovery コマンドと同時に設定して使用します。
3. 本コマンドは，power-control，schedule-power-control mode，schedule-power-control max-bsu，schedule-power-control standby-bsu，schedule-power-control time-range および adaptive-power-control enable コマンドが設定されていないときに設定できます。
4. 本コマンドを設定している場合，redundancy max-bsu で設定した BSU 数を超えた BSU は起動されません。

［関連コマンド］

no system recovery

redundancy bsu-load-balancing smac

redundancy max-bsu【AX6700S】

稼働させる BSU の枚数を設定します。

[入力形式]

情報の設定・変更
　redundancy max-bsu <max bsu>

情報の削除
　no redundancy max-bsu

[入力モード]

(config)

[パラメータ]

<max bsu>

運用系の枚数を設定します。枚数を多くすることで，パケット転送性能を向上できます。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。

1. 本パラ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

[コマンド省略時の動作]

稼働させる BSU の枚数を 3 枚とします。

[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. スケジューリングによる省電力機能の動作中は schedule-power-control max-bsu コマンドの設定に従い動作します。
2. トラフィック量による省電力機能の動作中は adaptive-power-control max-bsu コマンドの設定に従い動作します。
3. すべての BSU を運用系とするときは，実装している BSU の枚数を本コンフィグレーションのパラメータに設定してください。

[関連コマンド]

なし

redundancy standby-bsu【AX6700S】

待機系の BSU モードの設定を行います。

[入力形式]

情報の設定・変更
　redundancy standby-bsu {hot | cold | cold2}

情報の削除
　no redundancy standby-bsu

[入力モード]

(config)

[パラメータ]

{hot | cold | cold2}

hot
　待機系 BSU の電力供給を ON にし，障害発生時に系切替を瞬時に行います。

cold
　待機系 BSU の電力供給を部分的に OFF にすることで，待機系 BSU の消費電力を抑えられます。運用系 BSU の障害発生時に自動的に起動し，系切替を行います。なお，系切替時に待機系 BSU を起動するため，系切替に時間が必要です。

cold2
　待機系 BSU の電力供給を完全に OFF にすることで，待機系 BSU の消費電力をほぼ 0（ゼロ）に抑えられます。運用系 BSU の障害発生時に自動的に起動し，系切替を行います。なお，系切替時に待機系 BSU を起動するため，系切替に時間が必要です。

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
   hot，cold，cold2

[コマンド省略時の動作]

待機系の電力供給を ON にして，障害発生時に系切替を瞬時に行います。

[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. 本コマンドの cold パラメータは，schedule-power-control mode，schedule-power-control max-bsu，schedule-power-control standby-bsu，schedule-power-control time-range および adaptive-power-control enable コマンドが設定されていないときに設定できます。
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 standby-bsu コマンドの設定に従い動作します。

3. トラフィック量による省電力機能の動作中は adaptive-power-control standby-bsu コマンドの設定に従い動作します。

［関連コマンド］

なし

16 PSP の冗長化【AX6600S】

redundancy max-psp【AX6600S】

redundancy standby-psp【AX6600S】

redundancy max-psp【AX6600S】

稼働させる PSP の枚数を設定します。

[入力形式]

情報の設定・変更
　redundancy max-psp <max psp>

情報の削除
　no redundancy max-psp

[入力モード]

(config)

[パラメータ]

<max psp>
　運用系の枚数を設定します。枚数を多くすることで，パケット転送性能を向上できます。
　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 ～ 2

[コマンド省略時の動作]

PSP の動作状態が稼働中のものすべてを運用系とします。

[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. スケジューリングによる省電力機能の動作中は schedule-power-control max-psp コマンドの設定に従い動作します。
2. トラフィック量による省電力機能の動作中は adaptive-power-control max-psp コマンドの設定に従い動作します。

[関連コマンド]

なし

redundancy standby-psp【AX6600S】

待機系の PSP モードを設定します。

[入力形式]

情報の設定・変更
　redundancy standby-psp {hot | cold2}

情報の削除
　no redundancy standby-psp

[入力モード]

(config)

[パラメータ]

{hot | cold2}

hot
　待機系 PSP の電力供給を ON にして，障害発生時に系切替を瞬時に行います。

cold2
　待機系 PSP の電力供給を完全に OFF にすることで，待機系 PSP の消費電力をほぼ 0（ゼロ）に抑えられます。運用系 PSP の障害発生時に自動的に起動し，系切替を行います。なお，系切替時に待機系 PSP を起動するため，系切替に時間が必要です。

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
   hot，cold2

[コマンド省略時の動作]

待機系 PSP の電力供給を ON にして，障害発生時に系切替を瞬時に行います。

[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. スケジューリングによる省電力機能の動作中は schedule-power-control standby-psp コマンドの設定に従い動作します。
2. トラフィック量による省電力機能の動作中は adaptive-power-control standby-psp コマンドの設定に従い動作します。

[関連コマンド]

なし

17 NIF 冗長制御【AX6700S】【AX6600S】

redundancy nif-group max-standby-nif【AX6700S】【AX6600S】

redundancy nif-group nif priority【AX6700S】【AX6600S】

redundancy nif-group max-standby-nif【AX6700S】【AX6600S】

NIF 冗長グループを指定し，グループ内で待機状態となる NIF の最大枚数を設定します。

［入力形式］

情報の設定・変更

redundancy nif-group <nif group no.> max-standby-nif <max standby nif>

情報の削除

no redundancy nif-group <nif group no.> max-standby-nif

［入力モード］

(config)

［パラメータ］

<nif group no.>

NIF 冗長グループ番号を指定します。

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

<max standby nif>

NIF 冗長グループ内で待機状態とする NIF の最大枚数を指定します。NIF 冗長グループ内の運用状態の NIF 枚数が本コマンドの指定枚数を超えている場合，指定枚数の NIF を待機状態とします。待機状態となる NIF の選択方法は次のとおりです。

- redundancy nif-group nif priority コマンドの設定による優先度の低い NIF
- 優先度が同じ場合は NIF 番号の大きい NIF

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

［コマンド省略時の動作］

NIF 冗長グループ内の稼働中の NIF すべてを運用状態とします。

［通信への影響］

NIF 冗長制御機能によって，運用状態の NIF が待機状態となった場合，待機状態となった NIF を使用した通信が停止します。

［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. schedule-power-control time-range コマンドによってスケジュール時間帯を設定している場合，該当

する時間帯は本コマンドによる設定は無効となり，schedule-power-contorl redundancy nif-group max-standby-nif コマンドの設定に従って動作します。

［関連コマンド］

redundancy nif-group nif priority

redundancy nif-group nif priority【AX6700S】【AX6600S】

NIF 冗長グループを指定し，グループに所属する NIF およびグループ内での該当 NIF の優先度を設定します。NIF 冗長グループ内の運用中の NIF 数が redundancy nif-group max-standby-nif に設定されている値を超える場合，同一グループ内で優先度の低い NIF が redundancy nif-group max-standby-nif で指定された枚数だけ，待機状態になります。

［入力形式］

情報の設定

redundancy nif-group <nif group no.> nif <nif no.> priority <priority>

情報の削除

no redundancy nif-group <nif group no.> nif <nif no.>

［入力モード］

(config)

［パラメータ］

<nif group no.>

NIF 冗長グループ番号を指定します。

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

nif <nif no.>

グループに所属する NIF 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」の <nif no.> の範囲を参照してください。

priority <priority>

グループ内での NIF の優先度を指定します。値が小さいほど優先度が高くなります。

本設定値は，NIF 冗長制御機能によって待機状態とする NIF の選択に利用されます。待機状態となる NIF の選択方法は次のとおりです。

- 本コマンドの設定による優先度の低い NIF
- 優先度が同じ場合は NIF 番号の大きい NIF

1. 本パラ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

［コマンド省略時の動作］

NIF 冗長グループを設定しません。

［通信への影響］

NIF 冗長制御機能によって，運用状態の NIF が待機状態となった場合，待機状態となった NIF を使用した通信が停止します。

［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. 一つの NIF は一つの NIF 冗長グループにだけ所属できます。
2. 一つの NIF 冗長グループには NIF は 2 枚まで所属できます。
3. リンクアグリゲーションを設定する場合には，スタティックモードを設定してください。

［関連コマンド］

redundancy nif-group max-standby-nif

schedule-power-control nif-group max-standby-nif

18 GSRP

advertise-holdtime
advertise-interval
backup-lock
flush-request-count
gsrp
gsrp-vlan
gsrp direct-link
gsrp exception-port
gsrp limit-control
gsrp no-flush-port
gsrp reset-flush-port
layer3-redundancy
no-neighbor-to-master
port-up-delay
reset-flush-time
selection-pattern
vlan-group disable
vlan-group priority
vlan-group vlan

advertise-holdtime

受信した GSRP Advertise フレームの保持時間を秒単位で指定します。GSRP Advertise フレームを受信しないまま，保持時間を経過したときの動作は次のとおりです。

マスタ状態の場合
　マスタ状態を維持します。

バックアップ状態の場合
　マスタ状態の対向装置を認識できなくなり，バックアップ（隣接不明）状態に遷移します。

[入力形式]

情報の設定・変更
　advertise-holdtime <seconds>

情報の削除
　no advertise-holdtime

[入力モード]

(config-gsrp)

[パラメータ]

<seconds>
　受信した GSRP Advertise フレームの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
　1 ～ 120

[コマンド省略時の動作]

受信した GSRP Advertise フレームの保持時間は 5 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. advertise-holdtime は advertise-interval より大きな値を設定してください。advertise-interval 以下の値を設定した場合，GSRP Advertise フレームの受信タイムアウトを検出します。

[関連コマンド]

なし

advertise-interval

GSRP Advertise 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
　advertise-interval <seconds>

情報の削除
　no advertise-interval

［入力モード］

(config-gsrp)

［パラメータ］

<seconds>

GSRP Advertise フレームの送信間隔を秒単位で指定します。0.5 秒刻みで指定できます。

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
   0.5 ～ 60

［コマンド省略時の動作］

GSRP Advertise フレームの送信間隔は 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. advertise-holdtime は advertise-interval より大きな値を設定してください。advertise-interval 以下の値を設定した場合，GSRP Advertise フレームの受信タイムアウトを検出します。

［関連コマンド］

なし

backup-lock

本装置の GSRP 状態をバックアップ状態に固定します。

[入力形式]

情報の設定
　backup-lock

情報の削除
　no backup-lock

[入力モード]

(config-gsrp)

[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]

通信断が発生します。

[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]

なし

[関連コマンド]

なし

flush-request-count

GSRP Flush request フレームを使って周囲のスイッチに対して MAC アドレステーブルのクリアを行う GSRP Flush request フレームの送信回数を指定します。

[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-gsrp)

[パラメータ]

<count>

GSRP Flush request 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

[コマンド省略時の動作]

GSRP Flush request 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. GSRP Flush request フレームを複数送信しますが，受信したスイッチでの MAC アドレステーブルエントリのクリア動作は 1 回だけ行います。

[関連コマンド]

なし

gsrp

GSRP に関する項目を設定します。

[入力形式]

情報の設定
　gsrp <gsrp group id>

情報の削除
　no gsrp <gsrp group id>

[入力モード]

(config)

[パラメータ]

<gsrp group id>

GSRP グループ ID を設定します。同じ GSRP グループに属する GSRP スイッチは同じ GSRP グループ ID を指定してください。GSRP グループごとには，ネットワーク内でユニークな番号を指定してください。入力後，config-gsrp モードに移行します。

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
   1 ～ 65535

[コマンド省略時の動作]

なし

[通信への影響]

通信断が発生します。gsrp exception-port コマンドを設定しているポート，および gsrp limit-control コマンドを設定している場合（VLAN グループに所属していないポートが対象）でも，一時的に通信断が発生します。

[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. スパニングツリーおよび VRRP との同時動作はできません。
2. vlan-group vlan コマンドで指定する VLAN に属していないポートの状態は，gsrp limit-control コマンドで設定する GSRP VLAN グループ限定制御機能で動作が異なります。GSRP VLAN グループ限定制御機能を設定していない場合は，ポートの状態はブロッキングとなります。

[関連コマンド]

なし

gsrp-vlan

GSRP 管理 VLAN として使用する VLAN を指定します。

[入力形式]

情報の設定・変更
　gsrp-vlan <vlan id>

情報の削除
　no gsrp-vlan

[入力モード]

(config-gsrp)

[パラメータ]

<vlan id>

GSRP 管理 VLAN として使用する 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]

GSRP 管理 VLAN 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

gsrp direct-link

ダイレクトリンクに使用するポートを設定します。

[入力形式]

情報の設定
　gsrp <gsrp group id> direct-link

情報の削除
　no gsrp <gsrp group id> direct-link

[入力モード]

(config-if)

[パラメータ]

<gsrp group id>
　GSRP グループ 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 ～ 65535

direct-link
　ダイレクトリンクポートを設定します。

[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. gsrp-vlan コマンドで指定した VLAN に所属しているポートを指定してください。所属していないポートを指定した場合，GSRP が動作しません。
2. gsrp reset-flush-port コマンド，gsrp no-flush-port コマンドを設定したポートには設定できません。

[関連コマンド]

gsrp-vlan

gsrp exception-port

GSRP の制御対象外とするポートを設定します。設定されたポートの状態は常にフォワーディングになります。

[入力形式]

情報の設定
　gsrp exception-port

情報の削除
　no gsrp exception-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]

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. 指定したポートの状態は常にフォワーディングになるため，指定するポートおよびリンクアグリゲーションによってはループが発生する場合があるので注意してください。

[関連コマンド]

なし

gsrp limit-control

GSRP VLAN グループ限定制御機能を設定します。

本コマンドで GSRP VLAN グループ限定制御機能を設定すると，VLAN グループに所属している VLAN だけを GSRP で制御します。VLAN グループに所属していない VLAN のポートはフォワーディング状態になります。

[入力形式]

情報の設定
　gsrp limit-control

情報の削除
　no gsrp limit-control

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

VLAN グループへの所属に関係なく，すべての VLAN を GSRP の制御対象にします。VLAN グループに所属していない VLAN のポートは，ブロッキング状態になります。

[通信への影響]

VLAN グループに所属していない VLAN のポートで，GSRP の制御対象外ポートは，一時的に通信断が発生します。

[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]

なし

[関連コマンド]

vlan-group vlan

gsrp no-flush-port

GSRP Flush request フレームを送信しないポートを指定します。

[入力形式]

情報の設定

gsrp <gsrp group id> no-flush-port

情報の削除

no gsrp <gsrp group id> no-flush-port

[入力モード]

(config-if)

[パラメータ]

<gsrp group id>

GSRP グループ 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 ～ 65535

no-flush-port

GSRP Flush request フレームの未送信機能を設定します。

[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. gsrp direct-link コマンド，gsrp reset-flush-port コマンドを設定したポートには設定できません。
2. axrp-ring-port コマンドを設定したポートには適用されません。

[関連コマンド]

なし

gsrp reset-flush-port

ポートリセット機能を実施するポートを指定します。

[入力形式]

情報の設定

gsrp <gsrp group id> reset-flush-port

情報の削除

no gsrp <gsrp group id> reset-flush-port

[入力モード]

(config-if)

[パラメータ]

<gsrp group id>

GSRP グループ 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 ～ 65535

reset-flush-port

ポートリセット機能を設定します。

[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. gsrp direct-link コマンド，gsrp no-flush-port コマンドを設定したポートには設定できません。
2. axrp-ring-port コマンドを設定したポートには適用されません。

[関連コマンド]

なし

layer3-redundancy

該当 GSRP グループでレイヤ 3 冗長切替機能の使用を設定します。

[入力形式]

情報の設定
　layer3-redundancy

情報の削除
　no layer3-redundancy

[入力モード]

(config-gsrp)

[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. GSRP グループ ID が 1 から 4 の場合だけ本コマンドを設定できます。
2. レイヤ 3 冗長切替機能を使用する場合，対向装置にも本コマンドを設定してください。
3. GSRP で運用する VLAN への IPv4 アドレスおよび IPv6 アドレスの設定は対向装置と合わせてください。

[関連コマンド]

なし

no-neighbor-to-master

バックアップ（隣接不明）状態からマスタ状態に切り替えるときに，手動（マスタ遷移コマンド入力）で切り替えるか，自動（ダイレクトリンクポート障害の検出時）で切り替えるかを選択します。

[入力形式]

情報の設定・変更

no-neighbor-to-master { manual | direct-down [forced-shift-time <seconds>] }

情報の削除

no no-neighbor-to-master

[入力モード]

(config-gsrp)

[パラメータ]

{ manual | direct-down [forced-shift-time <seconds>] }

バックアップ（隣接不明）状態からマスタ状態に遷移する動作モードを指定します。

manual

GSRP Advertise フレームを受信，またはマスタ遷移コマンド（運用コマンド set gsrp master）が入力されるまで，バックアップ（隣接不明）状態のまま待機し続けます。

direct-down [forced-shift-time <seconds>]

ダイレクトリンクに指定したすべてのポートが障害状態の場合，マスタとして動作を開始します。GSRP スイッチ単独起動時のマスタ遷移機能によって，GSRP スイッチが単独で起動する時も自動的にマスタとして動作させる場合は，forced-shift-time パラメータを設定します。

- forced-shift-time <seconds>
  <seconds> は，GSRP スイッチが単独で起動する時に，自動的にマスタとして動作するまでの時間を秒単位で指定します。指定できる時間の範囲は，0 ～ 3600 秒です。

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
   manual または direct-down を指定します。
   GSRP スイッチが単独で起動する時も自動的にマスタとして動作させる場合は，forced-shift-time と自動マスタ遷移待ち時間をあわせて設定します。

[コマンド省略時の動作]

バックアップ（隣接不明）状態からマスタ状態への切り替えは，手動による切り替え（manual）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. バックアップ（隣接不明）状態からマスタ状態に遷移する動作モードを direct-down に設定した場合，ダイレクトリンクに指定したすべてのポートが障害状態になると，マスタとして動作を開始します。ただし，次に示す動作後，ダイレクトリンクに指定したポートで GSRP Advertise フレームを一度も受信していない場合，バックアップ（隣接不明）状態のまま待機し続けます。マスタとして動作させたい場合は，マスタ遷移コマンド（運用コマンド set gsrp master）を入力してください。
   - 装置起動
   - 系切替
   - 運用コマンド restart vlan の実行
   - 運用コマンド restart gsrp の実行
   - no-neighbor-to-master で direct-down を指定
   - direct-link によるダイレクトリンクポートの設定
   - 運用コマンド copy によるランニングコンフィグレーションへの反映
   - 運用コマンド inactivate bsu の実行で，すべての BSU が inactive 状態**【AX6700S】**
2. GSRP スイッチ単独起動時のマスタ遷移機能による自動マスタ遷移は，装置起動時に一回だけ動作します。ただし，次に示す動作が行われると，再度動作します。
   - 系切替
   - 運用コマンド restart vlan の実行
   - 運用コマンド restart gsrp の実行
   - 運用コマンド copy によるランニングコンフィグレーションへの反映
   - 運用コマンド activate bsu を実行し，最初の BSU が active 状態**【AX6700S】**

[関連コマンド]

なし

port-up-delay

ポートがアップした場合に，アクティブポート数のカウント対象に反映するまでの遅延時間を設定します。GSRP ではマスタ／バックアップの選択要因として，アクティブポート数を使用します。そのため，ポートのアップ，ダウンが頻発するなどのポートが不安定な状態になった場合にアクティブポート数の増減が多発し，結果マスタ状態とバックアップ状態の切り替えが連続して発生するおそれがあります。ポートが不安定な状態の際，本コマンドで遅延時間を指定することで，不要な切り替えを抑止できます。

遅延時間中にアクティブポートにカウントさせる際には，アクティブポート反映コマンド（運用コマンド clear gsrp port-up-delay）を入力してください。

[入力形式]

情報の設定・変更
　port-up-delay <seconds>

情報の削除
　no port-up-delay

[入力モード]

(config-gsrp)

[パラメータ]

<seconds>
　ポートがアップした場合にアクティブポート数のカウント対象に反映するまでの遅延時間を秒単位で指定します。「infinity」と指定した場合は，遅延時間を無限とし，自動ではアクティブポートにカウントしません。
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 ～ 43200 または infinity

[コマンド省略時の動作]

ポートがアップするとアクティブポート数のカウント対象に即時反映（0 秒）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

reset-flush-time

ポートリセット機能使用時のポートダウン時間を設定します。

[入力形式]

情報の設定・変更
　reset-flush-time <seconds>

情報の削除
　no reset-flush-time

[入力モード]

(config-gsrp)

[パラメータ]

<seconds>

　ポートリセット機能使用時のポートダウン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

[コマンド省略時の動作]

ポートダウン時間は 3 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. gsrp reset-flush-port コマンドを設定したすべてのポートに対して有効です。

[関連コマンド]

なし

selection-pattern

GSRP のマスタ，バックアップ状態を切り替えるときの，選択要因（アクティブポート数，優先度，装置 MAC アドレス）の優先順を設定します。

[入力形式]

情報の設定・変更
　selection-pattern { ports-priority-mac | priority-ports-mac }

情報の削除
　no selection-pattern

[入力モード]

(config-gsrp)

[パラメータ]

{ ports-priority-mac | priority-ports-mac }
　マスタ／バックアップ選択方法のパターンを指定します。

ports-priority-mac
　Active ポート数→ Priority →装置 MAC アドレスの順で選択します。

priority-ports-mac
　Priority → Active ポート数→装置 MAC アドレスの順で選択します。

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
   ports-priority-mac または priority-ports-mac

[コマンド省略時の動作]

