AXprimoM210

CLI レファレンスガイド

第 4 版

AXprimo-S001-30

■対象製品

このマニュアルは AXprimoM210 を対象に記載しています。

■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。
Firefox は，米国およびその他の国における The Mozilla Foundation の登録商標です。
Google Chrome は，米国およびその他の国における Google LLC の登録商標または商標です。
Internet Explorer は，米国 Microsoft Corporation の米国およびその他の国における登録商用または商標です。
Linux は，米国およびその他の国における The Linux Foundation 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。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商用または商標です。
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

２０２０年　１０月　（第４版）　ＡＸｐｒｉｍｏ－Ｓ００１－３０

■著作権

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

変更内容

【第 2 版】

表　変更内容

章・節・項・タイトル	追加・変更内容
このマニュアルの読み方	IPv6 ACLs (中継パケットフィルタのみ)をサポートしました。
8.10 EAPOL の透過	本節を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【第 3 版】

表　変更内容

章・節・項・タイトル	追加・変更内容
このマニュアルの読み方	ゼロタッチプロビジョニングをサポートしました。
4.4.12 / 8.3.3 / 8.3.7 / 8.4.1 / 8.4.6	各コマンドの応答待ち時間の最大設定範囲を 60sec に変更
11.1.2	1000BASE-BX(SFP)を追加

なお，単なる誤字・脱字などはお断りなく訂正しました。

【第 4 版】

表　変更内容

章・節・項・タイトル	追加・変更内容
このマニュアルの読み方	PoE 機能における時間範囲設定をサポートしました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

はじめに

■対象製品

このマニュアルは AXprimoM210 を対象に記載しております。

■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/

■ドキュメント体系

AXprimoM210 のマニュアルを以下に示します。
・AXprimoM210 ハードウェア取扱説明書 （AXprimo-H001）
・AXprimoM210 CLI レファレンスガイド （AXprimo-S001）
・AXprimoM210 Web 管理ガイド （AXprimo-S002）

このマニュアルの読み方

■将来サポート機能

このマニュアルの内容には将来サポート予定の機能に関する記述も掲載しております。将来サポート予定の機能を以下に示します。

・IPv6 機能全般（以下の代表的な機能以外に、各コマンドのパラメータも含む、但しパケットフィルタ除く）

MLD snooping	22.3 章、22.4 章
IPv6 DHCP Client	25.1 章
IPv6 インタフェース	26.2 章
・IGMP snooping proxy 機能	22.1 章
・リモート認証(Tacacs+)	8.4 章
・レート制御機能	15.1 章
・VLAN 状態変更	19.1.2 章
・MIB 書込みアクセス	5 章

■機能間の共存について

複数の機能を併用する際、共存不可または制限事項がある機能があります。機能間の共存についての制限事項を次の表に示します。

使用したい機能	制限のある機能	制限の内容
リンクアグリゲーション	ACL	共存不可
	QoS	共存不可
	優先制御	共存不可
	IPv4 ソースガード	共存不可
ARP 検査	ACL	共存不可
MAC アドレス学習無効化	ポートセキュリティ	共存不可
時間範囲設定	ACL	共存不可

■注意事項

本装置の運用には、コンソールもしくはリモート端末からのログインが可能ですが、複数ユーザによる運用はしないようお願いいたします。

本装置で以下に示すコンフィグレーション編集を行った場合、必ず save およびバックアップを行ってください。また運用開始前に装置再起動が必要になります。

・IGMP snooping 機能
・スパニングツリー機能
・ループ検知機能
・QoS 機能
・IP インタフェース機能

目次

1 スイッチの初期設定 23
1.1 スイッチへの接続 24
1.1.1 設定オプション 24
1.1.2 コンソールポートへの接続 25
1.1.3 コマンドラインインタフェースへのログオン 25
1.1.4 パスワードの設定 25
1.1.5 リモート接続 26
1.2 リモート管理 28
1.2.1 ネットワークインタフェースの使用 28
1.2.2 IP アドレスの設定 28
1.3 SNMP による管理 33
1.3.1 コミュニティ文字列(SNMP バージョン 1 および 2c クライアント用) 33
1.3.2 トラップレシーバ 33
1.3.3 SNMP バージョン 3 クライアントへのアクセス 34
1.4 システムファイルの管理 35
1.4.1 オペレーションコードのアップグレード 35
1.4.2 コンフィグレーションの保存と復元 37
1.5 オペレーションコードとコンフィグレーションの自動インストール 39
1.5.1 ファイルサーバからのオペレーションコードのダウンロード 39
1.5.2 DHCP クライアント識別子の指定 45
1.6 ゼロタッチプロビジョニング 47
1.7 システムクロックの設定 52
1.7.1 時刻の手動設定 52
1.7.2 SNTP の設定 53
1.7.3 NTP の設定 53
2 コマンドラインインタフェースの使用 55
2.1 CLI へのアクセス 56
2.1.1 コンソール接続 56
2.1.2 Telnet 接続 56
2.2 コマンドの入力 58
2.2.1 キーワードおよび引数 58
2.2.2 最小略称 58
2.2.3 補完 58
2.2.4 コマンドに関するヘルプの入手 58
2.2.5 部分キーワード検索 61
2.2.6 コマンド削除または機能無効化 61
2.2.7 コマンド履歴の使用 61
2.2.8 コマンドモードについて 61
2.2.9 Exec コマンド 62
2.2.10 Configuration コマンド 62

2.2.11 コマンドライン処理 64
2.2.12 ステータス情報の表示 64
2.3 CLI コマンドグループ 66
3 一般コマンド 68
3.1.1 prompt 68
3.1.2 reload (Global Configuration) 69
3.1.3 enable 70
3.1.4 quit 71
3.1.5 show history 71
3.1.6 configure 72
3.1.7 disable 73
3.1.8 reload (Privileged Exec) 73
3.1.9 show reload 74
3.1.10 end 74
3.1.11 exit 75
4 システム管理コマンド 76
4.1 デバイスの指定 77
4.1.1 hostname 77
4.2 システムステータス 78
4.2.1 show access-list tcam-utilization 78
4.2.2 show memory 79
4.2.3 show process cpu 80
4.2.4 show process cpu guard 81
4.2.5 show process cpu task 82
4.2.6 show running-config 83
4.2.7 show startup-config 85
4.2.8 show system 86
4.2.9 show tech-support 87
4.2.10 show users 104
4.2.11 show version 105
4.2.12 show watchdog 106
4.2.13 watchdog software 106
4.3 フレームサイズ 108
4.3.1 jumbo frame 108
4.4 ファイル管理 110
4.4.1 ソフトウェアの管理 110
4.4.2 boot system 110
4.4.3 copy 111
4.4.4 delete 115
4.4.5 dir 115
4.4.6 whichboot 117
4.4.7 upgrade opcode auto 117

4.4.8 upgrade opcode path 118
4.4.9 upgrade opcode reload 119
4.4.10 show upgrade 120
4.4.11 ip tftp retry 120
4.4.12 ip tftp timeout 121
4.4.13 show ip tftp 122
4.5 Line 123
4.5.1 line 123
4.5.2 databits 124
4.5.3 exec-timeout 125
4.5.4 login 126
4.5.5 parity 127
4.5.6 password 127
4.5.7 password-thresh 128
4.5.8 silent-time 129
4.5.9 speed 129
4.5.10 stopbits 130
4.5.11 timeout login response 131
4.5.12 disconnect 131
4.5.13 terminal 132
4.5.14 show line 133
4.6 イベントロギング 135
4.6.1 logging command 135
4.6.2 logging facility 136
4.6.3 logging history 136
4.6.4 logging host 137
4.6.5 logging on 138
4.6.6 logging trap 139
4.6.7 clear log 139
4.6.8 show log 140
4.6.9 show logging 141
4.7 SMTP アラート 143
4.7.1 logging sendmail 143
4.7.2 logging sendmail destination-email 143
4.7.3 logging sendmail host 144
4.7.4 logging sendmail level 145
4.7.5 logging sendmail source-email 145
4.7.6 show logging sendmail 146
4.8 時刻設定 147
4.8.1 sntp client 147
4.8.2 sntp poll 148
4.8.3 sntp server 149

4.8.4 show sntp 150
4.8.5 ntp authenticate 150
4.8.6 ntp authentication-key 151
4.8.7 ntp client 152
4.8.8 ntp server 153
4.8.9 show ntp 153
4.8.10 clock summer-time (date) 154
4.8.11 clock summer-time (predefined) 155
4.8.12 clock summer-time (recurring) 156
4.8.13 clock timezone 158
4.8.14 calendar set 158
4.8.15 show calendar 159
4.9 時間範囲設定 160
4.9.1 time-range 160
4.9.2 absolute 160
4.9.3 periodic 161
4.9.4 show time-range 162
5 SNMP コマンド 164
5.1 SNMP の基本コマンド 166
5.1.1 snmp-server 166
5.1.2 snmp-server community 166
5.1.3 snmp-server contact 167
5.1.4 snmp-server location 167
5.1.5 show snmp 168
5.2 SNMP 通知コマンド 170
5.2.1 snmp-server enable traps 170
5.2.2 snmp-server host 171
5.2.3 snmp-server enable port-traps link-up-down 173
5.2.4 snmp-server enable port-traps mac-notification 173
5.2.5 show snmp-server enable port-traps 174
5.3 SNMPv3 コマンド 175
5.3.1 snmp-server engine-id 175
5.3.2 snmp-server group 176
5.3.3 snmp-server user 177
5.3.4 snmp-server view 178
5.3.5 show snmp engine-id 179
5.3.6 show snmp group 180
5.3.7 show snmp user 181
5.3.8 show snmp view 182
5.4 通知ログコマンド 184
5.4.1 nlm 184
5.4.2 snmp-server notify-filter 184

5.4.3 show nlm oper-status 185
5.4.4 show snmp notify-filter 186
5.5 プライベートトラップコマンド 187
5.5.1 memory 187
5.5.2 process cpu 187
5.5.3 process cpu guard 188
6 RMON コマンド 190
6.1 コマンド説明 191
6.1.1 rmon alarm 191
6.1.2 rmon event 192
6.1.3 rmon collection history 193
6.1.4 rmon collection rmon1 194
6.1.5 show rmon alarms 195
6.1.6 show rmon events 195
6.1.7 show rmon history 196
6.1.8 show rmon statistics 196
7 sFlow コマンド 198
7.1 コマンド説明 199
7.1.1 sflow owner 199
7.1.2 sflow polling instance 200
7.1.3 sflow sampling instance 200
7.1.4 show sflow 201
8 ログインセキュリティ 203
8.1 ユーザアカウントおよび特権レベル 204
8.1.1 enable password 204
8.1.2 username 205
8.1.3 privilege 206
8.1.4 show privilege 207
8.2 認証シーケンス 208
8.2.1 authentication enable 208
8.2.2 authentication login 209
8.3 RADIUS Client 211
8.3.1 radius-server acct-port 211
8.3.2 radius-server auth-port 211
8.3.3 radius-server host 212
8.3.4 radius-server key 213
8.3.5 radius-server encrypted-key 214
8.3.6 radius-server retransmit 214
8.3.7 radius-server timeout 215
8.3.8 show radius-server 216
8.4 TACACS+ Client 217

8.4.1 tacacs-server host 217
8.4.2 tacacs-server key 218
8.4.3 tacacs-server encrypted-key 218
8.4.4 tacacs-server port 219
8.4.5 tacacs-server retransmit 219
8.4.6 tacacs-server timeout 220
8.4.7 show tacacs-server 221
8.5 AAA 222
8.5.1 aaa accounting commands 222
8.5.2 aaa accounting exec 223
8.5.3 aaa accounting update 224
8.5.4 aaa authorization commands 225
8.5.5 aaa authorization exec 225
8.5.6 aaa group server 226
8.5.7 server 227
8.5.8 accounting commands 228
8.5.9 accounting exec 228
8.5.10 authorization commands 229
8.5.11 authorization exec 229
8.5.12 show accounting 230
8.5.13 show authorization 231
8.6 Web サーバ 233
8.6.1 ip http authentication 233
8.6.2 ip http port 234
8.6.3 ip http server 234
8.6.4 ip http secure-port 235
8.6.5 ip http secure-server 235
8.7 Telnet サーバ 238
8.7.1 ip telnet max-sessions 238
8.7.2 ip telnet port 239
8.7.3 ip telnet server 239
8.7.4 telnet (client) 239
8.7.5 show ip telnet 240
8.8 SSH 241
8.8.1 設定ガイドライン 241
8.8.2 ip ssh authentication-retries 243
8.8.3 ip ssh server 243
8.8.4 ip ssh server-key size 244
8.8.5 ip ssh timeout 245
8.8.6 delete public-key 245
8.8.7 ip ssh crypto host-key generate 246
8.8.8 ip ssh crypto zeroize 247
8.8.9 ip ssh save host-key 247

8.8.10 show ip ssh 248
8.8.11 show public-key 248
8.8.12 show ssh 249
8.9 IP フィルタの管理 251
8.9.1 management 251
8.9.2 show management 252
8.10 EAPOL の透過 254
8.10.1 dot1x eapol-pass-through 254
9 セキュリティの設定 255
9.1 ポートセキュリティ 256
9.1.1 mac-learning 256
9.1.2 port security 257
9.1.3 show port security 258
9.2 DHCPv4 スヌーピング 261
9.2.1 ip dhcp snooping 261
9.2.2 ip dhcp snooping information option 263
9.2.3 ip dhcp snooping information option encode no-subtype 264
9.2.4 ip dhcp snooping information option remote-id 265
9.2.5 ip dhcp snooping information option tr101 board-id 266
9.2.6 ip dhcp snooping information policy 267
9.2.7 ip dhcp snooping verify mac-address 267
9.2.8 ip dhcp snooping vlan 268
9.2.9 ip dhcp snooping information option circuit-id 269
9.2.10 ip dhcp snooping max-number 270
9.2.11 ip dhcp snooping trust 271
9.2.12 clear ip dhcp snooping binding 272
9.2.13 clear ip dhcp snooping database flash 272
9.2.14 ip dhcp snooping database flash 272
9.2.15 show ip dhcp snooping 273
9.2.16 show ip dhcp snooping binding 274
9.3 IPv4 ソースガード 275
9.3.1 ip source-guard binding 275
9.3.2 ip source-guard 277
9.3.3 ip source-guard max-binding 278
9.3.4 ip source-guard mode 279
9.3.5 clear ip source-guard binding blocked 280
9.3.6 show ip source-guard 281
9.3.7 show ip source-guard binding 281
9.4 ARP 検査 283
9.4.1 ip arp inspection 283
9.4.2 ip arp inspection filter 284
9.4.3 ip arp inspection log-buffer logs 285

9.4.4 ip arp inspection validate 286
9.4.5 ip arp inspection vlan 287
9.4.6 ip arp inspection limit 288
9.4.7 ip arp inspection trust 288
9.4.8 show ip arp inspection configuration 289
9.4.9 show ip arp inspection interface 289
9.4.10 show ip arp inspection log 290
9.4.11 show ip arp inspection statistics 290
9.4.12 show ip arp inspection vlan 291
9.5 DoS 攻撃プロテクション 292
9.5.1 dos-protection echo-chargen 292
9.5.2 dos-protection smurf 293
9.5.3 dos-protection tcp-flooding 293
9.5.4 dos-protection tcp-null-scan 294
9.5.5 dos-protection tcp-syn-fin-scan 294
9.5.6 dos-protection tcp-xmas-scan 295
9.5.7 dos-protection udp-flooding 295
9.5.8 dos-protection win-nuke 296
9.5.9 show dos-protection 296
9.6 トラフィックセグメンテーション 298
9.6.1 traffic-segmentation 298
9.6.2 traffic-segmentation session 299
9.6.3 traffic-segmentation uplink/downlink 300
9.6.4 traffic-segmentation uplink-to-uplink 301
9.6.5 show traffic-segmentation 302
10 アクセス制御リスト 303
10.1 IPv4 ACLs 304
10.1.1 access-list ip 304
10.1.2 permit, deny (Standard IP ACL) 305
10.1.3 permit, deny (Extended IPv4 ACL) 306
10.1.4 ip access-group 308
10.1.5 show ip access-group 309
10.1.6 show ip access-list 309
10.2 IPv6 ACLs 311
10.2.1 access-list ipv6 311
10.2.2 permit, deny (Standard IPv6 ACL) 312
10.2.3 permit, deny (Extended IPv6 ACL) 313
10.2.4 ipv6 access-group 315
10.2.5 show ipv6 access-group 316
10.2.6 show ipv6 access-list 316
10.3 MAC ACLs 317
10.3.1 access-list mac 317

10.3.2 permit, deny (MAC ACL) 318
10.3.3 mac access-group 320
10.3.4 show mac access-group 321
10.3.5 show mac access-list 321
10.4 ARP ACLs 323
10.4.1 access-list arp 323
10.4.2 permit, deny (ARP ACL) 324
10.4.3 show access-list arp 325
10.5 ACL 情報 326
10.5.1 clear access-list hardware counters 326
10.5.2 show access-group 326
10.5.3 show access-list 327
11 インタフェースコマンド 329
11.1 インタフェース設定 331
11.1.1 interface 331
11.1.2 capabilities 331
11.1.3 description 332
11.1.4 flowcontrol 333
11.1.5 history 334
11.1.6 media-type 335
11.1.7 negotiation 335
11.1.8 shutdown 336
11.1.9 speed-duplex 337
11.1.10 clear counters 337
11.1.11 show interfaces brief 338
11.1.12 show interfaces counters 339
11.1.13 show interfaces history 343
11.1.14 show interfaces status 344
11.1.15 show interfaces switchport 346
11.2 トランシーバ閾値設定 348
11.2.1 transceiver-monitor 348
11.2.2 transceiver-threshold-auto 348
11.2.3 transceiver-threshold current 349
11.2.4 transceiver-threshold rx-power 350
11.2.5 transceiver-threshold temperature 351
11.2.6 transceiver-threshold tx-power 351
11.2.7 transceiver-threshold voltage 352
11.2.8 show interfaces transceiver 353
11.2.9 show interfaces transceiver-threshold 354
11.3 ケーブル診断 356
11.3.1 test cable-diagnostics 356
11.3.2 show cable-diagnostics 356

12 リンクアグリゲーションコマンド 358
12.1 ガイドライン 359
12.2 静的トランク設定コマンド 360
12.2.1 port channel load-balance 360
12.2.2 channel-group 361
12.3 動的トランク設定コマンド 362
12.3.1 lacp 362
12.3.2 lacp admin-key (Ethernet Interface) 363
12.3.3 lacp system-priority 364
12.3.4 lacp admin-key (Port Channel) 365
12.3.5 lacp timeout 365
12.4 トランクステータス表示コマンド 367
12.4.1 show lacp 367
12.4.2 show port-channel load-balance 370
13 PoE コマンド 371
13.1 コマンド説明 372
13.1.1 power inline compatible 372
13.1.2 power inline maximum allocation mode 372
13.1.3 power mainpower maximum allocation 373
13.1.4 power inline 374
13.1.5 power inline maximum allocation 375
13.1.6 power inline priority 376
13.1.7 power inline time-range 377
13.1.8 show power inline status 377
13.1.9 show power inline time-range 379
13.1.10 show power mainpower 379
14 ポートミラーリングコマンド 381
14.1 ローカルポートミラーリングコマンド 382
14.1.1 port monitor 382
14.1.2 show port monitor 383
14.2 RSPAN ミラーリングコマンド 384
14.2.1 rspan source 385
14.2.2 rspan destination 386
14.2.3 rspan remote vlan 387
14.2.4 no rspan session 388
14.2.5 show rspan 388
15 輻輳制御コマンド 390
15.1 レート制限コマンド 391
15.1.1 rate-limit 391
15.2 ストームコントロールコマンド 394
15.2.1 switchport packet-rate 394

16 ループ検知コマンド 396
16.1 使用上のガイドライン 397
16.2 コマンド説明 398
16.2.1 loopback-detection 398
16.2.2 loopback-detection action 398
16.2.3 loopback-detection recover-time 399
16.2.4 loopback-detection transmit-interval 400
16.2.5 loopback-detection trap 400
16.2.6 loopback-detection release 401
16.2.7 show loopback-detection 402
17 MAC アドレステーブルコマンド 403
17.1 コマンド説明 404
17.1.1 mac-address-table aging-time 404
17.1.2 mac-address-table static 404
17.1.3 clear mac-address-table dynamic 405
17.1.4 show mac-address-table 406
17.1.5 show mac-address-table aging-time 407
17.1.6 show mac-address-table count 408
18 スパニングツリーコマンド 409
18.1 コマンド説明 411
18.1.1 spanning-tree 411
18.1.2 spanning-tree forward-time 411
18.1.3 spanning-tree hello-time 412
18.1.4 spanning-tree max-age 413
18.1.5 spanning-tree mode 413
18.1.6 spanning-tree mst configuration 415
18.1.7 spanning-tree pathcost method 415
18.1.8 spanning-tree priority 416
18.1.9 spanning-tree system-bpdu-flooding 417
18.1.10 spanning-tree transmission-limit 417
18.1.11 max-hops 418
18.1.12 mst priority 418
18.1.13 mst vlan 419
18.1.14 name 420
18.1.15 revision 421
18.1.16 spanning-tree bpdu-filter 421
18.1.17 spanning-tree bpdu-guard 422
18.1.18 spanning-tree cost 423
18.1.19 spanning-tree edge-port 424
18.1.20 spanning-tree link-type 425
18.1.21 spanning-tree loopback-detection 426

18.1.22 spanning-tree loopback-detection action 426
18.1.23 spanning-tree loopback-detection release-mode 427
18.1.24 spanning-tree loopback-detection trap 428
18.1.25 spanning-tree mst cost 428
18.1.26 spanning-tree mst port-priority 429
18.1.27 spanning-tree port-bpdu-flooding 430
18.1.28 spanning-tree port-priority 431
18.1.29 spanning-tree root-guard 431
18.1.30 spanning-tree spanning-disabled 432
18.1.31 spanning-tree tc-prop-stop 433
18.1.32 spanning-tree loopback-detection release 433
18.1.33 spanning-tree protocol-migration 434
18.1.34 show spanning-tree 435
18.1.35 show spanning-tree mst configuration 437
19 VLAN コマンド 439
19.1 VLAN グループの設定 440
19.1.1 vlan database 440
19.1.2 vlan 440
19.2 VLAN インタフェースの設定 442
19.2.1 interface vlan 442
19.2.2 switchport acceptable-frame-types 443
19.2.3 switchport allowed vlan 444
19.2.4 switchport forbidden vlan 445
19.2.5 switchport mode 446
19.2.6 switchport native vlan 446
19.3 VLAN 情報の表示 448
19.3.1 show vlan 448
19.4 IEEE 802.1Q トンネリングの設定 449
19.4.1 dot1q-tunnel system-tunnel-control 450
19.4.2 dot1q-tunnel tpid 450
19.4.3 switchport dot1q-tunnel mode 451
19.4.4 show dot1q-tunnel 452
19.5 プロトコルベースの VLAN の設定 453
19.5.1 protocol-vlan protocol-group (Configuring Groups) 453
19.5.2 protocol-vlan protocol-group (Configuring Interfaces) 454
19.5.3 show protocol-vlan protocol-group 455
19.5.4 show interfaces protocol-vlan protocol-group 455
19.6 MAC ベースの VLAN の設定 457
19.6.1 mac-vlan 457
19.6.2 show mac-vlan 458
20 CoS コマンド 459
20.1 優先制御コマンド（レイヤ 2） 460

20.1.1 queue mode 460
20.1.2 queue weight 461
20.1.3 switchport priority default 462
20.1.4 show queue mode 463
20.1.5 show queue weight 464
20.2 優先制御コマンド（レイヤ 3 および 4） 465
20.2.1 qos map cos-queue 465
20.2.2 qos map dscp-queue 466
20.2.3 qos map trust-mode 467
20.2.4 show qos map cos-queue 468
20.2.5 show qos map dscp-queue 469
20.2.6 show qos map trust-mode 470
21 QoS コマンド 471
21.1 コマンド説明 473
21.1.1 class-map 473
21.1.2 description 473
21.1.3 match 474
21.1.4 rename 475
21.1.5 policy-map 476
21.1.6 class 476
21.1.7 police rate 477
21.1.8 set cos 478
21.1.9 set ip dscp 479
21.1.10 service-policy 480
21.1.11 show class-map 480
21.1.12 show policy-map 481
21.1.13 show policy-map interface 482
22 マルチキャストフィルタリングコマンド 483
22.1 IGMP snooping 484
22.1.1 ip igmp snooping 485
22.1.2 ip igmp snooping mrouter-forward-mode dynamic 485
22.1.3 ip igmp snooping proxy-reporting 486
22.1.4 ip igmp snooping querier 487
22.1.5 ip igmp snooping router-alert-option-check 487
22.1.6 ip igmp snooping router-port-expire-time 488
22.1.7 ip igmp snooping tcn-flood 489
22.1.8 ip igmp snooping tcn-query-solicit 489
22.1.9 ip igmp snooping unregistered-data-flood 490
22.1.10 ip igmp snooping unsolicited-report-interval 491
22.1.11 ip igmp snooping version 491
22.1.12 ip igmp snooping version-exclusive 492
22.1.13 ip igmp snooping vlan general-query-suppression 493

22.1.14 ip igmp snooping vlan immediate-leave 494
22.1.15 ip igmp snooping vlan last-memb-query-count 494
22.1.16 ip igmp snooping vlan last-memb-query-intvl 495
22.1.17 ip igmp snooping vlan mrouter 496
22.1.18 ip igmp snooping vlan proxy-address 497
22.1.19 ip igmp snooping vlan query-interval 498
22.1.20 ip igmp snooping vlan query-resp-intvl 498
22.1.21 ip igmp snooping vlan static 499
22.1.22 clear ip igmp snooping groups dynamic 500
22.1.23 clear ip igmp snooping statistics 501
22.1.24 show ip igmp snooping 501
22.1.25 show ip igmp snooping group 502
22.1.26 show ip igmp snooping mrouter 503
22.1.27 show ip igmp snooping statistics 504
22.2 IGMP フィルタリングおよびスロットリング 508
22.2.1 ip igmp filter (Global Configuration) 508
22.2.2 ip igmp profile 509
22.2.3 permit, deny 510
22.2.4 range 510
22.2.5 ip igmp filter (Interface Configuration) 511
22.2.6 ip igmp max-groups 512
22.2.7 ip igmp max-groups action 512
22.2.8 ip igmp query-drop 513
22.2.9 ip multicast-data-drop 514
22.2.10 show ip igmp filter 514
22.2.11 show ip igmp profile 515
22.2.12 show ip igmp query-drop 516
22.2.13 show ip igmp throttle interface 516
22.2.14 show ip multicast-data-drop 517
22.3 MLD snooping 519
22.3.1 ipv6 mld snooping 520
22.3.2 ipv6 mld snooping proxy-reporting 520
22.3.3 ipv6 mld snooping querier 521
22.3.4 ipv6 mld snooping query-interval 521
22.3.5 ipv6 mld snooping query-max-response-time 522
22.3.6 ipv6 mld snooping robustness 523
22.3.7 ipv6 mld snooping router-port-expire-time 524
22.3.8 ipv6 mld snooping unknown-multicast mode 524
22.3.9 ipv6 mld snooping unsolicited-report-interval 525
22.3.10 ipv6 mld snooping version 526
22.3.11 ipv6 mld snooping vlan immediate-leave 526
22.3.12 ipv6 mld snooping vlan mrouter 527

22.3.13 ipv6 mld snooping vlan static 528
22.3.14 clear ipv6 mld snooping groups dynamic 528
22.3.15 clear ipv6 mld snooping statistics 529
22.3.16 show ipv6 mld snooping 529
22.3.17 show ipv6 mld snooping group 530
22.3.18 show ipv6 mld snooping mrouter 533
22.3.19 show ipv6 mld snooping statistics 533
22.4 MLD フィルタリングおよびスロットリング 538
22.4.1 ipv6 mld filter (Global Configuration) 538
22.4.2 ipv6 mld profile 539
22.4.3 permit, deny 540
22.4.4 range 540
22.4.5 ipv6 mld filter (Interface Configuration) 541
22.4.6 ipv6 mld max-groups 542
22.4.7 ipv6 mld max-groups action 543
22.4.8 ipv6 mld query-drop 543
22.4.9 show ipv6 mld filter 544
22.4.10 show ipv6 mld profile 545
22.4.11 show ipv6 mld query-drop 545
22.4.12 show ipv6 mld throttle interface 546
23 LLDP コマンド 548
23.1 コマンド説明 550
23.1.1 lldp 550
23.1.2 lldp holdtime-multiplier 550
23.1.3 lldp med-fast-start-count 551
23.1.4 lldp notification-interval 551
23.1.5 lldp refresh-interval 552
23.1.6 lldp reinit-delay 553
23.1.7 lldp tx-delay 553
23.1.8 lldp admin-status 554
23.1.9 lldp basic-tlv management-ip-address 554
23.1.10 lldp basic-tlv port-description 555
23.1.11 lldp basic-tlv system-capabilities 555
23.1.12 lldp basic-tlv system-description 556
23.1.13 lldp basic-tlv system-name 557
23.1.14 lldp dot1-tlv proto-ident 557
23.1.15 lldp dot1-tlv proto-vid 558
23.1.16 lldp dot1-tlv pvid 558
23.1.17 lldp dot1-tlv vlan-name 559
23.1.18 lldp dot3-tlv link-agg 559
23.1.19 lldp dot3-tlv max-frame 560
23.1.20 lldp dot3-tlv poe 560

23.1.21 lldp med-notification 561
23.1.22 lldp med-tlv ext-poe 562
23.1.23 lldp med-tlv inventory 562
23.1.24 lldp med-tlv location 563
23.1.25 lldp med-tlv med-cap 564
23.1.26 lldp med-tlv network-policy 564
23.1.27 lldp notification 565
23.1.28 show lldp config 565
23.1.29 show lldp info local-device 567
23.1.30 show lldp info remote-device 568
23.1.31 show lldp info statistics 570
24 ドメインネームサービスコマンド 572
24.1 DNS コマンド 573
24.1.1 ip domain-list 573
24.1.2 ip domain-lookup 574
24.1.3 ip domain-name 575
24.1.4 ip host 575
24.1.5 ip name-server 576
24.1.6 ipv6 host 577
24.1.7 clear dns cache 578
24.1.8 clear host 578
24.1.9 show dns 579
24.1.10 show dns cache 579
24.1.11 show hosts 580
24.2 マルチキャスト DNS コマンド 582
24.2.1 ip mdns 582
24.2.2 show ip mdns 582
25 DHCP コマンド 583
25.1 DHCP クライアント 584
25.1.1 ip dhcp dynamic-provision 584
25.1.2 ip dhcp client class-id 586
25.1.3 ip dhcp restart client 587
25.1.4 show ip dhcp dynamic-provision 588
25.1.5 ipv6 dhcp client rapid-commit 588
25.1.6 ipv6 dhcp restart client vlan 589
25.1.7 show ipv6 dhcp duid 590
25.1.8 show ipv6 dhcp vlan 591
26 IP インタフェースコマンド 592
26.1 IPv4 インタフェース 593
26.1.1 基本的な IPv4 のコマンド 593
26.1.2 ip address 593

26.1.3 show ip interface 595
26.1.4 show ip traffic 595
26.1.5 traceroute 597
26.1.6 ping 598
26.1.7 ARP のコマンド 599
26.1.8 arp 599
26.1.9 ip proxy-arp 600
26.1.10 clear arp-cache 601
26.1.11 show arp 601
26.2 IPv6 インタフェース 603
26.2.1 ipv6 default-gateway 603
26.2.2 ipv6 address 604
26.2.3 ipv6 address autoconfig 606
26.2.4 ipv6 address eui-64 607
26.2.5 ipv6 address link-local 609
26.2.6 ipv6 enable 610
26.2.7 ipv6 mtu 612
26.2.8 show ipv6 default-gateway 613
26.2.9 show ipv6 interface 613
26.2.10 show ipv6 mtu 615
26.2.11 show ipv6 traffic 616
26.2.12 clear ipv6 traffic 620
26.2.13 ping6 621
26.2.14 traceroute6 622
26.2.15 ipv6 nd dad attempts 623
26.2.16 ipv6 nd ns-interval 625
26.2.17 ipv6 nd reachable-time 626
26.2.18 clear ipv6 neighbors 627
26.2.19 show ipv6 neighbors 627
27 IP ルーティングコマンド 629
27.1 グローバルルーティング設定 630
27.1.1 ip route 630
27.1.2 show ip route 631
付録 633
付録 A トラブルシューティング 634
付録 A.1 管理インタフェースへのアクセスに関する問題 634
付録 A.2 システムログの使用 634
付録 B 用語集 636

1 スイッチの初期設定

本章には、スイッチへの接続および基本設定手順に関する情報が含まれます。

1.1 スイッチへの接続

スイッチには、ネットワーク管理エージェントが含まれます。エージェントは、SNMP、RMON および Web ベースインタフェースを含む、あらゆる管理オプションを提供します。またコマンドラインインタフェース(CLI)を介して、設定および監視のために、PC を直接スイッチに接続することもできます。

Note: このスイッチの IPv4 アドレスは、デフォルトで DHCP を介して取得されます。このアドレスを変更するには、「1.2.2　IP アドレスの設定」を参照してください。

1.1.1 設定オプション

スイッチの HTTP web エージェントにより、スイッチパラメータ、監視ポートを設定し、Internet Explorer はバージョン 11 以上、Mozilla Firefox または Google Chrome は、最新バージョンもしくは最新より 1 つ古いバージョンの標準 Web ブラウザを使って統計を表示します。スイッチの Web 管理インタフェースは、ネットワークに接続されているどのコンピュータからも、アクセスすることができます。

CLI プログラムは、スイッチのコンソールポートに直接接続するか、ネットワーク経由で Telnet 接続することで、リモートからアクセスすることができます。

スイッチの管理エージェントは、SNMP(簡易ネットワーク管理プロトコル)もサポートしています。この SNMP エージェントは、ネットワーク管理ソフトウェアを使用して、ネットワーク内のどのシステムからでもスイッチを管理できるようにします。

スイッチの Web インタフェース、コンソールインタフェース、および SNMP エージェントを使用すると、次の管理機能を実行することができます:

- ユーザ名とパスワードの設定
- VLAN 用 IP インタフェースの設定
- SNMP パラメータの構成
- ポートの有効/無効化
- ポートのスピード/デュプレックスモードの設定
- 入力または出力レートを制限することによる、任意のポートの帯域幅の設定
- 静的アドレスフィルタリングを通じた、ポートアクセスの制御
- アクセス制御リスト(ACLs)を使用した、パケットのフィルタリング
- 最大 4094 IEEE 802.1Q VLANs の構成
- ユニキャストトラフィックのための IP ルートの構成
- IGMP マルチキャストフィルタリングの構成
- HTTP(Web インタフェースを使用)または FTP/ TFTP(コマンドラインまたは Web インタフェースを使用)を介した、システムのソフトウェアあるいは構成ファイルのアップロードおよびダウンロード。
- スパニングツリーパラメータの構成
- サービスクラス(CoS)優先順位付きキューイングの構成
- 静的または LACP のリンクアグリゲーション構成(最大 8 ポート)
- ポートミラーリングの有効化
- 過剰なブロードキャスト、マルチキャスト、または未知のユニキャストトラフィックを抑止するために、任意のポートでのストーム制御の設定

◆ システム情報および統計の表示

1.1.2 コンソールポートへの接続

スイッチは、PC または端末に接続してスイッチを監視および設定するためのコンソールポートがあります。

ターミナルエミュレーションプログラムを実行している VT100 互換のターミナル、または PC をスイッチに接続します。

端末をコンソールポートに接続するには、以下のステップに従ってください;

1. 端末、または端末エミュレーションソフトウェアを実行している PC のシリアルポートにコンソールケーブルを接続します。
2. ケーブルのもう一方の端を、スイッチのコンソールポートに接続します。
3. 端末エミュレーションソフトウェアが、以下のように設定されているかどうか確認してください;
   - 適切なシリアルポートを選択します。
   - ボーレートを 115200 bps に設定します。
   - データフォーマットを 8 データビット、1 ストップビット、パリティ無しに設定します。
   - フロー制御を”none”に設定します。
   - エミュレーションモードを VT100 に設定します。
   - HyperTerminal,を使用している場合には、Windows キーではなく、Terminal キーを選択してください。
4. スイッチの電源を入れます。
   システムがブートサイクルを完了後、ログオン画面が表示されます。

1.1.3 コマンドラインインタフェースへのログオン

CLI プログラムでは、通常アクセスレベル(Normal Exec)と特権アクセスレベル(Privileged Exec)の、2 つの異なるコマンドラインを提供します。Normal Exec で使用できるコマンドは、Privileged Exec レベルで使用可能なコマンドに比べて限定されており、情報の表示と基本的なユーティリティのコマンドのみ使用できます。スイッチパラメータを完全に構成するには、Privileged Exec レベルで CLI にアクセスする必要があります。

両方の CLI レベルへのアクセスは、ユーザ名とパスワードで制御されています。スイッチには、レベルごとにデフォルトユーザ名とパスワードがあります。デフォルトユーザ名とパスワードを使用して、Privileged Exec レベルで CLI にログインするには、以下のステップを実行してください;

1. コンソール接続を開始するには、<Enter>を押します。「ユーザアクセスの検証」手順が開始されます。
2. 「ユーザ名」のプロンプト画面で、admin を入力します。
3. 「パスワード」のプロンプト画面でも、admin と入力します。(パスワードの文字は、コンソール画面には表示されません。)
4. セッションが開き、CLI は Privileged Exec レベルでアクセスできることを示す、”Console#” プロンプトを表示します。

1.1.4 パスワードの設定

CLI プログラムに初めてログインする場合、username コマンドを使用して両方のデフォルトユーザ名の新しいパスワードを定義し、それらを記録して安全な場所に置く必要があります。

パスワードは、アルファベット最大 16 文字で構成され、大文字と小文字が区別されます。スイッチへの不

正アクセスを防ぐために、パスワードを以下のように設定してください;

1. Privileged Exec レベルにアクセスするには、デフォルトのユーザ名とパスワード "admin"を使用してコンソールインタフェースを開きます。
2. “configure”と入力し、<Enter>を押します。
3. Normal Exec レベルでは、“username guest password 0 password,” と入力してください。password はパスワードに指定する文字列を入力します。<Enter>を押します。
4. Privileged Exec レベルでは、“username admin password 0 password,” と入力してください。password はパスワードに指定する文字列を入力します。<Enter>を押します。

```
Username: admin
Password:

 CLI session with the AXprimoM210-08T※ is opened.
 To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

注※ 本マニュアルは AXprimoM210-08T Gigabit Ethernet スイッチと AXprimoM210-08P Gigabit Ethernet PoE スイッチ.について、カバーしています。ポートタイプの違いと PoE のサポート以外に、大きな違いはありません。

1.1.5 リモート接続

ネットワーク接続を介してスイッチにアクセスする前に、コンソール接続、BOOTP または DHCP プロトコルを使用して、有効な IPv4 または IPv6 アドレス、サブネットマスク、およびデフォルトゲートウェイを設定する必要があります。

スイッチの IPv4 アドレスは、デフォルトで DHCP を介して取得されます。このアドレスを手動で設定するか、または DHCP 経由で動的アドレス割当てを有効にするには、「1.2.2　IP アドレスの設定」を参照してください。

スイッチの IP パラメータを設定後、接続されたネットワーク内のどこからでもスイッチにアクセスすることができます。スイッチは、ネットワークに接続された任意のコンピュータから Telnet または SSH を使用してアクセスできます。　このスイッチは、Web ブラウザ(Internet Explorer はバージョン 11 以上、Mozilla Firefox または Google Chrome は、最新バージョンもしくは最新より 1 つ古いバージョン)を使用するコンピュータ、または SNMP ネットワーク管理ソフトウェアを使用するネットワークコンピュータから管理することもできます。

Note: 本スイッチは 8 つの Telnet セッション、または SSH セッションをサポートします。 但し、複数ユーザによる運用は控えてください。同時に接続できるセッション数の制限は Telnet セッションのみ設定可能です。

Note: どの VLAN グループにも、スイッチを管理するための IP インタフェースアドレスを割当てることができます。

1　スイッチの初期設定

スイッチは、基本的な構成機能へのアクセスのみを提供します。SNMP 管理機能のすべてにアクセスするには、SNMP ベースのネットワーク管理ソフトウェアを使用する必要があります。

1.2 リモート管理

1.2.1 ネットワークインタフェースの使用

スイッチは、帯域内管理と呼ばれる運用ネットワークを通じて管理することができます。帯域内管理トラフィックは、運用ネットワークトラフィックと混在しているため、ACL や VLAN タグなどの標準ネットワークポートに通常適用されるすべてのフィルタリングルールの影響を受けます。帯域内ネットワーク管理は、任意のネットワークポートへの接続を介してアクセスできます。

1.2.2 IP アドレスの設定

ネットワーク経由で管理アクセスを許可するには、スイッチの IP アドレス情報を設定する必要があります。これは、以下のいずれかの方法で実行することができます。

- 手動 – IP アドレスおよびサブネットマスクを含む、情報を入力する必要があります。もし管理ステーションが、スイッチと同じ IP サブネットでない場合、デフォルトゲートウェイルータを指定する必要もあります。
- 動的 — このスイッチは、IPv4 設定要求をネットワーク上の BOOTP または DHCP アドレス割当てサーバに送信するか、ルータアドバタイズメントメッセージで受信したローカルサブネットアドレスプレフィクスにもとづいて一意の IPv6 ホストアドレスを自動的に生成します。ローカルネットワークで使用する IPv6 リンクローカルアドレスは、動的に生成することもできます。

このスイッチはルータとして設計されているので、IPv6 用の DHCP をサポートしていません。IPv6 グローバルユニキャストアドレスを複数のサブネットを含むネットワークで使用する場合は、手動でのみ構成することができます。

(1) 手動コンフィグレーション

IP アドレスをスイッチへ、手動で割当てることができます。また、このデバイスと別のネットワークセグメントに存在する管理ステーションとの間に存在するデフォルトゲートウェイを指定する必要があります。有効な IPv4 アドレスは、ピリオドで区切られた 0 から 255 の 4 つの 10 進数で構成されます。このフォーマット以外のものは、CLI プログラムによって受け入れられません。

Note: デフォルトゲートウェイが定義されていない場合の VLAN 1 のデフォルト IPv4 アドレスとサブネットマスクは、192.168.2.10 255.255.255.255 です。

(a) IPv4 アドレスの割当て

スイッチへ IP アドレスを割当てる前に、ネットワーク管理者から以下の情報を取得する必要があります:

- スイッチの IP アドレス
- ネットワークのネットワークマスク

スイッチへ IPv4 アドレスを割当てるには、下記のステップを完了させてください:

1. “Global Configuration”モードのプロンプトで、”interface-configuration”モードにアクセスするには、”interface vlan 1”と入力します。<Enter>を押します。
2. “ip address ip-address netmask”と入力します。”ip-address”にはスイッチの IP アドレス、”netmask”にはネットワークのネットワークマスクを入力します。<Enter>を押します。
3. “exit”と入力して、グローバル設定モードプロンプトに戻ります。<Enter>を押します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
```

(b) IPv6 アドレスの割当て

本章では、ローカルサブネット内での接続にのみ“link local”アドレスを設定する方法と、マルチセグメントネットワークで使用するネットワークプレフィックスと、ネットワークセグメントのホスト部分を含む“global unicast”アドレスを設定する方法についても説明します。

IPv6 プレフィックスまたはアドレスは、RFC 2373 “IPv6 Addressing Architecture” に従って、8 つのコロンで区切られた 16 ビットの 16 進数を使用して書式設定する必要があります。1 つのダブルコロンを使用して、未定義フィールドを埋めるために必要なゼロの適切な数を示すことができます。IPv6 アドレスの他の割当て方法に関する情報については、「26.2 IPv6 インタフェース」を参照してください。

リンクローカルアドレス - すべてのリンクローカルアドレスは、FE80 から FEBF の範囲内のプレフィックスで構成する必要があります。このアドレスタイプは、同じローカルサブネットにのみ接続されたすべてのデバイスに対して、IPv6 経由でスイッチにアクセスできるようにします。また、スイッチが設定したアドレスがサブネット上の別のデバイスで使用中のアドレスと競合したことを検出すると、問題のアドレスの使用を停止し、ローカルサブネット上の他のデバイスと競合しない、リンクローカルアドレスを自動的に生成します。

スイッチの IPv6 リンクローカルアドレスを構成するには、下記のステップを完了させてください:

1. “Global Configuration”モードのプロンプトで、”interface-configuration”モードにアクセスするには、”interface vlan 1”と入力します。<Enter>を押します。
2. “ipv6 address”と入力し、例に示すような ipv6-address のコロンで区切った 16 ビットの 16 進数を 8 つ続け、”ink-local コマンドパラメータを続けて入力します。次に<Enter>を押します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::260:3EFF:FE11:6700 link-local
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  fe80::260:3eff:fe11:6700%1/64
Global unicast address(es):
(None)
Joined group address(es):
ff02::1:ff11:6700
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

```
Console#
```

マルチセグメントネットワークのアドレス - マルチセグメントネットワークへの接続に使用するスイッチに IPv6 アドレスを割当てる前に、ネットワークの管理者から次の情報を入手する必要があります。

- ◆ ネットワークのプレフィックス
- ◆ スイッチの IP アドレス
- ◆ ネットワークのデフォルトゲートウェイ

複数の異なるサブネットを含むネットワークの場合は、ネットワークプレフィックスとスイッチのホストアドレスなど、完全なアドレスを定義する必要があります。 IPv6 全アドレス、または IPv6 アドレスとプレフィックス長のいずれかを指定することができます。 IPv6 ネットワークのプレフィックス長は、ネットワークアドレスを形成するプレフィックスのビット数(左から)であり、10 進数で表示されます。たとえば、73 の最初のバイト(16 進数)で始まるすべての IPv6 アドレスは、73：0：0：0：0：0：0：0/8 または 73::/8 として表すことができます。

スイッチの IPv6 グローバルユニキャストアドレスを生成するには、以下のステップを完了する必要があります:

1. “Global Configuration”モードプロンプトから、“interface vlan 1”を入力し、” interface-configuration”モードにアクセスします。<Enter>を押します。
2. インタフェースのプロンプトで、“ipv6 address ipv6-address”または“ipv6-address/prefix-length”と入力します。”prefix-length”はアドレスのネットワーク部分を形成するために使用されるアドレスビットを示します。 (ネットワークアドレスはプレフィックスの左側から始まり、ipv6-address ビットの一部を取り囲む必要があります。)残りのビットはホストインタフェースに割当てられます。<Enter>を押します。
3. “exit”と入力して、グローバル設定モードプロンプトに戻ります。<Enter>を押します。
4. スイッチが所属するネットワークの IPv6 デフォルトゲートウェイの IP アドレスを設定するには、” ipv6 default-gateway gateway”と入力します。”gateway”はデフォルトゲートウェイの IPv6 アドレスです。<Enter>を押します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::/64
Console(config-if)#exit
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)end
Console#show ipv6 interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-12-E2-00-00-FD
  Index: 1001, MTU: 1500
  Address Mode is DHCP
IPv6 is enabled.
Link-local address:
  fe80::260:3eff:fe11:6700%1/64
Global unicast address(es):
  2001:db8:2222:7272::/64, subnet is 2001:db8:2222:7272::/64
Joined group address(es):
ff02::1:ff00:0
ff02::1:ff11:6700
ff02::1
```

```
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#show ipv6 default-gateway
IPv6 default gateway 2001:db8:2222:7272::254
Console#
```

(2) 動的コンフィグレーション

(a) IPv4 アドレスの取得

“bootp”または“dhcp”オプションを選択する場合、システムは直ちにブロードキャスティングサービス要求を開始します。IP は有効化されますが、BOOTP または DHCP 返信を受信するまで機能しません。要求は IP 構成情報が BOOTP または DHCP サーバから取得されるまで、指数バックオフを使用して、数分ごとにブロードキャストされます。BOOTP および DHCP 値には、IP アドレス、サブネットマスク、およびデフォルトゲートウェイを含めることができます。DHCP / BOOTP サーバの応答が遅い場合は、"ip dhcp restart client"コマンドを使用して、サービス要求のブロードキャストを再開する必要があります。

ip dhcp restart client コマンドを使用して、BOOTP または DHCP を介してアドレスの割当てを取得するように設定された、すべての VLAN のブロードキャストサービス要求を開始することもできます。DHCP で VLAN を設定し、以前にシャットダウンしていたメンバーポートが有効になっている場合は、このコマンドを使用する必要があります。

ネットワーク上の BOOTP または DHCP アドレス割当てサーバと通信してスイッチを自動的に設定するには、以下の手順を完了してください。

1. “Global Configuration”モードのプロンプトで、”interface-configuration”モードにアクセスするには、”interface vlan 1”と入力します。<Enter>を押します。
2. ” interface-configuration”モードプロンプトで、下記のうち 1 つのコマンドを使用します:
   - DHCP を使用して IP 設定を取得するには、”ip address dhcp”を入力して、<Enter>を押します。
   - BOOTP を介して IP 設定を取得するには、“ip address bootp”を入力して、<Enter>を押します。
3. “end”を入力し、” Privileged Exec”モードに戻ります<Enter>を押します。
4. 数分待った後、“show ip interface”コマンドを入力して、IP コンフィグレーションを確認します。<Enter>を押します。
5. 次に、“copy running-config startup-config”を入力して、構成の変更を保存します。スタートアップファイル名を入力して、<Enter>を押します。

"bootp"または "dhcp"オプションが”startup-config”ファイルに保存されている場合、スイッチは電源がオンになるとすぐにブロードキャストサービス要求を開始します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
```

```
  Address is 00-12-E2-03-01-D0
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.13.239 Mask: 255.255.255.128
  Proxy ARP is disabled
  DHCP Client Vendor Class ID (text): AXprimoM210-08T
  DHCP Relay Server:
Console#copy running-config startup-config
Startup configuration file name []: startup
¥Write to FLASH Programming.
¥Write to FLASH finish.
Success.
```

(b) IPv6 アドレスの取得

リンクローカルアドレス - IPv6 アドレスを構成するために、複数の方法があります。簡単な方法は、自動的に”リンクローカル”アドレスを生成することです(FE80~FEBF の範囲で、アドレスプレフィックスを識別)。このアドレスタイプを使用すると、同じローカルサブネットに接続されているすべてのデバイスのスイッチが、IPv6 経由でアクセス可能になります。

スイッチの IPv6 リンクローカルアドレスを生成するには、下記のステップを完了させてください:

1. “Global Configuration”モードのプロンプトで、”interface-configuration”モードにアクセスするには、”interface vlan 1”と入力します。<Enter>を押します。
2. “ipv6 enable”を入力し、<Enter>を押します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  fe80::2e0:cff:fe00:fd%1/64
Global unicast address(es):
  2001:db8:2222:7272::/64, subnet is 2001:db8:2222:7272::/64
Joined group address(es):
ff02::1:ff00:0
ff02::1:ff11:6700
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

1.3 SNMP による管理

スイッチは、SNMP (Simple Network Management Protocol) アプリケーションからの管理コマンドを受け入れるように設定することができます。SNMP 要求に応答するように、または SNMP トラップを生成するようにスイッチを設定できます。

SNMP 管理ステーションがスイッチに要求を送信すると(情報の戻し、またはパラメータの設定)、スイッチは要求したデータか、または指定したパラメータを提供します。またスイッチは、トラップメッセージを通じて(マネージャから要求されることなく)SNMP マネージャに情報を送信するように構成することもできます。このメッセージは、マネージャに特定のイベントが発生したことを通知します。

このスイッチには、SNMP バージョン 1、2c および 3 のクライアントをサポートする、SNMP エージェントが含まれます。バージョン 1 または 2c クライアントにアクセスするには、コミュニティ文字列を提供する必要があります。スイッチは、デフォルトで MIB ツリー全体の読み取りアクセス権を持つ“public”と読み取り/書き込みアクセス権を持つ”Private”のコミュニティストリングの MIB ビュー（SNMPv3 構成）を提供します。ただし、特定のセキュリティ要件に適合するバージョン 1 または 2c のコミュニティ文字列に新しいビューを割当てることができます (snmp-server view コマンドを参照してください)。

1.3.1 コミュニティ文字列(SNMP バージョン 1 および 2c クライアント用)

コミュニティ文字列は、SNMP バージョン 1 への管理アクセスを制御するために使用されます。スイッチからトラップメッセージを受信するように SNMP ステーションを認可することもできます。したがって、指定されたユーザにコミュニティ文字列を割当て、アクセスレベルを設定する必要があります。

SNMP バージョン 1 または 2c クライアントからスイッチへの認可されていないアクセスを阻止するために、デフォルトコミュニティ文字列を変更することを、推奨します。

コミュニティ文字列を構成するには、以下のステップを実行してください:

1. Privileged Exec レベルのグローバル設定モードのプロンプトで、“snmp-server community string mode,”と入力します。“string”はコミュニティアクセス文字列で、“mode”は rw (読み取り/書き込み)または ro (読み取り専用)です。<Enter>を押します。(デフォルトモードは読み取り専用となっています)。
2. 既存の文字列を削除するには、“no snmp-server community string,”と入力します。“string”は、削除するためのコミュニティアクセス文字列です。<Enter>を押します。

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```

Note: コミュニティ文字列が無い場合には、SNMP v1 および v2c クライアントからの SNMP 管理アクセスは、無効となります。

1.3.2 トラップレシーバ

スイッチからのトラップを受信するための、SNMP ステーションも指定することができます。トラップレシーバを構成するには、” snmp-server host”コマンドを使用してください。Privileged Exec レベルグローバル設定モードのプロンプトで、以下を入力してください。

“snmp-server host host-address community-string [version {1 | 2c | 3 {auth | noauth | priv}}]”

ここでの“host-address”は、トラップレシーバの IP アドレスで、“community-string”では、バージョン 1 /2c ホストのアクセス権を指定するか、バージョン 3 ホストのユーザ名を指定し、 "version"は SNMP クライアントのバージョンを示し、 "auth | noauth | priv "は、認証、認証なし、または認証とプライバシーが v3 クライアントで使用されることを意味します。次に<Enter>を押します。これらのパラメータの詳細については、snmp-server host コマンドを参照してください。下記の例は、SNMP クライアントの各タイプのトラップホストを作成します。

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

1.3.3 SNMP バージョン 3 クライアントへのアクセス

SNMPv3 クライアントへの管理アクセスを構成するには、最初にクライアントが読み書きできる MIB の部分を定義するビューを作成し、そのビューをグループに割当ててから、ユーザをグループに割当てます。下記の例では、MIB-2 ツリーブランチ全体を含む”mib-2”というビューと、IEEE 802.1d ブリッジ MIB を含む別のビューを作成します。これらのそれぞれの読み取りおよび書き込み/書き込みビューをグループ呼び出し "r&d"に割当て、MD5 または SHA によるグループ認証を指定します。最後のステップでは、MD5 が認証に使用されることを示す v3 ユーザをこのグループに割当て、認証パスワード”greenpeace”と暗号化パスワード”einstien”を、提供します。

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth read mib-2 write 802.1d
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv des56 einstien
Console(config)#
```

SNMP v3 クライアントからのアクセスのための、スイッチの構成方法に関する詳細については、「5 SNMP コマンド」か、Web 管理ガイドを参照してください。

1.4 システムファイルの管理

スイッチのフラッシュメモリは、CLI プログラム、Web インタフェース、または SNMP で管理することができる、3 タイプのシステムファイルをサポートします。スイッチのファイルシステムは、ファイルに対してアップロードやダウンロード、コピー、削除およびスタートアップファイルとして使用できます。

ファイルタイプについては、以下の通りです;

- Configuration– このファイルタイプは、システム情報を格納し、コンフィグレーションを保存するときに作成されます。保存された設定ファイルは、システム起動ファイルとして選択したり、FTP / TFTP を介してサーバにアップロードしてバックアップすることもできます。 "Factory_Default_Config.cfg" という名前のファイルには、システムの全デフォルト設定が含まれており、システムから削除することはできません。工場出荷時のデフォルト設定でシステムがブートされた場合、スイッチはスイッチの初期化のためのシステム設定を含む "ztp_startup.cfg"という名前のファイルも作成します。その中には、スイッチ初期化のためのユニット識別子、スイッチの MAC アドレスなどのシステム設定情報が含まれます。工場出荷時のデフォルト構成ファイルのコンフィグレーションがこのファイルにコピーされ、スイッチをブートするために使用されます。
- Operation Code — ブートアップ後に実行されるシステムソフトウェアで、ランタイムコードとしても知られています。このコードは、スイッチ操作を実行し、CLI と Web 管理インタフェースを提供します。
- Diagnostic Code — システムブートアップ中に実行されるソフトウェアであり、POST (パワーオンセルフテスト)としても知られています。

Note: ブート ROM とローダは、FTP/ TFTP サーバからアップロードまたはダウンロードできません。

フラッシュメモリのサイズ制限のため、スイッチは 2 つのオペレーションファイルのみサポートします。また、ユーザ定義設定ファイルは、最大 8 ファイルサポートします。なお、スイッチには、システムファイル用に合計 32M バイトのフラッシュメモリがあります。

システムフラッシュメモリでは、起動ファイルとして各種類のファイルを 1 つ設定する必要があります。システムの起動中に、起動ファイルとして設定された診断およびオペレーションコードファイルが実行され、起動設定ファイルがロードされます。

設定ファイルは、ファイル設定の内容または使用法を反映するファイル名を使用してダウンロードする必要があります。“running-config”に直接ダウンロードすると、システムが再起動し、設定を”running-config”からスタートアップコンフィグレーションファイルにコピーする必要があります。

警告: システムファイル管理を正確に実施するために、システムファイルの管理について変更等の操作を行う場合は、本スイッチへのセッションが 1 つであることを確認の上、実施してください。

1.4.1 オペレーションコードのアップグレード

下記の例では、スイッチへの新規ソフトウェアのダウンロード方法と、起動方法について示します。TFTP サーバは、Windows または Linux 上で実行されている標準準拠のサーバであればどれでもかまいません。FTP サーバからダウンロードする場合、ログオンインターフェイスはリモートサーバで設定されたユーザ名とパスワードの入力を求めます。“anonymous”がデフォルトのユーザ名として設定されていることに、注意してください。

スイッチ上のファイル名は大文字と小文字が区別されます。宛先ファイル名にスラッシュ（¥または/）を含めないでください。ファイル名の最大長は、スイッチ上のファイルの場合は 32 文字、サーバ上のファイルの場合は 127 文字です。　(有効な文字: A-Z, a-z, 0-9, “.”, “-”)

1.TFTP サーバより新バージョンのソフトウェアを本装置にダウンロードします。

```
Console#copy tftp file
TFTP server IP address: 192.168.13.230
Choose file type:
 1. config; 2. opcode: 2
Source file name: AXprimoM210_V1.2.3.X.bix
Destination file name: AXprimoM210_V1.2.3.X.bix
Flash programming started.
Flash programming completed.
Success.
```

2.フラッシュメモリ内のファイル一覧を表示し、ダウンロードに成功していることを確認します。

```
Console#dir
File Name                       Type    Startup Modified Time       Size (bytes)
------------------------------ ------- ------- ------------------- ------------
 Unit 1:
AXprimoM210_V1.2.3.X.bix        OpCode  N       20XX-08-07 13:22:35    9,785,608
AXprimoM210_V1.2.2.2X.bix       OpCode  Y       20XX-07-25 02:39:49    9,130,248
Factory_Default_Config.cfg      Config  N       20XX-07-25 02:37:46          477
startup1.cfg                    Config  Y       20XX-07-25 04:33:48        1,312
ztp_startup.cfg                 Config  N       20XX-07-16 11:39:57          867
------------------------------------------------------------------------------
                      Free space for compressed user config files: 14,635,920
                                                     Total space: 33,554,432
```

3.ダウンロードしたソフトウェアを、次回ブートアップ時に実行するシステムソフトウェアに設定します。

```
Console#configure
Console(config)#boot system opcode:AXprimoM210_V1.2.3.X.bix
Success.
Console(config)#exit
```

4. フラッシュメモリ内のファイル一覧を表示し、次回ブートアップ時に実行するシステムソフトウェアが変更されていることを確認します。

```
Console#dir
File Name                       Type    Startup Modified Time       Size (bytes)
------------------------------ ------- ------- ------------------- ------------
 Unit 1:
AXprimoM210_V1.2.3.X.bix        OpCode  Y       20XX-08-07 13:22:35    9,785,608
AXprimoM210_V1.2.2.2X.bix       OpCode  N       20XX-07-25 02:39:49    9,130,248
Factory_Default_Config.cfg      Config  N       20XX-07-25 02:37:46          477
startup1.cfg                    Config  Y       20XX-07-25 04:33:48        1,312
ztp_startup.cfg                 Config  N       20XX-07-16 11:39:57          867
------------------------------------------------------------------------------
                      Free space for compressed user config files: 14,635,920
                                                     Total space: 33,554,432
```

5.装置を再起動します。

```
Console#reload
System will be restarted, continue <y/n>? y
```

1.4.2 コンフィグレーションの保存と復元

設定コマンドは、実行中の設定ファイルのみ変更し、スイッチがリブートされた時に保存されません。不揮発性ストレージにすべての設定変更を保存するには、copy コマンドを使用して、ランニングコンフィグレーションファイルをスタートアップコンフィグレーションファイルにコピーする必要があります。

新規のスタートアップコンフィグレーションファイルには、指定した名前を付ける必要があります。スイッチ上のファイル名は大文字と小文字が区別されます。1 から 31 文字の間で設定することが出来、スラッシュ（¥または/）を含めず、ファイル名の先頭文字はピリオド(.)にしないでください。(有効な文字: A-Z, a-z, 0-9, “.”, “-”, “_”)

スイッチのフラッシュメモリに、複数のユーザ定義の設定ファイルを保存することができますが、スイッチが起動するときにロードされる“startup”ファイルとして、1 つだけが指定されます。copy running-config startup-config コマンドは、常に新しいファイルをスタートアップファイルとして設定します。前回、保存した設定ファイルを選択するには、boot system config:<filename> コマンドを使用します。

保存される設定ファイルの最大数は、使用可能なフラッシュメモリによります。使用可能なフラッシュメモリの量は、dir コマンドを使用して確認できます。

現在の設定を保存するには、以下のコマンドを入力してください:

1. Privileged Exec プロンプトから、” copy running-config startup-config”を入力し、<Enter>を押します。
2. スタートアップファイル名を入力します。<Enter>を押します。

```
Console#copy running-config startup-config
Startup configuration file name []: startup
¥Write to FLASH Programming.

¥Write to FLASH finish.
Success.

Console#
```

バックアップサーバからコンフィグレーションを復元するには、以下のコマンドを入力してください:

1. Privileged Exec モードプロンプトから、“copy tftp startup-config”を入力し、<Enter>を押します。
2. TFTP サーバのアドレスを入力します。<Enter>を押します。
3. サーバに保存されているスタートアップファイル名を、入力します。<Enter>を押します。
4. スイッチ上のスタートアップファイル名を、入力します。<Enter>を押します。

```
Console#copy tftp startup-config
TFTP server IP address: 192.168.0.4
Source configuration file name: startup-rd.cfg
Startup configuration file name [startup1.cfg]:

Success.
Console#
```

1　スイッチの初期設定

1.5 オペレーションコードとコンフィグレーションの自動インストール

1.5.1 ファイルサーバからのオペレーションコードのダウンロード

自動アップグレードは、現在インストールされているファイルよりも新しいファイルがファイルサーバ上で検出されたときに、オペレーションコードファイルを自動的にダウンロードすることができます。ファイルがサーバから転送され、ファイルシステムに正常に書き込まれると、自動的にスタートアップファイルとして設定され、スイッチが再起動されます。

使用上のガイドライン

- この機能が有効化されると、スイッチは起動シーケンス中に定義された URL を一度検索します。
- FTP (ポート 21)と TFTP (ポート 69)の両方がサポートされます。TCP/UDP ポートバインディングは、非標準ポートで待ち受けているサーバをサポートするよう、変更できないことに注意してください。
- 自動アップグレードを実施する時、IP インタフェースは装置に 1 つのみとしてください。
- アップグレードファイルの場所の URL のホスト部分は、有効な IPv4 IP アドレスである必要があります。DNS ホスト名は認識されません。有効な IP アドレスは、ピリオドで区切られた 0～255 の 4 つの数字で構成されます。
- ディレクトリへのパスも、定義する必要があります。ファイルが FTP/TFTP サービスのルートディレクトリに保存されると、“/”を使用してこれを示します(例; ftp://192.168.0.1/)。
- ファイル名は、アップグレードファイルの場所の URL に含めないでください。リモートサーバに保存されたコードのファイル名は、(指示されたように、小文字を使用して) AXprimoM210.bix でなければなりません。
- FTP は、有効化された PASV モードで接続されます。FTP トラフィックがブロックされていない場合でも、PASV モードがいくつかのファイアウォールを通過する必要があります。　PASV モードを無効にすることはできません。
- スイッチベースの検索機能は、大文字または小文字のファイル名を受け入れるという点で大文字と小文字を区別しません(つまり、AXprimoM210.bix が要求されても、スイッチはサーバから AXprimoM210.BIX を受け入れます)。しかし、Unix や Unix に似たシステム(FreeBSD、NetBSD、OpenBSD や、ほとんどの Linux ディストリビューションなど）のような多くのオペレーティングシステムのファイルシステムでは、大文字と小文字が区別されます。つまり、同じディレクトリにある 2 つのファイル、axprimom210.bix および AXprimoM210.BIX は一意のファイルとみなされます。したがって、アップグレードファイルが AXprimoM210.BIX（または AxprimoM210.bix）を入力すると、スイッチ（AXprimoM210.BIX を要求)サーバは要求されたファイル名と保存されているファイル名が等しいと認識しないため、アップグレードされません。大文字と小文字を区別する Unix ライクなオペレーティングシステムのリストにある注目すべき例外は Mac OS X で、デフォルトでは大文字と小文字を区別しません。ファイルシステムの動作が不明な場合は、ご使用のサーバのオペレーティングシステムマニュアルを確認してください。
- スイッチ自体は、大文字のファイル名と小文字のファイル名を区別せず、サーバに保存されているファイルが現在のランタイムイメージより新しいかどうかを確認するだけです。
- 2 つのオペレーションコードイメージファイルが既にスイッチのファイルシステムに保存されている場合には、起動していないイメージファイルはアップグレードイメージファイルが転送される前に削除されます。
- 自動アップグレード処理が、スイッチの正常な動作(データの切り替えなど)を妨げることなく動作しま

す。

- ◆ 自動検索および転送処理中に、管理者は他のオペレーションコードイメージ、設定ファイル、パブリックキー、または HTTPS 証明書の転送またはアップグレードすることができません(例; コンフィグレーションの保存等の他の同時ファイル管理操作は不可能です)。
- ◆ アップグレード用オペレーションコードイメージは、ファイルシステムへの書き込みに成功した後に、起動イメージとして設定されます。
- ◆ スイッチは SNMP トラップを送信し、すべてのアップグレードの成功と失敗時にログエントリを作成します。
- ◆ スイッチは、アップグレードファイルがファイルシステムに書き込まれ、起動イメージとして設定された直後に、再開します。
- ◆ 自動アップグレードとゼロタッチプロビジョニングの両方が有効である場合、まずゼロタッチプロビジョニングが動作し、その後に自動アップグレードが動作します。

自動アップグレードを有効にするには、下記のコマンドを入力してください:

1. TFTP または FTP サーバを指定し、新しいオペレーションコードを確認します。
   - ■ TFTP サーバを指定した場合、下記の構文を使用する必要があります。filedir は、新規イメージが含まれるディレクトリへのパスを示します。
     tftp://192.168.0.1[/filedir]/
   - ■ FTP サーバを指定した場合、下記の構文を使用する必要があります。filedir は、新規イメージが含まれるディレクトリへのパスを示します。
     ftp://[username[:password@]]192.168.0.1[/filedir]/
     ユーザ名を省略する場合、接続のために“anonymous”が使用されます。パスワードを省略する場合、接続に空列(“”)が使用されます。
     接続にユーザ名もパスワードも要求されていない場合には、パス名に“@”の文字は使用できません。

新規コードが保存されている、TFTP サーバの指定方法を、下記に示します。

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

新規コードが保存されている、FTP サーバの指定方法を、下記に示します。

```
Console(config)#upgrade opcode path ftp://site9:billy@192.168.0.1/sm24/
Console(config)#
```

2. オペレーションコードのアップグレードが完了後、自動的に再起動して新しいコードをロードするようにスイッチを設定します。

```
Console(config)#upgrade opcode reload
Console(config)#
```

3. 新しいバージョンがサーバ上で検出されたときに、現在のオペレーションコードを自動的にアップグレードするようにスイッチを設定します。スイッチが起動し、このコマンドによって自動イメージアップグレードが有効になると、スイッチは起動時に次の手順に従います:
   a. upgrade opcode path コマンドで指定された場所で、新しいバージョンのイメージを検索します。

FTP / TFTP サーバに保存されている新しいイメージの名前は、AXprimoM210.bix である必要があります。スイッチが現在使用中のコードバージョンよりも新しいコードバージョンを検出すると、新しいイメージがダウンロードされます。2 つのコードイメージがすでにスイッチに保存されている場合には、システムを起動するように設定されていないイメージは、新しいバージョンによって上書きされます。

b. イメージがダウンロードされた後、アップグレード操作が成功したかどうかにかかわらず、スイッチはトラップメッセージを送信してログに記録します。

c. 起動イメージとして、新しいバーションを設定します。

d. 新しいイメージを使用して、システムを再起動します。

```
Console(config)#upgrade opcode auto
Console(config)#
```

4. 自動アップグレード設定を表示します。

```
Console#show upgrade
Auto Image Upgrade Global Settings:
  Status     : Enabled
  Reload Status : Enabled
  Path       : tftp://192.168.13.230/
  File Name : AXprimoM210.bix
Console#
```

アップグレード処理の例は、以下の通りです。

```
Console#dir
File Name                           Type    Startup Modified Time       Size (bytes)
--------------------------- ------- ------- ------------------- ------------
 Unit 1:
AXprimoM210_V1.2.2.2X.bix      OpCode  Y       20XX-07-15 08:11:14    9,130,248
Factory_Default_Config.cfg     Config  N       20XX-07-25 02:37:42          477
startup1.cfg                   Config  Y       20XX-08-07 13:40:14        1,218
------------------------------------------------------------------------------
                      Free space for compressed user config files: 22,368,256
                                                     Total space: 33,554,432
Console#reload
System will be restarted. Continue <y/n>? y
Console#Restarting system.