アクティブポート数，優先度，装置 MAC アドレスの優先順（ports-priority-mac）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

vlan-group disable

VLAN グループ単位に GSRP 機能を無効にします。

［入力形式］

情報の設定

vlan-group <vlan group id> disable

情報の削除

no vlan-group <vlan group id> disable

［入力モード］

(config-gsrp)

［パラメータ］

<vlan group id>

GSRP 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 ～ 128

［コマンド省略時の動作］

各 VLAN グループに対して GSRP 機能は有効です。

［通信への影響］

通信断が発生します。

［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］

なし

［関連コマンド］

なし

vlan-group priority

GSRP で運用する VLAN グループの優先度を設定します。

［入力形式］

情報の設定・変更

vlan-group <vlan group id> priority <priority>

情報の削除

no vlan-group <vlan group id> priority

［入力モード］

(config-gsrp)

［パラメータ］

<vlan group id>

GSRP 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 ～ 128

priority <priority>

本 VLAN グループの優先度を指定します。数字が大き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 ～ 255

［コマンド省略時の動作］

VLAN グループの優先度は 100 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

vlan-group vlan

GSRP で運用する VLAN グループに参加する VLAN を設定します。

［入力形式］

情報の設定

vlan-group <vlan group id> vlan <vlan id list>

情報の変更

vlan-group <vlan group id> vlan { <vlan id list> | add <vlan id list> | remove <vlan id list> }

情報の削除

no vlan-group <vlan group id> vlan

［入力モード］

(config-gsrp)

［パラメータ］

<vlan group id>

GSRP 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 ～ 128

vlan <vlan id list>

VLAN グループに参加する VLAN の VLAN ID を指定します。VLAN ID 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。

add <vlan id list>

指定済みの 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>

指定済みの 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

[通信への影響]

なし

[設定値の反映契機]

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 GSRP を併用する場合，VLAN マッピング ID と GSRP の VLAN グループ ID で，次に示す範囲の同じ値は同時に使用できません。
   同時使用できない ID の範囲：108 ～ 128
2. GSRP と VRF 機能を併用する（vrf mode コマンドで gsrp-enable-ipv4-ipv6 パラメータを設定している）場合，一つの VLAN グループに所属させる VLAN 数は 250 以下にしてください。**【OP-NPAR】**

[関連コマンド]

vlan

19 VRRP

track check-reply-interface

track check-status-interval

track check-trial-times

track failure-detection-interval

track failure-detection-times

track interface

track ip route

track recovery-detection-interval

track recovery-detection-times

vrrp accept

vrrp authentication

vrrp follow

vrrp ietf-ipv6-spec-07-mode

vrrp ietf-unified-spec-02-mode

vrrp ip

vrrp ipv6

vrrp name

vrrp preempt

vrrp preempt delay

vrrp priority

vrrp timers advertise

vrrp timers non-preempt-swap

vrrp track

vrrp-vlan

track check-reply-interface

VRRP ポーリングの Reply を受信したインタフェースと Request を送信したインタフェースが一致するかどうかの確認の有無を設定します。

[入力形式]

情報の設定

track <track number> check-reply-interface

情報の削除

no track <track number> check-reply-interface

[入力モード]

(config)

[パラメータ]

<track number>

設定を保存する track 番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   1 ～ 255

[コマンド省略時の動作]

VRRP ポーリングの Reply を受信したインタフェースと Request を送信したインタフェースが一致するか確認を行いません。

[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]

1. 本コマンドによる設定は，track interface コマンドで ip routing を指定した track に対してだけ有効です。

[関連コマンド]

ip address

track interface

track ip route

vrrp ip

vrrp track

track check-status-interval

VRRP ポーリングの実行間隔を設定します。

[入力形式]

情報の設定・変更

track <track number> check-status-interval <seconds>

情報の削除

no track <track number> check-status-interval

[入力モード]

(config)

[パラメータ]

<track number>

設定を保存する track 番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   1 ～ 255

<seconds>

VRRP ポーリングを行う間隔（秒）を指定します。設定した間隔で VRRP ポーリングを行い，パケットの欠落・回復が発生した場合，インタフェース障害発生／障害回復の検証動作を行います。本コマンドを指定する track には，track interface コマンドで ip routing を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
   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]

VRRP ポーリングを 6 秒間隔で行います。

[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. 本コマンドによる設定は，track interface コマンドで ip routing を指定した track に対してだけ有効です。

[関連コマンド]

interface vlan

ip address

track interface

track ip route

vrrp ip

vrrp track

track check-trial-times

インタフェース障害発生／障害回復の検証中の VRRP ポーリング試行回数を設定します。

[入力形式]

情報の設定・変更

track <track number> check-trial-times <count>

情報の削除

no track <track number> check-trial-times

[入力モード]

(config)

[パラメータ]

<track number>

設定を保存する track 番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   1 ～ 255

<count>

インタフェース障害発生／障害回復の検証中の VRRP ポーリング試行回数を指定します。本コマンドを指定する track には，track interface コマンドで ip routing を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
   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]

インタフェース障害発生／障害回復の検証中の VRRP ポーリング試行回数を 4 回とします。

[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. 本コマンドによる設定は，track interface コマンドで ip routing を指定した track に対してだけ有効です。

[関連コマンド]

interface vlan

ip address

track interface

track ip route

vrrp ip

vrrp track

track failure-detection-interval

VRRP ポーリングの障害発生検証中の VRRP ポーリング試行間隔を設定します。

［入力形式］

情報の設定・変更
　track <track number> failure-detection-interval <seconds>

情報の削除
　no track <track number> failure-detection-interval

［入力モード］

(config)

［パラメータ］

<track number>
　設定を保存する track 番号を指定します。
　1. 本パラメータ省略時の初期値
　　省略できません
　2. 値の設定範囲
　　1 ～ 255

<seconds>
　障害発生検証中の VRRP ポーリング試行間隔（秒）を指定します。本コマンドを指定する track には，track interface コマンドで ip routing オプションを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
　　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］

障害発生検証中の VRRP ポーリング試行間隔を 2 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. 本コマンドによる設定は，track interface コマンドで ip routing を指定した track に対してだけ有効です。

［関連コマンド］

ip address

track interface

track ip route

vrrp ip

vrrp track

track failure-detection-times

VRRP ポーリングの障害発生検証中の VRRP ポーリング成功回数を設定します。

[入力形式]

情報の設定・変更
　track <track number> failure-detection-times <count>

情報の削除
　no track <track number> failure-detection-times

[入力モード]

(config)

[パラメータ]

<track number>

設定を保存する track 番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   1 ～ 255

<count>

障害発生検証中の VRRP ポーリング成功回数を指定します。ただし，check-trial-times の値以下になるようにしてください。本コマンドを指定する track には，track interface コマンドで ip routing オプションを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
   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]

障害発生検証中の VRRP ポーリング成功回数を 3 回とします。

[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. 本コマンドによる設定は，track interface コマンドで ip routing を指定した track に対してだけ有効です。

[関連コマンド]

ip address

track interface

track ip route

vrrp ip

vrrp track

track interface

障害監視に使用するインタフェースを指定します。また，VLAN の障害監視を設定する場合，VRRP ポーリングを行うか，障害監視インタフェースを行うかを設定します。

［入力形式］

情報の設定

track <track number> interface { vlan <vlan id> { line-protocol | ip routing } | <interface type> <interface number> line-protocol }

情報の変更

track <track number> interface { vlan <vlan id> | <interface type> <interface number> }
line-protocol

track <track number> interface vlan <vlan id> ip-routing

情報の削除

no track <track number> interface

［入力モード］

(config)

［パラメータ］

<track number>

設定を保存する track 番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   1 ～ 255

vlan <vlan id>

障害監視を行う VLAN の VLAN 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
   <vlan id> には interface vlan コマンドで設定した VLAN ID を指定します。

{ line-protocol | ip routing }

line-protocol

障害監視インタフェースを行います。

ip routing

VRRP ポーリングを行います。

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
   line-protocol または ip routing

<interface type> <interface number>

障害監視を行うインタフェースを指定します。

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 type> <interface number> には，次を指定できます。
   ・gigabitethernet <nif no.>/<port no.>
   ・tengigabitethernet <nif no.>/<port no.>
   <nif no.>/<port no.> 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。
   ・port-channel <channel group number>
   <channel group number> 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]

1. 設定可能な track 数は装置当たり最大 255 です。
2. 障害監視を行う VLAN インタフェースには IP アドレスが設定されている必要があります。
3. track を ip routing パラメータから line-protocol パラメータへ変更する場合は，一度本コマンドを削除してから再設定してください。また，line-protocol パラメータから ip routing パラメータへ変更する場合も同様に，一度削除してから再設定してください。
4. ip routing パラメータを指定する場合，track ip route コマンドで VRRP ポーリングをする宛先アドレスを設定してください。設定しない場合，障害監視インタフェースとして動作します。

[関連コマンド]

ip address

track ip route

vrrp ip

vrrp track

track ip route

VRRP ポーリングを行う場合の VRRP ポーリング宛先を設定します。

[入力形式]

情報の設定・変更

track <track number> ip route {<ip address> | <ipv6 address>} reachability

情報の削除

no track <track number> ip route [{<ip address> | <ipv6 address>} reachability]

[入力モード]

(config)

[パラメータ]

<track number>

設定を保存する track 番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   1 ～ 255

{<ip address> | <ipv6 address>} reachability

VRRP ポーリングをする宛先の IPv4 アドレスまたは IPv6 アドレスを指定します。本コマンドを指定する track は，track interface コマンドで ip routing オプションを指定する必要があります。宛先 IP アドレスまでの経路に関する問題は，ルーティングプロトコルによって解決してください。

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
   IPv4 アドレスおよび reachability，または IPv6 アドレスおよび reachablilty

[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. 本コマンドによる設定は，track interface コマンドで ip routing を指定した track に対してだけ有効です。
2. VRRP ポーリング宛先 IP アドレスは，track interface コマンドで指定した VLAN の IP アドレスと同一アドレスファミリで設定してください。
3. VRRP ポーリングの宛先アドレスのアドレスファミリを変更する場合は，コンフィグレーションを一度削除してから再設定してください。

［関連コマンド］

ip address

track interface

vrrp ip

vrrp track

track recovery-detection-interval

VRRP ポーリングの障害回復検証中の VRRP ポーリング試行間隔を設定します。

［入力形式］

情報の設定・変更

track <track number> recovery-detection-interval <seconds>

情報の削除

no track <track number> recovery-detection-interval [<seconds>]

［入力モード］

(config)

［パラメータ］

<track number>

設定を保存する track 番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   1 ～ 255

<seconds>

障害回復検証中の VRRP ポーリング試行間隔（秒）を指定します。本コマンドを指定する track には，track interface コマンドで ip routing オプションを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
   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］

障害回復検証中の VRRP ポーリング試行間隔を 2 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. 本コマンドによる設定は，track interface コマンドで ip routing を指定した track に対してだけ有効です。

［関連コマンド］

ip address

track interface

track ip route

vrrp ip

vrrp track

track recovery-detection-times

VRRP ポーリングの障害回復検証中の VRRP ポーリング成功回数を設定します。

[入力形式]

情報の設定・変更
　track <track number> recovery-detection-times <count>

情報の削除
　no track <track number> recovery-detection-times

[入力モード]

(config)

[パラメータ]

<track number>

設定を保存する track 番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   1 ～ 255

<count>

障害回復検証中の VRRP ポーリング成功回数を指定します。ただし，check-trial-times の値以下になるようにしてください。本コマンドを指定する track には，track interface コマンドで ip routing オプションを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
   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]

障害回復検証中の VRRP ポーリング成功回数を 3 回とします。

[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. 本コマンドによる設定は，track interface コマンドで ip routing を指定した track に対してだけ有効です。

[関連コマンド]

ip address

track interface

track ip route

vrrp ip

vrrp track

vrrp accept

仮想ルータのアクセプトモードの設定を行います。本コマンドでアクセプトモードを有効に設定すると，マスタ状態の仮想ルータはアドレス所有者でなくても IP パケットを受信できます。

[入力形式]

情報の設定

vrrp <vrid> accept

情報の削除

no vrrp <vrid> accept

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの 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 ～ 255

[コマンド省略時の動作]

アクセプトモードを無効とします。

[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. IP アドレス所有者に，アクセプトモードを有効に設定した場合は，アドレス所有者として動作します。
2. 本コマンドは実 IP アドレスと仮想 IP アドレスが同一のネットワーク上にある場合にだけ指定できます。
3. アクセプトモードを有効に設定している VRRP の仮想 IP アドレスと同じ実 IP アドレスを同一ネットワーク上に設定すると，IP アドレスの重複状態となります。
   また，IP アドレス所有者の仮想 IP アドレスと実 IP アドレスを同一ネットワーク上に設定すると，アクセプトモードの有効設定と同様に，IP アドレスの重複状態となります。
4. IPv6 アドレスの重複を検出した場合は，IP パケットの送受信ができなくなります。IPv6 アドレスの重複を検出した場合は設定を見直し，該当するインタフェースの UP/DOWN（運用コマンドの activate/inactivate）を行ってください。

[関連コマンド]

なし

vrrp authentication

仮想ルータの ADVERTISEMENT パケット認証で使用するパスワードを設定します。

[入力形式]

情報の設定・変更
　vrrp <vrid> authentication <text>

情報の削除
　no vrrp <vrid> authentication

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの 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 ～ 255

<text>

ADVERTISEMENT パケット認証で使用するパスワード（SIMPLE TEXT PASSWORD）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
   8 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]

パスワードなしとなります。ADVERTISEMENT パケット認証は行いません。

[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]

1. vrrp ietf-ipv6-spec-07-mode コマンド，vrrp ietf-unified-spec-02-mode コマンドを設定している場合，本設定は無効です。
2. vrrp follow コマンドを設定している場合，本設定は無効です。

[関連コマンド]

なし

vrrp follow

プライマリ仮想ルータを指定し，仮想ルータをフォロー仮想ルータに設定します。フォロー仮想ルータに設定されたトラッキング機能，優先度設定，PREEMPT モード設定，VRRP 動作モード設定，ADVERTISEMENT パケット送信間隔設定は無効となり，プライマリ仮想ルータの動作に従います。

[入力形式]

情報の設定・変更

vrrp <vrid> follow <string>

情報の削除

no vrrp <vrid> follow

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの 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 ～ 255

<string>

プライマリ仮想ルータ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
   15 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. 本コマンドは，仮想ルータがアドレス所有者の場合，設定できません。
2. 本コマンドは，ほかの仮想ルータからプライマリ仮想ルータに指定されている場合，設定できません。
   また，自分自身の仮想ルータ名，フォロー仮想ルータ名は指定できません。

[関連コマンド]

vrrp name

vrrp-vlan

vrrp ietf-ipv6-spec-07-mode

IPv6 の仮想ルータが draft-ietf-vrrp-ipv6-spec-07 に従った動作となるよう設定します。

本コマンドは，IPv6 の仮想ルータを設定している場合に有効になります。

［入力形式］

情報の設定

vrrp <vrid> ietf-ipv6-spec-07-mode

情報の削除

no vrrp <vrid> ietf-ipv6-spec-07-mode

［入力モード］

(config-if)

［パラメータ］

<vrid>

仮想ルータの 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 ～ 255

［コマンド省略時の動作］

IPv6 の仮想ルータは，vrrp ietf-unified-spec-02-mode コマンド設定時は draft-ietf-vrrp-unified-spec-02 に，設定なしの場合は draft-ietf-vrrp-ipv6-spec-02 に従った動作となります。

［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. 本設定を行うことによって，ADVERTISEMENT パケットのフォーマットも変更されます。VRRP を組む装置間で本設定が一致していないと，VRRP の状態遷移が正常に行われず，複数のマスタルータが存在するようになります。
2. VRRP を組んでいる装置間で本設定または同等の設定を変更するとき，一時的にマスタルータが複数存在します。VRRP を構成している全装置の設定がそろうと，自動的にマスタルータは一つだけになります。
3. ほかの VRRP 動作モードが設定されている仮想ルータには設定できません。
4. 本設定入力時に，vrrp timers advertise の設定値が 40 を超えている場合は，ADVERTISEMENT パケットの送信間隔はデフォルトの 1 秒となります。

［関連コマンド］

ipv6 address

vrrp ipv6

vrrp ietf-unified-spec-02-mode

仮想ルータが，draft-ietf-vrrp-unified-spec-02 に従った動作となるよう設定します。

［入力形式］

情報の設定

vrrp <vrid> ietf-unified-spec-02-mode

情報の削除

no vrrp <vrid> ietf-unified-spec-02-mode

［入力モード］

(config-if)

［パラメータ］

<vrid>

仮想ルータの 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 ～ 255

［コマンド省略時の動作］

IPv4 の仮想ルータは，RFC3768 に従った動作となります。

IPv6 の仮想ルータは，vrrp ietf-ipv6-spec-07-mode コマンド設定時は draft-ietf-vrrp-ipv6-spec-07 に，設定なしの場合は draft-ietf-vrrp-ipv6-spec-02 に従った動作となります。

［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. 本設定を行うことによって，ADVERTISEMENT パケットのフォーマットも変更されます。VRRP を組む装置間で本設定が一致していないと，VRRP の状態遷移が正常に行われず，複数のマスタルータが存在するようになります。
2. VRRP を組んでいる装置間で本設定または同等の設定を変更するとき，一時的にマスタルータが複数存在します。VRRP を構成している全装置の設定がそろうと，自動的にマスタルータは一つだけになります。
3. ほかの VRRP 動作モードが設定されている仮想ルータには設定できません。
4. 本設定入力時に，vrrp timers advertise の設定値が 40 を超えている場合は，ADVERTISEMENT パケットの送信間隔はデフォルトの 1 秒となります。
5. vrrp follow コマンドを設定している場合，本設定は無効です。

[関連コマンド]

vrrp ietf-ipv6-spec-07-mode

vrrp ip

仮想ルータに IPv4 アドレスを割り当てます。

[入力形式]

情報の設定・変更
　vrrp <vrid> ip <ip address>

情報の削除
　no vrrp <vrid> ip

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの 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 ～ 255

<ip address>

仮想ルータの IP 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

[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. 装置当たりに設定可能な仮想ルータ数は，IPv4 の仮想ルータと IPv6 の仮想ルータを合わせて最大 255 です。ただし，グループ機能を利用し，フォロー仮想ルータを作成することで，最大 4095 の仮想ルータを動作させることができます。
2. 本コマンドで仮想ルータに IP アドレスを割り当てると，仮想ルータが動作を始めます。
3. vrrp follow コマンドを設定された仮想ルータは，アドレス所有者に設定できません。

[関連コマンド]

ip address

vrrp ipv6

仮想ルータにIPv6アドレスを割り当てます。

[入力形式]

情報の設定・変更
　vrrp <vrid> ipv6 <ipv6 address>

情報の削除
　no vrrp <vrid> ipv6

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの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 ～ 255

<ipv6 address>

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

[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. 装置当たりに設定可能な仮想ルータ数は，IPv4の仮想ルータとIPv6の仮想ルータを合わせて最大255です。ただし，グループ機能を利用し，フォロー仮想ルータを作成することで，最大4095の仮想ルータを動作させることができます。
2. 本コマンドで仮想ルータにIPv6アドレスを割り当てると，仮想ルータが動作を始めます。

[関連コマンド]

ipv6 address

vrrp name

仮想ルータに名称を設定します。

[入力形式]

情報の設定
　vrrp <vrid> name <string>

情報の削除
　no vrrp <vrid> name

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの 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 ～ 255

<string>

プライマリ仮想ルータ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
   15 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. 本コマンドが設定された仮想ルータは，トラッキング機能で障害を検出し，仮想ルータの優先度が 0 となった場合，仮想ルータが設定されている IP インタフェースをダウンさせません。

[関連コマンド]

vrrp follow

vrrp preempt

仮想ルータの自動切り戻しを設定します。自動切り戻しが有効の場合，自ルータよりも低い優先度を持ったマスタルータを検出すると，自ルータが自動的にマスタルータになります。

[入力形式]

情報の設定
　no vrrp <vrid> preempt

情報の削除
　vrrp <vrid> preempt

[入力モード]

(config-if)

[パラメータ]

<vrid>
　仮想ルータの 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 ～ 255

[コマンド省略時の動作]

自動切り戻しを有効とします。

[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. swap vrrp コマンドが自動切り戻し抑止設定時に投入された場合は，コマンドを優先して切り戻しを行います。
2. 自ルータがマスタルータのダウンを検出したときは，自動切り戻しの設定にかかわらずマスタルータになります。
3. vrrp follow コマンドを設定している場合，本設定は無効です。

[関連コマンド]

なし

vrrp preempt delay

自動切り戻しを抑止する時間を設定します。自動切り戻しが有効の場合，切り戻しを行う前に設定した時間だけ処理を抑止します。

[入力形式]

情報の設定・変更

vrrp <vrid> preempt delay <seconds>

情報の削除

no vrrp <vrid> preempt delay

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの 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 ～ 255

<seconds>

自動切り戻しを抑止する時間（秒）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]

自動切り戻し抑止時間を 0 秒とします。自動切り戻しを抑止しません。

[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. vrrp follow コマンドを設定している場合，本設定は無効です。

[関連コマンド]

なし

vrrp priority

仮想ルータの優先度を設定します。

[入力形式]

情報の設定・変更
　vrrp <vrid> priority <priority>

情報の削除
　no vrrp <vrid> priority

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの 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 ～ 255

<priority>

仮想ルータの優先度を指定します。VLAN に指定された IP アドレスと仮想ルータの IP アドレスが同一の場合（IP アドレスの所有者の場合），仮想ルータの優先度は本指定にかかわらず 255 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
   1（低優先度）～ 254（高優先度）

[コマンド省略時の動作]

VLAN に指定された IP アドレスと仮想ルータの IP アドレスが同一の場合（IP アドレスの所有者の場合），仮想ルータの優先度を 255 とします。

IP アドレスの所有者以外の場合，仮想ルータの優先度を 100 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. vrrp follow コマンドを設定している場合，本設定は無効です。

[関連コマンド]

なし

vrrp timers advertise

仮想ルータの ADVERTISEMENT パケット送信間隔を設定します。

[入力形式]

情報の設定・変更

vrrp <vrid> timers advertise <seconds>

vrrp <vrid> timers advertise msec <milli seconds>

情報の削除

no vrrp <vrid> timers advertise

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの 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 ～ 255

<seconds>

ADVERTISEMENT パケットの送信間隔（秒）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

msec <milli seconds>

ADVERTISEMENT パケットの送信間隔（ミリ秒）を 10 ミリ秒刻みで指定します。

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
   250 ～ 40950 の範囲で 10 の倍数

[コマンド省略時の動作]

ADVERTISEMENT パケットの送信間隔を 1 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. vrrp ietf-ipv6-spec-07-mode コマンド，vrrp ietf-unified-spec-02-mode コマンド設定時に msec パラ

メータを指定していない場合は，40 より大きな値を指定しても無効となり，デフォルトの 1 秒で動作します。

2. msec パラメータは，vrrp ietf-ipv6-spec-07-mode コマンドまたは vrrp ietf-unified-spec-02-mode コマンドが設定されている場合，有効になります。
   msec パラメータが設定され，vrrp ietf-ipv6-spec-07-mode コマンドかつ vrrp ietf-unified-spec-02-mode コマンドが設定されていない場合，デフォルトの 1 秒で動作します。
3. vrrp follow コマンドを設定している場合，本設定は無効です。
4. チャネルグループ上の VLAN で仮想ルータが動作している場合，msec パラメータに小さい値を指定すると，チャネルグループに属するポートの回線障害に伴って，一時的に複数のマスタルータが存在することがあります。チャネルグループのポート切り替えが完了すると自動的にマスタルータは一つになります。

［関連コマンド］

なし

vrrp timers non-preempt-swap

自動切り戻し抑止中に切り戻しを行う場合の，切り戻しを抑止する時間を設定します。

[入力形式]

情報の設定・変更

vrrp <vrid> timers non-preempt-swap <seconds>

情報の削除

no vrrp <vrid> timers non-preempt-swap

[入力モード]

(config-if)

[パラメータ]

<vrid>

仮想ルータの 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 ～ 255

<seconds>

自動切り戻し抑止中に切り戻しを行う場合の，切り戻しを抑止する時間を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 ～ 65535

[コマンド省略時の動作]

自動切り戻し抑止中に切り戻しを行う場合の，切り戻しを抑止する時間は 0 秒です。切り戻しを抑止しません。

[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. vrrp follow コマンドを設定している場合，本設定は無効です。

[関連コマンド]

vrrp preempt

vrrp track

仮想ルータにトラッキング機能を設定します。

［入力形式］

情報の設定・変更

vrrp <vrid> track <track number> [{ priority | decrement } <priority>]

情報の削除

no vrrp <vrid> track <track number>

［入力モード］

(config-if)

［パラメータ］

<vrid>

仮想ルータの 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 ～ 255

<track number>

障害監視を行うために仮想ルータに割り当てる track 番号を指定します。

{priority | decrement} <priority>

トラッキング機能で障害検出時に仮想ルータに設定する優先度を決めるパラメータです。

priority <priority>

トラッキング機能で障害検出時に仮想ルータへ設定する優先度を 0 ～ 254 の範囲で指定します。また，仮想ルータの優先度（vrrp priority コマンドで指定）より小さい値を指定してください。仮想ルータの優先度以上の値を指定した場合は，本コマンドの指定は無効になって優先度 0 が使用されます。また，仮想ルータが IP アドレス所有者の場合も，本コマンドの指定は無効になって優先度 0 が使用されます。priority を指定した track は，仮想ルータごとに一つだけ設定できます。

decrement <priority>

トラッキング機能で障害検出時に仮想ルータの現在の優先度から減算する値を 1 ～ 255 の範囲で指定してください。decrement で指定した track は，仮想ルータごとに複数登録できます。

1. 本パラメータ省略時の初期値
   decrement と優先度 255 が使用されます
2. 値の設定範囲
   priority <priority> の場合，優先度の範囲は 0 ～ 254。
   decrement <priority> の場合，優先度から減算する値の範囲は 1 ～ 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. 本コマンドの priority パラメータを指定して仮想ルータに割り当てられる track 数は，仮想ルータ当たり 1 個です。
2. 本コマンドの priority パラメータを指定して仮想ルータに割り当てた track を，本コマンドの decrement パラメータに変更したい場合は，いったん本コマンドを削除してください。
3. 本コマンドの decrement パラメータを指定して仮想ルータに割り当てた track を，本コマンドの priority パラメータに変更したい場合は，いったんその仮想ルータに割り当てている track をすべて削除してください。
4. 本コマンドを設定された仮想ルータは，トラッキング機能で障害を検出し，仮想ルータの優先度が 0 となった場合，仮想ルータが設定されている IP インタフェースをダウンさせます。
5. vrrp follow コマンドを設定している場合，本設定は無効です。

［関連コマンド］

track interface

vrrp-vlan

VRRP 管理 VLAN として使用する VLAN を指定します。本装置に設定された仮想ルータがマスタへ遷移した際，本コマンドで指定した VRRP 管理 VLAN に対して，Flush Request フレーム（MAC アドレステーブルエントリのクリアを促すフレーム）を送信します。

[入力形式]

情報の設定

vrrp-vlan <vlan id>

情報の削除

no vrrp-vlan

[入力モード]

(config)

[パラメータ]

<vlan id>

VRRP 管理 VLAN として使用する 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
   詳細は ,「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

vrrp ip

vrrp ipv6

vrrp follow

20 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

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
   対象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
   udld

[コマンド省略時の動作]

対象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，対象ポートを 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 パラメータが指定されない場合，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指定します。回数に達した時に該当ポートを 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

[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

21 ストームコントロール

storm-control（global）
storm-control（interface）

storm-control（global）

ストームコントロール機能の対象とするフレーム種別を設定します。

[入力形式]

情報の設定

no storm-control broadcast
no storm-control multicast
no storm-control unicast

情報の削除

storm-control broadcast
storm-control multicast
storm-control unicast

[入力モード]

(config)

[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外にします。

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外にします。

unicast

ユニキャストフレームをストームコントロールの対象外にします。

[コマンド省略時の動作]

ブロードキャスト，マルチキャスト，ユニキャストフレームすべてをストームコントロール機能の対象にします。

[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. ブロードキャスト，マルチキャスト，ユニキャストのすべてをストームコントロールの対象外に設定すると，ストームコントロール機能は動作しなくなります。
2. ストームコントロール機能を使用するためには，upc-storm-control mode コマンドで upc-in-and-storm-control が設定されている必要があります。

[関連コマンド]

storm-control

upc-storm-control mode

storm-control（interface）

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。閾値を超えるフレームを受信してストームを検出したとき，ポートを inactive 状態にしたり，SNMP Trap を発行したり，ログメッセージを表示したりできます。また，ストーム検出後に受信したフレームが閾値を下回ったことによってストームの回復を検出し，SNMP Trap を発行したり，ログメッセージを表示したりできます。

［入力形式］

情報の設定・変更

storm-control level { <rate> | bps {<kbit/s> | <Mbit/s>M | <Gbit/s>G }}

情報の設定

storm-control action inactivate
storm-control action trap
storm-control action log

情報の削除

no storm-control level
no storm-control action inactivate
no storm-control action trap
no storm-control action log

［入力モード］

(config-if)

［パラメータ］

level { <rate> | bps {<kbit/s> | <Mbit/s>M | <Gbit/s>G }}

ストームコントロールを行う受信帯域の閾値を指定します。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。

<rate>

閾値を回線速度に対する割合（パーセント）で指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   0 ～ 100

bps {<kbit/s> | <Mbit/s>M | <Gbit/s>G }

閾値を帯域幅で指定します。

1. 本パラメータ省略時の初期値
   なし
2. 値の設定範囲
   設定範囲を次の表に示します。

表 21-1　ストームコントロール閾値の値の設定範囲

設定範囲		刻み値
G 単位	1G ～ 10G	1G ※1

設定範囲		刻み値
M 単位	1M ～ 10000M	1M ※1
k 単位	1000 ～ 10000000	100k ※2
	128 ～ 960	64k ※3

注※1　1G，1M は，それぞれ 1000000k，1000k 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（128，192，256，…，960）。

action inactivate

ストームの発生を検出した場合に，対象ポートを inactive 状態にします。

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，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。

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，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
   ストームの発生を検出した場合，ログメッセージを出力しません。

[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]

1. ストームコントロールは，対象フレームの帯域で制御され，フレーム数には関係しません。
2. 受信フレームが閾値を超えた場合，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 で指定した動作は，受信フレームの帯域が受信インタフェースに設定した storm-control level で設定した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。閾値を設定していない場合は storm-control action で指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 の送信先を設定しておく必要があり

ます。

6. 閾値を回線速度に対する割合で指定した場合の回線速度は，該当インタフェースで使用できる最大の速度（1 ギガビットイーサネットインタフェースの場合は 1Gbit/s，10 ギガビットイーサネットインタフェースの場合は 10Gbit/s）です。オートネゴシエーションやコンフィグレーションで最大速度よりも低い速度で動作している場合でも，ストームコントロールの閾値は最大速度に対する割合として動作します。
7. ストームコントロール機能を使用するためには，upc-storm-control mode コマンドで upc-in-and-storm-control が設定されている必要があります。
8. リンクアグリゲーションのポートに storm-control action を設定する場合，該当リンクアグリゲーションの全ポートに同じ設定を行ってください。
9. リンクアグリゲーションのポートに storm-control action inactivate を設定し，ストームを検出した場合，該当リンクアグリゲーションの全ポートを inactive 状態にします。
10. ストームコントロールを行う受信帯域の値に 0 を設定する場合，storm-control action を設定できません。

［関連コマンド］

snmp-server host

storm-control（global）

upc-storm-control mode

22 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 ループ検知機能における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 inactive 状態にします。

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 inactive 状態にします。

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，または 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. ポート種別を変更すると，次に示す情報がクリアされます。

- inactive 状態にするまでの L2 ループ検知フレーム受信数
- 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されません。

［関連コマンド］

loop-detection enable

loop-detection auto-restore-time

inactive 状態にしたポートを自動的に active 状態にするまでの時間を秒単位で指定します。

[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>

inactive 状態にしたポートを自動的に active 状態にする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
   60 ～ 86400

[コマンド省略時の動作]

inactive 状態に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，残り時間を一度クリアしたあと，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 ループ検知機能を有効にします。

［入力形式］

情報の設定・変更
　loop-detection enable id <loop detection id>

情報の削除
　no loop-detection enable

［入力モード］

(config)

［パラメータ］

id <loop detection id>

L2 ループ検知機能の ID を設定します。ネットワーク内の複数の本装置で L2 ループ検知機能を動作させる場合，ユニークな番号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 ～ 64

［コマンド省略時の動作］

L2 ループ検知機能を無効にします。

［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

loop-detection hold-time

inactive 状態にするまでの L2 ループ検知フレーム受信数の保持時間を秒単位で指定します。最後に L2 ループ検知フレームを受信したあと，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 inactive 状態にするまでの L2 ループ検知フレーム受信数はクリアされます。

[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>
　inactive 状態にするまでの L2 ループ検知フレーム受信数の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
　　1 ～ 86400

[コマンド省略時の動作]

inactive 状態にするまでの L2 ループ検知フレーム受信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状態でパラメータを変更した場合，L2 ループ検知フレーム受信数の保持時間が残っていれば，残り時間を一度クリアしたあと，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 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 ～ 3600

［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］

loop-detection enable

loop-detection threshold

ポートを inactive 状態にするまでの L2 ループ検知フレーム受信数を設定します。

[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 inactive 状態にするまでの L2 ループ検知フレーム受信数を指定します。

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 ～ 10000

[コマンド省略時の動作]

ポートを inactive 状態にするまでの L2 ループ検知フレーム受信数は 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状態でパラメータを変更した場合，受信済みの L2 ループ検知フレーム数を保持していれば，受信数を一度クリアしたあと，変更後の値が運用に反映されます。

[関連コマンド]

loop-detection enable

23 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

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指定します。

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。
   <name> には，ホスト名を 63 文字以内で指定します。使用できる文字については,「パラメータに指定できる値」を参照してください。
   <mac> には 0000.0000.0000 ～ feff.ffff.ffff の値を設定します。ただし，マルチキャスト MAC アドレス（先頭バイトの最下位ビットが 1 のアドレス）は設定できません。
   <id> には 0 ～ 65535 の値を設定します。

[コマンド省略時の動作]

no-present で動作します。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. no-present 以外のパラメータを指定し，ma name コマンドで str <strings> パラメータに 43 文字を超える文字列を指定した場合，指定したパラメータの先頭 1 文字が CCM に付けられます。

[関連コマンド]

ethernet cfm domain

ethernet cfm cc alarm-priority

CC で検知する障害レベルを設定します。設定した障害レベル以上の障害が検知対象になります。

［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 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

<priority>

CC で検知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
   設定値に対応する障害内容を次の表に示します。

表 23-1　設定値と障害内容

設定値	障害種別	コマンドでの表示	障害内容
0	none	-	障害を検知しない
1	DefRDICCM	RDI	障害フラグが ON の CCM を受信
2	DefMACstatus	PortState	受信 CCM 内に，ポートまたはインタフェース状態がダウンの情報有り
3	DefRemoteCCM	Timeout	リモート MEP からの CCM がタイムアウト

設定値	障害種別	コマンドでの表示	障害内容
4	DefErrorCCM	ErrorCCM	MEP の構成エラーや CCM 送信間隔不一致の CCM を受信
5	DefXconCCM	OtherCCM	MA が異なる CCM を受信

[コマンド省略時の動作]

障害レベル 2 以上を検知します。

[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 cc enable

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm cc alarm-reset-time

CC で連続して障害を検知する場合，再検知と見なす時間を設定します。障害検知後，本コマンドで設定した時間内に検知した障害は再検知と見なし，トラップは通知しません。

ただし，再検知の場合でも，現在検知している障害よりも障害レベルが高い障害を検知したときは，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

<time>

障害を再検知したと見なす時間を設定します。500 ミリ秒単位に切り上げた値で動作します。

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
   2500 ～ 10000（ミリ秒）

［コマンド省略時の動作］

再検知と見なす時間は 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]

なし

[関連コマンド]

ethernet cfm cc enable

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm cc alarm-start-time

CC で障害を検知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

<time>

障害検知時にトラップを通知するまでの時間を設定します。500 ミリ秒単位に切り上げた値で動作します。

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
   2500 〜 10000（ミリ秒）

[コマンド省略時の動作]

障害を検知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 cc enable

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

{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 または 10min

［コマンド省略時の動作］

CCM 送信間隔は 1 分です。

［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. CCM 送信間隔を初期値より短い時間に設定すると，装置の CPU 使用率が高くなり，通信に影響が出るおそれがあります。

［関連コマンド］

ethernet cfm cc enable

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

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

[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]

domain name

ethernet cfm cc enable

ma name

ma vlan-group

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

[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 mip

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 mep

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

{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。
   <vlan id> には，1 ～ 4095 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

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

<vlan id list>

該当の MA で使用する 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
   <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 を指定します。

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 ～ 4095
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

24 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 informs
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。また，SNMP の Set オペレーションによって SNMP マネージャから本名称を変更できます。SNMP の Set オペレーションによって本名称を変更した場合，その名称はコンフィグレーションに反映されます。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

ip domain lookup

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 no.> falling-threshold <value> falling-event-index <event no.> [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指定します。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指定します。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）で囲んで指定します。最大 63 文字で指定可能なオブジェクト識別子だけ有効です。また，指定するオブジェクトは，Integer，TimeTicks，Counter や Gauge タイプのオブジェクト識別子を指定してください。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。

<interval>

閾値チェックを行う時間間隔（秒）を指定します。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

{ delta | absolute }

閾値チェック方式を指定します。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>

上方閾値の値を指定します。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 no.>

上方閾値を超えたときのイベント方法の識別番号を指定します。イベント方法は，コンフィグレーションコマンドの event で指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 no.> にコンフィグレーションコマンドの event コマンドで指定した制御情報の情報識別番号（1 ～ 65535）

falling-threshold <value>

下方閾値の値を指定します。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 no.>

下方閾値を超えたときのイベント方法の識別番号を指定します。イベント方法は，コンフィグレーションコマンドの event で指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 no.> にコンフィグレーションコマンドの event コマンドで指定した制御情報の情報識別番号（1 ～ 65535）

owner <string>

本設定の設定者の識別情報を指定します。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。

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指定します。rising を指定した場合，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 を指定した場合，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 の値はコンフィグレーションで設定したイベントグループの情報識別番号を設定してください。
3. コンフィグレーションで設定したアラームグループと SNMP マネージャから Set で設定したアラームグループを合わせて，最大 128 エントリ設定できます。最大エントリを設定した状態で，コンフィグレーションにアラームグループを設定しても，追加したアラームグループは動作しません。不要な alarm 設定を削除してから，再設定してください。
4. SNMP マネージャから RMON alarmTable の Set を行った場合，コンフィグレーションには反映されません。
5. alarm のコンフィグレーション数が多い場合や，interval に設定した値が 60 秒以内である場合など，一部の alarm で MIB 情報を収集できなくなると alarm が動作しないことがあります。そのような状態では，alarmStatus の MIB 値は invalid(4) になります。このような状態になっているときは，interval 値を 60 秒より大きくするか，または不要な alarm 設定を削除してください。
6. interval 値が大きく設定されている場合，5. などの理由で，alarmStatus が valid(1) から invalid(4) になるまでしばらくは valid(1) で応答します（目安としては，interval 値の約半分の時間が掛かります）。

[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。

［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指定します。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指定します。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。

buckets <bucket number>

統計情報を格納する来歴エントリ数を指定します。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 を指定した場合，50 を指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）を指定します。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
2. 値の設定範囲
1 ～ 3600

[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. コンフィグレーションで設定したヒストリグループと SNMP マネージャから Set で設定したヒストリグループを合わせて，最大 32 エントリ設定できます。最大エントリを設定した状態で，コンフィグレーションにヒストリグループを設定しても，追加したヒストリグループは動作しません。不要な history 設定を削除してから，再設定してください。
3. SNMP マネージャから RMON historyControlTable の Set を行った場合，コンフィグレーションには反映されません。
4. RMON の history コンフィグレーションで設定した interface の該当する NIF が inactivate 状態の場合，inactivate 後の etherHistory 情報が取得できなくなります。このため，historyControlStatus 値は invalid(4) で応答します。ただし，interval 値が長く設定されている場合は，historyControlStatus が valid(1) から invalid(4) へ変化するまで時間が掛かります（目安は interval 値の半分の時間です）。

[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 no.> [log] [trap <community>] [description <string>] [owner <string>]

情報の削除

no rmon event <event no.>

［入力モード］

(config)

［パラメータ］

<event no.>

RMON イベントグループの制御情報の情報識別番号を指定します。本パラメータは RFC1757 の eventIndex に対応します。

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

log

アラーム（イベント）の方法を指定するパラメータで，アラームのログを残します。本パラメータは RFC1757 の eventType に対応します。

1. 本パラメータ省略時の初期値
   アラームのログを残しません
2. 値の設定範囲
   なし

trap <community>

アラーム（イベント）の方法を指定するパラメータで，<community> で指定したコミュニティに対して SNMP のトラップまたはインフォームを送信します。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
   トラップまたはインフォームを発行しません
2. 値の設定範囲
   trap およびコミュニティ名を設定します。
   <community> には 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。

description <string>

イベントの内容を文字列で指定します。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。

owner <string>

本設定の設定者の識別情報を指定します。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 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またはインフォームを送信するときは，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またはインフォーム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 ” を指定してください。
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またはインフォームを送信します。
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。
5. コンフィグレーションで設定したイベントグループと SNMP マネージャから Set で設定したイベントグループを合わせて，最大 16 エントリ設定できます。最大エントリを設定した状態で，コンフィグレーションにイベントグループを設定しても，追加したイベントグループは動作しません。不要な event 設定を削除してから，再設定してください。
6. SNMP マネージャから RMON eventTable の Set を行った場合，コンフィグレーションには反映されません。

[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。本コマンドで登録できるアドレスは最大 50 となります。

［入力形式］

情報の設定・変更

snmp-server community <community> [{ ro | rw }] [{<access list number> | <access list name>}] [vrf <vrf id>]

情報の削除

no snmp-server community <community> [vrf <vrf id>]

［入力モード］

(config)

［パラメータ］

<community>

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 }

指定したコミュニティ名称に属する指定した 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 を指定した場合，Get Request，GetNext Request を許可し，rw を指定した場合，Get Request，GetNext Request，Set Request を許可します。

1. 本パラメータ省略時の初期値
   ro
2. 値の設定範囲
   ro または rw

{<access list number> | <access list name>}

本コミュニティに対する許可を設定したアクセスリストを番号または名前で指定します。指定した {<access list number> | <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
   すべてのアクセスを許可します
2. 値の設定範囲
   <access list number> の場合は，1 ～ 99，1300 ～ 1999（10 進数）を指定します。
   <access list name> の場合は，31 文字以内の名前を指定します。
   詳細は，「パラメータに指定できる値」を参照してください。

vrf <vrf id>【OP-NPAR】

<vrf id> で指定された VRF からのアクセスを許可します。

1. 本パラメータ省略時の初期値
   グローバルネットワークからのアクセスを許可します。
2. 値の設定範囲
   <vrf id> に VRF ID を指定します。
   詳細は ,「パラメータに指定できる値」を参照してください。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