U-Boot 2011.12.(2.1.4.53590.Candidate-4)0.2.1.1 (Oct 05 20XX - 09:49:05)

CPU:500MHz LXB:200MHz MEM:300MHz
DRAM:  256 MB
SPI-F: 1x32 MB
Loading 131072B env. variables from offset 0x100000
```

```
Switch Port Count: 10
Net:   Net Initialization Skipped
eth#0
Booting...  0
<5>UC_MGR_Init: UC_MEM_Header_T: 8fa00000
<5>UC_MGR_Allocate: alloc: 8fa0010c
warm start
partition changed to nor0,3
Scanning JFFS2 FS: .. done.
### JFFS2 loading '.fs/.fmapping' to 0x83de0098
### JFFS2 load complete: 144 bytes loaded to 0x83de0098
### JFFS2 loading '.fs/AXprimoM210_V1.2.2.2X.bix' to 0x81000000
### JFFS2 load complete: 9130248 bytes loaded to 0x81000000
## Booting kernel from Legacy Image at 81000000 ...
   Image Name:   RUNTIME
   Created:      20XX-07-25  15:13:34 UTC
   Image Type:   MIPS Linux Multi-File Image (uncompressed)
   Data Size:    9130148 Bytes = 8.7 MB
   Load Address: 80000000
   Entry Point:  80283000
   Version: 1.2.2.2X
   PID: 000081ff
   Contents:
      Image 0: 2760856 Bytes = 2.6 MB
      Image 1: 6369280 Bytes = 6.1 MB
   Verifying Checksum ... OK
## Loading init Ramdisk from multi component Legacy Image at 81000000 ...
   Loading Multi-File Image ... OK
OK

Starting kernel ...

init started: BusyBox v1.7.3 (20XX-02-23 10:41:36 CST)
starting pid 591, tty '': '/etc/rc'
running rc ...
insmod module alaxala module ...
insmod module rtcore ...

Setting transition mode ...Assigned Unit ID:[1]
done

Finished setting transition mode ...
Entering transition mode ...
Finished transition mode ...
Entering master mode ...
Load certificate files : Starting
Load certificate files : Finished
---- Master state preemption
```

```
Finished master mode ...
Performing startup provision ...

.....................................................................................
.....................................................................................
.....................................................................................
.............................................................
CLI provision has been completed

Notifying provision complete

Pre-provision complete ...
Finished pre-provision complete ...
Provision complete ...
Finished provision complete ...


Press ENTER to start session
Automatic Upgrade is looking for a new image
Find new version
New image detected: current version 1.2.2.2X; new version 1.2.2.XX
Image upgrade in progress
Downloading new image
Find new version
Synchronizing to Unit 1
Flash programming started
Flash programming completed
Success
The switch will now restart
Restarting system.


U-Boot 2011.12.(2.1.4.53590.Candidate-4)0.2.1.1 (Oct 05 20XX - 09:49:05)

CPU:500MHz LXB:200MHz MEM:300MHz
DRAM:  256 MB
SPI-F: 1x32 MB
Loading 131072B env. variables from offset 0x100000
Switch Port Count: 10
Net:   Net Initialization Skipped
eth#0
Booting...  0
<5>UC_MGR_Init: UC_MEM_Header_T: 8fa00000
<5>UC_MGR_Allocate: alloc: 8fa0010c
warm start
partition changed to nor0,3
Scanning JFFS2 FS: .. done.
### JFFS2 loading '.fs/.fmapping' to 0x83de0098
### JFFS2 load complete: 144 bytes loaded to 0x83de0098
```

```
### JFFS2 loading '.fs/op1.bix' to 0x81000000
### JFFS2 load complete: 9130248 bytes loaded to 0x81000000
## Booting kernel from Legacy Image at 81000000 ...
   Image Name:   RUNTIME
   Created:      20XX-07-31  12:36:32 UTC
   Image Type:   MIPS Linux Multi-File Image (uncompressed)
   Data Size:    9130148 Bytes = 8.7 MB
   Load Address: 80000000
   Entry Point:  80283000
   Version: 118.7.31.1
   PID: 000081ff
   Contents:
      Image 0: 2760856 Bytes = 2.6 MB
      Image 1: 6369280 Bytes = 6.1 MB
   Verifying Checksum ... OK
## Loading init Ramdisk from multi component Legacy Image at 81000000 ...
   Loading Multi-File Image ... OK
OK

Starting kernel ...

init started: BusyBox v1.7.3 (20XX-02-23 10:41:36 CST)
starting pid 591, tty '': '/etc/rc'
running rc ...
insmod module alaxala module ...
insmod module rtcore ...

Setting transition mode ...Assigned Unit ID:[1]
done

Finished setting transition mode ...
Entering transition mode ...
Finished transition mode ...
Entering master mode ...
Load certificate files : Starting
Load certificate files : Finished
---- Master state preemption

Finished master mode ...
Performing startup provision ...

.....................................................................................
.....................................................................................
.....................................................................................
.............................................................
CLI provision has been completed

Notifying provision complete
```

```
Pre-provision complete ...
Finished pre-provision complete ...
Provision complete ...
Finished provision complete ...


Press ENTER to start session
Automatic Upgrade is looking for a new image
No new image detected


User Access Verification

Username: admin
Password:

      CLI session with the AXprimoM210-08P is opened.
      To end the CLI session, enter [Exit].

Console#dir
File Name                      Type    Startup Modified Time       Size (bytes)
------------------------------ ------- ------- ------------------- ------------
 Unit 1:
AXprimoM210_V1.2.2.2X.bix      OpCode  N       20XX-07-15 08:11:14    9,130,248
op1.bix                        OpCode  Y       20XX-08-08 09:44:13    9,130,248
Factory_Default_Config.cfg     Config  N       20XX-07-25 02:37:42          477
startup1.cfg                   Config  Y       20XX-08-07 13:40:14        1,218
------------------------------------------------------------------------------
                        Free space for compressed user config files: 14,450,688
                                                        Total space: 33,554,432
Console#
```

なお、新しいバージョンがサーバ上で検出されなかったときは、”No new image detected”のメッセージを出力し処理を終了します。

1.5.2 DHCP クライアント識別子の指定

DHCP サーバは、クライアントの Media Access Control(MAC)アドレス、または一意のクライアント識別子を使用して、アドレスバインディングのデータベースをインデックス付けします。クライアント識別子は、DHCP サーバへのスイッチのベンダクラスと構成を識別するために使用され、DHCP サーバはこの情報を使用してクライアントのサービス方法、または返される情報の種類を決定します。

DHCP クライアント識別子(オプション 60)は、DHCP クライアントが一意の識別子を指定するために使用します。クライアント識別子はオプションで、プライマリネットワークインターフェイスで DHCP を設定する際に指定できます。DHCP オプション 60 は、デフォルトでは無効になっています。

この DHCP オプションの一般的なフレームワークは、RFC 2132(オプション 60)に規定されています。この情報は、クライアントに関するコンフィグレーションやその他の識別情報を伝えるために使用されますが、使用する特定の文字列は、サービスプロバイダまたはネットワーク管理者が提供する必要がありま

す。次の章で説明するように、オプション 60(ベンダクラス識別子)、66(tftp-server-name)および 67(bootfile-name)ステートメントを、サーバデーモンの構成ファイルに追加することができます。

DHCP サーバがサービスを要求しているスイッチのインデックスエントリを持っている場合、TFTP サーバ名とブートファイル名で応答する必要があります。ベンダクラス識別子は、テキストまたは 16 進数のいずれかで形成することができますが、クライアントとサーバの両方で使用される形式は同じである必要があります。

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

1.6 ゼロタッチプロビジョニング

ゼロタッチプロビジョニング(以降、ダイナミックプロビジョニングと呼びます)は、スイッチをネットワークに接続したときに DHCP サーバからコンフィグレーションおよびその他パラメータを自動的にダウンロードする機能です。

DHCP サーバからスイッチに渡される情報には、ダウンロードする設定ファイルと、そのファイルにアクセスできる TFTP サーバ、およびその他のパラメータも含まれます。工場出荷時設定ファイルを使用して起動時にスイッチをプロビジョニングする場合、DHCP サーバから IP 設定を要求するだけでなく、起動設定ファイルの名前とそのファイルが保存されている TFTP サーバについても尋ねられます。

スイッチが、リモートブートアップファイルのダウンロードを許可する情報を受信すると、スイッチはこのファイルをローカルバッファに保存してから、プロビジョニングプロセスを再開します。

下記の DHCP クライアント動作に留意してください:

- DHCP サーバを通じて、ダイナミックプロビジョニングを有効化するには、ip dhcp dynamic-provision コマンドを使用して、この機能を有効にする必要があります。
- ダイナミックプロビジョニングを実施する時、IP インタフェースは装置に 1 つのみとしてください。
- TFTP サーバから受信したブートアップ設定ファイルが、そのままスイッチに保存されます。このファイル名がスイッチに既存している場合には、ファイルは上書きされます。
- ブートアップ設定ファイルの名前が工場出荷時のデフォルト設定ファイルと同じ場合、ダウンロード処理は中止され、スイッチはそれ以上の DHCP クライアント要求を送信しません。
- スイッチが、DHCP サーバから受信した情報に基づいてブートアップ設定ファイルのダウンロードに失敗した場合、スイッチはそれ以上の DHCP クライアント要求を送信しません。
- ブートアップ処理完了前に、スイッチが DHCP の応答を受信しない場合、DHCP クライアント要求を 1 分ごとに送信し続けます。これらの要求は、スイッチのアドレスが手動で設定された場合のみ中止されますが、アドレスモードが DHCP に設定されている場合は再開します。

スイッチにブートアップ設定ファイルを正常に送信するには、DHCP デーモン(この例では Linux ベースのシステムを使用しています)に、以下の情報を設定する必要があります:

- オプション 60、66 および 67 ステートメントを、デーモンの設定ファイルに追加することができます。

表 1-1 オプション 60、66 および 67 ステートメント

オプション	ステートメント	
	キーワード	パラメータ
60	vendor-class-identifier	ベンダクラス識別子を示す文字列
66	tftp-server-name	tftp サーバ名を示す文字列
67	bootfile-name	bootfile 名を示す文字列

- デフォルトでは、DHCP オプション 66/67 のパラメータは DHCP サーバの応答には含まれません。オプション 66/67 情報で DHCP 応答を要求するには、このスイッチから送信された DHCP クライアント要求に、この情報を要求する“parameter request list”が含まれています。これらの項目に加えて、クライアント要求には、DHCP サーバがデバイスを識別し、ダウンロードするための適切な設定ファイルを選択することを可能にする”vendor class identifier”も含まれています。この情報はオプション 55 および 124 に含まれています。

表 1-2 オプション 55 および 124 ステートメント

オプション	ステートメント	
	キーワード	パラメータ
55	dhcp-parameter-request-list	カンマ','で区切られた、パラメータの一覧
124	vendor-class-identifier	ベンダクラス識別子を示す文字列

次の設定例は、Linux ベースの DHCP デーモン(dhcpd.conf ファイル)に提供されています。“Vendor class” セクションでは、サーバはオプション 66 と 67 を送信して、スイッチにサーバ 192.168.255.101 から”test” 設定ファイルをダウンロードするように指示します。

```
ddns-update-style ad-hoc;

default-lease-time 600;
max-lease-time 7200;

log-facility local7;

server-name "Server1";
Server-identifier 192.168.255.250;
#option 66, 67
 option space dynamicProvision code width 1 length 1 hash size 2;
 option dynamicProvision.tftp-server-name code 66 = text;
 option dynamicProvision.bootfile-name code 67 = text;

subnet 192.168.255.0 netmask 255.255.255.0 {
  range 192.168.255.160 192.168.255.200;
  option routers 192.168.255.101;
  option tftp-server-name "192.168.255.100"; #Default Option 66
  option bootfile-name "bootfile";           #Default Option 67
}

class "Option66,67_1" {              #DHCP Option 60 Vendor class two
  match if option vendor-class-identifier = "AXprimoM210-08T";
  option tftp-server-name "192.168.255.101";
  option bootfile-name "test";
}
```

Note: “dhcpd.conf”ファイルの中の、vendor class identifier は“AXprimoM210-08T”を使用してください。

ダイナミックプロビジョニング処理の例は、以下の通りです。

```
Console#dir
File Name                      Type    Startup Modified Time       Size (bytes)
------------------------------ ------- ------- ------------------- ------------
 Unit 1:
AXprimoM210_V1.2.3.X.bix       OpCode  Y       20XX-07-15 08:11:14    9,130,248
Factory_Default_Config.cfg     Config  N       20XX-07-25 02:37:42          477
startup1.cfg                   Config  N       20XX-08-07 13:40:14        1,218
ztp_startup.cfg                Config  Y       20XX-09-20 14:15:30          885
-------------------------------------------------------------------------------
                      Free space for compressed user config files: 22,367,371
                                                     Total space: 33,554,432
Console#reload
System will be restarted. Continue <y/n>? y
Console#Restarting system.


U-Boot 2011.12.(2.1.4.53590.Candidate-4)0.2.1.1 (Oct 05 20XX - 09:49:05)

CPU:500MHz LXB:200MHz MEM:300MHz
DRAM:  256 MB
SPI-F: 1x32 MB
Loading 131072B env. variables from offset 0x100000
Switch Port Count: 10
Net:   Net Initialization Skipped
eth#0
Booting...  0
<5>UC_MGR_Init: UC_MEM_Header_T: 8fa00000
<5>UC_MGR_Allocate: alloc: 8fa0010c
warm start
partition changed to nor0,3
Scanning JFFS2 FS: .. done.
### JFFS2 loading '.fs/.fmapping' to 0x83de0098
### JFFS2 load complete: 144 bytes loaded to 0x83de0098
### JFFS2 loading '.fs/AXprimoM210_V1.2.3.X.bix' to 0x81000000
### JFFS2 load complete: 9130248 bytes loaded to 0x81000000
## Booting kernel from Legacy Image at 81000000 ...
   Image Name:   RUNTIME
   Created:      20XX-07-25  15:13:34 UTC
   Image Type:   MIPS Linux Multi-File Image (uncompressed)
   Data Size:    9785508 Bytes = 9.3 MB
   Load Address: 80000000
   Entry Point:  80283000
   Version: 1.2.3.X
   PID: 000081ff
   Contents:
      Image 0: 2760856 Bytes = 2.6 MB
      Image 1: 6369280 Bytes = 6.1 MB
```

```
   Verifying Checksum ... OK
## Loading init Ramdisk from multi component Legacy Image at 81000000 ...
   Loading Multi-File Image ... OK
OK

Starting kernel ...

init started: BusyBox v1.7.3 (20XX-02-23 10:41:36 CST)
starting pid 591, tty '': '/etc/rc'
running rc ...
insmod module alaxala module ...
insmod module rtcore ...

Setting transition mode ...Assigned Unit ID:[1]
done

Finished setting transition mode ...
Entering transition mode ...
Finished transition mode ...
Entering master mode ...
Load certificate files : Starting
Load certificate files : Finished
---- Master state preemption

Finished master mode ...
Performing startup provision ...

................................................................................
................................................................................
................................................................................
............................................................
CLI provision has been completed

Notifying provision complete

Pre-provision complete ...
Finished pre-provision complete ...
Provision complete ...
Finished provision complete ...


Press ENTER to start session
Performing the second startup provision ...
 Waiting for getting TFTP configuration file ...
 -/-¥-/-¥-/-¥-/-¥-/-¥-Writing to flash.
 /Flash programming started.
 -¥Success.
 -Warning: Startup config file will be changed.
 Warning: Startup provision will be performed again.
```

```
 admiAssigned Unit ID:[1]

 Setting transition mode ...
 Finished setting transition mode ...
 Entering transition mode ...
 CLI entering transition mode
 Finished transition mode ...
 Entering master mode ...
 Load certificate files : Starting
 Load certificate files : Finished

 Finished master mode ...
 Performing startup provision ...

.....................................................................................
.....................................................................................
.............................................................
 CLI provision has been completed

 Notifying provision complete

 Pre-provision complete ...
 Finished pre-provision complete ...
 Provision complete ...
 Finished provision complete ...

Press ENTER to start session
User Access Verification

Username: admin
Password:

      CLI session with the AXprimoM210-08P is opened.
      To end the CLI session, enter [Exit].

Console#dir
File Name                       Type    Startup Modified Time       Size (bytes)
------------------------------ ------- ------- ------------------- ------------
 Unit 1:
AXprimoM210_V1.2.3.X.bix        OpCode  Y       20XX-07-15 08:11:14    9,130,248
Factory_Default_Config.cfg      Config  N       20XX-07-25 02:37:42          477
startup1.cfg                    Config  N       20XX-08-07 13:40:14        1,218
ztp_startup.cfg                 Config  N       20XX-09-20 14:15:30          885
AXprimoM210-08P_#1.cfg          Config  Y       20XX-10-16 11:14:51       11,545
------------------------------------------------------------------------------
                      Free space for compressed user config files: 22,355,826
                                                     Total space: 33,554,432
```

1.7 システムクロックの設定

タイムサーバからの定期的なアップデートに基づいてスイッチの内部クロックを設定するために、簡易ネットワークタイムプロトコル(SNTP）またはネットワークタイムプロトコル(NTP)を使用することができます。スイッチの正確な時刻を維持することで、システムログにイベントエントリの意味のある日時を記録することができます。また手動でクロックを設定することもできます。クロックが手動で設定されていない場合や、SNTP または NTP を介して設定されていない場合には、スイッチは最後の起動時に設定された、出荷時のデフォルト設定からの時刻のみを記録します。

警告: スイッチイベントを正確に記録するために、SNTP または NTP を使うことを強く推奨します。システムクロックの手動での設定の場合、システムイベントのタイムスタンプが正確でない場合があります。

SNTP クライアントが有効な場合、スイッチは設定されたタイムサーバに時刻更新の要求を定期的に送信します。最大 3 つのタイムサーバ IP アドレスを設定することができます。　スイッチは、設定された順序で各サーバのポーリングを試みようとします。

またスイッチは、以下の時間設定についてもサポートします:

- タイムゾーン -　グリニッジ標準時間(GMT)とも呼ばれる、協定世界時(UTC)からのオフセットを指定することができます。
- サマータイム(DST) -一部の地域では、秋と春に 1 時間ずつ時間がずれます。スイッチは、1 回または定期的なクロックシフトの手動入力をサポートしています。

1.7.1 時刻の手動設定

手動でクロックを 20XX 年 4 月 1 日の 14:11:36 に設定する場合、以下のコマンドを入力します。

```
Console#calendar set 14 11 36 1 April 20XX
Console#
```

タイムゾーンを設定するには、以下のようにコマンドを入力します。

```
Console(config)#clock timezone Japan hours 8 after-UTC
Console(config)#
```

サマータイムのタイムシフトを設定するには、以下のようにコマンドを入力します。

```
Console(config)#clock summer-time SUMMER date 2 april 20XX 0 0 30 june 20XX 0 0
Console(config)#
```

クロック設定内容を表示するには、以下のコマンドを入力します。

```
Console#show calendar
 Current Time          : Jul 28 00:54:20 20XX
 Time Zone             : Japan, 08:00
```

```
 Summer Time           : SUMMER, offset 60 minutes
                         Apr 2 20XX 00:00 to Jun 30 20XX 00:00
 Summer Time in Effect : Yes
Console#
```

1.7.2 SNTP の設定

SNTP サーバをベースにしてクロックを設定すると、手動で設定した時刻よりも、ネットワークスイッチ間でより正確なクロック同期を提供できます。SNTP を設定するには、スイッチを SNTP クライアントとして設定し、それからポーリング間隔を設定し、次の例のようにタイムサーバを指定します。

```
Console(config)#sntp client
Console(config)#sntp poll 60
Console(config)#sntp server 10.1.0.19
Console(config)#exit
Console#show sntp
Current Time   : Apr  2 16:06:07 20XX
Poll Interval  : 60 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 10.1.0.19
Current Server : 10.1.0.19
Console#
```

1.7.3 NTP の設定

NTP サーバから時刻を要求することが、最も安全な方法です。NTP 認証を有効にすると、認証された NTP サーバからの信頼できる更新が確実に受信されます。認証キーとそれに関連するキー番号は一元的に管理し、NTP サーバとクライアントに手動で配布する必要があります。キー番号とキー値は、サーバとクライアントの両方で一致する必要があります。

複数のタイムサーバが設定されている場合、クライアントはすべてのタイムサーバをポーリングし、応答を比較してスイッチの最も信頼性の高い正確な時刻アップデートを決定します。

NTP 時刻同期を設定するには、以下に類似したコマンドを入力します。

```
Console(config)#ntp client
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#ntp authenticate
Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#exit
Console#show ntp
Current Time             : Apr 29 13:57:32 20XX
Polling                  : 1024 seconds
Current Mode             : unicast
NTP Status               : Enabled
NTP Authenticate Status  : Enabled
```

```
Last Update NTP Server   : 192.168.0.88        Port: 123
Last Update Time         : Mar 12 02:41:01 20XX UTC
NTP Server 192.168.0.88 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.4.22 version 3 key 19
NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885

Current Time             : Apr  2 16:28:34 20XX
Polling                  : 1024 seconds
Current Mode             : unicast
NTP Status               : Enabled
NTP Authenticate Status  : Enabled
Last Update NTP Server   : 192.168.5.23     Port: 0
Last Update Time         : Apr  2 16:00:00 20XX UTC
NTP Server 192.168.3.20 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.5.23 version 3 key 19
NTP Authentication Key 45 md5 2662T75S5658RU5424180034777
Console#
```

2 コマンドラインインタフェースの使用

本章では、コマンドラインインタフェース (CLI) の使用方法について説明します。

Note: スタックのマスターユニットを介してのみ、コンソールインタフェースにアクセスできます。

2.1 CLI へのアクセス

コンソールポートへの直接接続、Telnet または Secure Shell 接続(SSH)を介したスイッチの管理インタフェースにアクセスして、コマンドキーワードとパラメータを入力することによって、スイッチを管理することができます。スイッチのコマンドラインインターフェイス(CLI)の使用方法は、UNIX システムでコマンドを入力する方法と非常に類似しています。

2.1.1 コンソール接続

コンソールポートを介してスイッチにアクセスするには、次のステップを実行してください:

1. プロンプト表示画面で、ユーザ名とパスワードを入力します。(デフォルトユーザ名は admin と guest で、それぞれに対応するパスワードも同じです。)ユーザ名とパスワードを入力すると、CLI に“Console#”プロンプトが表示されるので、特権アクセスモード(例; Privileged Exec)を入力します。しかしながら、ゲストユーザ名とパスワードを入力した場合には、CLI には“Console>”プロンプトが表示されるので、通常アクセスモード(例; Normal Exec)を入力します。
2. 必要な作業を完了させるために、必要なコマンドを入力します。
3. 作業が終了したら、quit または exit コマンドで、セッションを終了します。

コンソールポートを介してシステムに接続後、ログイン画面が表示されます。

```
User Access Verification

Username: admin
Password:
  CLI session with the AXprimoM210-08T is opened.
  To end the CLI session, enter [Exit].

Console#
```

2.1.2 Telnet 接続

Telnet は、IP トランスポートプロトコルを通じて作動します。この環境では、管理ステーションとネットワークを通じて管理したいネットワークデバイスには、有効な IP アドレスを持つ必要があります。IP アドレスは 0 から 255 の間の 4 桁で構成され、ピリオドで区切られます。各アドレスはネットワークポーションとホストポーションで構成されます。たとえば、このスイッチに割り当てられた IP アドレス 10.1.0.1 は、ネットワーク部分(10.1.0)とホスト部分(1)で構成されています。

Note: スイッチの IP アドレスは、デフォルトでは DHCP を通じて取得されます。

Telnet セッションを通じてスイッチにアクセスするには、別の IP サブネットからスイッチを管理している場合は、まずマスターユニットの IP アドレスを設定し、デフォルトルートを設定する必要があります。下記に例を示します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
```

```
Console(config)# ip route 0.0.0.0 0.0.0.0 10.1.0.254
Console(config)#
```

企業ネットワークが、他の社外ネットワークやインターネットに接続されている場合には、登録済み IP アドレスを申請する必要があります。しかしながら、隔離されたネットワークに接続されている場合は、接続しているネットワークセグメントに一致する任意の IP アドレスを使用することができます。

スイッチに IP アドレスを設定後、下記のステップを実行すれば Telnet セッションをオープンすることができます。

1. リモートホストから、Telnet コマンドと、アクセスしたいデバイスの IP アドレスとホスト名を入力します。
2. プロンプトで、ユーザ名とシステムパスワードを入力します。CLI は、管理者が特権アクセスモード(例; Privileged Exec)を使用していることを示す“Vty-n#”プロンプト、またはゲストが通常アクセスモード(例; Normal Exec)を使用していることをゲストに示す“Vty-n>”プロンプトを表示します 。ここでは、n は現在の Telnet セッションの番号を示します。
3. 必要な作業を完了させるために、必要なコマンドを入力します。
4. 作業が終了したら、“quit”または“exit”コマンドで、セッションを終了します。

Telnet コマンド入力後、ログイン画面が表示されます。

```
Username: admin
Password:

  CLI session with the AXprimoM210-08T is opened.
  To end the CLI session, enter [Exit].

Vty-0#
```

Note: Telnet または SSH を通じて、最大 8 セッションをオープンすることができます。但し、複数ユーザによる運用は控えてください。

2.2 コマンドの入力

この章では、CLI コマンドの入力方法について説明します。

2.2.1 キーワードおよび引数

CLI コマンドは、キーワードと引数のシリーズです。キーワードはコマンドを識別し、引数が設定パラメータを指定します。たとえば、“show interfaces status ethernet 1/5,” コマンドで、show interfaces および status はキーワード、ethernet はインタフェースタイプを指定する引数、 1/5 はユニット/ポートを指定します。

以下のようにコマンドを入力することができます:

- 単一コマンドを入力するには、コマンドキーワードを入力します。
- 複数のコマンドを入力するには、各コマンドを必要な順に入力します。たとえば、” Privileged Exec” コマンドモードを有効化して、スタートアップコンフィグレーションを表示するには、以下のコマンドを入力します。”Normal Exec”モードから”Privileged Exec”モードに変更するには、デフォルトパスワード”super”を使用します。

```
Console>enable
Password:
Console#show startup-config
```

- パラメータを必要とするコマンドを入力するには、コマンドキーワードの後に必要なパラメータを入力します。たとえば、管理者のパスワードを設定するには、以下のように入力します:

```
Console(config)#username admin password 0 smith
```

2.2.2 最小略称

CLI は、コマンドを一意に識別する最小数の文字を受け入れます。たとえば、コマンド“configure”は con.として入力できます。入力が曖昧な場合には、プロンプトで、さらに入力するよう要求されます。

2.2.3 補完

Tab キーで入力を中止すると、CLI は部分的なキーワードの残りの文字を曖昧な点まで表示されます。“logging history”の例では、log の後にタブを入力すると、logging までのコマンドが表示されます。

2.2.4 コマンドに関するヘルプの入手

help コマンドを入力すると、ヘルプシステムの簡単な説明を表示することができます。また、記号“?”を使用してキーワードまたはパラメータを一覧化するための、コマンド構文を表示することができます。

コマンドの表示

コマンドプロンプトで“?”入力すると、キーワードまたはコマンドグループの最初のレベルを表示します。また特定コマンドに対して有効キーワードを表示することもできます。たとえば、コマンド“show system ?” では、可能な show コマンドのリストを表示します。

```
Console#show ?
  cluster               Display cluster
  dns                   DNS information
  dot1q-tunnel          802.1Q tunnel
  sflow                 Shows the sflow information
  upgrade               Shows upgrade information
  access-group          Access groups
  access-list           Access lists
  accounting            Uses the specified accounting list
  arp                   Information of ARP cache
  authorization         Enables EXEC accounting
  bridge-ext            Bridge extension information
  cable-diagnostics     Shows the information of cable diagnostics
  calendar              Date and time information
  class-map             Displays class maps
  debug                 State of each debugging option
  dns                   DNS information
  dos-protection        Shows the system dos-protection summary information
  dot1q-tunnel          802.1Q tunnel
  dot1x                 802.1X content
  erps                  Displays ERPS configuration
  history               Shows history information
  hosts                 Host information
  interfaces            Shows interface information
  ip                    IP information
  ipv6                  IPv6 information
  lacp                  LACP statistics
  license               Show license
  line                  TTY line information
  lldp                  LLDP
  log                   Log records
  logging               Logging setting
  loopback-detection    Shows loopback detection information
  mac                   MAC access list
  mac-address-table     Configuration of the address table
  mac-vlan              MAC-based VLAN information
  management            Shows management information
  memory                Memory utilization
  network-access        Shows the entries of the secure port.
  nlm                   Show notification log
  ntp                   Network Time Protocol configuration
  policy-map            Displays policy maps
  port                  Port characteristics
  port-channel          Port channel information
  power-save            Shows the power saving information
  privilege             Shows current privilege level
  process               Device process
  protocol-vlan         Protocol-VLAN information
  public-key            Public key information
```

```
  qos                   Quality of Service
  queue                 Priority queue information
  radius-server         RADIUS server information
  reload                Shows the reload settings
  rmon                  Remote monitoring information
  rspan                 Display status of the current RSPAN configuration
  running-config        Information on the running configuration
  sflow                 Shows the sflow information
  snmp                  Simple Network Management Protocol configuration and
                        statistics
  snmp-server           Displays SNMP server configuration
  sntp                  Simple Network Time Protocol configuration
  spanning-tree         Spanning-tree configuration
  ssh                   Secure shell server connections
  startup-config        Startup system configuration
  subnet-vlan           IP subnet-based VLAN information
  system                System information
  tacacs-server         TACACS server information
  tech-support          Technical information
  time-range            Time range
  traffic-segmentation  Traffic segmentation information
  upgrade               Shows upgrade information
  users                 Information about users logged in
  version               System hardware and software versions
  vlan                  Shows virtual LAN settings
  voice                 Shows the voice VLAN information
  watchdog              Displays watchdog status
  web-auth              Shows web authentication configuration
Console#show
```

“show interfaces ?” コマンドでは、下記の情報を表示します:

```
Console#show interfaces ?
  brief                  Shows brief interface description
  counters               Interface counters information
  history                Historical sample of interface counters information
  protocol-vlan          Protocol-VLAN information
  status                 Shows interface status
  switchport             Shows interface switchport information
  transceiver            Interface of transceiver information
  transceiver-threshold  Interface of transceiver-threshold information
Console#
```

複数ページの情報を表示するコマンドが(例：show running-config)一時停止し、もう一度ページを表示するには[Space]バー、もう一行を表示するには[Enter]キー、 停止せずに残りの情報を表示するには[a]キーを押す必要があります。他のキーを押すと、表示を終了することができます。

2.2.5 部分キーワード検索

疑問符で部分的なキーワードを中止すると、最初の文字と一致する代替語句が提供されます。(コマンドと疑問符の間にはスペースを入れないでください。)たとえば、 “s?” には、“s.”で始まるすべてのキーワードが表示されます。

```
Console#show s?
sflow           snmp            snmp-server     sntp            spanning-tree
ssh             startup-config  system
Console#show s
```

2.2.6 コマンド削除または機能無効化

多くの設定コマンドでは、コマンドの設定を取り消すか、設定をデフォルト値にリセットするために、プレフィックスキーワード “no” を入力することができます。たとえば、logging コマンドは、システムメッセージをホストサーバに記録します。”logging”を無効にするには、no logging コマンドを指定します。本書では、適用可能なすべてのコマンドの否定効果について説明します。

2.2.7 コマンド履歴の使用

CLI は、入力したコマンドの履歴を保持します。上矢印キーを押して、コマンドの履歴をスクロールバックすることができます。履歴リストに表示されたコマンドは、再度実行するか、最初に変更してから実行することができます。

show history コマンドを使用すると、最近実行されたコマンドのリストが表示されます。

2.2.8 コマンドモードについて

コマンドセットは、Exec と Configuration クラスに分割されます。通常、Exec コマンドはシステム状態に関する情報を表示、または統計カウンタをクリアします。一方、Configuration コマンドは、インタフェースパラメータの変更や、特定のスイッチング機能を有効にします。これらのクラスはさらに異なるモードに分割されています。使用可能なコマンドは、選択したモードによって異なります。現在のモードで使用可能なコマンドのリストを表示するには、プロンプトで疑問符 “?”を入力します。 コマンドクラスおよび関連モードについて、下記の表に示します:

表 2-1 一般コマンドモード

クラス	モード	
Exec	Normal Privileged	
Configuration	Global※	Access Control List Class Map DHCP IGMP Profile Interface Line Multiple Spanning Tree Policy Map Time Range VLAN Database

注※ ” Global”設定モードにアクセスするには、” Privileged Exec”モードでなければなりません。他のモードにアクセスするためには、” Global Configuration”である必要があります。

2.2.9 Exec コマンド

ユーザ名とパスワード "guest"を使用してスイッチ上で新しいコンソールセッションを開くと、システムは”Normal Exec”コマンドモード(またはゲストモード)になり、 "Console>"コマンドプロンプトが表示されます。このモードでは、ごく限られた数のコマンドしか使用できません。すべてのコマンドは、” Privileged Exec”コマンドモード(または管理者モード)からのみアクセスすることができます。“Privilege Exec”モードにアクセスするには、ユーザ名とパスワード "admin"を使用して、新しいコンソールセッションを開きます。システムは "Console#"コマンドプロンプトを表示します。“Privilege Exec”モードに入るには、通常の”Normal Exec”で、enable コマンドの後に特権レベルのパスワード "super"が続きます。

“Privileged Exec”モードに入るには、次のユーザ名とパスワードを入力します:

```
Username: admin
Password: [admin login password]

  CLI session with the AXprimoM210-08T is opened.
  To end the CLI session, enter [Exit].

Console#



Username: guest
Password: [guest login password]

  CLI session with the AXprimoM210-08T is opened.
  To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

2.2.10 Configuration コマンド

Configuration コマンドは、スイッチ設定を変更するための特権レベルコマンドです。これらのコマンドは、ランニングコンフィグレーションのみ変更し、スイッチがリブートされた時に保存されません。ランニングコンフィグレーションを不揮発性ストレージに保存するには、copy running-config startup-config コマンドを使用します。

“Configuration”コマンドは、異なるモードで組織されます:

- Global Configuration - これらのコマンドは、システムレベル設定を変更し、hostname や snmp-server community のようなコマンドを設定します。
- Access Control List Configuration - これらのコマンドは、パケットフィルタリングに使用されます。
- Class Map Configuration - 指定したトラフィックタイプの” DiffServ”クラスマップを作成します。
- IGMP Profile - プロファイルグループを作成し、IGMP フィルタプロファイル設定モードを開始します。

- Interface Configuration - これらのコマンドは、speed-duplex や negotiation のような、ポート設定を変更します。
- Line Configuration - これらのコマンドは、コンソールポートと Telnet 設定を変更し、parity や databits などを設定します。
- Multiple Spanning Tree Configuration - これらのコマンドは、選択した複数のスパニングツリーインスタンスを設定します。
- Policy Map Configuration - 複数のインタフェースに対して、DiffServ ポリシーマップを作成します。
- Time Range - PoE 機能で使用するための時間範囲を設定します。
- VLAN Configuration - VLAN グループを作成するためのコマンドが含まれます。

“Global Configuration”モードを開始するには、コマンド configure を” Privileged Exec”モードで入力します。システムプロンプトが“Console(config)#”に変わり、すべての” Global Configuration”コマンドへのアクセス特権が付与されます。

```
Console#configure
Console(config)#
```

他のモードに移行するには、コンフィグレーションプロンプトで次のようなコマンドを入力します。Privileged Exec モードに戻るには、exit または end コマンドを使用してください。

表 2-2 Configuration コマンドモード

モード	コマンド	プロンプト
Access Control List	access-list arp access-list ip standard access-list ip extended access-list ipv6 standard access-list ipv6 extended access-list mac	Console(config-arp-acl) Console(config-std-acl) Console(config-ext-acl) Console(config-std-ipv6-acl) Console(config-ext-ipv6-acl) Console(config-mac-acl)
Class Map	class-map	Console(config-cmap)
Interface	interface {ethernet port | port-channel id | vlan id}	Console(config-if)
Line	line {console | vty}	Console(config-line)
MSTP	spanning-tree mst-configuration	Console(config-mstp)
Policy Map	policy-map	Console(config-pmap)
Time Range	time-range	Console(config-time-range)
VLAN	vlan database	Console(config-vlan)

たとえば、インタフェース設定モードを開始するために、以下のコマンドを使用することができます。その後に、” Privileged Exec”モードに戻ります。

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

2.2.11 コマンドライン処理

コマンドは大文字と小文字を区別しません。現在使用可能な他のコマンドやパラメータと区別するのに十分な文字が含まれていれば、コマンドとパラメータを省略することができます。“Tab”キーを使用して部分的なコマンドを入力するか、部分的なコマンドの後に "?"文字を入力すると、一致する可能性のあるリストが表示されます。コマンドライン処理には、次の編集キー入力を使用することもできます:

表 2-3 キー入力コマンド

キー入力	機能
Ctrl-A	カーソルを、コマンドラインの開始点に移動します。
Ctrl-B	カーソルを、左の 1 文字に移動します。
Ctrl-C	現在のタスクを終了し、コマンドプロンプトを表示します。
Ctrl-E	カーソルを、コマンドラインの最後に移動します。
Ctrl-F	カーソルを、右の 1 文字に移動します。
Ctrl-K	カーソルから行末までの、すべての文字を削除します。
Ctrl-L	新しい行に、現在のコマンドラインを繰り返します。
Ctrl-N	履歴バッファに、次のコマンドラインを入力します。
Ctrl-P	最後のコマンドを入力します。
Ctrl-R	新しい行に、現在のコマンドラインを繰り返します。
Ctrl-U	カーソルから行の先頭までを削除します。
Ctrl-W	入力したすべての単語を削除します。
Esc-B	カーソルを 1 単語後ろに移動します。
Esc-D	カーソルから単語の最後までを削除します。
Esc-F	カーソルを 1 単語前に移動します。
Delete キーまたは BackSpace キー	コマンド入力時に間違いを消去します。

2.2.12 ステータス情報の表示

指定した処理に設定内容やステータスを表示する、あらゆる種類の show コマンドがあります。これらのコマンドの多くは、スイッチが正しく設定されていないと情報を表示しない場合があります。また、コマンドが適用されるインタフェースがアップしていないと情報を表示しない場合もあります。

たとえば、静的ルータポートが設定されている場合、対応する show コマンドは IGMP スヌーピングが無効で、静的ルータポートのリンクがアップでない限り情報を表示しません。

```
Console#configure
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#end
Console#show ip igmp snooping mrouter
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
Console#configure
Console(config)#ip igmp snooping
Console(config)#end
Console#show ip igmp snooping mrouter
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
 1    Eth 1/11            Static
```

```
Console#
```

2.3 CLI コマンドグループ

システムコマンドは、以下のように機能グループで分類することができます。

表 2-4 コマンドグループインデックス

コマンドグループ	説明
一般コマンド	特権アクセスモードの開始、システムの再起動、または CLI を終了するための基本コマンドです。
システム管理コマンド	システム情報、基本動作モード、最大フレームサイズ、ファイル管理、コンソールポートと telnet 設定、システムログ、SMTP アラート、およびシステムクロックの表示と設定。
SNMP コマンド	コミュニティアクセス文字列とトラップ受信者を設定して、認証失敗トラップをアクティブにします。
RMON コマンド	統計、履歴、アラームおよびイベントグループをサポートします。
ログインセキュリティ	ユーザ名とパスワード、コマンド特権レベル、ローカルまたはリモート認証を使用したログオンアクセス、Web サーバ、Telnet サーバとともに、Secure Shell による管理アクセス、ポートセキュリティ、および指定された IP アドレスに基づく制限付きアクセスを構成します。
セキュリティの設定	共通のデータポートに接続されたクライアントのトラフィックを分離します。有効な静的または動的アドレスの設定、MAC アドレス認証、DHCP 要求と応答のフィルタリング、および無効な ARP 応答の破棄による、不正なアクセスを防止します。
アクセス制御リスト	IPv4 フレーム(アドレス、プロトコル、TCP / UDP ポート番号または TCP 制御コードに基づく)、IPv6 フレーム(アドレス、DSCP トラフィッククラス、または次のヘッダーに基づく)、または非 IP フレーム(MAC アドレスまたは イーサネットタイプ)を提供します。
インタフェースコマンド	すべてのイーサネットポート、集約リンク、および VLAN の接続パラメータを設定します。
リンクアグリゲーションコマンド	ポートトランクの Link Aggregation Control Protocol を設定して、複数のポートを 1 つの論理トランクに静的にグループ化します。
PoE コマンド	接続されたデバイスの電源出力を設定します。
ポートミラーリングコマンド	監視対象のポートの通過やパフォーマンスに影響を与えることなく、別のポートにデータをミラーリングして分析します。
輻輳制御コマンド	設定されたレート制限のトリガーまたはポートのシャットダウンに使用できるブロードキャスト、およびマルチキャストストームの入出力レート制限、トラフィックストーム閾値、およびスレッシュホールドを設定します。
ループ検知コマンド	ハードウェアの問題またはプロトコル設定の障害によって引き起こされる 一般的なループバック状態を検出します。
MAC アドレステーブルコマンド	指定されたアドレスをフィルタリングするためのアドレステーブルを設定や、現在のエントリの表示、テーブルのクリア、またはエージングタイムの設定をします。
スパニングツリーコマンド	スイッチのスパニングツリーを設定します。
VLAN コマンド	VLAN を設定し、VLAN グループのポートメンバーシップを定義します。また、プライベート VLAN、プロトコル VLAN、

コマンドグループ	説明
	Voice VLAN、および QinQ トンネリングを有効化、または設定します。
CoS コマンド	タグなしフレームのポートプライオリティの設定、厳密なプライオリティ、または重み付きラウンドロビンの選択、各プライオリティキューの相対ウェイト、および DSCP のプライオリティの設定をおこないます。
QoS コマンド	QoS を構成します。
マルチキャストフィルタリングコマンド	IGMP マルチキャストフィルタリング、クエリー、プロファイル、およびプロキシのパラメータを設定します。マルチキャストルータに接続されているポートを指定します。また、マルチキャスト VLAN 登録と IPv6 MLD スヌーピングも設定します。
LLDP コマンド	隣接デバイスに関する情報検出を有効化するために、LLDP を設定します。
ドメインネームサービスコマンド	DNS サービスを設定します。
DHCP コマンド	DHCP クライアントとリレー機能を設定します。
IP インタフェースコマンド	スイッチインタフェースの IP アドレスを設定します。また ARP パラメータも設定します。
IP ルーティングコマンド	静的および動的ユニキャストルーティングを設定します。

表に示されるアクセスモードの省略形については、以下の通りです:

ACL (Access Control List Configuration)

CM (Class Map Configuration)

GC (Global Configuration)

IC (Interface Configuration)

IPC (IGMP Profile Configuration)

LC (Line Configuration)

MST (Multiple Spanning Tree)

NE (Normal Exec)

PE (Privileged Exec)

PM (Policy Map Configuration)

VC (VLAN Database Configuration)

3 一般コマンド

一般コマンドは、コマンドアクセスモード、設定モードおよびその他の基本機能を制御するために使用されます。

表 3-1 一般コマンド

コマンド	機能	モード
prompt	CLI プロンプトをカスタマイズします。	GC
reload	指定した時刻、指定した遅延の後、または定期的にシステムを再起動します。	GC
enable	Privileged Exec モードをアクティブにします。	NE
quit	CLI セッションを終了します。	NE, PE
show history	コマンド履歴バッファを示します。	NE, PE
configure	グローバル設定モードをアクティブにします。	PE
disable	Privileged Exec モードから通常アクセスモードに戻します。	PE
reload	システムを直ちに戻します。	PE
show reload	現在のリロード設定と、次にスケジュールされたリロードが行われる時刻を表示します。	PE
end	“Privileged Exec”モードに戻ります。	全構成モード
exit	以前の設定モードに戻るか、または CLI を終了します。	以前の設定モードに戻るか、または CLI を終了します。
help	ヘルプの使用方法について示します。	以前の設定モードに戻るか、または CLI を終了します。
?	コマンド完了のオプションを表示します(コンテキスト依存)。	以前の設定モードに戻るか、または CLI を終了します。

3.1.1 prompt

このコマンドは、CLI プロンプトをカスタマイズします。デフォルトのプロンプトを復元するには、no 形式を使用してください。

構文

prompt *string*

no prompt

string - CLI プロンプトに使用するための英数字の文字列。(最長 32 文字)

デフォルト設定

Console

コマンドモード

Global Configuration

コマンドの使用方法

このコマンドは、下記の例で示すようにコマンドラインプロンプトを設定するために、使用することができます。コマンドの no 形式を使用すると、デフォルトのコマンドラインプロンプトが復元されます。

例

```
Console(config)#prompt RD2
RD2(config)#
```

3.1.2 reload (Global Configuration)

このコマンドは、指定された時間、指定された遅延の後、または定期的な間隔でシステムを再起動します。システムを直ちに再起動することも、指定した時間後にリセットするようにスイッチを設定することもできます。設定を削除するには、キャンセルオプションを使用します。

構文

reload {at *hour minute* [{*month day* | *day month*} [*year*]] |

in {hour *hours* | minute *minutes* | hour *hours* minute *minutes*} |

regulary *hour minute* [period {daily | weekly *day-of-week* |

monthly *day-of-month*}] | cancel [at | in | regulary]}

reload at - スイッチをリロードする指定時間。

hour - リロードする時間(範囲: 0 から 23)

minute - リロードする分(範囲: 0 から 59)

month - リロードする月(1 月から 12 月)

day - リロードする日付(範囲: 1 から 31)

year - リロードする年(範囲: 1970 から 2037)

reload in - スイッチをリロードする間隔

hours - スイッチがリセットされる前の時間(分)(範囲: 0 から 576)

minutes - スイッチがリセットされるまでの時間(分)(範囲: 0 から 59)

reload regulary - スイッチをリロードする定期的な間隔

hour - リロードする時間(範囲: 0 から 23)

minute - リロードする分(範囲: 0 から 59)

day-of-week - リロードする曜日

(範囲: 月曜から土曜日)

day-of-month -リロードする日付(範囲: 1 から 31)

reload cancel - 指定したリロードオプションをキャンセルします。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- このコマンドは、システム全体をリセットします。
- リロードオプションの任意の組み合わせを指定することができます。同じオプションを再指定すると、前の設定が上書きされます。
- システムを再起動すると、常にパワーオンセルフテストが実行されます。また、copy running-config startup-config コマンドによって、不揮発性メモリに保存されているすべての設定情報も保持されます。

例

この例では、30 秒後にリセットする方法について示しています:

```
Console(config)#reload in minute 30
***
*** --- Rebooting at January  1 02:10:43 20XX ---
***

Are you sure to reboot the system at the specified time? <y/n>
```

3.1.3 enable

このコマンドでは、Privileged Exec モードをアクティブにします。Privileged Exec モードでは、追加コマンドを使用することが出来るようになり、特定コマンドの追加情報が表示されます。「2.2.8　コマンドモードについて」を参照してください。

構文

enable [*level*]

level - デバイスにログインするために特権レベルです。

このデバイスには、2 つの事前定義された特権レベルがあります（0: Normal Exec, 15: Privileged ）。Exec.Privileged Exec モードにアクセスするには、レベル 15 を入力してください。

デフォルト設定

Level 15

コマンドモード

Normal Exec

コマンドの使用方法

- ◆ コマンドモードを Normal Exec から Privileged Exec に変更するためにはパスワードが必要です。(パスワードについては enable password コマンドを参照してください。)
- ◆ プロンプトの末尾に “#”文字が追加され、システムが特権アクセスモードになっていることを示します。

例

```
Console>enable
Password: [privileged level password]
Console#
```

関連コマンド

disable

enable password

3.1.4 quit

本コマンドは設定プログラムを終了します。

デフォルト設定

無し

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

quit および exit コマンドは、設定プログラムを終了することができます。

例

以下の例では、CLI セッションの終了方法について示しています。

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

3.1.5 show history

本コマンドでは、コマンド履歴バッファの内容を示しています。

デフォルト設定

無し

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

履歴バッファサイズは、10 の Execution コマンドと 10 の Configuration コマンドに固定されています。

例

この例では、”show history”コマンド、コマンド履歴バッファの内容を一覧表示します。

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

!コマンドは、Normal Exec または Privileged Exec モードのときに、Execution コマンド履歴バッファからのコマンドを繰り返します。任意の設定モードに入っているときに、Configuration コマンド履歴バッファから命令します。この例では、!2 コマンドが、実行履歴バッファ(config)内の 2 番目のコマンドを繰り返します。

```
Console#!2
Console#config
Console(config)#
```

3.1.6 configure

本コマンドは、Global Configuration モードをアクティブにします。スイッチ上の設定を変更するために、このモードに入る必要があります。インタフェース設定、回線設定、および VLAN データベース設定など）が含まれます。「2.2.8　コマンドモードについて」を参照してください。

デフォルト設定

無し

コマンドモード

Privileged Exec

例

```
Console#configure
Console(config)#
```

関連コマンド

end

3.1.7 disable

このコマンドは、Privileged Exec モードから通常アクセスモード（Normal Exec モード）に戻ります。通常アクセスモードでは、スイッチの設定またはイーサネット統計情報に関する基本情報のみを表示できます。すべてのコマンドにアクセスするには、Privileged Exec モードを使用する必要があります。「2.2.8　コマンドモードについて」を参照してください。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

プロンプトの末尾に ”>” 文字が追加され、システムが通常アクセスモードになっていることを示します。

例

```
Console#disable
Console>
```

関連コマンド

enable

3.1.8 reload (Privileged Exec)

本コマンドは、システムを再起動します。

Note: システムを再起動すると、常にパワーオンセルフテストが実行されます。また、copy running-config startup-config コマンドによって、不揮発性メモリに保存されている設定情報は再起動後も保持されます。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

このコマンドは、システム全体をリセットします。

例

以下の例では、スイッチのリセット方法について示しています。

```
Console#reload
System will be restarted, continue <y/n>? y
```

3.1.9 show reload

本コマンドでは、現在のリロード設定と、次にスケジュールされたリロードが行われる時刻を表示します。現在のリロード設定と、次にスケジュールされたリロードが行われる時刻を表示します。

コマンドモード

Privileged Exec

例

```
Console#show reload
Reloading switch in time:                 0 hours 29 minutes.

The switch will be rebooted at January  1 02:11:50 20XX.
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

3.1.10 end

本コマンドで、Privileged Exec モードに戻ります。

デフォルト設定

無し

コマンドモード

Global Configuration、Interface Configuration、Line Configuration、VLAN Database Configuration および Multiple Spanning Tree Configuration。

例

以下の例では、Interface Configuration モードから、Privileged Exec モードへ戻る方法について示しています。

```
Console(config-if)#end
Console#
```

3.1.11 exit

本コマンドにより、以前の設定モードに戻るか、または設定プログラムを終了します。

デフォルト設定

無し

コマンドモード

任意

例

以下の例では、Global Configuration モードから Privileged Exec モードへ戻り、その次に CLI セッションを終了する方法を示しています。

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

4 システム管理コマンド

本システム管理コマンドは、システムログ、パスワード、ユーザ名、管理オプションを制御し、その他のあらゆるシステムを表示または設定するために、使用することができます。

表 4-1　システム管理コマンド

コマンドグループ	機能
デバイスの指定	このスイッチを一意に識別する情報を設定します。
システムステータス	システム設定、アクティブマネージャおよびバージョン情報を表示します。
フレームサイズ	ジャンボフレームのサポートを有効にします。
ファイル管理	コードイメージまたはスイッチ設定ファイルを管理します。
Line	ボーレートとコンソールタイムアウトを含むシリアルポートの通信パラメータを設定します。
イベントロギング	エラーメッセージのロギングを制御します。
SMTP アラート	SMTP 電子メール警告を設定します。
時刻設定	NTP/SNTP サーバを通じて自動的に、または手動でシステムクロックを設定します。
時間範囲設定	PoE で使用する時間範囲を設定します。

4.1 デバイスの指定

この章では、スイッチを一意に識別する情報を設定するために使用されるコマンドについて説明します。

表 4-2　デバイス指定コマンド

コマンド	機能	モード
hostname	スイッチのホスト名を指定します。	GC

4.1.1 hostname

本コマンドは、デバイスのホスト名を指定または変更します。デフォルトホスト名を復元するには、no 形式を使用してください。

構文

hostname *name*

no hostname

name - このホスト名です。(最長: 32 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

◆　このコマンドで指定されたホスト名は、show system コマンドで表示されます。

例

```
Console(config)#hostname RD#1
Console(config)#
```

4.2 システムステータス

本章では、システム情報を表示するためのコマンドについて、説明します。

表 4-3 システムステータスコマンド

コマンド	機能	モード
show access-list tcam-utilization	TCAM の使用率パラメータを示します。	PE
show memory	メモリ使用率パラメータを示します。	PE
show process cpu	CPU 使用率パラメータを示します。	PE
show process cpu guard	CPU 使用率基準値および閾値を示します。	NE
show process cpu task	処理ごとの CPU 使用率を示します。	PE
show running-config	現在使用中の設定データを示します。	PE
show startup-config	システムを起動させるために使用される、設定ファイル(フラッシュメモリに格納)の内容を示します。	PE
show system	システム情報を示します。	NE, PE
show tech-support	テクニカルサポートで、設定や機能の問題を解決するためのシステム設定の詳細な一覧を表示します。	PE
show users	ユーザ名、アイドル時間、Telnet クライアントの IP アドレスなど、すべてのアクティブなコンソールセッションと Telnet セッションを表示します。	NE, PE
show version	システムのバージョン情報を示します。	NE, PE
show watchdog	ウォッチドッグデバッグが、有効になっているかどうかについて、示します。	PE
watchdog software	キープロセスを監視し、これらのプロセスのいずれかが正しく応答しない場合、システムを自動的に再起動します。	PE

4.2.1 show access-list tcam-utilization

本コマンドは、使用中のポリシー制御エントリ数、空きエントリ数を含む、TCAM(Ternary Content Addressable Memory)の使用状況を表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

アクセス制御リスト(ACL)、IP ソースガードフィルタルール、QoS(Quality of Service)プロセス、トラップなど、ルールベースの検索に依存する、さまざまなシステム機能によって、ポリシー制御エントリ(PCE)が使用されます。

たとえば、ACL をポートにバインドする場合、ACL の各ルールは 2 つの PCE を使用します。 また、ポートに IP ソースガードフィルタルールを設定すると、システムは 2 つの PCE も使用します。

例

```
Console#show access-list tcam-utilization
Pool capability code:
```

```
  AM - MAC ACL, A4 - IPv4 ACL, A6S - IPv6 Standard ACL,
  A6E - IPv6 extended ACL, DM - MAC diffServ, D4 - IPv4 diffServ,
  D6S - IPv6 standard diffServ, D6E - IPv6 extended diffServ,
  W - Web authentication,
  I - IP source guard, C - CPU interface, L - Link local,
  MV - Mac based VLAN, PV - Protocol based VLAN, VV - Voice VLAN,
  R - Routing, QINQ - QinQ, Reserved - Reserved,
  ALL - All supported function,

Unit Device Pool Total Used  Free  Capability
---- ------ ---- ----- ----- ----- ---------------------------------------
   1      0    0   128   128     0 R
   1      0    1    64     0    64 A6S A6E
   1      0    2   128     0   128 A4
   1      0    3   128     0   128 AM
   1      0    4    64     0    64 D6S D6E
   1      0    5   128     0   128 D4 W
   1      0    6   128     0   128 DM
   1      0    7   128     0   128 MV PV VV
   1      0    8    64     0    64 I
   1      0    9    64    64     0 Reserved
   1      0   10    64    64     0 C
   1      0   11    64    64     0 C L

Console#
```

表 4-4 show access-list tcam-utilization - 表示の説明

フィールド	説明
Pool Capability Code	TCAM リストに示されているプロセスの略語です。
Unit	スタックユニットの識別子です。
Device	指定されたプールに使用される、メモリチップです。
Pool	ルールスライス(またはコールグループ)。各スライスごとに使用される機能が決まっています。
Total	各プールに割り当てられた、最大ポリシー制御入力数です。
Used	オペレーティングシステムで使用されている、ポリシー制御エントリです。
Free	未使用のポリシー制御エントリです。
Capability	各プールに割り当てられている処理です。

4.2.2 show memory

本コマンドでは、メモリ使用状況および警告閾値について、示します。

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

本コマンドでは、現在使用可能なメモリの量、アクティブなプロセスに割り当てられているメモリの量、システムメモリの合計量、およびアラームの閾値を示します。

例

```
Console#show memory
 Status Bytes      %
 ------ ---------- ---
 Free    111706112  41
 Used    156729344  59
 Total   268435456

 Alarm Configuration
  Rising Threshold         : 95%
  Falling Threshold        : 90%

Console#
```

関連コマンド

memory

4.2.3 show process cpu

本コマンドでは、CPU 使用状況、警告ステータスおよび警告閾値について、示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show process cpu
 CPU Utilization in the past 5 seconds : 24%

 CPU Utilization in the past 60 seconds
  Average Utilization      : 24%
  Maximum Utilization      : 25%

 Alarm Status
  Current Alarm Status     : Off
  Last Alarm Start Time    : Dec 31 00:00:19 20XX
  Last Alarm Duration Time : 15 seconds

 Alarm Configuration
  Rising Threshold         : 90%
```

```
  Falling Threshold         : 70%

Console#
```

関連コマンド

process cpu

4.2.4 show process cpu guard

本コマンドでは、CPU 使用率基準値および閾値の設定について示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show process cpu guard
 CPU Guard Configuration
  Status             : Disabled
  High Watermark     : 90%
  Low Watermark      : 70%
  Maximum Threshold : 500 packets per second
  Minimum Threshold : 50 packets per second
  Trap Status        : Disabled
 CPU Guard Operation
  Current Threshold : 500 packets per second

Console#
```

表 4-5 show process cpu guard - 表示の説明

フィールド	説明
CPU Guard Configuration	
Status :	CPU ガードが有効になっているかどうかについて、示します。
High Watermark	CPU 使用率のパーセンテージが最高水準点よりも高い場合、使用時間が最低水準点を下回るまで、(バッファに既に入っているパケットを CPU で処理できるように)スイッチは CPU へのパケット受信を停止します。
Low Watermark	高水準点を超えた後に CPU へのパケット受信が停止した場合、使用量が低水準点を下回った後に、CPU へのパケット受信停止を解除します。
Maximum Threshold	CPU によって処理されているパケットの数が最大閾値よりも高い場合、スイッチは処理中のパケットの数が最小閾値を下回るまで、CPU へのパケット受信を停止します。
Minimum Threshold	高水準点を超えた後に CPU へのパケット受信が停止した場合、使用量が最低閾値を下回った後に、CPU へのパケット受信停止を解除します。
Trap Status	使用率が最高水準点を超えているか、あるいは、最大閾値を超えた場合に、警告メッセージが生成されるかどうかを示します。

フィールド	説明
CPU Guard Operation	
Current Threshold	設定された閾値を、パケット/秒で表示します。

関連コマンド

process cpu guard

4.2.5 show process cpu task

本コマンドでは、プロセスごとの CPU 使用率について示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show process cpu guard
Task            Util (%) Avg (%)  Max (%)
--------------- -------- -------- --------
AMTR_ADDRESS        0.00     0.00     0.00
AMTRL3              0.00     0.00     0.00
AMTRL3_GROUP        0.00     0.00     0.00
APP_PROTOCOL_PR     0.00     0.00     0.00
AUTH_GROUP          0.00     0.00     0.00
AUTH_PROC           0.00     0.00     0.00
BGP_TD              0.00     0.00     0.00
CFGDB_TD            0.00     0.00     0.00
CFM_GROUP           0.00     0.00     0.00
CLITASK0            0.00     0.00     0.00
CORE_UTIL_PROC      0.00     0.00     0.00
DHCPSNP_GROUP       0.00     0.00     0.00
DOT1X_SUP_GROUP     0.00     0.00     0.00
DRIVER_GROUP        1.00     0.75     2.00
DRIVER_GROUP_FR     0.00     0.00     0.00
DRIVER_GROUP_TX     0.00     0.00     0.00
FS                  0.00     0.00     0.00
HTTP_TD             0.00     0.00     5.00
HW_WTDOG_TD         0.00     0.00     0.00
IML_TX              0.00     0.00     0.00
IP_SERVICE_GROU     0.00     0.00     0.00
KEYGEN_TD           0.00     0.00     0.00
L2_L4_PROCESS       0.00     0.00     4.00
L2MCAST_GROUP       0.00     0.00     0.00
L2MUX_GROUP         0.00     0.00     0.00
L4_GROUP            0.00     0.00     0.00
LACP_GROUP          0.00     0.00     0.00
MSL_TD              0.00     0.00     0.00
```

```
NETACCESS_GROUP      0.00      0.00      0.00
NETACCESS_NMTR       0.00      0.25      2.00
NETCFG_GROUP         0.00      0.00      0.00
NETCFG_PROC          0.00      0.08      1.00
NIC                  0.00      0.00      0.00
NMTRDRV              1.00      1.66      4.00
NSM_GROUP            0.00      0.00      0.00
NSM_PROC             0.00      0.00      0.00
NSM_TD               0.00      0.00      0.00
OSPF6_TD             0.00      0.00      0.00
OSPF_TD              0.00      0.00      0.00
PIM_GROUP            0.00      0.00      0.00
PIM_PROC             0.00      0.00      0.00
PIM_SM_TD            0.00      0.00      0.00
POE_PROC             0.00      0.00      0.00
RIP_TD               0.00      0.00      0.00
SNMP_GROUP           0.00      0.00      0.00
SNMP_TD              0.00      0.00      0.00
SSH_GROUP            0.00      0.00      0.00
SSH_TD               0.00      0.00      0.00
STA_GROUP            0.00      0.00      0.00
STKCTRL_GROUP        0.00      0.00      0.00
STKTPLG_GROUP        0.00      0.00      0.00
SWCTRL_GROUP         0.00      0.00      0.00
SWCTRL_TD            0.00      0.00      0.00
SWDRV_MONITOR       21.00     19.25     21.00
SYS_MGMT_PROC        0.00      0.00      0.00
SYSDRV               0.00      0.00      0.00
SYSLOG_TD            0.00      0.00      0.00
SYSMGMT_GROUP        0.00      0.00      0.00
SYSTEM               0.00      0.00      0.00
UDLD_GROUP           0.00      0.00      0.00
WTDOG_PROC           0.00      0.00      0.00
XFER_GROUP           0.00      0.00      0.00
XFER_TD              0.00      0.00      0.00

Console#
```

4.2.6 show running-config

本コマンドでは、現在使用している設定情報について示します。

構文

show running-config [interface *interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan *vlan-id* (範囲: 1-4094)

コマンドモード

Privileged Exec

コマンドの使用方法

- interface キーワードを使用して、指定したインタフェースの設定データを表示します。
- このコマンドを show startup-config コマンドと組み合わせて使用すると、実行中のメモリの情報と不揮発性メモリに格納されている情報を比較することができます。
- このコマンドでは、キーコマンドモードの設定を表示します。各モードグループは、"！”記号で区切られ、設定モードコマンドとそれに対応するコマンドが含まれています。このコマンドでは、以下の情報を表示します。
  - MAC アドレス
  - SNMP コミュニティ文字列
  - ユーザ(名、アクセスレベルおよび暗号化パスワード)
  - VLAN データベース(VLAN ID、名称および状態)
  - 各インタフェースの VLAN 設定内容
  - マルチプルスパニングツリーのインスタンス(名称およびインタフェース)
  - LAN 用に設定された IP アドレス
  - スパニングツリー設定
  - インタフェース設定
  - コンソールポートおよび Telnet 用に設定された内容
- セキュリティの理由により、ユーザパスワードは暗号化形式でのみ、表示されます。

例

```
Console#show running-config
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-12-e2-00-00-fd_03</stackingMac>
!
snmp-server community public ro
snmp-server community private rw
!
enable password 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 VLAN 1 name DefaultVlan media ethernet
!
spanning-tree mst configuration
!
interface ethernet 1/1
 no negotiation
```

```
...
interface ethernet 1/10
 no negotiation
!
interface vlan 1
 ip address dhcp
!
interface vlan 1
!
line console
!
line vty
!
end
!
Console#
```

関連コマンド

show startup-config

4.2.7 show startup-config

本コマンドでは、システムを起動するために使用される不揮発性メモリに格納された、設定ファイルを表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

- このコマンドを show running-config コマンドと組み合わせて使用すると、実行中のメモリの情報と不揮発性メモリに格納されている情報を比較することができます。
- このコマンドでは、キーコマンドモードの設定を表示します。各モードグループは、"！”記号で区切られ、設定モードコマンドとそれに対応するコマンドが含まれています。このコマンドでは、以下の情報を表示します。
  - MAC アドレス
  - SNMP コミュニティ文字列
  - SNMP トラップ認証
  - ユーザ(名、アクセスレベルおよび暗号化パスワード)
  - VLAN データベース(VLAN ID、名称および状態)
  - 複数のスパニングツリーインスタンス(名称およびインタフェース)
  - 各インタフェースのインタフェース設定および VLAN 設定内容
  - VLAN 用の IP アドレス
  - コンソールポートおよび Telnet 用に設定された内容

例

ランニングコンフィグレーションファイルの例を参照してください。

関連コマンド

show running-config

4.2.8 show system

本コマンドでは、システム情報を示します。

デフォルト設定

無し

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show system
System Description : AXprimoM210-08T
System OID String  : 1.3.6.1.4.1.21839.2.2.26.101
System Information
 System Up Time         : 0 days, 0 hours, 4 minutes, and 38.91 seconds
 System Name            :
 System Location        :
 System Contact         :
 MAC Address (Unit 1)   : 00-12-E2-03-01-D0
 Web Server             : Enabled
 Web Server Port        : 80
 Web Secure Server      : Enabled
 Web Secure Server Port : 443
 Telnet Server          : Enabled
 Telnet Server Port     : 23
 Jumbo Frame            : Disabled
Unit 1

 Main Power Status      : Up
```