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 <contact>

情報の削除
　no snmp-server contact

[入力モード]

(config)

[パラメータ]

<contact>

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。また，SNMP の Set オペレーションによって SNMP マネージャから本名称を変更できます。SNMP の Set オペレーションによって本名称を変更した場合，その名称はコンフィグレーションに反映されます。本パラメータは RFC1213 の sysContact 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 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：企業コードと 0x80000000 とのビット OR

5 オクテット：4 固定

6 〜 32 オクテット：<engineid string> 設定値

装置に設定される SNMP エンジン ID は，運用コマンド snmp で参照できます。次に例を示します。

```
> snmp get snmpEngineID.0
Name: snmpEngineID.0
Value:80 00 FF FF 04 73 6E 6D 70 5F 54 6F 6B 79 6F 31
```

1. 本パラ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：企業コードと 0x80000000 とのビット OR

5 オクテット：128 固定

6 〜 9 オクテット：ランダム値

10 〜 13 オクテット：自動生成時のユニバーサルタイマ値

［通信への影響］

なし

[設定値の反映契機]

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 user コマンドで設定されたユーザ数が多い（最大 50 ユーザ）場合，snmp-server engineID local コマンドの設定／変更／削除に最大 20 秒程度の時間が掛かります。

[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。セキュリティレベル情報，snmp-server view コマンドで設定した SNMP ビュー情報で構成されるアクセス制御情報をグループ単位にまとめます。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 }

アクセス制御のセキュリティレベルを設定します。SNMP パケット受信時には，受信したパケットが本パラメータで設定したセキュリティレベルと一致しているかをチェックします。SNMP パケット送信時には，本パラメータで設定したセキュリティレベルで SNMP パケットを生成します。

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>

アクセス制御の Read ビュー名を設定します。次の PDU タイプの SNMP パケットを受信したとき，<view name> に指定した Read ビュー名が SNMP MIB ビュー情報に存在していれば，MIB ビューのチェックを行います。

・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>

アクセス制御の Write ビュー名を設定します。PDU タイプが SetRequest-PDU の SNMP パケットを受信したとき，<view name> に指定した Write ビュー名が SNMP MIB ビュー情報に存在していれば，MIB ビューのチェックを行います。

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>

アクセス制御の Notify ビュー名を設定します。トラップ（PDU タイプが SNMPv2-Trap-PDU の SNMP パケット）を送信するとき，<view name> に指定した Notify ビュー名が SNMP MIB ビュー情報に存在していれば，MIB ビューのチェックを行います。

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無効となりますので，ご注意ください。

[関連コマンド]

snmp-server engineID local

snmp-server view

snmp-server user

snmp-server host

snmp-server host

トラップまたはインフォーム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> [vrf <vrf id>] { traps | informs } <string> [version { 1 | 2c | 3 { noauth | auth | priv } }] [snmp] [{ospf_state | ospf_state_private }] [{ ospf_error | ospf_error_private }] [bgp] [vrrp] [rmon] [oadp] [air-fan] [power] [login] [memory] [system-msg] [standby_system] [temperature] [gsrp] [axrp] [frame_error_snd] [frame_error_rcv] [storm-control] [efmoam] [loop-detection] [cfm] [power-control] [static-route] [policy-base] [track-object]

情報の削除

no snmp-server host <manager address> [vrf <vrf id>]

［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。

vrf <vrf id>【OP-NPAR】

vrf definition コマンドの <vrf id> で指定された VRF にトラップまたはインフォームを発行します。

1. 本パラメータ省略時の初期値
   グローバルネットワークにトラップまたはインフォームを発行します。
2. 値の設定範囲
   <vrf id> に VRF ID を指定します。
   詳細は ,「パラメータに指定できる値」を参照してください。

{traps | informs}

SNMP マネージャに発行するイベント通知の種別を設定します。

- traps を指定した場合，トラップを発行します。SNMP マネージャは応答を返しません。
- informs を指定した場合，インフォームを発行します。SNMP マネージャに応答を要求するため，SNMP エージェントは応答を監視し，応答がない場合は再送します。SNMPv2C バージョンだけで使用できます。

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
   traps または informs のどちらかを指定します。

<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。

1. 本パラ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。

version { 1 | 2c | 3 { noauth | auth | priv }}

指定したコミュニティ名称に属する指定した IP アドレスの SNMP マネージャに対する送信バージョンを設定します。1 を指定した場合，SNMPv1 バージョンのトラップを，2c を指定した場合，SNMPv2C バージョンのトラップまたはインフォームを，3 を指定した場合，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 を指定した場合，認証なし，暗号化なしでトラップが送信されます。
- auth を指定した場合，認証あり，暗号化なしでトラップが送信されます。
- priv を指定した場合，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 のどれかを指定します。
   3 を指定した場合，さらに noauth，auth，または priv のどれかを指定します。

[snmp] [{ospf_state | ospf_state_private }] [{ ospf_error | ospf_error_private }] [bgp] [vrrp] [rmon] [oadp] [air-fan] [power] [login] [memory] [system-msg] [standby_system] [temperature] [gsrp] [axrp] [frame_error_snd] [frame_error_rcv] [storm-control] [efmoam] [loop-detection] [cfm] [power-control] [static-route] [policy-base] [track-object]

各パラメータを設定することによって，送信するトラップまたはインフォームを選択します。各パラメータを設定した際に送信するトラップまたはインフォームを次の表に示します。

表 24-1　パラメータとトラップ・インフォームの対応

パラメータ	トラップ・インフォーム
snmp	coldStart
	warmStart
	linkUp
	linkDown
	authenticationFailure
ospf_state	ospfVirtNbrStateChange
	ospfNbrStateChange
	ospfVirtIfStateChange
	ospfIfStateChange
ospf_state_private	axsOspfVirtNbrStateChange
	axsOspfNbrStateChange
	axsOspfVirtIfStateChange
	axsOspfIfStateChange

パラメータ	トラップ・インフォーム
ospf_error	ospfVirtIfConfigError
	ospfIfConfigError
	ospfVirtIfAuthFailure
	ospfIfAuthFailure
ospf_error_private	axsOspfVirtIfConfigError
	axsOspfIfConfigError
	axsOspfVirtIfAuthFailure
	axsOspfIfAuthFailure
bgp	bgpEstablished
	bgpBackwardTransition
vrrp	vrrpTrapNewMaster
	vrrpTrapAuthFailure
	vrrpTrapProtoError
rmon	risingAlarm
	fallingAlarm
oadp	axsOadpNeighborCachelastChangeTrap
air-fan	ax6700sAirFanStopTrap【AX6700S】 ax6600sAirFanStopTrap【AX6600S】 ax6300sAirFanStopTrap【AX6300S】
power	ax6700sPowerSupplyFailureTrap【AX6700S】 ax6600sPowerSupplyFailureTrap【AX6600S】 ax6300sPowerSupplyFailureTrap【AX6300S】
login	ax6700sLoginSuccessTrap【AX6700S】 ax6600sLoginSuccessTrap【AX6600S】 ax6300sLoginSuccessTrap【AX6300S】
	ax6700sLoginFailureTrap【AX6700S】 ax6600sLoginFailureTrap【AX6600S】 ax6300sLoginFailureTrap【AX6300S】
	ax6700sLogoutTrap【AX6700S】 ax6600sLogoutTrap【AX6600S】 ax6300sLogoutTrap【AX6300S】
memory	ax6700sMemoryUsageTrap【AX6700S】 ax6600sMemoryUsageTrap【AX6600S】 ax6300sMemoryUsageTrap【AX6300S】
system-msg	ax6700sSystemMsgTrap【AX6700S】 ax6600sSystemMsgTrap【AX6600S】 ax6300sSystemMsgTrap【AX6300S】
standby_system	ax6700sStandbySystemUpTrap【AX6700S】 ax6700sStandbyBsuUpTrap【AX6700S】 ax6700sStandbyNifUpTrap【AX6700S】 ax6600sStandbySystemUpTrap【AX6600S】 ax6600sStandbyNifUpTrap【AX6600S】 ax6300sStandbySystemUpTrap【AX6300S】

パラメータ	トラップ・インフォーム
	ax6700sStandbySystemDownTrap【AX6700S】 ax6700sStandbyBsuDownTrap【AX6700S】 ax6700sStandbyNifDownTrap【AX6700S】 ax6600sStandbySystemDownTrap【AX6600S】 ax6600sStandbyNifDownTrap【AX6600S】 ax6300sStandbySystemDownTrap【AX6300S】
temperature	ax6700sTemperatureTrap【AX6700S】 ax6600sTemperatureTrap【AX6600S】 ax6300sTemperatureTrap【AX6300S】
gsrp	ax6700sGsrpStateTransitionTrap【AX6700S】 ax6600sGsrpStateTransitionTrap【AX6600S】 ax6300sGsrpStateTransitionTrap【AX6300S】
axrp	ax6700sAxrpStateTransitionTrap【AX6700S】 ax6600sAxrpStateTransitionTrap【AX6600S】 ax6300sAxrpStateTransitionTrap【AX6300S】
frame_error_snd	ax6700sFrameErrorSendTrap【AX6700S】 ax6600sFrameErrorSendTrap【AX6600S】 ax6300sFrameErrorSendTrap【AX6300S】
frame_error_rcv	ax6700sFrameErrorReceiveTrap【AX6700S】 ax6600sFrameErrorReceiveTrap【AX6600S】 ax6300sFrameErrorReceiveTrap【AX6300S】
storm-control	ax6700sStormDetectTrap【AX6700S】 ax6600sStormDetectTrap【AX6600S】 ax6300sStormDetectTrap【AX6300S】
	ax6700sStormPortInactivateTrap【AX6700S】 ax6600sStormPortInactivateTrap【AX6600S】 ax6300sStormPortInactivateTrap【AX6300S】
	ax6700sStormRecoverTrap【AX6700S】 ax6600sStormRecoverTrap【AX6600S】 ax6300sStormRecoverTrap【AX6300S】
efmoam	ax6700sEfmoamUdldPortInactivateTrap【AX6700S】 ax6600sEfmoamUdldPortInactivateTrap【AX6600S】 ax6300sEfmoamUdldPortInactivateTrap【AX6300S】
	ax6700sEfmoamLoopDetectPortInactivateTrap【AX6700S】 ax6600sEfmoamLoopDetectPortInactivateTrap【AX6600S】 ax6300sEfmoamLoopDetectPortInactivateTrap【AX6300S】
loop-detection	ax6700sL2ldLinkDown【AX6700S】 ax6600sL2ldLinkDown【AX6600S】 ax6300sL2ldLinkDown【AX6300S】
	ax6700sL2ldLinkUp【AX6700S】 ax6600sL2ldLinkUp【AX6600S】 ax6300sL2ldLinkUp【AX6300S】
	ax6700sL2ldLoopDetection【AX6700S】 ax6600sL2ldLoopDetection【AX6600S】 ax6300sL2ldLoopDetection【AX6300S】
cfm	dot1agCfmFaultAlarm
power-control	ax6700sPowerControlModeChangeStartTrap【AX6700S】 ax6600sPowerControlModeChangeStartTrap【AX6600S】

パラメータ	トラップ・インフォーム
	ax6700sPowerControlModeChangeCompleteTrap【AX6700S】 ax6600sPowerControlModeChangeCompleteTrap【AX6600S】
static-route	axsStaticGatewayStateChange
	axsStaticIpv6GatewayStateChange
policy-base	axsPolicyBaseRoutingRouteChange
	axsPolicyBaseSwitchingRouteChange
track-object	axsTrackObjectStateChange

snmp

coldStart，warmStart，linkDown，linkUp，authenticationFailure のトラップまたはインフォームを送信します。

{ospf_state | ospf_state_private}

OSPF の状態変更を通知するトラップまたはインフォームを送信します。ospf_state を指定した場合，RFC に準拠した標準のトラップまたはインフォームを発行します。ただし，OSPF ドメイン分割を行っている場合，ドメイン番号が最小のドメイン以外は，プライベートのトラップまたはインフォームを発行します。ospf_state_private を指定した場合，すべての OSPF ドメインでプライベートのトラップまたはインフォームを発行します。
発行するトラップまたはインフォームを次に示します。

表 24-2　パラメータごとの発行トラップ・インフォーム（OSPF の状態変更通知）

パラメータ	発行トラップ・インフォーム
ospf_state	ドメイン番号が最小のドメイン • ospfVirtIfStateChange • ospfNbrStateChange • ospfVirtNbrStateChange • ospfIfStateChange ドメイン番号が最小でないドメイン • axsOspfVirtIfStateChange • axsOspfNbrStateChange • axsOspfVirtNbrStateChange • axsOspfIfStateChange
ospf_state_private	全ドメイン • axsOspfVirtIfStateChange • axsOspfNbrStateChange • axsOspfVirtNbrStateChange • axsOspfIfStateChange

{ospf_error | ospf_error_private}

OSPF のエラーパケット受信を通知するトラップまたはインフォームを送信します。ospf_error を指定した場合，RFC に準拠した標準のトラップまたはインフォームを発行します。ただし，OSPF ドメイン分割を行っている場合，ドメイン番号が最小のドメイン以外は，プライベートのトラップまたはインフォームを発行します。ospf_error_private を指定した場合，すべての OSPF ドメインでプライベートのトラップまたはインフォームを発行します。
発行するトラップまたはインフォームを次に示します。

表 24-3　パラメータごとの発行トラップ・インフォーム（OSPF のエラーパケット受信通知）

パラメータ	発行トラップ・インフォーム
ospf_error	ドメイン番号が最小のドメイン • ospfIfConfigError • ospfVirtIfConfigError • ospfIfAuthFailure • ospfVirtIfAuthFailure ドメイン番号が最小でないドメイン • axsOspfIfConfigError • axsOspfVirtIfConfigError • axsOspfIfAuthFailure • axsOspfVirtIfAuthFailure
ospf_error_private	全ドメイン • axsOspfIfConfigError • axsOspfVirtIfConfigError • axsOspfIfAuthFailure • axsOspfVirtIfAuthFailure

bgp

BGP リンク確立と切断のトラップまたはインフォームを送信します。

vrrp

vrrp の状態が変化したときのトラップまたはインフォームを送信します。

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またはインフォームを送信します。

oadp

OADP 隣接ノードに関する情報が更新されたときにトラップまたはインフォームを送信します。

air-fan

ファンがストップしたときにトラップまたはインフォームを送信します。

power

一つの電源に障害発生したときにトラップまたはインフォームを送信します。

login

ログインの成功，失敗，ログアウトの発生時にトラップまたはインフォームを送信します。

memory

BCU，CSU または MSU のメモリが不足したときにトラップまたはインフォームを送信します。

system-msg

システムメッセージを出力したときのトラップまたはインフォームを送信します。

standby_system

- AX6700S の場合
  待機系 BCU，BSU，または NIF の動作状態が，稼働中から稼働中以外，または稼働中以外から稼働中となった場合に，トラップまたはインフォームを送信します。
- AX6600S の場合
  待機系 CSU または NIF の動作状態が，稼働中から稼働中以外，または稼働中以外から稼働中になった場合に，トラップまたはインフォームを送信します。
- AX6300S の場合
  待機系 MSU の動作状態が，稼働中から稼働中以外，または稼働中以外から稼働中になった場

合に，トラップまたはインフォームを送信します。

temperature
温度状態の変化のトラップを送信します。

gsrp
GSRP 状態が変化したときにトラップまたはインフォームを送信します。

axrp
リングの障害監視状態が変化したときにトラップまたはインフォームを送信します。

frame_error_snd
フレーム受信エラー発生時のトラップまたはインフォームを送信します。

frame_error_rcv
フレーム送信エラー発生時のトラップまたはインフォームを送信します。

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またはインフォームを送信します。

efmoam
片方向リンク障害検出時のトラップまたはインフォームを送信します。

loop-detection
L2 ループ検知時のトラップまたはインフォームを送信します。

cfm
CC で障害検知のトラップまたはインフォームを送信します。

power-control【AX6700S】【AX6600S】
スケジューリングまたはトラフィック量による省電力機能による電力制御モード変更開始と電力制御モード変更完了のトラップまたはインフォームを送信します。

static-route
スタティックの動的監視機能を使用しているゲートウェイの状態が遷移した場合にトラップまたはインフォームを発行します。

policy-base
ポリシーベースルーティングの経路情報，またはポリシーベーススイッチングの送信先インタフェース情報に変化があった場合に，トラップまたはインフォームを送信します。

track-object
ポリシーベースルーティングのトラッキング機能でのトラック状態が変わったときのプライベート MIB 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またはインフォームを発行しません
2. 値の設定範囲
   snmp，ospf_state または ospf_state_private，ospf_error または ospf_error_private，bgp，vrrp，rmon，oadp，air-fan，power，login，memory，system-msg，standby_system，temperature，gsrp，axrp，frame_error_snd，frame_error_rcv，storm-control，efmoam，loop-detection，cfm，power-control，static-route，policy-base，track-object

［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. version に 3 を設定していて，snmp-server user コマンドで設定されていないセキュリティユーザ名を本コマンドに設定した場合，本コマンドに設定したセキュリティユーザの情報は無効となりますので，ご注意ください。

[関連コマンド]

snmp-server engineID local

snmp-server view

snmp-server user

snmp-server group

snmp-server informs

インフォームの送信条件を設定します。本設定は，snmp-server host コマンドで informs パラメータを設定した SNMP マネージャに対して有効です。

［入力形式］

情報の設定・変更

snmp-server informs [retries <retries>] [timeout <seconds>] [pending <pending>]

情報の削除

no snmp-server informs

［入力モード］

(config)

［パラメータ］

retries <retries>

SNMP マネージャに対するインフォームの最大再送回数を設定します。0 を設定した場合は再送しません。

1. 本パラメータ省略時の初期値
   3
2. 値の設定範囲
   0 ～ 100

timeout <seconds>

SNMP マネージャに対するインフォームのタイムアウト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
   30
2. 値の設定範囲
   1 ～ 21474835

pending <pending>

本装置が同時に保持できるインフォームイベントの最大数を設定します。SNMP マネージャからの応答がない場合にインフォームイベントを保持します。最大数を超える場合は古いものから順に廃棄します。

1. 本パラメータ省略時の初期値
   25
2. 値の設定範囲
   1 ～ 21000

［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]

なし

[関連コマンド]

snmp-server host

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 <location>

情報の削除
　no snmp-server location

[入力モード]

(config)

[パラメータ]

<location>

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。また，SNMP の Set オペレーションによって SNMP マネージャから本名称を変更できます。SNMP の Set オペレーションによって本名称を変更した場合，その名称はコンフィグレーションに反映されます。本パラメータは RFC1213 の sysLocation 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

トラップまたはインフォーム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>]

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 24-4　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 • 系切替したとき
unlimited_coldstart_trap	• 装置を起動したとき • コンフィグレーションの変更によって VLAN の IP アドレスを追加，削除，変更したとき • copy コマンドによってランニングコンフィグレーションを変更したとき • set clock コマンドで時間を変更したとき • 系切替したとき

1. 本パラメータ省略時の初期値
   limited_coldstart_trap
2. 値の設定範囲
   limited_coldstart_trap または unlimited_coldstart_trap

link_trap_bind_info {private | standard}

linkDown トラップと linkUp トラップ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 linkDown トラップと linkUp トラップの発行の際，付加する MIB を次の表に示します。

表 24-5　パラメータごとの linkDown トラップと linkUp トラップ発行時に付加する MIB

パラメータ	link up/down Trap 発行時に付加する MIB
private	• (SNMPv1/SNMPv2C 共通) ifIndex，ifDescr，ifType
standard	• (SNMPv1 の場合) ifIndex • (SNMPv2C 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>

プライベートトラップまたはインフォームのうち，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。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 24-6　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。
7	SOFTWARE 部障害以上のシステムメッセージトラップを送信します。
6	NIF 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	待機系 BCU，待機系 BSU，待機系 CSU，待機系 MSU 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
注　<Level> に 1 ～ 3 の値を指定した場合，3 を指定したときと同じ動作になります。

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 アドレスを指定します。Trap-PDU 内に agent address フィールドを持つのは SNMPv1 形式だけのため，本コマンドで指定したアドレスは SNMPv1 のトラップに適用されます。
なお，本パラメータはグローバルネットワークに発行されるトラップにだけ適用されます。

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，interface loopback に IPv4 アドレス設定されているときはそのアドレスが agent address に使用されます。設定されていない場合トラップ通知フレーム内の agent address の値として最若番の ifIndex 番号を持つインタフェースの IPv4 アドレスが使用されます。ただし，対象となるインタフェースはマネージメントポートおよび VLAN です。装置に IPv4 アドレスが設定されていない場合は，0.0.0.0 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）を指定します。

[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。

[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，認証プロトコルと暗号プロトコルを設定します。暗号プロトコルは，認証プロトコルを設定していないと設定できません。認証プロトコルと暗号プロトコルの組み合わせを次の表に示します。

表 24-7　認証プロトコルと暗号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	暗号プロトコル
1	なし	なし
2	MD5 または SHA	なし
3	MD5 または SHA	DES

[入力形式]

情報の設定・変更

snmp-server user <user name> <group name> v3 [auth { md5 | sha } <authentication password> [priv des <privacy password>]] [vrf <vrf id>]

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 } <authentication password> [priv des <privacy password>]]

auth { md5 | sha } <authentication password>

認証プロトコルおよび認証パスワードを指定します。
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。

priv des <privacy password>

暗号プロトコルおよび暗号パスワードを指定します。

1. 本パラメータ省略時の初期値
   auth 以降を省略した場合，認証プロトコルを使用しない設定になります。
   priv des 以降を省略した場合，暗号プロトコルを使用しない設定になります。
2. 値の設定範囲
   v3 auth md5 <authentication password>，v3 auth sha <authentication password>，v3 auth md5 <authentication password> priv des <privacy password> または v3 auth sha <authentication password> priv des <privacy password>
   <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。

vrf <vrf id>【OP-NPAR】

<vrf id> で指定された VRF からのアクセスを許可します。

1. 本パラメータ省略時の初期値
   グローバルネットワークからのアクセスを許可します。
2. 値の設定範囲
   <vrf id> に VRF ID を指定します。
   詳細は ,「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. snmp-server group コマンドで設定されていないセキュリティグループ名を本コマンドに設定した場合，本コマンドに設定したセキュリティグループの情報は無効となりますので，ご注意ください。

[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。MIB ビュー情報は，SNMP パケットの PDU に含まれる Variable Bindings のオブジェクト ID のチェックに使用されます。MIB ビューは一つまたは複数のサブツリーで構成されます。サブツリーは，オブジェクト ID とビュータイプの組み合わせで設定します。本コマンドで作成した MIB ビューは snmp-server group コマンドで使用します。

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 24-8　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	装置当たり 50 エントリ
2	サブツリー	MIB ビュー当たり 30 エントリ
3		装置当たり 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 をドット記法で指定します。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（*）を指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 を指定します。サブツリーを MIB ビューから除く場合は excluded 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
included または excluded のどちらかを指定します。

[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. 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（*）を指定すると，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 を指定すると，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。
（例）

```
(config)# show snmp-server
snmp-server view "READ_VIEW" 1.0.1.1 included
snmp-server view "READ_VIEW" 1.1.1.1 excluded
(config)# snmp-server view "READ_VIEW" 1.*.1.1 included
(config)# show snmp-server
snmp-server view "READ_VIEW" 1.*.1.1 included
snmp-server view "READ_VIEW" 1.1.1.1 excluded
(config)# no snmp-server view "READ_VIEW" 1.0.1.1
(config)# show snmp-server
snmp-server view "READ_VIEW" 1.1.1.1 excluded
```

[関連コマンド]

snmp-server engineID local

snmp-server user

snmp-server group

snmp-server host

snmp trap link-status

回線がリンクアップまたはダウンした場合に，トラップまたはインフォーム（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］

トラップまたはインフォーム（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

25 ログ出力機能

logging email
logging email-event-kind
logging email-from
logging email-interval
logging email-server
logging event-kind
logging facility
logging host
logging syslog-dump
logging trap

logging email

ログ情報を E-Mail で出力するための E-Mail アドレスを設定します。本コマンドでは最大 64 エントリを設定できます。

[入力形式]

情報の設定
　logging email <e-mail address>

情報の削除
　no logging email <e-mail address>

[入力モード]

(config)

[パラメータ]

<e-mail address>

E-Mail 送信先のメール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
   255 文字以内の英数字，－（ハイフン），＿（アンダースコア），.（ドット），@（アットマーク）だけ使用できます。

[コマンド省略時の動作]

なし

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. あらかじめ logging email-server コマンドでメール配送先の SMTP サーバを設定しておく必要があります。
2. あらかじめ DNS リゾルバ機能に関連する設定をしておく必要があります。
3. 指定したメールアドレスが送信先 SMTP サーバに設定されているものと一致することを十分ご確認ください。
4. E-Mail の送信に失敗した場合，当該メールはそのまま廃棄されます。
5. ループバックインタフェースに IP アドレスが設定されている場合，SMTP サーバとの通信時の送信元 IP アドレスとしてその IP アドレスを使用します。
6. メールアドレス内に@（アットマーク）を使用する場合，メールアドレス先頭や末尾に設定しないでください。また，複数設定もしないでください。

[関連コマンド]

logging email-server

hostname

ip domain name

ip name-server

ip domain lookup

logging email-event-kind

E-Mail で出力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 email-event-kind <event kind>

情報の削除
　no logging email-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，rtm，err，evt，mrp，mr6，aut，acl，dsn，tro の中から指定します。

[コマンド省略時の動作]

イベント種別は「evt」および「err」となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドで設定したイベント種別は，ログ E-Mail 情報で指定されたすべての E-Mail アドレス宛に対して適用されます。
2. 本コマンドでイベント種別を設定した場合，デフォルトのイベント種別（evt，err）は無効になり，設定したイベント種別だけが有効になります。

[関連コマンド]

logging email

logging email-from

ログ情報を E-Mail で出力する E-Mail の送信元を設定します。

[入力形式]

情報の設定・変更
　logging email-from <e-mail address>

情報の削除
　no logging email-from

[入力モード]

(config)

[パラメータ]

<e-mail address>

E-Mail 送信元のメール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
   255 文字以内の英数字，－（ハイフン），＿（アンダースコア），.（ドット），@（アットマーク）だけ使用できます。

[コマンド省略時の動作]

E-Mail 送信元は「装置名 <nobody>」となります。ここで装置名は，hostname コマンドで指定した名称です。

[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. 本コマンドで設定した E-Mail 送信元は，ログ E-Mail 情報で指定されたすべての E-mail アドレス宛に対して適用されます。
2. メールアドレス内に@（アットマーク）を使用する場合，メールアドレス先頭や末尾に設定しないでください。また，複数設定もしないでください。

[関連コマンド]

logging email

logging email-interval

ログ情報を E-Mail で出力するための送信間隔を設定します。

[入力形式]

情報の設定・変更
　logging email-interval <seconds>

情報の削除
　no logging email-interval

[入力モード]

(config)

[パラメータ]

<seconds>

E-Mail の送信間隔を指定します。

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 ～ 3600（秒）

[コマンド省略時の動作]

E-Mail 送信間隔は「1」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 E-Mail 送信間隔は，ログ E-Mail 情報で指定されたすべての E-mail アドレス宛に対して適用されます。

[関連コマンド]

logging email

logging email-server

ログ情報を E-Mail で出力するために，SMTP サーバの情報を設定します。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

logging email-server {<host name> | <ip address>} [port <port number>]

情報の削除

no logging email-server {<host name> | <ip address>}

[入力モード]

(config)

[パラメータ]

{<host name> | <ip address>}

SMTP サーバのホスト名または IP 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
   <host name>
   ホスト名を 64 文字以内で指定します。使用できる文字については，「パラメータに指定できる値」を参照してください。
   <ip address>
   IPv4 アドレスをドット記法で指定します。

port <port number>

SMTP 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
   25
2. 値の設定範囲
   0 ～ 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. 指定した SMTP サーバ情報（ホスト名または IP アドレス，ポート番号）が接続先の SMTP サーバに設定されているものと一致しているかどうか十分に確認してください。E-Mail 送信時に，SMTP サーバとの接続に失敗した場合，当該メールはそのまま廃棄されます。
2. 本機能は IPv4 でだけ使用できます。そのため，SMTP サーバに ipv6 host コマンドで IPv6 アドレス

だけ設定されているホスト名を指定した場合，当該サーバ宛て E-Mail は廃棄されます。

3. ホスト名として localhost を設定できません。
4. ホスト名は大文字と小文字を区別しません。
5. IPv4 アドレスとして 127.*.*.* を設定できません。
6. IPv4 アドレスとしてクラス D およびクラス E のアドレスを指定できません。
7. 一度に大量のログ情報が発生した場合，E-Mail 情報に抜けが発生することがあります。

［関連コマンド］

ip host

logging email

hostname

ip domain name

ip name-server

ip domain lookup

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，rtm，err，evt，mrp，mr6，aut，acl，dsn，tro の中から指定します。

[コマンド省略時の動作]

イベント種別は「evt」および「err」となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドで設定したイベント種別は，ログ host 情報で指定されたすべての出力先に対して適用されます。
2. 本コマンドでイベント種別を設定した場合，デフォルトのイベント種別（evt，err）は無効になり，設定したイベント種別だけが有効になります。

[関連コマンド]

logging host

logging facility

ログ情報を syslog インタフェースで出力するためのファシリティを設定します。

[入力形式]

情報の設定・変更
　logging facility <facility>

情報の削除
　no logging facility

[入力モード]

(config)

[パラメータ]

<facility>

　syslog のファシリティを指定します。

　1. 本パラメータ省略時の初期値
　　省略できません
　2. 値の設定範囲
　　local0，local1，local2，local3，local4，local5，local6，local7 のどれか一つを指定します。

[コマンド省略時の動作]

ファシリティは「local0」となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

1. 本コマンドで設定したファシリティは，ログ host 情報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 20 エントリの設定ができます。

［入力形式］

情報の設定

logging host <host name> [no-date-info]
logging host { <ip address> | <ipv6 address> } [vrf <vrf id>] [no-date-info]

情報の削除

no logging host <host name>
no logging host { <ip address> | <ipv6 address> } [vrf <vrf id>]

［入力モード］

(config)

［パラメータ］

<host name>

ログ出力先の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
   ホスト名を 64 文字以内で指定します。使用できる文字については，「パラメータに指定できる値」を参照してください。

{ <ip address> | <ipv6 address> }

ログ出力先の IPv4 アドレスまたは 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
   <ip address>
   IPv4 アドレスをドット記法で指定します。
   <ipv6 address>
   IPv6 アドレスをコロン記法で指定します。

vrf <vrf id>【OP-NPAR】

vrf definition コマンドの <vrf id> パラメータで指定した VRF にログ情報を送信します。

1. 本パラメータ省略時の初期値
   グローバルネットワークにログ情報を送信します。
2. 値の設定範囲
   <vrf id> に VRF ID を指定します。
   詳細は，「パラメータに指定できる値」を参照してください。

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，付加情報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. ループバックインタフェースに IP アドレスが設定されている場合，syslog 情報の送信元 IP アドレスとしてその IP アドレスを使用します。
3. ホスト名として localhost は指定できません。
4. ホスト名は大文字と小文字を区別しません。
5. IPv4 アドレスとして 127.*.*.* を設定できません。
6. IPv4 アドレスとしてクラス D およびクラス E のアドレスを設定できません。
7. IPv6 アドレスとしては，グローバルアドレスおよびサイトローカルアドレスが指定できます。
8. 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。
9. 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。
10. 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。

[関連コマンド]

ip host

ipv6 host

hostname

ip domain name

ip name-server

ip domain lookup

logging syslog-dump

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（/usr/var/log/system.log），種別ログ（/usr/var/log/error.log）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. 本設定がされている場合でも，本装置を起動する際に出力する起動ログと起動要因ログは内蔵フラッシュメモリに保存します。
4. 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 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
   指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 25-1　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，ログ host 情報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

26 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 30.1.3(2)(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（NextHop など）の送信を許容します。

gateway

ゲートウェイ情報（AS 番号など）の送信を許容します。

user

ユーザ情報（TACACS/RADIUS 情報など）の送信を許容します。

url

URL 情報（URL 情報など）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。

[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]

なし

[関連コマンド]

なし

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]

なし

[関連コマンド]

なし

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設定されている MTU 長（バイト）以下の値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
   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　30.1.3(2)(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 26-1　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
   1，2，8，32，128，512，2048，8192，32768，131072，524288，2097152，8388608，33554432，134217728，536870912
   1 または式（2 × 4 ^ n）の n に 0 ～ 14 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 26-2　サンプリング間隔繰り上げ表」に示します。

表 26-1　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
4kpps 以下	8	
16kpps 以下	32	
64kpps 以下	128	100Mbit/s イーサネット× 1 本
256kpps 以下	512	
1Mpps 以下	2048	1Gbit/s イーサネット× 1 本
4Mpps 以下	8192	10Gbit/s イーサネット× 1 本
16Mpps 以下	32768	
64Mpps 以下	131072	1Gbit/s イーサネット× 48 本
256Mpps 以下	524288	
1Gpps 以下	2097152	

表 26-2　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
1	1
2	2
3 ～ 8	8
9 ～ 32	32
33 ～ 128	128
129 ～ 512	512
513 ～ 2048	2048
2049 ～ 8192	8192
8193 ～ 32768	32768
32769 ～ 131072	131072
131073 ～ 524288	524288
524289 ～ 2097152	2097152
2097153 ～ 8388608	8388608
8388609 ～ 33554432	33554432
33554433 ～ 134217728	134217728
134217729 ～ 536870912	536870912

（例）

<sample count> に 1000 が指定された場合は，2048（=2 × 4 ^ 5）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 536870912（=2 × 4 ^ 14）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. sflow forward コマンドで egress 指定を利用している場合は，サンプリング間隔は 2 以上でだけ設定できます。

[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]

本コマンドを指定しなかった場合，次の優先度に従い IP アドレスが設定されます。同様に，指定した IP アドレス形式が sflow destination コマンドで指定したアドレスタイプと異なっている場合も，次の優先度に従い IP アドレスが設定されます。

優先度 1

loopback アドレス（コンフィグレーションコマンドで設定している場合）

優先度 2

本装置のポートに割り付けられている IP アドレスから自動的に割り当てます。

[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. 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，本装置のポート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

27 LLDP

lldp enable
lldp hold-count
lldp interval-time
lldp run

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指定します。

[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 コマンドで指定した値に対する倍率で指定します。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指定します。

[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
   5 ～ 32768

[コマンド省略時の動作]

本装置が送信する LLDP フレームの送信間隔は 30 秒となります。

[通信への影響]

なし

[設定値の反映契機]

設定値更新後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

lldp run

lldp run

LLDP 機能を有効にします。

[入力形式]

情報の設定
　lldp run

情報の削除
　no lldp run

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

LLDP 機能は無効となります。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後，すぐに運用に反映されます。

[注意事項]

なし

[関連コマンド]

なし

28 OADP

oadp cdp-listener
oadp enable
oadp hold-time
oadp ignore-vlan
oadp interval-time
oadp run

oadp cdp-listener

本装置で CDP 受信機能を有効にするかどうかを指定します。

[入力形式]

情報の設定
　oadp cdp-listener

情報の削除
　no oadp cdp-listener

[入力モード]

(config)

[パラメータ]

なし

[コマンド省略時の動作]

CDP 受信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

oadp enable

ポートおよびリンクアグリゲーションで OADP 機能を有効にします。

[入力形式]

情報の設定
　oadp enable

情報の削除
　no oadp 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]

1. リンクアグリゲーションを構成しているポートに対して設定しても OADP 機能は動作しません。リンクアグリゲーション単位での動作となります。

[関連コマンド]

oadp run

oadp cdp-listener

oadp hold-time

本装置が送信する OADP フレームに対して隣接装置が保持する時間を指定します。

[入力形式]

情報の設定・変更
　oadp hold-time <seconds>

情報の削除
　no oadp hold-time

[入力モード]

(config)

[パラメータ]

<seconds>

本装置が送信する OADP フレームに対して，隣接装置が保持する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
   10 ～ 255

[コマンド省略時の動作]

本装置が送信する OADP フレームに対する隣接装置が保持する時間は，oadp interval-time コマンドで設定した値の 3 倍の値になります。3 倍の値が 255 秒を超える場合は 255 秒になります。

oadp interval-time コマンドも省略されている場合は，180 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. oadp interval-time コマンドよりも oadp hold-time コマンドの値が大きくなければなりません。

[関連コマンド]

oadp run

oadp ignore-vlan

指定したVLAN IDから受信するOADPフレームを無視する場合に指定します。

[入力形式]

情報の設定・変更
　oadp ignore-vlan <vlan id list>

情報の削除
　no oadp ignore-vlan

[入力モード]

(config)

[パラメータ]

<vlan id list>

　OADPフレームを無視する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。

[コマンド省略時の動作]

すべてのVLAN IDからのOADPフレームを受け付けます。

[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]

なし

[関連コマンド]

oadp run

oadp interval-time

本装置が送信する OADP フレームの送信間隔を指定します。

[入力形式]

情報の設定・変更
　oadp interval-time <seconds>

情報の削除
　no oadp interval-time

[入力モード]

(config)

[パラメータ]

<seconds>

本装置が送信する OADP フレームの送信間隔を秒単位で指定します。実際には，指定した値の 3 分の 2 から 2 分の 3 の範囲のランダムな間隔で送信します。

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
   5 ～ 254

[コマンド省略時の動作]

OADP フレームの送信間隔は 60 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. oadp interval-time コマンドよりも oadp hold-time コマンドの値が大きくなければなりません。

[関連コマンド]

oadp run

oadp run

OADP 機能を有効にします。

［入力形式］

情報の設定
　oadp run

情報の削除
　no oadp run

［入力モード］

(config)

［パラメータ］

なし

［コマンド省略時の動作］

OADP 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

29 ポートミラーリング

monitor option

monitor session

monitor option

ポートミラーリング機能のサンプリング係数を設定します。ミラーリングでサンプリング機能を指定することで，ミラーポートの帯域を低くできます。

[入力形式]

情報の設定・変更

monitor option sample <sample count>

情報の削除

no monitor option

[入力モード]

(config)

[パラメータ]

sample <sample count>

装置全体で使用するポートミラーリングのサンプリング係数を指定します。ミラーリングは，サンプリング係数で指定した数のフレームから 1 個のフレームを抜き出して行います。

1. 省略時の初期値
   省略できません
2. 値の設定範囲
   1，2，8，32，128，512，2048，8192，32768，131072，524288，2097152，8388608，33554432，134217728，536870912
   1 または式（2 × 4 ^ n）の n に 0 ～ 14 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次の表に示します。

表 29-1　サンプリング設定数値一覧

項番	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
1	1	1
2	2	2
3	3 ～ 8	8
4	9 ～ 32	32
5	33 ～ 128	128
6	129 ～ 512	512
7	513 ～ 2048	2048
8	2049 ～ 8192	8192
9	8193 ～ 32768	32768
10	32769 ～ 131072	131072
11	131073 ～ 524288	524288
12	524289 ～ 2097152	2097152
13	2097153 ～ 8388608	8388608
14	8388609 ～ 33554432	33554432
15	33554433 ～ 134217728	134217728

項番	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
16	134217729 ～ 536870912	536870912

（例）

<sample count> に 1000 が指定された場合は，2048（=2 × 4 ^ 5）で動作します。

[コマンド省略時の動作]

ポートミラーリング機能では，サンプリングしないで対象となる全フレームをミラーリングします。

[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. サンプリングは，指定した係数の数のフレームから 1 個の割合でランダムに行います。

[関連コマンド]

monitor session

monitor session

ポートミラーリング機能を設定します。

[入力形式]

情報の設定・変更

monitor session <session no.> source interface <interface id list> [{rx | tx | both}] destination interface {gigabitethernet | tengigabitethernet } <nif no.>/<port no.>

情報の変更

monitor session <session no.> { source interface add <interface id list> | source interface remove <interface id list> }

情報の削除

no monitor session <session no.>

[入力モード]

(config)

[パラメータ]

<session no.>

ポートミラーリングセッションの番号を指定します。

1. 本パラメータ省略時の初期値
   省略できません
2. 値の設定範囲
   1 ～ 191

source interface <interface id list>

ポートミラーリングのモニター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
   「パラメータに指定できる値」を参照してください。

source interface add <interface id list>

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。

source interface remove <interface id list>

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
   rx，tx または both

destination interface {gigabitethernet | tengigabitethernet} <nif no.>/<port no.>

ポートミラーリングのミラーポートを指定します。レイヤ 2 情報を設定したポートは指定できません。

{gigabitethernet | tengigabitethernet}

ミラーポートの種別を指定します。

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
   gigabitethernet または tengigabitethernet

<nif no.>/<port no.>

ミラーポートの NIF 番号，Port 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]

運用中の回線をミラーポートに指定した場合，その回線で通信できなくなります。モニターポートに指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. 複数のモニターポートに対して一つのミラーポートを設定できます。また，一つのモニターポートを送信ポートミラーリングセッションと受信ポートミラーリングセッションに設定できます。ただし，ポートミラーリングでコピーした受信フレームを複数のミラーポートに送信したり，コピーした送信フレームを複数のミラーポートに送信したりできません。
2. ポートミラーリングでコピーしたフレームの量が回線帯域を超えた場合，そのフレームは廃棄されます。
3. ミラーポートに設定したポートでは，通常のフレーム送受信はできません。
4. 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。すでにレイヤ 2 情報を設定済みのポートをミラーポートとして使用する場合は，該当インタフェースのレイヤ 2 情報を削除し

てからミラーポートに設定してください。
5. すでにミラーポートとして設定しているポートを，モニターポートには設定できません。
6. モニターポートまたはミラーポートに設定しているポートが収容されている NIF を，別の種類の NIF に差し替えたときは，該当するポートミラーリングセッションが削除されます。モニターポートにポートリストを指定している場合，そのリスト中に上記に該当するポートがあるときは，該当するポートミラーリングセッション全体が削除されます。

［関連コマンド］

なし

30 コンフィグレーション編集時のエラーメッセージ

30.1　コンフィグレーション編集時のエラーメッセージ

30.1 コンフィグレーション編集時のエラーメッセージ

30.1.1 共通

「コンフィグレーションコマンドレファレンス Vol.1　21.1.1 共通」を参照してください。

30.1.2 フローモード情報

表 30-1　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 mac mode.	次の理由のため，MAC モードの変更または設定ができません。 • 指定したインタフェースにアクセスリストまたは QoS フローリストが設定されているため，MAC モードの変更ができません。 MAC モードを変更する場合には，該当するインタフェースからアクセスリストの適用，QoS フローリストの適用をすべて削除してから行ってください。 • 指定した VLAN に属するイーサネットインタフェースにアクセスリストまたは QoS フローリストが設定されているため，MAC モードの設定ができません。 MAC モードを設定する場合には，指定した VLAN に属するイーサネットインタフェースからアクセスリストの適用，QoS フローリストの適用をすべて削除してから行ってください。
Cannot set the flow mac mode, because of fldm.	設定されているフロー配分パターンでは，MAC モードを設定できません。 MAC モードを設定する場合，フロー配分パターンには standard または extended を指定してください。