表 4-6　show system -表示の説明

パラメータ	説明
System Description	モデル名です。
System OID String	スイッチのネットワーク管理サブシステムの MIB II オブジェクト ID です。
System Up Time	管理エージェントがアップされた時間の長さです。
System Name	スイッチシステムに割り当てられた名称です。

パラメータ	説明
System Location	システムの位置を指定します。
System Contact	システム担当の管理者です。
MAC Address	スイッチに割り当てられた MAC アドレスです。
Web Server/Port	ウェブサーバと UDP ポート番号の管理ステータスを示します。
Web Secure Server/Port	安全なウェブサーバと UDP ポート番号の管理ステータスを示します。
Telnet Server/Port	Telnet サーバと TCP ポート番号の管理ステータスを示します。
Jumbo Frame	ジャンボフレームが有効になっているか、無効になっているかについて示します。
Main Power Status	内部電力供給の状態について、示します。

4.2.9 show tech-support

本コマンドでは、テクニカルサポートが設定または機能上の問題を解決するのに役立つように設計された、システム設定の詳細なリストを表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドは、詳細なシステムおよびインタフェース設定を含む情報のリストを生成します。したがって、端末エミュレーションプログラムで提供されている適切な出力キャプチャ機能を使用して、出力をファイルに転送することを推奨します。

例

```
Console#show tech-support

dir:
File Name                       Type    Startup Modified Time       Size (bytes)
------------------------------ ------- ------- ------------------- ------------
 Unit 1:
op1.bix                         OpCode  Y       20XX-07-25 02:39:49    9,130,248
Factory_Default_Config.cfg      Config  N       20XX-07-25 02:37:46          477
startup1.cfg                    Config  Y       20XX-08-07 13:30:09        1,527
------------------------------------------------------------------------------
                      Free space for compressed user config files: 22,372,352
                                                     Total space: 33,554,432

show arp:

IP Address      MAC Address       Type      Interface
--------------- ----------------- --------- -----------
192.168.13.230  00-12-E2-00-30-16 dynamic   VLAN13
192.168.13.239  00-12-E2-03-01-D0 other     VLAN13

Total entry : 2
```

```
show interfaces brief:
Interface Name              Status    PVID Pri Speed/Duplex  Type         Trunk
--------- ----------------- --------- ---- --- ------------ ------------ -----
Eth 1/ 1                    Up           1   0 Auto-1000full 1000BASE-T   None
Eth 1/ 2                    Up           1   0 Auto-1000full 1000BASE-T   None
Eth 1/ 3                    Up           1   0 Auto-1000full 1000BASE-T   None
Eth 1/ 4                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 5                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 6                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 7                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 8                    Down         1   0 Auto          1000BASE-T   1
Eth 1/ 9                    Down         1   0 Auto          1000BASE SFP None
Eth 1/10                    Down         1   0 Auto          1000BASE SFP None
Trunk  1                    Down         1   0 Auto          1000BASE-T   1

show interfaces counters:
Ethernet 1/ 1
 ===== IF table Stats =====
                     433 Octets Input
                   35077 Octets Output
                       1 Unicast Input
                      77 Unicast Output
                       0 Discard Output
                       0 Error Input
 ===== Extended Iftable Stats =====
                       3 Multi-cast Input
                     205 Multi-cast Output
                       0 Broadcast Input
                      11 Broadcast Output
 ===== Ether-like Stats =====
                       0 FCS Errors
                       0 Single Collision Frames
                       0 Multiple Collision Frames
                       0 Deferred Transmissions
                       0 Late Collisions
                       0 Excessive Collisions
                       0 Internal Mac Transmit Errors
                       0 Frames Too Long
                       0 Symbol Errors
                       0 Pause Frames Input
                       0 Pause Frames Output
 ===== RMON Stats =====
                       0 Drop Events
                   35510 Octets
                     101 Packets
                      11 Broadcast PKTS
                     208 Multi-cast PKTS
                       0 Undersize PKTS
```

```
                        0 Oversize PKTS
                        0 Fragments
                        0 Jabbers
                        0 CRC Align Errors
                        0 Collisions
                       78 Packet Size <= 64 Octets
                      196 Packet Size 65 to 127 Octets
                       12 Packet Size 128 to 255 Octets
                       11 Packet Size 256 to 511 Octets
                        0 Packet Size 512 to 1023 Octets
                        0 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                        0 Octets Input in kbits per second
                        0 Packets Input per second
                     0.00 % Input Utilization
                        0 Octets Output in kbits per second
                        0 Packets Output per second
                     0.00 % Output Utilization
Ethernet 1/ 2
 ===== IF table Stats =====
                    11946 Octets Input
                    29977 Octets Output
                       78 Unicast Input
                       39 Unicast Output
                        0 Discard Output
                        0 Error Input
 ===== Extended Iftable Stats =====
                       15 Multi-cast Input
                      203 Multi-cast Output
                       29 Broadcast Input
                        4 Broadcast Output
 ===== Ether-like Stats =====
                        0 FCS Errors
                        0 Single Collision Frames
                        0 Multiple Collision Frames
                        0 Deferred Transmissions
                        0 Late Collisions
                        0 Excessive Collisions
                        0 Internal Mac Transmit Errors
                        0 Frames Too Long
                        0 Symbol Errors
                        0 Pause Frames Input
                        0 Pause Frames Output
 ===== RMON Stats =====
                        0 Drop Events
                    41923 Octets
                      175 Packets
                       33 Broadcast PKTS
                      218 Multi-cast PKTS
```

```
                      78 Undersize PKTS
                       0 Oversize PKTS
                       0 Fragments
                       0 Jabbers
                       0 CRC Align Errors
                       0 Collisions
                      62 Packet Size <= 64 Octets
                     193 Packet Size 65 to 127 Octets
                      25 Packet Size 128 to 255 Octets
                      10 Packet Size 256 to 511 Octets
                       0 Packet Size 512 to 1023 Octets
                       0 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                       0 Octets Input in kbits per second
                       0 Packets Input per second
                    0.00 % Input Utilization
                       0 Octets Output in kbits per second
                       0 Packets Output per second
                    0.00 % Output Utilization
Ethernet 1/ 3
 ===== IF table Stats =====
                  156364 Octets Input
                 1294531 Octets Output
                    1371 Unicast Input
                    1373 Unicast Output
                       0 Discard Output
                       0 Error Input
 ===== Extended Iftable Stats =====
                     293 Multi-cast Input
                      29 Multi-cast Output
                      29 Broadcast Input
                      13 Broadcast Output
 ===== Ether-like Stats =====
                       0 FCS Errors
                       0 Single Collision Frames
                       0 Multiple Collision Frames
                       0 Deferred Transmissions
                       0 Late Collisions
                       0 Excessive Collisions
                       0 Internal Mac Transmit Errors
                       0 Frames Too Long
                       0 Symbol Errors
                       0 Pause Frames Input
                       0 Pause Frames Output
 ===== RMON Stats =====
                       0 Drop Events
                 1450895 Octets
                    2650 Packets
                      42 Broadcast PKTS
```

```
                     322 Multi-cast PKTS
                     155 Undersize PKTS
                       0 Oversize PKTS
                       0 Fragments
                       0 Jabbers
                       0 CRC Align Errors
                       0 Collisions
                    1415 Packet Size <= 64 Octets
                     458 Packet Size 65 to 127 Octets
                      25 Packet Size 128 to 255 Octets
                      97 Packet Size 256 to 511 Octets
                      85 Packet Size 512 to 1023 Octets
                     873 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                       3 Octets Input in kbits per second
                       4 Packets Input per second
                    0.00 % Input Utilization
                      28 Octets Output in kbits per second
                       3 Packets Output per second
                    0.00 % Output Utilization
Ethernet 1/ 4
 ===== IF table Stats =====
                       0 Octets Input
                       0 Octets Output
                       0 Unicast Input
                       0 Unicast Output
                       0 Discard Output
                       0 Error Input
 ===== Extended Iftable Stats =====
                       0 Multi-cast Input
                       0 Multi-cast Output
                       0 Broadcast Input
                       0 Broadcast Output
 ===== Ether-like Stats =====
                       0 FCS Errors
                       0 Single Collision Frames
                       0 Multiple Collision Frames
                       0 Deferred Transmissions
                       0 Late Collisions
                       0 Excessive Collisions
                       0 Internal Mac Transmit Errors
                       0 Frames Too Long
                       0 Symbol Errors
                       0 Pause Frames Input
                       0 Pause Frames Output
 ===== RMON Stats =====
                       0 Drop Events
                       0 Octets
                       0 Packets
```

```
                        0 Broadcast PKTS
                        0 Multi-cast PKTS
                        0 Undersize PKTS
                        0 Oversize PKTS
                        0 Fragments
                        0 Jabbers
                        0 CRC Align Errors
                        0 Collisions
                        0 Packet Size <= 64 Octets
                        0 Packet Size 65 to 127 Octets
                        0 Packet Size 128 to 255 Octets
                        0 Packet Size 256 to 511 Octets
                        0 Packet Size 512 to 1023 Octets
                        0 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                        0 Octets Input in kbits per second
                        0 Packets Input per second
                     0.00 % Input Utilization
                        0 Octets Output in kbits per second
                        0 Packets Output per second
                     0.00 % Output Utilization
Ethernet 1/ 5
 ===== IF table Stats =====
                        0 Octets Input
                        0 Octets Output
                        0 Unicast Input
                        0 Unicast Output
                        0 Discard Output
                        0 Error Input
 ===== Extended Iftable Stats =====
                        0 Multi-cast Input
                        0 Multi-cast Output
                        0 Broadcast Input
                        0 Broadcast Output
 ===== Ether-like Stats =====
                        0 FCS Errors
                        0 Single Collision Frames
                        0 Multiple Collision Frames
                        0 Deferred Transmissions
                        0 Late Collisions
                        0 Excessive Collisions
                        0 Internal Mac Transmit Errors
                        0 Frames Too Long
                        0 Symbol Errors
                        0 Pause Frames Input
                        0 Pause Frames Output
 ===== RMON Stats =====
                        0 Drop Events
                        0 Octets
```

```
                        0 Packets
                        0 Broadcast PKTS
                        0 Multi-cast PKTS
                        0 Undersize PKTS
                        0 Oversize PKTS
                        0 Fragments
                        0 Jabbers
                        0 CRC Align Errors
                        0 Collisions
                        0 Packet Size <= 64 Octets
                        0 Packet Size 65 to 127 Octets
                        0 Packet Size 128 to 255 Octets
                        0 Packet Size 256 to 511 Octets
                        0 Packet Size 512 to 1023 Octets
                        0 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                        0 Octets Input in kbits per second
                        0 Packets Input per second
                     0.00 % Input Utilization
                        0 Octets Output in kbits per second
                        0 Packets Output per second
                     0.00 % Output Utilization
Ethernet 1/ 6
 ===== IF table Stats =====
                        0 Octets Input
                        0 Octets Output
                        0 Unicast Input
                        0 Unicast Output
                        0 Discard Output
                        0 Error Input
 ===== Extended Iftable Stats =====
                        0 Multi-cast Input
                        0 Multi-cast Output
                        0 Broadcast Input
                        0 Broadcast Output
 ===== Ether-like Stats =====
                        0 FCS Errors
                        0 Single Collision Frames
                        0 Multiple Collision Frames
                        0 Deferred Transmissions
                        0 Late Collisions
                        0 Excessive Collisions
                        0 Internal Mac Transmit Errors
                        0 Frames Too Long
                        0 Symbol Errors
                        0 Pause Frames Input
                        0 Pause Frames Output
 ===== RMON Stats =====
                        0 Drop Events
```

```
                        0 Octets
                        0 Packets
                        0 Broadcast PKTS
                        0 Multi-cast PKTS
                        0 Undersize PKTS
                        0 Oversize PKTS
                        0 Fragments
                        0 Jabbers
                        0 CRC Align Errors
                        0 Collisions
                        0 Packet Size <= 64 Octets
                        0 Packet Size 65 to 127 Octets
                        0 Packet Size 128 to 255 Octets
                        0 Packet Size 256 to 511 Octets
                        0 Packet Size 512 to 1023 Octets
                        0 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                        0 Octets Input in kbits per second
                        0 Packets Input per second
                     0.00 % Input Utilization
                        0 Octets Output in kbits per second
                        0 Packets Output per second
                     0.00 % Output Utilization
Ethernet 1/ 7
 ===== IF table Stats =====
                        0 Octets Input
                        0 Octets Output
                        0 Unicast Input
                        0 Unicast Output
                        0 Discard Output
                        0 Error Input
 ===== Extended Iftable Stats =====
                        0 Multi-cast Input
                        0 Multi-cast Output
                        0 Broadcast Input
                        0 Broadcast Output
 ===== Ether-like Stats =====
                        0 FCS Errors
                        0 Single Collision Frames
                        0 Multiple Collision Frames
                        0 Deferred Transmissions
                        0 Late Collisions
                        0 Excessive Collisions
                        0 Internal Mac Transmit Errors
                        0 Frames Too Long
                        0 Symbol Errors
                        0 Pause Frames Input
                        0 Pause Frames Output
 ===== RMON Stats =====
```

```
                        0 Drop Events
                        0 Octets
                        0 Packets
                        0 Broadcast PKTS
                        0 Multi-cast PKTS
                        0 Undersize PKTS
                        0 Oversize PKTS
                        0 Fragments
                        0 Jabbers
                        0 CRC Align Errors
                        0 Collisions
                        0 Packet Size <= 64 Octets
                        0 Packet Size 65 to 127 Octets
                        0 Packet Size 128 to 255 Octets
                        0 Packet Size 256 to 511 Octets
                        0 Packet Size 512 to 1023 Octets
                        0 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                        0 Octets Input in kbits per second
                        0 Packets Input per second
                     0.00 % Input Utilization
                        0 Octets Output in kbits per second
                        0 Packets Output per second
                     0.00 % Output Utilization
Ethernet 1/ 8
 ===== IF table Stats =====
                        0 Octets Input
                        0 Octets Output
                        0 Unicast Input
                        0 Unicast Output
                        0 Discard Output
                        0 Error Input
 ===== Extended Iftable Stats =====
                        0 Multi-cast Input
                        0 Multi-cast Output
                        0 Broadcast Input
                        0 Broadcast Output
 ===== Ether-like Stats =====
                        0 FCS Errors
                        0 Single Collision Frames
                        0 Multiple Collision Frames
                        0 Deferred Transmissions
                        0 Late Collisions
                        0 Excessive Collisions
                        0 Internal Mac Transmit Errors
                        0 Frames Too Long
                        0 Symbol Errors
                        0 Pause Frames Input
                        0 Pause Frames Output
```

```
 ===== RMON Stats =====
                        0 Drop Events
                        0 Octets
                        0 Packets
                        0 Broadcast PKTS
                        0 Multi-cast PKTS
                        0 Undersize PKTS
                        0 Oversize PKTS
                        0 Fragments
                        0 Jabbers
                        0 CRC Align Errors
                        0 Collisions
                        0 Packet Size <= 64 Octets
                        0 Packet Size 65 to 127 Octets
                        0 Packet Size 128 to 255 Octets
                        0 Packet Size 256 to 511 Octets
                        0 Packet Size 512 to 1023 Octets
                        0 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                        0 Octets Input in kbits per second
                        0 Packets Input per second
                     0.00 % Input Utilization
                        0 Octets Output in kbits per second
                        0 Packets Output per second
                     0.00 % Output Utilization
Ethernet 1/ 9
 ===== IF table Stats =====
                        0 Octets Input
                        0 Octets Output
                        0 Unicast Input
                        0 Unicast Output
                        0 Discard Output
                        0 Error Input
 ===== Extended Iftable Stats =====
                        0 Multi-cast Input
                        0 Multi-cast Output
                        0 Broadcast Input
                        0 Broadcast Output
 ===== Ether-like Stats =====
                        0 FCS Errors
                        0 Single Collision Frames
                        0 Multiple Collision Frames
                        0 Deferred Transmissions
                        0 Late Collisions
                        0 Excessive Collisions
                        0 Internal Mac Transmit Errors
                        0 Frames Too Long
                        0 Symbol Errors
                        0 Pause Frames Input
```

```
                        0 Pause Frames Output
  ===== RMON Stats =====
                        0 Drop Events
                        0 Octets
                        0 Packets
                        0 Broadcast PKTS
                        0 Multi-cast PKTS
                        0 Undersize PKTS
                        0 Oversize PKTS
                        0 Fragments
                        0 Jabbers
                        0 CRC Align Errors
                        0 Collisions
                        0 Packet Size <= 64 Octets
                        0 Packet Size 65 to 127 Octets
                        0 Packet Size 128 to 255 Octets
                        0 Packet Size 256 to 511 Octets
                        0 Packet Size 512 to 1023 Octets
                        0 Packet Size 1024 to 1518 Octets
  ===== Port Utilization (recent 300 seconds) =====
                        0 Octets Input in kbits per second
                        0 Packets Input per second
                     0.00 % Input Utilization
                        0 Octets Output in kbits per second
                        0 Packets Output per second
                     0.00 % Output Utilization
Ethernet 1/10
  ===== IF table Stats =====
                        0 Octets Input
                        0 Octets Output
                        0 Unicast Input
                        0 Unicast Output
                        0 Discard Output
                        0 Error Input
  ===== Extended Iftable Stats =====
                        0 Multi-cast Input
                        0 Multi-cast Output
                        0 Broadcast Input
                        0 Broadcast Output
  ===== Ether-like Stats =====
                        0 FCS Errors
                        0 Single Collision Frames
                        0 Multiple Collision Frames
                        0 Deferred Transmissions
                        0 Late Collisions
                        0 Excessive Collisions
                        0 Internal Mac Transmit Errors
                        0 Frames Too Long
                        0 Symbol Errors
```

```
                    0 Pause Frames Input
                    0 Pause Frames Output
 ===== RMON Stats =====
                    0 Drop Events
                    0 Octets
                    0 Packets
                    0 Broadcast PKTS
                    0 Multi-cast PKTS
                    0 Undersize PKTS
                    0 Oversize PKTS
                    0 Fragments
                    0 Jabbers
                    0 CRC Align Errors
                    0 Collisions
                    0 Packet Size <= 64 Octets
                    0 Packet Size 65 to 127 Octets
                    0 Packet Size 128 to 255 Octets
                    0 Packet Size 256 to 511 Octets
                    0 Packet Size 512 to 1023 Octets
                    0 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                    0 Octets Input in kbits per second
                    0 Packets Input per second
                 0.00 % Input Utilization
                    0 Octets Output in kbits per second
                    0 Packets Output per second
                 0.00 % Output Utilization
Trunk 1
 ===== IF table Stats =====
                    0 Octets Input
                    0 Octets Output
                    0 Unicast Input
                    0 Unicast Output
                    0 Discard Output
                    0 Error Input
 ===== Extended Iftable Stats =====
                    0 Multi-cast Input
                    0 Multi-cast Output
                    0 Broadcast Input
                    0 Broadcast Output
 ===== Ether-like Stats =====
                    0 FCS Errors
                    0 Single Collision Frames
                    0 Multiple Collision Frames
                    0 Deferred Transmissions
                    0 Late Collisions
                    0 Excessive Collisions
                    0 Internal Mac Transmit Errors
                    0 Frames Too Long
```

```
                    0 Symbol Errors
                    0 Pause Frames Input
                    0 Pause Frames Output
 ===== RMON Stats =====
                    0 Drop Events
                    0 Octets
                    0 Packets
                    0 Broadcast PKTS
                    0 Multi-cast PKTS
                    0 Undersize PKTS
                    0 Oversize PKTS
                    0 Fragments
                    0 Jabbers
                    0 CRC Align Errors
                    0 Collisions
                    0 Packet Size <= 64 Octets
                    0 Packet Size 65 to 127 Octets
                    0 Packet Size 128 to 255 Octets
                    0 Packet Size 256 to 511 Octets
                    0 Packet Size 512 to 1023 Octets
                    0 Packet Size 1024 to 1518 Octets
 ===== Port Utilization (recent 300 seconds) =====
                    0 Octets Input in kbits per second
                    0 Packets Input per second
                 0.00 % Input Utilization
                    0 Octets Output in kbits per second
                    0 Packets Output per second
                 0.00 % Output Utilization

show interfaces status:
Information of Eth 1/1
 Basic Information:
  Port Type              : 1000BASE-T
  MAC Address            : 00-12-E2-03-01-D1
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Disabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  MAC Learning           : Enabled
```

```
  Link-up-down Trap      : Enabled
  Media Type             : None
 Current Status:
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 1000full
  Up Time                : 0w 0d 0h 6m 25s (385 seconds)
  Flow Control Type      : None
  Max Frame Size         : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status    : Enabled

Information of Eth 1/2
 Basic Information:
  Port Type              : 1000BASE-T
  MAC Address            : 00-12-E2-03-01-D2
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Disabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  MAC Learning           : Enabled
  Link-up-down Trap      : Enabled
  Media Type             : None
 Current Status:
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 1000full
  Up Time                : 0w 0d 0h 6m 24s (384 seconds)
  Flow Control Type      : None
  Max Frame Size         : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status    : Enabled

Information of Eth 1/3
 Basic Information:
  Port Type              : 1000BASE-T
  MAC Address            : 00-12-E2-03-01-D3
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
```

```
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Disabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  MAC Learning           : Enabled
  Link-up-down Trap      : Enabled
  Media Type             : None
 Current Status:
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 1000full
  Up Time                : 0w 0d 0h 6m 25s (385 seconds)
  Flow Control Type      : None
  Max Frame Size         : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status    : Enabled

Information of Eth 1/4
 Basic Information:
  Port Type              : 1000BASE-T
  MAC Address            : 00-12-E2-03-01-D4
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Disabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  MAC Learning           : Enabled
  Link-up-down Trap      : Enabled
  Media Type             : None
 Current Status:
  Link Status            : Down
  Operation Speed-duplex : 1000full
  Flow Control Type      : None
  Max Frame Size         : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status    : Enabled
```

```
Information of Eth 1/5
 Basic Information:
  Port Type              : 1000BASE-T
  MAC Address            : 00-12-E2-03-01-D5
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Disabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  MAC Learning           : Enabled
  Link-up-down Trap      : Enabled
  Media Type             : None
 Current Status:
  Link Status            : Down
  Operation Speed-duplex : 1000full
  Flow Control Type      : None
  Max Frame Size         : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status    : Enabled

Information of Eth 1/6
 Basic Information:
  Port Type              : 1000BASE-T
  MAC Address            : 00-12-E2-03-01-D6
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Disabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  MAC Learning           : Enabled
  Link-up-down Trap      : Enabled
```

```
  Media Type              : None
 Current Status:
  Link Status             : Down
  Operation Speed-duplex  : 1000full
  Flow Control Type       : None
  Max Frame Size          : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status     : Enabled

Information of Eth 1/7
 Basic Information:
  Port Type               : 1000BASE-T
  MAC Address             : 00-12-E2-03-01-D7
 Configuration:
  Name                    :
  Port Admin              : Up
  Speed-duplex            : Auto
  Capabilities            : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm         : Disabled
  Broadcast Storm Limit   : 500 packets/second
  Multicast Storm         : Disabled
  Multicast Storm Limit   : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control            : Disabled
  LACP                    : Disabled
  MAC Learning            : Enabled
  Link-up-down Trap       : Enabled
  Media Type              : None
 Current Status:
  Link Status             : Down
  Operation Speed-duplex  : 1000full
  Flow Control Type       : None
  Max Frame Size          : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status     : Enabled

Information of Eth 1/8
 Basic Information:
  Member port of trunk 1 was created by user.
  Port Type               : 1000BASE-T
  MAC Address             : 00-12-E2-03-01-D8
 Configuration:
  Name                    :
  Port Admin              : Up
  Speed-duplex            : Auto
  Capabilities            : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm         : Disabled
  Broadcast Storm Limit   : 500 packets/second
  Multicast Storm         : Disabled
```

```
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  MAC Learning           : Enabled
  Link-up-down Trap      : Enabled
  Media Type             : None
 Current Status:
  Link Status            : Down
  Operation Speed-duplex : 1000full
  Flow Control Type      : None
  Max Frame Size         : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status    : Enabled

Information of Eth 1/9
 Basic Information:
  Port Type              : 1000BASE SFP
  MAC Address            : 00-12-E2-03-01-D9
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 1000full
  Broadcast Storm        : Disabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  MAC Learning           : Enabled
  Link-up-down Trap      : Enabled
  Media Type             : None
 Current Status:
  Link Status            : Down
  Operation Speed-duplex : 1000full
  Flow Control Type      : None
  Max Frame Size
```

4.2.10 show users

ユーザ名、アイドル時間、Telnet クライアントの IP アドレスなど、すべてのアクティブなコンソールセッションと Telnet セッションを表示します。

デフォルト設定

無し

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

コマンドを実行するために使用されたセッションは、ライン(例; セッション)インデックス番号の次に、”*” 記号で示されます。

例

```
Console#show users
User Name Accounts:
User Name            Privilege  Public-Key
-------------------- ---------- --------------
admin                       15 None
guest                        0 None

Online Users:
Line      Session ID User Name            Idle Time (h:m:s) Remote IP Addr
--------- ---------- -------------------- ----------------- -----------------
*Console           0 admin                          0:00:01

Web Online Users:
Line       User Name            Idle Time (h:m:s)    Remote IP Addr
---------- -------------------- -------------------- --------------------

Console#
```

4.2.11 show version

本コマンドでは、システムのハードウェアおよびソフトウェアバージョン情報が表示されます。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show version
Unit 1
 Serial Number          : PA0M21008T00J7S003
 Hardware Version       : R01
 Number of Ports        : 10
 Main Power Status      : Up
```

```
Role                    : Master
Loader Version          : 0.2.1.1
Linux Kernel Version    : 2.6.19
Operation Code Version : 1.2.2.17
```

表 4-7 show system -表示の説明

パラメータ	説明
Serial Number	スイッチのシリアル番号です。
Hardware Version	メインボードのハードウェアバージョンです。
Number of Ports	内蔵ポートの数です。
Main Power Status	内部電力供給の状態について、示します。
Role	マスターと表示します。
Loader Version	ローダーコードのバージョン番号です。
Linux Kernel Version	Linux カーネルのバージョン番号です。
Operation Code Version	ランタイムコードのバージョン番号です。

4.2.12 show watchdog

本コマンドでは、ウォッチドッグデバッグが有効になっているかどうかについて、示します。

コマンドモード

Privileged Exec

例

```
Console#show watchdog
Software Watchdog Information
 Status :    Enabled
 AutoReload :    Enabled
Console#
```

4.2.13 watchdog software

本コマンドでは、キープロセスを監視し、これらのプロセスのいずれかが正しく応答しない場合、システムを自動的に再起動します。

構文

watchdog software {disable | enable}

デフォルト設定

有効

コマンドモード

Privileged Exec

例

```
Console#watchdog software disable
Console#
```

4.3 フレームサイズ

本章では、スイッチのイーサネットフレームサイズを設定するために使用されるコマンドについて説明します。

表 4-8　フレームサイズコマンド

コマンド	機能	モード
jumbo frame	ジャンボフレームのサポートを有効にします。	GC

4.3.1 jumbo frame

本コマンドでは、ギガビットおよび 10 ギガビットのレイヤ 2 ジャンボフレームのサポートを、有効にします。無効にするには、no 形式を使用します。

構文

[no] jumbo frame

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- このスイッチは、ギガビットおよび 10 ギガビットイーサネットポート上のレイヤ 2 ジャンボフレーム、または 10240 バイトまでのトランクをサポートすることにより、大規模な順次データ転送に対してより効率的なスループットを提供します。ジャンボフレームを使用すると、1.5KB までしか実行されない標準イーサネットフレームと比較すると、プロトコルカプセル化フィールドを処理するために必要なパケットごとのオーバーヘッドが大幅に削減されます
- ジャンボフレームを使用するには、送信元と宛先の両方のエンドノード(コンピュータやサーバーなど)がこの機能をサポートしている必要があります。また、接続が全二重で動作している場合、2 つのエンドノード間のネットワーク内のすべてのスイッチは、拡張フレームサイズを受け入れる必要があります。また、半二重接続の場合、衝突ドメイン内のすべてのデバイスが、ジャンボフレームをサポートしていなければなりません。
- ジャンボフレームの現在の設定を、show system コマンドで表示することができます。

例

```
Console(config)#jumbo frame
Console(config)#
```

関連コマンド

show system

show ipv6 mtu

4.4 ファイル管理

4.4.1 ソフトウェアの管理

ソフトウェアを FTP/ TFTP でアップロードしたり、ダウンロードすることができます。FTP/ TFTP サーバにファイル、ランタイムコードを保存することにより、操作を復元するためのファイルを、スイッチへダウンロードすることができます。また、以前のバージョンを上書きすることなく、新しいソフトウェアを使用するようにスイッチを設定することもできます。

ランタイムコードをダウンロードするとき、現在のランタイムコードファイルとは異なる名前でファイルをダウンロードした後、スタートアップファイルとして新しいファイルをダウンロードすることができます。

設定内容の保存または復元

設定内容は、FTP/ TFTP サーバからダウンロードしたり、アップロードしたりすることができます。設定ファイルは、スイッチ設定を復元するためにダウンロードすることができます。

設定ファイルを新しいファイル名でダウンロードして、スタートアップファイルとして設定することができます。なお、ファイル Factory_Default_Config.cfg を、FTP/ TFTP サーバへコピーすることができますが、スイッチの宛先として使用できないことに、留意してください。

表 4-9 フラッシュ/ファイルコマンド

コマンド	機能	モード
一般コマンド		
boot system	システムの起動に使用するファイルまたはイメージを指定します。	GC
copy	フラッシュメモリまたは FTP / TFTP サーバとの間で、コードイメージまたはスイッチ設定をコピーします。	PE
delete	ファイルまたはコードイメージを削除します。	PE
dir	フラッシュメモリ内のファイルのリストを表示します。	PE
whichboot	ブートしたファイルを表示します。	PE
自動コードアップグレードコマンド		
upgrade opcode auto	指定サーバ上で新規バージョンが検知された際、現在のイメージを自動的にアップグレードします。	GC
upgrade opcode path	新規のオペレーションコードが保存されている、FTP/ TFTP サーバおよびディレクトリを指定します。	GC
upgrade opcode reload	オペレーションコードのアップグレード完了時に、スイッチを自動的にリロードします。	GC
show upgrade	オペレーションコードの設定内容を表示します。	PE
TFTP 設定コマンド		
ip tftp retry	スイッチが TFTP サーバへの要求送信を再試行できる回数を指定します。	GC
ip tftp timeout	スイッチが TFTP サーバからの応答を待つ時間を指定して、要求を再送信するか、最後の再試行のためにタイムアウトするまでの時間を指定します。	GC
show ip tftp	TFTP 設定に関する情報を表示します。	PE

4.4.2 boot system

本コマンドは、システムを開始するために使用される、ファイルまたはイメージを指定します。

構文

boot system [*unit no.*:] {config | opcode}: *filename*

config※ - 設定ファイル

opcode※ - ランタイムオペレーションコードです。

unit no. - スイッチのユニット番号です。(コロン(:)が続く)

filename - 設定ファイル名またはコードイメージの名称です。

注※ コロン(:)が必要です。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

◆ 指定ファイルタイプの後にコロン(:)が必要となります。

◆ ファイルにエラーが含まれている場合には、デフォルトファイルとして設定することはできません。

例

```
Console(config)#boot system config: startup
Console(config)#
```

関連コマンド

dir

whichboot

4.4.3 copy

本コマンドでは、コードイメージまたは設定ファイルを、スイッチのフラッシュメモリと FTP/ TFTP サーバ間で、移動(アップロード/ダウンロード)します。システムコードまたはコンフィグレーション設定を FTP / TFTP サーバ上のファイルに保存すると、そのファイルを後でスイッチにダウンロードしてシステム操作を復元できます。ファイル転送が成功するかどうかは、FTP/TFTP サーバのアクセシビリティとネットワーク接続の品質によって異なります。

構文

copy file {file | ftp | running-config | startup-config | tftp}

copy ftp {add-to-running-config | file | https-certificate | public-key | running-config | startup-config}

copy running-config {file | startup-config | tftp}

copy startup-config {file | running-config | tftp}

copy tftp {add-to-running-config | file | https-certificate | public-key |

running-config | startup-config}

add-to-running-config - 指定されたファイルにリストされている設定を、ランニングコンフィグレーションに追加するキーワードです。

file - ファイル間でコピーするためのキーワードです。

ftp - FTP サーバ間でコピーするためのキーワードです。

https-certificate - HTTPS セキュアサイト証明書をコピーできるキーワードです。

public-key - TFTP サーバから SSH キーをコピーするためのキーワードです。（「8.8　SSH」を参照してください。）

running-config - 現在実行中の設定間のコピーをするためのキーワードです。

startup-config - システム初期化に使用される設定です。

tftp - TFTP サーバと間でコピーをするためのキーワードです。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

- copy コマンドを完了するために必要なデータを要求する、プロンプトが表示されます。
- 宛先ファイル名には、スラッシュ(¥ または /)は含めず、スイッチ上のファイルのファイル名の最長文字数は 32 文字で、サーバ上のファイルの最長文字数は 127 文字です。(有効な文字: A-Z, a-z, 0 9, “.”, “-”)
- スイッチは 2 つのオペレーションコードファイルのみサポートしますが、ユーザ定義設定ファイルは、最大 8 ファイルサポートします。
- システムデフォルト設定ファイルからコピーするためのソースとして、 Factory_Default_Config.cfg を使用することができますが、宛先ファイルとしては使用できません。
- スタートアップコンフィグレーションを置換するために、宛先として startup-config を使用する必要があります。
- ブート ROM とローダは、FTP / TFTP サーバからアップロードまたはダウンロードすることはできません。ブート ROM とローダは、FTP/ TFTP サーバからアップロードまたはダウンロードできません。
- https 証明書の指定については、「Web 管理ガイド」の「デフォルトのセキュアサイト証明書の置換」を参照してください。安全な接続に HTTPS を使用するようにスイッチを設定する方法については、ip http secure-server コマンドを参照してください。
- リロードコマンドは、フラッシュメモリへのコピー中は、受け付けられません。
- FTP サーバへロギング中は、インタフェースは、リモートサーバ上で設定されたユーザ名とパスワードを要求します。anonymous がデフォルトのユーザ名として設定されていることに、留意してください。
- リロードコマンドは、フラッシュメモリへのコピー中は、受け付けられません。
- copy コマンドは、サーバからの応答待ちやファイル転送中は、受け付けられません。

例

以下の例では、TFTP サーバからの新規ソフトウェアのダウンロード方法について示しています:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: 2
Source file name: m360.bix
Destination file name: m360.bix
¥Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

以下の例では、TFTP サーバのファイルへの設定内容のアップロード方法について示しています。

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

以下の例では、スタートアップファイルへのランニングコンフィグレーションのコピー方法について示しています。

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
¥Write to FLASH finish.
Success.

Console#
```

以下の例では、設定ファイルのダウンロード方法について示しています。

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.
```

```
¥Write to FLASH finish.
Success.

Console#
```

以下の例では、TFTP サーバからセキュアサイト証明書をコピーする例を示します。次に、スイッチをリブートして証明書をアクティブにします。

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

以下の例では、SSH で使用されるパブリックキーを TFTP サーバからコピーする方法について示しています。SSH によるパブリックキー認証は、スイッチ上でローカルに設定されたユーザに対してのみサポートされています。

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1.RSA:  2.DSA: <1-2>: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

以下の例では、FTP サーバからのファイルのコピー方法について示します。

```
Console#copy ftp file
FTP server IP address: 169.254.1.11
User[anonymous]: admin
Password[]: *****
Choose file type:
 1. config:  2. opcode: 2
Source file name: BLANC.BIX
Destination file name: BLANC.BIX
Console#
```

4.4.4 delete

本コマンドにより、ファイルまたはイメージが削除されます。

構文

delete {file name *filename* | https-certificate | public-key *username* [dsa | rsa]}

file - ファイルの削除をするためのキーワードです。

name - ファイルを示すキーワードです。

filename - 設定ファイル名またはコードイメージの名称です。

https-certificate - HTTPS セキュアサイト証明書を削除できるキーワードです。デフォルトの証明書をロードするには、スイッチを再起動する必要があります。

public-key - スイッチ上の SSH キーを削除するキーワードです。（「8.8　SSH」を参照してください。）

username - SSH ユーザの名前です。(範囲: 1-32 文字)

dsa - DSA パブリックキータイプです。

rsa - RSA パブリックキータイプです。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

- ファイルタイプがシステムスタートアップに使用されている場合、このファイルは削除できません。
- “Factory_Default_Config.cfg”は削除できません。
- パブリックキータイプが指定されていない場合、DSA および RSA キーは削除されます。

例

以下の例では、フラッシュメモリから、test2.cfg 設定ファイルの削除方法について示しています。

```
Console#delete file name test2.cfg
Console#
```

関連コマンド

dir

delete public-key

4.4.5 dir

本コマンドでは、フラッシュメモリ内のファイル一覧を表示します。

構文

dir {config | opcode}: [*filename*]}

config - スイッチ設定ファイルです。

opcode - ランタイムオペレーションコードのイメージファイルです。

filename - 設定ファイル名またはコードイメージの名称です。ファイルが存在していても中身がエラーの場合には、ファイルの情報は表示されません。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

dir コマンドをパラメータ無しで入力した場合、システムは全ファイルを表示します。

ファイル情報は以下の通りです:

表 4-10 ファイルディレクトリ情報

列見出し	説明
File Name	ファイルの名称です。
File Type	ファイルタイプ: オペレーションコードおよび設定ファイルです。
Startup	システム開始時にファイルが使用されているかどうかについて、表示します。
Modify Time	ファイルの最終更新日時です。
Size	ファイルの長さをバイトで示します。

例

以下の例では、全ファイル情報の表示方法について示します。

```
Console#
Console#dir
File Name                      Type    Startup Modified Time       Size (bytes)
------------------------------ ------- ------- ------------------- ------------
 Unit 1:
op1.bix                        OpCode  Y       20XX-07-25 02:39:49    9,130,248
Factory_Default_Config.cfg     Config  N       20XX-07-25 02:37:46          477
startup1.cfg                   Config  Y       20XX-08-07 13:30:09        1,527
------------------------------------------------------------------------------
                      Free space for compressed user config files: 22,372,352
                                                      Total space: 33,554,432
Console#
```

4.4.6 whichboot

本コマンドでは、システムの電源投入時にどのファイルがブートしたかを表示します。

構文

whichboot

デフォルト設定

無し

コマンドモード

Privileged Exec

例

以下の例では、whichboot コマンドで表示される情報について示します。コマンドで表示されるファイル情報の詳細については、dir コマンドの下の表を参照してください。

```
Console#whichboot
File Name                      Type    Startup Modified Time       Size (bytes)
------------------------------ ------- ------- ------------------- ------------
 Unit 1:
AXprimoM210_V1.2.2.2X.bix      OpCode  Y       20XX-04-07 13:18:37      8790280
startup1.cfg                   Config  Y       20XX-07-01 07:24:22         1343
Console#
```

4.4.7 upgrade opcode auto

本コマンドでは、upgrade opcode path コマンドで指定されたサーバ上で、新しいバージョンが検出されたときに、現在のオペレーションコードを自動的にアップグレードします。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

[no] upgrade opcode auto

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

◆ 本コマンドは、オペレーションコードの自動アップグレードを有効または無効にするために、使用されます。スイッチが起動し、このコマンドによって自動イメージアップグレードが有効になると、スイッチは起動時に、以下の手順に従います。

1. upgrade opcode path コマンドで指定された場所で、新しいバージョンのイメージを検索します。TFTP サーバに保存されている新しいイメージの名前は、AXprimoM210.bix である必要があります。スイッチが現在使用中のコードバージョンよりも新しいコードバージョンを検出すると、新しいイメージがダウンロードされます。2 つのコードイメージがすでにスイッチに保存されている場合には、システムを起動するように設定されていないイメージは、新しいバージョンによって上書きされます。
2. イメージがダウンロードされた後、アップグレード操作が成功したかどうかにかかわらず、スイッチはトラップメッセージを送信してログに記録します。
3. 起動イメージとして、新しいバーションを設定します。

◆ デフォルト設定に加えたすべての変更点について、show running-config または show startup-config コマンドで表示することができます。

◆ 自動アップグレードとダイナミックプロビジョニングの両方が有効である場合、まずダイナミックプロビジョニングが動作し、その後に自動アップグレードが動作します。

例

```
Console(config)#upgrade opcode auto
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

指定した場所で新しいイメージが検出されると、ブートアップ中に以下のメッセージタイプが表示されます。

```
.
.
.
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.1.0; new version 1.1.1.2
Image upgrade in progress
The switch will restart after upgrade succeeds
Downloading new image
Flash programming started
Flash programming completed
The switch will now restart
.
.
.
```

4.4.8 upgrade opcode path

本コマンドでは、新しいオペレーションコードが格納されている FTP / TFTP サーバとディレクトリを指定します。現在の設定をクリアするには、このコマンドの no 形式を使用します。

構文

upgrade opcode path *opcode-dir-url*

no upgrade opcode path

opcode-dir-url - 新規コードの場所です。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- 本コマンドは、upgrade opcode auto コマンドと組み合わせて使用され、このコマンドが示す場所に格納されている新しいオペレーションコードの自動アップグレードを容易にします。
- TFTP サーバに保存されている新しいイメージの名前は、AXprimoM210.bix である必要があります。ただし、ファイル名がこのコマンドに含まれていないことに留意してください。
- path 名の文字数は、末尾のスラッシュ(¥ または /)を含めて、最長 130 文字です。
- TFTP サーバを指定する場合、以下の構文を使用する必要があります。ここで filedir は、新しいイメージを含むディレクトリへのパスを示します。
  tftp://192.168.0.1[/filedir]/
- FTP サーバを指定した場合、下記の構文を使用する必要があります。ここで filedir は、新しいイメージを含むディレクトリへのパスを示します。
  ftp://[username[:password@]]192.168.0.1[/filedir]/
  ユーザ名を省略する場合、接続のために“anonymous”が使用されます。パスワードを省略する場合、接続に空列(“”)が使用されます。

例

新規コードが保存されている、TFTP サーバの指定方法を、下記に示します。

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

新規コードが保存されている、FTP サーバの指定方法を、下記に示します。

```
Console(config)#upgrade opcode path ftp://admin:billy@192.168.0.1/sm24/
Console(config)#
```

4.4.9 upgrade opcode reload

本コマンドは、オペレーションコードのアップグレード完了時に、スイッチを自動的にリロードします。この機能を無効にするには、no 形式を使用してください。

構文

[no] upgrade opcode reload

デフォルト設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#upgrade opcode reload
Console(config)#
```

4.4.10 show upgrade

本コマンドでは、オペレーションコードの自動アップグレード設定について示します。

コマンドモード

Privileged Exec

例

```
Console#show upgrade
Auto Image Upgrade Global Settings:
  Status    : Disabled
  Reload Status : Disabled
  Path      :
  File Name : AXprimoM210.bix
Console#
```

4.4.11 ip tftp retry

本コマンドでは、スイッチが設定した TFTP サーバからの応答タイムアウト時間を待っても応答を受信しない場合に、TFTP サーバへの要求送信をリトライできる回数を指定します。デフォルト設定を復元するには、no 形式を使用します。

構文

ip tftp retry *retries*

no ip tftp retry

retries -スイッチが接続を中断する前に、TFTP サーバに要求をリトライできる回数です。(範囲: 1-16)

デフォルト設定

15

コマンドモード

Global Configuration

コマンドの使用方法

◆ スイッチが TFTP サーバからの応答を待つ時間の最大値は、本コマンドと ip tftp timeout コマンドとの組み合わせで決定します。以下に示す TFTP サーバからの最大応答待ち時間の算出式を参考に、最大応答時間が 300 秒以内になるように設定してください。

最大応答待ち時間 ＝ 応答待ち時間 ×（リトライ回数＋１）

例

```
Console(config)#ip tftp retry 10
Console(config)#
```

4.4.12 ip tftp timeout

本コマンドでは、TFTP サーバからの応答待ちタイムアウト時間を指定します。デフォルト設定を復元するには、no 形式を使用します。

構文

ip tftp timeout *seconds*

no ip tftp timeout

seconds -TFTP サーバからの応答待ちタイムアウト時間です。 (範囲: 1-60 seconds)

デフォルト設定

5 秒

コマンドモード

Global Configuration

コマンドの使用方法

◆ スイッチが TFTP サーバからの応答を待つ時間の最大値は、本コマンドと ip tftp retry コマンドとの組み合わせで決定します。以下に示す TFTP サーバからの最大応答待ち時間の算出式を参考に、最大応答待ち時間が 300 秒以内になるように設定してください。

最大応答待ち時間 ＝ 応答待ちタイムアウト ×（リトライ回数＋１）

例

```
Console(config)#ip tftp timeout 10
Console(config)#
```

4.4.13 show ip tftp

本コマンドでは、スイッチ上の TFTP 設定に関する情報を表示します。

構文

show ip tftp

コマンドモード

Privileged Exec

例

```
Console#show ip tftp
TFTP Settings:
  Retries : 15
  Timeout : 5 seconds
Console#
```

4.5 Line

サーバのシリアルポートに VT100 互換のデバイスを接続すると、スイッチにアクセスできます。これらのコマンドは、シリアルポートまたは Telnet(例; 仮想端末)の通信パラメータを設定するために使用されます。

表 4-11 ラインコマンド

コマンド	機能	モード
line	設定のためのラインを識別し、ラインコンフィグレーションモードを開始します。	GC
accounting commands	特定の CLI 特権レベルで入力されたコマンドに、アカウンティング方式を適用します。	LC
accounting exec	ローカルコンソール、Telnet または SSH 接続に、アカウンティング方式を適用します。	LC
authorization commands	特定の CLI 特権レベルで入力されたコマンドに、認証方法を適用します。	LC
authorization exec	ローカルコンソール、Telnet または SSH 接続に、アカウンティング方式を適用します。	LC
databits※	ハードウェアによって解釈され、生成される 1 文字あたりのデータビット数を設定します。	LC
exec-timeout	ユーザ入力が検出されるまで、コマンドインタープリタが待機する間隔を設定します。	LC
login	ログイン時のパスワードチェックを有効にします。	LC
parity※	パリティビットの生成を定義します。	LC
password	ラインのパスワードを指定します。	LC
password-thresh	パスワード入力の閾値を設定します。これにより、ログオンに失敗した回数が制限されます。	LC
silent-time※	ログオン試行の失敗した回数が、password-thresh コマンドで設定した閾値を超えた後で、管理コンソールにアクセスできない時間を設定します。	LC
speed※	端末のボーレートを設定します。	LC
stopbits※	バイトごとに送信される、ストップビットの数を設定します。	LC
timeout login response	システムがログイン試行を待つ間隔を設定します。	LC
disconnect	回線接続を終了します。	PE
terminal	エスケープ文字、行の長さ、端末の種類、および幅を含む、端末を設定します。	PE
show line	端末回線のパラメータを表示します。	NE, PE

注※ これらのコマンドは、シリアルポートにのみ適用されます。

4.5.1 line

本コマンドでは、設定のためのラインを識別し、後続のライン設定コマンドを処理します。

構文

line {console | vty}

console - コンソール端末行です。

vty - リモートコンソールアクセス用の仮想端末です(例; Telnet)。

デフォルト設定

デフォルトラインはありません。

コマンドモード

Global Configuration

コマンドの使用方法

Telnet は仮想端末接続とみなされ、show users のような画面表示では”VTY”と表示されます。しかしながら、シリアル通信パラメータ(例; データビット)は、Telnet 接続に影響を与えません。

例

コンソールラインモードに入るには、以下のコマンドを入力します:

```
Console(config)#line console
Console(config-line)#
```

関連コマンド

show line

show users

4.5.2 databits

本コマンドでは、コンソールポートによって解釈、生成される 1 文字あたりのデータビット数を設定します。デフォルト値を復元するには、no 形式を使用します。

構文

databits {7 | 8}

no databits

7 - 1 文字あたり 7 データビットです。

8 - 1 文字あたり 8 データビットです。

デフォルト設定

1 文字あたり 8 データビットです。

コマンドモード

Line Configuration

コマンドの使用方法

databits コマンドは、パリティ付き 7 データビットを生成するデバイスからの入力の上位ビットをマスクするために使用できます。パリティが生成されている場合は、1 文字につき 7 データビットを指定します。

パリティを必要としない場合は、1 文字につき 8 データビットを指定します。

例

7 データビットを指定するには、以下のコマンドを入力してください:

```
Console(config-line-console)#databits 7
Console(config-line-console)#
```

関連コマンド

parity

4.5.3 exec-timeout

本コマンドにより、ユーザ入力が検出されるまでシステムが待機する間隔を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

exec-timeout [*seconds*]

no exec-timeout

seconds - タイムアウト間隔を指定する整数です。(範囲: 60 から 65535 秒; 0: タイムアウト無し)

デフォルト設定

600 秒

コマンドモード

Line Configuration

コマンドの使用方法

- タイムアウト時間内にユーザの入力が検知されると、セッションは開いたままになります。そうでなければ、セッションは終了します。
- 本コマンドは、ローカルコンソールと Telnet コンソールの両方に適用されます。
- Telnet のタイムアウトは無効にできません。
- タイムアウトを指定せずにコマンドを使用すると、デフォルト設定が復元されます。
- タイムアウト無し設定は console にのみ設定できます。

例

タイムアウトを 2 分に設定するには、以下のコマンドを入力してください:

```
Console(config-line-console)#exec-timeout 120
Console(config-line-console)#
```

4.5.4 login

本コマンドでは、ログイン時のパスワードチェックを有効にします。パスワードチェック無効にして、パスワード無しで接続を許可するには、no 形式を使用します。

構文

login [local]

no login

local -ローカルパスワードチェックを選択します。認証は username コマンドで指定されたユーザ名にもとづいています。

デフォルト設定

login local

コマンドモード

Line Configuration

コマンドの使用方法

- ログイン時にスイッチ自身が提供する認証モードは、以下の 3 つがあります:
  - login を選択すると、password line 設定コマンドで指定された 1 つのグローバルパスワードで認証を行います。この方法を使用する場合、管理インタフェースは Normal Exec（NE）モードで起動します。
  - login local を選択すると、username コマンドで指定されたユーザ名とパスワードで認証を行います（デフォルト設定)。この方法を使用する場合、管理インタフェースは、ユーザの特権レベル（それぞれ 0 または 15）に応じて、Normal Exec（NE）または Privileged Exec（PE）モードで起動します。
  - no login を選択すると、認証を行いません。この方法を使用する場合、管理インタフェースは Normal Exec（NE）モードで起動します。
- このコマンドは、スイッチ自体を介したログイン認証を制御します。リモート認証サーバのユーザ名とパスワードを構成するには、それらのサーバーにインストールされている RADIUS または TACACS ソフトウェアを使用する必要があります。

例

```
Console(config-line-console)#login local
Console(config-line-console)#
```

関連コマンド

username

password

4.5.5 parity

パリティビットの生成を定義します。デフォルト設定を復元するには、no 形式を使用します。

構文

parity {none | even | odd}

no parity

none - パリティ無し

even - 偶数パリティ

odd - 奇数パリティ

デフォルト設定

パリティ無し

コマンドモード

Line Configuration

コマンドの使用方法

端末やモデル等のデバイスにより提供される通信プロトコルは、頻繁に特定のパリティビット設定を要求します。

例

パリティ無しを指定するには、以下のコマンドを入力してください。

```
Console(config-line-console)#parity none
Console(config-line-console)#
```

4.5.6 password

本コマンドでは、ラインのパスワードを指定します。パスワードを消去するには、no 形式を使用してください。

構文

password {0 | 7} *password*

no password

{0 | 7} - 0 は、通常パスワードであり、7 は暗号化パスワードを意味します。

password - ラインパスワードを指定する文字列です。(最長: 16 文字のプレーンテキストまたは暗号化、大文字と小文字を区別します)

デフォルト設定

パスワードは指定されていません。

コマンドモード

Line Configuration

コマンドの使用方法

- パスワード保護された回線で接続が開始されると、システムはパスワードの入力を求めます。正しいパスワードを入力すると、プロンプトが表示されます。password-thresh コマンドを使用すると、システムが回線接続を終了して端末をアイドル状態に戻す前に、不正なパスワードを入力できる回数を設定できます。
- 暗号化されたパスワードは、システムの起動時に FTP サーバから設定ファイルを読み取る際に、従来のパスワード設定(プレーンテキストまたは暗号化)との互換性のために必要となります。暗号化されたパスワードを手動で設定する必要はありません。

例

```
Console(config-line-console)#password 0 secret
Console(config-line-console)#
```

関連コマンド

login

password-thresh

4.5.7 password-thresh

本コマンドにより、ログイン試行の失敗回数を制限するパスワード入力の閾値を設定します。閾値を削除するには、no 形式を使用してください。

構文

password-thresh [*threshold*]

no password-thresh

threshold - 許可されたパスワード試行の回数です。(範囲: 1 から 120 回; 0: 閾値無し)

デフォルト設定

デフォルト値は、3 回です。

コマンドモード

Line Configuration

コマンドの使用方法

ログオン試行の閾値に達すると、次のログオン試行を許可する前にシステムインタフェースが指定された時間だけ管理コンソールへアクセスできません。(この間隔を設定するには、silent-time コマンドを使用します。)Telnet でこの閾値に達すると、Telnet ログオンインタフェースはシャットダウンします。

例

パスワード閾値を 5 回に設定するには、以下のコマンドを入力します。

```
Console(config-line-console)#password-thresh 5
Console(config-line-console)#
```

関連コマンド

silent-time

4.5.8 silent-time

本コマンドにより、失敗したログオン試行の回数が password-thresh コマンドで設定した閾値を超過後に、管理コンソールにアクセスできない時間を設定します。設定を削除するには、no 形式を使用します。

構文

silent-time [*seconds*]

no silent-time

seconds -コンソール応答を無効にする秒数です。(範囲: 0 から 65535 秒; 0 は無効の意味です)

デフォルト設定

無効

コマンドモード

Line Configuration

例

サイレント時間を 60 秒に設定するには、以下のコマンドを入力してください:

```
Console(config-line-console)#silent-time 60
Console(config-line-console)#
```

関連コマンド

password-thresh

4.5.9 speed

本コマンドにより、端末回線のボーレートを設定します。このコマンドは、送信(端末へ)と受信(端末から)の両方の速度を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

speed *bps*

no speed

bps -ボーレート(ビット/秒)です。

(オプション: 9600, 19200, 38400, 57600, 115200 bps)

デフォルト設定

115200 bps

コマンドモード

Line Configuration

コマンドの使用方法

シリアルポートに接続されているデバイスのボーレートと一致するように速度を設定します。ポートに接続されているデバイスで使用可能なボーレートの一部がサポートされていない可能性があります。システムは、選択した速度がサポートされていないかどうかが示されます。

例

57600 bps を指定するには、以下のコマンドを入力してください:

```
Console(config-line-console)#speed 57600
Console(config-line-console)#
```

4.5.10 stopbits

本コマンドにより、バイトごとに送信されるストップビットの数を設定します。デフォルト設定を復元するには、no 形式を使用します。

構文

stopbits {1 | 2}

no stopbits

1 - 1 ストップビット

2 - 2 ストップビット

デフォルト設定

1 ストップビット

コマンドモード

Line Configuration

例

2 ストップビットを指定するには、以下のコマンドを入力してください:

```
Console(config-line-console)#stopbits 2
Console(config-line-console)#
```

4.5.11 timeout login response

本コマンドにより、ユーザが CLI にログインするまでシステムが待機する間隔を設定します。デフォルト設定を復元するには、no 形式を使用します。

構文

timeout login response [*seconds*]

no timeout login response

seconds - タイムアウト間隔を指定する整数です。

(範囲: 10 から 300 秒)

デフォルト設定

300 秒

コマンドモード

Line Configuration

コマンドの使用方法

- タイムアウト間隔内にログイン試行が検出されない場合、セッションは接続が終了します。
- 本コマンドは、ローカルコンソールと Telnet コンソールの両方に適用されます。
- Telnet のタイムアウトは無効にできません。
- タイムアウトを指定せずにコマンドを使用すると、デフォルト設定が復元されます。

例

タイムアウトを 2 分に設定するには、以下のコマンドを入力してください:

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

4.5.12 disconnect

本コマンドは、SSH、Telnet またはコンソール接続を終了します。

構文

disconnect *session-id*

session-id - SSH、Telnet またはコンソール接続のセッション識別子です。(範囲: 0-8)

コマンドモード

Privileged Exec

コマンドの使用方法

セッション識別子”0”を指定すると、コンソール接続が切断されます。アクティブセッションのその他の識別子を指定すると、SSH または Telnet 接続が切断されます。

例

```
Console#disconnect 1
Console#
```

関連コマンド

show ssh

show users

4.5.13 terminal

本コマンドは、エスケープ文字、表示される行、端末のタイプ、幅、およびコマンド履歴を含む、端末を設定します。適切なキーワードとともに no 形式を使用して、デフォルト設定に戻します。

構文

terminal {escape-character {ascii-number | *character*} | history [size *size*] | length *length* | terminal-type {ansi-bbs | vt-100 | vt-102} | width *width*}

escape-character - 現在の行入力からエスケープするための、キーボード文字です。

ascii-number - ASCII 10 進数相当(範囲: 0-255)

character -すべての有効文字。

history - コマンドバッファに格納され、矢印キーを使用して呼び出される行数。(範囲: 0-256)

length - 画面に表示される行数。(範囲: 24 から 200．0 は一時停止しないことを意味します)

terminal-type - 使用される端末エミュレーションのタイプです。

ansi-bbs - ANSI-BBS

vt-100 - VT-100

vt-102 - VT-102

width - 端末に表示される文字列の数です(範囲: 80-300)

デフォルト設定

escape-character: 27 (ASCII 番号)

history: 10

length: 24

terminal-type: VT100

width: 80

コマンドモード

Privileged Exec

例

以下の例では、show running-config などの長い出力を持つコマンドで表示される行数を、48 行に設定します。

```
Console#terminal length 48
Console#
```

4.5.14 show line

本コマンドにより、端末回線のパラメータを表示します。

構文

show line [console | vty]

console - コンソール端末です。

vty - リモートコンソールアクセス用の仮想端末です(例; Telnet)。

デフォルト設定

すべての行を表示します。

コマンドモード

Normal Exec, Privileged Exec

例

すべての行を表示するには、以下のコマンドを入力してください:

```
Console#show line
 Terminal Configuration for this session:
  Length                          : 24
  Width                           : 80
  History Size                    : 10
  Escape Character(ASCII-number) : 27
  Terminal Type                   : VT100

 Console Configuration:
  Password Threshold : 3 times
  EXEC Timeout       : 600 seconds
  Login Timeout      : 300 seconds
  Silent Time        : Disabled
  Baud Rate          : 115200
  Data Bits          : 8
  Parity             : None
  Stop Bits          : 1

 VTY Configuration:
```

```
  Password Threshold : 3 times
  EXEC Timeout       : 600 seconds
  Login Timeout      : 300 sec.
  Silent Time        : Disabled
Console#
```

4.6 イベントロギング

この章では、スイッチのイベントロギングの設定に使用されるコマンドについて、説明します。

表 4-12 イベントロギングコマンド

コマンド	機能	モード
logging command	シスログの RAM およびフラッシュに CLI コマンド実行記録を格納します。	GC
logging facility	シスログメッセージのリモートロギングのファシリティタイプを設定します。	GC
logging history	重要度にもとづいてスイッチメモリに保存される、シスログメッセージを制限します。	GC
logging host	ロギングメッセージを受信する、シスログサーバのホスト IP アドレスを設定します。	GC
logging on	エラーメッセージのロギングを制御します。	GC
logging trap	重要度にもとづいてリモートサーバに保存される、シスログメッセージを制限します。	GC
clear log	ロギングバッファからのメッセージをクリアします	PE
show log	ログメッセージを表示します。	PE
show logging	ロギングの状態を表示します。	PE

4.6.1 logging command

本コマンドは、CLI コマンド実行レコードを、シスログ RAM とフラッシュに保存します。この機能を無効にするには、no 形式を使用してください。

構文

[no] logging command

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

格納されるレコードには、CLI から実行されたコマンド、コマンド実行時間、およびユーザ名、ユーザインタフェース(コンソール、Telnet、SSH)およびユーザ IP アドレスを含む CLI ユーザに関する情報が含まれます。このレコードタイプの重要度は 6 です(logging facility コマンドを参照してください)。

例

```
Console(config)#logging command
Console(config)#
```

4.6.2 logging facility

本コマンドは、シスログメッセージのリモートロギングのファシリティタイプを設定します。タイプをデフォルトの状態に復元するには、no 形式を使用します。

構文

logging facility *type*

no logging facility

type -ログメッセージを適切に処理するために、シスログサーバが使用する機能を示す番号です。(範囲: 16 から 23)

デフォルト設定

23

コマンドモード

Global Configuration

コマンドの使用方法

本コマンドでは、シスログメッセージにファシリティタイプタグを指定します。(RFC 3164 を参照)このタイプは、スイッチから報告されるメッセージの種類には影響を与えません。しかしながら、メッセージを整理したり、対応したデータベースにメッセージを格納するために、シスログサーバによって使用される場合があります。

例

```
Console(config)#logging facility 19
Console(config)#
```

4.6.3 logging history

本コマンドは、重要度にもとづいてスイッチメモリに保存されるシスログメッセージを制限します。シスログメッセージのロギングを、デフォルトレベルに戻すには、no 形式を使用してください。

構文

logging history {flash | ram} *level*

no logging history {flash | ram}

flash - フラッシュメモリに格納されるイベント履歴です(例; パラメータメモリ)。

ram - 一時的な RAM に格納されるイベント履歴(例; 電源リセット時にフラッシュされたメモリ)。

level - 以下に記載するレベルです。(範囲: 0-7)

表 4-13 ロギングレベル

レベル	重要度の名称	説明
7	debugging	メッセージのデバッグです。

レベル	重要度の名称	説明
6	informational	情報メッセージのみです。
5	notifications	コールドスタートなどの正常だが、重要な状態です。
4	warnings	警告状態(例; 不良戻り、予期しない返品など)
3	errors	エラー状態(例; 無効な入力、デフォルトの使用)
2	critical	重大な状態(例; メモリ割り当て、またはフリーメモリエラー - リソースの枯渇)
1	alerts	直ちに対処が必要です。
0	emergencies	システムが使用不可です。

デフォルト設定

Flash: errors (レベル 3 から 0)

RAM: debugging (レベル 7 から 0)

コマンドモード

Global Configuration

コマンドの使用方法

フラッシュメモリ用に指定するメッセージレベルは、RAM 用に指定するメッセージレベルより優先度を高くなければなりません(例; 数値的に低い)。

例

```
Console(config)#logging history ram 0
Console(config)#
```

4.6.4 logging host

本コマンドは、ロギングメッセージを受信するシスログサーバのホスト IP アドレスを設定します。シスログサーバホストを削除するには、no 形式を使用します。

構文

logging host *host-ip-address* [port *udp-port*]

no logging host *host-ip-address*

host-ip-address - シスログの IPv4 または IPv6 アドレスです。

udp-port - リモートサーバで使用される UDP ポート番号です。(範囲: 1-65535)

デフォルト設定

host-ip-address：無し

UDP Port: 514

コマンドモード

Global Configuration

コマンドの使用方法

◆　このコマンドを複数回使用して、ホストの IP アドレス一覧を構築します。

◆　許容されている最大 IP アドレス数は、5 つです。

例

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

4.6.5 logging on

本コマンドは、エラーメッセージのロギングを制御し、デバッグまたはエラーメッセージをロギング処理に送信します。ロギング処理を無効にするには、no 形式を使用してください。

構文

[no] logging on

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

ロギング処理は、メモリに保存、またはリモートシスログサーバに送信されるエラーメッセージを制御します。logging history コマンドを使用すると、メモリに格納されているエラーメッセージのタイプを制御できます。logging trap コマンドを使用して、指定されたシスログサーバに送信されるエラーメッセージのタイプを制御することができます。

例

```
Console(config)#logging on
Console(config)#
```

関連コマンド

logging history

logging trap

clear log

4.6.6 logging trap

本コマンドは、リモートサーバへのシステムメッセージのロギングを有効にするか、または重要度にもとづいて、リモートサーバに保存されるシスログメッセージを制限します。リモートログを有効にするには、このコマンドを使用します。リモートロギングを無効にするには、no 形式を使用してください。

構文

logging trap [level *level*]

no logging trap [level]

level - シスログ重要度を 1 つ指定します。シスログ重要度については「表 4-13　ロギングレベル」を参照してください。

デフォルト設定

無効

Level 7

コマンドモード

Global Configuration

コマンドの使用方法

- 指定したレベルでこのコマンドを使用すると、リモートロギングが有効になり、保存する最小重要度レベルが設定されます。
- 指定したレベルを指定せずにこのコマンドを使用すると、リモートロギングも有効になりますが、最小重要度レベルがデフォルトに戻されます。

例

```
Console(config)#logging trap level 4
Console(config)#
```

4.6.7 clear log

本コマンドにより、ログバッファからのメッセージがクリアされます。

構文

clear log [flash | ram]

flash - フラッシュメモリに格納されたイベント履歴です(例; パラメータメモリ)。

ram - 一時的な RAM に格納されたイベント履歴(例; 電源リセット時に消去されるメモリ)。

デフォルト設定

flash および RAM

コマンドモード

Privileged Exec

例

```
Console#clear log
Console#
```

関連コマンド

show log

4.6.8 show log

本コマンドでは、ローカルメモリに格納されたログメッセージを表示します。

構文

show log {flash | ram}

flash - フラッシュメモリに格納されたイベント履歴です(例; パラメータメモリ)。

ram - 一時的な RAM に格納されたイベント履歴(例; 電源リセット時にフラッシュされたメモリ)。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

- ◆ すべてのログメッセージは、ウォームリスタート後(例; コマンドインタフェースで電源がリセットされた後)に RAM およびフラッシュに保持されます。
- ◆ すべてのログメッセージは、コールドリスタート後(例; 電源を切ってから電源を入れた後)、フラッシュメモリに保持され、RAM から消去されます。

例

以下の例では、RAM に格納されているイベントメッセージを示しています。

```
Console#show log ram
[1] 00:01:30 20XX-01-01
   "VLAN 1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 20XX-01-01
   "Unit 1, Port  1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
Console#
```

4.6.9 show logging

本コマンドでは、メッセージをローカルスイッチメモリ、SMTP イベントハンドラ、またはリモートシスログサーバに記録するためのコンフィグレーションを表示します。

構文

show logging {command | flash | ram | sendmail | trap}

command - CLI コマンド実行レコードを、シスログ RAM およびフラッシュに格納するかどうかの設定を表示します。

flash - イベントメッセージをフラッシュメモリに格納するための設定を表示します(例; パラメータメモリ)。

ram - イベントメッセージを一時的な RAM に格納するための設定を表示します (例; 電源リセット時にフラッシュされたメモリ)。

sendmail - SMTP イベントハンドラの設定を表示します。

trap - トラップ機能の設定を表示します。

デフォルト設定

無し

コマンドモード

Privileged Exec

例

以下の例では、システムログが有効であり、フラッシュメモリのメッセージレベルが“errors”(デフォルトレベル 3 から 0）であり、RAM のメッセージレベルが“debugging”(デフォルトレベル 7 から 0）であることを示しています。

```
Console#show logging flash
Global Configuration:
  Syslog Logging           : Enabled
Flash Logging Configuration:
  History Logging in Flash : Level Errors (3)
Console#show logging ram
Global Configuration:
  Syslog Logging           : Enabled
Ram Logging Configuration:
  History Logging in RAM   : Level Debugging (7)
Console#
```

表 4-14 show logging flash/ram - 表示の説明

フィールド	説明
Syslog Logging	システムロギングが、logging on コマンドを通じて有効になっているかどうかを示しています。

フィールド	説明
History Logging in Flash	logging history コマンドをベースに報告された、メッセージレベルです。
History Logging in RAM	logging history コマンドをベースに報告された、メッセージレベルです。

以下の例では、トラップ機能の設定を示しています。