30.1.3 VLAN リスト情報

表 30-2　VLAN リストのエラーメッセージ

メッセージ	内容
Cannot change the VLAN list.	指定した VLAN リストはアクセスリストまたは QoS フローリストの検出条件に指定されているため，変更できません。 指定した VLAN リストはアクセスリストまたは QoS フローリストの検出条件に指定されているため，変更することによってフロー検出条件の VLAN ID が変更されました。 イーサネットインタフェースにアクセスリストまたは QoS フローリストを指定する場合には，該当リスト内のフロー検出条件の VLAN リストに含まれるすべての 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。
Cannot delete the VLAN list.	指定した VLAN リストはアクセスリストまたは QoS フローリストの検出条件に指定されているため，削除できません。 VLAN リストを削除する場合には，アクセスリストおよび QoS フローリストから該当する VLAN リストの指定を削除してから行ってください。
The maximum number of entries are exceeded.	エントリ数が収容条件を超えました。 指定した VLAN リストはアクセスリストまたは QoS フローリストの検出条件に指定されているため，変更することによってエントリ数が収容条件を超えました。 VLAN リストを変更する場合には，次に示す方法があります。 • アクセスリストおよび QoS フローリストから該当する VLAN リストの指定を削除後，変更する • 収容条件を超えない範囲に変更する

30.1.4 アクセスリスト情報

表 30-3 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 mac mode is set.	次の理由のため，アクセスリストを適用できません。 • VLAN に IPv4 アクセスリストまたは IPv6 アクセスリストを適用した場合 IPv4 アクセスリストまたは IPv6 アクセスリストは，MAC モードの場合に VLAN インタフェースのレイヤ 2 中継への適用はできません。 IPv4 アクセスリストまたは IPv6 アクセスリストを適用する場合には，MAC モードを削除してから行ってください。 • イーサネットインタフェースにアクセスリストを適用した場合 指定したイーサネットインタフェースが属する VLAN に MAC モードが設定されているため，アクセスリストを適用できません。 アクセスリストをイーサネットインタフェースに適用する場合には，指定イーサネットインタフェースが属するすべての VLAN から MAC モードを削除してください。
Cannot attach this list because IPv6 source address prefix-length exceeds 64.	フロー検出条件の送信元 IPv6 アドレスが上位 65 ビット以上の検出条件は適用できません。 次に示す条件を満たす必要があります。 • フロー検出条件の送信元 IPv6 アドレスのレングスは 64 以内で指定してください。 • フロー検出条件の送信元 IPv6 アドレスに host を指定しないでください。
Cannot change the configuration because there is an inconsistency between fwdm and policy based routing.	経路系テーブルエントリ配分パターンの設定内容と，ポリシーベースルーティングの設定内容に矛盾が生じているため，コンフィグレーションの変更ができません。 コンフィグレーションの内容を見直してください。
Cannot set policy based routing entry because specified destination address is invalid.	フィルタ条件で指定した宛先アドレスが，ポリシーベースルーティングでサポートしていないため，エントリが設定できません。 IPv4 ポリシーベースルーティング指定の場合，宛先アドレスには，マルチキャストアドレス，制限付きブロードキャストアドレス，内部ループバックアドレス以外の IP アドレスを指定してください。 IPv6 ポリシーベースルーティング指定の場合，宛先アドレスには，マルチキャストアドレス，リンクローカルアドレス以外の IPv6 アドレスを指定してください。
Cannot set policy based routing entry because specified source address is invalid.	フィルタ条件で指定した送信元アドレスが，ポリシーベースルーティングでサポートしていないため，エントリが設定できません。 IPv4 ポリシーベースルーティング指定の場合，送信元アドレスには，マルチキャストアドレス，内部ループバックアドレス以外の IP アドレスを指定してください。 IPv6 ポリシーベースルーティング指定の場合，送信元アドレスには，マルチキャストアドレス，リンクローカルアドレス以外の IPv6 アドレスを指定してください。
Cannot set the access list logging, because hardware mode doesn't correspond to access list logging.	system hardware-mode の access-log が設定されていないため，動作指定に log を指定したアクセスリストが設定できません。 動作指定に log を指定したアクセスリストを設定する場合，system hardware-mode の access-log を設定してください。
Cannot set the configuration because there is an inconsistency between vlan and policy based switching.	フィルタ条件の VLAN パラメータの設定内容と，ポリシーベーススイッチングの設定内容に矛盾が生じているため，エントリが設定できません。 ポリシーベーススイッチングを指定する場合，フィルタの検出条件にポリシーベーススイッチングリスト情報で指定した出力先の VLAN ID と同じ VLAN ID を指定してください。このとき，VLAN リスト名称では指定できません。
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。

メッセージ	内容
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 maximum number of access-list entries are exceeded.	アクセスリストのエントリ数が最大数を超えました。 アクセスリストのフィルタ条件は最大 4000 エントリまで設定できます。 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は，show running-config で該当するアクセスリストのフィルタ条件コマンドのエントリ数を確認してください。 次のコマンドが対象になります。 • access-list コマンド • deny（ip access-list standard）コマンド • deny（ip access-list extended）コマンド • deny（ipv6 access-list）コマンド • deny（mac access-list extended）コマンド • deny（advance access-list）コマンド • permit（ip access-list standard）コマンド • permit（ip access-list extended）コマンド • permit（ipv6 access-list）コマンド • permit（mac access-list extended）コマンド • permit（advance access-list）コマンド
The maximum number of entries are exceeded.	フィルタ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ファイル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 access-list and qos-flow-list entries are exceeded.	アクセスリストのエントリおよび QoS フローリストのエントリが最大数を超えました。 アクセスリストのフィルタ条件および QoS フローリストのフロー検出および動作指定は最大 32000 エントリまで設定できます。 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は，運用コマンド show running-config で，該当するアクセスリストのフィルタ条件コマンド，および QoS フローリストのフロー検出ならびに動作指定のエントリ数を確認してください。 次のコマンドが対象になります。 • access-list コマンド • deny（ip access-list standard）コマンド • deny（ip access-list extended）コマンド • deny（ipv6 access-list）コマンド • deny（mac access-list extended）コマンド • deny（advance access-list）コマンド • permit（ip access-list standard）コマンド • permit（ip access-list extended）コマンド • permit（ipv6 access-list）コマンド • permit（mac access-list extended）コマンド • permit（advance access-list）コマンド • qos（ip qos-flow-list）コマンド • qos（ipv6 qos-flow-list）コマンド • qos（mac qos-flow-list）コマンド • qos（advance qos-flow-list）コマンド
This list cannot be set to the layer-2 forwarding, because the list includes TCP flag parameter.	このアクセスリストの検出条件はレイヤ 2 中継への適用はできません。 アクセスリスト内のフロー検出条件に TCP 制御フラグが指定されている場合には，そのアクセスリストはレイヤ 2 中継への適用はできません。レイヤ 3 中継へ適用するか，上記パラメータを検出条件に含まないように変更してください。
This list cannot be set to the layer-2 forwarding, because the list includes tos parameter.	このアクセスリストの検出条件はレイヤ 2 中継への適用はできません。 アクセスリスト内のフロー検出条件に tos が指定されている場合には，そのアクセスリストはレイヤ 2 中継への適用はできません。レイヤ 3 中継へ適用するか，上記パラメータを検出条件に含まないように変更してください。

メッセージ	内容
This list cannot be set to the layer-2 forwarding, because the list includes traffic-class parameter.	このアクセスリストの検出条件はレイヤ 2 中継への適用はできません。 アクセスリスト内のフロー検出条件にトラフィッククラスが指定されている場合には，そのアクセスリストはレイヤ 2 中継への適用はできません。 レイヤ 3 中継へ適用するか，上記パラメータを検出条件に含まないように変更してください。
This list cannot be set to the outbound of this interface because this list includes policy based routing entry.	このアクセスリストは，ポリシーベースルーティングを含むため，インタフェースの送信側に適用できません。 ポリシーベースルーティングの設定を削除してから，インタフェースの送信側に適用してください。
This list cannot be set to this interface, because the list includes own or own-address parameter.	このアクセスリストの検出条件はこのインタフェースへの適用はできません。 次の条件をすべて満たす必要があります。 • VLAN インタフェースに適用する • 適用する VLAN インタフェースにはアドレスを設定する • IPv6 グローバルアドレスは一つだけ設定する
This list cannot be set to this interface because this list includes policy based routing entry.	このアクセスリストは，ポリシーベースルーティングを含むため，イーサネットインタフェースには適用できません。 ポリシーベースルーティングの設定を削除してから，イーサネットインタフェースに適用してください。
This list cannot be set to this interface specifying layer2-forwarding, because this list includes policy based routing entry.	このアクセスリストは，ポリシーベースルーティングを含むため，layer2-forwarding を指定してインタフェースに適用できません。 ポリシーベースルーティングの設定を削除してから，layer2-forwarding を指定してインタフェースに適用してください。
This list cannot be set to this port.	このアクセスリストはこのイーサネットインタフェースには適用できません。 イーサネットインタフェースにアクセスリストを適用する場合には，アクセスリスト内のフロー検出条件の VLAN ID，または VLAN リストに含まれるすべての VLAN ID が適用するイーサネットインタフェースの設定内容に含まれている必要があります。
This list cannot be set to VLAN.	このアクセスリストは VLAN インタフェースには適用できません。 アクセスリスト内のフロー検出条件に VLAN ID または VLAN リスト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 または VLAN リストの指定を削除してください。
This list cannot be set, because fldm prefer qos-only extended.	フロー配分パターンが qos-only の場合，アクセスリストを適用できません。 アクセスリストを適用したい場合は，フロー配分パターンを変更してください。
This list cannot be set, because of fldm.	設定されているフロー配分パターンでは，このリストを設定できません。 advance access-list をインタフェースに適用する場合，フロー配分パターンには standard-advance または extended-advance を指定してください。
This list cannot be set to the outbound of this interface because this list includes policy based switching entry.	このアクセスリストは，ポリシーベーススイッチングを含むため，インタフェースの送信側に適用できません。 ポリシーベーススイッチングの設定を削除してから，インタフェースの送信側に適用してください。
This list name is being used as other protocol type by other definition.	ほかのアクセスリストで使用済みの名称です。 ほかのアクセスリストで使用していない名称または対象となるアクセスリストを指定してください。
This policy-list number is not defined.	そのポリシーベースルーティングのリスト番号は指定できません。 対象となる作成済みのポリシーベースルーティングのリスト番号を指定してください。
This policy-switch-list number is not defined.	そのポリシーベーススイッチングのリスト番号は指定できません。 対象となる作成済みのポリシーベーススイッチングのリスト番号を指定してください。

メッセージ	内容
This vlan-list name is not defined.	その VLAN リスト名称は指定できません。 対象となる作成済み VLAN リスト名称を指定してください。

30.1.5 アクセスリストロギング情報

表 30-4 アクセスリストロギングのエラーメッセージ

メッセージ	内容
Cannot set the access list logging, because hardware mode doesn't correspond to access list logging.	system hardware-mode の access-log が設定されていないため，アクセスリストロギングが設定できません。 アクセスリストロギングの設定をする場合，system hardware-mode の access-log を設定してください。

30.1.6 QoS 情報

表 30-5 QoS のエラーメッセージ

メッセージ	内容
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，half 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。
Cannot attach this list because flow mac mode is set.	次の理由のため，QoS フローリストを適用できません。 • VLAN に IPv4QoS フローリストまたは IPv6QoS フローリストを適用した場合 IPv4QoS フローリストまたは IPv6QoS フローリストは，MAC モードの場合に VLAN インタフェースのレイヤ 2 中継への適用はできません。 IPv4QoS フローリストまたは IPv6QoS フローリストを適用する場合には，MAC モードを削除してから行ってください。 • イーサネットインタフェースに QoS フローリストを適用した場合 指定したイーサネットインタフェースが属する VLAN に MAC モードが設定されているため，QoS フローリストを適用できません。 QoS フローリストをイーサネットインタフェースに適用する場合には，指定イーサネットインタフェースが属するすべての VLAN から MAC モードを削除してください。
Cannot attach this list because IPv6 source address prefix-length exceeds 64.	フロー検出条件の送信元 IPv6 アドレスが上位 65 ビット以上の検出条件は適用できません。 次に示す条件を満たす必要があります。 • フロー検出条件の送信元 IPv6 アドレスのレングスを 64 以内に指定してください。 • フロー検出条件の送信元 IPv6 アドレスに host を指定しないでください。
Cannot change hierarchical shaper because a user is specified in a flow-qos-list.	ユーザ ID（<user id>，llrlq1，llrlq2）がフロー QoS コンフィグレーションに設定されているため，階層化シェーパコンフィグレーション（number-of-queue，mode，shaper auto-configuration）を変更できません。
Cannot change shaper mode when there is a shaper configuration in the interface.	シェーパモードが変更できません。 指定した NIF 番号のインタフェースの (config-if) 階層に，シェーパコンフィグレーションの設定がない状態で変更してください。
Cannot change shaper number-of-queue when there is a shaper configuration in the interface.	シェーパキュー数が変更できません。 指定した NIF 番号のインタフェースの (config-if) 階層に，シェーパコンフィグレーションの設定がない状態で変更してください。
Cannot set hierarchical shaper and legacy shaper simultaneously.	階層化シェーパ機能とレガシーシェーパ機能は同時に設定できません。

メッセージ	内容
Cannot set shaper nif and shaper auto-configuration simultaneously.	シェーパ自動設定機能とシェーパ NIF 情報は同時に設定できません。
Cannot set the upc-storm-control mode.	インタフェースに帯域監視が設定されているため，帯域監視ストームコントロールモードが設定できません。 帯域監視ストームコントロールモードを設定する場合には，適用されている QoS フローリストの帯域監視の指定をすべて削除してから行ってください。
Duplicate shaper user id configuration.	ポート内でユーザ ID が重複しています。ユーザ ID にはまだ設定されていない番号を指定してください。
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。
Min-rate is less than llpq-peak-rate.	最低帯域値が LLPQ 帯域制御値より小さいです。 • 値の設定範囲 <kbit/s>：64 ～ 1000000 <Mbit/s>：1M ～ 1000M
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。
NIF does not support hierarchical shaper.	この NIF は階層化シェーパ機能をサポートしていません。
NIF does not support legacy shaper.	この NIF はレガシーシェーパ機能をサポートしていません。
NIF does not support this shaper mode.	この NIF はこのシェーパモードをサポートしていません。
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。
Peak-rate is less than llpq-peak-rate.	最大帯域値が LLPQ 帯域制御値より小さいです。 • 値の設定範囲 <kbit/s>：64 ～ 1000000 <Mbit/s>：1M ～ 1000M
Peak-rate is less than min-rate.	最大帯域値が最低帯域値より小さいです。 • 値の設定範囲 <kbit/s>：64 ～ 1000000 <Mbit/s>：1M ～ 1000M
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 <value1> and shaper mode are inconsistent.	<value1> とシェーパモードの関連性が不一致です。 指定した NIF のシェーパモードに llrlq を設定してください。
	<value1>：llrlq1-burst，llrlq2-burst
Relations between <value1> and shaper mode are inconsistent.	<value1> とシェーパモードの関連性が不一致です。 シェーパモードに llrlq を設定してください。
	<value1>：llrlq1，llrlq2
Relations between max-psp and UPC entry are inconsistent.	設定している稼働 PSP 数と帯域監視を指定した QoS フローリストの設定で矛盾が生じているため，コンフィグレーションを変更できません。 受信側の VLAN インタフェースに帯域監視を指定した QoS フローリストを適用する場合，次のコマンドで設定する稼働 PSP 数をすべて 1 にしてください。 • redundancy max-psp • schedule-power-control max-psp • adaptive-power-control max-psp

メッセージ	内容
Relations between max-psp and upc-storm-control mode are inconsistent.	設定している稼働 PSP 数と帯域監視ストームコントロールモードの設定で矛盾が生じているため，コンフィグレーションを変更できません。 帯域監視ストームコントロールモードを upc-in-out に変更する場合，次のコマンドで設定する稼働 PSP 数をすべて 1 にしてください。 • redundancy max-psp • schedule-power-control max-psp • adaptive-power-control max-psp
Relations between number-of-queue and shaper mode are inconsistent.	キュー数とシェーパモードの関連性が不一致です。 シェーパモードが llpq4 の場合，キュー数 4 は指定できません。
Shaper mode configuration is required beforehand to set the shaper configuration to the interface.	シェーパモードの設定がないため，インタフェースにシェーパコンフィグレーションを設定できません。 指定したインタフェースの NIF にシェーパモードを設定してください。
Shaper port rate-limit is less than shaper wgq-group rate-limit.	ポート帯域制御値が WGQ 帯域制御値より小さいです。 • 値の設定範囲 <kbit/s>：64 ～ 1000000 <Mbit/s>：1M ～ 1000M
Shaper port rate-limit must be greater than the peak-rate of each shaper user and peak-rate of shaper default-user.	ポート帯域制御値は各ユーザの最大帯域およびデフォルトユーザの最大帯域以上でなければなりません。
Shaper port rate-limit must be greater than the sum of max-rate of llrlq1 and max-rate of llrlq2.	ポート帯域制御値は llrlq1 の最大帯域および llrlq2 の最大帯域の合計値以上でなければなりません。
Shaper port rate-limit must be greater than the sum of min-rate of each shaper user, and min-rate of default-user.	ポート帯域制御値は各ユーザの最低帯域およびデフォルトユーザの最低帯域の合計値以上でなければなりません。
Shaper port rate-limit must be greater than the sum of min-rate of each shaper user, min-rate of default-user, max-rate of llrlq1, and max-rate of llrlq2.	ポート帯域制御値はすべてのユーザの最低帯域，デフォルトユーザの最低帯域，llrlq1 の最大帯域および llrlq2 の最大帯域の合計値以上でなければなりません。
Specified rate value of WFQ is incorrect, or it is out of range.	指定した WFQ の rate が不正な値であるか，または設定範囲を超えています。
Specified traffic-shape rate value is incorrect, or it is out of range.	指定したポート帯域制御の帯域が不正な値であるか，または設定範囲を超えています。
Storm-control must be with "upc-storm-control mode upc-in-and-storm-control"	インタフェースにストームコントロールが設定されているため，帯域監視ストームコントロールモードが変更できません。 • AX6700S の場合 帯域監視ストームコントロールモードを変更する場合には，ストームコントロールの設定を削除してから行ってください。 • AX6600S または AX6300S の場合 帯域監視ストームコントロールモードを upc-in-in または upc-in-out に変更する場合には，ストームコントロールの設定を削除してから行ってください。
The list cannot be applied in the inbound direction, because shaper nif configuration is missing or inconsistent among the nif ports.	シェーパ自動設定機能が設定されていない，またはシェーパモードを設定している装置内の NIF でシェーパ設定（シェーパモード，シェーパキュー数）がすべて同じでないため，動作指定にユーザ ID（<user id>，llrlq1，llrlq2）を含む QoS フローリストを Inbound に設定できません。 シェーパ自動設定機能を設定するか，シェーパモードを設定しているすべての NIF でシェーパ設定を同じにしてください。

メッセージ	内容
The list cannot be applied in the outbound direction, because shaper nif configuration is missing or inconsistent among the vlan ports.	シェーパ自動設定機能が設定されていない，またはVLANに含まれているインタフェースが属するNIFでシェーパ設定（シェーパモード，シェーパキュー数）がすべて同じでないため，動作指定にユーザID（<user id>，llrlq1，llrlq2）を含むQoSフローリストをOutboundに設定できません。 シェーパ自動設定機能を設定するか，VLANに含まれているインタフェースが属するNIFで次の条件を満たすように設定してください。 • シェーパモードを設定しているすべてのNIFでシェーパ設定が同じ
The list cannot be applied to the interface, because the list contains user id parameter.	動作指定にユーザID（<user id>，llrlq1，llrlq2）を指定したリストはこのインタフェースに適用できません。 現在のシェーパ設定（シェーパモード，シェーパキュー数，シェーパ自動設定機能）は，動作指定に設定した<user id>が範囲外，または動作指定にllrlq1またはllrlq2を設定しているため，QoSフローリストを適用できません。ユーザIDの指定可能な条件については「コンフィグレーションガイドVol.2　6.4階層化シェーパの解説」を参照してください。
The list cannot be set to the vlan interface, because the vlan has no ethernet port which is configured shaper mode.	シェーパ自動設定機能が設定されていない，またはVLANインタフェースにシェーパモードを設定しているNIFのイーサネットインタフェースが一つも含まれていないため，動作指定にユーザID（<user id>，llrlq1，llrlq2）を含むQoSフローリストをOutboundに設定できません。 シェーパ自動設定機能を設定するか，VLANインタフェースにシェーパモードを設定しているNIFのイーサネットインタフェースを一つ以上含むように変更してください。
The list contains user id, but shaper nif is not configured.	シェーパ自動設定機能が設定されていない，またはシェーパモードが設定されていないため，動作指定にユーザID（<user id>，llrlq1，llrlq2）を含むQoSフローリストを設定できません。 シェーパ自動設定機能を設定するか，シェーパモードを設定してください。
The maximum number of access-list and qos-flow-list entries are exceeded.	アクセスリストのエントリおよびQoSフローリストのエントリが最大数を超えました。 アクセスリストのフィルタ条件，QoSフローリストのフロー検出，および動作指定は，最大32000エントリまで設定できます。 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は，運用コマンドshow running-configで，該当するアクセスリストのフィルタ条件コマンド，およびQoSフローリストのフロー検出ならびに動作指定のエントリ数を確認してください。 次のコマンドが対象になります。 • access-listコマンド • deny（ip access-list standard）コマンド • deny（ip access-list extended）コマンド • deny（ipv6 access-list）コマンド • deny（mac access-list extended）コマンド • deny（advance access-list）コマンド • permit（ip access-list standard）コマンド • permit（ip access-list extended）コマンド • permit（ipv6 access-list）コマンド • permit（mac access-list extended）コマンド • permit（advance access-list）コマンド • qos（ip qos-flow-list）コマンド • qos（ipv6 qos-flow-list）コマンド • qos（mac qos-flow-list）コマンド • qos（advance qos-flow-list）コマンド
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。