```
Console#show logging trap
Global Configuration:
  Syslog Logging           : Enabled
Remote Logging Configuration:
  Status                   : Disabled
  Facility Type            : Local use 7 (23)
  Level Type               : Debugging messages (7)
Console#
```

表 4-15 show logging trap - 表示の説明

フィールド	説明
Global Configuration	
Syslog logging	システムロギングが、logging on コマンドを通じて有効になっているかどうかを示しています。
Remote Logging Configuration	
Status :	リモートロギングが、logging trap コマンドを通じて有効になっているかどうかを示しています。
Facility Type	logging facility コマンドで指定された、シスログメッセージのリモートロギングのファシリティタイプです。
Level Type	logging trap コマンドで指定されたリモートサーバに送信される、シスログメッセージの重要度の閾値です。

関連コマンド

show logging sendmail

4.7 SMTP アラート

本コマンドでは、SMTP イベントハンドリングを設定し、警告メッセージを指定した SMTP サーバと電子メール受信者に転送します。

表 4-16 イベントロギングコマンド

コマンド	機能	モード
logging sendmail	SMTP イベント処理を有効にします。	GC
logging sendmail destination-email	警告メッセージの電子メール受信者を設定します。	GC
logging sendmail host	警告メッセージを受信する SMTP サーバを設定します。	GC
logging sendmail level	警告メッセージの送信対象とする、イベント重要度の閾値を設定します。	GC
logging sendmail source-email	警告メッセージの「From」フィールドに使用される電子メールアドレスを設定します。	GC
show logging sendmail	SMTP イベントハンドラ設定を表示します。	NE, PE

4.7.1 logging sendmail

本コマンドは、SMTP イベント処理を有効にします。この機能を無効にするには、no 形式を使用してください。

構文

[no] logging sendmail

デフォルト設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#logging sendmail
Console(config)#
```

4.7.2 logging sendmail destination-email

本コマンドでは、警告メッセージの電子メール受信者を指定します。受信者を削除するには、no 形式を使用してください。

構文

[no] logging sendmail destination-email *email-address*

email-address - 警告メッセージで使用されるソース電子メールアドレスです。(範囲: 1 から 41 文字)。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

警告メッセージには、最大 5 つの受信者を指定することができます。しかしながら、各受信者を特定するために、別コマンドを入力する必要があります。

例

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

4.7.3 logging sendmail host

本コマンドでは、警告メッセージを送信する SMTP サーバを指定します。SMTP サーバを削除するには、no 形式を使用してください。

構文

[no] logging sendmail host *ip-address*

ip-address - イベント処理の警告メッセージを送信する、SMTP サーバの IPv4 アドレスです。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- イベント処理用に最大 3 つの SMTP サーバを指定することができます。
- 電子メールで警告メッセージを送信するために、スイッチは最初に接続を開き、キュー内で待機しているすべての電子メール警告を送信し、最後に接続を閉じます。
- 接続を開くために、スイッチは最後にメールを送信したサーバ、またはこのコマンドで設定されたいづれかのサーバを選択します。メールの送信に失敗すると、スイッチはリスト内の他のサーバを選択し、再度メール送信を試みます。それでも送信失敗すると、システムは定期的な間隔で処理を繰り返します。

例

```
Console(config)#logging sendmail host 192.168.1.19
```

```
Console(config)#
```

4.7.4 logging sendmail level

本コマンドでは、警告メッセージを送信対象とする、イベント重要度の閾値を設定します。デフォルト設定を復元するには、no 形式を使用します。

構文

logging sendmail level *level*

no logging sendmail level

level - システムメッセージレベルを指定します。(範囲: 0 から 7):

デフォルト設定

Level 7

コマンドモード

Global Configuration

コマンドの使用方法

指定したレベルは、イベント閾値を示します。このレベル以上のすべてのイベントは、設定された電子メール受信者に送信されます。(たとえば、レベル 7 を使用すると、レベル 7 からレベル 0 までのすべてのイベントが報告されます。)

例

以下の例では、レベル 3 から 0 までのシステムエラーの電子メール警告が送信されます。

```
Console(config)#logging sendmail level 3
Console(config)#
```

4.7.5 logging sendmail source-email

本コマンドでは、警告メッセージの「From」フィールドに使用される電子メールアドレスを設定します。デフォルト値を復元するには、no 形式を使用します。

構文

logging sendmail source-email *email-address*

no logging sendmail source-email

email-address - 警告メッセージで使用されるソース電子メールアドレスです。(範囲: 1 から 41 文字)。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

スイッチを識別するシンボリック電子メールアドレス、またはスイッチを担当する管理者のアドレスを使用できます。

例

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

4.7.6 show logging sendmail

本コマンドでは、SMTP イベントハンドラの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show logging sendmail
SMTP Servers
-------------------------------------------
192.168.1.19

SMTP Minimum Severity Level: 7

SMTP Destination E-mail Addresses
-------------------------------------------
ted@this-company.com

SMTP Source E-mail Address: bill@this-company.com

SMTP Status: Enabled
Console#
```

4.8 時刻設定

システムクロックは、指定されたタイムサーバ(NTP または SNTP)のセットをポーリングすることによって、動的に設定することができます。スイッチの正確な時刻を維持することで、システムログにイベントエントリの意味のある日時を記録することができます。クロックが設定されていない場合、スイッチは工場出荷時のデフォルト設定の時刻で動作します。

警告: スイッチイベントを正確に記録するために、SNTP または NTP を使うことを強く推奨します。システムクロックの手動での設定の場合、システムイベントのタイムスタンプが正確でない場合があります。

表 4-17 タイムコマンド

コマンド	機能	モード
SNTP コマンド		
sntp client	指定されたタイムサーバからの時刻を受け入れます。	GC
sntp poll	クライアントが時間をポーリングする間隔を設定します。	GC
sntp server	時刻を取得するタイムサーバを指定します。	GC
show sntp	現在の SNTP コンフィグレーションを示します。	NE, PE
NTP コマンド		
ntp authenticate	NTP トラフィックの認証を有効にします。	GC
ntp authentication-key	認証キーを設定します。	GC
ntp client	指定したサーバからの時刻更新のために、NTP クライアントを有効にします。	GC
ntp server	時間更新をポーリングする、NTP サーバを指定します。	GC
show ntp	現在の NTP コンフィグレーションを示します。	NE, PE
マニュアルコンフィグレーションコマンド		
clock summer-time (date)	スイッチの内部クロック用※にサマータイム を設定します。	GC
clock summer-time (predefined)	スイッチの内部クロック用※にサマータイム を設定します。	GC
clock summer-time (recurring)	スイッチの内部クロック用※にサマータイム を設定します。	GC
clock timezone	スイッチの内部クロック用にタイムゾーンを設定します。	GC
calendar set	システム日時を設定します。	PE
show calendar	現在の日時を表示します。	NE, PE

注※ サマータイム

4.8.1 sntp client

本コマンドにより、sntp server コマンドで指定された NTP または SNTP タイムサーバからの時刻同期のための、SNTP クライアント要求を有効にします。SNTP クライアント要求を無効にするには、no 形式を使用します。

構文

[no] sntp client

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- SNTP および NTP サーバは、同時に有効にすることはできません。コマンドを使用する前に NTP クライアントを無効にしてください。
- タイムサーバから取得した時刻は、ログイベントの正確な日時を記録するために使用されます。SNTP または NTP を使用しない場合、スイッチは工場出荷時のデフォルトの時刻となります(例;20XX 年 12 月 31 日 07:32:04)。
- 本コマンドは、sntp server コマンドで指定されたタイムサーバへのクライアントの時刻要求を有効にします。sntp poll コマンドで設定した間隔にもとづいて、時間同期要求を発行します。

例

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current Time:  Dec 23 2:52:44 20XX
Poll Interval: 60
Current Mode: Unicast
SNTP Status : Enabled
SNTP Server 192.168.140.80 0.0.0.0 0.0.0.0
Current Server: 192.168.140.80
Console#
```

関連コマンド

sntp server

sntp poll

show sntp

4.8.2 sntp poll

本コマンドは、スイッチが SNTP クライアントモードに設定されているときの送信時間の間隔を設定します。デフォルトを復元するには、no 形式を使用してください。

構文

sntp poll *seconds*

no sntp poll

seconds - 時刻要求間の間隔。(範囲: 16 から 16384 秒)

デフォルト設定

16 秒

コマンドモード

Global Configuration

例

```
Console(config)#sntp poll 60
Console#
```

関連コマンド

sntp client

4.8.3 sntp server

本コマンドは、SNTP 時間要求を発行するサーバの IP アドレスを設定します。現在の一覧から特定サーバをクリアするには、no 形式を使用してください。

構文

sntp server *ip1* [*ip2* [*ip3*]]

no sntp server *ip1* [*ip2* [*ip3*]]

ip - タイムサーバの IPv4 または IPv6 アドレスです(NTP or SNTP)。

(範囲: 1 から 3 アドレス)。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

本コマンドでは、SNTP クライアントモードに設定されている場合、スイッチが時間の更新をポーリングするタイムサーバを指定します。クライアントは、応答が受信されるまで指定された順序でタイムサーバをポーリングします。sntp poll コマンドで設定した間隔にもとづいて、時間同期要求を発行します。

例

```
Console(config)#sntp server 10.1.0.19
Console#
```

関連コマンド

sntp client

sntp poll

show sntp

4.8.4 show sntp

本コマンドでは、SNTP クライアントの現在時刻とコンフィグレーションを表示し、スイッチの時刻が適切に更新されているかについて示します。

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

本コマンドでは、現在時刻、時刻同期要求を送信するために使用されるポーリング間隔、使用中のモードを表示します。

例

```
Console#show sntp
Current Time   : Nov  5 18:51:22 20XX
Poll Interval  : 16 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 192.168.140.80
               : 192.168.140.90
               : 192.168.140.99
Current Server : 192.168.140.80
Console#
```

4.8.5 ntp authenticate

本コマンドでは、NTP クライアントとサーバの通信の認証を有効にします。認証を無効にするには、no 形式を使用してください。

構文

[no] ntp authenticate

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

NTP 認証を有効にすると、認証された NTP サーバからの時刻のみ許容します。認証キーとそれに関連するキー番号は一元的に管理し、NTP サーバとクライアントに手動で配布する必要があります。キー番号とキー値は、サーバとクライアントの両方で一致する必要があります。

例

```
Console(config)#ntp authenticate
Console(config)#
```

関連コマンド

ntp authentication-key

4.8.6 ntp authentication-key

本コマンドでは、NTP 認証が有効な場合に使用する認証キーとキー番号を設定します。現在のリストから特定の認証キーまたはすべてのキーをクリアするには、コマンドの no 形式を使用してください。

構文

ntp authentication-key *number* md5 *key*

no ntp authentication-key [*number*]

number - NTP 認証キーID 番号です。(範囲: 1-65533)

md5 -MD5 を使用して、認証することを示します。

key - MD5 認証キー文字列。キー文字列は、最大 32 文字の大文字と小文字を区別できる印字可能な ASCII 文字(スペースなし)です。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- キーID 番号は、NTP 認証キーリストの中のキー値を指定します、スイッチでは最高 32 文字まで設定することができます。設定する各サーバのコマンドを再度入力してください。
- NTP 認証キーID 番号と値は、サーバとクライアント上の両方で合致している必要があります。

- NTP 認証はオプションです。ntp authenticate コマンドで有効にした場合、このコマンドを使用して最低 1 つのキーID 番号を設定する必要があります。
- このコマンドの no 形式を引数無しで使用すると、リスト内のすべての認証キーがクリアされます。

例

```
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#
```

関連コマンド

ntp authenticate

4.8.7 ntp client

本コマンドにより、ntp servers コマンドで指定された NTP タイムサーバから時刻同期のための NTP クライアント要求を有効にします。NTP クライアント要求を無効にするには、no 形式を使用してください。

構文

[no] ntp client

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- SNTP および NTP サーバは、同時に有効にすることはできません。コマンドを使用する前に SNTP クライアントを無効にしてください。
- タイムサーバから取得した時刻は、ログイベントの正確な日時を記録するために使用されます。NTP あるいは SNTP を使用しない場合、スイッチは工場出荷時のデフォルトの時刻となります(例; 20XX 年 12 月 10 日 16:04:43)。
- 本コマンドにより、ntp servers コマンドで指定されたタイムサーバへのクライアント時間要求を有効にします。ntp poll コマンドで設定した間隔にもとづいて、時間同期要求を発行します。

例

```
Console(config)#ntp client
Console(config)#
```

関連コマンド

sntp client

ntp server

4.8.8 ntp server

本コマンドでは、NTP 時間要求が発行されるサーバの IP アドレスを設定します。現在のリストから特定のタイムサーバ、またはすべてのサーバをクリアするには、コマンドの no 形式を使用してください。

構文

ntp server *ip-address* [key *key-number*]

no ntp server [*ip-address*]

ip-address - NTP タイムサーバの IP アドレスです。

key-number - サーバとの通信で使用するための認証キーの数です。(範囲: 1-65535)

デフォルト設定

バージョン番号: 3

コマンドモード

Global Configuration

コマンドの使用方法

- 本コマンドでは、NTP クライアントモードに設定されている場合、スイッチが時間の更新をポーリングするタイムサーバを指定します。ntp poll コマンドで設定した間隔にもとづいて、時間同期要求を発行します。クライアントは設定されたすべてのタイムサーバをポーリングし、受信したレスポンスをフィルタリングおよび比較して、スイッチの最も信頼性の高い正確な時刻にアップデートします。
- スイッチに最大 3 の NTP サーバを設定できます。設定する各サーバのコマンドを再度入力してください。
- NTP 認証はオプションです。ntp authenticate コマンドで有効にした場合、ntp authentication-key コマンドを使用して、最低 1 つのキー番号を設定する必要があります。
- このコマンドの no 形式を引数無しで使用すると、リスト内のすべての認証キーがクリアされます。

例

```
Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#
```

関連コマンド

ntp client

show ntp

4.8.9 show ntp

本コマンドでは、現在時刻と NTP クライアントのコンフィグレーションが表示され、スイッチの時刻が適

切にアップデートされているかどうかについて、示します。

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

本コマンドでは、現在時刻、時刻同期要求を送信するために使用されるポーリング間隔、および認証の設定が有効かを表示します。

例

```
Console#show ntp
Current Time             : Apr 29 13:57:32 20XX
Current Mode             : unicast
NTP Status               : Disabled
NTP Authenticate Status  : Enabled
Last Update NTP Server   : 0.0.0.0        Port: 0
Last Update Time         : Jan  1 00:00:00 20XX UTC
NTP Server 192.168.3.20 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.4.22 version 3 key 19
NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885
Console#
```

4.8.10 clock summer-time (date)

本コマンドでは、スイッチのサマータイムの開始日時、終了日時、およびオフセット時間を設定します。サマータイムを無効にするには、no 形式を使用してください。

構文

clock summer-time *name* date *b-date b-month b-year b-hour b-minute e-date e-month e-year e-hour e-minute* [*offset*]

no clock summer-time

name - サマータイムが有効時のゾーン名です。(範囲: 1-30 文字)

b-date -サマータイムが始まる月日です。(範囲: 1 から 31)

b-month -サマータイムが開始する月です。(オプション: 1 月 | 2 月 | 3 月 | 4 月 | 5 月 | 6 月 | 7 月 | 8 月 | 9 月 | 10 月 | 11 月 | 12 月)

b-year-サマータイムが開始する年です。

b-hour - サマータイムが開始する時間です。(範囲: 0 から 23 時間)

b-minute -サマータイムが開始する分です。(範囲: 0 から 59 分)

e-date -サマータイムが終わる日付です。(範囲: 1-31)

e-month -サマータイムが終わる月です。(オプション: 1 月 | 2 月 | 3 月 | 4 月 | 5 月 | 6 月 | 7 月 | 8 月 | 9 月 | 10 月 | 11 月 | 12 月)

e-year -サマータイムが終わる年です。

e-hour - サマータイムが終わる時間です。(範囲: 0 から 23 時間)

e-minute -サマータイムが終わる分です。(範囲: 0 から 59 分)

offset -標準時間帯からのオフセット（偏差）です(分単位)。(範囲: 1 から 120 分)

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- 国や地域によっては、時計は夏の季節に調整され、午後には昼間が長く午前中は短くなります。これは、サマータイムまたは夏時間(DST)として知られています。通常、クロックは春の開始時に 1 時間前に調整され、その後秋には後ろに調整されます。
- 本コマンドは、現在設定されているタイムゾーンを基準に夏時間のタイムゾーンを設定します。サマータイムが有効になっている現地時間に対応する時間を指定するには、夏時間のタイムゾーンが通常のタイムゾーン(オフセット)から逸脱する分数を指定する必要があります。

例

下記の例では、20XX 年のサマータイムを 3 月 9 日の 60 分先に設定し、11 月 2 日に通常の時間に戻します。

```
Console(config)#clock summer-time DEST date march 9 20XX 01 59 november       2 20XX 01 59 60
Console(config)#
```

関連コマンド

show sntp

4.8.11 clock summer-time (predefined)

本コマンドでは、世界のいくつかの主要地域に対して事前定義された設定を使用して、サマータイムのステータスとスイッチを設定します。サマータイムを無効にするには、no 形式を使用してください。

構文

clock summer-time *name* predefined [australia | europe | new-zealand | usa]

no clock summer-time

name -夏時間が有効な間のタイムゾーンの名称です。(範囲: 1-30 文字)

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- 国や地域によっては、時計は夏の季節に調整され、午後には昼間が長く午前中は短くなります。これは、サマータイムまたは夏時間(DST)として知られています。通常、クロックは春の開始時に 1 時間前に調整され、その後秋には後ろに調整されます。
- このコマンドは、設定されたタイムゾーンに関連するサマータイム時間を設定します。サマータイムが有効になっている現地時間に対応する時間を指定するには、自分の地域に適した夏時間のタイムゾーンを事前に選択するか、あらかじめ定義された設定が自分の地域に該当しない場合は夏時間を手動で設定します(clock summer-time (date)または clock summer-time (recurring)を参照してください)。

表 4-18 事前定義された夏時間パラメータ

地域	開始時間、日、週および月	終了時間、日、週および月	Rel.オフセット
オーストラリア（australia）	10 月第 1 日曜日 02:00:00	4 月第 1 日曜日 01:59:59	60 分
ヨーロッパ（europe）	3 月最終日曜日 01:00:00	10 月最終土曜日 23:59:59	60 分
ニュージーランド（new-zealand）	9 月最終日曜日 02:00:00	4 月第 1 日曜日 01:59:59	60 分
アメリカ（usa）	3 月第 2 日曜日 02:00:00	11 月第 1 日曜日 00:59:59	60 分

例

以下の例では、ヨーロッパの事前定義設定を使用するために使用する夏時間の設定について、説明します。

```
Console(config)#clock summer-time MESZ predefined europe
Console(config)#
```

関連コマンド

show sntp

4.8.12 clock summer-time (recurring)

本コマンドによりユーザは、スイッチのサマータイムの開始時期（曜日）、終了時期（曜日）、およびオフセット時間を、年単位で繰り返すように設定をすることができます。サマータイムを無効にするには、no 形式を使用してください。

構文

clock summer-time *name* recurring *b-week b-day b-month b-hour b-minute e-week e-day e-month e-hour e-minute* [*offset*]

no clock summer-time

name -サマータイムが有効な間のタイムゾーンの名称です。(範囲: 1-30 文字)

b-week - サマータイムが始まる月の週です。(範囲: 1-5)

b-day - サマータイムが始まる曜日です。(オプション: 日曜日 | 月曜日 | 火曜日 | 水曜日 | 木曜日 | 金曜日 | 土曜日)

b-month -サマータイムが開始する月です。(オプション: 1 月 | 2 月 | 3 月 | 4 月 | 5 月 | 6 月 | 7 月 | 8 月 | 9 月 | 10 月 | 11 月 | 12 月)

b-hour -サマータイムが開始する時間です。(範囲: 0 から 23 時間)

b-minute -サマータイムが開始する分です。(範囲: 0 から 59 分)

e-week - サマータイムが終わる月の週です。(範囲: 1-5)

e-day - サマータイムが終わる曜日です。(オプション: 日曜日 | 月曜日 | 火曜日 | 水曜日 | 木曜日 | 金曜日 | 土曜日)

e-month -サマータイムが終わる月です。(オプション: 1 月 | 2 月 | 3 月 | 4 月 | 5 月 | 6 月 | 7 月 | 8 月 | 9 月 | 10 月 | 11 月 | 12 月)

e-hour -サマータイムが終わる時間です。(範囲: 0 から 23 時間)

e-minute -サマータイムが終わる分です。(範囲: 0 から 59 分)

offset -標準時間帯からのオフセット（偏差）です(分単位)。(範囲: 1 から 120 分)

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- 国や地域によっては、時計は夏の季節に調整され、午後には昼間が長く午前中は短くなります。これは、サマータイムまたは夏時間(DST)として知られています。通常、クロックは春の開始時に 1 時間前に調整され、その後秋には後ろに調整されます。
- 本コマンドは、現在設定されているタイムゾーンを基準に夏時間のタイムゾーンを設定します。サマータイムが有効になっている現地時間に対応する時間を表示するには、夏時間のタイムゾーンが通常のタイムゾーン(オフセット)から逸脱している分数を指定する必要があります。

例

以下の例では、60 分の夏時間を定期的に繰り返して、3 月の第 1 週の金曜日に 01:59 時間に開始し、夏時間は、第 2 週の土曜日に 01:59 時間に終了します。

```
Console(config)#clock summer-time MESZ recurring 1 friday march 01 59 3 saturday november 1 59
60
Console(config)#
```

関連コマンド

show sntp

4.8.13 clock timezone

本コマンドでは、スイッチの内部クロックのタイムゾーンを設定します。

構文

clock timezone *name* hours *hours* [minute *minutes* | before-utc | after-utc]

name - タイムゾーン名称、通常は頭字語です。(範囲: 1-30 文字)

hours - UTC の前後の時間数です。(範囲: UTC の 0-12 時間前、UTC の 0-13 時間後）

minutes - UTC の前後の分数です。(範囲: 0 から 59 分)

before-utc - ローカルタイムゾーンを UTC の前（東）に設定します。

after-utc - ローカルタイムゾーンを UTC の後(西)に設定します。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

本コマンドでは、地球本来の子午線(経度 0 度)にもとづいて、協定世界時間(UTC、以前はグリニッジ標準時または GMT)を基準にしたローカルタイムゾーンを設定します。現地時間に対応する時間を表示するには、時間帯が UTC の東(前)または西(後)にある時間と分の数を指定する必要があります。

例

```
Console(config)#clock timezone Japan hours 9 minute 0 after-UTC
Console(config)#
```

関連コマンド

show sntp

4.8.14 calendar set

本コマンドでは、システムクロックを設定します。これは使用しているネットワークにタイムサーバが無い場合や、タイムサーバからシグナルを受信するようにスイッチを構成していない場合に、使用されます。

構文

calendar set *hour min sec* {*day month year* | *month day year*}

hour - Hour in 24-hour format.(範囲: 0 から 23)

min - 分です。(範囲: 0 から 59)

sec - 秒です。(範囲: 0 から 59)

day - 月の日付です。(範囲: 1 から 31)

month january | february | march | april | may | june | july | august | september | october | november | december

year - 年(4 桁)です。(範囲: 1970 から 2037)

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

SNTP が有効な場合には、クロックは手動で設定されません。

例

以下の例では、システムクロックを 20XX 年 2 月 1 日 15:12:34 に設定する方法について、示しています。

```
Console#calendar set 15:12:34 1 February 20XX
Console#
```

4.8.15 show calendar

本コマンドでは、システムクロックを表示します。

デフォルト設定

無し

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show calendar
 Current Time          : May 13 14:08:18 20XX
 Time Zone             : UTC, 08:00
 Summer Time           : Not configured
 Summer Time in Effect : No
Console#
```

4.9 時間範囲設定

本章では、PoE 機能で使用するための、時間範囲を設定するコマンドについて説明します。

表 4-19 タイムレンジコマンド

コマンド	機能	モード
time-range	時間範囲の名称を指定し、時間範囲設定モードに入ります。	GC
absolute	絶対時間範囲を設定します。	TR
periodic	定期実行の時間範囲を指定します。	TR
show time-range	設定した時間範囲を示します。	PE

4.9.1 time-range

本コマンドでは、時間範囲の名称を指定して時間範囲設定モードに入ります。以前に指定した時間範囲を削除するには、no 形式を使用してください。

構文

[no] time-range *name*

name - 時間範囲の名称です。(範囲: 1-32 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

◆ 本コマンドでは、PoE 機能で使用される時間範囲を設定します。

◆ 時間範囲には、最大 8 つのルールを設定することができます。

例

```
Console(config)#time-range poe-timer
Console(config-time-range)#
```

関連コマンド

PoE

4.9.2 absolute

本コマンドでは、コマンド実行のための絶対時間範囲を設定します。以前に指定した時間を削除するには、no 形式を使用してください。

構文

absolute start *hour minute day month year*

[end hour minutes day month year]

absolute end *hour minutes day month year*

no absolute

hour - Hour in 24-hour format.(範囲: 0 から 23)

minute - 分です。(範囲: 0 から 59)

day - 月の日付です。(範囲: 1 から 31)

month - 1 月 | 2 月 | 3 月 | 4 月 | 5 月 | 6 月 | 7 月 | 8 月 | 9 月 | 10 月 | 11 月 | 12 月

year - 年(4 桁)です。(範囲: 2013 から 2037)

デフォルト設定

無し

コマンドモード

Time Range Configuration

コマンドの使用方法

- ◆ 時間範囲が既に設定されている場合には、新しい時間範囲を設定する前に既存の入力を削除するために、no 形式を使用する必要があります。
- ◆ 同じ時間範囲に絶対時間ルールと複数の定期ルールの両方が設定されている場合には(例; 名前付きエントリ)、現在の時間が絶対時間範囲と定期的時間範囲の中にある場合のみ、このエントリが有効となります。
- ◆ 設定した時間範囲の適用には最大±60sec の誤差が生じる場合があります。

例

以下の例では、イベントが 1 回発生する時間を設定します。

```
Console(config)#time-range poe-timer
Console(config-time-range)#absolute start 1 1 1 april 20XX end 2 1 1 april 20XX
Console(config-time-range)#
```

4.9.3 periodic

本コマンドでは、コマンドの定期実行の時間範囲を設定します。以前に指定した時間範囲を削除するには、no 形式を使用してください。

構文

[no] periodic {daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend} *hour minute* to {daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend | *hour minute*}

daily - 毎日

friday - 金曜日

monday - 月曜日

saturday - 土曜日

sunday - 日曜日

thursday - 木曜日

tuesday - 火曜日

wednesday - 水曜日

weekdays - 平日

weekend - 週末

hour - 24 時間形式の時間です。(範囲: 0 から 23)

minute - 分です。(範囲: 0 から 59)

デフォルト設定

無し

コマンドモード

Time Range Configuration

コマンドの使用方法

- 時間範囲が既に設定されている場合には、新しい時間範囲を設定する前に既存の入力を削除するために、no 形式を使用する必要があります。
- 同じ時間範囲に絶対時間ルールと複数の定期ルールの両方が設定されている場合には(例; 名前付きエントリ)、現在の時間が絶対時間範囲と定期的時間範囲の中にある場合のみ、このエントリが有効となります。
- daily, weekday, weekend では 0:00~23:59 の範囲でのみ設定可能です
- 設定した時間範囲の適用には最大±60sec の誤差が生じる場合があります。

例

以下の例では、イベントの定期的発生の時間範囲を設定します。

```
Console(config)#time-range sales
Console(config-time-range)#periodic daily 1 1 to 2 1
Console(config-time-range)#
```

4.9.4 show time-range

本コマンドでは、設定した時間範囲を示します。

構文

show time-range [*name*]

name - 時間範囲の名称です。(範囲: 1-32 文字)

デフォルト設定

無し

コマンドモード

Privileged Exec

例

```
Console#show time-range poe-timer
 Time-range poe-timer:
   status: inactive
   absolute start 01:01 01 April 20XX
   periodic    Daily 01:01 to    Daily 02:01
   periodic    Daily 2:01 to    Daily 3:01
Console#
```

5 SNMP コマンド

SNMP コマンドは、SNMP(Simple Network Management Protocol)を使用して管理ステーションからこのスイッチへのアクセスを制御し、トラップマネージャに送信されるエラータイプも制御します。

SNMP バージョン 3 は、メッセージの整合性、認証、および暗号化をカバーするセキュリティ機能も提供します。MIB ツリーの特定の領域へのユーザアクセスを制御することができます。SNMPv3 を使用するには、最初に SNMP エンジン ID を設定するか(またはデフォルトを受け入れる)、MIB ツリーの読み取りと書き込みのアクセスビューを指定し、必要なセキュリティモデル(SNMP v1、v2c または v3)およびセキュリティレベル(例; AuthPriv)、次に特定の認証パスワードとプライバシーパスワードと共に SNMP ユーザをこれらのグループに割り当てます。

表 5-1 SNMP コマンド

コマンド	機能	モード
SNMP の基本コマンド		
snmp-server	SNMP エージェントを有効にします。	GC
snmp-server community	SNMP コマンドへのアクセスを許可するための、コミュニティアクセス文字列を設定します。	GC
snmp-server contact	システムコンタクト文字列を設定します。	GC
snmp-server location	システムロケーション文字列を設定します。	GC
show snmp	SNMP コミュニケーションステータスを表示します。	NE, PE
SNMP 通知コマンド		
snmp-server enable traps	SNMP トラップを送信するためにデバイスを有効にします(例; SNMP 通知)。	GC
snmp-server host	SNMP 通知動作の受信者を指定します。	GC
snmp-server enable port-traps link-up-down	SNMP トラップを送信するためにデバイスを有効にします(例; SNMP 通知)。	IC
snmp-server enable port-traps mac-notification	リンクアップまたはリンクダウン状態の変更時に SNMP トラップを送信するために、デバイスを有効にします(例; SNMP 通知)	IC
show snmp-server enable port-traps	動的 MAC アドレスが追加、または削除された時に SNMP トラップ(例; SNMP 通知)を送信するために、デバイスを有効にします。	PE
SNMPv3 コマンド		
snmp-server engine-id	SNMP エンジン ID を設定します。	GC
snmp-server group	SNMP グループ、マッピングユーザをビューに追加します。	GC
snmp-server user	SNMP グループにユーザを追加します。	GC
snmp-server view	SNMP ビューを追加します。	GC

コマンド	機能	モード
show snmp engine-id	SNMP エンジン ID を追加します。	PE
show snmp group	SNMP グループを表示します。	PE
show snmp user	SNMP ユーザを表示します。	PE
show snmp view	SNMP ビューを表示します。	PE
通知ログコマンド		
nlm	指定した通知ログを有効にします。	GC
snmp-server notify-filter	通知ログを作成し、ターゲットホストを指定します。	GC
show nlm oper-status	設定した通知ログの動作ステータスを表示します。	PE
show snmp notify-filter	設定した通知ログを表示します。	PE
プライベートトラップコマンド		
memory	メモリ使用率アラームの上昇および下降閾値を設定します。	GC
process cpu	CPU 使用率アラームの上昇および下降閾値を設定します。	GC
process cpu guard	CPU 使用率基準および閾値を設定します。	GC

5.1 SNMP の基本コマンド

5.1.1 snmp-server

本コマンドでは、すべての管理クライアント(例; バージョン 1,2c、3)の SNMPv3 エンジンとサービスを有効にします。サーバを無効にするには、no 形式を使用してください。

構文

[no] snmp-server

デフォルト設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server
Console(config)#
```

5.1.2 snmp-server community

本コマンドでは、SNMP v1 または v2c を使用してクライアントによる管理アクセスを認可するために使用される、コミュニティアクセス文字列を定義します。指定コミュニティ文字列を削除するには、no 形式を使用してください。

構文

snmp-server community *string* [ro | rw]

no snmp-server community *string*

string - SNMP プロトコルへのアクセスを許可するためのパスワードのような働きをする、コミュニティ文字列です。(最長: 16 文字、大文字小文字を区別; コミュニティの最大設定数: 5):

ro - 読み取り専用アクセスのみ指定します。認可された管理ステーションは、MIB オブジェクトの取得のみ、おこなうことができます。

rw -読み取り/書き込みアクセスです認可された管理ステーションは、MIB オブジェクトの取得と変更の両方をおこなうことができます。

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server community alpha ro
Console(config)#
```

5.1.3 snmp-server contact

本コマンドでは、システムコンタクト文字列を設定します。システムコンタクト情報を削除するには、no 形式を使用してください。

構文

snmp-server contact *string*

no snmp-server contact

string - システムコンタクト情報を説明する文字列です。(最長: 255 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server contact Paul
Console(config)#
```

関連コマンド

snmp-server location

5.1.4 snmp-server location

本コマンドでは、システムロケーション文字列を設定します。ロケーション文字列を削除するには、no 形式を使用してください。

構文

snmp-server location *text*

no snmp-server location

text - システムロケーションを説明する文字列です。(最長: 255 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server location WC-19
Console(config)#
```

関連コマンド

snmp-server contact

5.1.5 show snmp

本コマンドは、SNMP 通信ステータスを確認するために使用することができます。

デフォルト設定

無し

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

本コマンドでは、コミュニティアクセス文字列、SNMP の入出力データユニットのカウンタ、および snmp-server enable traps コマンドを使用して、SNMP ロギングが有効になっているかどうかについての情報を提供します。

例

```
Console#show snmp

SNMP Agent : Enabled

SNMP Traps :
 Authentication : Enabled
 MAC-notification : Disabled
 MAC-notification interval : 1 second(s)

SNMP Communities :
   1. public, and the access level is read-only
   2. private, and the access level is read/write

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
```

```
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP Logging: Disabled
Console#
```

5.2 SNMP 通知コマンド

5.2.1 snmp-server enable traps

本コマンドにより、デバイスは Simple Network Management Protocol トラップの送信または通知(例; SNMP 通知)を有効にします。SNMP 通知を無効にするには、no 形式を使用してください。

構文

[no] snmp-server enable traps [authentication | mac-notification [interval *seconds*]]

authentication - 認証エラー通知を発行するキーワードです。

mac-notification - 動的 MAC アドレスが追加または削除された時にトラップを発行するためのキーワードです。

interval - 連続する 2 つのトラップを発行する間隔を指定します。(範囲: 1 から 3600 秒; デフォルト: 1 秒)

デフォルト設定

認証トラップを発行

他のトラップは無効

コマンドモード

Global Configuration

コマンドの使用方法

- snmp-server enable traps コマンドを入力しない場合、このコマンドで制御される通知は送信されません。SNMP 通知を送信するようにこのデバイスを設定するには、少なくとも 1 つの snmp-server enable traps コマンドを入力する必要があります。キーワードを指定しないでコマンドを入力すると、両方の認証通知が有効になります。キーワードを指定してコマンドを入力すると、そのキーワードに関連する通知タイプだけが有効になります。
- snmp-server enable traps コマンドは、snmp-server host コマンドとの組み合わせで使用されます。snmp-server host コマンドを使って、どのホストが SNMP 通知を受信するかを指定します。通知を送信するには、最低 1 つの snmp-server host コマンドを入力する必要があります。
- 認証トラップはレガシー通知であるため、SNMP バージョン 3 ホストで使用する場合は、snmp-server group コマンドで割り当てられた通知ビューの対応するエントリとともに有効にする必要があります。
- MAC アドレステーブル変更のトラップでインターバル時間が設定されている場合、MAC アドレステーブルの変更があると、最初にトラップがバッファに格納されます。バッファに保存されたトラップは、バッファが空になるまで継続的に送信されます。 バッファデータを送信した後、インターバル時間に達していない状態で新たにトラップが発行されると、トラップがバッファに保持され、インターバル時間が経過すると、この新しいバッファデータが送信されます。

  たとえば、トラップインターバルが 15 分に設定され、最初の MAC アドレステーブル変更のトラップが 10:00 に送信されたとします。 10:00 のトラップ送信後から 10:15 までの間に発行されるトラップはバッファに格納されます。そして 10:15 になるとバッファに格納されたトラップがすべて送信されます。このように以降 15 分間隔でトラップがまとめて送信されます。

例

```
Console(config)#snmp-server enable traps authentication
Console(config)#
```

関連コマンド

snmp-server host

5.2.2 snmp-server host

本コマンドは、Simple Network Management Protocol 通知操作の受信者を指定します。指定した受信者を削除するには、no 形式を使用してください。

構文

snmp-server host *host-addr* [inform [retry *retries* | timeout *seconds*]] *community-string* [version {1 | 2c | 3 {auth | noauth | priv} [udp-port *port*]}

host-addr - ホストの IPv4 または IPv6 アドレスです(対象受信者)。(最大ホストアドレス: 5 トラップ宛先 IP アドレスエントリ)

inform - 通知が情報メッセージとして送信されます。オプションはバージョン 2c と 3 ホストにのみ使用することができます。(デフォルト: トラップを使用)

retries - 受信者が受信確認を確認しなかった場合に、通知メッセージを再送信する最大回数です。(範囲: 0 から 255; デフォルト: 3):

seconds - 通知メッセージを再送信するまでの確認応答を待機する秒数です。(範囲: 0 から 2147483647 センチ秒: デフォルト: 1500 センチ秒)

community-string - SNMP V1 および V2c ホストに通知操作とともに送信されるパスワードのようなコミュニティストリングです。この文字列は、snmp-server host コマンドを単独で使用して設定することもできますが、snmp-server host コマンドを使用する前に、snmp-server community コマンドを使用して定義することを推奨します。(最長: 16 文字)

version - SNMP バージョン 1、2c、または 3 のトラップとして通知を送信するかどうかを指定します。(範囲: 1,2c、3; デフォルト: 1):

auth | noauth | priv - SNMPv3 を認証有り、認証なし、または認証と暗号化有りで使用します。これらの認証および暗号化オプションの詳細については、「Web 管理ガイド」の「SNMP」を参照してください。

port - 使用するホスト UDP プールです。(範囲: 1 から 65535; デフォルト: 162):

デフォルト設定

ホストアドレス無し

通知タイプトラップ

SNMP バージョン: 1

UDP ポート 162

コマンドモード

Global Configuration

コマンドの使用方法

- snmp-server host コマンドを入力しない場合、通知は送信されません。SNMP 通知を送信するようにこのデバイスを設定するには、少なくとも 1 つの snmp-server host コマンドを入力する必要があります。複数のホストを有効にするには、各ホストに対して別々の snmp-server host コマンドを発行してください。
- snmp-server enable traps コマンドと一緒に snmp-server host コマンドが使用されます。トラップの送信を有効にするか、どの SNMP 通知をグローバルに送信するかについて通知または指定するには、snmp-server enable traps コマンドを使用してください通知を受信するホストについては、そのホストに対して、最低 1 つの snmp-server enable traps コマンドと snmp-server host コマンドを有効にする必要があります。
- いくつかの通知タイプは snmp-server enable traps コマンドでは制御できません。たとえば、いくつかの通知タイプは常に有効になっています。
- 通知はデフォルトでトラップメッセージとしてスイッチによって発行されます。トラップメッセージの受信者は、スイッチに応答を送信しません。したがって、トラップは通知メッセージのように信頼性が高くなく、受信確認の要求を含みます。インフォームを使用して、重要な情報がホストによって確実に受信されるようにすることができます。ただし、情報が応答を受信するまでメモリに保持されなければならないため、情報はより多くのシステムリソースを消費することに注意してください。インフォームはネットワークトラフィックにも追加されます。トラップや通知として通知を発行するかどうかを決定するときは、これらの影響を考慮する必要があります。
  SNMPv2c ホストにインフォームを送信するには、下記のステップを完了させてください:
  1. SNMP エージェントを有効にします。
  2. 必要な通知メッセージでビューを作成します。
  3. 必要な通知ビューを含むグループを作成します。
  4. SNMP トラップを送信するスイッチを許容します。
  5. この章で説明するように、snmp-server host コマンドで通知メッセージを受信するターゲットホストを指定します。

  SNMPv3 ホストにインフォームを送信するには、下記のステップを完了させてください:
  1. SNMP エージェントを有効にします。
  2. メッセージ交換処理で使用するリモート SNMPv3 ユーザを作成します。
  3. 必要な通知メッセージでビューを作成します。
  4. 必要な通知ビューを含むグループを作成します。
  5. SNMP トラップを送信するスイッチを許容します。
  6. この章で説明するように、snmp-server host コマンドで通知メッセージを受信するターゲットホストを指定します。
- 管理ステーションがサポートする SNMP バージョンに応じて、スイッチは SNMP バージョン 1、2c または 3 の通知をホスト IP アドレスに送信できます。snmp-server host コマンドで SNMP バージョンが指定されていない場合、デフォルトでは SNMP バージョン 1 の通知が送信されます。
- SNMP バージョン 3 ホストを指定すると、コミュニティ文字列は SNMP ユーザ名として解釈されます。ユーザ名は、まず snmp-server user コマンドで定義する必要があります。それ以外の場合は、指定したコミュニティストリングの名前と読み取り、書き込み、および通知ビューのデフォルト設定を使用して、SNMPv3 グループが snmp-server host コマンドによって自動的に作成されます。

例

```
Console(config)#snmp-server host 10.1.19.23 admin
Console(config)#
```

関連コマンド

snmp-server enable traps

5.2.3 snmp-server enable port-traps link-up-down

本コマンドでは、リンクアップまたはリンクダウンの状態が変わった際に、SNMP トラップを送信するためのデバイスを有効にします(例; SNMP 通知)。SNMP トラップを送信するためにデバイスを有効にします(例; SNMP 通知)。この機能を無効にするには、no 形式を使用します。

構文

[no] snmp-server enable port-traps link-up-down

link-up-down - リンクアップまたはリンクダウンの状態が変わった際に、トラップを発行するためのキーワードです。

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps link-up-down
Console(config)#
```

5.2.4 snmp-server enable port-traps mac-notification

本コマンドでは、動的 MAC アドレスが追加または削除されたときにデバイスが SNMP トラップ(SNMP 通知)を送信できるようになります。デフォルト設定を復元するには、no 形式を使用してください。

構文

[no] snmp-server enable port-traps mac-notification

mac-notification - 動的 MAC アドレスが追加または削除された時に、トラップを発行するためのキーワードです。

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

本コマンドでは、snmp-server enable traps mac-authentication コマンドでグローバルレベルでも有効になっている場合に限り、現在のインタフェース上で MAC アドレストラップを有効にすることができます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps mac-notification
Console(config)#
```

5.2.5 show snmp-server enable port-traps

本コマンドでは、指定したインタフェース上で SNMP トラップが有効になっているか無効になっているかについて表示します。

構文

show snmp-server enable port-traps interface [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

コマンドモード

Privileged Exec

例

```
Console#show snmp-server enable port-traps interface
Interface MAC Notification Trap
--------- ---------------------
Eth 1/1                     No
Eth 1/2                     No
Eth 1/3                     No
.
.
.
```

5.3 SNMPv3 コマンド

5.3.1 snmp-server engine-id

本コマンドでは、SNMPv3 エンジンの識別文字列を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

snmp-server engine-id {local | remote {*ip-address*}} *engineid-string*

no snmp-server engine-id {local | remote {*ip-address*}}

local - スイッチの SNMP エンジンを指定します。

remote - リモートデバイスの SNMP エンジンを指定します。

ip-address - リモートデバイスの IPv4 アドレスです。

engineid-string - エンジン ID を識別する文字列です。(範囲: 9 から 64 の 16 進数)

デフォルト設定

MAC アドレスをベースにスイッチによって、固有のエンジン ID が生成されます。

コマンドモード

Global Configuration

コマンドの使用方法

- SNMP エンジンは、このスイッチまたはリモートデバイスのいずれかにある独立した SNMP エージェントです。このエンジンは、メッセージの再送、遅延、およびリダイレクトから保護します。エンジン ID は、ユーザパスワードと組み合わせて使用され、SNMPv3 パケットの認証と暗号化のためのセキュリティキーを生成します。
- SNMPv3 通知を使用する場合は、リモートエンジン ID が必要です。(snmp-server host を参照してください。)リモートエンジン ID は、スイッチとリモートホスト上のユーザ間で渡されるパケットの認証と暗号化のためのセキュリティダイジェストを計算するために使用されます。SNMP パスワードは、権限のあるエージェントのエンジン ID を使用してローカライズされています。informs の場合、権限のある SNMP エージェントはリモートエージェントです。　したがって、プロキシ要求または通知を送信する前に、リモートエージェントの SNMP エンジン ID を設定する必要があります。
- エンジン ID を固有に指定するために、末尾のゼロを入力する必要はありません。つまり、値「0123456789」は、「0123456789」に相当し、その後にローカルエンジン ID について 16 個のゼロが続きます。
- スイッチに固有のローカルエンジン ID が自動的に生成されます。これはデフォルトのエンジン ID と呼ばれます。ローカルエンジン ID が削除または変更された場合、すべての SNMP ユーザがクリアされます。　既存のすべてのユーザを再構成する必要があります。

例

```
Console(config)#snmp-server engine-id local 1234567890
Console(config)#snmp-server engine-id remote 192.168.1.19 9876543210
Console(config)#
```

関連コマンド

snmp-server host

5.3.2 snmp-server group

このコマンドは、SNMP グループとマッピング SNMP ユーザを SNMP ビューに追加します。SNMP グループを削除するには、no 形式を使用してください。

構文

snmp-server group *groupname*

{v1 | v2c | v3 {auth | noauth | priv}}

[read *readview*] [write *writeview*] [notify *notifyview*]

no snmp-server group *groupname*

groupname - SNMP グループの名称です。(範囲: 1-32 文字)

v1 | v2c | v3 - SNMP バージョン 1、1c または 3 を使用します。

auth | noauth | priv - SNMPv3 を認証あり、認証なし、または認証と暗号化ありで使用します。これらの認証および暗号化オプションの詳細については、「Web 管理ガイド」の「SNMP」を参照してください。

readview - 読み取りアクセスのビューを定義します。(1-32 文字)

writeview - 書き込みアクセスのビューを定義します。(1-32 文字)

notifyview - 通知のビューを定義します。(1-32 文字)

デフォルト設定

デフォルトグループ: public※1 (read only), private※2 (read/write)

readview - インターネット OID スペース(1)に属するすべてのオブジェクトです。

writeview - 何も定義されていません。

notifyview - 何も定義されていません。

注※1 ビューが定義されていません。

注※2 Defaultview にマップします。

コマンドモード

Global Configuration

コマンドの使用方法

- グループは割り当てられたユーザに対し、アクセスポリシーを設定します。
- 認証が選択された場合、snmp-server user コマンドに指定されているように、MD5 または SHA アルゴリズムが選択されます。
- プライバシーが選択された場合、データ暗号化のために DES 56 ビットアルゴリズムが使用されます。
- このスイッチでサポートされている通知メッセージの追加情報については、「Web 管理ガイド」の表「サポートされている通知メッセージ」を参照してください。また認証、リンクアップおよびリンク

ダウンメッセージはレガシートラップなので、snmp-server enable traps コマンドで有効にする必要があります。

例

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

5.3.3 snmp-server user

本コマンドはユーザを SNMP グループに追加し、特定の SNMP Read ビュー、Write ビューまたは Notify ビューにユーザを制限します。SNMP グループからユーザを削除するには、no 形式を使用してください。

構文

snmp-server user *username groupname*

{v1 | v2c | v3 [encrypted] [auth {md5 | sha} *auth-password* [priv {3des | aes128 | aes192 | aes256 | des56} *priv-password*]]

snmp-server user *username groupname* remote *ip-address*

{v3 [encrypted] [auth {md5 | sha} *auth-password* [priv {3des | aes128 | aes192 | aes256 | des56} *priv-password*]]

no snmp-server user *username* {v1 | v2c | v3 | remote *ip-address* v3}

username - SNMP エージェントへ接続しているユーザ名です。(範囲: 1 から 32 文字)

groupname - ユーザが割り当てられている SNMP グループ名です。(範囲: 1 から 32 文字)

remote - リモートデバイスの SNMP エンジンを指定します。

ip-address - リモートデバイスの IPv4 アドレスです。

v1 | v2c | v3 - SNMP バージョン 1、1c または 3 を使用します。

encrypted - パスワードを暗号化入力として受け取ります。

auth - SNMPv3 を認証で使用します。

md5 | sha - MD5 または SHA 認証を使用します。

auth-password - 認証パスワードです。encrypted オプションを使用していない場合には、プレーンテキストとして入力します。それ以外は暗号化パスワードを入力してください。(範囲: 非暗号化パスワードの場合 8 から 16 文字)

encrypted オプションを使用している場合には、暗号化パスワードを入力してください。(範囲: MD5 暗号化パスワードの場合は 16 文字、SHA 暗号化パスワードの場合は 40 文字)

3des - プライバシー付きの SNMPv3 を 3DES(168 ビット)暗号化で使用します。

aes128 - AES128 暗号化でプライバシー付きの SNMPv3 を使用します。

aes192 - AES192 暗号化でプライバシー付きの SNMPv3 を使用します。

aes256 - AES256 暗号化でプライバシー付きの SNMPv3 を使用します。

des56 - DES56 暗号化でプライバシー付きの SNMPv3 を使用します。

priv-password - プライバシーパスワードです。encrypted オプションを使用していない場合には、プレーンテキストとして入力します。それ以外は暗号化パスワードを入力してください。(範囲: 8 から 16 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- ローカルユーザ(例; コマンドでリモートエンジン識別子が指定されていない)は、SNMPv3 クライアントの管理アクセスを許可するか、あるいは、ローカルスイッチから送信された SNMPv3 トラップメッセージの送信元を識別するように設定する必要があります。
- ローカルスイッチから送信された SNMPv3 通知メッセージの送信元を識別するように、リモートユーザ(例; リモートエンジン識別子を指定するコマンド)を設定する必要があります。
- SNMP エンジン ID は、パスワードからの認証/プライバシーダイジェストを計算するために使用されます。したがって、この設定コマンドを使用する前に、snmp-server engine-id コマンドでエンジン ID を設定する必要があります。
- リモートユーザを設定する前に、snmp-server engine-id コマンドを使用して、ユーザが常駐するリモートデバイスのエンジン ID を指定します。次に、snmp-server user コマンドを使用してユーザとそのユーザが常駐するリモートデバイスの IP アドレスを指定します。リモートエージェントの SNMP エンジン ID は、ユーザのパスワードから認証/プライバシーダイジェストを計算するために使用されます。リモートエンジン ID が最初に設定されていない場合、リモートユーザを指定する snmp-server user コマンドは失敗します。
- SNMP パスワードは、権限のあるエージェントのエンジン ID を使用してローカライズされています。informs の場合、権限のある SNMP エージェントはリモートエージェントです。したがって、プロキシ要求または通知を送信する前に、リモートエージェントの SNMP エンジン ID を設定する必要があります。

例

```
Console(config)#snmp-server user steve r&d v3 auth md5 greenpeace priv des56 einstien
Console(config)#snmp-server engine-id remote 192.168.1.19 9876543210
Console(config)#snmp-server user mark r&d remote 192.168.1.19 v3 auth md5 greenpeace priv des56
einstien
Console(config)#
```

5.3.4 snmp-server view

本コマンドでは、MIb へのユーザアクセスを制御する SNMP ビューを追加します。SNMP ビューを削除するには、no 形式を使用してください。

構文

snmp-server view *view-name oid-tree* {included | excluded}

no snmp-server view *view-name*

view-name - SNMP ビューの名称です。(範囲: 1-32 文字)

oid-tree - MIB ツリー内のブランチのオブジェクト識別子です。OID 文字列の特定部分をマスクするためにワイルドカードを使用することができます。(例を参照してください。)

included - 含まれたビューを定義します。

excluded - 除外されたビューを定義します。

デフォルト設定

defaultview (MIB ツリー全体へのアクセスを含む)

コマンドモード

Global Configuration

コマンドの使用方法

- ビューは snmp-server group コマンドで使用され、MIB ツリーの指定された部分へのユーザアクセスを制限します。
- 定義済みビュー "defaultview"には、MIB ツリー全体へのアクセスが含まれます。

例

このビューには、MIB-2 が含まれます。

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

このビューには、MIB-2 インタフェーステーブル、ifDescr が含まれます。ワイルドカードは、次の表のすべてのインデックス値を選択するために使用されます。

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
Console(config)#
```

このビューには、MIB-2 インタフェーステーブルが含まれ、マスクがすべてのインデックス入力を選択します。

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
Console(config)#
```

5.3.5 show snmp engine-id

本コマンドでは、SNMP エンジン ID を表示します。

コマンドモード

Privileged Exec

例

以下の例では、デフォルトエンジン ID を示します。

```
Console#show snmp engine-id
Local SNMP EngineID: 8000002a8000000000e8666672
Local SNMP EngineBoots: 1

Remote SNMP Engine ID                          IP address
80000000030004e2b316c54321                     192.168.1.19
Console#
```

表 5-2 show snmp engine-id - 表示説明

フィールド	説明
Local SNMP engineID	エンジン ID を識別する文字列です。
Local SNMP engineBoots	snmp EngineID が最後に設定されてからエンジンが(再)初期化された回数です。
Remote SNMP engineID	リモートデバイスでエンジン ID を識別する文字列です。
IP address	対応するリモート SNMP エンジンを含むデバイスの IP アドレスです。

5.3.6 show snmp group

4 つのデフォルトグループが提供されます - SNMPv1 読み取り専用アクセスと読み取り/書き込みアクセス、および SNMPv2c 読み取り専用アクセスと読み取り/書き込みアクセスです。

コマンドモード

Privileged Exec

例

```
Console#show snmp group
Group Name     : r&d
Security Model : v3
Security Level : Authentication and privacy
Read View      : No readview specified
Write View     : No writeview specified
Notify View    : No notifyview specified
Storage Type   : Nonvolatile
Row Status     : Active

Group Name     : public
Security Model : v1
Read View      : defaultview
Write View     : No writeview specified
Notify View    : No notifyview specified
Storage Type   : Volatile
Row Status     : Active
```

```
Group Name     : public
Security Model : v2c
Read View      : defaultview
Write View     : No writeview specified
Notify View    : No notifyview specified
Storage Type   : Volatile
Row Status     : Active

Group Name     : private
Security Model : v1
Read View      : defaultview
Write View     : defaultview
Notify View    : No notifyview specified
Storage Type   : Volatile
Row Status     : Active

Group Name     : private
Security Model : v2c
Read View      : defaultview
Write View     : defaultview
Notify View    : No notifyview specified
Storage Type   : Volatile
Row Status     : Active
Console#
```

表 5-3 show snmp group - 表示説明

フィールド	説明
Group Name	SNMP グループの名称です。
Security Model	SNMP バージョンです。
Security Level	この関連セキュリティレベルでは、認証、認証なし、または認証とプライバシーで SNMPv3 を使用できます。
Read View	関連する読み取りビューです。
Write View	関連する書き込みビューです。
Notify View	関連付けられた通知ビューです。
Storage Type	このエントリの格納タイプです。
Row Status	このエントリの行ステータスです。

5.3.7 show snmp user

本コマンドでは、SNMP ユーザの情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show snmp user
Engine ID               : 800001030300e00c0000fd0000
User Name               : steve
Group Name              : rd
Security Model          : v1
Security Level          : Authentication and privacy
Authentication Protocol : None
Privacy Protocol        : None
Storage Type            : Nonvolatile
Row Status              : Active

SNMP remote user
Engine ID               : 0000937564846450000
User Name               : mark
Group Name              : public
Security Model          : v3
Security Level          : Anthentication and privacy
Authentication Protocol : MD5
Privacy Protocol        : DES56
Storage Type            : Nonvolatile
Row Status              : Active
Console#
```

表 5-4 show snmp user - 表示説明

フィールド	説明
Engine ID	エンジン ID を識別する文字列です。
User Name	SNMP エージェントに接続しているユーザ名です。
Group Name	SNMP グループの名称です。
Security Model	ユーザセキュリティモード: SNMP v1, v2c または v3.
Security Level	認証または暗号化が使用されているかについて示します。
Authentication Protocol	SNMPv3 で使用された認証プロトコルです。
Privacy Protocol	SNMPv3.で使用されているプライバシープロトコルです。
Storage Type	このエントリの格納タイプです。
Row Status	このエントリの行ステータスです。
SNMP remote user	リモートデバイスでの SNMP エンジンに関連するユーザです。

5.3.8 show snmp view

本コマンドでは、SNMP ビューの情報について示します。

コマンドモード

Privileged Exec

例

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name    : defaultview
Subtree OID  : 1
View Type    : included
Storage Type : volatile
Row Status   : active
Console#
```

表 5-5 show snmp view - 表示説明

フィールド	説明
View Name	SNMP ビューの名称です。
Subtree OID	SNMP ビューの名称です。
View Type	ビューが含まれているかいないかについて示しています。
Storage Type	このエントリの格納タイプです。
Row Status	このエントリの行ステータスです。

5.4 通知ログコマンド

5.4.1 nlm

本コマンドでは、指定した通知ログを有効または無効にします。

構文

[no] nlm *filter-name*

filter-name - 通知ログ名です。(範囲: 1 から 32 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- ◆ 通知ロギングはデフォルトで有効になっていますが、nlm コマンドによって snmp-server notify-filter コマンドで指定されたロギングプロファイルが有効になるまで、情報の記録を開始しません。
- ◆ このコマンドでロギングを無効にしても、通知ログに格納されているエントリは削除されません。

例

この例では、通知ログ A1 を有効にします。

```
Console(config)#nlm A1
Console(config)#
```

5.4.2 snmp-server notify-filter

本コマンドは、SNMP 通知ログを作成します。このログを削除するには、no 形式を使用してください。

構文

[no] snmp-server notify-filter *profile-name* remote *ip-address*

profile-name - 通知ログプロファイル名です。(範囲: 1 から 32 文字)

ip-address - リモートデバイスの IPv4 または IPv6 アドレスです。指定したターゲットホストは、snmp-server host コマンドを使用して既に設定されている必要があります。

Note: 通知ログはローカルで保存します。リモートデバイスには送信されません。このリモートホストパラメータは、SNMP 通知 MIB の必須フィールドを完了させる場合のみ必要となります。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- SNMP をサポートするシステムでは、再送信制限を超えている可能性のあるトラップやインフォームがあるかどうかに関わらず、通知情報の紛失に対する記録として記録する仕組みが必要となる場合が多くなります。通知ログ MIB(NLM、RFC 3014)は、他の MIB からの情報が記録されるインフラを提供します。
- NLM によって提供されるサービスが提供されると、個々の MIB は通知メッセージが失われる可能性を考慮して、イベントに関連する過渡情報を記録する責任を負うことが少なくなり、アプリケーションはログをポーリングして、 重要な通知が抜けていないかについて確認します。
- スイッチのリブート時に、通知ロギングが設定されておらず有効になっていない場合には、いくつかの SNMP トラップ(ウォームスタート等)は記録されません。
- この問題を回避するために、snmp-server notify-filter コマンドと nlm コマンドを使って通知ロギングを設定および有効にする必要があります。そしてこれらのコマンドは、スタートアップコンフィグレーションファイルに格納されています。スイッチリブート時に、SNMP トラップ(ウォームスタート等)に記録できるようになります。
- コマンド実行時に、通知ログが(RFC 3014 で定義されたデフォルトパラメータで)作成されます。通知ロギングはデフォルトで有効化されますが(nlm コマンドを参照)、このコマンドで指定されたロギングプロファイルが nlm コマンドで使用可能になるまで、情報の記録を開始しません。
- RFC 3014 で使用されたデフォルト設定をベースに、通知ログには最大 256 エントリを含むことができます。そして、エントリエージングタイムは 1440 分です。通知ログに記録された情報とエントリエージングタイムは、ネットワーク管理ステーションからの SNMP を使用してのみ、設定することができます。
- snmp-server host コマンドでトラップホストが作成されると、show snmp notify-filter コマンドの例に示すように、デフォルトの通知フィルタが作成されます。

例

下記の例では、リモートホストのエントリを最初に作成し、その次にスイッチに、指定通知ログのリモートホストとしてこのデバイスを記録するよう、指示します。

```
Console(config)#snmp-server host 10.1.19.23 admin
Console(config)#snmp-server notify-filter A1 remote 10.1.19.23
Console#
```

5.4.3 show nlm oper-status

本コマンドでは、設定した通知ログの動作ステータスを示します。

コマンドモード

Privileged Exec

例

```
Console#show nlm oper-status
Filter Name: A1
Oper-Status: Operational
Console#
```

5.4.4 show snmp notify-filter

本コマンドでは、設定した通知ログを表示します。

コマンドモード

Privileged Exec

例

以下の例では、設定した通知ログと関連ターゲットホストを表示します。

```
Console#show snmp notify-filter
Filter profile name            IP address
-----------------------------  ---------------
A1                             10.1.19.23
Console#
```

5.5 プライベートトラップコマンド

5.5.1 memory

本コマンドでは、メモリ使用率に設定された閾値に基づいて SNMP トラップを設定します。デフォルト設定を復元するには、no 形式を使用します。

構文

memory {rising *rising-threshold* | falling *falling-threshold*}

no memory {rising | falling}

rising-threshold - メモリ使用率アラームの上昇閾値は、パーセンテージで表されます。(範囲: 1 から 100)

falling-threshold - メモリ使用率アラームの下降閾値は、パーセンテージで表されます。(範囲: 1 から 100)

デフォルト設定

上昇閾値: 90%

下降閾値: 70%

コマンドモード

Global Configuration

コマンドの使用方法

一度上昇アラーム閾値を超えると、アラームが停止する前に使用率は下降閾値を下回る必要があります。そして、他のアラームの引き金となる前に上昇閾値を再度超えなければなりません。

例

```
Console(config)#memory rising 80
Console(config)#memory falling 60
Console#
```

関連コマンド

show memory

5.5.2 process cpu

本コマンドでは、CPU 使用率の設定閾値をベースに SNMP トラップを設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

process cpu {rising *rising-threshold* | falling *falling-threshold*}

no process cpu {rising | falling}

rising-threshold - CPU アラームの上昇閾値は、パーセンテージで表されます。(範囲: 1 から 100)

falling-threshold - CPU アラームの下降閾値は、パーセンテージで表されます。(範囲: 1 から 100)

デフォルト設定

上昇閾値: 90%

下降閾値: 70%

コマンドモード

Global Configuration

コマンドの使用方法

一度上昇アラーム閾値を超えると、アラームが停止する前に使用率は下降閾値を下回る必要があります。そして、他のアラームの引き金となる前に上昇閾値を再度超えなければなりません。

例

```
Console(config)#process cpu rising 80
Console(config)#process cpu falling 60
Console#
```

関連コマンド

show process cpu

5.5.3 process cpu guard

本コマンドでは、CPU 使用率の上限と下限の基準値を、使用された CPU 時間のパーセンテージと、CPU の上限と下限の閾値を毎秒処理されるパケット数で設定します。すべてのデフォルト設定を復元するには、このコマンドの no 形式をパラメータ無しで使用するか、またはその項目のデフォルト設定を復元する特定のパラメータを使用します。

構文

process cpu guard [high-watermark *high-watermark* |

low-watermark *low-watermark* | max-threshold *max-threshold* |

min-threshold *min-threshold* | trap]

high-watermark - CPU 使用時間のパーセンテージが高基準値より高い場合には、スイッチが CPU へのパケットフローを停止します(バッファにすでに入っているパケットに追いつくことができます)。使用時間が低基準値を下回るまで、スイッチは停止します。(範囲: 40 から 100％)

low-watermark - パケットフローが、高基準値を超えた後に停止した場合、使用率が低基準値を下回った後に、通常フローが復元されます。(範囲: 40 から 100％)

max-threshold - CPU によって処理されている 1 秒あたりのパケット数が最大閾値を超えている場合、スイッチは処理中のパケット数が最小閾値を下回るまで、CPU へのパケットフローを停止します(バッファ内のパケットに追いつくことができます)。(範囲: 50 から 500pps)

min-threshold - 最大閾値を超えてパケットフローが停止した場合、使用率が最小閾値を下回った後に通常フローが復元されます。(範囲: 50 から 500pps)

trap - トラップが有効になっている場合、CPU 使用率が CPU 使用率のパーセンテージで最高水準点を超えた場合、または CPU によって処理されているパケット数の最大閾値を超えた場合、スイッチはアラームメッセージを送信します。

デフォルト設定

ガードステータス: 無効

高水準値: 90%

低水準値: : 70%

最大閾値: 1 秒あたり 500 パケット

最小閾値: 1 秒あたり 50 パケット

トラップステータス: 無効

コマンドモード

Global Configuration

コマンドの使用方法

- 一度高水準値を超えると、アラームが停止する前に使用率は低水準値を下回る必要があります。そして、他のアラームの引き金となる前に高水準値を再度超えなければなりません。
- 一度最大閾値を超えると、アラームが停止する前に使用率は最低閾値を下回る必要があります。そして、他のアラームの引き金となる前に最大閾値を再度超えなければなりません。

例

```
Console(config)#process cpu guard high-watermark 80
Console(config)#process cpu guard low-watermark 60
Console(config)#
```

関連コマンド

show process cpu guard

6 RMON コマンド

リモート監視により、リモートデバイスは情報の収集や独立した基準で特定のイベントに応答することができます。このスイッチは RMON 対応デバイスであり、幅広いタスクを独立して実行できるため、ネットワーク管理トラフィックを大幅に削減することができます。診断を継続して実行し、ネットワークパフォーマンスに関する情報を記録できます。イベントがトリガされると、自動的にネットワーク管理者に障害を通知し、イベントに関する履歴情報を提供することができます。管理エージェントに接続できない場合は指定されたタスクの実行を継続し、次に連絡を受けたときに管理ステーションにデータを戻します。

このスイッチは、Statistics、History、Event、および Alarm グループで構成されるミニ RMON をサポートしています。　RMON が有効になると、システムは物理インタフェースに関する情報を徐々に構築し、この情報を関連する RMON データベースグループに格納します。管理エージェントは、SNMP プロトコルを使用してスイッチと定期的に通信します。ただし、スイッチが重大なイベントに遭遇した場合、スイッチは管理エージェントに自動的にトラップメッセージを送信できます。トラップメッセージが設定されていれば、イベントに応答することができます。

表 6-1　RMON コマンド

コマンド	機能	モード
rmon alarm	監視対象変数の閾値範囲を設定します。	GC
rmon event	アラームの応答イベントを作成します。	GC
rmon collection history	統計を定期的にサンプリングします。	IC
rmon collection rmon1	統計の収集を有効にします。	IC
show rmon alarms	すべての設定済みアラームの設定内容を表示します。	PE
show rmon events	すべての設定済みイベントの設定内容を表示します。	PE
show rmon history	各エントリのサンプリングパラメータを表示します。	PE
show rmon statistics	収集した統計を表示します。	PE

6.1 コマンド説明

6.1.1 rmon alarm

本コマンドでは、監視対象変数の閾値を設定します。アラームを削除するには、no 形式を使用してください。

構文

rmon alarm *index variable interval* {absolute | delta}

rising-threshold *threshold* [*event-index*] falling-threshold *threshold* [*event-index*] [owner *name*]

no rmon alarm *index*

index - このエントリのインデックスです。(範囲: 1 から 65535)

variable - サンプリングされる MIB 変数のオブジェクト識別子です。etherStatsEntry.n.n の変数のみがサンプリングされます。 etherStatsEntry.n は MIB 変数を一意に定義し、etherStatsEntry.n.n は MIB 変数と etherStatsIndex を定義します。 たとえば、1.3.6.1.2.1.16.1.1.1.6.1 は etherStatsBroadcastPkts と etherStatsIndex の 1 を示します。

interval - ポーリングの間隔です。(範囲: 1 から 65535 秒)

absolute - 変数は、サンプリング期間の終わりに閾値と直接比較されます。

delta - 最後のサンプルが現在の値から減算され、その差が閾値と比較されます。

threshold - サンプリングされた変数のアラーム閾値です。

(範囲: 0 から 2147483647):

event-index - アラームがトリガされた際に使用するイベントのインデックスです。イベント制御テーブルに対応するエントリが無い場合には、イベントは生成されません。(範囲: 1 から 65535)

name - このエントリを作成した人の名前です。(範囲: 1 から 32 文字)

デフォルト設定

1.3.6.1.4.1.21839.10.1.43.104.1 - 1.3.6.1.4.1.21839.10.1.43.102.26/1.3.6.1.4.1.21839.10.1.43.101.52

デルタサンプルを 30 秒ごとに取得します。

上昇閾値は 892800 で、イベント 0 に割り当てられています。

下降閾値は 446400 で、イベント 0 に割り当てられています。

コマンドモード

Global Configuration

コマンドの使用方法

- イベントが既にインデックス用に定義されている場合、コマンドで変更する前にエントリを削除する必要があります。
- 現在の値が上昇閾値以上で、最後のサンプル値がこの閾値より小さい場合は、アラームが生成されます。上昇イベントが生成された後、サンプリングされた値が上昇閾値を下回って下降閾値に達し、再び上昇閾値に戻るまで、別のイベントは生成されません。
- 現在の値が下限閾値以下で、最後のサンプル値がこの閾値より大きい場合、アラームが生成されます。 下降イベントが生成された後、サンプリングされた値が下降閾値を上回って上昇閾値に達し、

再び下限閾値に戻るまで、別のイベントは生成されません。

例

```
Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta
rising-threshold 100 1 falling-threshold 30 1 owner mike
Console(config)#
```

6.1.2 rmon event

本コマンドでは、アラームに対する応答イベントを作成します。イベントを削除するには、no 形式を使用してください。

構文

rmon event *index* [log] | [trap *community*] | [description *string*] | [owner *name*]

no rmon event *index*

index - このエントリのインデックスです。(範囲: 1 から 65535)

log - イベントがトリガされたときに RMON ログエントリを生成します。イベントログの現在の設定内容にもとづいて処理されます（「4.6　イベントロギング」を参照してください)。

trap - すべての設定済みトラップマネージャにトラップメッセージを送信します(snmp-server host コマンドを参照)。

community - SNMP v1 および v2c ホストにトラップ操作で送信されたパスワードのようなコミュニティストリングです。この文字列は、rmon event コマンドを単独で使用して設定することもできますが、rmon event コマンドを使用する前に snmp-server community コマンドを使用して文字列を定義することを、推奨します。(範囲: 1 から 16 文字)

string - このイベントを説明するコメントです。(範囲: 1 から 127 文字)

name - このエントリを作成した人の名前です。

(範囲: 1 から 32 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- イベントが既にインデックス用に定義されている場合、コマンドで変更する前にエントリを削除する必要があります。
- 指定されたイベントによってアラームがこのイベントを契機にするときに、実行するアクションが決定します。　アラームへの応答には、アラームの記録やトラップマネージャへのメッセージの送信が含まれます。

例

```
Console(config)#rmon event 2 log description urgent owner mike
Console(config)#
```

6.1.3 rmon collection history

本コマンドでは、物理インタフェースの統計情報を定期的にサンプリングします。定期サンプリングを無効にするには、no 形式を使用してください。

構文

rmon collection history controlEntry *index*

[buckets *number* [interval *seconds*]] |

[interval *seconds*] |

[owner *name* [buckets *number* [interval *seconds*]]

no rmon collection history controlEntry *index*

index - このエントリのインデックスです。(範囲: 1 から 65535)

number - このエントリに要求されたバケットの数です。(範囲: 1 から 65536)

seconds - ポーリング間隔(範囲: 1 から 3600 秒)

name - このエントリを作成した人の名前です。

(範囲: 1 から 32 文字)

デフォルト設定

1.3.6.1.4.1.21839.10.1.43.104.1 - 1.3.6.1.4.1.21839.10.1.43.104.102.26/

1.3.6.1.4.1.21839.10.1.43.101.52

バケット: 8

間隔: 偶数番号のエントリの場合は、30 秒、

奇数番号のエントリの場合は、1800 秒

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- デフォルトでは、各インデックス番号はスイッチ上のポートと同じですが、現在使用されていない番号に変更することができます。
- インタフェースで定期サンプリングがすでに有効になっている場合には、このコマンドで変更する前にエントリを削除する必要があります。
- 各サンプルに対して収集した情報には、以下が含まれます:
  入力オクテット、パケット、ブロードキャストパケット、マルチキャストパケット、アンダーサイズパケット、オーバーサイズパケット、フラグメント、ジャバー、CRC アラインメントエラー、コリジョン、ドロップイベント、およびネットワーク使用率。

◆ スイッチは各ポートに 2 つの controlEntry インデックスエントリを予約します。このコマンドでデフォルトのインデックスエントリを別のポートに再割り当てすると、show running-config コマンドは、このインデックスが通常割り当てられているポートで使用できないことを示すメッセージを表示します。たとえば以下に表示しているように、制御エントリ 15 がポート 5 に割り当てられている場合、show running-config コマンドでは、ポート 8 のエントリは入手できないことを示します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#rmon collection history controlEntry 15
Console(config-if)#end
Console#show running-config
!
interface ethernet 1/5
 rmon collection history controlEntry 15 buckets 50 interval 1800
...
interface ethernet 1/8
 no rmon collection history controlEntry 15
```

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection history controlentry 21 owner mike buckets 24 interval 60
Console(config-if)#
```

6.1.4 rmon collection rmon1

本コマンドでは、物理インタフェースにおける統計の収集を有効にします。統計の収集を無効にするには、no 形式を使用してください。

構文

rmon collection rmon1 controlEntry *index* [owner *name*]

no rmon collection rmon1 controlEntry *index*

index - このエントリのインデックスです。(範囲: 1 から 65535)

name - このエントリを作成した人の名前です。

(範囲: 1 から 32 文字)

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

◆ デフォルトでは、各インデックス番号はスイッチ上のポートと同じですが、現在使用されていない番

号に変更することができます。

- インタフェースで統計の収集がすでに有効になっている場合には、このコマンドで変更する前にエントリを削除する必要があります。
- 各サンプルに対して収集した情報には、以下が含まれます:各サンプルに対して収集した情報には、以下が含まれます:
  入力オクテット、パケット、ブロードキャストパケット、マルチキャストパケット、アンダーサイズパケット、オーバーサイズパケット、フラグメント、ジャバー、CRC アライメントエラー、コリジョン、ドロップイベント、および指定された長さのパケット。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection rmon1 controlEntry 1 owner mike
Console(config-if)#
```

6.1.5 show rmon alarms

本コマンドでは、すべての設定済みアラームの設定内容を表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon alarms
Alarm 1 is valid, owned by
 Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds
 Taking delta samples, last value was 0
 Rising threshold is 892800, assigned to event 0
 Falling threshold is 446400, assigned to event 0
.
.
```

6.1.6 show rmon events

本コマンドでは、すべての設定済みイベントの設定内容を表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon events
Event 2 is valid, owned by mike
```

```
 Description is urgent
 Event firing causes log and trap to community , last fired  00:00:00
Console#
```

6.1.7 show rmon history

本コマンドでは、履歴グループ内の各エントリに対して設定したサンプリングパラメータについて表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon history
Entry 1 is valid, and owned by
 Monitors 1.3.6.1.2.1.2.2.1.1.1 every 1800 seconds
 Requested # of time intervals, ie buckets, is 8
 Granted # of time intervals, ie buckets, is 8
  Sample # 1 began measuring at 00:00:01
  Received 77671 octets, 1077 packets,
  61 broadcast and 978 multicast packets,
  0 undersized and 0 oversized packets,
  0 fragments and 0 jabbers packets,
  0 CRC alignment errors and 0 collisions.
  # of dropped packet events is 0
  Network utilization is estimated at 0
.
.
.
```

6.1.8 show rmon statistics

本コマンドでは、統計グループの中のすべての設定済みエントリに対して収集した情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon statistics
Interface 1 is valid, and owned by
 Monitors 1.3.6.1.2.1.2.2.1.1.1 which has
 Received 164289 octets, 2372 packets,
 120 broadcast and 2211 multicast packets,
```

```
  0 undersized and 0 oversized packets,
  0 fragments and 0 jabbers,
  0 CRC alignment errors and 0 collisions.
  # of dropped packet events (due to lack of resources): 0
  # of packets received of length (in octets):
   64: 2245, 65-127: 87, 128-255: 31,
   256-511: 5, 512-1023: 2, 1024-1518: 2
.
.
.
```

7 sFlow コマンド

フローサンプリング(sFlow)をリモート sFlow コレクタとともに使用すると、ネットワークに存在するトラフィックのタイプとレベルの正確で詳細なリアルタイムの概要を提供することができます。sFlow Agent は、スイッチが受信するすべてのデータから n 個のパケットのうち 1 つをサンプリングし、サンプルを sFlow データグラムとして再カプセル化して、sFlow コレクタに送信します。　このサンプリングは、すべてのトラフィックが表示される内部ハードウェアレベルで行われますが、従来のプローブでは、監視されたインタフェースでサンプリングされたトラフィックの一部分しか表示されません。さらに、ローカル解析が行われないため、sFlow エージェントが課すプロセッサとメモリの負荷は最小限に抑えられます。

Note: 本章では、「コレクタ」、「受信者」、および「所有者」という用語はすべて、スイッチの sFlow エージェントによって生成された sFlow データグラムを受信できるリモートサーバを指します。

表 7-1　sFlow コマンド

コマンド	機能	モード
sflow owner	サンプルを送信するためにスイッチが使用する sFlow コレクタを作成します。	PE
sflow polling instance	時間にもとづいてサンプルを定期的に取得する sFlow ポーリングデータソースを設定します。	PE
sflow sampling instance	パケットカウントにもとづいて定期的にサンプリングする sFlow サンプリングデータソースを設定します。	PE
show sflow	sFlow 処理のグローバルおよびインタフェース設定を表示します。	PE

7.1 コマンド説明

7.1.1 sflow owner

本コマンドでは、スイッチの sFlow コレクタを作成します。sFlow 受信者を削除するには、no 形式を使用してください。

構文

sflow owner *owner-name* timeout *timeout-value*

destination {*ipv4-address* | *ipv6-address*}] [port *destination-udp-port*] [max-datagram-size *max-datagram-size*] [version {v4 | v5}]

no sflow owner *owner-name*

owner-name - コレクタの名前です。(範囲: 1 から 30 の英数字)

timeout-value - 受信者にサンプルを送信するために sFlow インタフェースが使用できる時間の長さ。その後、所有者と関連付けられたポーリングおよびサンプリングデータソースインスタンスが設定から削除されます。(範囲: 30 から 10000000 秒)

ipv4-address - sFlow コレクタの IPv4 アドレスです。有効な IPv4 アドレスは、ピリオドで区切られた 0 から 255 の 4 つの 10 進数で構成されます。

ipv6-address - sFlow コレクタの IPv6 アドレスです。ネットワークプレフィックスとホストアドレスビットを含むフル IPv6 アドレスです。IPv6 アドレスは、8 つのコロンで区切られた 16 ビットの 16 進数で構成されています。 1 つの二重コロンを使用して、未定義フィールドを埋めるために必要なゼロの適切な数を示すことができます。

destination-udp-port - コレクタが sFlow ストリームをリスニングする UDP ポートです。(範囲: 1 から 65535)

max-datagram-size - sFlow データグラムペイロードの最大サイズです。(範囲: 200 から 1500 バイト)

version {v4 | v5} - 受信者に v4 または v5 sFlow データグラムを送信します。

デフォルト設定

所有者は設定されていません。

UDP ポート: 6343

バージョン: v4

最大データグラムサイズ: 1400 バイト

コマンドモード

Privileged Exec

コマンドの使用方法

- sflow owner コマンドを使用して、sFlow コレクタの所有者インスタンスを作成します。ソケットポート、最大データグラムサイズ、およびデータグラムのバージョンが指定されていない場合には、デフォルト値が使用されます。
- 一度、所有者が作成されると、sflow owner コマンドを再度使用して所有者のポート番号を変更することができます。ポートが変更されている場合には、所有者のパラメータ値はすべて保持されます。
- コレクタを削除するには、no sflow owner コマンドを使用してください。

◆ sflow owner コマンド発行時に、関連タイムアウト値が直ちにカウントダウンを開始します。タイムアウト値がゼロ秒に到達すると、sFlow 所有者と関連サンプリングソースは設定から削除されます。

例

以下の例では、スイッチで作成されている sflow コレクタを表示しています。

```
Console#sflow owner stat_server1 timeout 100 destination 192.168.220.225 port 22500 max-
datagram-size 512 version v5
Console#
```

7.1.2 sflow polling instance

本コマンドでは、指定した時間間隔にもとづいて定期的にポーリングする指定されたインタフェースの sFlow ポーリングデータソースを有効にします。スイッチの sFlow 設定からポーリングデータソースインスタンスを削除するには、no 形式を使用してください。

構文

sflow polling {interface *interface*} instance *instance-id* receiver *owner-name* polling-interval *seconds*

no sflow polling {interface *interface*} instance *instance-id*

interface - 指定された間隔でサンプルが採取され、コレクタに送られるソースです。

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

instance-id - サンプリングソースを識別するインスタンス ID です。(範囲: 1):

owner-name - サンプルが送信される関連受信者です。(範囲: 1 から 30 の英数字)

polling-interval - sFlow プロセスがサンプルデータグラムにカウンタ値を追加する時間間隔です。(範囲 1-10000000 秒)

デフォルト設定

sFlow ポーリングインスタンスは設定されていません。

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドは、ポーリングデータソースを有効にし、カウンタ値がサンプルデータグラムに追加される間隔を設定します。

7.1.3 sflow sampling instance

本コマンドでは、処理したパケット数にもとづいて定期的に採取する指定されたインタフェースの sFlow データソースインスタンスを有効にします。スイッチの sFlow 設定からサンプリングデータソースインスタンスを削除するには、no 形式を使用してください。

構文

sflow sampling {interface *interface*} instance *instance-id* receiver *owner-name* sampling-rate *sample-rate*

[max-header-size *max-header-size*]

no sflow sample {interface *interface*} instance *instance-id*

interface - サンプルを採取してコレクタに送信するソースです。

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

instance-id - サンプリングソースを識別するインスタンス ID です。(範囲: 1):

owner-name - サンプルが送信される関連受信者です。(範囲: 1 から 30 の英数字)

sample-rate - パケットサンプリングレート、または 1 つのサンプルが採取されるパケットの数です。(範囲: 2-65535 パケット)

max-header-size - sFlow データグラムヘッダの最大サイズです。(範囲: 64 から 256 バイト)

デフォルト設定

sFlow サンプリングインスタンスは設定されていません。

最大ヘッダサイズ: 128 バイト

コマンドモード

Privileged Exec

例

以下の例では、イーサネットインタフェース 1/1 上のサンプリングデータソース、関連する受信者「owner1」、および 100 のうちのサンプリングレートを有効にします。最大ヘッダサイズも 200 バイトに設定されています。

```
Console# sflow sampling interface ethernet 1/1 instance 1 receiver owner1 sampling-rate 100
max-header-size 200
Console#
```

以下のコマンドで、イーサネットインタフェース 1/1 からサンプリングデータを削除します。

```
Console# no sflow sampling interface ethernet 1/1 instance 1
Console#
```

7.1.4 show sflow

本コマンドは、sFlow プロセスのグローバルおよびインタフェース設定を表示します。

構文

show sflow [owner *owner-name* | interface *interface*]

owner-name - サンプルが送信される関連受信者です。(範囲: 1 から 30 の英数字)

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

```
Console#show sflow interface ethernet 1/2

  Receiver Owner Name   : stat1
  Receiver Timeout      : 99633 sec
  Receiver Destination  : 192.168.32.32
  Receiver Socket Port  : 6343
  Maximum Datagram Size : 1400 バイト
  Datagram Version      : 4

  Data Source           : Eth 1/2
  Sampling Instance ID  : 1
  Sampling Rate         : 512
  Maximum Header Size   : 128 バイト

Console#
```

8 ログインセキュリティ

ローカルまたはリモート認証方式を使用して管理アクセス用にシステムにログインするユーザを認証するように、このスイッチを設定できます。

表 8-1 認証コマンド

コマンドグループ	機能
ユーザアカウントおよび特権レベル	管理アクセスの基本ユーザ名とパスワードを設定し、指定されたコマンドグループまたは個々のコマンドに特権レベルを割り当てます。
認証シーケンス	ログオン認証方法と優先順位を定義します。
RADIUS Client	RADIUS サーバを介した認証を設定します。
TACACS+ Client	TACACS+サーバを介した認証を設定します。
AAA	ネットワークアクセスの認証、権限およびアカウンティングを設定します。
Web サーバ	ウェブブラウザを介した管理アクセスを有効にします。
Telnet サーバ	Telnet を介した管理アクセスを有効にします。
SSH	Telnet の安全な置換を提供します。
IP フィルタの管理	管理アクセスが許可されている IP アドレスを設定します。
EAPOL の透過	EAPOL フレームの透過を有効にします。

8.1 ユーザアカウントおよび特権レベル

本章では、管理アクセスおよびコマンド特権レベルの割り当てに必要な基本コマンドを示します。このスイッチには、コンソールまたは Telnet 接続、リモート認証サーバを介したユーザ認証、および特定のポートのホストアクセス認証によるパスワードチェック等のオプションも含まれています。

表 8-2 ユーザアクセスコマンド

コマンド	機能	モード
enable password	Privileged Exec レベルへのアクセスを制御するためのパスワードを設定します。	GC
username	ログインで、ユーザ名ベース認証を確立します。	GC
privilege	指定コマンドまたは個別コマンドに特権レベルを割り当てます。	GC
show privilege	現在のユーザの特権レベル、または privilege コマンドで変更されたコマンドの特権レベルを表示します。	PE

8.1.1 enable password

最初にシステムにログオン後、Privileged Exec パスワードを設定する必要があります。パスワードは必ず安全な場所に保管してください。このコマンドは Normal Exec レベルから Privileged Exec レベルへのアクセスを制御します。デフォルトパスワードにリセットするには、no 形式を使用してください。

構文

enable password [level *level*] {0 | 7} *password*

no enable password [level *level*]

level *level* - コマンドアクセス特権を設定します。(範囲: 0 から 15)

レベル 0、8 および 15 は、ユーザ(ゲスト)、マネージャ(ネットワークメンテナンス)、および管理者(上位アクセス)に割り当てられます。その他のレベルは、設定された特殊アクセスプロファイルに使用することができます。

レベル 0 から 7 は、コマンドプロンプト“Console>”の下で、Normal Exec モードで同じデフォルトアクセス権を提供します。

レベル 8 から 14 は、Normal Exec モードでの追加コマンドと、Privileged Exec モードでのコマンドのサブセットを含むコマンドプロンプト“Console#”の下で、同じデフォルトアクセス権を提供します。

レベル 15 は、すべてのコマンドへのフルアクセスを提供します

どのコマンドにも関連する特権コマンドは、privilege コマンドを使用して変更することができます。

{0 | 7} - 0 は、通常パスワード、7 は暗号化パスワードの意味です。

password - 特権レベルのパスワードです。(最長: 16 文字の通常テキストまたは暗号化(32 文字固定)、大文字と小文字を区別します)

デフォルト設定

デフォルトレベルは 15 です。

デフォルトパスワードは”super”です。

コマンドモード

Global Configuration

コマンドの使用方法

- 無効なパスワードを設定することはできません。コマンドモードを enable コマンドで Normal Exec から Privileged Exec に変更するためのパスワードを入力する必要があります。
- 暗号化されたパスワードは、システム起動時に設定ファイルを読み込む際に従来のパスワード設定(通常テキストまたは暗号化)との互換性のために必要です。暗号化されたパスワードを手動で設定する必要はありません。

例

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

関連コマンド

enable

authentication enable

8.1.2 username

本コマンドは、指定ユーザの追加やログイン時の認証要求、ユーザパスワードの指定または変更、パスワードが必要でないことの指定、あるいはユーザのアクセスレベルの指定や変更をします。ユーザ名を削除するには、no 形式を使用してください。

構文

username *name* {access-level *level* | nopassword | password {0 | 7} *password*}

no username *name*

name - ユーザ名です。(最長: 32 文字、大文字小文字の区別、最小ユーザ数: 16):

このデバイスには、特権レベル 0(Normal Exec)が割り当てられ、制限された数のコマンドにアクセスできる guest と、特権レベル 15 が割り当てられ、すべてのコマンドに完全にアクセスできる admin の 2 つの事前定義済みユーザがあります。

access-level *level* - 指定したコマンドアクセス権です。(範囲: 0 から 15)

レベル 0、8 および 15 は、ユーザ(ゲスト)、マネージャ(ネットワークメンテナンス)、および管理者(上位アクセス)に割り当てられます。その他のレベルは、設定された特殊アクセスプロファイルに使用することができます。

レベル 0 から 7 は、コマンドプロンプト“Console>”の下で、Normal Exec モードで同じデフォルトアクセス権を提供します。

レベル 8 から 14 は、Normal Exec モードでの追加コマンドと、Privileged Exec モードでのコマンドのサブセットを含むコマンドプロンプト“Console#”の下で、同じデフォルトアクセス権を提供します。

レベル 15 は、すべてのコマンドへのフルアクセスを提供します

どのコマンドにも関連する特権コマンドは、privilege コマンドを使用して変更することができます。

すべての特権レベルは、より低い特権レベルに割り当てられたすべてのコマンドにアクセスできます。たとえば、特権レベル 8 は、特権レベル 7 から 0 に割り当てられたすべてのコマンドにアクセスできます。また、privilege コマンドを使用してレベル 7 から 0 に割り当てられた他のコマンドにもアクセスすることができます。

nopassword - ユーザの認証パスワードを設定しません。

{0 | 7} - 0 は、通常パスワード、7 は暗号化パスワードの意味です。

password *password* - ユーザの認証パスワードです。(最長: 16 文字の通常テキストまたは暗号化(32 文字固定)、大文字と小文字を区別します)

デフォルト設定

デフォルトアクセスレベルは 0 です(Normal Exec)。

工場出荷時のデフォルトユーザ名とパスワードは、以下の通りです:

表 8-3 デフォルトログイン設定

ユーザ名	アクセスレベル	パスワード
guest	0	guest
admin	15	admin

コマンドモード

Global Configuration

コマンドの使用方法

暗号化されたパスワードは、システム起動時に設定ファイルを読み込む際に従来のパスワード設定(通常テキストまたは暗号化)との互換性のために必要です。暗号化されたパスワードを手動で設定する必要はありません。

例

以下の例では、ユーザのアクセスレベルとパスワードの設定方法について表示しています。

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

8.1.3 privilege

本コマンドでは、指定したコマンドグループまたは個別コマンドに特権レベルを割り当てます。デフォルト設定を復元するには、no 形式を使用してください。

構文

privilege *mode* [all] level *level command*

no privilege *mode* [all] *command*

mode - 指定 *command* を含む設定モードです。

（「2.2.8　コマンドモードについて」および「2.2.10　Configuration コマンド」を参照してください。）

all - 指定 *command* の下のすべてのサブコマンドの特権レベルを変更します。

level *level* - 指定 *command.*の特権レベルを指定します。username コマンドの下のアクセスレベルパラメータについて説明したデフォルト設定を参照してください。(範囲: 0 から 15)

command - 指定 *mode* に含まれるすべてのコマンドを指定します。

デフォルト設定

特権レベル 0 は、スイッチの現在のステータスだけでなくいくつかのデータベースクリアおよびリセット機能を表示する限られた数のコマンドへのアクセスを提供します。レベル 8 では、さまざまな認証およびセキュリティ機能を制御するものを除き、すべての表示ステータスおよび設定コマンドにアクセスすることができます。レベル 15 は、すべてのコマンドへのフルアクセスを提供します

コマンドモード

Global Configuration

例

以下の例では、ping コマンドに対し特権レベルを Privileged Exec に設定します。

```
Console(config)#privilege exec level 15 ping
Console(config)#
```

8.1.4 show privilege

本コマンドでは、現在のユーザの特権レベル、または privilege コマンドで変更したコマンドの特権レベルを示します。

構文

show privilege [command]

command - privilege コマンドで変更した、すべてのコマンドの特権レベルを表示します。

コマンドモード

Privileged Exec

例

以下の例では、privilege コマンドで変更したすべてのコマンドの特権レベルを示します。

```
Console#show privilege command
privilege line all level 0 accounting
privilege exec level 15 ping
Console(config)#
```

8.2 認証シーケンス

3 つの認証方法を指定して、管理アクセス用にシステムにログインしているユーザを認証できます。本章のコマンドは、認証方法とシーケンスを定義するために使用することができます。

表 8-4 認証シーケンスコマンド

コマンド	機能	モード
authentication enable	コマンドモード変更のための認証方法と優先順位を定義します。	GC
authentication login	ログオン認証方法と優先順位を定義します。	GC

8.2.1 authentication enable

本コマンドでは、enable コマンドで Exec コマンドモードから Privileged Exec コマンドモードへ変更する際に使用する認証方法と優先順位を定義します。デフォルトの状態に復元するには、no 形式を使用します。

構文

authentication enable {[local] [radius] [tacacs]}

no authentication enable

local - ローカルパスワードのみを使用します。

radius - RADIUS サーバパスワードのみ使用します。

tacacs - TACACS サーバパスワード使用します。

デフォルト設定

ローカル

コマンドモード

Global Configuration

コマンドの使用方法

- RADIUS は UDP を使用し、TACACS +は TCP を使用します。UDP はベストエフォート型の配信のみを提供し、TCP はコネクション型のトランスポートを提供します。また、RADIUS はクライアントからサーバへのアクセス要求パケットのパスワードだけを暗号化し、TACACS +はパケットの本体全体を暗号化します。
- RADIUS および TACACS +ログオン認証では、各ユーザ名とパスワードのペアに対して特定の特権レベルが割り当てられます。ユーザ名、パスワード、および特権レベルは、認証サーバで設定する必要があります。
- 1 つのコマンドで 3 つの認証方法を指定して、認証順序を指定できます。たとえば、“authentication enable radius tacacs local”と入力すると、RADIUS サーバのユーザ名とパスワードが最初に確認されます。RADIUS サーバが使用できない場合、TACACS +サーバで認証が実行されます。TACACS +サーバが使用できない場合には、ローカルユーザ名とパスワードがチェックされます。

例

```
Console(config)#authentication enable radius
```

```
Console(config)#
```

関連コマンド

enable password - コマンドモード変更のためにパスワードが設定されます

8.2.2 authentication login

本コマンドでは、ログイン認証方式と優先順位を定義します。デフォルトを復元するには、no 形式を使用してください。デフォルトの状態に復元するには、no 形式を使用します。

構文

authentication login {[local] [radius] [tacacs]}

no authentication login

local - ローカルパスワードを使用します。

radius - RADIUS サーバパスワード使用します。

tacacs - TACACS サーバパスワード使用します。

デフォルト設定

ローカル

コマンドモード

Global Configuration

コマンドの使用方法

- RADIUS は UDP を使用し、TACACS +は TCP を使用します。UDP はベストエフォート型の配信のみを提供し、TCP はコネクション型のトランスポートを提供します。また、RADIUS はクライアントからサーバへのアクセス要求パケットのパスワードだけを暗号化し、TACACS +はパケットの本体全体を暗号化します。
- RADIUS および TACACS +ログオン認証では、各ユーザ名とパスワードのペアに対して特定の特権レベルが割り当てられます。ユーザ名、パスワード、および特権レベルは、認証サーバで設定する必要があります。
- 1 つのコマンドで 3 つの認証方法を指定して、認証順序を指定できます。たとえば、“authentication login radius tacacs local”と入力すると、RADIUS サーバのユーザ名とパスワードが最初に確認されます。RADIUS サーバが使用できない場合、TACACS +サーバで認証が実行されます。TACACS +サーバが使用できない場合には、ローカルユーザ名とパスワードがチェックされます。

例

```
Console(config)#authentication login radius
Console(config)#
```

関連コマンド

username - ローカルユーザ名とパスワードの設定用です

8.3 RADIUS Client

リモート認証ダイヤルインユーザサービス(RADIUS)は、ネットワーク上の RADIUS 対応デバイスへのアクセスを制御するために、中央サーバ上で動作するソフトウェアを使用するログオン認証プロトコルです。認証サーバには、スイッチへの管理アクセスを必要とする各ユーザまたはグループに関連する特権レベルを持つ複数のユーザ名/パスワードペアのデータベースが含まれています。

表 8-5 RADIUS クライアントコマンド

コマンド	機能	モード
radius-server acct-port	RADIUS サーバネットワークポートを設定します。	GC
radius-server auth-port	RADIUS サーバネットワークポートを設定します。	GC
radius-server host	RADIUS サーバを指定します。	GC
radius-server key	RADIUS 暗号化鍵を設定します。	GC
radius-server encrypted-key	RADIUS 暗号化鍵を設定します。	GC
radius-server retransmit	リトライ回数を設定します。	GC
radius-server timeout	認証要求を送信する間隔を設定します。	GC
show radius-server	現在の RADIUS の設定内容を表示します。	PE

8.3.1 radius-server acct-port

本コマンドでは、アカウンティングメッセージの RADIUS ネットワークポートを設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

radius-server acct-port *port-number*

no radius-server acct-port

port-number - アカウンティングメッセージに使用される RADIUS サーバ UDP ポートです。(範囲: 1 から 65535)

デフォルト設定

1813

コマンドモード

Global Configuration

例

```
Console(config)#radius-server acct-port 181
Console(config)#
```

8.3.2 radius-server auth-port

本コマンドでは、RADIUS サーバネットワークポートを設定します。デフォルトの状態に復元するには、

no 形式を使用します。

構文

radius-server auth-port *port-number*

no radius-server auth-port

port-number - 認証メッセージに使用される RADIUS サーバ UDP ポートです。(範囲: 1 から 65535)

デフォルト設定

1812

コマンドモード

Global Configuration

例

```
Console(config)#radius-server auth-port 181
Console(config)#
```

8.3.3 radius-server host

本コマンドでは、プライマリ RADIUS サーバとバックアップ RADIUS サーバ、および各サーバに適用される認証とアカウンティングのパラメータを指定します。指定サーバを削除またはデフォルト値を復元するには、no 形式を使用してください。

構文

[no] radius-server *index* host *host-ip-address* [acct-port *acct-port*] [auth-port *auth-port*] [key *key*] [encrypted-key *key*] [retransmit *retransmit*] [timeout *timeout*]

index - 最大 3 サーバを指定することができます。これらのサーバはサーバが応答するか、再送信期間が終了するまで、順番に照会されます。

host-ip-address - サーバの IP アドレスです。

acct-port - アカウンティングメッセ―ジに使用される RADIUS サーバ UDP ポートです。(範囲: 1 から 65535)

auth-port - 認証メッセ―ジに使用される RADIUS サーバ UDP ポートです。(範囲: 1 から 65535)

key - クライアントの認証ログオンアクセスに使用される暗号化鍵です。空白を含む文字列をダブルクォート（"）で囲んでください。(最長: 48 文字)

encrypted-key - RADIUS サーバでクライアントの認証に使用される暗号化鍵です。”A-Z”または”a-z”に限定した ascii 文字列エンコードです。このキーが暗号化鍵として送られます。(最長: 48 文字)

retransmit - RADIUS サーバを介しておこなわれる認証ログオンアクセス回数です。(範囲: 1 から 30)

timeout - スイッチが要求を再送信するまでに応答を待つ秒数です。(範囲: 1 から 60)

デフォルト設定

auth-port - 1812

acct-port - 1813

timeout - 5 秒

retransmit - 2

コマンドモード

Global Configuration

コマンドの使用方法

◆ スイッチが Radius サーバからの応答を待つ時間の最大値は、*retransmit* と *timeout* との組み合わせで決定します。以下に示す Radius サーバからの最大応答待ち時間の算出式を参考に、すべての Radius サーバからの応答時間の最大値が 300 秒以内になるように設定してください。

最大応答待ち時間 ＝ *timeout* ×（*retransmit*＋１）

例

```
Console(config)#radius-server 1 host 192.168.1.20 auth-port 181 timeout 10 retransmit 5 key
green
Console(config)#
```

関連コマンド

本コマンドのデフォルト値が変更されます

radius-server acct-port

radius-server auth-port

radius-server retransmit

radius-server timeout

8.3.4 radius-server key

本コマンドでは、RADIUS 暗号化鍵を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

radius-server key *key-string*

no radius-server key

key-string - クライアントの認証ログオンアクセスに使用される暗号化鍵です。空白を含む文字列をダブルクォート（"）で囲んでください。

(最長: 48 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#radius-server key green
Console(config)#
```

8.3.5 radius-server encrypted-key

本コマンドでは、RADIUS 暗号化鍵を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

radius-server encrypted-key *key-string*

no radius-server key

key-string - クライアントの認証ログオンアクセスに使用される暗号化鍵です。ASCII 文字 "A-Z"または "a-z"を使用して任意の文字列を囲みます。 （最大長：48 文字）

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#radius-server encrypted-key Z3JlZW4=
Console(config)#
```

8.3.6 radius-server retransmit

本コマンドでは、リトライ回数を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

radius-server retransmit *number-of-retries*

no radius-server retransmit

number-of-retries - スイッチが RADIUS サーバを介してログオンアクセスを認証する回数です。(範囲: 1 から 30)

デフォルト設定

2

コマンドモード

Global Configuration

コマンドの使用方法

◆ スイッチが Radius サーバからの応答を待つ時間の最大値は、本コマンドと radius-server timeout コマンドとの組み合わせで決定します。以下に示す Radius サーバからの最大応答待ち時間の算出式を参考に、最大応答時間が 300 秒以内になるように設定してください。

最大応答待ち時間 ＝ 応答待ち時間 ×（リトライ回数＋1）

例

```
Console(config)#radius-server retransmit 5
Console(config)#
```

8.3.7 radius-server timeout

本コマンドでは、RADIUS サーバへの認証要求の送信間隔を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

radius-server timeout *number-of-seconds*

no radius-server timeout

number-of-seconds - スイッチが要求を再送信するまでに応答を待つ秒数です(範囲: 1 から 60)

デフォルト設定

5

コマンドモード

Global Configuration

コマンドの使用方法

◆ スイッチが Radius サーバからの応答を待つ時間の最大値は、本コマンドと radius-server retransmit コマンドとの組み合わせで決定します。以下に示す Radius サーバからの最大応答待ち時間の算出式を参考に、すべての Radius サーバからの応答時間の最大値が 300 秒以内になるように設定してください。

最大応答待ち時間 ＝ 応答待ち時間 ×（リトライ回数＋1）

例

```
Console(config)#radius-server timeout 10
Console(config)#
```

8.3.8 show radius-server

本コマンドでは、RADIUS サーバの現在の設定を表示します。

デフォルト設定

無し

コマンドモード

Privileged Exec

例

```
Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
 Authentication Port Number : 1812
 Accounting Port Number     : 1813
 Retransmit Times           : 2
 Request Timeout            : 5

Server 1:
 Server IP Address          : 192.168.1.1
 Authentication Port Number : 1812
 Accounting Port Number     : 1813
 Retransmit Times           : 2
 Request Timeout            : 5

RADIUS Server Group:
Group Name                Member Index
------------------------- -------------
radius                    1
Console#
```

8.4 TACACS+ Client

ターミナルアクセスコントローラアクセス制御システム(TACACS +)は、ネットワーク上の TACACS 対応デバイスへのアクセスを制御するために中央サーバ上で動作するソフトウェアを使用するログオン認証プロトコルです。認証サーバには、スイッチへの管理アクセスを必要とする各ユーザまたはグループに関連する特権レベルを持つ複数のユーザ名/パスワードのペアのデータベースが含まれています。

表 8-6 TACACS+クライアントコマンド

コマンド	機能	モード
tacacs-server host	TACACS+サーバとオプショナルパラメータを指定します。	GC
tacacs-server key	TACACS+暗号化鍵を設定します。	GC
tacacs-server encrypted-key	TACACS+暗号化鍵を設定します。	GC
tacacs-server port	TACACS+サーバネットワークポートを指定します。	GC
tacacs-server retransmit	リトライ回数を設定します。	GC
tacacs-server timeout	認証要求を送信する間隔を設定します。	GC
show tacacs-server	現在の TACACS+の設定内容を表示します。	GC

8.4.1 tacacs-server host

本コマンドでは、TACACS+サーバとオプショナルパラメータを指定します。サーバを削除したりデフォルト値を復元するには、no 形式を使用してください。

構文

tacacs-server *index* host *host-ip-address* [key *key*] [port *port-number*] [retransmit *retransmit*] [timeout *timeout*]

no tacacs-server *index*

index - サーバのインデックスです。(範囲: 1):

host-ip-address - TACACS+サーバの IP アドレスです。

key - クライアントの認証ログオンアクセスに使用される暗号化鍵です。空白を含む文字列をダブルクォート（"）で囲んでください。

(最長: 48 文字)

port-number - 認証メッセージに使用される TACACS+サーバ TCP ポートです。(範囲: 1 から 65535)

retransmit - TACACS+サーバを介しておこなわれる認証ログオンアクセス回数です。(範囲: 1 から 30)

timeout - スイッチが要求を再送信するまでに応答を待つ秒数です。(範囲: 1 から 60)

デフォルト設定

authentication port - 49

timeout - 5 秒

retransmit - 2

コマンドモード

Global Configuration

コマンドの使用方法

◆ スイッチが TACACS+サーバからの応答を待つ時間の最大値は、*retransmit* と *timeout* との組み合わせで決定します。以下に示す TACACS+サーバからの最大応答待ち時間の算出式を参考に、最大応答時間が 300 秒以内になるように設定してください。

最大応答待ち時間 ＝ *timeout* ×（*retransmit*＋１）

例

```
Console(config)#tacacs-server 1 host 192.168.1.25 port 181 timeout 10 retransmit 5 key green
Console(config)#
```

8.4.2 tacacs-server key

本コマンドでは、TACACS+暗号化鍵を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

tacacs-server key *key-string*

no tacacs-server key

key-string - クライアントの認証ログオンアクセスに使用される暗号化鍵です。空白を含む文字列をダブルクォート（"）で囲んでください。

(最長: 16 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server key green
Console(config)#
```

8.4.3 tacacs-server encrypted-key

本コマンドでは、TACACS+暗号化鍵を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

tacacs-server encrypted-key *key-string*

no tacacs-server key

key-string - クライアントの認証ログオンアクセスに使用される暗号化鍵です。ASCII 文字 "A-Z"または "a-z"を使用して任意の文字列を囲みます。 （最大長：48 文字）

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server encrypted-key Z3JlZW4=
Console(config)#
```

8.4.4 tacacs-server port

本コマンドでは、TACACS+サーバネットワークポートを指定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

tacacs-server port *port-number*

no tacacs-server port

port-number - 認証メッセージに使用される TACACS+サーバ TCP ポートです。(範囲: 1 から 65535)

デフォルト設定

49

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server port 181
Console(config)#
```

8.4.5 tacacs-server retransmit

本コマンドでは、リトライ回数を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

tacacs-server retransmit *number-of-retries*

no tacacs-server retransmit

number-of-retries - スイッチが RADIUS サーバを介してログオンアクセスを認証する回数です。(範囲: 1 から 30)

デフォルト設定

2

コマンドモード

Global Configuration

コマンドの使用方法

◆ スイッチが TACACS+サーバからの応答を待つ時間の最大値は、本コマンドと tacacs-server timeout コマンドとの組み合わせで決定します。以下に示す TACACS+サーバからの最大応答待ち時間の算出式を参考に、最大応答時間が 300 秒以内になるように設定してください。

最大応答待ち時間 ＝ 応答待ち時間 ×（リトライ回数＋１）

例

```
Console(config)#tacacs-server retransmit 5
Console(config)#
```

8.4.6 tacacs-server timeout

本コマンドでは、TACACS+サーバへの認証要求の送信間隔を設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

tacacs-server timeout *number-of-seconds*

no tacacs-server timeout

number-of-seconds - スイッチが要求を再送信するまでに応答を待つ秒数です(範囲: 1 から 60)

デフォルト設定

5

コマンドモード

Global Configuration

コマンドの使用方法

◆ スイッチが TACACS+サーバからの応答を待つ時間の最大値は、本コマンドと tacacs-server retransmit コマンドとの組み合わせで決定します。以下に示す TACACS+サーバからの最大応答待ち時間の算出式を参考に、最大応答時間が 300 秒以内になるように設定してください。

最大応答待ち時間 ＝ 応答待ち時間 ×（リトライ回数＋１）

例

```
Console(config)#tacacs-server timeout 10
Console(config)#
```

8.4.7 show tacacs-server

本コマンドでは、TACACS+サーバへの認証要求の送信間隔を設定します。

デフォルト設定

無し

コマンドモード

Privileged Exec

例

```
Console#show tacacs-server

Remote TACACS+ Server Configuration:

Global Settings:
 Server Port Number : 49
 Retransmit Times   : 2
 Timeout            : 5

Server 1:
 Server IP Address  : 10.11.12.13
 Server Port Number : 49
 Retransmit Times   : 2
 Timeout            : 4

TACACS+ Server Group:
Group Name               Member Index
------------------------ ------------
tacacs+                  1
Console#
```

8.5 AAA

認証、認可、およびアカウンティング (AAA)機能は、スイッチのアクセス制御を設定するための主要なフレームワークを提供します。AAA 機能では、ネットワーク内に設定された RADIUS サーバまたは TACACS +サーバを使用する必要があります。

表 8-7 AAA コマンド

コマンド	機能	モード
aaa accounting commands	Exec モードコマンドのアカウンティングを有効にします。	GC
aaa accounting exec	Exec サービスのアカウンティングを有効にします。	GC
aaa accounting update	アカウンティングサーバへ送信するための、定期更新を有効にします。	GC
aaa authorization commands	Exec モードコマンドのアカウンティングを有効にします。	GC
aaa authorization exec	Exec セッションの認証を有効にします。	GC
aaa group server	定義済みリストにセキュリティサーバをグループ化します。	GC
server	グループリストの中のサーバ IP アドレスを設定します。	SG
accounting commands	ユーザが入力した CLI コマンドにアカウンティング方式を適用します。	Line
accounting exec	ローカルコンソール、Telnet または SSH 接続にアカウンティング方式を適用します。	Line
authorization commands	ユーザが入力した CLI コマンドの認証方式を適用します。	Line
authorization exec	ローカルコンソール、Telnet または SSH 接続に認証方式を適用します。	Line
show accounting	すべてのアカウンティング情報を表示します。	PE
show authorization	すべての認証情報を表示します。	PE

8.5.1 aaa accounting commands

本コマンドでは、Exec モードコマンドのアカウンティングを有効にします。アカウンティングサービスを無効にするには、no 形式を使用してください。

構文

aaa accounting commands *level* {default | *method-name*} start-stop group {tacacs+ | *server-group*}

no aaa accounting commands *level* {default | *method-name*}

level - コマンドを実行するための特権レベルです。(範囲: 0 から 15)

default - サービス要求に対するデフォルトアカウンティング方式を指定します。

method-name - サービス要求に対するデフォルトアカウンティング方式を指定します。(範囲: 1-64 文字)

start-stop - 開始地点から停止地点までのアカウンティングを記録します。

group - 使用するサーバグループを指定します。

tacacs+ - tacacs-server host コマンドで設定したすべての TACACS+ホストを指定します。

server-group - aaa group server コマンドで設定したサーバグループ名を指定します。(範囲: 1 から 64 文字)

デフォルト設定

アカウンティングは有効になっていません。

サーバが指定されていません。

コマンドモード

Global Configuration

コマンドの使用方法

- Exec モードコマンドのアカウンティングは、TACACS+サーバのみにサポートされています。
- デフォルトおよび method-name フィールドは、指定された TACACS +サーバで設定されたアカウンティング方式を記述するためにのみ使用され、実際に使用する方法についてはサーバに情報を送信しません。

例

```
Console(config)#aaa accounting commands 15 default start-stop group tacacs+
Console(config)#
```

8.5.2 aaa accounting exec

本コマンドでは、ネットワークアクセスのために要求された Exec サービスのアカウンティングを有効にします。アカウンティングサービスを無効にするには、no 形式を使用してください。

構文

aaa accounting exec {default | *method-name*}

start-stop group {radius | tacacs+ |*server-group*}

no aaa accounting exec *method-name*

default - サービス要求に対するデフォルトアカウンティング方式を指定します。

method-name - サービス要求に対するデフォルトアカウンティング方式を指定します。(範囲: 1-64 文字)

start-stop - 開始地点から停止地点までのアカウンティングを記録します。

group - 使用するサーバグループを指定します。

radius - radius-server host コマンドで設定したすべての RADIUS ホストを指定します。

tacacs+ - tacacs-server host コマンドで設定したすべての TACACS+ホストを指定します。

server-group - aaa group server コマンドで設定したサーバグループ名を指定します。(範囲: 1 から 64 文字)

デフォルト設定

アカウンティングは有効になっていません。

サーバが指定されていません。

コマンドモード

Global Configuration

コマンドの使用方法

- 本コマンドにより、ローカルコンソールおよび Telnet 接続の Exec サービス要求のアカウンティングを実行します。
- デフォルトおよび method-name フィールドは、指定された TACACS +サーバで設定されたアカウンティング方式を記述するためにのみ使用され、実際に使用する方法についてはサーバに情報を送信しません。

例

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

8.5.3 aaa accounting update

本コマンドにより、定期的な更新をアカウンティングサーバに送信することができます。アカウンティングの更新を無効にするには、no 形式を使用してください。

構文

aaa accounting update [periodic *interval*]

no aaa accounting update

interval - 暫定アカウンティングレコードをこの間隔でサーバに送信します。(範囲: 1 から 2147483647 分)

デフォルト設定

1 分

コマンドモード

Global Configuration

コマンドの使用方法

- アカウンティング更新が有効の場合、スイッチはシステム上のすべてのユーザの定期的な暫定アカウンティングレコードを発行します。
- 暫定間隔を指定せずにコマンドを使用すると、デフォルト設定に間隔設定が変更されます。

例

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

8.5.4 aaa authorization commands

本コマンドでは、Exec モードコマンドの承認を有効にします。承認サービスを無効にするには、no 形式を使用してください。

構文

aaa authorization commands *level* {default | *method-name*} start-stop group {tacacs+ | *server-group*}

no aaa authorization commands *level* {default | *method-name*}

level - コマンドを実行するための特権レベルです。(範囲: 0 から 15)

default - サービス要求に対するデフォルトアカウンティング方式を指定します。

method-name - サービス要求に対するデフォルトアカウンティング方式を指定します。(範囲: 1-64 文字)

start-stop - 開始地点から停止地点までのアカウンティングを記録します。

group - 使用するサーバグループを指定します。

tacacs+ - tacacs-server host コマンドで設定したすべての TACACS+ホストを指定します。

server-group - aaa group server コマンドで設定したサーバグループ名を指定します。(範囲: 1 から 64 文字)

デフォルト設定

アカウンティングは有効になっていません。

サーバが指定されていません。

コマンドモード

Global Configuration

コマンドの使用方法

- Exec モードコマンドのアカウンティングは、TACACS+サーバのみにサポートされています。
- default および method-name フィールドは、指定された TACACS +サーバで設定されたアカウンティング方式を記述するためにのみ使用され、実際に使用する方法についてはサーバに情報を送信しません。

例

```
Console(config)#aaa authorization commands 15 default start-stop group tacacs+
Console(config)#
```

8.5.5 aaa authorization exec

本コマンドは、Exec アクセスの承認を有効にします。承認サービスを無効にするには、no 形式を使用してください。

構文

aaa authorization exec {default | *method-name*}

group {tacacs+ | *server-group*}

no aaa authorization exec {default | *method-name*}

default - Exec アクセスに対しデフォルト承認方式を指定します。

method-name - Exec アクセスに対し承認方式を指定します。(範囲: 1-64 文字)

group - 使用するサーバグループを指定します。

tacacs+ - tacacs-server host コマンドで設定したすべての TACACS+ホストを指定します。

server-group - aaa group server コマンドで設定したサーバグループ名を指定します。(範囲: 1 から 64 文字)。

デフォルト設定

アカウンティングは有効になっていません。

サーバが指定されていません。

コマンドモード

Global Configuration

コマンドの使用方法

- 本コマンドは、ローカルコンソール、Telnet または SSH 接続に対してユーザが Exec の実行を許可されているかどうかについて承認を実行します。
- AAA 認証は、承認が有効になる前に有効にする必要があります。
- このコマンドが指定された名前付き方式なしで発行された場合、名前付き方式が明示的に定義されているものを除き、すべてのインタフェースまたは行(この承認タイプが適用される)にデフォルトの方式リストが適用されます。

例

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

8.5.6 aaa group server

セキュリティサーバホストに名前を付けるためにこのコマンドを使用します。設定リストからサーバグループを削除するにはコマンドの、no 形式を入力してください。

構文

[no] aaa group server {radius | tacacs+} *group-name*

radius - RADIUS サーバグループを定義します。

tacacs+ - TACACS+サーバグループを定義します。

group-name - セキュリティサーバグループに名前を付けるテキスト文字です。

(範囲: 1-64 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

8.5.7 server

このコマンドは、AAA サーバグループにセキュリティサーバを追加します。グループから関連サーバを削除するには、no 形式を使用してください。

構文

[no] server {*index* | *ip-address*}

index - サーバインデックスを指定します。(範囲: RADIUS 1-5, TACACS+ 1)

ip-address - サーバのホスト IP アドレスを指定します。

デフォルト設定

無し

コマンドモード

Server Group Configuration

コマンドの使用方法

- RADIUS サーバのインデックスを指定する際、そのサーバインデックスは、radius-server host コマンドで定義済みである必要があります。
- TACACS+サーバのインデックスを指定する際、そのサーバインデックスは、tacacs-server host コマンドで定義済みである必要があります。
- 複数サーバを設定しての優先度処理は将来サポート予定です。

例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

8.5.8 accounting commands

本コマンドは、アカウンティング方式を入力した CLI コマンドに適用します。入力した CLI コマンドのアカウンティングを無効にするには、no 形式を使用してください。

構文

accounting commands *level* {default | *list-name*}

no accounting commands *level*

level - コマンドを実行するための特権レベルです。(範囲: 0 から 15)

default - aaa accounting commands コマンドで作成したデフォルト方式を指定します。

list-name - aaa accounting commands コマンドで作成した方式リストを指定します。

デフォルト設定

無し

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line)#accounting commands 15 default
Console(config-line)#
```

8.5.9 accounting exec

本コマンドは、アカウンティング方式をローカルコンソール、Telnet または SSH 接続に適用します。ライン上のアカウンティングを無効にするには、no 形式を使用してください。

構文

accounting exec {default | *list-name*}

no accounting exec

default - aaa accounting exec コマンドで作成したデフォルト方式を指定します。

list-name - aaa accounting exec コマンドで作成した方式リストを指定します。

デフォルト設定

無し

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#
```

8.5.10 authorization commands

本コマンドは、入力した CLI コマンドに承認方式を適用します。入力した CLI コマンドの承認を無効にするには、no 形式を使用してください。

構文

authorization commands *level* {default | *list-name*}

no authorization commands *level*

level - コマンドを実行するための特権レベルです。(範囲: 0 から 15)

default - aaa authorization commands コマンドで作成したデフォルト方式を指定します。

list-name - aaa authorization commands コマンドで作成した方式リストを指定します。

デフォルト設定

無し

コマンドモード

Line Configuration

コマンドの使用方法

コマンド「authorization commands 0」が実行された場合、スイッチは特権レベル 0 ユーザによって発行されたすべてのコマンドをブロックします。 ユーザレベルの承認済みコマンドは、AAA サーバで設定する必要があります。

例

```
Console(config)#line console
Console(config-line)#authorization commands 15 default
Console(config-line)#
```

8.5.11 authorization exec

本コマンドは、ローカルコンソール、Telnet または SSH 接続に認証方式を適用します。ライン上の認証を無効にするには、no 形式を使用してください。

構文

authorization exec {default | *list-name*}

no authorization exec

default - aaa authorization exec コマンドで作成したデフォルト方式を指定します。

list-name - aaa authorization exec コマンドで作成した方式リストを指定します。

デフォルト設定

無し

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#
```

8.5.12 show accounting

本コマンドでは、機能およびポートごとに現在のアカウンティング設定について表示します。

構文

show accounting [commands [*level*]] |

[[dot1x [statistics [username *user-name* | interface *interface*]] | exec [statistics] | statistics]

commands - コマンドアカウンティング情報を表示します。

level - 特定コマンドレベルのコマンドアカウンティング情報を表示します。

dot1x - dot1x アカウンティグ情報を表示します。

exec - Exec アカウンティング記録を表示します。

statistics - アカウンティング記録を表示します。

user-name - 特定ユーザ名のアカウンティング記録を表示します。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

デフォルト設定

無し

コマンドモード

Privileged Exec

例

```
Console#show accounting
Accounting Type : dot1x
  Method List   : default
  Group List    : radius
  Interface     : Eth 1/1

  Method List   : tps
  Group List    : radius
  Interface     : Eth 1/2

Accounting Type : EXEC
  Method List   : default
  Group List    : tacacs+
  Interface     : vty

Accounting Type : Commands 0
  Method List   : default
  Group List    : tacacs+
  Interface     :
.
.
.
Accounting Type : Commands 15
  Method List   : default
  Group List    : tacacs+
  Interface     :

Console#
```

8.5.13 show authorization

本コマンドにより、機能およびポートごとの現在の承認設定について表示します。

構文

show authorization [commands [*level*] | exec]

commands - コマンド承認情報を表示します。

level - 特定コマンドレベルのコマンド承認情報を表示します。

exec - Exec 承認記録を表示します。

デフォルト設定

無し

コマンドモード

Privileged Exec

例

```
Console#show authorization
Authorization Type : EXEC
  Method List   : default
  Group List    : tacacs+
  Interface     : vty

Authorization Type : Commands 0
  Method List   : default
  Group List    : tacacs+
  Interface     :
.
.
.
Authorization Type : Commands 15
  Method List   : default
  Group List    : tacacs+
  Interface     :

Console#
```

8.6 Web サーバ

本章では、スイッチへの Web ブラウザ管理アクセスを設定するために使用するコマンドについて説明します。

表 8-8 Web サーバコマンド

コマンド	機能	モード
ip http authentication	EXEC セッションの EXEC 認証の方式リストを設定します。	GC
ip http port	Web ブラウザインタフェースで使用されるポートを指定します。	GC
ip http server	スイッチがブラウザから監視または設定できるように許容します。	GC
ip http secure-port	HTTPS の TCP ポート番号を指定します。	GC
ip http secure-server	暗号化通信のために HTTPS (HTTP/SSL)を有効にします。	GC
show authorization	すべての承認情報を表示します。	PE

Note: 300 秒間入力が検知されなかった場合、ユーザは HTTP サーバまたは HTTPS サーバから自動的にログオフされます。

8.6.1 ip http authentication

本コマンドでは、Web ブラウザインタフェースで使用される EXEC セッションを開始するための EXEC 認証方式リストを指定します。デフォルトポートを使うには、no 形式を使用してください。

構文

ip http authentication aaa exec-authorization {default | *list-name*}

no ip http authentication aaa exec-authorization

default - 認証要求のためにデフォルト方式を指定します。

list-name - aaa authorization commands コマンドで作成した方式リストを指定します。

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#ip http authentication aaa exec-authorization default
Console(config)#
```

関連コマンド

aaa authorization commands

ip http server

show system

8.6.2 ip http port

本コマンドでは、Web ブラウザインタフェースで使用される TCP ポート番号を指定します。デフォルトポートを使うには、no 形式を使用してください。

構文

ip http port *port-number*

no ip http port

port-number - ブラウザインタフェースで使用される TCP ポートです。(範囲: 1 から 65535)

デフォルト設定

80

コマンドモード

Global Configuration

例

```
Console(config)#ip http port 769
Console(config)#
```

関連コマンド

ip http server

show system

8.6.3 ip http server

本コマンドは、デバイスのブラウザからの監視または設定を許可します。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip http server

デフォルト設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#ip http server
Console(config)#
```

関連コマンド

ip http authentication

show system

8.6.4 ip http secure-port

本コマンドにより、スイッチの Web インタフェースへの HTTPS 接続に使用される TCP ポート番号を指定します。デフォルトのポートを復元するには、no 形式を使用してください。

構文

ip http secure-port *port_number*

no ip http secure-port

port_number - HTTPS に使用される TCP ポートです。(範囲: 1 から 65535)

デフォルト設定

443

コマンドモード

Global Configuration

コマンドの使用方法

- HTTP および HTTPS に同じポート番号を設定できません。
- HTTPS ポート番号を変更するには、HTTPS サーバに接続を試みているクライアントは URL でポートバ番号を次のフォーマットで指定する必要があります: https://*device*:*port_number*

例

```
Console(config)#ip http secure-port 1000
Console(config)#
```

関連コマンド

ip http secure-server

show system

8.6.5 ip http secure-server

本コマンドにより、Secure Socket Layer(SSL)上でセキュアハイパーテキスト転送プロトコル(HTTPS)を有効

にし、スイッチの Web インタフェースへの安全なアクセス(例; 暗号化された接続))を提供します。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip http secure-server

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- スイッチ上で HTTP と HTTPS の両方のサービスを個別に有効にすることができます。ただし、HTTP および HTTPS に同じ UDP ポート番号を設定できません。
- HTTPS を有効にするには、ブラウザで指定した下記の URL に HTTPS を指定する必要があります。
  https://*device*[:*port_number*]
- HTTPS を開始すると、下記の方法で接続が確立されます:
  - サーバデジタル証明を使用して、クライアントがサーバを認証します。
  - クライアントとサーバは、接続に使用する一連のセキュリティプロトコルをネゴシエートします。
  - クライアントとサーバは、暗号化および非暗号化データのために、セッション鍵を生成します。
- クライアントとサーバは、安全な暗号化接続を確立します。
  Internet Explorer 11 以上、Mozilla Firefox、または Google Chrome は、最新バージョンもしくは最新より 1 つ古いバージョンの標準 Web ブラウザのステータスバーに、南京錠のアイコンが表示されなければなりません。
  以下の Web ブラウザおよびオペレーティングシステムで、HTTPS をサポートしています:

表 8-9 HTTPS システムサポート

Web ブラウザ	オペレーティングシステム
Internet Explorer 11 またはそれ以降	Windows 7, 8, 10
Mozilla Firefox 最新または最新の 1 つ前のバージョン	Windows 7, 8, 10, Linux
Google Chrome 最新または最新の 1 つ前のバージョン	Windows 7, 8, 10

- セキュアサイト証明書を指定するには、「Web 管理ガイド」の「デフォルトのセキュアサイト証明書の置換」を参照してください。また、copy tftp https-certificate コマンドも参照してください。
- IPv6 リンクローカルアドレスを使用する HTTPS では、Web インタフェースへの接続はサポートされていません。

例

```
Console(config)#ip http secure-server
Console(config)#
```

関連コマンド

ip http secure-port

copy tftp https-certificate

show system

8.7 Telnet サーバ

本章では、スイッチへの Telnet 管理アクセスに使用されるコマンドについて説明します。

表 8-10 Telnet サーバコマンド

コマンド	機能	モード
ip telnet max-sessions	このシステムに同期的に接続できる、最大 Telnet セッション数を指定します。	GC
ip telnet port	Telnet インタフェースで使用するポートを指定します。	GC
ip telnet server	スイッチがブラウザから監視または設定できるように許容します。	GC
telnet (client)	Telnet 接続を使用してリモートデバイスにアクセスします。	PE
show ip telnet	Telnet サーバのコンフィグレーションについて表示します。	PE

Note: このスイッチは、Telnet クライアント機能もサポートしています。Privileged Exec 設定レベルで telnet コマンドを入力することにより、このスイッチから別のデバイスに Telnet 接続することができます。

8.7.1 ip telnet max-sessions

本コマンドにより、このシステムに同時に接続できる Telnet セッションの最大数を指定します。デフォルトの設定に戻すには、no を使用してください。

構文

ip telnet max-sessions *session-count*

no ip telnet max-sessions

session-count - Telnet セッションの最大許容回数です。(範囲: 0 から 8)

デフォルト設定

8 セッション

コマンドモード

Global Configuration

コマンドの使用方法

Telnet と Secure Shell に対して最大 8 つのセッションを同時に開くことができます(例; Telnet と SSH の両方が最大 8 セッションを共有します)。

例

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

8.7.2 ip telnet port

本コマンドにより、Telnet インタフェースにより使用される TCP ポート番号を指定します。デフォルトポートを使うには、no 形式を使用してください。

構文

ip telnet port *port-number*

no telnet port

port-number - ブラウザインタフェースで使用される TCP ポート番号です。(範囲: 1 から 65535)

デフォルト設定

23

コマンドモード

Global Configuration

例

```
Console(config)#ip telnet port 123
Console(config)#
```

8.7.3 ip telnet server

本コマンドにより、監視または設定できるようにデバイスを許容します。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip telnet server

デフォルト設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#ip telnet server
Console(config)#
```

8.7.4 telnet (client)

本コマンドは、Telnet 接続を使用してリモートデバイスにアクセスします。

構文

telnet *host*

host - リモートデバイスの IP アドレスまたはエイリアスです。

コマンドモード

Privileged Exec

例

```
Console#telnet 192.168.2.254
Connect To 192.168.2.254...