メッセージ	内容
The maximum number of qos-flow-list entries are exceeded.	QoS フローリストのエントリ数が最大数を超えました。 QoS フローリストのフロー検出および動作指定は最大 4000 エントリまで設定できます。 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は，show running-config で該当する QoS フローリストのフロー検出および動作指定のエントリ数を確認してください。 次のコマンドが対象になります。 • qos（ip qos-flow-list）コマンド • qos（ipv6 qos-flow-list）コマンド • qos（mac qos-flow-list）コマンド • qos（advance qos-flow-list）コマンド
The maximum number of shaper user entries is exceeded.	シェーパユーザのエントリ数が収容条件を超えています。
The maximum rate for the queue is inconsistent with the other queue's rate.	キューごとの最大送信帯域値の総和が 100% を超えているか，キュー番号（high）の最大送信帯域値がキュー番号（low）の最大送信帯域値より小さい値です。キューごとの最大送信帯域値の総和が 100% 以内で，かつキュー番号（high）の最大送信帯域値がキュー番号（low）の最大送信帯域値以上となるように設定してください。
The unit of the specified traffic-shape rate is unjustified.	指定したポート帯域の刻み値が不正です。
This list cannot be set to the inbound, because upc-storm-control mode <upc-storm-control mode>.	帯域監視ストームコントロールモードが upc-in-in ではない場合，受信側ではフロー検出条件に対する最大帯域制御および最低帯域監視の同時設定はできません。 フロー検出条件に対する最大帯域制御および最低帯域監視の同時設定をする場合は，帯域監視ストームコントロールモードを変更してください。
	<upc-storm-control mode>： • AX6700S の場合 upc-in-and-storm-control • AX6600S または AX6300S の場合 upc-in-and-storm-control，upc-in-out
This list cannot be set to the layer-2 forwarding, because the list includes replace-dscp or penalty-dscp parameter.	この QoS フローリストの動作指定はレイヤ 2 中継への適用はできません。 QoS フローリスト内の動作指定に DSCP 書き換えまたは違反時 DSCP 書き換えが指定されている場合には，その QoS フローリストはレイヤ 2 中継への適用はできません。VLAN インタフェースのレイヤ 3 中継へ適用するか，DSCP 書き換えおよび違反時 DSCP 書き換えを行わないように変更してください。
This list cannot be set to the layer-2 forwarding, because the list includes TCP flag parameter.	この QoS フローリストの検出条件はレイヤ 2 中継への適用はできません。 QoS フローリスト内のフロー検出条件に TCP 制御フラグが指定されている場合には，その QoS フローリストはレイヤ 2 中継への適用はできません。レイヤ 3 中継へ適用するか，上記パラメータを検出条件に含まないように変更してください。
This list cannot be set to the layer-2 forwarding, because the list includes tos parameter.	この QoS フローリストの検出条件はレイヤ 2 中継への適用はできません。 QoS フローリスト内のフロー検出条件に tos が指定されている場合には，その QoS フローリストはレイヤ 2 中継への適用はできません。レイヤ 3 中継へ適用するか，上記パラメータを検出条件に含まないように変更してください。
This list cannot be set to the layer-2 forwarding, because the list includes traffic-class parameter.	この QoS フローリストの検出条件はレイヤ 2 中継への適用はできません。 QoS フローリスト内のフロー検出条件にトラフィッククラスが指定されている場合には，その QoS フローリストはレイヤ 2 中継への適用はできません。レイヤ 3 中継へ適用するか，上記パラメータを検出条件に含まないように変更してください。
This list cannot be set to the outbound, because it includes a flow entry which sets both the maxrate and the minrate.	送信側ではフロー検出条件に対する最大帯域制御および最低帯域監視の同時設定はできません。 フロー検出条件に対して最大帯域制御または最低帯域監視のどちらかを指定する QoS フローリストに変更してください。

メッセージ	内容
This list cannot be set to the outbound, because it includes the UPC entry.	送信側では帯域監視はできません。 帯域監視ができるのは，受信側だけです。
This list cannot be set to the outbound, because upc-storm-control mode <upc-storm-control mode>.	帯域監視ストームコントロールモードが upc-in-and-storm-control または upc-in-in の場合，送信側では帯域監視はできません。 送信側で帯域監視する場合は，帯域監視ストームコントロールモードを変更してください。
	<upc-storm-control mode>：upc-in-and-storm-control，upc-in-in
This list cannot be set to the VLAN interface, because it includes the UPC entry.	VLAN インタフェースでは帯域監視はできません。 帯域監視ができるのは，イーサネットインタフェースだけです。
This list cannot be set to this interface, because the list includes own or own-address parameter.	この QoS フローリストの検出条件はこのインタフェースへの適用はできません。 次の条件をすべて満たす必要があります。 • VLAN インタフェースに適用する • 適用する VLAN インタフェースにはアドレスを設定する • IPv6 グローバルアドレスは一つだけ設定する
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，または VLAN リストに含まれるすべての 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，または VLAN リスト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，または VLAN リストの設定を削除してください。
This list cannot be set, because fldm prefer filter-only extended.	フロー配分パターンが filter-only の場合，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したい場合は，フロー配分パターンを変更してください。
This list cannot be set, because of fldm.	設定されているフロー配分パターンでは，このリストは設定できません。 advance qos-flow-list をインタフェースに適用する場合，フロー配分パターンには standard-advance または extended-advance を指定してください。
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。
This vlan-list name is not defined.	その VLAN リスト名称は指定できません。 対象となる作成済み VLAN リスト名称を指定してください。

30.1.7 IEEE802.1X 情報

表 30-6 IEEE802.1X のエラーメッセージ

メッセージ	内容
ChGr <channel group number>: Inconsistency is found between the dot1x port-control and the dot1x vlan <vlan id> enable configuration.	VLAN 単位認証（静的）の VLAN とポート単位認証のチャネルグループとの関係が不一致です。 VLAN 単位認証（静的）を設定した VLAN に所属しているチャネルグループにポート単位認証は設定できません。 ポート単位認証を設定したチャネルグループが所属している VLAN に VLAN 単位認証（静的）は設定できません。
	<channel group number>：チャネルグループ番号 <vlan id>：VLAN ID

メッセージ	内容
ChGr <channel group number>: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	ポート単位認証のチャネルグループとレイヤ 2 インタフェース属性との関係が不一致です。 ポート単位認証を設定したチャネルグループに switchport mode でアクセスモード以外のモードは設定できません。 switchport mode でアクセスモード以外のモードを設定したチャネルグループにポート単位認証は設定できません。
	<channel group number>：チャネルグループ番号
ChGr <channel group number>: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	ポート単位認証のチャネルグループの ignore-eapol-start と reauthentication との関係が不一致です。 reauthentication が設定されていない場合，ignore-eapol-start は設定できません。 reauthentication を設定したあとで ignore-eapol-start を設定してください。
	<channel group number>：チャネルグループ番号
ChGr <channel group number>: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	ポート単位認証のチャネルグループの ignore-eapol-start と supplicant-detection との関係が不一致です。 ignore-eapol-start が設定されている場合，supplicant-detection に disable を設定できません。 supplicant-detection に disable が設定されている場合，ignore-eapol-start は設定できません。
	<channel group number>：チャネルグループ番号
Inconsistency is found between the dot1x and the fense configuration.	IEEE802.1X コンフィグレーションと認証 VLAN コンフィグレーションとの関係が不一致です。 dot1x system-auth-control は，次のどれかと同時に設定できません。 • fense vaa-name • fense vlan • fense server
Inconsistency is found between the dot1x and the gsrp configuration.	IEEE802.1X コンフィグレーションと GSRP コンフィグレーションとの関係が不一致です。 dot1x system-auth-control と gsrp を同時に設定できません。
Inconsistency is found between the dot1x and the l2protocol-tunnel eap configuration.	IEEE802.1X コンフィグレーションと EAPOL フォワーディングコンフィグレーションとの関係が不一致です。 ポート単位認証と EAPOL フォワーディングを設定した VLAN を同一のポート，チャネルグループには設定できません。 VLAN 単位認証（静的，動的）と EAPOL フォワーディングを同一の VLAN には設定できません。
Inconsistency is found between the dot1x and the mac-address-table limit configuration.	IEEE802.1X コンフィグレーションと MAC アドレス学習制限との関係が不一致です。 IEEE802.1X と MAC アドレス学習制限を同一のポート，チャネルグループ，および VLAN には設定できません。
Inconsistency is found between the dot1x and the no mac-address-table learning configuration.	IEEE802.1X コンフィグレーションと MAC アドレス学習抑止との関係が不一致です。 ポート単位認証と MAC アドレス学習抑止を設定した VLAN を同一のポート，チャネルグループには設定できません。 VLAN 単位認証（静的，動的）と MAC アドレス学習抑止を同一の VLAN には設定できません。
Inconsistency is found between the dot1x vlan enable and the switchport mode configuration.	VLAN 単位認証（静的）の VLAN とレイヤ 2 インタフェース属性との関係が不一致です。 トンネリングポートが所属している VLAN に VLAN 単位認証（静的）は設定できません。

メッセージ	内容
Inconsistency is found between the dot1x vlan enable or dot1x vlan dynamic radius-vlan <vlan id> and the vlan configuration.	VLAN 単位認証（静的）または VLAN 単位認証（動的）の VLAN と VLAN コンフィグレーションとの関係が不一致です。 VLAN 単位認証（静的）または VLAN 単位認証（動的）が設定されている VLAN を削除できません。 VLAN 単位認証（静的）または VLAN 単位認証（動的）の VLAN の設定を削除したあとで，VLAN を削除してください。
	<vlan id>：VLAN ID
Inconsistency is found between the vrf and the dot1x configuration.	IEEE802.1X コンフィグレーションと VRF コンフィグレーションとの関係が不一致です。 dot1x system-auth-control と vrf mode は同時に設定できません。
port <nif no.>/<port no.>: Inconsistency is found between the dot1x port-control and the dot1x vlan <vlan id> enable configuration.	VLAN 単位認証（静的）の VLAN とポート単位認証のポートとの関係が不一致です。 VLAN 単位認証（静的）を設定した VLAN に所属しているポートにポート単位認証は設定できません。 ポート単位認証を設定したポートが所属している VLAN に VLAN 単位認証（静的）は設定できません。
	<nif no.>/<port no.>：NIF 番号 / ポート番号 <vlan id>：VLAN ID
port <nif no.>/<port no.>: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	ポート単位認証のポートとレイヤ 2 インタフェース属性との関係が不一致です。 ポート単位認証を設定したポートに switchport mode でアクセスモード以外のモードは設定できません。 switchport mode でアクセスモード以外のモードを設定したポートにポート単位認証は設定できません。
	<nif no.>/<port no.>：NIF 番号 / ポート番号
port <nif no.>/<port no.>: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	ポート単位認証のポートの ignore-eapol-start と reauthentication との関係が不一致です。 reauthentication が設定されていない場合，ignore-eapol-start は設定できません。 reauthentication を設定したあとで ignore-eapol-start を設定してください。
	<nif no.>/<port no.>：NIF 番号 / ポート番号
port <nif no.>/<port no.>: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	ポート単位認証のポートの ignore-eapol-start と supplicant-detection との関係が不一致です。 ignore-eapol-start が設定されている場合，supplicant-detection に disable を設定できません。 supplicant-detection に disable が設定されている場合，ignore-eapol-start は設定できません。
	<nif no.>/<port no.>：NIF 番号 / ポート番号
The total count of dot1x vlan definitions is beyond the maximum value (1024).	VLAN 単位認証（静的，動的）を設定した VLAN の合計が上限を超えています。 上限（1024）の範囲で設定してください。
The total count of dot1x vlan ports and port-channel combined is beyond the maximum value (1024).	VLAN 単位認証（静的，動的）を設定した VLAN に所属するポートとチャネルグループの合計が上限を超えています。 上限（1024）の範囲で設定してください。

メッセージ	内容
vlan <vlan id>: Inconsistency is found between the dot1x vlan enable and the switchport configuration.	VLAN 単位認証（静的）の VLAN とプロトコル VLAN ポートまたは MAC VLAN ポートとの関係が不一致です。 VLAN 単位認証（静的）を設定した VLAN に switchport protocol-vlan でプロトコル VLAN のネイティブ VLAN または switchport mac-vlan で MAC VLAN のネイティブ VLAN は設定できません。 switchport protocol-vlan でプロトコル VLAN のネイティブ VLAN，または switchport mac-vlan で MAC VLAN のネイティブ VLAN を設定した VLAN に VLAN 単位認証（静的）は設定できません。
	<vlan id>：VLAN ID
vlan <vlan id>: Inconsistency is found between the dot1x vlan enable and the vlan configuration.	VLAN 単位認証（静的）の VLAN と VLAN コンフィグレーションとの関係が不一致です。 VLAN 単位認証（静的）の VLAN に指定した VLAN に vlan コマンドでポート VLAN が設定されていません。 vlan コマンドでポート VLAN を設定した VLAN を VLAN 単位認証（静的）の VLAN に指定してください。
	<vlan id>：VLAN ID
vlan <vlan id>: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	VLAN 単位認証（静的）の VLAN の ignore-eapol-start と reauthentication との関係が不一致です。 reauthentication が設定されていない場合，ignore-eapol-start は設定できません。 reauthentication を設定したあとで ignore-eapol-start を設定してください。
	<vlan id>：VLAN ID
vlan <vlan id>: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	VLAN 単位認証（静的）の VLAN の ignore-eapol-start と supplicant-detection との関係が不一致です。 ignore-eapol-start が設定されている場合，supplicant-detection に disable を設定できません。 supplicant-detection に disable が設定されている場合，ignore-eapol-start は設定できません。
	<vlan id>：VLAN ID
vlan dynamic: Inconsistency is found between the radius-vlan <vlan id> and the vlan configuration.	VLAN 単位認証（動的）の VLAN と VLAN コンフィグレーションとの関係が不一致です。 VLAN 単位認証（動的）の VLAN に指定した VLAN に vlan コマンドで MAC VLAN が設定されていません。 vlan コマンドで MAC VLAN を設定した VLAN を VLAN 単位認証（動的）の VLAN に指定してください。
	<vlan id>：VLAN ID
vlan dynamic: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	VLAN 単位認証（動的）の ignore-eapol-start と reauthentication との関係が不一致です。 reauthentication が設定されていない場合，ignore-eapol-start は設定できません。 reauthentication を設定したあとで ignore-eapol-start を設定してください。
vlan dynamic: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	VLAN 単位認証（動的）の ignore-eapol-start と supplicant-detection との関係が不一致です。 ignore-eapol-start が設定されている場合，supplicant-detection に disable を設定できません。 supplicant-detection に disable が設定されている場合，ignore-eapol-start は設定できません。

30.1.8 Web 認証情報

表 30-7 Web 認証のエラーメッセージ

メッセージ	内容
Duplicate IP address.	同じ IP アドレスがすでに使われています。 インタフェース，ローカルアドレスに使われていない IP アドレスを指定してください。
Duplicate network address.	Web 認証専用 IP アドレスに，インタフェースに設定したサブネットに含まれるアドレスが設定されています。
Duplicate web authentication 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。
Inconsistency is found between the VAA configuration and the web-authentication configuration.	FENSE コマンドが設定されている場合，Web 認証起動コマンドは実行できません。
Inconsistency is found between the vrf and the web-authentication configuration.	vrf mode コマンドが設定されている場合，Web 認証起動コマンドは実行できません。
Inconsistency is found between the web-authentication vlan command and web-authentication port command.	装置内でレガシーモードとダイナミック VLAN モードまたは固定 VLAN モードは混在できません。
Invalid access-list ID for authentication.	認証用のアクセスリストを設定できるのは一つの装置で一つまでです。
Invalid max-timer . -- <value>	最大接続時間が範囲外です。 10 ～ 1440 または infinity を設定してください。
	<value>：Web 認証最大接続時間
Invalid max-user . -- <value>	最大接続ユーザ数が範囲外です。 1 ～ 4096 を設定してください。
	<value>：Web 認証最大接続ユーザ
Invalid vlan . -- <value>	VLAN ID が範囲外です。 2 ～ 4095 を設定してください。
	<value>：Web 認証後の VLAN の VLAN ID，または Web 認証の URL リダイレクト VLAN の VLAN ID
Invalid VLAN ID <vlan id>, not MAC VLAN	設定した VLAN ID に該当する VLAN が MAC VLAN ではありません。
	<vlan id>：認証後 VLAN の VLAN ID
Maximum number of web authentication port is exceeded.	Web 認証用ポート番号として追加可能な登録数は，http 用と https 用で合わせて二つまでです。 Web 認証用ポート番号を追加する場合は，http 用と https 用で合わせて二つ以内にしてください。
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。
Relations between the vlan configuration and the web-authentication redirect-vlan configuration are inconsistent.	URL リダイレクトを実施する VLAN を指定する場合，その VLAN ID は MAC VLAN 以外である必要があります。
Relations between the web-authentication configuration and the channel-group configuration within same port.	ポートチャネルのコンフィグレーションと Web 認証のコンフィグレーションは同一ポートには設定できません。
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。

メッセージ	内容
Relations between the web-authentication dynamic VLAN mode and the web-authentication static VLAN mode are inconsistent.	装置内でモード（固定 VLAN モード，ダイナミック VLAN モード）の違う Web 認証は混在できません。
Relations between the web-authentication logout polling configuration is inconsistent.	Web 認証のポーリング機能関連のコンフィグレーションに矛盾が生じたため，実行できません。
Relations between web-authentication configuration and l2protocol-tunnel eap configuration are inconsistent.	装置内で Web 認証の URL リダイレクト機能と EAPOL フォワーディング機能は同時に設定できません。

30.1.9 MAC 認証情報

表 30-8 MAC 認証のエラーメッセージ

メッセージ	内容
Inconsistency is found between the VAA configuration and the mac-authentication configuration.	FENSE コマンドが設定されている場合，MAC 認証起動コマンドを実行できません。
Inconsistency is found between the vrf and the mac-authentication configuration.	vrf mode コマンドが設定されている場合，MAC 認証起動コマンドを実行できません。
Relations between the mac-authentication configuration and the channel-group configuration within same port.	ポートチャネルのコンフィグレーションと MAC 認証のコンフィグレーションは同一ポートには設定できません。
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 mac-authentication configuration and the web-authentication dynamic VLAN configuration are inconsistent.	装置内で MAC 認証と Web 認証のレガシーモードは混在できません。

30.1.10 認証 VLAN 情報【OP-VAA】

表 30-9 認証 VLAN のエラーメッセージ

メッセージ	内容
fense: duplicate server address <server address>.	fense server に設定した IP アドレスは，ほかの VAA_ID に設定されている IP アドレスと重複しています。
	<server address>：認証サーバの IP アドレス
fense: duplicate vlan subnet address <subnet address> and subnet mask <subnet mask>.	サブネットがすでに設定された値と重複しています。
	<subnet address>：認証済み VLAN のサブネットアドレス <subnet mask>：認証済み VLAN のサブネットマスク
fense: Inconsistency is found between the dot1x and the fense configuration.	IEEE802.1X コマンドの dot1x system-auth-control が設定されている場合，認証 VLAN 関連コマンドは実行できません。
fense: Inconsistency is found between the vlan suspend the fense vlan configuration.	認証 VLAN で使用している MAC VLAN はサスペンドできません。さらに，サスペンドしている MAC VLAN は認証 VLAN で使用できません。
fense: the set of VLAN ID <vlan id> and subnet is different from configured set.	VLAN ID に対して設定されたサブネットが，すでに設定された VLAN ID とサブネットのセットと異なっています。 VLAN ID に対応するサブネットは，<VAA ID> を通して一意となるよう設定してください。

メッセージ	内容
	<vlan id>：認証済み VLAN の VLAN ID
Inconsistency is found between the vrf and the fense configuration.	vrf mode コマンドが設定されている場合，認証 VLAN 関連起動コマンドは実行できません。

30.1.11 DHCP snooping 情報

表 30-10 DHCP snooping のエラーメッセージ

メッセージ	内容
Cannot change the configuration because there is an inconsistency between fldm and ip dhcp snooping.	DHCP snooping の設定とフロー配分パターンの設定に矛盾が生じているため，コンフィグレーションは変更できません。 DHCP snooping の設定を行う場合，フロー配分パターンは次に示すパラメータ以外を指定してください。 • fldm prefer default standard • fldm prefer {default | filter-only | qos-only | filter | qos} extended • fldm prefer qos-only extended-advance
Cannot change the DHCP snooping, because the maximum number of entries are exceeded.	DHCP snooping の設定を変更すると収容条件を超えてしまいます。 DHCP snooping の設定を変更する場合は，設定されているフローエントリが，変更後の収容条件に収まるように設定してから行ってください。
The VLAN target of the DHCP snooping and ARP inspection is not suitable.	DHCP snooping とダイナミック ARP 検査の対象 VLAN が適切ではありません。 ダイナミック ARP 検査は DHCP snooping 対象の VLAN を指定してください。