************************************************************

WARNING - MONITORED ACTIONS AND ACCESSES

User Access Verification

Username:

Console(config)#
```

8.7.5 show ip telnet

本コマンドにより、Telnet サーバのコンフィグレーションについて表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show ip telnet
IP Telnet Configuration:

Telnet Status: Enabled
Telnet Service Port: 23
Telnet Max Session: 8
Console#
```

8.8 SSH

本章では、SSH サーバの設定に使用するコマンドについて説明します。ここのプロトコルを使用してスイッチを設定する場合は、SSH クライアントを管理ステーションにインストールする必要があります。

Note: このスイッチは SSH バージョン 1.5 および 2.0 クライアントの両方をサポートします。

表 8-11 Secure Shell コマンド

コマンド	機能	モード
ip ssh authentication-retries	クライアントにより許容された、リトライ数を指定します。	GC
ip ssh server	スイッチ上の SSH サーバを有効にします。	GC
ip ssh server-key size	SSH サーバ鍵サイズを設定します。	GC
ip ssh timeout	SSH サーバの認証タイムアウトを指定します。	GC
copytftp public-key	ユーザ公開鍵を TFTP サーバからスイッチにコピーします。	PE
delete public-key	指定したユーザの公開鍵を削除します。	PE
ip ssh crypto host-key generate	ホスト鍵を生成します。	PE
ip ssh crypto zeroize	RAM からのホスト鍵をクリアにします。	PE
ip ssh save host-key	RAM からフラッシュメモリへのホスト鍵を保存します。	PE
show ip ssh	SSH サーバのステータスと認証タイムアウト、および再試行の設定値を表示します。	PE
show public-key	指定したユーザまたはホストの公開鍵を表示します。	PE
show ssh	現在の SSH セッションのステータスを表示します。	PE

8.8.1 設定ガイドライン

このスイッチの SSH サーバは、パスワードと公開鍵の両方の認証をサポートしています。SSH クライアントによってパスワード認証が指定されている場合は、authentication login コマンドで指定されているように、ローカルまたは RADIUS または TACACS +リモート認証サーバを介してパスワードを認証できます。クライアントによって公開鍵認証が指定されている場合は、次の章で説明するように、クライアントとスイッチの両方で認証鍵を設定する必要があります。公開鍵認証を使用するかパスワード認証を使用するかにかかわらず、スイッチで認証鍵を生成して SSH サーバを有効にする必要があります。

SSH サーバを使用するには、次のステップを完了させてください:

1. ホスト鍵ペアの生成 - ホストの公開鍵/秘密鍵ペアを作成するには、ip ssh crypto host-key generate コマンドを使用します。
2. クライアントへのホスト公開鍵の提供 - 多くの SSH クライアントプログラムは、スイッチの初期接続設定中にホスト公開鍵を自動的にインポートします。それ以外の場合は、管理ステーションに既知のホストファイルを手動で作成し、そのホストに公開鍵を配置する必要があります。既知のホストファイル内の公開鍵の入力は、以下の例のようになります:
   10.1.0.54 1024 35 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761 17
3. スイッチへのクライアントの公開鍵のインポート - copy tftp public-key コマンドを使用して、スイッ

チに許可されたすべての SSH クライアントのパスワードを含むファイルをコピーします。(これらのクライアントは、username コマンドを使用してスイッチ上でローカルに設定する必要があります。）次に、クライアントはこれらの鍵を使用して認証されます。現在のソフトウェアは、RSA 鍵の次の例に示すように、標準の UNIX 形式にもとづいて公開鍵ファイルのみを受け入れます。

1024 35
134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19

4. オプショナルパラメータの設定 - 認証タイムアウト、リトライ数およびサーバ鍵サイズを含む、その他のオプショナルパラメータを設定します。
5. SSH サービスの有効化 - ip ssh server コマンドを使用して、スイッチ上の SSH サーバを有効にします。
6. 認証 - 以下の認証方法のうちの 1 つを採用します:
   パスワード認証 (SSH v1.5 または V2 クライアント)
   a. クライアントがサーバにパスワードを送信します。
   b. スイッチが、クライアントパスワードをメモリに格納されている他のクライアントパスワードと比較します。
   c. 合致した場合、接続が許可されます。

Note: パスワード認証のみで SSH を使用するには、初期接続中または既知のホストファイルに手動で入力した場合でも、ホスト公開鍵をクライアントに与えなければなりません。ただし、クライアントの鍵を設定する必要はありません。

公開鍵認証- SSH クライアントがスイッチに接続しようとすると、SSH サーバはホスト鍵ペアを使用してセッション鍵と暗号化方式をネゴシエートします。スイッチに格納されている公開鍵に対応する秘密鍵を持つクライアントだけがアクセスできます。このプロセス中に以下の交換が行われます:

SSH v1.5 クライアントの認証

a. クライアントがスイッチに公開鍵を送信します。
b. スイッチが、クライアント公開鍵をメモリに格納されている他のクライアント公開鍵と比較します。
c. 一致した場合には、スイッチは秘密鍵を使用してランダムな 256 ビット文字列をチャレンジとして生成し、この文字列をユーザの公開鍵で暗号化してクライアントに送信します。
d. クライアントは秘密鍵を使用してチャレンジ文字列を復号化し、MD5 チェックサムを計算し、チェックサムをスイッチに返します。
e. スイッチは、クライアントから送信されたチェックサムと、送信した元の文字列の計算結果を比較します。2 つのチェックサムが一致する場合、これはクライアントの秘密鍵が許可された公開鍵に対応し、クライアントが認証されていることを意味します。

SSH v2 クライアントの認証

a. クライアントはまずスイッチに照会して、優先アルゴリズムを使用する DSA 公開鍵認証が受け入れ可能かどうかについて判断します。
b. 指定されたアルゴリズムがスイッチによってサポートされている場合、認証プロセスを進めるようにクライアントに通知します。そうでなければ、要求を拒否します。
c. クライアントが、秘密鍵を使用して生成された署名をスイッチに送信します。

d. サーバはこのメッセージを受信すると、指定された鍵が認証に適しているかどうかをチェックし、そうであれば、署名が正しいかどうかをチェックします。両方のチェックが成功すると、クライアントは認証されます。

Note: SSH サーバは、最大 8 つのクライアントセッションをサポートします。クライアントセッションの最大数には、現在の Telnet セッションと SSH セッションの両方が含まれます。

Note: SSH サーバには、スイッチ上の設定済みの IPv4 または IPv6 インタフェースアドレスを使用してアクセスすることができます。

8.8.2 ip ssh authentication-retries

本コマンドにより、SSH サーバがユーザの再認証する回数を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

ip ssh authentication-retries *count*

no ip ssh authentication-retries

count - 許可された認証試行回数です。その後、インタフェースはリセットされます。(範囲: 1 から 5)

デフォルト設定

3

コマンドモード

Global Configuration

例

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

関連コマンド

show ip ssh

8.8.3 ip ssh server

本コマンドにより、スイッチの Secure Shell (SSH)サーバを有効にします。このサービスを無効にするには、no 形式を使用してください。

構文

[no] ip ssh server

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- SSH サーバは、最大 8 つのクライアントセッションをサポートします。クライアントセッションの最大数には、現在の Telnet セッションと SSH セッションの両方が含まれます。
- SSH サーバは、クライアントが最初にスイッチとの接続を確立した後、クライアントと交渉してデータ暗号化用の DES(56 ビット)または 3DES(168 ビット)のいずれかを選択するときに、鍵交換に DSA または RSA を使用します。
- SSH サーバを確立する前に、DSA ホスト鍵および RSA ホスト鍵の両方を生成する必要があります。

例

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

関連コマンド

ip ssh crypto host-key generate

show ssh

8.8.4 ip ssh server-key size

本コマンドにより、SSH サーバ鍵サイズを設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

ip ssh server-key size *key-size*

no ip ssh server-key size

key-size - サーバ鍵のサイズです。(範囲: 512 から 896 ビット)

デフォルト設定

768 ビット

コマンドモード

Global Configuration

コマンドの使用方法

サーバ鍵は、スイッチの外部では決して共有されない秘密鍵です。

ホスト鍵は SSH クライアントと共有され、1024 ビット固定です。

例

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

8.8.5 ip ssh timeout

本コマンドにより、SSH サーバのタイムアウトを設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

ip ssh timeout *seconds*

no ip ssh timeout

seconds - SSH ネゴシエーション中のクライアント応答のタイムアウトです。(範囲: 1 から 120)

デフォルト設定

120 秒

コマンドモード

Global Configuration

コマンドの使用方法

タイムアウトは、スイッチが SSH ネゴシエーションフェーズ中にクライアントからの応答を待つ間隔を指定します。SSH セッションが確立されると、ユーザ入力のタイムアウトは、vty セッションの exec-timeout コマンドによって制御されます。

例

```
Console(config)#ip ssh timeout 60
Console(config)#
```

関連コマンド

exec-timeout

show ip ssh

8.8.6 delete public-key

本コマンドにより、指定したユーザの公開鍵を削除します。

構文

delete public-key *username*

username - SSH ユーザ名です。(範囲: 1-32 文字)

デフォルト設定

DSA 鍵と RSA 鍵の両方を削除します。

コマンドモード

Privileged Exec

例

```
Console#delete public-key admin dsa
Console#
```

8.8.7 ip ssh crypto host-key generate

本コマンドにより、ホスト鍵ペア(DSA 鍵と RSA 鍵の両方)を生成します。

構文

ip ssh crypto host-key generate

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

- スイッチは SSHv1.5 クライアントでは RSA バージョン 1 のみ、SSHv2 クライアントでは DSA バージョン 2 のみを使用します。
- このコマンドは、ホスト鍵ペアをメモリ(例; RAM)に格納します。ip ssh save host-key コマンドを使用して、ホスト鍵ペアをフラッシュメモリに保存します。
- 一部の SSH クライアントプログラムは、設定プロセスの一環として既知のホストファイルに公開鍵を自動的に追加します。それ以外の場合は、既知の hosts ファイルを手動で作成し、その中にホスト公開鍵を置く必要があります。
- SSH サーバは、このホスト鍵を使用して、接続しようとするクライアントとのセッション鍵と暗号化方法をネゴシエートします。
- SSH サーバを確立する前に、DSA ホスト鍵および RSA ホスト鍵の両方を生成する必要があります。

例

```
Console#ip ssh crypto host-key generate
Console#
```

関連コマンド

ip ssh crypto zeroize

ip ssh save host-key

8.8.8 ip ssh crypto zeroize

本コマンドにより、メモリからホスト鍵をクリアします(例; RAM)。

構文

ip ssh crypto zeroize

デフォルト設定

DSA 鍵と RSA 鍵の両方をクリアします。

コマンドモード

Privileged Exec

コマンドの使用方法

- ◆ 本コマンドにより、ホスト鍵を揮発性メモリ(RAM)からクリアします。
- ◆ このコマンドを実行する前に、SSH サーバを無効にする必要があります。

例

```
Console#ip ssh crypto zeroize
Console#
```

関連コマンド

ip ssh crypto host-key generate

ip ssh save host-key

no ip ssh server

8.8.9 ip ssh save host-key

本コマンドにより、RAM からフラッシュメモリにホスト鍵を保存します。

構文

ip ssh save host-key

デフォルト設定

DSA 鍵と RSA 鍵の両方を保存します。

コマンドモード

Privileged Exec

例

```
Console#ip ssh save host-key
Console#
```

関連コマンド

ip ssh crypto host-key generate

8.8.10 show ip ssh

このコマンドは、SSH サーバへのクライアントアクセスを認証するときに使用される接続設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip ssh
SSH Enabled - Version 2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
Server Key Size     : 768 ビット
Console#
```

8.8.11 show public-key

本コマンドでは、指定ユーザまたはホストの公開鍵を表示します。

構文

show public-key [user [*username*]| host]

username - SSH ユーザ名です。(範囲: 1-32 文字)

デフォルト設定

すべての公開鍵を表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

- パラメータが入力されていない場合、すべての鍵が表示されます。ユーザキーワードが入力されていて、ユーザ名が指定されていない場合は、すべてのユーザの公開鍵が表示されます。
- RSA 鍵が表示された時、最初のフィールドがホスト鍵のサイズ(例; 1024)。2 つ目のフィールドに暗号化公開指数(例; 35)、そして最後の文字列に暗号化モジュールが表示されます。DSA 鍵が表示されると、最初のフィールドに SSH によって使用される暗号化方式は Digital Signature Standard(DSS)にもとづいていて、最後のフィールドが暗号化モジュールであることが表示されます。

例

```
Console#show public-key host
Host:
RSA:
1024 65537 13236940658254764031382795526536375927835525327972629521130241
  07194210616557594245909392360969540503627752575562510038661309893938345231033280214988866192l
  59556859887989191950588394018138744046890877916030583776818549000283134162500834871844952208 7
  42921225569166565529632816351696404083155476606641516571163 81
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/DgOh2Hxc
  YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
  JlPdOkFgzLGMinvSNYQwiQXbKTBHOZ4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEA
  sy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMUO1VFDly3IR
  2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
  iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
  DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
  o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1YgOfhLwuHpOSKdxT3kk475S7 wOW
Console#
```

8.8.12 show ssh

本コマンドでは、現在の SSH サーバ接続を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ssh
Connection Version State              Username Encryption
  1          2.0   Session-Started     admin   ctos aes128-cbc-hmac-md5
                                               stoc aes128-cbc-hmac-md5
Console#
```

表 8-12 show ssh - 表示説明

フィールド	説明
Connection	セッション番号です。(範囲: 1 から 8)
Version	Secure Shell バージョン番号です。
State	認証ネゴシエーション状態です。 (値: ネゴシエーション-開始、認証-開始、セッション-開始)
Username	クライアントのユーザ名です。

8.9 IP フィルタの管理

本章では、スイッチへの IP 管理アクセスを設定するために使用されるコマンドについて説明します。

表 8-13 管理 IP フィルタコマンド

コマンド	機能	モード
management	管理アクセスが許可されている IP アドレスを設定します。	GC
show management	ブラウザから監視または設定するスイッチを表示します。	PE

8.9.1 management

本コマンドでは、さまざまなプロトコルを使用してスイッチに管理アクセスを許可するクライアント IP アドレスを指定します。最大 15 の IP アドレスまたは IP アドレスグループのリストを指定することができます。デフォルト設定を復元するには、no 形式を使用してください。

構文

[no] management {all-client | http-client | snmp-client | telnet-client} *start-address* [*end-address*]

all-client - 全グループに IP アドレスを追加します。

http-client - Web ブラウザに全アドレスを追加します。

snmp-client - SNMP グループに IP アドレスを追加します。

telnet-client - Telnet グループに IP アドレスを追加します。

start-address - 単一の IP アドレス、または範囲の開始アドレス。

end-address - 範囲の終了アドレス。

デフォルト設定

すべてのアドレス

コマンドモード

Global Configuration

コマンドの使用方法

- 管理インタフェースは、デフォルトですべての IP アドレスに対して開いています。フィルタリストにエントリを追加すると、そのインタフェースへのアクセスは指定されたアドレスに制限されます。
- 誰かが無効なアドレスからスイッチの管理インタフェースにアクセスしようとすると、スイッチは接続を拒否し、システムログにイベントメッセージを入力し、トラップメッセージをトラップマネージャに送信します。
- IP アドレスは、それぞれ SNMP、Web、および Telnet アクセス用に設定できます。これらの各グループには個々のアドレスまたはアドレス範囲のいずれかで、最大 5 つの異なるアドレスセットを含めることができます。
- 同一グループのアドレスを入力する時(例; SNMP、Web、または Telnet)、スイッチは重複したアドレス範囲は受け付けません。異なるグループのアドレスを入力する場合、スイッチは重複したアドレス範囲を受け付けます。
- 指定した範囲から個々のアドレスを削除することはできません。範囲全体を削除し、アドレスを再入力する必要があります。

◆ 開始アドレスを指定するだけでアドレス範囲を削除することも、開始アドレスと終了アドレスの両方を指定することもできます。

例

以下の例では、指定アドレスへの管理アクセスを制限します。

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

8.9.2 show management

本コマンドでは、さまざまなプロトコルを通じてスイッチへの管理アクセスが許可されているクライアント IP アドレスを表示します。

構文

show management {all-client | http-client | snmp-client | telnet-client}

all-client - 全グループの IP アドレスを表示します。

http-client - Web グループの IP アドレスを表示します。

snmp-client - SNMP グループの IP アドレスを表示します。

telnet-client - SNMP グループの IP アドレスを表示します。 Telnet グループの IP アドレスを表示します。

コマンドモード

Privileged Exec

例

```
Console#show management all-client
Management Ip Filter
 HTTP-Client:
   Start IP address      End IP address
-----------------------------------------------
1.192.168.1.19          192.168.1.19
2.192.168.1.25          192.168.1.30

 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------
1.192.168.1.19          192.168.1.19
2.192.168.1.25          192.168.1.30

 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
```

```
1.192.168.1.19          192.168.1.19
2.192.168.1.25          192.168.1.30

Console#
```

8.10 EAPOL の透過

本章では、スイッチで EAPOL フレームを中継するために使用されるコマンドについて説明します。

表 8-14 EAPOL 透過コマンド

コマンド	機能	モード
dot1x eapol-pass-through	スイッチの EAPOL フレームの中継を有効にします。	GC

8.10.1 dot1x eapol-pass-through

本コマンドでは、スイッチの EAPOL フレームの中継を有効にします。無効にするには、no 形式を使用してください。

構文

[no] dot1x eapol-pass-through

デフォルト設定

無効。EAPOL フレームを中継せず廃棄します。

コマンドモード

Global Configuration

コマンドの使用方法

- 本装置をクライアントと認証スイッチの間に設置する場合、dot1x eapol-pass-through コマンドにより IEEE802.1X 認証で使用される EAPOL フレームを中継できるので、認証スイッチと端末間で IEEE802.1X 認証を行うことができます。
- 本装置をエッジスイッチとして設置するが、いかなるクライアントに対しても認証が不要な場合、no dot1x eapol-pass-through コマンドで不要な EAPOL フレームを廃棄することができます。
- EAPOL フレーム透過の設定はコマンドラインインタフェースでのみ設定できます。
- DHCP snooping 機能と連携して、IP ソースガード機能を使用する場合、IP ソースガード機能は ACL モードを使用してください。

例

この例では、スイッチの EAPOL フレームの中継を有効にします。

```
Console(config)#dot1x eapol-pass-through
Console(config)#
```

9 セキュリティの設定

このスイッチは、各データポートに接続されたクライアントのトラフィックを分離し、許可されたクライアントだけがネットワークにアクセスできるようにするための方法をサポートしています。DHCP クライアントに割り当てられたアドレスは、IP ソースガードおよび DHCP スヌーピングコマンドを使用して慎重に制御することもできます

表 9-1 一般的なセキュリティコマンド

コマンドグループ	機能
ポートセキュリティ※	ポートのセキュアアドレスを設定します。
DHCPv4 スヌーピング※	DHCPv4 スヌーピングバインディングテーブルを構築して維持することによって、非セキュアポート上の信頼できない DHCPv4 メッセージをフィルタリングします。
IPv4 ソースガード※	DHCP スヌーピングまたは静的ソースバインディングを介して送信元アドレスを識別できない安全でないポート上の IP トラフィックをフィルタリングします。
ARP 検査	ARP パケットの MAC-to-IP アドレスバインディングを検証します。
DoS 攻撃プロテクション	Denial-of-Service 攻撃から保護します。
トラフィックセグメンテーション	指定されたダウンリンクおよびアップリンクポートにもとづいて、異なるクライアントセッションのトラフィックセグメンテーションを設定します。

注※ これらのフィルタリングコマンドの実行の優先順位は、ポートセキュリティ、アクセス制御リスト、DHCP スヌーピング、IPv4 ソースガードです。

9.1 ポートセキュリティ

これらのコマンドは、ポート上のポートセキュリティを有効にするために使用することができます。

インタフェース上で MAC アドレス学習が無効になっている場合、このポートの動的または静的アドレステーブルにすでに格納されている送信元アドレスを持つ受信トラフィックだけが、ネットワークへのアクセスを許可されます。

ポートセキュリティを使用すると、設定された最大数に達したときに、指定したポートで新しい MAC アドレスの学習が停止されます。このポートの動的または静的アドレステーブルにすでに格納されている送信元アドレスを持つ受信トラフィックだけが、ネットワークへのアクセスを許可されます。ポートは、未知の、または別のポートから以前に学習された送信元 MAC アドレスを持つ受信フレームを破棄します。許可されていない MAC アドレスを持つデバイスがスイッチポートを使用しようとすると、侵入が検出され、スイッチは自動的にポートを無効にしてトラップメッセージを送信することができます。

表 9-2 管理 IP フィルタコマンド

コマンド	機能	モード
mac-learning	選択した物理インタフェースまたは VLAN で、MAC アドレス学習を有効にします。	IC
port security	セキュアポートを設定します。	IC
show port security	ポートセキュリティステータスとセキュアアドレスカウントを表示します。	PE

9.1.1 mac-learning

本コマンドでは、選択したインタフェースで MAC アドレス学習を有効にします。MAC アドレス学習を無効にするには、no 形式を使用してください。

構文

[no] mac-learning

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネットまたはポートチャネル)

コマンドの使用方法

- no mac-learning コマンドは指定ポートまたはトラック上で、スイッチが新規に MAC アドレスを学習することを直ちに停止します。静的アドレステーブルに格納されていない送信元アドレスを持つ受信トラフィックは通信できません。ただし、DHCP スヌーピングなどのセキュリティ機能が有効になっていて MAC ラーニングが無効の場合、静的アドレステーブルに格納されている送信元アドレスの受信トラフィックだけが受け入れられ、その他のパケットはすべて廃棄されます。MAC アドレス学習が無効になったときにアドレステーブルに格納された動的アドレスは、システムから消去され、MAC アドレス学習が再度有効になるまで動的アドレスは学習されません。
- mac-learning コマンドは、同じインタフェース上で port security コマンドで MAC Address Security が有効になっている場合には使用することができません。

例

以下の例では、ポート 2 の MAC アドレス学習を無効にします。

```
Console(config)#interface ethernet 1/2
Console(config-if)#no mac-learning
Console(config-if)#
```

関連コマンド

show interfaces status

9.1.2 port security

本コマンドは、ポートセキュリティを有効または設定します。ポートセキュリティを無効にするには、キーワード無しで、no 形式を使用してください。適切なキーワードとともに no 形式を使用して、セキュリティ違反に対する応答または許可されたアドレスの最大数に対するデフォルト設定を復元します。

構文

port security [action {shutdown | trap | trap-and-shutdown} |

max-mac-count *address-count*]

no port security [action | max-mac-count]

action - ポートセキュリティが違反だった場合の対処方法です。

shutdown - ポートを無効にします。

trap - SNMP トラップメッセージを発行します。

trap-and-shutdown - SNMP トラップメッセージを発行してポートを無効にします。

max-mac-count

address-count - ポート上で学習できる最大 MAC アドレス数です。(範囲: 0 から 1024。0 は MAC アドレスの学習が無効になります)

デフォルト設定

ステータス: 無効

アクション: 無し

最大アドレス数: 0

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- セキュアポートで許可される MAC アドレスのデフォルト最大数はゼロです(例; ポートセキュリティは無効です)。ポートセキュリティを使用するには、port security max-mac-count コマンドを使用して、ポートで許可される最大アドレス数を設定する必要があります。
- port security コマンドを使用してポートセキュリティを有効にした場合、またはポートセキュリティを有効にした後で最大数または許可アドレスを現在の制限よりも小さい値に設定した場合、スイッチは

まず動的に学習されたエントリをアドレステーブルからすべてクリアします。指定されたポートで新しい MAC アドレスの学習を開始し、設定された最大数に達するとアドレス学習を停止します。 動的または静的アドレステーブルにすでに格納されている送信元アドレスを持つ受信トラフィックだけが、受け入れられます。

- ポートで学習できるアドレスエントリの最大数を設定するには、許可されている動的アドレスの最大数を指定します。スイッチは、ポートで受信したフレームの許可されたアドレスペアの最大数<送信元 MAC アドレス、VLAN>を学習します。(指定された最大アドレスカウントは、ポートセキュリティが有効または無効の場合に有効です。) mac-address-table static コマンドを使用すると、ポートにセキュアアドレスを手動で追加することができます。ポートが MAC アドレスの最大数に達すると、ポートは新しいアドレスの学習を停止します。すでにアドレステーブルにある MAC アドレスは保持され、期限切れになりません。
- ポートセキュリティが有効で、最大許容アドレス数がゼロ以外の値に設定されている場合、ポートの使用を試みているアドレステーブルにないすべてのデバイスが MAC アドレス数監視の対象となります。
- セキュリティ違反のためにポートが無効になっている場合には、no shutdown コマンドを使用して手動で再有効化する必要があります。
- セキュア MAC アドレスは、静的 MAC エントリとして保存され、エージングされません。
- セキュア MAC アドレスは、装置あたり最大 1024 となります。これは、mac-address-table static コマンドで設定した静的 MAC エントリとの合算になります。
- セキュアポートには以下の制限があります:
  - ネットワーク相互接続デバイスへの接続はできません。
  - トランクポートにすることはできません。
  - RSPAN とポートセキュリティは、相互に排他的な機能です。ポートセキュリティがポート上で有効な場合、ポートは RSPAN アップリンクポートとして設定することはできません。また、ポートが RSPAN アップリンクポートとして設定されている場合、送信元ポートまたは宛先ポート、ポートセキュリティはポート上で有効にできません。
  - MAC アドレス学習を無効化している状態では、ポートセキュリティは有効に出来ません。

例

以下の例では、ポート 5 のポートセキュリティを有効にし、トラップメッセージを発行するためにセキュリティ違反への応答を設定します:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

関連コマンド

show interfaces status

shutdown

mac-address-table static

9.1.3 show port security

本コマンドでは、ポートセキュリティステータスとセキュアアドレスカウントを表示します。

構文

show port security [interface *interface*]

interface - ポートインタフェースを指定します。

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

以下の例では、ポートセキュリティ設定と全ポートのセキュアアドレス数を表示します。

```
Console#show port security
Global Port Security Parameters
 Secure MAC Aging Mode : Disabled

Port Security Port Summary
 Port     Port Security Port Status  Intrusion Action  MaxMacCnt CurrMacCnt
 ------------------------------------------------------------------------
 Eth 1/ 1 Disabled      Secure/Down  None              0         2
 Eth 1/ 2 Enabled       Secure/Up    None              10        0
 Eth 1/ 3 Disabled      Secure/Down  None              0         0
 Eth 1/ 4 Disabled      Secure/Down  None              0         0
 Eth 1/ 5 Disabled      Secure/Down  None              0         0
 .
 .
 .
```

表 9-3 show port security - 表示説明

フィールド	説明
Port Security	設定ステータスです(有効または無効)。
Port Status	以下のオペレーションステータスです: ・Secure/Down - ポートセキュリティが無効です。 ・Secure/Up - ポートセキュリティが有効です。 ・Shutdown - ポートセキュリティ違反の応答のため、ポートはシャットダウンしています。
Intrusion Action	侵入に対するアクションの設定内容です。
MaxMacCnt	このインタフェースのアドレステーブルに格納できるアドレスの最大数です(動的または静的)。
CurrMacCnt	アドレステーブルの現在のセキュアエントリ数です。

以下の例では、指定ポートのポートセキュリティ設定とセキュアアドレス数を示しています。Last Intrusion MAC および Last Time Detected Intrusion MAC フィールドでは、最後に検出した侵入 MAC アドレスに情報について表示しています。これらのフィールドは、侵入が検出されなかったり、ポートセキュリティが無

効になっている場合には適用されません。MAC Filter ID フィールドは、Disabled 固定になります。

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
 Secure MAC Aging Mode : Disabled

Port Security Details
 Port                                : 1/2
 Port Security                       : Enabled
 Port Status                         : Secure/Up
 Intrusion Action                    : None
 Max MAC Count                       : 0
 Current MAC Count                   : 0
 MAC Filter                          : Disabled
 Last Intrusion MAC                  : NA
 Last Time Detected Intrusion MAC    : NA
Console#
```

以下の例では、検出された侵入に関する情報を示します。

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
 Secure MAC Aging Mode : Disabled

Port Security Details
 Port                                : 1/2
 Port Security                       : Enabled
 Port Status                         : Secure/Up
 Intrusion Action                    : None
 Max MAC Count                       : 0
 Current MAC Count                   : 0
 MAC Filter                          : Disabled
 Last Intrusion MAC                  : 00-10-22-00-00-01
 Last Time Detected Intrusion MAC    : 20XX/7/29 15:13:03
Console#
```

9.2 DHCPv4 スヌーピング

DHCPv4 スヌーピングにより、スイッチは不正な DHCPv4 サーバまたはポート関連の情報を DHCPv4 サーバに送信する他のデバイスからネットワークを保護できます。この情報は物理ポートに戻って IP アドレスを追跡する際に有益です。このセクションでは、DHCPv4 スヌーピングを設定するために使用されるコマンドについて説明します。

表 9-4 DHCP スヌーピングコマンド

コマンド	機能	モード
ip dhcp snooping	DHCP スヌーピングをグローバルに有効にします。	GC
ip dhcp snooping information option	DHCP Option 82 の使用を有効または無効にし、remote-id のフレームフォーマットを指定します。	GC
ip dhcp snooping information option encode no-subtype	Option 82 情報の中の CID / RID でのサブタイプとサブ長の使用を無効にします。	GC
ip dhcp snooping information option remote-id	リモート ID をスイッチの IP アドレス、MAC アドレス、または任意の文字列、TR-101 準拠のノード ID に設定するか、あるいは TR101 フィールドの最後から VLAN ID を削除します。	GC
ip dhcp snooping information option tr101 board-id	TR-101 構文にもとづいて、Option 82 情報で使用されるボード ID を設定します。	GC
ip dhcp snooping information policy	Option 82 情報を含む DHCP クライアントパケットの情報オプションポリシーを設定します。	GC
ip dhcp snooping verify mac-address	DHCP パケットに格納されているクライアントのハードウェアアドレスを、イーサネットヘッダーの送信元 MAC アドレスと照合して検証します。	GC
ip dhcp snooping vlan	指定 VLAN 上の DHCP スヌーピングを有効にします。	GC
ip dhcp snooping information option circuit-id	DHCP Option 82 情報サーキット ID サブオプションの使用を有効または無効にします。	IC
ip dhcp snooping max-number	インタフェースごとにサポートできる DHCP クライアントの最大数設定します。	IC
ip dhcp snooping trust	指定インタフェースを、信頼できるものとして設定します。	IC
clear ip dhcp snooping binding	DHCP スヌーピングバインディングテーブルエントリを RAM から消去します。	PE
clear ip dhcp snooping database flash	すべての動的に学習した、スヌーピングエントリをフラッシュメモリから消去します。	PE
ip dhcp snooping database flash	すべての動的に学習したスヌーピングエントリを、フラッシュメモリに書き込みます。	PE
show ip dhcp snooping	DHCP スヌーピングコンフィグレーションを表示します。	PE
show ip dhcp snooping binding	DHCP スヌーピングバインディングエントリを表示します。	PE

9.2.1 ip dhcp snooping

本コマンドは、DHCP スヌーピングをグローバルに有効にします。デフォルト設定に復元するには、no 形式を使用してください。

構文

[no] ip dhcp snooping

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- 悪意のある DHCP メッセージが外部の送信元から受信されると、ネットワークトラフィックが中断される可能性があります。DHCP スヌーピングは、ネットワークまたはファイアウォールの外側から非セキュアインタフェースで受信した DHCP メッセージをフィルタリングするために使用されます。このコマンドで DHCP スヌーピングをグローバルに有効にし、ip dhcp snooping vlan コマンドで VLAN インタフェースを有効にすると、(no ip dhcp snooping trust コマンドで指定された)信頼できないインタフェースで受信された DHCP メッセージは、 DHCP スヌーピングテーブルが破棄されます。
- 有効になった際、信頼できないインタフェースに入る DHCP メッセージは、DHCP スヌーピングを介して学習された動的エントリにもとづいてフィルタリングされます。
- テーブルエントリは、信頼されたインタフェースに対してのみ学習されます。各エントリには、MAC アドレス、IP アドレス、リース時間 VLAN 識別子、およびポート識別子が含まれています。
- DHCP スヌーピングが有効になると、スイッチが処理できる DHCP メッセージ数のレート制限は 100 パケット/秒です。この制限を超える DHCP パケットはすべて破棄されます。
- フィルタリングルールは以下のように導入します:
  - グローバル DHCP スヌーピングが無効の場合、すべての DHCP パケットが転送されます。
  - グローバル DHCP スヌーピングがグローバルに有効で、DHCP パケットが受信される VLAN 上でも有効な場合は、すべての DHCP パケットは信頼できるポートに転送されます。受信したパケットが DHCP ACK メッセージの場合には、動的 DHCP スヌーピングエントリもバインディングテーブルに追加されます。
  - DHCP スヌーピングがグローバルに有効化され、また DHCP パケットが受信される VLAN でも有効化されるが、ポートが信頼できない場合には、以下のように処理します:
    - DHCP パケットが DHCP サーバからのリプライパケット(OFFER、ACK または NAK メッセージを含む)の場合、パケットは破棄されます。
    - DHCP パケットが、DECLINE または RELEASE メッセージのようなクライアントからの場合、対応エントリがバインディングテーブルで見つかった時、スイッチはパケットのみを転送します。
    - DISCOVER、REQUEST、INFORM、DECLINE または RELEASE メッセージなどの DHCP パケットがクライアントからのものである場合、MAC アドレス検証が無効になっているとパケットが転送されます（ip dhcp snooping verify mac-address コマンドで指定）。ただし、MAC アドレス検証が有効な場合、DHCP パケットに格納されているクライアントのハードウェアアドレスがイーサネットヘッダーの送信元 MAC アドレスと同じである場合にのみ、パケットは転送されます
    - DHCP パケットが認識可能なタイプでない場合、これは破棄されます。
  - クライアントからの DHCP パケットが上記のフィルタリング基準を満たす場合、その VLAN は同じ VLAN 内の信頼できるポートにのみ転送されます。

- 信頼されたポートでサーバからの DHCP パケットが受信された場合、そのパケットは同じ VLAN 内の信頼できるポートと信頼されていないポートの両方に転送されます。

◆ DHCP スヌーピングがグローバルに無効になった場合、すべての動的バインディングはバインディングテーブルから消去されます。

◆ スイッチ自体が DHCP クライアントの場合の追加の考慮事項 - スイッチがクライアント要求を DHCP サーバに送信するポートは、信頼できるものとして設定する必要があります(ip dhcp snooping trust コマンドを使用)。 DHCP サーバから ACK メッセージを受信すると、スイッチはバインディングテーブルにダイナミックエントリを追加しません。 また、スイッチが DHCP クライアントパケットを送信すると、フィルタリングは行われません。 ただし、スイッチが DHCP サーバからメッセージを受信すると、信頼できないポートから受信したパケットはすべて廃棄されます。

例

以下の例では、スイッチの DHCP をグローバルに有効にします。

```
Console(config)#ip dhcp snooping
Console(config)#
```

関連コマンド

ip dhcp snooping vlan

ip dhcp snooping trust

9.2.2 ip dhcp snooping information option

本コマンドでは、スイッチの DHCP Option 82 情報の使用を有効にし、Option 82 情報がスイッチで生成されるときに使用されるフレームフォーマットを指定します。この機能を無効にするには、キーワードなしの no 形式を使用します。

構文

ip dhcp snooping information option

no ip dhcp snooping information option

デフォルト設定

Option 82: 無効

DHCP Snooping Information Option Sub-option Format: サブタイプを含む

DHCP Snooping Information Option Remote ID: MACアドレス(16進数)

コマンドモード

Global Configuration

コマンドの使用方法

◆ DHCP はスイッチの情報を送信するためのリレーメカニズムと、DHCP サーバへの DHCP クライアントについて提供します。DHCP Option 82 と呼ばれ、互換性のある DHCP サーバが IP アドレスを割り当てるときに情報を使用したり、クライアントに他のサービスまたはポリシーを設定したりすること

ができます。

- DHCP スヌーピング情報 Option 82 が有効になると、要求側のクライアント(または自身を記述するために情報フィールドを使用した中間のリレーエージェント）が、スイッチによって転送された DHCP 要求パケットと送信された応答パケット DHCP サーバから戻ってきます。
- DHCP スヌーピング情報オプションが有効になっている場合、クライアントは MAC アドレスではなく、接続先のスイッチポートで識別できます。DHCP クライアント/サーバ交換メッセージは、VLAN 全体にフラッディングすることなく、サーバとクライアント間で直接転送されます。
- DHCP Option 82 情報をパケットに挿入するには、DHCP スヌーピングを有効にする必要があります。有効にすると、スイッチは受信 DHCP パケットに Option 82 情報を追加/削除しますが、リレーすることはできません。 パケットは次のように処理されます。
  - 受信パケットがオプション 82 情報を含む DHCP 要求パケットである場合、ip dhcp snooping information policy コマンドで指定された設定に従って Option 82 情報を変更します。
  - 受信パケットが Option 82 情報の無い DHCP 要求パケットである場合、DHCP スヌーピング情報オプションを有効にすると、Option 82 情報がパケットに追加されます。
  - 受信パケットが Option 82 情報を持つ DHCP 応答パケットである場合、DHCP スヌーピング情報オプションを有効にすると、パケットから Option 82 情報が消去されます。

例

以下の例では、DHCP スヌーピング情報オプションを有効にします。

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

9.2.3 ip dhcp snooping information option encode no-subtype

本コマンドにより、スイッチによって生成された Option 82 情報のサーキット ID(CID)およびリモート ID(RID)のサブタイプおよびサブ長フィールドの使用を無効にします。これらのフィールドの使用を有効にするには、no 形式を使用してください。

構文

[no] ip dhcp snooping information option encode no-subtype

デフォルト設定

有効

コマンドモード

Global Configuration

コマンドの使用方法

このスイッチで使用されるサーキット識別子/リモート識別子は、sub-type から始まります。以下の情報が含まれています:

- sub-type - Option82 情報の異なるタイプを判別します。
- sub-length - Option82 情報対応の長さです。

- access node identifier –リモート ID サブオプションのデフォルトはスイッチ CPU の MAC アドレスです。
- eth –R-124 文字列の場合 2 つ目のフィールドは固定文字列“eth”です。
- slot - スロットは、このシステムのスタックユニットを表します。
- port - DHCP 要求を受信したポートです。パケットがトランクを介して到着した場合、値はトランクの ifIndex です。
- vlan - DHCP 要求を受信した VLAN のタグです。
- 上記で説明したデフォルト設定に変更するには、ip dhcp snooping information option circuit-id コマンドを使用することができます。

◆ TR101 オプション 82 のフォーマットは: “<IP> eth <SID>/<PORT>[:<VLAN>]”.SID(スイッチ ID)は常に 0 であることに留意してください。デフォルトでは、PVID はタグ無しパケットの TR101 フィールドの末尾に追加されます。タグ付きパケットの場合、VLAN ID は常に追加されます。

例

この例では、サーキット ID(CID)およびリモート ID(RID)のサブタイプおよびサブ長フィールドの使用を有効にします。

```
Console(config)#no ip dhcp snooping information option encode no-subtype
Console(config)#
```

9.2.4 ip dhcp snooping information option remote-id

本コマンドにより、リモート ID には、スイッチの IP アドレス、MAC アドレス、または任意の文字列、または TR-101 準拠のノード ID を設定します。また、TR101 フィールドの最後から VLAN ID を削除することを設定します。デフォルト設定に復元するには、no 形式を使用してください。

構文

ip dhcp snooping information option remote-id

{ip-address [encode {ascii | hex}] |

mac-address [encode {ascii | hex}] | string *string* |

tr101 {node-identifier {ip | sysname} | no-vlan-field}

no ip dhcp snooping information option remote-id

[ip-address encode] | [mac-address encode] | [tr101 no-vlan-field]

mac-address - DHCP スヌーピングエージェントのリモート ID サブオプション(スイッチの CPU の MAC アドレス)に MAC アドレスを挿入します。

ip-address - DHCP スヌーピングエージェントのリモート ID サブオプションに、IP アドレスを挿入します(管理インタフェースの IP アドレス)。

encode - ASCII または 16 進数コード化を指定します。

string - リモート識別子フィールドに挿入された任意の文字列です。(範囲: 1 から 32 文字)

tr101 node-identifier -スイッチにより生成されたリモート ID は、TR-101 構文をベースにします(R-124、Access_Node_ID)。

ip - ノード識別子として、スイッチの IP アドレスを指定します。

sysname - ノード識別子として、システム名を指定します。

tr101 no-vlan-field - タグ無しパケットの場合、TR101 フィールドに ":VLAN"を追加しません。

デフォルト設定

DHCP Snooping Information Option Remote ID: MACアドレス(16進数)

DHCP Snooping Information Option Remote ID TR101 VLANフィールド: 有効

コマンドモード

Global Configuration

コマンドの使用方法

TR101 オプション 82 のフォーマットは: “<IP> eth <SID>/<PORT>[:<VLAN>]”.SID(スイッチ ID)は常に 0 であることに留意してください。デフォルトでは、PVID はタグ無しパケットの TR101 フィールドの末尾に追加されます。タグ付きパケットの場合、VLAN ID は常に追加されます。タグなしパケットの場合、TR101 フィールドの最後から VLAN ID を削除するには、ip dhcp snooping information option remote-id tr101 no-vlan-field コマンドを使用します。TR101 フィールドの最後にタグなしパケットの PVID を追加するには、このコマンドの no 形式を使用してください。

例

この例では、スイッチの IP アドレスを、リモート ID に設定します。

```
Console(config)#ip dhcp snooping information option remote-id tr101 node-identifier ip
Console(config)#
```

9.2.5 ip dhcp snooping information option tr101 board-id

本コマンドにより、TR-101 の構文をもとに Option 82 情報の中で使用されるボード識別子を設定します。ボード識別子を削除するには、no 形式を使用してください。

構文

ip dhcp snooping information option tr101 board-id *board-id*

no ip dhcp snooping information option tr101 board-id

board-id - TR101 ボード ID.(範囲: 0 から 9)

デフォルト設定

未定義

コマンドモード

Global Configuration

例

この例では、ボード ID に 0 を設定します。

```
Console(config)#ip dhcp snooping information option tr101 board-id 0
Console(config)#
```

9.2.6 ip dhcp snooping information policy

本コマンドにより、オプション 82 情報を含む DHCP クライアントパケットの、DHCP スヌーピング情報オプションポリシーを設定します。デフォルト設定に復元するには、no 形式を使用してください。

構文

ip dhcp snooping information policy {drop | keep | replace}

drop - クライアント要求パケットを、リレーする代わりに破棄します。

keep - クライアント要求内の Option 82 情報を保持し、信頼できるポートに転送します。

replace - クライアント要求内の Option 82 情報の circuit-id フィールドと remote id フィールドをリレーエージェント自体に関する情報で置換し、リレーエージェントのアドレスを挿入し(DHCP スヌーピングが有効な場合)、パケットを信頼できるポートに転送します。

デフォルト設定

replace

コマンドモード

Global Configuration

コマンドの使用方法

スイッチが、DHCP オプション 82 情報を既に含んでいるクライアントから DHCP パケットを受信した際、これらのパケットのアクションポリシーを設定するために、スイッチを構成することができます。DHCP パケットをドロップするか、既存の情報を保持するか、スイッチのリレー情報で置換します。

例

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

9.2.7 ip dhcp snooping verify mac-address

本コマンドでは、DHCP パケットに格納されているクライアントのハードウェアアドレスをイーサネットヘッダーの送信元 MAC アドレスと照合して検証します。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip dhcp snooping verify mac-address

デフォルト設定

Enabled

コマンドモード

Global Configuration

コマンドの使用方法

MAC アドレス検証が有効で、パケットのイーサネットヘッダーの中のソース MAC アドレスが、DHCP パケットの中のクライアントハードウェアアドレスと異なる場合、パケットは破棄されます。

例

この例では、MAC アドレス検証を有効にします。

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

関連コマンド

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping trust

9.2.8 ip dhcp snooping vlan

本コマンドにより、指定した VLAN 上の DHCP スヌーピングを有効にします。デフォルト設定に復元するには、no 形式を使用してください。

構文

[no] ip dhcp snooping vlan *vlan-id*

vlan-id - 設定した VLAN の ID です。1 から 4094)

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- ip dhcp snooping コマンドを使用して DHCP スヌーピングがグローバルに有効で、且つこのコマンドで VLAN が有効な場合、DHCP パケットフィルタリングは、ip dhcp snooping trust コマンドで指定された VLAN 内の信頼できないポートで実行されます。
- DHCP スヌーピングがグローバルに無効になっている場合でも、特定の VLAN に対して DHCP スヌーピングを設定することはできますが、DHCP スヌーピングをグローバルに再度有効にするまでは変更

は反映されません。

◆ DHCP スヌーピングがグローバルに有効化され、VLAN 上で無効になると、この VLAN について学習されたすべての動的バインディングがバインディングテーブルから削除されます

例

この例では、VLAN1 の DHCP スヌーピングを有効にします。

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

関連コマンド

ip dhcp snooping

ip dhcp snooping trust

9.2.9 ip dhcp snooping information option circuit-id

本コマンドにより、DHCP Option 82 circuit-id サブオプション情報を指定します。デフォルト設定を使うには、no 形式を使用してください。

構文

ip dhcp snooping information option circuit-id

{string *string* | {tr101 {node-identifier {ip | sysname} |

no-vlan-field}

no dhcp snooping information option circuit-id [tr101 no-vlan-field]

string – サーキット ID フィールドに挿入された、任意の文字列です。(範囲: 1 から 32 文字)。

tr101 node-identifier- スイッチにより生成されたサーキット ID は、TR-101 システムをベースにします (R-124、Access_Node_ID)。

ip - ノード識別子として、スイッチの IP アドレスを指定します。

sysname - ノード識別子として、システム名を指定します。

tr101 no-vlan-field - タグ無しパケットの場合、TR101 フィールドに ":VLAN"を追加しません。

デフォルト設定

DHCP Snooping Information Option Circuit ID:VLAN ユニットポート

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

◆ DHCP はスイッチの情報を送信するためのリレーメカニズムと、DHCP サーバへの DHCP クライアントについて提供します。DHCP Option 82 では、互換性のある DHCP サーバが IP アドレスを割り当てる際に情報を使用したり、クライアントに他のサービスやポリシーを設定したりすることができます。この処理の詳細については、ip dhcp snooping information option コマンドの、「コマンドの使用」の

章を参照してください。

◆ スイッチによって生成された Option 82 情報は、下記を基本としています:

表 9-5 Option 82 情報

82	3-69	1	1-67	x1	x2	x3	x4	x5	x63
opt82	opt-len	sub-opt1	string-len	サーキット識別子					

このスイッチで使用されるサーキット識別子は、sub-type から始まります。以下の情報が含まれています:

- sub-type – サーキット ID の異なるタイプを判別します。
- sub-length – サーキット ID 対応の長さです。
- access node identifier サーキット ID
- eth - R-124 文字列の場合 2 つ目のフィールドは固定文字列“eth”です。
- slot - スロットは、このシステムのスタックユニットを表します。
- port - DHCP 要求を受信したポートです。パケットがトランクを介して到着した場合、値はトランクの ifIndex です。
- vlan - DHCP 要求を受信した VLAN のタグです。
- 上記で説明したデフォルト設定に変更するには、ip dhcp snooping information option circuit-id コマンドを使用することができます。

TR101 オプション 82 のフォーマットは: “<IP> eth <board-id>/<SID>/<PORT>[:<VLAN>]”.SID(スイッチ ID)は常に 1 であることに留意してください。デフォルトでは、PVID はタグ無しパケットの TR101 フィールドの末尾に追加されます。タグ付きパケットの場合、VLAN ID は常に追加されます。

例

この例では、DHCP スヌーピング情報の circuit-id サブオプション文字列を設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip dhcp snooping information option circuit-id string 4500
Console(config-if)#
```

9.2.10 ip dhcp snooping max-number

本コマンドでは、インタフェースごとに停止できる DHCP クライアントの最大数を設定します。デフォルト設定に復元するには、no 形式を使用してください。

構文

ip dhcp snooping max-number *max-number*

no dhcp snooping max-number

max-number - DHCP クライアントの最大数です。(範囲: 1 から 32)

デフォルト設定

16

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

例

この例では、ポート 1 から 2 でサポートされる DHCP クライアントの最大数を設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip dhcp snooping max-number 2
Console(config-if)#
```

9.2.11 ip dhcp snooping trust

本コマンドでは、指定されたインタフェースを信頼できるものとして設定します。デフォルト設定に復元するには、no 形式を使用してください。

構文

[no] ip dhcp snooping trust

デフォルト設定

すべてのインタフェースは信頼できません。

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- 信頼できるインタフェースは、ネットワーク内からのメッセージのみを受信するように設定されたインタフェースです。信頼できないインタフェースとは、ネットワークの外側、またはファイアウォールからのメッセージを受信するように設定されたインタフェースです。
- ローカルネットワークまたはファイアウォール内の DHCP サーバに接続されているすべてのポートを信頼できるものに設定し、ローカルネットワークまたはファイアウォール外の他のすべてのポートは信頼できないものに設定します。
- ip dhcp snooping コマンドを使用して DHCP スヌーピングをグローバルにイネーブルにし、VLAN 上で ip dhcp snooping vlan コマンドを使用してイネーブルにし、DHCP パケットフィルタリングは、デフォルト状態に応じて、または no ip dhcp snooping trust コマンドを使用してインタフェース用に設定されたとおりに、VLAN 内の信頼できないポートで実行されます。
- 信頼できないポートが信頼できるポートに変更される場合、ポートに関連するすべての動的 DHCP スヌーピングバインディングは削除されます。
- スイッチ自体が DHCP クライアントだった場合の、追加考慮点 - クライアント要求を DHCP サーバに送信する際に使用するポートは、信頼できるものとして設定する必要があります。

例

この例では、ポート 5 を信頼できないものとして、設定します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

関連コマンド

ip dhcp snooping

ip dhcp snooping vlan

9.2.12 clear ip dhcp snooping binding

本コマンドでは、RAM からの DHCP スヌーピングバインディングエントリをクリアします。バインディングテーブルからすべてのエントリをクリアするには、オプションのキーワード無しでこのコマンドを使用してください。

構文

clear ip dhcp snooping binding *mac-address ip-address*

mac-address - MAC アドレスエントリを指定します。(形式: xx-xx-xx-xx-xx-xx)

ip-address - このエントリにバインドしている IP アドレスを指定します。

コマンドモード

Privileged Exec

例

```
Console#clear ip dhcp snooping binding 11-22-33-44-55-66 vlan 1
Console#
```

9.2.13 clear ip dhcp snooping database flash

本コマンドでは、動的に学習したすべてのスヌーピングエントリを、フラッシュメモリから削除します。

コマンドモード

Privileged Exec

例

```
Console#clear ip dhcp snooping database flash
Console#
```

9.2.14 ip dhcp snooping database flash

本コマンドでは、動的に学習したすべてのエントリをフラッシュメモリに書き込みます。

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドでは、現在学習している動的 DHCP スヌーピングエントリをフラッシュメモリに保存することができます。スイッチがリセットされると、これらのエントリはスヌーピングテーブルに復元されます。ただし、フラッシュメモリから復元された動的エントリのリース期間は有効ではなくなります。

例

```
Console#ip dhcp snooping database flash
Console#
```

9.2.15 show ip dhcp snooping

本コマンドでは、DHCP スヌーピングコンフィグレーションを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp snooping
Global DHCP Snooping Status: disabled
DHCP Snooping Information Option Status: disabled
DHCP Snooping Information Option Sub-option Format: extra subtype included
DHCP Snooping Information Option Remote ID: MAC Address (hex encoded)
DHCP Snooping Information Option Remote ID TR101 VLAN Field: enabled
DHCP Snooping Information Option TR101 Board ID: none
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:

Verify Source MAC-Address: enabled
                            Circuit-ID      Circuit-ID    Circuit-ID
Interface Trusted Max-Number Mode            Value         TR101 VLAN Field
--------- ------- ---------- --------------- ------------  ----------------
Eth 1/1   No      16         VLAN-Unit-Port  ---           enabled
Eth 1/2   No      16         VLAN-Unit-Port  ---           enabled
Eth 1/3   No      16         VLAN-Unit-Port  ---           enabled
Eth 1/4   No      16         VLAN-Unit-Port  ---           enabled
Eth 1/5   No      16         VLAN-Unit-Port  ---           enabled
.
.
.
```

9.2.16 show ip dhcp snooping binding

本コマンドでは、DHCP スヌーピングバインディングエントリを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp snooping binding
MAC Address       IP Address      Lease(sec) Type                VLAN Interface
----------------- --------------- ---------- ------------------- ---- ---------
11-22-33-44-55-66 192.168.0.99         26121 dhcp-snooping          13 Eth 1/1
Console#
```

9.3 IPv4 ソースガード

IPv4 ソースガードは、IPv4 ソースガードテーブルの手動で設定されたエントリ、または有効になっている場合の DHCPv4 スヌーピングテーブルの動的エントリにもとづいて、ネットワークインタフェース上の IPv4 トラフィックをフィルタリングするセキュリティ機能です。IPv4 ソースガードは、ホストが隣接した IPv4 アドレスを使用してネットワークにアクセスしようとした時に発生するトラフィック攻撃を防止するために使用することができます。本章では、IPv4 ソースガードの設定に使用するコマンドについて説明します。このセクションでは、IPv4 スヌーピングを設定するために使用されるコマンドについて説明します。

表 9-6 IPv4 ソースガードコマンド

コマンド	機能	モード
ip source-guard binding	静的アドレスをソースガードバインディングテーブルに追加します。	GC
ip source-guard	インバウンドトラフィックをフィルタリングするためのスイッチを、ソース IP アドレス、またはソース IP アドレスと対応する MAC アドレスをベースに設定します。	IC
ip source-guard max-binding	インタフェースにバウンドすることができる、最大エントリ数を設定します。	IC
ip source-guard mode	ソースガード学習モードを設定して、ACL バインディングテーブルまたは MAC アドレスバインディングテーブルのアドレスを検索します。	IC
clear ip source-guard binding blocked	すべてのブロックされた記録を削除します。	PE
show ip source-guard	各インタフェースにおいて、ソースガードが有効または無効になっているについて表示します。	PE
show ip source-guard binding	ソースガードバインディングテーブルを表示します。	PE

9.3.1 ip source-guard binding

本コマンドでは、ソースガード ACL または MAC アドレスバインディングテーブルに静的アドレスを追加します。静的エントリを削除するには、no 形式を使用してください。

構文

ip source-guard binding [mode {acl | mac}] *mac-address*

vlan *vlan-id ip-address* interface ethernet *unit/port-list*

no ip source-guard binding [mode {acl | mac}] *mac-address ip-address*

mode - バインディングモードを指定します。

acl - ACL テーブルにバインディングを追加します。

mac - MAC アドレステーブルにバインディングを追加します。

mac-address - 有効なユニキャスト MAC アドレス

vlan-id - ACL フィルタリングテーブル用に設定された VLAN の ID、または MAC アドレスフィルタリングテーブル用の VLAN の範囲です。リストを指定するには、コンマで区切りスペースを含まない非連続 VLAN 識別子を分離します; ハイフンを使用して ID の範囲を指定します。(範囲: 1 から 4094)

ip-address - クラスタイプ A、B または C を含む有効ユニキャスト IP アドレスです。

unit - ユニット識別子です。(範囲: 1)

port-list - 物理ポート番号またはポート番号のリストです。非連続ポート番号をコンマで区切り、スペースは入れないでください; ハイフンを使用してポート番号の範囲を指定することもできます。(範囲: 1 から 10)

デフォルト設定

設定されていないエントリ

コマンドモード

Global Configuration

コマンドの使用方法

- バインディングモードがこのコマンドで指定されない場合、エントリはデフォルトで ACL テーブルにバインドされます。
- MAC アドレス、IP アドレス、リースタイム、エントリタイム(静的 IP-SG バインディング、動的 DHCP バインディング)を含むテーブルエントリです。
- すべての静的エントリは、無期限のリース時間を使用して設定されます。これは、show ip source-guard コマンドによってゼロの値で示されます。
- ソースガードが有効な場合、トラフィックは DHCP スヌーピングか、またはこのコマンドを使用してソースガードバインディングテーブルで設定されている静的アドレスを介して学習した、動的エントリをベースにフィルタリングされます。
- 同じ MAC アドレスと異なる VLAN ID を持つエントリを、バインディングテーブルに追加することはできません。
- 静的バインディングは、以下のように処理されます:
  - 下記の条件のうちの一つが正しい場合、有効な静的 IP ソースガードエントリは、ACL モードの中のバインディングテーブルに追加されます:
    - 同じ VLAN ID および MAC アドレスでバインディングエントリが無い場合、静的 IP ソースガードバインディングを使用して、新しいエントリがバインディングテーブルに追加されます。
    - 同じ VLAN ID および MAC アドレスでエントリがあり、エントリタイプが静的 IP ソースガードバインディングの場合には、新規のエントリが古いエントリと置換されます。
    - 同じ VLAN ID および MAC アドレスでエントリがあり、エントリタイプが動的 DHCP スヌーピングバインディングの場合には、新規のエントリが古いエントリと置き換えられ、エントリタイプが静的 IP ソースガードバインディングに変更されます。
  - 下記の条件のうちの一つが正しい場合、有効な静的 IP ソースガードエントリは、MAC モードのバインディングテーブルに追加されます:
    - 同じ IP アドレスおよび MAC アドレスでバインディングエントリが無い場合、静的 IP ソースガードバインディングエントリを使用して、新しいエントリがバインディングテーブルに追加されます。
    - 同じ IP アドレスおよび MAC アドレスでエントリがある場合、新規のエントリが古いエントリと置換されます。
- 静的バインディングには、ユニキャストアドレスのみが受け入れられます。

例

この例では、ポート 5 における静的ソースガードバインディングを設定します。バインディングモードが指定されていないため、エントリはデフォルトで ACL テーブルにバインディングされます。

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1 192.168.0.99 interface
ethernet 1/5
Console(config-if)#
```

関連コマンド

ip source-guard

ip dhcp snooping

ip dhcp snooping vlan

9.3.2 ip source-guard

本コマンドでは、ソース IP アドレス、ソース IP アドレス、および対応する MAC アドレスにもとづいて、インバウンドトラフィックをフィルタリングするようにスイッチを設定します。この機能を無効にするには、no 形式を使用してください。

構文

ip source-guard {sip | sip-mac}

no ip source-guard

sip - バインディングテーブルに格納されている IP アドレスをベースに、トラフィックをフィルタリングします。

sip-mac - バインディングテーブルに格納されている IP アドレスと対応する MAC アドレスをベースに、トラフィックをフィルタリングします。

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- ソースガードは、ネットワークまたはファイアウォールの外部からのメッセージを受信する安全でないポート上のトラフィックをフィルタリングするために使用されるため、隣接の IP アドレスを使用しようとするホストによって引き起こされるトラフィック攻撃を受ける可能性があります。
- sip または sip-mac にソースガードを設定することにより、選択したポートで機能を有効にします。sip オプションを使用して、バインディングテーブルのすべてのエントリに対して VLAN ID、ソース IP アドレス、およびポート番号を確認します。sip-mac オプションを使用してこれらの同じパラメータとソース MAC アドレスを確認します。選択したポートでこの機能を無効にするには、no ip source guard コマンドを使用してください。
- 有効にすると、トラフィックは DHCP スヌーピングを介して学習した動的エントリ、またはソース

ガードバインディングテーブルの中に設定した静的アドレスをベースに、フィルタリングします。

- テーブルエントリは、MAC アドレス、IP アドレス、リースタイム、エントリタイプ(静的 IP-SG バインディング、動的 DHCP バインディング、VLAN 識別子、およびポート識別子)を含みます。
- ip source-guard binding コマンドを使用してソースガードバインディングテーブルに入力された静的アドレスは、無期限のリース時間で自動的に設定されます。DHCP スヌーピングを介して学習された動的エントリは、DHCP サーバ自体によって設定されます。
- IP ソースガードが有効になると、インバウンドパケットの IP アドレス(sip オプション)または IP アドレスと対応する MAC アドレス(sip-mac オプション)の両方がバインディングテーブルと照合されます。　一致するエントリが見つからない場合には、パケットは破棄されます。
- フィルタリングルールは以下のように導入します:
  - DHCPv4 スヌーピングが無効になると、IP ソースガードは、VLAN ID、ソース IP アドレス、ポート番号、およびソース MAC アドレス(sip-mac オプション)をチェックします。　一致するエントリがバインディングテーブルに見つかり、エントリタイプが静的 IP ソースガードバインディングの場合には、パケットは転送されます。
  - DHCP スヌーピングが有効になっている場合、IP ソースガードは VLAN ID、ソース IP アドレス、ポート番号、およびソース MAC アドレス(sip-mac オプション)をチェックします。一致するエントリがバインディングテーブルに見つかり、エントリタイプが静的 IP ソースガードバインディングまたは動的 DHCP スヌーピングバインディングの場合には、パケットは転送されます。
  - IP ソースバインディング(DHCP スヌーピングまたは手動設定によって動的に学習された)がまだ設定されていないインタフェースで IP ソースガードが有効になっている場合、スイッチは DHCP スヌーピングで許可された DHCP パケットを除いて、ポート上のすべての IP トラフィックを破棄します。
  - 静的バインディングには、ユニキャストアドレスのみが受け入れられます。

例

この例では、ポート 5 の IP ソースガードを有効にします。

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

関連コマンド

ip source-guard binding

ip dhcp snooping

ip dhcp snooping vlan

9.3.3 ip source-guard max-binding

本コマンドでは、インタフェースにバインディングすることができる、最大エントリ数を設定します。デフォルト設定に復元するには、no 形式を使用してください。

構文

ip source-guard [mode {acl | mac}] max-binding *number*

no ip source-guard [mode {acl | mac}] max-binding

mode - 学習モードを指定します。

acl - ACL テーブル内のアドレスを検索します。

mac - MAC アドレステーブル内のアドレスを検索します。

number - バインディングテーブルのインタフェースにマッピングできる、最大 IP アドレス数です。(範囲: ACL モードは 1 から 5; MAC モードは 1 から 32)

デフォルト設定

モード: ACL、最大バインディング数: 5

モード: MAC、最大バインディング数: 16

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- 本コマンドでは、DHCP スヌーピングによって検出された動的エントリ、および ip source-guard コマンドによって設定された静的エントリを含む指定されたモード(ACL バインディングテーブルまたは MAC アドレステーブル)のバインディングテーブルのインタフェースにマップできるアドレスエントリの最大数を設定します。
- ACL モードの最大バインディングは、ポートごとの「アクティブな」エントリの数を制限します。バインディングエントリが IP ソースガードの最大数を超える場合、バインディングエントリの最大数だけが設定されます。最大数を超える動的バインディングエントリが作成されますが、アクティブではありません。
- MAC モードの最大バイディングは、ポートごとに学習した MAC アドレスの数を制限します。ソース MAC アドレスが異なる認証済み IP トラフィックは、この最大数を超えると学習することができません。

例

この例では、ポート 5 のバインディングテーブルに許可されているエントリの最大数を 1 つのエントリに設定します。モードは指定されていないため、デフォルトで ACL バインディングテーブルが使用されます。

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
Console(config-if)#
```

9.3.4 ip source-guard mode

本コマンドでは、ACL バインディングテーブルまたは MAC アドレスバインディングテーブルに中のアドレスを検索するために、ソースガード学習モードを設定します。デフォルト設定に復元するには、no 形式を使用してください。

構文

ip source-guard mode {acl | mac}

no ip source-guard mode

mode - 学習モードを指定します。

acl - ACL バインディングテーブルの中のアドレスを検索します。

mac - MAC アドレステーブルの中のアドレスを検索します。

デフォルト設定

ACL

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

フィルタリングテーブルには、以下 2 つのモードがあります:

- ACL - IP トラフィックは、ACL モードバインディングテーブルのチェックプロセスにパスすると転送されます。
- MAC - IP トラフィックが MAC モードバインディングテーブルのチェックプロセスにパスすると、MAC エントリが MAC アドレステーブルに追加されます。

例

本コマンドでは、指定したインタフェースのバインディングテーブルモードを MAC モードに設定します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard mode mac
Console(config-if)#
```

9.3.5 clear ip source-guard binding blocked

本コマンドでは、RAM からソースガードバインディングテーブルエントリをクリアします。

構文

clear ip source-guard binding blocked

コマンドモード

Privileged Exec

コマンドの使用方法

IP ソースガードが無効なパケットを検出すると、ブロックされたレコードが作成されます。これらのレコードは、show ip source-guard binding blocked コマンドを使用して表示することができます。スイッチが新しいブロックレコードで最も古いレコードを上書きする前に、最大 512 のブロックレコードを保存できます。このテーブルをクリアするには、clear ip source-guard binding blocked コマンドを使用します。

例

本コマンドでは、ブロックされたレコードテーブルをクリアします。

```
Console(config)#clear ip source-guard binding blocked
Console(config)#
```

9.3.6 show ip source-guard

本コマンドでは、各インタフェースにおいてソースガードが有効になっているか、無効になっているかを表示します。各インタフェースにおいて、ソースガードが有効または無効になっているについて表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip source-guard
                                          ACL Table     MAC Table
Interface   Filter-type   Filter-table    Max-binding   Max-binding
---------   -----------   ------------    -----------   -----------
Eth 1/1     Disabled      ACL                       5            16
Eth 1/2     Disabled      ACL                       5            16
Eth 1/3     Disabled      ACL                       5            16
Eth 1/4     Disabled      ACL                       5            16
Eth 1/5     Disabled      ACL                       5            16
.
.
```

9.3.7 show ip source-guard binding

本コマンドでは、ソースガードバインディングテーブルを表示します。

構文

show ip source-guard binding [dhcp-snooping | static [acl | mac] |

blocked [vlan *vlan*-id | interface *interface*]

dhcp-snooping - DHCP スヌーピングコマンドで設定した動的エントリを表示します。

static - ip source-guard binding コマンドで設定した静的エントリを表示します。

acl - ACL バインディングテーブルの中の静的エントリを表示します。

mac - MAC アドレスバインディングテーブルの中の静的エントリを表示します。

blocked - IP ソースガードによりブロックされている MAC アドレスを表示します。

vlan-id - 設定した VLAN の ID です。(範囲: 1 から 4094)

interface - ポートインタフェースを指定します。

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

```
Console#show ip source-guard binding
MAC Address       IP Address      Type           VLAN      Interface
----------------- --------------- -------------- --------- ---------
00-12-e2-f4-d0-01 10.2.44.96      static-acl             1 Eth 1/1
Console#
```

9.4 ARP 検査

ARP 検査では、アドレス解決プロトコル(ARP)パケットの MAC-to-IP アドレスバインディングを検証します。特定の "man-in-the-middle"攻撃の基盤となる無効なアドレスバインディングで ARP トラフィックを保護します。これはすべての ARP 要求と応答を傍受し、ローカル ARP キャッシュが更新されるか、またはパケットが適切な宛先に転送される前にこれらのパケットのそれぞれを検証し、無効な ARP パケットを破棄します。

ARP 検査では、信頼できるデータベース(DHCP スヌーピングバインディングデータベース)に格納されている有効な IP-MAC アドレスバインディングにもとづいて、ARP パケットの妥当性を判断します。 ARP 検査では、静的に設定された IP アドレスを持つホストのユーザ設定 ARP アクセス制御リスト(ACL)に対して ARP パケットを検証することもできます。

本章では、ARP 検査の設定に使用されるコマンドについて説明します。

表 9-7 ARP 検査コマンド

コマンド	機能	モード
ip arp inspection	ARP 検査をスイッチにおいて、グローバルに有効化します。	GC
ip arp inspection filter	1 つ以上の VLAN に適用するために、ARP ACL を指定します。	GC
ip arp inspection log-buffer logs	ログメッセージに保存されるエントリの最大数を設定し、これらのメッセージのレートが送信されます。	GC
ip arp inspection validate	ARP パケット内のアドレスコンポーネントの追加検証を指定します。	GC
ip arp inspection vlan	指定 VLAN または VLAN の範囲の ARP 検査を有効にします。	GC
ip arp inspection limit	ポートで受信した ARP パケットのレート制限を設定します。	IC
ip arp inspection trust	ポートを信頼できるものとして設定し、ARP 検査を免除します。	IC
show ip arp inspection configuration	ARP 検査のグローバルコンフィグレーションを表示します。	PE
show ip arp inspection interface	ポートの信頼ステータスと検査レートを表示します。	PE
show ip arp inspection log	関連 VLAN、ポートおよびアドレスコンポーネントを含む、ログに保管されたエントリ情報を表示します。	PE
show ip arp inspection statistics	処理された、あるいはあらゆる理由により破棄された ARP パケット数の統計を表示します。	PE
show ip arp inspection vlan	ARP 検査ステータス、ARP ACL 名、および ACL 検証が完了した後で DHCP スヌーピングデータベースが使用されているかどうかなど、VLAN の設定を表示します。	PE

9.4.1 ip arp inspection

以下の例では、スイッチの DHCP をグローバルに有効にします。この機能を無効にするには、no 形式を使用してください。

構文

本コマンドでは、スイッチ上で ARP 検査をグローバルに有効化します。

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- このコマンドで ARP 検査がグローバルに有効になって場合、ip arp inspection vlan コマンドで有効になっている VLAN 上でのみアクティブになります。
- ARP 検査がグローバルに有効化され選択された VLAN で有効になると、それらの VLAN 上のすべての ARP 要求パケットとリプライパケットが CPU にリダイレクトされ、そのスイッチングは ARP 検査エンジンによって処理されます。
- ARP 検査がグローバルに無効になると、ARP 検査が有効になっている VLAN を含むすべての VLAN で非アクティブになります。
- ARP 検査が無効になると、すべての ARP 要求および応答パケットは ARP 検査エンジンをバイパスし、そのスイッチング方式は他のすべてのパケットのものと一致します。
- グローバル ARP 検査を無効にして再度有効にしても、すべての VLAN の ARP 検査設定には影響しません。
- ARP 検査をグローバルに無効にした場合、個々の VLAN に対して ARP 検査を設定することは可能です。　これらの設定変更は、ARP 検査がグローバルに再度有効にされた後にのみアクティブになります。

例

```
Console(config)#ip arp inspection
Console(config)#
```

9.4.2 ip arp inspection filter

本コマンドでは、1 つ以上の VLAN に適用するために ARP ACL を指定します。ACL バインディングを削除するには、no 形式を使用してください。ACL バインディングを削除するには、no 形式を使用してください。

構文

ip arp inspection filter *arp-acl-name* vlan {*vlan-id* | *vlan-range*} [static]

no ip arp inspection filter *arp-acl-name* vlan {*vlan-id* | *vlan-range*}

arp-acl-name - ARP ACL の名称です。(最長: 16 文字)

vlan-id - VLAN ID.(範囲: 1 から 4094)

vlan-range - ハイフンを使用して指定された VLAN の連続範囲、または各エントリがコンマで区切られたランダムな VLAN グループです。

static - ARP パケットは指定された ACL に対してのみ検証され、DHCP スヌーピングデータベースのアドレスバインディングはチェックされません。

デフォルト設定

ARP ACL はどの VLAN にもバインディングされていません。

静的モードは有効になっていません。

コマンドモード

Global Configuration

コマンドの使用方法

- ARP ACL のコマンドについては、「10.4 ARP ACLs」を参照してください。
- 静的モードが有効な場合、スイッチは ARP パケットを指定された ARP ACL と比較します。許可または拒否ルール内の IP-MAC アドレスバインディングに一致するパケットは、それに応じて処理されます。ACL ルールに一致しないパケットは廃棄されます。DHCP スヌーピングデータベースのアドレスバインディングはチェックされません。
- 静的モードが無効な場合、パケットは指定された ARP ACL に対して最初に検証されます。拒否ルールに一致するパケットは破棄されます。残りのすべてのパケットは、DHCP スヌーピングデータベース内のアドレスバインディングに対して検証されます。

例

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

9.4.3 ip arp inspection log-buffer logs

本コマンドでは、ログメッセージに保存されている最大エントリ数と、これらのメッセージが送信されるレートを設定します。デフォルト設定に復元するには、no 形式を使用してください。

構文

ip arp inspection log-buffer logs *message-number* interval *seconds*

no ip arp inspection log-buffer logs

message-number - ログメッセージに保存されている最大エントリ数です。(範囲: 0 から 256。0 はイベントが保存されておらず、メッセージが送信されていないことを意味しています。)

seconds - ログメッセージが送信される間隔です。(範囲: 0 から 86400)

デフォルト設定

メッセージ番号: 20

間隔: 10 秒

コマンドモード

Global Configuration

コマンドの使用方法

- ARP 検査は、コマンドがスイッチに受け入れられる前に、ip arp inspection コマンドで有効にする必要があります。
- デフォルトでは、ARP 検査のロギングはアクティブであり、無効にすることはできません。
- スイッチがパケットを破棄する際、ログバッファにエントリを配置します。各エントリには、受信 VLAN、ポート番号、送信元および宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスなどのフロー情報が含まれています。
- 複数の同一の無効な ARP パケットが同じ VLAN 上で連続して受信された場合、ロギングファシリティはログバッファに一つのエントリとそれに対応するシステムメッセージのみを生成します。
- ログバッファに格納できるエントリの最大数は、message-number パラメータによって決定されます。メッセージが送信される前にログバッファが満杯になると、最も古いエントリが最新のものに置き換えられます。
- スイッチは、秒単位の値によって決まるレート制御の基準でシステムメッセージを生成します。システムメッセージが生成されると、すべてのエントリがログバッファからクリアされます。

例

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

9.4.4 ip arp inspection validate

本コマンドにより、ARP パケット内のアドレスコンポーネントの追加検証を指定します。デフォルト設定に復元するには、no 形式を使用してください。

構文

ip arp inspection validate

{dst-mac [ip [allow-zeros] [src-mac]] |

ip [allow-zeros] [src-mac]] | src-mac}

no ip arp inspection validate

dst-mac - イーサネットヘッダーの宛先 MAC アドレスを ARP 本体のターゲット MAC アドレスと照合します。このチェックは、ARP 応答に対して実行されます。有効にした場合、MAC アドレスの異なるパケットは無効と分類され廃棄されます。

ip - ARP 本体の無効で予期しない IP アドレスを確認します。アドレスには、0.0.0.0,255.255.255.255、およびすべての IP マルチキャストアドレスが含まれます。送信者 IP アドレスはすべての ARP 要求と応答でチェックされ、ターゲット IP アドレスは ARP 応答でのみチェックされます。

allow-zeros - 送信者 IP アドレスが 0.0.0.0 となることを許可します。

src-mac -イーサネットヘッダーの送信元 MAC アドレスを ARP 本体の送信側 MAC アドレスと照合します。このチェックは、ARP 要求と応答の両方で実行されます。　有効にした場合、MAC アドレスの異なるパケットは無効と分類され廃棄されます。

デフォルト設定

追加検証は実施されません。

コマンドモード

Global Configuration

コマンドの使用方法

デフォルトでは、ARP 検証は ARP ACL または DHCP スヌーピングデータベースで指定された、IP-MAC アドレスバインディングのみチェックします。

例

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

9.4.5 ip arp inspection vlan

本コマンドでは、指定した VLAN または VLAN の範囲に対して ARP 検査を有効にします。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip arp inspection vlan {*vlan-id* | *vlan-range*}

vlan-id - VLAN ID.(範囲: 1 から 4094)

vlan-range - ハイフンを使用して指定された VLAN の連続範囲、または各エントリがコンマで区切られたランダムな VLAN グループです。

デフォルト設定

すべての VLAN において無効です。

コマンドモード

Global Configuration

コマンドの使用方法

- ip arp inspection コマンドで ARP 検査がグローバルに有効になっている場合、このコマンドで有効になっている VLAN のみアクティブになります。
- ARP 検査がグローバルに有効化され選択された VLAN で有効になると、それらの VLAN 上のすべての ARP 要求パケットとリプライパケットが CPU にリダイレクトされ、そのスイッチングは ARP 検査エンジンによって処理されます。
- ARP 検査がグローバルに無効になると、ARP 検査が有効になっている VLAN を含むすべての VLAN で非アクティブになります。
- ARP 検査が無効になると、すべての ARP 要求および応答パケットは ARP 検査エンジンをバイパスし、そのスイッチング方式は他のすべてのパケットのものと一致します。
- グローバル ARP 検査を無効にして再度有効にしても、すべての VLAN の ARP 検査設定には影響しません。
- ARP 検査をグローバルに無効にした場合、個々の VLAN に対して ARP 検査を設定することは可能です。これらの設定変更は、ARP 検査がグローバルに再度有効にされた後にのみアクティブになりま

す。

例

```
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

9.4.6 ip arp inspection limit

本コマンドにより、ポート上で受信した ARP パケットのレート制限を設定します。デフォルト設定に復元するには、no 形式を使用してください。

構文

ip arp inspection limit {rate *pps* | none}

no ip arp inspection limit

pps - 信頼できるまたは信頼できないポート上で 1 秒間あたりに CPU で処理が可能な、最大 ARP パケット数です。(範囲: 0 から 2048、0 は ARP パケットを転送できないことを意味します。)

none - CPU が処理できる ARP パケットの数に制限はありません。

デフォルト設定

15

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- 本コマンドは、信頼できるポートと信頼できないポートの両方に適用されます。
- ARP パケットの受信レートが設定制限を超えた場合、スイッチは、制限を超えたすべての ARP パケットを廃棄します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit rate 150
Console(config-if)#
```

9.4.7 ip arp inspection trust

本コマンドでは、ポートを信頼できるポートとして設定し、ARP 検査を免除します。デフォルト設定に復元するには、no 形式を使用してください。

構文

[no] ip arp inspection trust

デフォルト設定

信頼できない

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

信頼できないポートに到着したパケットは、設定された ARP 検査および追加の妥当性チェックの対象となります。信頼できるポートに到着したパケットは、これらのチェックをすべて回避し通常のスイッチングルールに従って転送されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

9.4.8 show ip arp inspection configuration

本コマンドでは、ARP 検査のグローバルコンフィグレーションを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection configuration

ARP Inspection Global Information:

Global IP ARP Inspection Status : disabled
Log Message Interval            : 1 s
Log Message Number              : 5
Need Additional Validation(s)   : Yes
Additional Validation Type      : Destination MAC address
Console#
```

9.4.9 show ip arp inspection interface

本コマンドでは、ポートの信頼ステータスおよび ARP 検査レートを表示します。

構文

show ip arp inspection interface [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection interface ethernet 1/1

Port Number        Trust Status             Rate Limit (pps)
-------------   --------------------    -------------------------------
Eth 1/1            Trusted                   150
Console#
```

9.4.10 show ip arp inspection log

本コマンドでは、関連する VLAN、ポート、およびアドレスコンポーネントを含め、ログに保存されているエントリに関する情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port Src IP Address  Dst IP Address  Src MAC Address  Dst MAC Address
--- ---- ---- --------------  --------------  ---------------  ---------------
1   1     11  192.168.2.2     192.168.2.1     00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF
Console#
```

9.4.11 show ip arp inspection statistics

本コマンドでは、あらゆる理由で処理または破棄された ARP パケット数に関する統計情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection statistics

ARP packets received                                              : 150
ARP packets dropped due to rate limt                              : 5
Total ARP packets processed by ARP Inspection                     : 150
ARP packets dropped by additional validation (source MAC address)     : 0
ARP packets dropped by additional validation (destination MAC address): 0
ARP packets dropped by additional validation (IP address)         : 0
ARP packets dropped by ARP ACLs                                   : 0
ARP packets dropped by DHCP snooping                              : 0

Console#
```

9.4.12 show ip arp inspection vlan

本コマンドにより、ARP 検査ステータス、ARP ACL 名、ARP ACL 検証の完了後に DHCP スヌーピングデータベースが使用されているかどうか等、VLAN の設定を表示します。

構文

show ip arp inspection vlan [*vlan-id* | *vlan-range*]

vlan-id - 設定済み VLAN の識別子です。

vlan-range - ハイフンを使用して指定された VLAN の連続範囲、または各エントリがコンマで区切られたランダムな VLAN グループです。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection vlan 1

VLAN ID     DAI Status            ACL Name            ACL Status
--------   ---------------    --------------------    --------------------
1           disabled              sales               static
Console#
```

9.5 DoS 攻撃プロテクション

Denial-of-Service 攻撃(DoS 攻撃)は、コンピュータまたはネットワークリソースによって提供されるサービスをブロックする攻撃です。この種の攻撃は、インターネットサイトやサービスが効率的に機能しないようにさせます。一般的に、DoS 攻撃は、ターゲットを強制的にリセットしたり、リソースの大部分を消費して意図したサービスを提供できないようにしたり、意図したユーザとターゲットとの間の通信メディアを妨害して、 適切に通信できないようにします。

本章では、DoS 攻撃から保護するコマンドについて説明します。

表 9-8 DoS 攻撃プロテクションコマンド

コマンド	機能	モード
dos-protection echo-chargen	DoS echo-chargen 攻撃から保護します。	GC
dos-protection smurf	DoS smurf 攻撃から保護します。	GC
dos-protection tcp-flooding	DoS TCP-flooding 攻撃から保護します。	GC
dos-protection tcp-null-scan	DoS TCP null-scan 攻撃から保護します。	GC
dos-protection tcp-syn-fin-scan	DoS TCP-SYN/FIN-scan 攻撃から保護します。	GC
dos-protection tcp-xmas-scan	DoS TCP-XMAS-scan 攻撃から保護します。	GC
dos-protection udp-flooding	DoS UDP-flooding 攻撃から保護します。	GC
dos-protection win-nuke	DoS WinNuke 攻撃から保護します。	GC
show dos-protection	DoS 攻撃プロテクションのコンフィグレーションを表示します。	PE

9.5.1 dos-protection echo-chargen

本コマンドでは、DoS echo-chargen 攻撃から保護します。echo は送信されたものと同じものを送り返すサービスで、chargen(character generator)は連続したデータストリームを生成するサービスです。 一緒に使用すると、無限ループが発生し DoS が発生します。この機能を無効にするには、ビットレートパラメータなしの no 形式を使用するか、デフォルトの帯域をビットレートパラメータに設定して元に戻してください。

構文

[no] dos-protection echo-chargen [bit-rate-in-kilo *rate*]

rate - 許容された最大レートです。(範囲: 64 から 2000 kbits/秒)

デフォルト設定

無効、1000 kbits /秒

コマンドモード

Global Configuration

例

```
Console(config)#dos-protection echo-chargen bit-rate-in-kilo 65
Console(config)#
```

9.5.2 dos-protection smurf

本コマンドにより、DoS smurf 攻撃から保護します。DoS smurf 攻撃では、攻撃者がブロードキャスト宛先 IP アドレス(255.255.255.255)に対して送信元アドレスを偽装した ICMP エコー要求を大量に送信します。これらのすべてが、攻撃対象の送信元アドレスに偽装されています。攻撃対象は、返ってくる大量の ICMP エコー応答パケットを処理するために多くの割り込みが必要なため、クラッシュしてしまいます。この機能を無効にするには、no 形式を使用してください。

構文

[no] dos-protection smurf

デフォルト設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#dos-protection smurf
Console(config)#
```

9.5.3 dos-protection tcp-flooding

本コマンドにより、DoS TCP-flooding 攻撃から保護します。DoS tcp-flooding 攻撃では、攻撃者がターゲットに TCP SYN 要求(送信元 IP が偽装されているかどうかにかかわらず)を連続して送信し、それに対する ACK パケットを返しません。これらのハーフオープン接続は、ターゲット上のリソースをバインドし新しい接続を行うことができず、これにより DoS が発生します。この機能を無効にするには、ビットレートパラメータなしの no 形式を使用するか、デフォルトの帯域をビットレートパラメータに設定して元に戻してください。

構文

[no] dos-protection tcp-flooding [bit-rate-in-kilo *rate*]

rate - 許容された最大レートです。(範囲: 64 から 2000 kbits/秒)

デフォルト設定

無効、1000 kbits /秒

コマンドモード

Global Configuration

例

```
Console(config)#dos-protection tcp-flooding bit-rate-in-kilo 65
```

```
Console(config)#
```

9.5.4 dos-protection tcp-null-scan

本コマンドにより、DoS TCP-null-scan 攻撃から保護します。DoS TCP-null-scan 攻撃では、TCP NULL スキャンメッセージを使用して開いている TCP ポートを識別します。このスキャンでは、シーケンス番号が 0 でフラグがない構成の TCP パケットが使用されます。ターゲットの TCP ポートが閉じている場合、ターゲットは TCP RST(リセット)パケットで応答します。　ターゲット TCP ポートが開いている場合には、単純に TCP NULL スキャンを破棄します。　この機能を無効にするには、no 形式を使用してください。

構文

[no] dos-protection tcp-null-scan

デフォルト設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#dos-protection tcp-null-scan
Console(config)#
```

9.5.5 dos-protection tcp-syn-fin-scan

本コマンドにより、DoS TCP-SYN / FIN-scan 攻撃から保護します。DoS TCP-SYN/FIN-scan 攻撃では、TCP SYN/FIN スキャンメッセージを使用して開いている TCP ポートを識別します。スキャンでは、SYN(同期)フラグと FIN(終了)フラグを含む構成の TCP パケットを使用します。ターゲットの TCP ポートが閉じている場合、ターゲットは TCP RST(リセット)パケットで応答します。ターゲット TCP ポートが開いている場合には、単純に TCP SYN FIN スキャンを破棄します。この機能を無効にするには、no 形式を使用してください。

構文

[no] dos-protection tcp-syn-fin-scan

デフォルト設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#dos-protection tcp-syn-fin-scan
Console(config)#
```

9.5.6 dos-protection tcp-xmas-scan

本コマンドにより、DoS TCP-xmas-scan 攻撃から保護します。DoS TCP-xmas-scan 攻撃では、TCP XMAS スキャンメッセージを使用して開いている TCP ポートを識別します。このスキャンは、シーケンス番号 0 と URG、PSH、および FIN フラグを含む構成の TCP パケットを使用します。ターゲットの TCP ポートがクローズされている場合、ターゲットは TCP RST パケットで応答します。ターゲット TCP ポートが開いている場合には、TCP XMAS スキャンを破棄します。この機能を無効にするには、no 形式を使用してください。

構文

[no] dos-protection tcp-xmas-scan

デフォルト設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#dos-protection tcp-xmas-scan
Console(config)#
```

9.5.7 dos-protection udp-flooding

本コマンドにより、DoS UDP-flooding 攻撃から保護します。DoS UDP-flooding 攻撃では、攻撃者はリモートホスト上のランダムなポートに多数の UDP パケット(送信元 IP アドレスが偽装されたかどうかにかかわらず）を送信します。ターゲットは、アプリケーションがそのポートで待機中であると判断し、ICMP Destination Unreachable パケットで応答します。多くの ICMP パケットを強制的に送信することになり、最終的に他のクライアントに到達できなくなります。この機能を無効にするには、ビットレートパラメータなしの no 形式を使用するか、デフォルトの帯域をビットレートパラメータに設定して元に戻してください。

構文

[no] dos-protection udp-flooding [bit-rate-in-kilo *rate*]

rate - 許容された最大レートです。(範囲: 64 から 2000 kbits/秒)

デフォルト設定

無効、1000 kbits /秒

コマンドモード

Global Configuration

例

```
Console(config)#dos-protection udp-flooding bit-rate-in-kilo 65
Console(config)#
```

9.5.8 dos-protection win-nuke

本コマンドは、Microsoft Windows 3.1x / 95 / NT オペレーティングシステムに影響を与えた DoS WinNuke 攻撃から保護します。この種の攻撃では、TCP URG フラグを含む OOB(OOB out-of-band)パケットの文字列をターゲットコンピュータの TCP ポート 139(NetBIOS)に送信することで、ロックして「ブルースクリーン 」の表示を引き起こします。これにより、コンピュータのハードディスクに何らの損害やデータの変更が生じることはありませんが、保存されていないデータは失われます。　マイクロソフトは WinNuke 攻撃を防ぐためにパッチを作成しましたが、OOB パケットは依然として利用可能なすべての CPU 時間を消費するタイトなループを引き起こします。　この機能を無効にするには、ビットレートパラメータなしの no 形式を使用するか、デフォルトの帯域をビットレートパラメータに設定して元に戻してください。

構文

[no] dos-protection win-nuke [bit-rate-in-kilo *rate*]

rate - 許容された最大レートです。(範囲: 64 から 2000 kbits/秒)

デフォルト設定

無効、1000 kbits /秒

コマンドモード

Global Configuration

例

```
Console(config)#dos-protection win-nuke bit-rate-in-kilo 65
Console(config)#
```

9.5.9 show dos-protection

本コマンドにより、DoS 攻撃プロテクションコマンドのコンフィグレーションを表示します。

コマンドモード

Privileged Exec

例

```
Console#show dos-protection
Global DoS Protection:

 Echo/Chargen Attack          : Disabled, 1000 kilobits per second
 Smurf Attack                 : Enabled
 TCP Flooding Attack          : Disabled, 1000 kilobits per second
 TCP Null Scan                : Enabled
 TCP SYN/FIN Scan             : Enabled
 TCP XMAS Scan                : Enabled
 UDP Flooding Attack          : Disabled, 1000 kilobits per second
 WinNuke Attack               : Disabled, 1000 kilobits per second
Console#
```

9.6 トラフィックセグメンテーション

異なるクライアントからのトラフィックをローカルネットワークのダウンリンクポートとアップリンクポートを介してサービスプロバイダーに渡すために、より厳しいセキュリティが必要な場合には、ポートベースのトラフィックセグメンテーションを使用して、個々のクライアントのトラフィックを分離することができます。

ダウンリンクポートは、各クライアント毎に使用するポートを分けることでトラフィックを分離します。一方、アップリンクポートもクライアント毎に使用するポートを分けてトラフィックを分離しますが、他のクライアントが使用するアップリンクポートを介してトラフィックを転送することもできます。

表 9-9 トラフィックセグメント設定のコマンド

コマンド	機能	モード
traffic-segmentation	トラフィックのセグメント化を有効にします。	GC
traffic-segmentation session	クライアントセッションを作成します。	GC
traffic-segmentation uplink/downlink	クライアントセッションのアップリンク/ダウンリンクを設定します。	GC
traffic-segmentation uplink-to-uplink	トラフィックを異なるクライアントセッションへ割り当てられたアップリンク間で転送できるか否かについて、指定します。	GC
show traffic-segmentation	設定したトラフィックセグメントを表示します。	PE

9.6.1 traffic-segmentation

本コマンドにより、トラフィックのセグメント化を有効にします。トラフィックのセグメント化を無効にするには、no 形式を使用してください。

構文

[no] traffic-segmentation

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- トラフィックのセグメント化では、ポートベースのセキュリティと VLAN 内のポート間の分離を提供します。ダウンリンクポート上のデータトラフィックは、指定されたアップリンクポートにのみ、またそこから転送することができます。同じセグメント化されたグループ内のダウンリンクポート間、または同じグループに属していないポート間では、データを渡すことはできません。
- トラフィックのセグメント化と通常 VLAN は、同じスイッチ内に同時に存在することができます。トラフィックは、セグメント化されたグループのアップリンクポートと通常の VLAN のポート間で自由に通過することができます。
- トラフィックのセグメント化が有効な場合の、異なるクライアントセッションに割り当てられたアップリンクおよびダウンリンクポートの転送状態について、以下に示します:

表 9-10 トラフィックセグメント化の転送

宛先 送信元	セッション#1 ダウンリンク	セッション#1 アップリンク	セッション#2 ダウンリンク	セッション#2 アップリンク	通常ポート
セッション#1 ダウンリンク ポート	ブロッキング	転送	ブロッキング	ブロッキング	ブロッキング
セッション#1 アップリンク ポート	転送	転送	ブロッキング	ブロッキング/ 転送※	転送
セッション#2 ダウンリンク ポート	ブロッキング	ブロッキング	ブロッキング	転送	ブロッキング
セッション#2 アップリンク ポート	ブロッキング	ブロッキング/ 転送※	転送	転送	転送
通常ポート	転送	転送	転送	転送	転送

注※ アップリンク - アップリンクポートのフォワーディングステートは、traffic-segmentation uplink to uplink コマンドによって設定されます。

- トラフィックのセグメント化が無効な場合、すべてのポートは VLAN およびスパニングツリープロトコルのような、その他の機能によって指定された設定にもとづいて、通常転送モードで作動します。
- トラフィックのセグメント化を有効にするには、パラメータ無しで traffic-segmentation コマンドを入力します。その次に traffic-segmentation uplink/downlink コマンドを使用して、セグメント化されたグループに対してインタフェースメンバーを設定します。
- トラフィックのセグメント化を無効にするには、no traffic-segmentation を入力しセグメント化されたグループのコンフィグレーションをクリアします。

例

この例では、スイッチ上におけるトラフィックのセグメント化を有効にします。

```
Console(config)#traffic-segmentation
Console(config)#
```

9.6.2 traffic-segmentation session

本コマンドでは、トラフィックセグメンテーションクライアントセッションを作成します。クライアントセッションを削除するには、no 形式を使用してください。

構文

[no] traffic-segmentation session *session-id*

session-id - トラフィックセグメンテーションセッションです。(範囲: 1 から 4)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- 新しいトラフィックセグメンテーションクライアントセッションを作成するために、このコマンドを使用します。
- このコマンドの no 形式を使用することにより、割り当てられたすべてのアップリンクまたはダウンリンクを削除し、インタフェースを通常動作モードに復元します。

例

```
Console(config)#traffic-segmentation session 1
Console(config)#
```

9.6.3 traffic-segmentation uplink/downlink

本コマンドでは、ポートのセグメント化されたグループのアップリンクおよびダウンリンクを設定します。セグメント化されたグループからポートを削除するには、no 形式を使用してください。

構文

[no] traffic-segmentation [session *session-id*] {uplink *interface-list* [downlink *interface-list*] | downlink *interface-list*}

session-id - トラフィックセグメンテーションセッションです。(範囲: 1 から 4)

uplink - アップリンクインタフェースを指定します。

downlink - ダウンリンクインターフェースを指定します。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

未定義の場合は、セッション 1

セグメント化されたグループは未定義

コマンドモード

Global Configuration

コマンドの使用方法

- アップリンクとダウンリンクリストの両方に同じポートを設定することはできません。
- ポートは、1 つのトラフィックセグメンテーションセッションにのみ割り当てることができます。
- アップリンクまたはダウンリンクを指定する際、ハイフンまたはカンマを使用して port フィールド

に、ポートのリストを入力できます。channel-id フィールドについては、リストはサポートされていないことに留意してください。

- ダウンリンクポートは、同じセッションの中でのみ、アップリンクポートと通信できます。故に、セッションに対してアップリンクポートが設定されていない場合には、割り当てられたダウンリンクポートは他のポートと通信することができません。
- セッションに対してダウンリンクポートが設定されていない場合、割り当てられたアップリンクポートは通常ポートとして動作します。
- トランクポートを指定して設定した場合、削除もトランクポート指定で実行してください。

例

この例では、トラフィックのセグメント化を有効にし、アップリンクとしてポート 10 を、ダウンリンクとしてポート 5 から 8 を設定します。

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/10 downlink ethernet 1/5-8
Console(config)#
```

9.6.4 traffic-segmentation uplink-to-uplink

本コマンドでは、異なるクライアントセッションに割り当てられたアップリンクポート間でトラフィックを転送できるかどうかについて指定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

[no] traffic-segmentation uplink-to-uplink {blocking | forwarding}

blocking - 異なるセッションに割り当てられたアップリンクポート間のトラフィックをブロックします。

forwarding - 異なるセッションに割り当てられたアップリンクポート間で、トラフィックを転送します。

デフォルト設定

ブロッキング

コマンドモード

Global Configuration

例

この例では、異なるクライアントセッションに割り当てられたアップリンクポート間での、トラフィックの転送を有効にします。

```
Console(config)#traffic-segmentation uplink-to-uplink forwarding
Console(config)#
```

9.6.5 show traffic-segmentation

本コマンドでは、設定したトラフィックセグメントを表示します。

コマンドモード

Privileged Exec

例

```
Console#show traffic-segmentation

Traffic segmentation Status :            Disabled
 Uplink-to-Uplink Mode       :            Forwarding

 Session   Uplink Ports                    Downlink Ports
--------- ------------------------------ ------------------------------
    1      Ethernet  1/1                   Ethernet  1/2
                                           Ethernet  1/3
                                           Ethernet  1/4
Console#
```

10 アクセス制御リスト

アクセス制御リスト(ACL)では、IPv4 フレーム(アドレス、プロトコル、レイヤ 4 プロトコルポート番号または TCP 制御フラグにもとづく)、IPv6 フレーム(アドレス、DSCP トラフィッククラス、またはネクストヘッダータイプにもとづく) 任意のフレーム(MAC アドレスまたはイーサネットタイプにもとづく)に対するパケットフィルタリングを提供します。パケットをフィルタリングするには、まずアクセスリストを作成し、必要なルールを追加してから、そのリストを特定のポートにバインドします。本章では、アクセス制御リストコマンドについて説明します

Note: アクセスリストは物理ポートにのみバインドできます。ポートチャネルにアクセスリストをバインドする場合は、一度トランクポートの設定を削除し、アクセスリストを物理ポートへバインドした後、再度トランクポートの設定を行ってください。

表 10-1 アクセス制御リストコマンド

コマンドグループ	機能
IPv4 ACLs	IPv4 アドレス、TCP/UDP ポート番号、プロトコルタイプ、および TCP 制御フラグをもとにした、ACL を設定します。
IPv6 ACLs	IPv6 アドレス、DSCP トラフィッククラス、またはネクストヘッダータイプをもとにした ACL を設定します。
MAC ACLs	ハードウェアアドレス、パケットフォーマット、およびイーサネットタイプをもとにした ACL を設定します。
ARP ACLs	ARP メッセージアドレスをもとにした、ACL を設定します。
ACL 情報	ACL と関連ルールを表示し、各ポートに割当てられた ACL を示します。

10.1 IPv4 ACLs

本章の中のこのコマンドでは、IPv4 アドレス、TCP / UDP ポート番号、プロトコルタイプ、および TCP 制御フラグにもとづいて、ACL を設定します。IPv4 ACL を設定するには、最初に必要な permit または deny ルールを含むアクセスリストを作成し、次にそのアクセスリストを 1 つ以上のポートにバインドします。

表 10-2 IPv4 ACL コマンド

コマンド	機能	モード
access-list ip	IP ACL を作成し、標準または拡張 IPv4 ACL の設定モードを入力します。	GC
permit, deny	指定したソース IPv4 アドレスに合致するパケットをフィルタリングします。	IPv4-STD-ACL
permit, deny	ソースおよび宛先 IPv4 アドレス、TCP / UDP ポート番号、プロトコルタイプ、および TCP 制御フラグを含む、指定された基準を満たすパケットをフィルタリングします。	IPv4-EXT-ACL
ip access-group	IPv4 ACL をポートにバインドします。	IC
show ip access-group	IPv4 ACL のポート割当てを表示します。	PE
show ip access-list	設定した IPv4 ACL のルールを表示します。	PE

10.1.1 access-list ip

本コマンドでは、IP アクセスリストを追加し、標準または拡張 IPv4 ACL の設定モードに移行します。指定した ACL を削除するには、no 形式を使用してください。

構文

[no] access-list ip {standard | extended} *acl-name*

standard - 送信元 IP アドレスをもとにフィルタリングする ACL を指定します。

extended - 送信元または宛先 IP アドレス、およびその他のより具体的な基準にもとづいてパケットをフィルタリングする ACL を指定します。

acl-name - ACL の名称です。(最長: 32 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- 新規 ACL を作成、または既存 ACL の設定モードに移行し、permit または deny コマンドを使って、リストの末尾に新規ルールを追加します。
- ルールを削除するには、no permit または no deny のあとに、以前に設定したルールの正確なテキストを続けて使用します。
- ACL には、最大 128 のルールを含めることができます。

例

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

関連コマンド

permit, deny

show ip access-list

10.1.2 permit, deny (Standard IP ACL)

本コマンドでは、標準 IPv4 ACL にルールを追加します。このルールでは、指定された送信元から発するパケットのフィルタ条件を設定します。ルールを削除するには、no 形式を使用してください。

構文

{permit | deny} {any | *source bitmask* | host *source*}

[time-range *time-range-name*]

no {permit | deny} {any | *source bitmask* | host *source*}

any - すべての送信元 IP アドレスです。

source - 送信元 IP アドレスです。

bitmask - 有効なアドレスビットを表すドット付き 10 進数です。

host - 特定の IP アドレスが続くキーワードです。

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

デフォルト設定

無し

コマンドモード

Standard IPv4 ACL

コマンドの使用方法

- 新規ルールがリストの末尾に追加されます。
- アドレスビットマスクはサブネットマスクに類似しており、0 から 255 の 4 つの整数が含まれ、それぞれはピリオドで区切られます。バイナリマスクは、「有効」を示すために 1 ビットを使用し、「無視」を示すために 0 ビットを使用します。ビットマスクは、指定された送信元 IP アドレスとビット単位で論理積を行い、この ACL が割当てられているポートに入る各 IP パケットのアドレスと比較されます。

例

この例では、特定のアドレス 10.1.1.21 に対して 1 つの permit ルールを設定し、ビットマスクを使用して 168.92.16.x～168.92.31.x のアドレス範囲に対して別のルールを設定します。

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

関連コマンド

access-list ip

Time Range

10.1.3 permit, deny (Extended IPv4 ACL)

本コマンドにより、拡張 IPv4 ACL にルールを追加します。このルールは特定送信元または宛先 IP アドレス、プロトコルタイプ、送信元あるいや宛先プロトコルポート、もしくは TCP 制御フラグを持つパケットのフィルタ条件を設定します。ルールを削除するには、no 形式を使用してください。

構文

{permit | deny} [*protocol-number* | udp]

{any | *source address-bitmask* | host *source*}

{any | *destination address-bitmask* | host *destination*}

[dscp *dscp*] [precedence *precedence*]

[source-port *sport* [*bitmask*]]

[destination-port *dport* [*port-bitmask*]]

[time-range *time-range-name*]

no {permit | deny} [*protocol-number* | udp]

{any | *source address-bitmask* | host *source*}

{any | *destination address-bitmask* | host *destination*}

[dscp *dscp*] [precedence *precedence*]

[source-port *sport* [*bitmask*]]

[destination-port *dport* [*port-bitmask*]]

{permit | deny} tcp

{any | *source address-bitmask* | host *source*}

{any | *destination address-bitmask* | host *destination*}

[dscp *dscp*] [precedence *precedence*]

[source-port *sport* [*bitmask*]]

[destination-port *dport* [*port-bitmask*]]

[control-flag *control-flags flag-bitmask*]

[time-range *time-range-name*]

no {permit | deny} tcp

{any | *source address-bitmask* | host *source*}

{any | *destination address-bitmask* | host *destination*}

[dscp *dscp*] [precedence *precedence*]

[source-port *sport* [*bitmask*]]

[destination-port *dport* [*port-bitmask*]]

[control-flag *control-flags flag-bitmask*]

protocol-number - 特定プロトコル番号です。(範囲: 0 から 255)

source - 送信元 IP アドレスです。

destination - 宛先 IP アドレスです。

address-bitmask - 有効なアドレスビットを表す 10 進数です。

host - 特定の IP アドレスが続くキーワードです。

dscp - DSCP 優先レベルです。(範囲: 0 から 63)

precedence - IP precedence レベルです。(範囲: 0 から 7)

sport - プロトコル※送信元ポート番号です。(範囲: 0 から 65535)

dport - プロトコル※宛先ポート番号です(範囲: 0 から 65535)

port-bitmask - 有効なポートビットを表す 10 進数です。(範囲: 0 から 65535)

control-flags - TCP ヘッダーのバイト 14 のフラグビットを指定する 10 進数(ビット文字列を表す）です。(範囲: 0 から 63)

flag-bitmask - 有効なフラグビットを表す 10 進数です。

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

注※ TCP、UDP、またはその他のプロトコルタイプが含まれます。

デフォルト設定

無し

コマンドモード

Extended IPv4 ACL

コマンドの使用方法

- 新規ルールがリストの末尾に追加されます。
- アドレスビットマスクはサブネットマスクに類似しており、0 から 255 の 4 つの整数が含まれ、それぞれはピリオドで区切られます。バイナリマスクは、「有効」を示すために 1 ビットを使用し、「無視」を示すために 0 ビットを使用します。ビットマスクは指定された送信元 IP アドレスとビット単位で論理積され、この ACL が割当てられているポートに入る各 IP パケットのアドレスと比較されます。
- 制御フラグビットマスクは、制御フラグに適用される 10 進数(等価ビットマスクを表す)です。等価バイナリビット "1"はビットが有効であることを意味し、 "0"はビットを無視することを意味する 10 進数を入力します。以下のビットを指定することができます:。
  - 1 (fin) - Finish
  - 2 (syn) - Synchronize
  - 4 (rst) - Reset
  - 8 (psh) - Push
  - 16 (ack) - Acknowledgement
  - 32 (urg) - Urgent Pointer

  たとえば、次のフラグを設定されているパケットを捕捉するには、フラグ値とマスクを使用します:

- SYN フラグが有効な場合、“control-flag 2 2”を使用します。
- SYN と ACK の両方が有効な場合、“control-flag 18 18”を使用します。
- SYN が有効で ACK が無効な場合、“control-flag 2 18”を使用します。

◆ 拡張 IPv4 ルールと MAC ルールが同じパケットと一致し、これらのルールが「permit」エントリと「deny」エントリを指定する場合、「deny」アクションが優先されます。

例

この例では、ソースアドレスがサブネット 10.7.1.x 以内の場合、受信パケットを受け入れます。たとえば、ルール(10.7.1.0 & 255.255.255.0)がマスクされたアドレス(10.7.1.2 & 255.255.255.0)と等しい場合、パケットは通過します。

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

この例では、宛先 TCP ポート 80(例; HTTP)に設定された場合、クラス C アドレス 192.168.1.0 から任意の宛先アドレスへの TCP パケットを許可します。

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port 80
Console(config-ext-acl)#
```

この例では、TCP 制御フラグが "SYN"に設定されたクラス C アドレス 192.168.1.0 からのすべての TCP パケットが許可されます。

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any control-flag 2 2
Console(config-ext-acl)#
```

関連コマンド

access-list ip

Time Range

10.1.4 ip access-group

本コマンドにより、IPv4 ACL をポートにバインドします。ポートから削除するには、no 形式を使用してください。

構文

ip access-group *acl-name* in

[time-range *time-range-name*] [counter]

no ip access-group *acl-name* in

acl-name - ACL の名称です。(最長: 32 文字)

in - リストが受信パケットに適用されることを示します。

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

counter - ACL 統計のカウンタを有効にします。

デフォルト設定

無し

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

ACL が既にポートにバインディングされ、異なる ACL をバインドする場合には、スイッチは古いバインディングを新規の物に置き換えます。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

関連コマンド

show ip access-list

Time Range

10.1.5 show ip access-group

本コマンドでは、IP ACL に割当てられたポートを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip access-group
Interface ethernet 1/2
 IP access-list david in
Console#
```

10.1.6 show ip access-list

本コマンドでは、設定した IPv4 ACL のルールを表示します。

構文

show ip access-list {standard | extended} [*acl-name*]

standard - 標準 IP ACL を指定します。

extended - 拡張 IP ACL を指定します。

acl-name - ACL の名称です。(最長: 32 文字)

コマンドモード

Privileged Exec

例

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

関連コマンド

permit, deny

10.2 IPv6 ACLs

本章のこのコマンドでは、IPv6 アドレス、DSCP トラフィッククラス、またはネクストヘッダータイプをもとに、ACL を設定します。IPv6 ACL を設定するには、最初に必要な permit または deny ルールを含むアクセスリストを作成し、次にアクセスリストを一つまたは複数のポートにバインドします。

表 10-3 IPv6 ACL コマンド

コマンド	機能	モード
access-list ipv6	IPv6 ACL を作成し、標準または拡張 IPv6 ACL の設定モードに移行します。	GC
permit, deny	指定した送信元 IPv6 アドレスに合致するパケットを、フィルタリングします。	IPv6- STD-ACL
permit, deny	送信元または宛先 IPv6 アドレス、DSCP トラフィッククラス、またはネクストヘッダータイプを含む指定された基準を満たすパケットをフィルタリングします。	IPv6- EXT-ACL
ipv6 access-group	IPv6 ACL をポートにバインドします。	IC
show ipv6 access-group	IPv6 ACL のポート割当てを表示します。	PE
show ipv6 access-list	設定した IPv6 ACL のルールを表示します。	PE

10.2.1 access-list ipv6

本コマンドでは、IPv6 アクセスリストを追加し、標準または拡張 IPv6 ACL の設定モードに移行します。指定した ACL を削除するには、no 形式を使用してください。

構文

[no] access-list ipv6 {standard | extended} *acl-name*

standard - 送信元 IP アドレスをもとにフィルタリングする ACL を指定します。

extended - 宛先 IP アドレスおよびその他のより具体的な基準をもとにフィルタリングする ACL を指定します。

acl-name - ACL の名称です。(最長: 32 文字)

デフォルト設定

None

コマンドモード

Global Configuration

コマンドの使用方法

- 新規 ACL を作成、または既存 ACL の設定モードに移行し、permit または deny コマンドを使って、リストの末尾に新規ルールを追加します。
- ルールを削除するには、no permit または no deny のあとに、以前に設定したルールの正確なテキストを続けて使用します。
- ACL には、最大 60 ルールまでとしてください。

例

```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#
```

関連コマンド

permit, deny (Standard IPv6 ACL)

permit, deny (Extended IPv6 ACL)

ipv6 access-group

show ipv6 access-list

10.2.2 permit, deny (Standard IPv6 ACL)

本コマンドでは、標準 IPv6 ACL にルールを追加します。このルールでは、指定された送信元から発するパケットのフィルタ条件を設定します。ルールを削除するには、no 形式を使用してください。

構文

{permit | deny} {any | host *source-ipv6-address* |

source-ipv6-address/prefix-length}

[time-range *time-range-name*]

no {permit | deny} {any | host *source-ipv6-address* |

source-ipv6-address/prefix-length}

any - すべての送信元 IPv6 アドレスです。

host - 特定の IPv6 アドレスが続くキーワードです。

source-ipv6-address - IPv6 送信元アドレスまたはネットワーククラスです。アドレスは、RFC 2373「IPv6 Addressing Architecture」フォーマットに従って、コロンで区切られた 8 つの 16 ビット 16 進数を使用する必要があります。1 つのダブルコロンをアドレスに使用して、定義されていないフィールドを埋めるために必要な、適切な数のゼロを示すことができます。

prefix-length - アドレスの左から数えて連続するビットがプレフィックスを構成することを示す 10 進数です。例; アドレスのネットワーク部分。(範囲: 0 から 128)

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

デフォルト設定

無し

コマンドモード

Standard IPv6 ACL

コマンドの使用方法

新規ルールがリストの末尾に追加されます。

例

この例では、特定のアドレス 2009：DB9：2229 :: 79 に対して 1 つの許可ルールを設定し、ネットワークプレフィックス 2009：DB9：2229：5 :: / 64 を持つアドレスの別ルールを構成します。

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79
Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64
Console(config-std-ipv6-acl)#
```

関連コマンド

access-list ipv6

Time Range

10.2.3 permit, deny (Extended IPv6 ACL)

本コマンドにより、拡張 IPv6 ACL にルールを追加します。このルールは、特定の送信元 IP アドレス、宛先アドレス、またはネクストヘッダータイプを持つパケットのフィルタ条件を設定します。ルールを削除するには、no 形式を使用してください。

構文

{permit | deny}

{any | host *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]}

{any | host *destination-ipv6-address* | *destination-ipv6-address*[*/prefix-length*]}

[next-header *next-header* [source-port *sport* [*bitmask*]] [destination-port *dport* [*port-bitmask*]]] | [dscp *dscp*]

[time-range *time-range-name*]

no {permit | deny}

{any | host *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]}

{any | host *destination-ipv6-address* | *destination-ipv6-address*[*/prefix-length*]}

[next-header *next-header* [source-port *sport* [*bitmask*]] [destination-port *dport* [*port-bitmask*]]] | [dscp *dscp*]

any - 任意の IPv6 アドレスです。（IPv6 プレフィックス:: / 0 の省略形）。

host - 特定の IPv6 アドレスが続くキーワードです。

source-ipv6-address - IPv6 送信元アドレスまたはネットワーククラスです。アドレスは、RFC 2373「IPv6 Addressing Architecture」フォーマットに従って、コロンで区切られた 8 つの 16 ビット 16 進数を使用する必要があります。1 つのダブルコロンをアドレスに使用して、定義されていないフィールドを埋めるために必要な、適切な数のゼロを示すことができます。

destination-ipv6-address - IPv6 宛先アドレスまたはネットワーククラスです。アドレスは、RFC 2373「IPv6 Addressing Architecture」フォーマットに従って、コロンで区切られた 8 つの 16 ビット 16 進数を使用する必要があります。1 つのダブルコロンをアドレスに使用して、定義されていないフィールドを埋めるために必要な、適切な数のゼロを示すことができます。(スイッチは宛先アドレスの最初の 128 ビットのみをチェックします。)

prefix-length - アドレスの左から数えて連続するビットがプレフィックスを構成することを示す 10 進数です。例; アドレスのネットワーク部分。(範囲: 送信元プレフィクスの場合は 0 から 128、宛先プレフィックスの場合は 0 から 128)

dscp - DSCP トラフィッククラスです。(範囲: 0 から 63)

next-header - IPv6 ヘッダー直後のヘッダータイプを識別します。(範囲: 0 から 255)

sport - プロトコル※送信元ポート番号です。(範囲: 0 から 65535)

dport - プロトコル※宛先ポート番号です(範囲: 0 から 65535)

port-bitmask - 有効なポートビットを表す 10 進数です。(範囲: 0 から 65535)

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

注※ TCP と UDP を含む。

デフォルト設定

無し

コマンドモード

Extended IPv6 ACL

コマンドの使用方法

- すべての新規ルールがリストの末尾に追加されます。
- オプションのインターネット層情報は、IPv6 ヘッダーとパケットの上位層レイヤヘッダーの間に置かれる別々のヘッダーに符号化されます。少数のそのような拡張ヘッダーがあり、それぞれ別個のネクストヘッダー値で識別されます。IPv6 では、RFC 1700 の IPv4 プロトコルフィールドに定義されている値をサポートしています。よく使われるヘッダーを次に示します。

0	: Hop-by-Hop Options	(RFC 2460)
6	: TCP Upper-layer Header	(RFC 1700)
17	: UDP Upper-layer Header	(RFC 1700)
43	: Routing	(RFC 2460)
44	: Fragment	(RFC 2460)
51	: Authentication	(RFC 2402)
50	: Encapsulating Security Payload	(RFC 2406)
60	: Destination Options	(RFC 2460)

例

この例では、宛先アドレスが 2009:DB9:2229::79/8 の場合、すべての受信パケットを受け取ります。

```
Console(config-ext-ipv6-acl)#permit any 2009:db90:2229::79/8
Console(config-ext-ipv6-acl)#
```

この例では、DSCP 値が 5 の場合任意の宛先アドレスへのパケットが許可されます。

```
Console(config-ext-ipv6-acl)#permit any any dscp 5
Console(config-ext-ipv6-acl)#
```

この例では、ネクストヘッダーが 43 のときに、任意の送信元から任意の宛先に送信されるパケットが許可されます。

```
Console(config-ext-ipv6-acl)#permit any any next-header 43
Console(config-ext-ipv6-acl)#
```

関連コマンド

access-list ipv6

Time Range

10.2.4 ipv6 access-group

このコマンドは、IPv6 ACL をポートにバインドします。ポートを削除するには、no 形式を使用してください。

構文

ipv6 access-group *acl-name* in

[time-range *time-range-name*] [counter]

no ipv6 access-group *acl-name* in

acl-name - ACL の名称です。(最長: 32 文字)

in - リストが受信パケットに適用されることを示します。

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

counter - ACL 統計のカウンタを有効にします。

デフォルト設定

無し

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

ポートがすでに ACL にバインドされていて、それを別の ACL にバインドすると、スイッチは古いバインドを新規のものに置き換えます。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#ipv6 access-group standard david in
Console(config-if)#
```

関連コマンド

show ipv6 access-list

Time Range

10.2.5 show ipv6 access-group

本コマンドは、IPv6 ACL に割当てられたポートを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ipv6 access-group
Interface ethernet 1/2
 IPv6 standard access-list david in
Console#
```

関連コマンド

ipv6 access-group

10.2.6 show ipv6 access-list

本コマンドでは、設定した IPv6 ACL のルールを表示します。

構文

show ipv6 access-list {standard | extended} [*acl-name*]

standard - 標準 IPv6 ACL を指定します。

extended - 拡張 IPv6 ACL を指定します。

acl-name - ACL の名称です。(最長: 32 文字)

コマンドモード

Privileged Exec

例

```
Console#show ipv6 access-list standard
IPv6 standard access-list david:
  permit host 2009:DB9:2229::79
  permit 2009:DB9:2229:5::/64
Console#
```

関連コマンド

permit, deny (Standard IPv6 ACL)

permit, deny (Extended IPv6 ACL)

ipv6 access-group

10.3 MAC ACLs

本章のコマンドは、ハードウェアアドレス、パケットフォーマット、およびイーサネットタイプに基づいて ACL を設定します。MAC ACL を設定するには、最初に必要な permit または deny ルールを含むアクセスリストを作成し、そのアクセスリストを 1 つまたは複数のポートにバインドします。

表 10-4　MAC ACL コマンド

コマンド	機能	モード
access-list mac	MAC ACL を作成し、設定モードに移行します	GC
permit, deny	指定された送信元および宛先アドレス、パケットフォーマット、およびイーサネットタイプに一致するパケットをフィルタリングします。	MAC-ACL
mac access-group	MAC ACL をポートにバインドします。	IC
show mac access-group	MAC ACL のポート割当てを表示します。	PE
show mac access-list	設定された MAC ACL のルールを表示します。	PE

10.3.1 access-list mac

このコマンドは、MAC ACL 設定モードに移行します。指定された MAC 送信元または宛先アドレス（例, 物理層アドレス）、またはイーサネットプロトコルタイプに一致するパケットをフィルタするためにルールを追加することができます。指定した ACL を削除するには、no 形式を使用してください。

構文

[no] access-list mac *acl-name*

acl-name - ACL の名称です。(最長: 32 文字。)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- 新規 ACL を作成、または既存 ACL の設定モードに移行し、permit または deny コマンドを使って、リストの末尾に新規ルールを追加します。
- ルールを削除するには、no permit または no deny のあとに、以前に設定したルールの正確なテキストを続けて使用します。
- ACL には、最大 128 ルールを含めることができます。

例

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

関連コマンド

permit, deny

mac access-group

show mac access-list

10.3.2 permit, deny (MAC ACL)

このコマンドは、MAC ACL にルールを追加します。ルールは、指定された MAC 送信元または宛先アドレス（例, 物理層アドレス）またはイーサネットプロトコルタイプに一致するパケットをフィルタリングします。ルールを削除するには、no 形式を使用してください。

構文

{permit | deny}

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

[cos *cos cos-bitmask*] [vid *vid vid-bitmask*]

[ethertype *ethertype* [*ethertype-bitmask*]]

[time-range *time-range-name*]

no {permit | deny}

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

[cos *cos cos-bitmask*] [vid *vid vid-bitmask*]

[ethertype *ethertype* [*ethertype-bitmask*]]

Note: デフォルトは、イーサネット II パケット用です。

{permit | deny} tagged-eth2

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

[cos *cos cos-bitmask*] [vid *vid vid-bitmask*]

[ethertype *ethertype* [*ethertype-bitmask*]]

[time-range *time-range-name*]

no {permit | deny} tagged-eth2

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

[cos *cos cos-bitmask*] [vid *vid vid-bitmask*]

[ethertype *ethertype* [*ethertype-bitmask*]]

{permit | deny} untagged-eth2

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

[ethertype *ethertype* [*ethertype-bitmask*]]

[time-range *time-range-name*]

no {permit | deny} untagged-eth2

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

[ethertype *ethertype* [*ethertype-bitmask*]]

{permit | deny} tagged-802.3

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

[cos *cos cos-bitmask*] [vid *vid vid-bitmask*]

[time-range *time-range-name*]

no {permit | deny} tagged-802.3

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

[cos *cos cos-bitmask*] [vid *vid vid-bitmask*]

{permit | deny} untagged-802.3

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

[time-range *time-range-name*]

no {permit | deny} untagged-802.3

{any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*}

tagged-eth2 - タグ付きイーサネット II パケットです。

untagged-eth2 - タグ無しイーサネット II パケットです。

tagged-802.3 - タグ付きイーサネット 802.3 パケットです。

untagged-802.3 - タグ無しイーサネット 802.3 パケットです。

any - 任意の MAC の送信元または宛先アドレスです。

host - 特定の MAC アドレスです。

source - 送信元 MAC アドレスです。

destination - 宛先 MAC アドレスです。

address-bitmask※ - MAC アドレスのビットマスクです（16 進形式）。

cos - Class-of-Service 値です。(範囲: 0 から 7)

cos-bitmask※ - Class-of-Service ビットマスクです。(範囲: 0 から 7)

vid - VLAN ID.です。(範囲: 1 から 4094)

vid-bitmask※ - VLAN ビットマスクです。(範囲: 1 から 4095)

ethertype - 特定のイーサネットプロトコル番号です。(範囲: 0 から ffff 16 進数)

ethertype-bitmask※ - プロトコルビットマスク(範囲: 0 から ffff 16 進数)

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

注※ すべてのビットマスクに対して、「1」は有効を、「0」は無視を意味します。

デフォルト設定

無し

コマンドモード

MAC ACL

コマンドの使用方法

- 新しいルールがリストの末尾に追加されます。
- ethertype オプションは、イーサネット II 形式のパケットをフィルタリングするためにのみ使用できます。
- イーサネットプロトコルタイプの詳細なリストは、RFC 1060 にあります。より一般的なタイプには、次のものがあります。
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX
- 拡張 IPv4 ルールと MAC ルールが同じパケットと一致し、これらのルールが「permit」エントリと「deny」エントリを指定する場合、「deny」アクションが優先されます。

例

このルールでは、任意の送信元 MAC アドレスから、イーサネットタイプが 0800 の宛先アドレス 00-e0-29-94-34-de へのパケットを許可します。

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

関連コマンド

access-list mac

Time Range

10.3.3 mac access-group

このコマンドは、MAC ACL をポートにバインドします。ポートを削除するには、no 形式を使用してください。

構文

mac access-group *acl-name* in

[time-range *time-range-name*] [counter]

no mac access-group *acl-name* in

acl-name - ACL の名称です。(最長: 32 文字)

in - リストが受信パケットに適用されることを示します。

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

counter - ACL 統計のカウンタを有効にします。

デフォルト設定

無し

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

ACL が既にポートにバインディングされ、異なる ACL をバインドする場合には、スイッチは古いバインディングを新規の物に置き換えます。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

関連コマンド

show mac access-list

Time Range

10.3.4 show mac access-group

このコマンドは、MAC ACL に割当てられたポートを表示します。

コマンドモード

Privileged Exec

例

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
Console#
```

関連コマンド

mac access-group

10.3.5 show mac access-list

このコマンドは、設定された MAC ACL のルールを表示します。

構文

show mac access-list [*acl-name*]

acl-name - ACL の名称です。(最長: 32 文字)

コマンドモード

Privileged Exec

例

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

関連コマンド

permit, deny

mac access-group

10.4 ARP ACLs

本章のコマンドは、ARP 要求および応答メッセージに含まれる IP または MAC アドレスに基づいて ACL を設定します。ARP ACL を設定するには、最初に必要な permit または deny ルールを含むアクセスリストを作成し、それから ip arp inspection vlan コマンドを使用してアクセスリストを 1 つまたは複数の VLAN にバインドします。

表 10-5　ARP ACL コマンド

コマンド	機能	モード
access-list arp	ARP ACL を作成し、設定モードに移行します	GC
permit, deny	ARP メッセージの中の特定の送信元または宛先アドレスに合致するパケットをフィルタリングします。	ARP-ACL
show access-list arp	設定済みの ARP ACL のルールを表示します。	PE

10.4.1 access-list arp

本コマンドは、ARP アクセスリストを追加し、ARP ACL 設定モードに移行します。指定した ACL を削除するには、no 形式を使用してください。

構文

[no] access-list arp *acl-name*

acl-name - ACL の名称です。(最長: 16 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- 新規 ACL を作成、または既存 ACL の設定モードに移行し、permit または deny コマンドを使って、リストの末尾に新規ルールを追加します。
- ルールを削除するには、no permit または no deny のあとに、以前に設定したルールの正確なテキストを続けて使用します。
- ACL には、最大 128 ルールを含めることができます。

例

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

関連コマンド

permit, deny

show access-list arp

10.4.2 permit, deny (ARP ACL)

このコマンドは、ARP ACL にルールを追加します。ルールは、ARP メッセージの指定された送信元または宛先アドレスと一致するパケットをフィルタリングします。ルールを削除するには、no 形式を使用してください。

構文

[no] {permit | deny} ip

{any | host *source-ip* | *source-ip ip-address-bitmask*}

[any | host *destination-ip* | *destination-ip ip-address-bitmask*]

mac {any | host *source-mac* | *source-mac mac-address-bitmask*}

[any | host *destination-mac* | *destination-mac mac-address-bitmask*] [log]

このフォームは、要求パケットまたは応答パケットのいずれかを示します。

[no] {permit | deny} request

ip {any | host *source-ip* | *source-ip ip-address-bitmask*}

[any | host *destination-ip* | *destination-ip ip-address-bitmask*]

mac {any | host *source-mac* | *source-mac mac-address-bitmask*}

[any | host *destination-mac* | *destination-mac mac-address-bitmask*] [log]

[no] {permit | deny} response

ip {any | host *source-ip* | *source-ip ip-address-bitmask*}

[any | host *destination-ip* | *destination-ip ip-address-bitmask*]

mac {any | host *source-mac* | *source-mac mac-address-bitmask*}

[any | host *destination-mac* | *destination-mac mac-address-bitmask*] [log]

source-ip - 送信元 IP アドレスです。

destination-ip - 宛先 IP アドレスです。

ip-address-bitmask※ - 有効なアドレスビットを表す IPv4 番号です。

source-mac - 送信元 MAC アドレスです。

destination-mac - 宛先 MAC アドレスです。

mac-address-bitmask※ - MAC アドレスのビットマスクです（16 進形式）。

log - パケットがアクセス制御エントリと一致した際にパケットを記録します。

注※ すべてのビットマスクに対して、バイナリ 「1」は有効を、 「0」は無視することを意味します。

デフォルト設定

無し

コマンドモード

ARP ACL

コマンドの使用方法

新しいルールがリストの末尾に追加されます。

例

このルールでは、任意の送信元 IP アドレスと MAC アドレスから宛先サブネットアドレス 192.168.0.0 までのパケットを許可します。

```
Console(config-arp-acl)#permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console(config-arp-acl)#
```

関連コマンド

access-list arp

10.4.3 show access-list arp

本コマンドは、設定された ARP ACL の規則を表示します。

構文

show access-list arp [*acl-name*]

acl-name - ACL の名称です。(最長: 32 文字)

コマンドモード

Privileged Exec

例

```
Console#show access-list arp
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

関連コマンド

permit, deny

10.5 ACL 情報

本章では、ACL 情報の表示に使用されるコマンドについて説明します。

表 10-6　ACL 情報コマンド

コマンド	機能	モード
clear access-list hardware counters	すべての ACL または指定された ACL のルールのヒットカウンタをクリアします。	PE
show access-group	各ポートに割当てられた ACL を表示します。	PE
show access-list	すべての ACL と関連ルールを表示します。	PE

10.5.1 clear access-list hardware counters

本コマンドは、すべての ACL のルールまたは指定された ACL のルールのヒットカウンタをクリアします。

構文

clear access-list hardware counters

[direction in [interface *interface*]] |

[interface *interface*] | [name *acl-name*] [direction in [interface *interface*]]

in - 受信ルールのカウンタをクリアします。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

acl-name - ACL の名称です。(最長: 32 文字)

コマンドモード

Privileged Exec

例

```
Console#clear access-list hardware counters
Console#
```

10.5.2 show access-group

このコマンドは、ACL に割当てられたポートを表示します。

構文

show access-group [ip | ipv6 | mac]

コマンドモード

Privileged Exec

例

```
Console#show access-group
Interface ethernet 1/2
 IP access-list david
 MAC access-list jerry
Console#
```

10.5.3 show access-list

本コマンドは、すべての ACL と関連ルールを表示します。

構文

show access-list

[[arp [*acl-name*]] |

[ip [extended [*acl-name*] | standard [*acl-name*]] |

[ipv6 [extended [*acl-name*] | standard [*acl-name*]] |

[mac [*acl-name*]] | [hardware counters]]

arp - ARP ACL の受信ルールを表示します。

hardware counters - すべての ACL の統計情報を表示します。※

ip extended - 拡張 IPv4 ACL の受信ルールを表示します。

ip standard - 標準 IPv4 ACL の受信ルールを表示します。

ipv6 extended - 拡張 IPv6 ACL の受信ルールを示します。

ipv6 standard - 標準 IPv6 ACL の受信ルールを表示します。

mac - MAC ACL の受信ルールを表示します。

acl-name - ACL の名称です。(最長: 32 文字)

注※ ハードウェアの制限により、このオプションは許可ルールの統計情報のみを表示します。

注 SNMP を使用して管理ステーションから ACL 情報を取得する場合は 63 個まで取得できます。

コマンドモード

Privileged Exec

例

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
```

```
  permit 10.7.1.1 255.255.255.0 any
  permit TCP 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit TCP 192.168.1.0 255.255.255.0 any control-flag 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny TCP any any control-flag 2 2
  permit any any
Console#
```

11 インタフェースコマンド

これらのコマンドは、イーサネットポート、集約リンク、または VLAN の通信パラメータを表示または設定するために使用されます。 また、指定されたインタフェースでケーブル診断を実行できます。

表 11-1 インタフェースコマンド

コマンド	機能	モード
インタフェース設定		
interface	インタフェースタイプを設定し、インタフェース設定モードを開始します。	GC
capabilities	オートネゴシエーションで使用するために、指定されたインタフェースの機能をアドバタイズします。	IC
description	インタフェース設定に説明を追加します。	IC
flowcontrol	指定されたインタフェースでフロー制御を有効にします。	IC
history	統計の定期サンプリングを設定し、サンプリング間隔とサンプル数を指定します。	IC
media-type	SFP ポートにトランシーバモードを使用させます。	IC
negotiation	指定されたインタフェースのオートネゴシエーションを有効にします。	IC
shutdown	インタフェースを無効にします。	IC
speed-duplex	オートネゴシエーションが無効の場合に、特定のインタフェースの速度および duplex 動作を設定します。	IC
clear counters	インタフェースの統計情報をクリアします。	PE
show interfaces brief	運用ステータス、ネイティブ VLAN ID、デフォルトプライオリティ、速度/duplex モード、および、ポートタイプなどのキー情報の要約を表示します。	PE
show interfaces counters	指定されたインタフェースの統計情報を表示します。	NE, PE
show interfaces history	サンプリング間隔、サンプル数、カウンタ値など、統計情報の定期的なサンプリングを表示します。	NE, PE
show interfaces status	指定されたインタフェースのステータスを表示します。	NE, PE
show interfaces switchport	インタフェースの管理ステータスと動作ステータスを表示します。	NE, PE
トランシーバ閾値設定		
transceiver-monitor	トランシーバの動作値のいずれかが指定された閾値を超えた場合にトラップを送信します。	IC
transceiver-threshold-auto	トランシーバから得られたデフォルトの閾値設定を使用して、アラームまたはトラップメッセージの送信時期を決定します。	IC
transceiver-threshold current	アラームまたは警告メッセージをトリガするために使用できるトランシーバ電流の閾値を設定します。	IC

コマンド	機能	モード
transceiver-threshold rx-power	アラームまたは警告メッセージをトリガするために使用できる受信信号のトランシーバ出力レベルの閾値を設定します	IC
transceiver-threshold temperature	アラームまたは警告メッセージをトリガするために使用できるトランシーバ温度の閾値を設定します。	IC
transceiver-threshold tx-power	アラームまたは警告メッセージをトリガするために使用できる送信信号のトランシーバ出力レベルの閾値を設定します。	IC
transceiver-threshold voltage	アラームまたは警告メッセージをトリガするために使用できるトランシーバ電圧の閾値を設定します	IC
show interfaces transceiver	温度、電圧、バイアス電流、送信電力、受信電力を表示します。	PE
show interfaces transceiver-threshold	温度、電圧、バイアス電流、送信電力、および受信電力のアラーム/警告の閾値を表示します。	PE
ケーブル診断		
test cable-diagnostics	指定されたポートでケーブル診断を実行します。	PE
show cable-diagnostics	ケーブル診断テストの結果を表示します。	PE

11.1 インタフェース設定

11.1.1 interface

本コマンドはインタフェースタイプを指定し、インタフェース設定モードを開始します。ポートチャネルインタフェース、VLAN インタフェースを削除するには、no 形式を使用します。

Note: VLAN インターフェイスを入力するには、最初に vlan database コマンドを使用して VLAN を設定する必要があります。 他のインターフェイスタイプはあらかじめ設定する必要はありません。

Note: スイッチは、VLAN インターフェイスへの最大 8 つのアドレスのバインディングをサポートしています。バインドは IPv4 と IPv6 の間で共有されます。 6 つの IPv4 アドレスが VLAN インターフェイスにバインドされている場合、2 つの IPv6 アドレスだけがバインドされます。

構文

[no] interface *interface*

interface

ethernet *unit*/*port-list*

unit - ユニット識別子です。(範囲: 1)

port-list - 物理ポート番号または物理ポート番号のリストです。非連続ポート番号を指定するときはコンマで区切り、スペースは入れないでください; ハイフンを使用してポート番号の範囲を指定することもできます。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan *vlan-id* (範囲: 1 から 4094)

デフォルト設定

無し

コマンドモード

Global Configuration

例

複数の異なるポートを指定するには、次のコマンドを入力します。

```
Console(config)#interface ethernet 1/1-3,10
Console(config-if)#
```

11.1.2 capabilities

本コマンドは、オートネゴシエーション中に特定のインタフェースのポート機能をアドバタイズします。アドバタイズされた能力を無効にするには、パラメータに no 形式を使用するか、またはパラメータ無しの no 形式を使用し、デフォルト値に復元します。

構文

[no] capabilities {1000full | 100full | 100half | 10full | 10half | flowcontrol}

1000full - 1 Gbps 全二重動作をサポートします。

100full - 100 Mbps の全二重動作をサポートします。

100half - 100 Mbps の半二重動作をサポートします。

10full - 10 Mbps の全二重動作をサポートします。

10half - 10 Mbps の半二重動作をサポートします。

flowcontrol - フロー制御をサポートします。

デフォルト設定

1000BASE-T: 10half, 10full, 100half, 100full, 1000full

1000BASE-SX/LX/LH/BX (SFP): 1000full

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

◆ negotiation コマンドでオートネゴシエーションを有効にすると、スイッチは capabilities コマンドに基づいてリンクの最適な設定をネゴシエートします。オートネゴシエーションが無効になっている場合は、speed-duplex コマンドと flowcontrol コマンドでリンク属性を手動で指定する必要があります。

例

次の例では、100half と 100full を含めるようにイーサネットポート 5 の機能を設定します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

関連コマンド

negotiation

speed-duplex

flowcontrol

11.1.3 description

本コマンドは、インタフェースに説明を追加します。説明を削除するには、no 形式を使用します。

構文

description *string*

no description

string - このインタフェースに何が付いているかを覚えておくためのコメントや説明です。(範囲: 1 から 64 文字)

デフォルト設定

無し

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

この説明は、show interfaces status コマンドとランニングコンフィグレーションファイルで表示されます。ネットワークマネージャがこのオブジェクトに格納する値の例は、製造元の名前と製品名です。

例

次の例では、ポート 4 に説明を追加します。

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

11.1.4 flowcontrol

このコマンドはフロー制御を有効にします。フロー制御を無効にするには、no 形式を使用します。

構文

[no] flowcontrol

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- フロー制御では、バッファが満杯になったときにスイッチに直接接続されたエンドステーションまたはセグメントからのトラフィックを制御することで、フレーム損失をなくすことができます。有効にすると、半二重動作にはバックプレッシャーが使用され、全二重動作には IEEE 802.3-2002（正式には IEEE 802.3x）が使用されます。
- フロー制御をオンまたはオフにするには（flowcontrol または no flowcontrol コマンドを使用するには）、no negotiation コマンドを使用して、選択したインタフェースのオートネゴシエーションを無効にします。
- negotiation コマンドを使用してオートネゴシエーションを有効にする場合、最適な設定は capabilities コマンドによって決定されます。オートネゴシエーションでフロー制御を有効にするには、

「flowcontrol」を任意のポートの機能リストに含める必要があります。

例

次の例では、ポート 5 でフロー制御を有効化します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

関連コマンド

negotiation

capabilities

11.1.5 history

このコマンドは、サンプリング間隔とサンプル数を指定して、統計の定期サンプリングを構成します。サンプリングテーブルから名前付きエントリを削除するには、no 形式を使用してください。

構文

history *name interval buckets*

no history *name*

name - サンプリングテーブル内のこのエントリの記号名です。(範囲: 1 から 32 文字)

interval - 統計をサンプリングする間隔です。(範囲: 1 から 1440 分。)

buckets - 取得するサンプルの数です。(範囲: 1 から 96)

デフォルト設定

15min - 15 分間隔、96 個のバケットです。

1day - 1 日間隔、7 つのバケットです。

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

例

この例では、標準統計値をポート 1 でサンプリングする間隔を 15 分に設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#history 15min 15 10
Console(config-if)#
```

11.1.6 media-type

このコマンドは、トランシーバモードを強制的に SFP ポートに使用します。デフォルトモードを復元するには、no 形式を使用してください。

構文

media-type {sfp-forced [*mode*]}

no media-type

sfp-forced - SFP ポートのトランシーバモードを強制します。

mode

1000sfp - 常に 1000BASE SFP モードを使用します。

デフォルト設定

SFP ポート: 無し

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

使用可能な sfp 強制モードには次のものがあります:

AXprimoM210-08T/08P: Ports 9-10 (1000BASE SFP)は 1000sfp をサポートします。

例

これにより、スイッチは強制的に SFP ポート 10 に 1000sfp モードを使用します。.

```
Console(config)#interface ethernet 1/10
Console(config-if)#media-type sfp-forced 1000sfp
Console(config-if)#
```

11.1.7 negotiation

本コマンドは、特定のインタフェースのオートネゴシエーションを有効化します。オートネゴシエーションを無効にするには、no 形式を使用してください。

構文

[no] negotiation

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

◆ オートネゴシエーションが有効の場合、スイッチは capabilities コマンドに基づいて最適なリンク設定をネゴシエートします。オートネゴシエーションが無効になっている場合は、speed-duplex コマンドと flowcontrol コマンドでリンク属性を手動で指定する必要があります。

例

次の例では、オートネゴシエーションを使用するようにポート 10 を設定しています。

```
Console(config)#interface ethernet 1/10
Console(config-if)#negotiation
Console(config-if)#
```

関連コマンド

capabilities

speed-duplex

11.1.8 shutdown

本コマンドは、インタフェースを無効にします。無効にしたインタフェースを再起動するには、no 形式を使用します。

構文

[no] shutdown

デフォルト設定

すべてのインタフェースが有効です。

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

このコマンドを使用すると、異常な動作（たとえば、過度の衝突）が起きた場合にポートを無効にして、問題が解決した後でポートを再び有効にすることができます。セキュリティ上の理由から、ポートを無効にすることもできます。

例

次の例では、ポート 5 を無効にします。

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

11.1.9 speed-duplex

このコマンドは、オートネゴシエーションが無効の場合に、特定のインタフェースの速度および duplex モードを設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

speed-duplex {100full | 100half | 10full | 10half}

100full - 強制的に 100 Mbps 全二重動作にします。

100half - 強制的に 100 Mbps の半二重動作にします。

10full - 強制的に 10 Mbps 全二重動作にします。

10half - 強制的に 10 Mbps の半二重動作にします。

デフォルト設定

- オートネゴシエーションはデフォルトで有効になっています。
- オートネゴシエーションが無効の場合、デフォルトの speed-duplex 設定は 1000BASE-T ポートの場合は 100full です。

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- speed-duplex コマンドで指定された速度および duplex モードに強制的に動作させるには、no negotiation コマンドを使用して、選択したインタフェースでオートネゴシエーションを無効にします。
- negotiation コマンドを使用してオートネゴシエーションを有効にする場合、最適な設定は capabilities コマンドによって決定されます。オートネゴシエーションで速度/duplex モードを設定するには、インタフェースの機能リストで必要なモードを指定する必要があります。

例

次に、ポート 5 を 100 Mbps、半二重動作に設定する例を示します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

関連コマンド

negotiation

capabilities

11.1.10 clear counters

このコマンドは、インタフェースの統計情報をクリアします。

構文

clear counters *interface*

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

統計は電源リセット時にのみ初期化されます。本コマンドは、現在の管理セッションで表示される統計情報のベース値をゼロに設定します。

例

次の例では、ポート 5 の統計情報を消去します。

```
Console#clear counters ethernet 1/5
Console#
```

11.1.11 show interfaces brief

本コマンドは、すべてのポートの動作ステータス、ネイティブ VLAN ID、デフォルトプライオリティ、速度/duplex モード、およびポートタイプを含むキー情報の要約を表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

◆ SFP トランシーバがポートに挿入されている場合、タイプフィールドには、イーサネット準拠コード（アドレス A0h のデータバイト 6）から解釈された SFP タイプが表示されます。イーサネットコンプライアンスコードはビットマップ値であり、そのうち 1 ビットはオンになっています。しかし、読み出し値が認識できない場合（例えば、2 ビット以上オンの場合、またはすべて 0 の場合）、タイプフィールドは生データ（16 進数）を表示するだけです。

例

```
Console#show interfaces brief
```

```
Interface Name              Status    PVID Pri Speed/Duplex  Type         Trunk
--------- ----------------- --------- ---- --- ------------- ------------ -----
Eth 1/ 1                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 2                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 3                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 4                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 5                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 6                    Down         1   0 Auto          1000BASE-T   None
.
.
.
```

トランクが設定されている場合、次のように表示されます。

```
Console#show interfaces brief
Interface Name              Status    PVID Pri Speed/Duplex  Type         Trunk
--------- ----------------- --------- ---- --- ------------- ------------ -----
Eth 1/ 1  StaticTrunk3      Up           1   0 Auto-1000full 1000BASE-T   3
Eth 1/ 2  StaticTrunk3      Up           1   0 Auto-1000full 1000BASE-T   3
Eth 1/ 3  StaticTrunk3      Up           1   0 Auto-1000full 1000BASE-T   3
Eth 1/ 4  StaticTrunk3      Up           1   0 Auto-1000full 1000BASE-T   3
Eth 1/ 5                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 6  DynamicTrunk1     Up           1   0 Auto-1000full 1000BASE-T   1
Eth 1/ 7                    Down         1   0 Auto          1000BASE-T   None
Eth 1/ 8  DynamicTrunk1     Up           1   0 Auto-1000full 1000BASE-T   1
Eth 1/ 9                    Down         1   0 Auto          1000BASE SFP None
Eth 1/10                    Down         1   0 Auto          1000BASE SFP None
Trunk  1  DynamicTrunk1     Up           1   0 Auto-1000full 1000BASE-T   1
Trunk  3  StaticTrunk3      Up           1   0 Auto-1000full 1000BASE-T   3
```