30.1.12 BSU/PSP/NIF 冗長化情報【AX6700S】【AX6600S】

表 30-11 BSU/PSP/NIF 冗長化のエラーメッセージ

メッセージ	内容
Cannot change <value1> configuration while "power-control" or "system recovery" exist.	power-control または system recovery がすでに設定されています。<value1> が設定できませんでした。 power-control または system recovery を削除するか，期待している情報が設定されているか確認してください。
	<value1>：コマンド名
Cannot change <value1> configuration while "redundancy bsu-load-balancing smac" or "redundancy bsu-mode fixed" exist.	redundancy bsu-load-balancing smac または redundancy bsu-mode fixed がすでに設定されています。<value1> を変更できませんでした。 redundancy bsu-load-balancing smac または redundancy bsu-mode fixed を削除するか，期待している情報が設定されているか確認してください。
	<value1>：コマンド名
Cannot set <value1> configuration while "schedule-power-control mode" or "schedule-power-control max-bsu" or "schedule-power-control standby-bsu" or "schedule-power-control time-range" or "adaptive-power-control enable" exist.	schedule-power-control mode，schedule-power-control max-bsu，schedule-power-control standby-bsu，schedule-power-control time-range または adaptive-power-control enable がすでに設定されています。<value1> が設定できませんでした。 schedule-power-control mode，schedule-power-control max-bsu，schedule-power-control standby-bsu，schedule-power-control time-range または adaptive-power-control enable を削除するか，期待している情報が設定されているか確認してください。

メッセージ	内容
	<value1>：コマンド名
Cannot set nif<value1>, because nif<value1> is already configured in redundancy nif group.	nif <value1> はすでに NIF 冗長グループに設定されているため，設定できません。 nif <value1> の NIF 冗長グループの設定を削除するか，期待している情報が設定されているか確認してください。
	<value1>：設定しようとした NIF 番号
Cannot set nif<value1>, because the maximum number of nif exist in this redundancy nif group.	この冗長グループに設定されている NIF 数がすでに上限に達しているため，nif <value1> を設定できません。 NIF 冗長グループ当たりの NIF 数を再確認してください。
	<value1>：設定しようとした NIF 番号
Relations between redundancy max-psp and UPC entry are inconsistent.	設定している稼働 PSP 数と帯域監視を指定した QoS フローリストの設定で矛盾が生じているため，コンフィグレーションを変更できません。 稼働 PSP 数を変更する場合，受信側の VLAN インタフェースに帯域監視を指定した QoS フローリストを削除してください。
Relations between redundancy max-psp and upc-storm-control mode are inconsistent.	設定している稼働 PSP 数と帯域監視ストームコントロールモードの設定で矛盾が生じているため，コンフィグレーションを変更できません。 稼働 PSP 数を変更する場合，帯域監視ストームコントロールモードに upc-in-in または upc-in-and-storm-control を指定してください。

30.1.13 GSRP 情報

表 30-12 GSRP のエラーメッセージ

メッセージ	内容
can not configure gsrp when spanning-tree is configured.	スパニングツリーの設定があるため，GSRP が設定できません。
can not configure gsrp when virtual-router is configured.	VRRP の設定があるため，GSRP が設定できません。
gsrp-<gsrp group id>: can not configure layer3-redundancy when GSRP ID is not in range from 1 to 4.	GSRP グループ ID が 1 から 4 以外の場合，layer3-redundancy は設定できません。 GSRP グループ ID を 1 から 4 の範囲で設定してください。
	<gsrp group id>：GSRP グループ ID
gsrp-<gsrp group id>: can not specify both any flush methods and direct-link on the channel-group <channel group number>.	ダイレクトリンクに設定したチャネルグループに reset-flush-port または no-flush-port を指定できません。 該当の設定からチャネルグループを削除するか別のチャネルグループを使用してください。
	<gsrp group id>：GSRP グループ ID <channel group number>：チャネルグループ番号
gsrp-<gsrp group id>: can not specify both any flush methods and direct-link on the port <nif no.>/<port no.>.	ダイレクトリンクに設定したポートに reset-flush-port または no-flush-port を指定できません。 該当の設定からポートを削除するか別のポートを使用してください。
	<gsrp group id>：GSRP グループ ID <nif no.>/<port no.>：NIF 番号 / ポート番号
gsrp-<gsrp group id>:can not specify the two or more flush methods on the channel-group <channel group number>.	同一チャネルグループに二つ以上のフラッシュ方法は指定できません。 該当の設定からチャネルグループを削除するか別のチャネルグループを使用してください。

メッセージ	内容
	<gsrp group id>：GSRP グループ ID <channel group number>：チャネルグループ番号
gsrp-<gsrp group id>:can not specify the two or more flush methods on the port <nif no.>/<port no.>.	同一ポートに二つ以上のフラッシュ方法は指定できません。 該当の設定からポートを削除するか別のポートを使用してください。
	<gsrp group id>：GSRP グループ ID <nif no.>/<port no.>：NIF 番号 / ポート番号
gsrp-<gsrp group id>-<vlan group id> is already configured in vlan-mapping.	指定された VLAN グループ ID は，すでに VLAN マッピング ID に設定されています。 Ring Protocol から該当 VLAN マッピング ID を削除するか，別の VLAN グループ ID を使用してください。
	<gsrp group id>：GSRP グループ ID <vlan group id>：VLAN グループ ID
gsrp-<gsrp group id>-<vlan group id>: vlan <vlan id> has been configured in another vlan-group.	指定された VLAN はすでにほかの 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 を使用してください。
	<gsrp group id>：GSRP グループ ID <vlan group id>：VLAN グループ ID <vlan id>：VLAN ID
Inconsistency is found between the vrf mode and the gsrp configuration.	VRF 機能の運用に伴い，次のどちらかの理由でコマンドを設定できません。 • vrf mode が gsrp-enable-ipv4-ipv6 以外の状態で，GSRP の設定はできません。 • GSRP のコンフィグレーションが設定されている状態で，vrf mode を gsrp-enable-ipv4-ipv6 以外に設定できません。

30.1.14 VRRP 情報

表 30-13 VRRP のエラーメッセージ

メッセージ	内容
Cannot configure vrrp when gsrp is configured.	GSRP が設定されているため，VRRP は設定できません。
Cannot follow Follow virtual router.	フォロー仮想ルータは，ほかの仮想ルータを追従できません。 プライマリ仮想ルータに指定された仮想ルータは，フォロー仮想ルータに設定しないでください。
Cannot set mode because the virtual router set other mode.	VRRP 動作モードは，複数設定できません。
Cannot set virtual router IP address because the other one of different address family already set.	異なるアドレスファミリの仮想 IP アドレスが設定済みなので，仮想 IP アドレスを設定できません。
Failure detection times is greater than check trial times.	failure detection times が check trial times を超えています。 check trial times 以下の値を設定してください。
Follow virtual router cannot become the address owner.	フォロー仮想ルータは，アドレス所有者になれません。 インタフェースに IP アドレスを設定する場合，フォロー仮想ルータに仮想 IP アドレスを設定する場合，追従するプライマリ仮想ルータを設定する場合は，フォロー仮想ルータがアドレス所有者にならないように設定してください。
Invalid virtual router IPv6 address. -- <value1>	仮想 IPv6 アドレスが不正です。

メッセージ	内容
Network address of VRRP virtual router ip address and IP address is different on accept mode.	VRRP の仮想 IP アドレスと実 IP アドレスのネットワークアドレスが異なります。 アクセプトモードを指定する場合，またはすでに指定している場合は，仮想 IP アドレスと実 IP アドレスのネットワークアドレスが一致するように指定してください。
Network prefix of VRRP virtual router ipv6 address and IPv6 address is different on accept mode.	VRRP の仮想 IPv6 アドレスと実 IPv6 アドレスのネットワークプレフィックスが異なります。 アクセプトモードを指定する場合，または，すでに指定している場合は，仮想 IPv6 アドレスと実 IPv6 アドレスのネットワークプレフィックスが一致するように指定してください。
Not found channel-group <channel group number>.	指定されたチャネルグループは設定されていません。
	<channel group number>：チャネルグループ番号
Only one track can assign for virtual router with priority mode.	一つの仮想ルータに割り当てられる優先度切替指定の track は一つだけです。
Only priority mode or decrement mode can specify as priority operation method at one virtual router.	一つの仮想ルータで優先度減算指定と優先度切替指定は混在できません。
Recovery detection times is greater than check trial times.	recovery detection times が check trial times を超えています。 check trial times 以下の値を設定してください。
The number of critical interfaces for virtual router is beyond limitation.	仮想ルータ当たりの Critical Interface の設定数が上限を超えました。
The number of Primary virtual routers exceeds limit.	プライマリ仮想ルータ数が，上限を超えました。

30.1.15 ストームコントロール情報

表 30-14 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
"storm-cotorol level 0" and "storm-cotorol action" are inconsistent.	ストームコントロールを行う受信帯域の値 "0" と "storm-control action" は同時に設定できません。
Storm-control must be with "upc-storm-control mode upc-in-and-storm-control"	ストームコントロール機能は，upc-storm-control mode で upd-in-and-storm-control を指定する必要があります。
Definition of "storm-cotorol action" must be same in Channel-Group.	チャネルグループ内で "storm-control action ” 設定は同じ設定である必要があります。

30.1.16 CFM 情報

表 30-15 CFM のエラーメッセージ

メッセージ	内容
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。
Cannot change cfm mep direction.	MEP の方向は変更できません。
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。
Cannot configure cfm mep to channel-group port.	ポートチャネルに参加しているインタフェースに，MEP を設定できません。

メッセージ	内容
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。
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
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
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
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
Maximum number of cfm mep are already defined.	MEP の最大設定数を超えています。 不要な MEP 設定を削除してください。
Maximum number of cfm mip are already defined.	MIP の最大設定数を超えています。 不要な MIP 設定を削除してください。
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
Not found VLAN ID <vlan id> in MA.	指定された VLAN ID が存在しません。MA で設定済みの VLAN ID を指定してください。
	<vlan id>：VLAN ID
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

30.1.17 SNMP 情報

表 30-16 SNMP のエラーメッセージ

メッセージ	内容
Group information exceeded 50 entries. <group name>	グループ情報が 50 エントリを超えました。 不要なグループ情報を削除してから追加してください。
	<group name>：グループ名
Informs is supported by only SNMPv2C.	インフォーム機能は SNMPv2C でサポートしています。 インフォーム機能を使用する場合は，SNMPv2C を選択してください。
Invalid oid-tree. <oid tree>	<oid tree> の値が不正です。 <oid tree> にはオブジェクト識別子をドット記法で指定してください。
	<oid tree>：サブツリー情報
MIB view exceeded 50 entries. <view name>	MIB ビューが 50 エントリを超えました。 不要な MIB ビューを削除してから追加してください。
	<view name>：MIB ビュー名
RMON alarm rising threshold is less than falling threshold.	上方閾値が下方閾値未満です。 上方閾値が下方閾値以上となるようにしてください。

メッセージ	内容
Subtree of the same MIB view exceeded 30 entries. <view name> <oid tree>	同一 MIB ビューのサブツリーが 30 エントリを超えました。 不要なサブツリーを削除してから追加してください。
	<view name>：MIB ビュー名 <oid tree>：サブツリー情報

30.1.18 sFlow 統計情報

表 30-17 sFlow 統計のエラーメッセージ

メッセージ	内容
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。
The sampling interval value must be set to a value that is higher than 2 when the "sflow forward egress" command enabled.	"sflow forward egress" コマンドを使用する場合は，サンプリング間隔は 2 以上である必要があります。

30.1.19 OADP 情報

表 30-18 OADP のエラーメッセージ

メッセージ	内容
Invalid parameter, hold-time must be longer than interval-time.	oadp interval-time コマンドで設定した値と oadp hold-time コマンドで設定した値の整合が取れません。 • oadp interval-time 設定時 oadp hold-time で設定した値より大きな値が設定されています。 • oadp hold-time 設定時 oadp interval-time で設定した値より小さな値が設定されています。

30.1.20 ポートミラーリング情報

表 30-19 ポートミラーリングのエラーメッセージ

メッセージ	内容
Mirror port and monitor port are inconsistent.	ミラーポートとモニターポートは同時に設定できません。
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。
Monitor port can be specified only in one monitor session, or in a pair of one tx session and one rx session.	モニターポートは，一つのモニターセッション，または一つの送信ポートミラーリングセッションと一つの受信ポートミラーリングセッションだけに設定できます。

索引

A

aaa accounting dot1x default 281
aaa accounting mac-authentication default start-stop group radius 375
aaa accounting web-authentication default start-stop group radius 345
aaa authentication dot1x default 282
aaa authentication mac-authentication default group radius 376
aaa authentication web-authentication default group radius 346
aaa authorization network default 283
access-list 30
access-log enable 140
access-log interval 141
access-log rate-limit 142
access-log threshold 143
advance access-group 41
advance access-list 44
advance access-list resequence 46
advance qos-flow-group 164
advance qos-flow-list 167
advance qos-flow-list resequence 168
advertise-holdtime 448
advertise-interval 449
authentication ip access-group 277

B

backup-lock 450

D

deny（advance access-list） 47
deny（ip access-list extended） 60
deny（ip access-list standard） 68
deny（ipv6 access-list） 70
deny（mac access-list extended） 77
domain name 528
dot1x force-authorized-port 284
dot1x ignore-eapol-start 285
dot1x logging enable 286
dot1x loglevel 287
dot1x max-req 289
dot1x max-supplicant 290
dot1x multiple-authentication 291
dot1x multiple-hosts 292
dot1x port-control 294
dot1x reauthentication 296
dot1x supplicant-detection 297
dot1x system-auth-control 299
dot1x timeout keep-unauth 300
dot1x timeout quiet-period 301
dot1x timeout reauth-period 302
dot1x timeout server-timeout 304
dot1x timeout supp-timeout 305
dot1x timeout tx-period 306
dot1x vlan dynamic enable 307
dot1x vlan dynamic ignore-eapol-start 308
dot1x vlan dynamic max-req 309
dot1x vlan dynamic max-supplicant 310
dot1x vlan dynamic radius-vlan 311
dot1x vlan dynamic reauthentication 313
dot1x vlan dynamic supplicant-detection 314
dot1x vlan dynamic timeout quiet-period 316
dot1x vlan dynamic timeout reauth-period 317
dot1x vlan dynamic timeout server-timeout 319
dot1x vlan dynamic timeout supp-timeout 320
dot1x vlan dynamic timeout tx-period 321
dot1x vlan enable 322
dot1x vlan ignore-eapol-start 324
dot1x vlan max-req 326
dot1x vlan max-supplicant 328
dot1x vlan reauthentication 330
dot1x vlan supplicant-detection 331
dot1x vlan timeout quiet-period 333
dot1x vlan timeout reauth-period 335
dot1x vlan timeout server-timeout 337
dot1x vlan timeout supp-timeout 338
dot1x vlan timeout tx-period 340

E

efmoam active 510
efmoam disable 511
efmoam udld-detection-count 512
ethernet cfm cc alarm-priority 530
ethernet cfm cc alarm-reset-time 532
ethernet cfm cc alarm-start-time 534
ethernet cfm cc enable 536
ethernet cfm cc interval 538
ethernet cfm domain 540
ethernet cfm enable（global） 542
ethernet cfm enable（interface） 543

ethernet cfm mep 544
ethernet cfm mip 546

F

fense alive-timer 392
fense retry-count 394
fense retry-timer 396
fense server 398
fense vaa-name 400
fense vaa-sync 402
fense vlan 403
flow mac mode 10
flush-request-count〔GSRP〕 451

G

gsrp 452
gsrp-vlan 453
gsrp direct-link 454
gsrp exception-port 455
gsrp limit-control 456
gsrp no-flush-port 457
gsrp reset-flush-port 458

H

hostname 552

I

ip access-group〔アクセスリスト〕 80
ip access-list extended 83
ip access-list resequence 85
ip access-list standard 87
ip arp inspection limit rate 406
ip arp inspection trust 407
ip arp inspection validate 408
ip arp inspection vlan 410
ip dhcp snooping 412
ip dhcp snooping database url 413
ip dhcp snooping database write-delay 415
ip dhcp snooping information option allow-untrusted 416
ip dhcp snooping limit rate 417
ip dhcp snooping logging enable 418
ip dhcp snooping loglevel 419
ip dhcp snooping trust 421
ip dhcp snooping verify mac-address 422
ip dhcp snooping vlan 423
ip qos-flow-group 170
ip qos-flow-list 173
ip qos-flow-list resequence 174
ip source binding 425
ip urpf 146
ipv6 access-list 89
ipv6 access-list resequence 91
ipv6 qos-flow-group 175
ipv6 qos-flow-list 178
ipv6 qos-flow-list resequence 179
ipv6 traffic-filter 92
ipv6 verify unicast source reachable-via 149
ip verify source 427
ip verify unicast source reachable-via 148

L

layer3-redundancy 459
lldp enable 622
lldp hold-count 623
lldp interval-time 624
lldp run 625
llrlq1-burst 180
llrlq2-burst 182
logging email 590
logging email-event-kind 592
logging email-from 593
logging email-interval 594
logging email-server 595
logging event-kind 597
logging facility 598
logging host 599
logging syslog-dump 601
logging trap 602
loop-detection 520
loop-detection auto-restore-time 522
loop-detection enable 523
loop-detection hold-time 524
loop-detection interval-time 525
loop-detection threshold 526

M

mac-authentication auth-interval-timer 377
mac-authentication auto-logout 378
mac-authentication dynamic-vlan max-user 379
mac-authentication logging enable 380
mac-authentication max-timer 381
mac-authentication password 382
mac-authentication port 383
mac-authentication radius-server host 384
mac-authentication static-vlan max-user 387
mac-authentication system-auth-control 388

mac-authentication vlan-check 389
mac access-group 95
mac access-list extended 97
mac access-list resequence 99
mac qos-flow-group 184
mac qos-flow-list 186
mac qos-flow-list resequence 187
ma name 547
ma vlan-group 549
mode〔QoS〕188
monitor option 636
monitor session 638

N

no-neighbor-to-master 460
number-of-queue 191

O

oadp cdp-listener 628
oadp enable 629
oadp hold-time 630
oadp ignore-vlan 631
oadp interval-time 632
oadp run 633

P

permit（advance access-list） 100
permit（ip access-list extended） 115
permit（ip access-list standard） 124
permit（ipv6 access-list） 126
permit（mac access-list extended） 134
port-up-delay 462
power redundancy-mode 430
predicted-tail-drop 193

Q

qos（advance qos-flow-list） 194
qos（ip qos-flow-list） 210
qos（ipv6 qos-flow-list） 221
qos（mac qos-flow-list） 231
qos-queue-group 236
qos-queue-list 238

R

redundancy bsu-load-balancing 432
redundancy bsu-mode 433
redundancy max-bsu 434
redundancy max-psp 438
redundancy nif-group max-standby-nif 442
redundancy nif-group nif priority 444
redundancy standby-bsu 435
redundancy standby-psp 439
remark〔QoS〕241
remark〔アクセスリスト〕137
reset-flush-time 463
rmon alarm 553
rmon collection history 556
rmon event 558

S

selection-pattern 464
set-default-user-priority 243
sflow destination 606
sflow extended-information-type 607
sflow forward egress 609
sflow forward ingress 610
sflow max-header-size 611
sflow max-packet-size 612
sflow packet-information-type 613
sflow polling-interval 614
sflow sample 615
sflow source 617
sflow url-port-add 619
sflow version 620
shaper auto-configuration 244
shaper default-user 246
shaper llrlq1 248
shaper llrlq2 250
shaper nif 252
shaper port buffer 253
shaper port rate-limit 255
shaper user 257
shaper user-list 260
shaper vlan-user-map 268
shaper wgq-group rate-limit 270
snmp-server community 561
snmp-server contact 563
snmp-server engineID local 564
snmp-server group 566
snmp-server host 569
snmp-server informs 577
snmp-server location 579
snmp-server traps 580
snmp-server user 583
snmp-server view 585
snmp trap link-status 587

storm-control（global） 514
storm-control（interface） 515

T

track check-reply-interface 470
track check-status-interval 471
track check-trial-times 473
track failure-detection-interval 475
track failure-detection-times 477
track interface 479
track ip route 481
track recovery-detection-interval 483
track recovery-detection-times 485
traffic-shape rate 271

U

upc-storm-control mode 273

V

vlan-group disable 465
vlan-group priority 466
vlan-group vlan 467
vlan-list 14
vrrp-vlan 507
vrrp accept 487
vrrp authentication 488
vrrp follow 490
vrrp ietf-ipv6-spec-07-mode 492
vrrp ietf-unified-spec-02-mode 494
vrrp ip 496
vrrp ipv6 497
vrrp name 498
vrrp preempt 499
vrrp preempt delay 500
vrrp priority 501
vrrp timers advertise 502
vrrp timers non-preempt-swap 504
vrrp track 505

W

web-authentication auto-logout 347
web-authentication ip address 348
web-authentication jump-url 350
web-authentication logging enable 351
web-authentication logout ping tos-windows 352
web-authentication logout ping ttl 353
web-authentication logout polling count 354
web-authentication logout polling enable 356
web-authentication logout polling interval 358
web-authentication logout polling retry-interval 360
web-authentication max-timer 362
web-authentication max-user 364
web-authentication port 365
web-authentication redirect-mode 366
web-authentication redirect-vlan 367
web-authentication static-vlan max-user 368
web-authentication system-auth-control 369
web-authentication vlan 370
web-authentication web-port 371

こ

コマンドの記述形式 2