11.1.12 show interfaces counters

本コマンドは、インタフェースの統計情報を表示します。

構文

show interfaces counters [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

すべてのインタフェースのカウンタを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

インタフェースが指定されていない場合、すべてのインタフェースに関する情報が表示されます。

例

```
Console#show interfaces counters ethernet 1/1
Ethernet 1/ 1
 ===== IF table Stats =====
                2166458 Octets Input
               14734059 Octets Output
                  14707 Unicast Input
                  19806 Unicast Output
                      0 Discard Input
                      0 Discard Output
                      0 Error Input
 ===== Extended Iftable Stats =====
                     23 Multi-cast Input
                   5525 Multi-cast Output
                    170 Broadcast Input
                     11 Broadcast Output
 ===== Ether-like Stats =====
                      0 FCS Errors
                      0 Single Collision Frames
                      0 Multiple Collision Frames
                      0 Deferred Transmissions
                      0 Late Collisions
                      0 Excessive Collisions
                      0 Internal Mac Transmit Errors
                      0 Frames Too Long
                      0 Symbol Errors
                      0 Pause Frames Input
                      0 Pause Frames Output
 ===== RMON Stats =====
                      0 Drop Events
               16900558 Octets
                  40243 Packets
                    170 Broadcast PKTS
                     23 Multi-cast PKTS
                      0 Undersize PKTS
                      0 Oversize PKTS
                      0 Fragments
                      0 Jabbers
                      0 CRC Align Errors
                      0 Collisions
```

```
                    5271 Packet Size <= 64 Octets
                    3589 Packet Size 65 to 127 Octets
                     222 Packet Size 128 to 255 Octets
                     313 Packet Size 256 to 511 Octets
                     190 Packet Size 512 to 1023 Octets
                     444 Packet Size 1024 to 1518 Octets
 ===== Port Utilization =====
                     111 Octets Input in kbits per second
                       0 Packets Input per second
                    0.00 % Input Utilization
                     606 Octets Output in kbits per second
                       1 Packets Output per second
                    0.00 % Output Utilization
Console#
```

表 11-2 show interfaces counters - 表示の説明

パラメータ	説明
IF table Stats	
Octets Input	フレーミング文字を含むインタフェースで受信されたオクテットの総数です。
Octets Output	フレーミング文字を含むインタフェースから送信されたオクテットの総数です。
Unicast Input	上位層プロトコルに配信されるサブネットワークユニキャストパケットの数です。
Unicast Output	上位プロトコルが要求したパケットのうち、破棄されたパケットや送信されなかったものを含め、サブネットワークユニキャストアドレスに送信されたパケットの総数です。
Discard Input	エラーが検出されていなくても破棄され、上位層のプロトコルに届かなかった受信パケットの数です。パケットバッファが解放されるとパケット破棄が発生する可能性があります。
Discard Output	エラーが検出されていなくても破棄された、送信パケットの数です。パケットバッファが解放されるとパケット破棄が発生する可能性があります。
Error Input	上位層のプロトコルに配信できないようなエラーを含む受信パケットの数です。
Extended IF Table Stats	
Multicast Input	上位（サブ）レイヤに配信された、このサブレイヤのマルチキャストアドレス宛てのパケット数です。
Multicast Output	上位プロトコルが送信を要求した、このサブレイヤのマルチキャストアドレス宛のパケットの総数です（破棄されたパケットまたは送信されなかったパケットを含む）。
Broadcast Input	上位（サブ）レイヤに配信された、このサブレイヤのブロードキャストアドレス宛てのパケット数です。
Broadcast Output	上位プロトコルが送信を要求した、このサブレイヤのブロードキャストアドレス宛のパケットの総数です（破棄されたパケットまたは送信されなかったパケットを含む）。
Etherlike Statistics	
FCS Errors	長さがオクテットの整数であるが、FCS チェックに合格しない特定のインタフェースで受信されたフレームの数です。このカウントには、frame-too-long または frame-too-short エラーで受信したフレームは含まれません。
Single Collision Frames	1 回のコリジョンによって送信が阻害された時に、正常に送信されたフレーム数です。

パラメータ	説明
Multiple Collision Frames	2 回以上のコリジョンによって送信が阻害された時に、正常に送信されたフレーム数です。
Deferred Transmissions	メディアがビジーとなった時に、特定のインタフェース上の最初の送信試行で遅延したフレーム数です。
Late Collisions	パケットの送信の 512 ビット時間後にコリジョンが検出された回数です。
Excessive Collisions	過度のコリジョンのために特定のインタフェースで送信が失敗したフレームの数です。このカウンタは、インタフェースが全二重モードで動作している場合は増加しません。
Internal MAC Transmit Errors	内部 MAC サブレイヤ送信エラーのために、特定のインタフェースでの送信が失敗したフレームの数です。
Frames Too Long	特定のインタフェースで受信されたフレームの最大許容フレームサイズを超えるフレーム数です。
Symbol Errors	100Mb/s で動作するインタフェースの場合、有効なキャリアが存在するときに無効なデータシンボルが存在した回数です。 1000 Mb/s の全二重モードで動作するインタフェースの場合、受信メディアが minFrameSize 以上の期間、non-idle 状態（キャリアイベント）を受信した回数です。この間に GMII 上で「データ受信エラー」を示すイベントが PHY で少なくとも 1 回発生しています。
RMON Statistics	
Octets	ネットワーク上で受信したデータの総オクテット数です。この統計値は、イーサネット使用率の妥当な指標として使用できます。
Packets	受信したパケットの総数です（不良、ブロードキャスト、マルチキャスト）。
Broadcast Packets	ブロードキャストアドレスに送信された正常パケットの総数です。これにはマルチキャストパケットは含まれないことに注意してください。
Multicast Packets	このマルチキャストアドレスに送信された正常パケットの総数です。
Undersize Packets	フレームフォーマットは正常だが、64 オクテット未満の長さ（フレーミングビットは除くが、FCS オクテットを含む）の受信パケットの総数です。
Oversize Packets	フレームフォーマットは正常だが、1518 オクテットより長い（フレーミングビットは除くが、FCS オクテットを含む）受信パケットの総数です。
Fragments	長さが 64 オクテット未満（フレーミングビットは除くが、FCS オクテットを含む）であり、FCS またはアライメントエラーのいずれかを持つ、受信フレームの総数です。
Jabbers	長さが 1518 オクテットよりも長く（フレーミングビットは除くが FCS オクテットを含む）、FCS またはアラインメントエラーのいずれかを持つ受信フレームの総数です。
CRC Align Errors	CRC エラーの起きた回数です。ハードウェアに問題がある可能性があります。
Collisions	このイーサネットセグメント上のコリジョン発生回数です。
64 Octets	長さが 64 オクテット未満（フレーミングビットは除くが、FCS オクテットを含む）だった送受信パケットの総数です（不良パケットを含む）。
65-127 Octets 128-255 Octets 256-511 Octets 512-1023 Octets 1024-1518 Octets	オクテット数が指定された範囲内にある（フレーミングビットを除くが、FCS オクテットを含む）送受信パケットの総数です（不良パケットを含む）。
Utilization Statistics	
Octets input per second	このインタフェースで 1 秒あたりに受信したオクテット数です（単位：kbits）。

パラメータ	説明
Packets input per second	このインタフェースで 1 秒あたりに受信したパケット数です。
Input utilization	このインタフェースの受信使用率です。
Octets output per second	このインタフェースで 1 秒あたりに送信したオクテット数です（単位：kbits）。
Packets output per second	このインタフェースで 1 秒あたりに送信したパケット数です。
Output utilization	このインタフェースの送信使用率です。

11.1.13 show interfaces history

本コマンドは、サンプリング間隔、サンプル数、およびカウンタ値など、統計情報の定期的なサンプリングを表示します。

構文

show interfaces history [*interface* [*name* [current | previous *index count*] [input | output]]]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

name - history コマンドで定義されているサンプル名称です。

(範囲: 1 から 32 文字)

current - 現在の間隔で記録された統計です。

previous - 以前の間隔で記録された統計です。

index - 以前のサンプルを含むバケットへのインデックスです。(範囲: 1 から 96)

count - 表示する履歴サンプルの数です。(範囲: 1 から 96)

input - 受信トラフィックです。

output - 送信トラフィックです。

デフォルト設定

すべてのインタフェースの履歴設定とステータスを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

インタフェースが指定されていない場合、すべてのインタフェースに関する情報が表示されます。

例

```
Console#show interfaces history ethernet 1/1 15min
```

```
Interface         : Eth 1/ 1
Name              : 15min
Interval          : 900 second(s)
Buckets Requested : 96
Buckets Granted   : 1
Status            : Active

Current Entries

 Start Time   %      Octets Input    Unicast       Multicast     Broadcast
 ------------ ------ --------------- ------------- ------------- ------------
 00d 00:15:04   0.00           72675           524            35           41

              Discards      Errors
              ------------- -------------
                         41             0

              %      Octets Output   Unicast       Multicast     Broadcast
              ------ --------------- ------------- ------------- -------------
                0.00          513760           653           336             0

              Discards
              -------------
                          0

Previous Entries

 Start Time   %      Octets Input    Unicast       Multicast     Broadcast
 ------------ ------ --------------- ------------- ------------- ------------
 00d 00:00:03   0.66        80758067        106273        619717         69176

 Start Time   Discards      Errors
 ------------ ------------- -------------
 00d 00:00:03         69176             2

 Start Time   %      Octets Output   Unicast       Multicast     Broadcast
 ------------ ------ --------------- ------------- ------------- ------------
 00d 00:00:03   0.00          677855           705           445            14

 Start Time   Discards
 ------------ -------------
 00d 00:00:03             0
Console#
```

11.1.14 show interfaces status

本コマンドは、インタフェースのステータスを表示します。

構文

show interfaces status [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan *vlan-id* (範囲: 1 から 4094)

デフォルト設定

すべてのインタフェースのステータスを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

インタフェースが指定されていない場合、すべてのインタフェースに関する情報が表示されます。

例

```
Console#show interfaces status ethernet 1/1
Information of Eth 1/1
 Basic Information:
  Port Type              : 1000BASE-T
  MAC Address            : 00-12-E2-00-00-FE
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Enabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  MAC Learning           : Enabled
  Link-up-down Trap      : Enabled
 Current Status:
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 100full
  Up Time                : 0w 0d 1h 11m 2s (4262 seconds)
```

```
  Flow Control Type      : None
  Max Frame Size         : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status    : Enabled
Console#
```

11.1.15 show interfaces switchport

このコマンドは、指定されたインタフェースの管理ステータスおよび動作ステータスを表示します。

構文

show interfaces switchport [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

すべてのインタフェースを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

インタフェースが指定されていない場合、すべてのインタフェースに関する情報が表示されます。

例

次に、ポート 1 の表示例を示します。

```
Console#show interfaces switchport ethernet 1/1
Information of Eth 1/1
 Broadcast Threshold           : Enabled, 500 packets/second
 Multicast Threshold           : Disabled
 Unknown Unicast Threshold     : Disabled
 LACP Status                   : Disabled
 Ingress Rate Limit            : Disabled, 1000M bits per second
 Egress Rate Limit             : Disabled, 1000M bits per second
 VLAN Membership Mode          : Hybrid
 Ingress Rule                  : Disabled
 Acceptable Frame Type         : All frames
 Native VLAN                   : 1
 Priority for Untagged Traffic : 0
 Allowed VLAN                  :     1(u)
 802.1Q Tunnel Status          : Disabled
```

```
 802.1Q Tunnel Mode            : Normal
 802.1Q Tunnel TPID            : 8100 (Hex)
Console#
```

表 11-3 show interfaces switchport - 表示の説明

フィールド	説明
Broadcast Threshold	ブロードキャストストーム抑制が有効か無効かを示します。 有効にすると、閾値レベルも表示されます。
Multicast Threshold	マルチキャストストーム抑制が有効か無効かを示します。 有効にすると、閾値レベルも表示されます。
Unknown Unicast Threshold	未知のユニキャストストーム抑制が有効か無効かを示します。 有効にすると、閾値レベルも表示されます。
LACP Status	リンク集約制御プロトコルが有効か無効かを表示します。
Ingress/Egress Rate Limit	帯域制限が有効になっているかどうか、および現在の制限帯域を表示します。
VLAN Membership Mode	メンバシップモードがトランクまたはハイブリッドであることを示します。
Ingress Rule	受信フィルタリングが有効か無効かを示します。
Acceptable Frame Type	受け入れ可能な VLAN フレームにすべてのタイプまたはタグ付きフレームのみが含まれているかどうかを表示します。
Native VLAN	デフォルトポート VLAN ID を示します。
Priority for Untagged Traffic	タグなしフレームのデフォルトの優先度を示します。
Allowed VLAN	このインタフェースが属する VLAN を示します。ここで、「（u）」はタグなしを示し、「（t）」はタグ付きを示します。
802.1Q-tunnel Status	このインタフェースで 802.1Q トンネルが有効になっているかどうかを表示します。
802.1Q-tunnel Mode	トンネルモードを[標準]、[802.1Q トンネル]、[802.1Q トンネルアップリンク]のいずれかで表示します。
802.1Q-tunnel TPID	パケットの学習と切り替えに使用されるタグプロトコル識別子を表示します。

11.2 トランシーバ閾値設定

11.2.1 transceiver-monitor

本コマンドは、トランシーバの動作値のいずれかが指定された閾値を超えた場合にトラップを送信します。トラップメッセージを無効にするには、no 形式を使用します。

構文

transceiver-monitor

デフォルト設定

無効

コマンドモード

Interface Configuration (SFP Ports)

例

```
Console(config)interface ethernet 1/10
Console(config-if)#transceiver-monitor
Console#
```

11.2.2 transceiver-threshold-auto

本コマンドは、トランシーバから得られたデフォルトの閾値設定を使用して、アラームまたは警告メッセージの送信時期を決定します。この機能を無効にするには、no 形式を使用してください。

構文

transceiver-threshold-auto

デフォルト設定

有効

コマンドモード

Interface Configuration (SFP Ports)

例

```
Console(config)interface ethernet 1/10
Console(config-if)#transceiver-threshold-auto
Console#
```

11.2.3 transceiver-threshold current

本コマンドは、アラームまたは警告メッセージをトリガするために使用できるトランシーバ電流の閾値を設定します。

構文

transceiver-threshold current {high-alarm | high-warning | low-alarm | low-warning} *threshold-value*

high-alarm - アラームメッセージの高電流閾値を設定します。

high-warning - 警告メッセージの高電流閾値を設定します。

low-alarm - アラームメッセージの低電流閾値を設定します。

low-warning - 警告メッセージの低電流閾値を設定します。

threshold-value - トランシーバ電流閾値を設定します。

(範囲: 0 から 13100、単位は 0.01mA）

デフォルト設定

High Alarm: 100 mA

HIgh Warning: 90 mA

Low Warning: 7 mA

Low Alarm: 6 mA

コマンドモード

Interface Configuration (SFP Ports)

コマンドの使用方法

- transceiver-monitor コマンドでトラップメッセージを有効にすると、現在の値が高閾値以上で、前回の値が高閾値よりも小さい場合に、高閾値のアラームまたは警告メッセージが送信されます。高閾値イベントが生成された後は、値が高閾値を下回り、低閾値に達するまで、別のイベントは生成されません。
- transceiver-monitor コマンドでトラップメッセージを有効にすると、現在の値が低閾値以下で、前回の値が低閾値よりも大きい場合に、低閾値のアラームまたは警告メッセージが送信されます。低閾値イベントが生成された後は、値が低閾値を上回り、高閾値に達するまで、別のイベントは生成されません。
- 電力レベルが閾値のちょうど上下で変動することで連続的にイベントメッセージを送信してしまうヒステリシス効果を回避するために、上記のように動作します。
- transceiver-monitor コマンドで有効にされたトラップメッセージは、snmp-server host コマンドで設定された管理ステーションに送信されます。

例

次の例では、ポート 10 のトランシーバ電流アラームの閾値を設定します。

```
Console(config)interface ethernet 1/10
Console(config-if)#transceiver-threshold current low-alarm 100
Console(config-if)#transceiver-threshold current high-alarm 9500
```

```
Console#
```

11.2.4 transceiver-threshold rx-power

本コマンドは、アラームまたは警告メッセージをトリガするために使用できる、トランシーバの受信信号の電力レベルの閾値を設定します。

構文

transceiver-threshold rx-power {high-alarm | high-warning | low-alarm | low-warning} *threshold-value*

high-alarm - アラームメッセージの高電力閾値を設定します。

high-warning - 警告メッセージの高電力閾値を設定します。

low-alarm - アラームメッセージの低電力閾値を設定します。

low-warning - 警告メッセージの低電力閾値を設定します。

threshold-value - 受信信号の電力閾値です。

(範囲: -4000 から 820、単位は 0.01 dBm)

デフォルト設定

High Alarm: -3.00 dBm

HIgh Warning: -3.50 dBm

Low Warning: -21.00 dBm

Low Alarm: -21.50 dBm

コマンドモード

Interface Configuration (SFP Ports)

コマンドの使用方法

- 閾値は、1 ミリワット（mW）を基準とした電力のデシベル単位の電力比(dB)です。
- トランシーバの閾値の設定の詳細については、transceiver-threshold current コマンドのコマンド使用方法の章を参照してください。
- transceiver-monitor コマンドで有効にされたトラップメッセージは、snmp-server host コマンドで設定された管理ステーションに送信されます。

例

次の例では、ポート 10 で受信した信号電力のアラーム閾値を設定します。

```
Console(config)interface ethernet 1/10
Console(config-if)#transceiver-threshold rx-power low-alarm -2300
Console(config-if)#transceiver-threshold rx-power high-alarm -200
Console#
```

11.2.5 transceiver-threshold temperature

本コマンドは、アラームまたは警告メッセージをトリガするために使用できるトランシーバ温度の閾値を設定します。

構文

transceiver-threshold temperature {high-alarm | high-warning | low-alarm | low-warning} *threshold-value*

high-alarm - アラームメッセージの高温閾値を設定します。

high-warning - 警告メッセージの高温閾値を設定します。

low-alarm - アラームメッセージの低温閾値を設定します。

low-warning - 警告メッセージの低温閾値を設定します。

threshold-value - トランシーバ温度の閾値です。

(範囲: -12800 から 12800、摂氏 0.01 度)

デフォルト設定

High Alarm: 75.00 °C

HIgh Warning: 70.00 °C

Low Alarm: -123.00 °C

Low Warning: 0.00 °C

コマンドモード

Interface Configuration (SFP Ports)

コマンドの使用方法

- トランシーバの閾値の設定の詳細については、transceiver-threshold current コマンドのコマンド使用方法の章を参照してください。
- transceiver-monitor コマンドで有効にされたトラップメッセージは、snmp-server host コマンドで設定された管理ステーションに送信されます。

例

次の例では、ポート 10 のトランシーバ温度のアラーム閾値を設定します。

```
Console(config)interface ethernet 1/10
Console(config-if)#transceiver-threshold temperature low-alarm -6000
Console(config-if)#transceiver-threshold temperature high-alarm 9000
Console#
```

11.2.6 transceiver-threshold tx-power

本コマンドは、アラームまたは警告メッセージをトリガするために使用できるトランシーバの送信信号の電力レベルの閾値を設定します。

構文

transceiver-threshold tx-power {high-alarm | high-warning | low-alarm | low-warning} *threshold-value*

high-alarm - アラームメッセージの高電力閾値を設定します。

high-warning - 警告メッセージの高電力閾値を設定します。

low-alarm - アラームメッセージの低電力閾値を設定します。

low-warning - 警告メッセージの低電力閾値を設定します。

threshold-value - 送信信号の電力閾値です。

(範囲: -4000 から 820、単位は 0.01 dBm)

デフォルト設定

High Alarm: -9.00 dBm

HIgh Warning: -9.50 dBm

Low Warning: -11.50 dBm

Low Alarm: -12.00 dBm

コマンドモード

Interface Configuration (SFP Ports)

コマンドの使用方法

- 閾値は、1 ミリワット（mW）を基準とした電力のデシベル単位の電力比(dB)です。
- トランシーバの閾値の設定の詳細については、transceiver-threshold current コマンドのコマンド使用方法の章を参照してください。
- transceiver-monitor コマンドで有効にされたトラップメッセージは、snmp-server host コマンドで設定された管理ステーションに送信されます。

例

次の例では、ポート 10 で送信される信号電力のアラーム閾値を設定します。

```
Console(config)interface ethernet 1/10
Console(config-if)#transceiver-threshold tx-power low-alarm -1000
Console(config-if)#transceiver-threshold tx-power high-alarm -800
Console#
```

11.2.7 transceiver-threshold voltage

本コマンドは、アラームまたは警告メッセージをトリガするために使用できるトランシーバ電圧の閾値を設定します。

構文

transceiver-threshold voltage {high-alarm | high-warning | low-alarm | low-warning} *threshold-value*

high-alarm - アラームメッセージの高電圧閾値を設定します。

high-warning - 警告メッセージの高電圧閾値を設定します。

low-alarm - アラームメッセージの低電圧閾値を設定します。

low-warning - 警告メッセージの低電圧閾値を設定します。

threshold-value - トランシーバ電圧の閾値です。

(範囲: 0 から 655、単位は 0.01V)

デフォルト設定

High Alarm: 3.50 Volts

HIgh Warning: 3.45 Volts

Low Warning: 3.15 Volts

Low Alarm: 3.10 Volts

コマンドモード

Interface Configuration (SFP Ports)

コマンドの使用方法

- トランシーバの閾値の設定の詳細については、transceiver-threshold current コマンドのコマンド使用方法の章を参照してください。
- transceiver-monitor コマンドで有効にされたトラップメッセージは、snmp-server host コマンドで設定された管理ステーションに送信されます。

例

次の例では、ポート 10 のトランシーバ電圧のアラーム閾値を設定します。

```
Console(config)interface ethernet 1/10
Console(config-if)#transceiver-threshold voltage low-alarm 200
Console(config-if)#transceiver-threshold voltage high-alarm 400
Console#
```

11.2.8 show interfaces transceiver

このコマンドは、コネクタのタイプやベンダ関連のパラメータ、温度、電圧、バイアス電流、送信電力、受信電力など、指定されたトランシーバの識別情報を表示します。

構文

show interfaces transceiver [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

デフォルト設定

すべての SFP インタフェースを表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

スイッチは、光トランシーバの診断モニタリングインタフェースの SFF-8472 仕様をサポートする SFP モジュールの診断情報を表示できます。この情報により、管理者は光デバイスの問題を遠隔から診断することができます。コマンドで表示されるデジタル診断モニタリング（DDM）と呼ばれるこの機能は、温度、電源電圧、レーザバイアス電流、レーザパワー、および受信光パワー、および関連するアラーム閾値などのトランシーバパラメータに関する情報を提供します。

例

```
Console#show interfaces transceiver ethernet 1/9
Information of Eth 1/9
 Connector Type        : LC
 Fiber Type            : Single Mode (SM)
 Eth Compliance Codes  : 1000BASE-LX
 Baud Rate             : 2100 MBd
 Vendor OUI            : 00-90-65
 Vendor Name           : FINISAR CORP.
 Vendor PN             : FTRJ1319P1BTL
 Vendor Rev            :
 Vendor SN             : P7M0U6S
 Date Code             : 10-09-14
 DDM Info
   Temperature         : 35.64 degree C
   Vcc                 : 3.25 V
   Bias Current        : 12.13 mA
   TX Power            : -2.36 dBm
   RX Power            : -21.20 dBm
 DDM Thresholds
                          Low Alarm   Low Warning  High Warning    High Alarm
   -----------          ------------  ------------  ------------  ------------
   Temperature(Celsius)       -45.00        -40.00         85.00         90.00
   Voltage(Volts)               2.90          3.00          3.60          3.70
   Current(mA)                  1.00          3.00         50.00         60.00
   TxPower(dBm)               -11.50        -10.50         -2.00         -1.00
   RxPower(dBm)               -23.98        -23.01         -1.00          0.00
Console#
```

11.2.9 show interfaces transceiver-threshold

このコマンドは、温度、電圧、バイアス電流、送信電力、および受信電力のアラーム/警告スレッショルド

を表示します。

構文

show interfaces transceiver-threshold [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

デフォルト設定

すべての SFP インタフェースを表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

- スイッチは、光トランシーバの診断モニタリングインタフェースの SFF-8472 仕様をサポートする SFP モジュールの診断情報を表示できます。この情報により、管理者は光デバイスの問題を遠隔から診断することができます。コマンドで表示されるデジタル診断モニタリング（DDM）と呼ばれるこの機能は、温度、電源電圧、レーザバイアス電流、レーザパワー、受信光パワー、および関連するアラーム閾値などのトランシーバパラメータに関する情報を提供します。
- このコマンドで表示される DDM 閾値は、DDM 準拠のトランシーバが挿入されているポートにのみ適用されます。

例

```
Console#show interfaces transceiver-threshold ethernet 1/10
Information of Eth 1/10
 DDM Thresholds
 Transceiver-monitor         : Disabled
 Transceiver-threshold-auto : Enabled
                           Low Alarm   Low Warning  High Warning    High Alarm
   -----------          -----------  -----------  -----------  -----------
   Temperature(Celsius)       -123.00         0.00        70.00        75.00
   Voltage(Volts)                3.10         3.15         3.45         3.50
   Current(mA)                   6.00         7.00        90.00       100.00
   TxPower(dBm)                -12.00       -11.50        -9.50        -9.00
   RxPower(dBm)                -21.50       -21.00        -3.50        -3.00
Console#
```

11.3 ケーブル診断

11.3.1 test cable-diagnostics

このコマンドは、指定されたポートでケーブル診断を実行して、ケーブル障害（ショート、オープンなど）を診断し、ケーブル長を報告します。

構文

test cable-diagnostics interface *interface*

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

コマンドの使用方法

- ケーブル診断は、ポートリンクアップ速度が 1 Gbps の場合、Digital Signal Processing（DSP）テスト方式を使用して実行されます。DSP はケーブルにパルス信号を送信し、そのパルスの反射を調べることによってケーブルを分析します。ポートのリンクアップ速度が 1 Gbps でない場合、Time Domain Reflectometry（TDR）テスト方法が使用されます。TDR は、ケーブルを介して信号を送信し、反射された信号を読み取ることによって、ケーブルの障害を検出します。ただし、TDR は、リンクが有効かどうかだけを判断することができます。
- このケーブルテストは、長さ 7 から 100 メートルのイーサネットケーブルに対してのみ正確です。
- テストには約 5 秒かかります。show cable-diagnostics コマンドを使用して、一般的なケーブルの障害、各ケーブルペアの状態およびおおよその長さなど、テストの結果を表示します。
- ケーブル診断を実行している間は、ポートはリンクダウンされています。

例

```
Console#test cable-diagnostics interface ethernet 1/8
Console#
```

11.3.2 show cable-diagnostics

このコマンドは、ケーブル診断テストの結果を表示します。

構文

show cable-diagnostics interface [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1):

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

コマンドの使用方法

- 結果には、一般的なケーブルの障害、障害の状態と近似距離、または障害がない場合のおおよそのケーブル長が含まれます。
- リンクダウンポートの場合、報告された障害までの距離は±2 メートル以内で正確です。リンクアップポートの場合、精度は±10 メートルです。
- 診断によって列挙される潜在的な状態は、以下の例の凡例によって示されます。次のテスト結果については、追加情報が提供されています。
  - OK: 正しく終了したペアです。
  - ON: オープンペア、リンク先がありません。
  - IE (Impedance mismatch): 終端インピーダンスが基準範囲内にありません。
  - NS (Not Supported): このメッセージは、1000 Mbps 未満の速度でリンクされたギガビットイーサネットポートに対して表示されます。
  - UN: 不明なエラーです。

例

```
Console#show cable-diagnostics interface ethernet 1/1
TF: Test failed
OK: OK
ON: Open
ST: Short
IE: Impedance error
NC: No cable
NT: Not tested
NS: Not supported
UN: Unknown
Port     Type Link     Pair A   Pair B   Pair C   Pair D   Last
              Status   meters   meters   meters   meters   Updated
-------- ---- -------- -------- -------- -------- -------- -------------------
Eth 1/ 1 GE   Down     OK (2)   OK (2)   OK (1)   OK (1)   20XX-07-31 04:42:32
Console#
```

12 リンクアグリゲーションコマンド

ポートを集約リンク（例, トランク）に静的にグループ化して、ネットワーク接続の帯域幅を増加したり、障害回復を確実に行うことができます。または、リンク集約制御プロトコル（LACP）を使用して、このスイッチと別のネットワークデバイス間のトランクリンクを自動的にネゴシエートできます。動的トランクの場合、スイッチは IEEE802.3ad の LACP に準拠する必要があります。このスイッチは、最大 8 のトランクをサポートします。たとえば、2 つの 1000 Mbps ポートで構成されるトランクは、全二重で動作している場合、4 Gbps の総帯域幅をサポートできます。

表 12-1　リンクアグリゲーションコマンド

コマンド	機能	モード
静的トランク設定コマンド		
port channel load-balance	集約されたリンク内のポート間の負荷分散方法を設定します。	GC
channel-group	トランクにポートを追加します。	IC (Ethernet)
動的トランク設定コマンド※1		
lacp	現在のインタフェースの LACP を設定します。	IC (Ethernet)
lacp admin-key	ポートの管理キーを設定します。	IC (Ethernet)
lacp mode	ポートの LACP モードを設定します。	IC (Ethernet)
lacp port-priority	ポートの LACP ポートプライオリティを設定します。	IC (Ethernet)
lacp system-priority	ポートの LACP システムプライオリティを設定します	IC (Ethernet)
lacp admin-key	ポートチャネルの管理キーを設定します。	IC (Port Channel)
lacp timeout	次の LACPDU を待つタイムアウトを設定します	IC (Port Channel)
トランクステータス表示コマンド		
show lacp	LACP 情報を表示します。	PE
show port-channel load-balance	集約リンクで使用される負荷分散方法を示します。	PE

注※1 設定変更を行う場合は、必ず lacp を無効にしてから各種設定の変更を行い、再度 lacp を有効にしてください。

12.1 ガイドライン

一般的なガイドライン -

- ループを作成しないように、スイッチ間で対応するネットワークケーブルを接続する前にトランクの設定を完了してください。
- 1 つのトランクは最大 8 つのポートを集約できます。
- 接続する両端の装置のポートで、トランクを設定する必要があります。
- トランク内のすべてのポートは、通信モード（速度とデュプレックスモード）、VLAN 割当て、CoS 設定など、同じ方法で設定する必要があります。
- フロントパネルのギガビットポートは、異なるメディアタイプのポートを含めて、一緒にトランクすることができます。
- STP、VLAN、および IGMP の設定は、指定されたポートチャネルを介してトランク全体に対してのみ行うことができます。
- 動的トランクの設定を変更する場合、トランク内ポートを shutdown する、またはケーブルを開放してリンクダウンした状態で行ってください。
- 動的トランクからポートを削除する場合、lacp を無効にしてからポートの Admin-Key を削除してください。

ポートチャネルを動的に作成 -

ポートチャネルにポートを割当てるには、次の基準を満たしている必要があります：

- ポートチャネル内の全てのポートは同じ LACP システムプライオリティを設定する必要があります。
- ポートにはポート管理キーの設定が必要です。ポートチャネルにはポートチャネル管理キーの設定が必要です。
- ポートをポートチャネルに割当てるには、ポート管理キーとポートチャネル管理キーを同じ値に設定する必要があります。

Note: interface port-channel コマンドを設定した場合、コンフィグレーションの show 表示の上部に静的ポートチャネル用のインタフェースが、下部には動的ポートチャネル用のインタフェースが表示されます。LACP のコンフィグレーションをポートチャネルインタフェースに設定すると、静的ポートチャネル用のインタフェースは自動的に削除されます。

Note: ポートチャネルインタフェースの初期値 no snmp-server enable port-traps link-up-down の設定は、該当のチャネルグループにイーサネットインタフェースが参加した場合、参加したイーサネットインタフェースの設定が優先されます。

Note: 同一チャネルに属する LACP ポートでは、装置起動時に構成する最若番ポートのインタフェース設定がその他のポートに動的に反映されます。

12.2 静的トランク設定コマンド

12.2.1 port channel load-balance

このコマンドは、集約されたリンクのポート間で負荷分散方式を設定します（静的トランクと動的トランクの両方）。　デフォルト設定に戻すには、no 形式を使用してください。

構文

port channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port channel load-balance

dst-ip - フレームを宛先 IP アドレスにもとづいてロードバランシングします。

dst-mac - フレームを宛先 MAC アドレスにもとづいてロードバランシングします。

src-dst-ip - フレームを送信元および宛先 IP アドレスにもとづいてロードバランシングします。

src-dst-mac - フレームを送信元 MAC アドレスと宛先 MAC アドレスにもとづいてロードバランシングします。

src-ip - フレームを送信元 IP アドレスにもとづいてロードバランシングします。

src-mac - フレームを送信元 MAC アドレスにもとづいてロードバランシングします。

デフォルト設定

src-dst-mac

コマンドモード

Global Configuration

コマンドの使用方法

- 本コマンドは、スイッチ上のすべての静的トランクと動的トランクに適用されます。
- スイッチのトラフィック負荷がトランク内のすべてのリンクに均等に分散されるようにするには、負荷バランス計算で使用される送信元アドレスと宛先アドレスを選択して、トランク接続に最適な結果を提供します。
  - dst-ip: 同じ宛先 IP アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを通過するトラフィックが多くの異なるホストに向けられているスイッチ間トランクリンクに最適です。宛先 IP アドレスがすべてのトラフィックで同じであるスイッチツーサーバトランクリンクには、このモードを使用しないでください。
  - dst-mac: 同じ宛先 MAC アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを通過するトラフィックが多くの異なるホストを宛先とするスイッチ間トランクリンクに最適です。宛先 MAC アドレスがすべてのトラフィックで同じであるスイッチ間トランクリンクには、このモードを使用しないでください。
  - src-dst-ip: 同じ送信元および宛先 IP アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを経由するトラフィックがさまざまなホストから受信され、多数の異なるホスト宛てのスイッチ間ルータトランクリンクに最適です。
  - src-dst-mac: 同じ送信元および宛先 MAC アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを経由するトラフィックが多くの異なるホストから受信され、多くの異なるホスト宛てのスイッチ間トランクリンクに最適です。

- src-ip: 同じ送信元 IP アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチ間トラフィックが多くの異なるホストから受信されるスイッチ間ルータまたはスイッチ間トランクリンクに最適です。
- src-mac: 同じ送信元 MAC アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを経由するトラフィックが多くの異なるホストから受信されるスイッチ間トランクリンクに最適です。

例

```
Console(config)#port channel load-balance dst-ip
Console(config)#
```

12.2.2 channel-group

このコマンドは、トランクにポートを追加します。　トランクからポートを削除するには、no 形式を使用してください。

構文

channel-group *channel-id*

no channel-group

channel-id - トランクインデックス（範囲: 1-8)

デフォルト設定

現在のポートがこのトランクに追加されます。

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

◆ トランクからポートグループを削除するには、no channel-group を 使用します。

◆ トランクをスイッチから削除するには、no interface port-channel を使用します。

例

次の例では、トランク 1 を作成してポート 10 を追加します。:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#
```

12.3 動的トランク設定コマンド

12.3.1 lacp

このコマンドは、現在のインタフェースの 802.3ad Link Aggregation Control Protocol（LACP）を有効にします。無効にするには、no 形式を使用してください。

構文

[no] lacp

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- LACP トランクの両端のポートは、強制モードまたはオートネゴシエーションのいずれかで全二重に設定する必要があります。
- LACP を使用して別のスイッチで形成されたトランクには、次に使用可能なポートチャネル ID が自動的に割当てられます。
- ターゲットスイッチが接続ポートで LACP も有効にしている場合、トランクは自動的にアクティブになります。
- 設定変更を行う場合は、必ず lacp を無効にしてから各種設定の変更を行い、再度 lacp を有効にしてください。

例

次に、ポート 1 から 3 で LACP を有効にした例を示します。LACP もリンクの反対側のポートで有効になっているため、show interfaces status port-channel 1 コマンドはトランク 1 が確立されていることを示します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/2
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/3
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic Information:
  Port Type             : 1000BASE-T
  MAC Address           : 12-34-12-34-12-3F
Configuration:
  Name                  :
```

```
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Enabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 500 packets/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Storm Threshold Resolution  : 1 packets/second
  Flow Control           : Disabled
  MAC Learning           : Enabled
  Link-up-down Trap      : Enabled
 Current status:
  Created By             : LACP
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 1000full
  Up Time                : 0w 0d 0h 0m 53s (53 seconds)
  Flow Control Type      : None
  Max Frame Size         : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status    : Enabled
  Member Ports           : Eth1/1, Eth1/2, Eth1/3,
  Active Member Ports    : Eth1/1, Eth1/2, Eth1/3,
Console#
```

12.3.2 lacp admin-key (Ethernet Interface)

このコマンドは、ポートの LACP 管理キーを設定します。デフォルト設定に戻すには、no 形式を使用します。LACP を使用する場合、必ずポートの LACP 管理キー及びポートチャネルの LACP 管理キーそれぞれのデフォルト以外の値に設定してください。また、構成するポートとポートチャネルとは必ず同じ LACP 管理キーを設定してください。

構文

lacp {actor | partner} admin-key *key*

no lacp {actor | partner} admin-key

actor - 集約リンクのローカル側です。

partner - 集約リンクのリモート側です。

key - 同じリンク集約グループ（LAG）に属するポートのポート管理キーを同じ値に設定する必要があります。(範囲: 0 から 65535)

デフォルト設定

Actor: ポートのリンク速度（1000f - 4、100f - 3、10f - 2）によって決定、Partner: 0

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

◆ （1）LACP システムの優先順位が一致する場合、(2）LACP ポートの管理キーが一致する場合、(3）LACP ポートチャネルキーが一致する場合（設定されている場合)、ポートは同じ LAG に参加できます。

Note: パートナー管理キーを設定しても、リモートまたはローカルのスイッチ操作には影響しません。ローカルスイッチは、ユーザ参照用のパートナー管理キーを記録するだけです。

◆ デフォルトでは、actor の操作キーはポートのリンク速度（1000f - 4、100f - 3、10f - 2）によって決定され、管理キーにコピーされます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

12.3.3 lacp system-priority

このコマンドは、ポートの LACP システムプライオリティを設定します。デフォルト設定に戻すには、no 形式を使用します。

構文

lacp {actor | partner} system-priority *priority*

no lacp {actor | partner} system-priority

actor - 集約リンクのローカル側です。

partner - 集約リンクのリモート側です。

priority - この優先順位は、リンクアグリゲーショングループ（LAG）メンバシップを決定し、LAG ネゴシエーション中にこのデバイスを他のスイッチに識別するために使用されます。(範囲: 0 から 65535)

デフォルト設定

32768

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

◆ 同じ LAG に参加するには、同じシステムプライオリティでポートを設定する必要があります。

◆ システムプライオリティはスイッチの MAC アドレスと組み合わされて LAG 識別子を形成します。この識別子は、他のシステムとの LACP ネゴシエーション中に特定の LAG を示すために使用されます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

12.3.4 lacp admin-key (Port Channel)

このコマンドは、ポートチャネルの LACP 管理キーを設定します。デフォルト設定に戻すには、no 形式を使用します。LACP を使用する場合、必ずポートの LACP 管理キー及びポートチャネルの LACP 管理キーそれぞれのデフォルト以外の値に設定してください。また、構成するポートとポートチャネルとは必ず同じ LACP 管理キーを設定してください。

構文

lacp admin-key *key*

no lacp admin-key

key - ポートチャネル管理キーは、このスイッチのローカル LACP 設定中に特定のリンクアグリゲーショングループ（LAG）を識別するために使用されます。(範囲: 0 から 65535)

デフォルト設定

0

コマンドモード

Interface Configuration (ポートチャネル)

コマンドの使用方法

◆ （1）LACP システムの優先順位が一致する場合、(2）LACP ポートの管理キーが一致する場合、(3）LACP ポートチャネルキーが一致する場合（設定されている場合)、ポートは同じ LAG に参加できます。

例

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

12.3.5 lacp timeout

このコマンドは、次の LACP データユニット（LACPDU）の受信タイムアウト時間を設定します。

構文

lacp timeout {long | short}

long - 90 秒のタイムアウト時間を指定します。

short - 3 秒のタイムアウト時間を指定します。

デフォルト設定

long

コマンドモード

Interface Configuration (ポートチャネル)

コマンドの使用方法

- ◆ このコマンドで設定されたタイムアウト時間は、送信 LACPDU のアクター状態フィールドの LACP タイムアウトビットに設定されます。パートナースイッチは、アクタースイッチから short が設定された LACPDU を受信すると、LACPDU の送信間隔を 1 秒に調整します。アクタースイッチから long が設定された LACPDU を受信すると、LACPDU の送信間隔が 30 秒に調整されます。
- ◆ 設定されたタイムアウト時間が経過する前にパートナースイッチから LACPDU を受信しない場合、アクタースイッチは当該ポートを LACP グループから削除します。
- ◆ 動的ポートチャネルのメンバポートがポートチャネルを離れると、デフォルトのタイムアウト時間がそのポートに復元されます。

例

```
Console(config)#interface port-channel 1
Console(config-if)#lacp timeout short
Console(config-if)#
```

12.4 トランクステータス表示コマンド

12.4.1 show lacp

このコマンドは、LACP 情報を表示します。

構文

show lacp [*port-channel*] {counters | internal | neighbors | sysid}

port-channel - リンク集約グループのローカル識別子です。(範囲: 1-8)

counters - LACP プロトコルメッセージの統計です。

internal - ローカル側のコンフィグレーションと動作状態です。

neighbors - リモート側のコンフィグレーションと動作状態です。

sysid - すべてのチャネルグループのシステムプライオリティと MAC アドレスの要約です。

コマンドモード

Privileged Exec

例

```
Console#show lacp 1 counters
Port Channel: 1
 Member Port                : Eth 1/8
 LACPDU Sent                : 7
 LACPDU Received            : 6
 MarkerPDU Sent             : 0
 MarkerPDU Received         : 0
 MarkerResponsePDU Sent     : 0
 MarkerResponsePDU Received : 0
 Unknown Packet Received    : 0
 Illegal Packet Received    : 0
.
.
.
```

表 12-2　show lacp counters - 表示の説明

フィールド	説明
LACPDUs Sent	このチャネルグループから送信された有効な LACPDU の数です。
LACPDUs Received	このチャネルグループで受信された有効な LACPDU の数です。
Marker Sent	このチャネルグループから送信された有効なマーカーPDU の数です。
Marker Received	このチャネルグループによって受信された有効なマーカーPDU の数です。
MarkerResponsePDU Sent	このチャネルグループから送信された有効な MarkerResponse PDU の数です。
MarkerResponsePDU Received	このチャネルグループによって受信された有効な MarkerResponse PDU の数です。

フィールド	説明
Unknown Packet Received	（1）Slow プロトコルイーサネットタイプの値を持つが、未知の PDU を含んでいる、または（2）Slow プロトコルグループの MAC アドレスに宛てられているが Slow プロトコルイーサネットタイプを搭載していない、のどちらかのフレーム数です。
Illegal Packet Received	Slow プロトコルイーサネットタイプ値を搭載しているが不正に形成された PDU またはプロトコルサブタイプの不正な値を含むフレームの数です。

```
Console#show lacp 1 internal
Port Channel : 1
Admin Key    : 0
Oper Key     : 4
Timeout      : Long
 ------------------------------------------------------------
 Member Port     : Eth 1/8
 Periodic Time   : 30 seconds
 System Priority : 32768
 Port Priority   : 32768
 Admin Key       : 4
 Oper Key        : 4
 Admin State     : Defaulted, Aggregatable, Long Timeout, Actvie LACP
 Oper State      : Distributing, Collecting, Synchronization, Aggregatable,
                   Long Timeout, Actvie LACP
.
.
.
```

表 12-3　show lacp internal - 表示の説明

フィールド	説明
Admin Key	集約ポートの鍵の現在の管理上の値です。
Oper Key	集約ポートの鍵の現在の操作上の値です。
Timeout	パートナーポート情報を削除する前に、次の LACPDU を待つ時間です。
Periodic Time	受信した LACPDU 情報を無効にするまでの秒数です。
System Priority	このポートチャネルに割当てられた LACP システムプライオリティです。
Port Priority	チャネルグループ内のこのインタフェースに割当てられた LACP ポートプライオリティです。
Admin State, Oper State	actor の状態パラメータの管理値または操作上の値です。 ・Expired - actor の受信機が期限切れの状態です。 ・Defaulted - actor の受信機は、既定の運用パートナー情報を使用しており、パートナーに対して管理的に構成されています。 ・Distributing - false の場合、このリンク上の発信フレームの配信は無効になります。 すなわち配信は現在無効であり、受信したプロトコル情報の管理上の変更または変更がない場合には有効になることは期待されません。 ・Collecting - このリンク上の受信フレームの収集が有効になっています。 すなわち収集が現在有効であり、受信したプロトコル情報の管理上の変更または変更がない場合には無効になることは期待されません。 ・Synchronization - システムは、このリンクを IN_SYNC と見なします。 すなわち、それが正しいリンク集約グループに割当てられており、そのグループ

フィールド	説明
	が互換性のあるアグリゲータに関連付けられており、リンク集約グループのアイデンティティが、送信されたシステム ID および操作上の鍵情報と一致しています。 ・ Aggregation - システムは、このリンクを集約可能と見なします。 すなわち、集約候補となる可能性があります。 ・ Long timeout - LACPDU の周期的な伝送は、遅い伝送速度を使用します。 ・ LACP-Activity - このリンクに関する活動制御値です。(0: Passive; 1: Active)

```
Console#show lacp 1 neighbors
Port Channel : 1
 ------------------------------------------------------------
 Member Port             : Eth 1/8
 Partner Admin System ID : 32768, 00-00-00-00-00-00
 Partner Oper System ID  : 32768, 00-12-E2-8F-2C-A7
 Partner Admin Port ID   : 32768, 8
 Partner Oper Port ID    : 32768, 8
 Partner Admin Key       : 0
 Partner Oper Key        : 4
 Partner Admin State     : Defaulted, Distributing, Collecting,
                           Synchronization, Long Timeout, Passive LACP
 Partner Oper State      : Distributing, Collecting, Synchronization,
                           Aggregatable, Long Timeout, Actvie LACP
.
.
.
```

表 12-4　show lacp neighbors - 表示の説明

フィールド	説明
Partner Admin System ID	ユーザが割当てた LAG パートナーのシステム ID です。
Partner Oper System ID	LACP プロトコルによって割当てられた LAG パートナーのシステム ID です。
Partner Admin Port Number	プロトコルパートナーのポート番号の現在の管理上の値です。
Partner Oper Port ID	ポートのプロトコルパートナーによってこの集約ポートに割当てられた操作ポート番号です。
Port Admin Priority	プロトコルパートナーのポート優先順位の現在の管理上の値です。
Port Oper Priority	パートナーによってこの集約ポートに割当てられたプライオリティ値です。
Admin Key	プロトコルパートナーの Key の現在の管理上の値です。
Oper Key	プロトコルパートナーの Key の現在の操作上の値です。
Admin State	パートナーの状態パラメータの管理値です。（上記の表を参照してください）。
Oper State	パートナーの状態パラメータの操作上の値です（上記の表を参照してください）。

```
 Console#show lacp 1 neighbors
Port Channel     System Priority    System MAC Address
-------------------------------------------------------------------------
           1              32768     00-12-E2-8F-2C-A7
           2              32768     00-12-E2-8F-2C-A7
           3              32768     00-12-E2-8F-2C-A7
           4              32768     00-12-E2-8F-2C-A7
           5              32768     00-12-E2-8F-2C-A7
           6              32768     00-12-E2-8F-2C-A7
           7              32768     00-12-E2-D4-73-A0
           8              32768     00-12-E2-D4-73-A0
.
.
.
```

表 12-5 show lacp sysid - 表示の説明

フィールド	説明
Channel group	このスイッチで設定されたリンク集約グループです。
System Priority※	このチャネルグループの LACP システムプライオリティです。
システム MAC アドレス※	システム MAC アドレスです。

注※ LACP システム優先順位とシステム MAC アドレスが連結され、LAG システム ID が形成されます。

12.4.2 show port-channel load-balance

このコマンドは、集約リンクで使用される負荷分散方法を示します。

コマンドモード

Privileged Exec

例

```
Console#show port-channel load-balance
Trunk Load Balance Mode: Destination IP address
Console#
```

13 PoE コマンド

本章のコマンドは、AXprimoM210-08P の RJ-45 ポート 1 から 8 に接続されている PoE 受電装置に供給される電力を制御します。

スイッチの電源管理により、スイッチの総電力と個々のポートの電力を設定された給電能力内で制御することができます。 接続されている受電装置のポート単位での給電を自動的にオン/オフすることができ、スイッチが割当てられた給電能力を絶対に超えないようにポート単位の電力優先順位を設定することができます。受電装置がスイッチポートに接続されている場合、電源が供給される前にスイッチによってその受電装置が要求する電力クラスの分類が検出されます。受電装置が必要とする電力がポートまたはスイッチ全体の給電能力を超える場合には、電力は供給されません。

表 13-1 PoE コマンド

コマンド	機能	モード
power inline compatible	標準互換の PoE デバイスに電力を供給します。	GC
power inline maximum allocation mode	ポートごとの最大電力割当モードを Class ベースまたは手動に設定します。	GC
power mainpower maximum allocation	装置で供給可能な最大電力量を設定します。	GC
power inline	特定ポートでの受電装置の自動検出をオン/オフします。	IC
power inline maximum allocation	特定ポートに供給可能な最大電力を設定します。	IC
power inline priority	特定ポートへの電力供給の優先順位を設定します。	IC
power inline time-range	特定ポートに、時間範囲での電力供給を設定します。	IC
show power inline status	特定ポートまたはすべてのポートの給電管理の現ステータスを表示します。	PE
show power mainpower	スイッチの電源管理の現ステータスを表示します。	PE
show power inline time-range	特定ポートまたはすべてのポートの時間範囲設定および現ステータスを表示します。	PE

13.1 コマンド説明

13.1.1 power inline compatible

本コマンドにより、スイッチは IEEE 802.3af 標準化より前に設計された受電装置に電力を検出して供給することができます。この機能を無効にするには、no 形式を使用してください。

構文

[no] power inline compatible [*interface*]

interface

ethernet

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 8)

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- スイッチは、ギガビットイーサネット UTP ポートを介して定期的にテスト電圧を送信することによって、接続された受電装置を自動的に検出します。IEEE 802.3af または 802.3at 互換受電装置がこれらのポートのいずれかに差し込まれると、受電装置は試験電圧をスイッチに反映し、スイッチからの給電をオンにすることができます。power inline compatible コマンドを使用すると、このスイッチは IEEE 802.3af または 802.3at 準拠の受電装置と、テスト電圧をスイッチに反映させた最新の 802.3af 準拠の受電装置を検出することができます。テスト電圧を反映しない他のレガシー受電装置を検出することはできません。
- このスイッチでサポートされているレガシー受電装置については、RJ-45 ポートに接続されたデータペアを介して電力を受け入れることができなければなりません。

例

```
Console(config)#power inline compatible
Console(config)#
```

13.1.2 power inline maximum allocation mode

本コマンドは、ポートごとの最大電力割当てモードを Class ベースまたは手動に設定します。デフィルト設定を復元するには、no 形式を使用してください

構文

power inline maximum allocation mode {class | user}

no power inline maximum allocation mode

class - 電力割当ては、受電装置の Class 分類に基づきます。

user - 電力割当ては、power mainpower maximum allocation コマンドまたは power inline maximum allocation コマンドで定義されているユーザ設定にもとづきます。

デフォルト設定

class

コマンドモード

Global Configuration

コマンドの使用方法

IEEE 標準での各電力クラスの最大出力電力を次の表に示します。

表 13-2　電力クラスと最大出力電力

電力クラス	最大出力電力(ワット)
Class 0	15.4
Class 1	4.0
Class 2	7.0
Class 3	15.4
Class 4	30.0

◆ user モードを選択した場合、power inline maximum allocation コマンドで、ポートごとの最適な最大電力割当て量を設定してください。

例

```
Console(config)#power inline maximum allocation mode user
Console(config)#
```

関連コマンド

power inline maximum allocation

13.1.3 power mainpower maximum allocation

本コマンドにより、装置で供給可能な最大電力量を手動で設定します。デフィルト設定を復元するには、no 形式を使用してください

構文

power mainpower maximum allocation *milliwatts*

milliwatts - スイッチの最大電力量です。

(範囲: AXprimoM210-08P は 50000 から 125000 mW)

デフォルト設定

AXprimoM210-08P は 125000 mW

コマンドモード

Global Configuration

コマンドの使用方法

- スイッチの最大電力量を設定すると、電源を集中管理し電源の過負荷状態を防止することができます。
- スイッチに接続された電力需要が電力量の設定を超過すると、供給電力を制限するためにスイッチはポートの電力優先順位設定を使用します。

例

```
Console(config)#power mainpower maximum allocation 180000
Console(config)#
```

関連コマンド

power inline priority

13.1.4 power inline

本コマンドでは、PoE 準拠の受電装置が指定されたポートに接続されているかどうかを自動的に検出し、それに応じて給電をオンまたはオフに切り替えるようにスイッチに指示します。自動検出を無効にする場合は no 形式を使用します

構文

power inline

no power inline

デフォルト設定

PoE 受電装置に対して検出が有効になっています。

コマンドモード

Interface Configuration (イーサネットポート 1 から 8)

コマンドの使用方法

- スイッチはギガビットイーサネット RJ-45 ポートにのみ、電力を供給します。
- PoE 受電装置に対して検出が有効な場合、ポートで検出された電力がポートの電力量またはスイッチの電力量を超えていない場合は、自動的に電力が供給されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#no power inline
Console(config-if)#
```

13.1.5 power inline maximum allocation

本コマンドにより、指定ポートに供給可能な最大電力を設定します。デフィルト設定を復元するには、no 形式を使用してください

構文

power inline maximum allocation *milliwatts*

no power inline maximum allocation

milliwatts - ポートの最大電力量です。

(範囲: 3000 から 33600 ミリワット)

デフォルト設定

33600 ミリワット

コマンドモード

Interface Configuration (イーサネットポート 1 から 8)

コマンドの使用方法

- 接続受電装置に同時に最大電力を供給することができるポート数について、以下の表に示されています。

表 13-3 同時給電を供給するポートの最大数

スイッチ	30W (802.3at)	15.4W (802.3af)	7.5W (802.3af)
AXprimoM210-08P	4	8	8

- 受電装置がスイッチポートに接続され、スイッチがポートまたはスイッチ全体に割当てられた最大電力を超えることが検出された場合には、デバイスに電力は供給されません(例; ポートパワーはオフのままです)。
- power inline maximum allocation mode コマンドで、ポートごとの最大電力割当てモードを手動設定とした場合、本コマンドでの設定が有効となります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline maximum allocation 8000
```

```
Console(config-if)#
```

関連コマンド

power inline maximum allocation mode

13.1.6 power inline priority

本コマンドにより、特定ポートに対して電力供給の優先度を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

power inline priority *priority*

no power inline priority

priority - ポートの電力供給の優先度です。

オプション: 1 (critical)、2(high)、または 3(low)

デフォルト設定

3 (low)

コマンドモード

Interface Configuration (イーサネットポート 1 から 8)

コマンドの使用方法

- 電力供給の優先度は、スイッチに接続されている受電装置からの電力要求がスイッチの電力量を超えた時、どのポートの電力供給を停止させるを決定します。
- 2 つのポートの優先度が同じ場合、ポート番号の小さいポートの方が優先度が高くなります。

  たとえば、すべてのポートの優先度を同じに設定した場合、電力供給の優先順序は port1>port2>port3> の順に優先度が低くなり、port8 が最低優先になります。
- スイッチに接続されている受電装置からの電力要求が、起動中に決定された電力量設定を超過している場合、スイッチはポート電力供給の優先度設定を使用して供給される電力を制御します。下記に例を示します。
  - スイッチが電力量を超過する低優先度ポートに接続された受電装置には、電力が供給されません。たとえば、すべてのポートの優先度が同じで、スイッチの電力量を上回った場合は port8 への電力供給を停止します。
  - critical または high の優先度設定がされたポートに受電装置が接続されることで、スイッチがブートアップ中に決定した電力量を超過した場合、スイッチは 1 つ以上の優先度の低いポートへの電力供給を停止し、優先度の高いポートにのみ電力供給を実施します。
    優先度の低いポート且つポート番号の大きいポートから順に電力供給を停止します。
    低い優先度ポートへの電源をオフにしても、クリティカルポートまたは高優先度ポートへ十分な電力を供給できない場合は、受電装置が接続されているポートのうち、優先度が最も低く、且つポート番号が最も大きいポートへの電力供給が停止します。
- スイッチのブートアップ後に受電装置がポートに接続され、電力量を超過する原因となる場合には、優先度の低いポート且つポート番号の大きいポートへの電力供給が停止されます。

- どのポートにも優先度が設定されておらず、PoE 消費量がスイッチから供給された最大電力を超過する場合には、ポート番号 8(老番)から逆の順序で電源が遮断されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline priority 2
Console(config-if)#
```

13.1.7 power inline time-range

本コマンドでは、PoE が接続された受電装置に供給されているポートに時間範囲での電力供給を設定します。この時間範囲での電力供給設定を削除するには、no 形式を使用してください。

構文

power inline time-range *time-range-name*

no power inline time-range

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

デフォルト設定

無し

コマンドモード

インタフェース設定

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline time-range poe-timer
Console(config-if)#
```

関連コマンド

time-range

13.1.8 show power inline status

本コマンドでは、全ポートまたは特定ポートの PoE 情報を表示します。

構文

show power inline status [*interface*]

interface

ethernet

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(イーサネットポート 1 から 8)

コマンドモード

Privileged Exec

例

```
Console#show power inline status
Unit: 1
Compatible  Mode : Disable
Maximum Allocation Mode : User mode
                  Time                Max      Used
Interface Admin   Range    Oper Class Power    Power    Priority
--------- ------- -------- ---- ----- -------- -------- --------
Eth 1/ 1  Enabled --       Off      -  3360 mW     0 mW Low
Eth 1/ 2  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/ 3  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/ 4  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/ 5  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/ 6  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/ 7  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/ 8  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/ 9  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/10  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/11  Enabled --       Off      - 33600 mW     0 mW Low
Eth 1/12  Enabled --       Off      - 33600 mW     0 mW Low
.
.
.
```

表 13-4 show power inline status - 表示説明

フィールド	説明
Compatible Mode	スイッチが IEEE 802.3af PoE 標準よりも前に設計された受電装置を検出して、電源を供給するかどうかを示します(power inline compatible を参照)。
Maximum Allocation Mode	装置全体の最大電力割当てモードです(power mainpower maximum allocation mode を参照)。
Interface	PoE ポートです。
Admin	ポートに設定された、自動検出設定の管理ステータスです(power inline を参照)。
Time-Range	電力供給時の時間範囲の設定です(time-range を参照)。
Oper	現在の動作状態です(オンまたはオフを表示します)。オーバーロードのために電源がオフになっている場合には、管理ステータスは、有効表示のままになっています。
Class	グローバル設定コマンドの power mainpower maximum allocation mode で

フィールド	説明
	Class 指定されている場合、最大電力割当てクラスが表示されます。クラス情報については、Oper = On の場合のみ表示されます。
Max Power	このポートに割当てられている最大電力量です(power inline maximum allocation を参照) power mainpower maximum allocation mode で Class 指定されている場合は「Class」と表示され、手動設定されている場合は最大電力量が表示されます。
Used Power	ポートでの現在の電力消費量(ミリワット)です。
Priority	ポートの電力供給の優先度設定です。(power inline priority を参照)

13.1.9 show power inline time-range

本コマンドでは、特定ポートまたは全ポートの時間範囲での電力供給状態について表示します。

構文

show power inline time-range *time-range-name* [*interface*]

time-range-name - 時間範囲の名称です。(範囲: 1 から 32 文字)

interface

ethernet

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 8)

コマンドモード

Privileged Exec

例

```
Console#show power inline time-range ethernet 1/5
Interface Time Range Name  Status
--------- ---------------- --------
Eth 1/ 5  poe-timer     Inactive
Console#
```

関連コマンド

power inline time-range

13.1.10 show power mainpower

本コマンドはスイッチの現在の電力供給の使用状況を表示します。

構文

show power mainpower *unit*

unit - ユニット識別子です。(範囲: 1)

コマンドモード

Privileged Exec

例

この例では、利用可能な最大 PoE 電力供給量と最大 PoE 電力割当てを示しています。

```
Console#show power mainpower
Unit 1 PoE Status
 PoE Maximum Available Power  : 740.0 Watts (using joint power)
 PoE Maximum Allocation Power : 370.0 Watts
 System Operation Status      : On
 PoE Power Consumption        : 0.0 Watts
 Software Version             : Version 00A1 (Hex), Build 09 (Hex)

Console#
```

表 13-5 show power mainpower - 表示説明

フィールド	説明
PoE Maximum Available Power	このスイッチが提供可能な最大電力量です。
PoE Maximum Allocation Power	装置全体の電力量です。スイッチに接続されている受電装置が装置全体の電力量より多くの電力を必要とする場合は、ポート単位の電力供給の優先順位設定を使用して、供給される電力を制御します。
System Operation Status	現在の電力供給状況(オン/オフ)を示します。
PoE Power Consumption	スイッチの現在の消費電力です(ワット)。
Software Version	PoE コントローラサブシステムで実行しているソフトウェアのバージョンです。

14 ポートミラーリングコマンド

ソフトウェア監視ツールまたはハードウェアプローブを使用してターゲットポートを分析するために、同じスイッチ上のローカルポートまたは別のスイッチ上のリモートポートからデータをミラーリングすることができます。このスイッチは、次のミラーリングモードをサポートしています。

表 14-1　ポートミラーリングコマンド

コマンド	機能
ローカルミラーリングコマンド	監視対象のポートのトラフィックに影響を与えることなく、別のポートにデータをミラーリングして分析します。
RSPAN ミラーリングコマンド	リモートスイッチからのデータを、専用 VLAN 経由でミラーリングします。

14.1 ローカルポートミラーリングコマンド

この章では、トラフィックを監視する対象のソースポート（送信元ポート）からコピーしたトラフィックを転送するミラーポート（宛先ポート）へのミラーリング方法について説明します。

表 14-2　ミラーポートコマンド

コマンド	機能	モード
port monitor	ミラーセッションを設定します。	IC
show port monitor	ミラーポートの設定を表示します。	PE

14.1.1 port monitor

本コマンドでは、ミラーセッションを設定します。ミラーセッションをクリアするには、no 形式を使用してください。

構文

port monitor *interface* [rx | tx | both]

no port monitor *interface*

interface

ethernet *unit*/*port* (source port)

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

rx - 受信したパケットをミラーリングします。

tx - 送信したパケットをミラーリングします。

both - 受信および送信した両パケットをミラーリングします。

デフォルト設定

- ミラーセッションは定義されていません。
- インタフェースで有効になっている場合、デフォルトミラーリングは受信パケットと送信パケットの両方に適用されます。

コマンドモード

Interface Configuration (イーサネット、宛先ポート)

コマンドの使用方法

- リアルタイム分析のために、送信元ポートから宛先ポートへトラフィックをミラーリングすることができます。
- interface configuration コマンドでイーサネットインタフェースを指定して宛先ポートを設定し、port monitor コマンドを使用してミラーリングするトラフィックの送信元を指定します。宛先ポートはトランクまたはトランクメンバーポートにすることはできません。
- ポートからトラフィックをミラーリングする際、送信元ポートと宛先ポートの速度は合致していなければなりません。合致していない場合、トラフィックが宛先ポートで廃棄される可能性があります。
- 複数のミラーセッションを作成することができます。

◆ 宛先ポートは、トランクまたはトランクメンバーポートにすることはできません。

例

この例では、すべてのパケットをポート 6 から 5 へミラーリングするためのスイッチを設定します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

14.1.2 show port monitor

本コマンドではミラー情報を表示します。

構文

show port monitor [*interface*]

interface - ethernet *unit*/*port* (source port)

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

デフォルト設定

全セッションを表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドにより、現在設定されている送信元ポート、宛先ポートおよびミラーモードを表示します(例; RX、TX、 RX/TX)。

例

以下の例では、設定されたポート 6 から 5 へのミラーリングを表示します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination Port (listen port)  : Eth 1/ 6
 Source Port (monitored Port)    : Eth 1/ 5
 Mode                            : RX/TX
Console#
```

14.2 RSPAN ミラーリングコマンド

リモートスイッチドポートアナライザ(RSPAN)を使用すると、リモートスイッチのトラフィックを異なるスイッチのポートで監視することができます。

表 14-3　RSPAN コマンド

コマンド	機能	モード
rspan source	ミラーリングするための送信元ポートとトラフィックタイプを指定します。	GC
rspan destination	ミラーリングしたトラフィックを監視するための宛先ポートを指定します。	GC
rspan remote vlan	RSPAN VLAN、スイッチの役割、およびアップリンクポートを特定します。スイッチの役割には、送信元ポートを含む「送信元スイッチ」、送信元ポートと宛先ポートを含まない「中間スイッチ」、宛先ポートを含む「宛先スイッチ」があります。	GC
no rspan session	設定した RSPAN セッションを削除します。	GC
show rspan	RSPAN セッションのためのコンフィグレーションを表示します。	PE

設定ガイドライン

RSPAN セッションを設定するには、以下のステップに従ってください:

1. vlan rspan コマンドを使用して、RSPAN で使用する VLAN を設定します。(デフォルト VLAN1 は禁止されています。)
2. rspan source コマンドを使用して、監視するインタフェースとトラフィックタイプ(RX、TX または両方)を指定します。
3. rspan destination コマンドを使用して、RSPAN セッションで監視されるトラフィックの宛先ポートを指定します。
4. rspan remote vlan コマンドを使用して、RSPAN セッションで使用する VLAN、ミラーリングされたトラフィックの送信元、中間リレー、または宛先としてスイッチの役割を指定し、ミラーリングしたトラフィックを転送するために使用するアップリンクポートを設定します。

RSPAN の制限

スイッチで RSPAN を使用するために、下記の制限が適用されます:

- RSPAN Ports - RSPAN 送信元、宛先またはアップリンクとして設定できるのはポートのみであり、静的および動的トランクは許容されません。ポートは、RSPAN インタフェースにおける送信元ポート、宛先ポート、またはアップリンクポートの何れかに設定できます。なお、送信元ポートと宛先ポートを同じスイッチ上で共存できません。
  また、宛先ポートとアップリンクポートは、802.1Q トランクまたはハイブリッド(例; 一般使用)ポートのみ設定することができます。アクセスポートは許容されません。詳細は、switchport mode コマンドを参照してください。。
- Local/Remote Mirror - ローカルミラーセッションの宛先(port monitor コマンドで作成)は、RSPAN トラフィックの宛先として使用することはできません。
- Spanning Tree - スパニングツリーが無効の場合、BPDU は RSPAN VLAN にフラッディングしません。RSPAN がスイッチで無効な場合、MAC アドレス学習は RSPAN アップリンクポートではサポートされません。そのため、RSPAN 設定後にスパニングツリーが有効になった場合でも、RSPAN アップリンクポートにおいて MAC アドレス学習は再開しません。

- Port Security - ポートセキュリティが任意のポートで有効になっている場合、そのポートは RSPAN 送信元ポートまたは宛先ポートとして設定できますが、RSPAN アップリンクポートとして設定することはできません。また、ポートが RSPAN アップリンクポートとして設定されている場合、そのポートでポートセキュリティを有効にすることはできません。

14.2.1 rspan source

このコマンドを使用して、リモートでミラーリングされる送信元ポートとトラフィックタイプを指定します。no 形式を使用して、指定したポートで RSPAN を無効にするか、トラフィックタイプキーワードを使用して、指定したタイプのミラーリングを無効にします。

構文

[no] rspan session *session-id* source interface *interface-list* [rx | tx | both]

session-id - この RSPAN セッションを識別する番号です。(範囲: 1 から 3)

RSPAN セッションに対して異なる VLAN を使用して、ローカルおよびリモート監視を含む、3 つのセッションが許容されています。

interface-list - 1 つ以上のソースポートです。ハイフンを使用して、ポートの連続したリストまたは連続していないポート間のコンマを指定してください。

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

rx - 受信したパケットをミラーリングします。

tx - 送信したパケットをミラーリングします。

both - 受信および送信した両パケットをミラーリングします。

デフォルト設定

TX および RX トラフィックの両方がミラーリングされています。

コマンドモード

Global Configuration

コマンドの使用方法

- 1 つ以上の送信元ポートを、同じスイッチ上または異なるスイッチ上で同じ RSPAN セッションに割り当てることができます。
- RSPAN ポートには、静的および動的トランクを指定できません。
- 802.1Q トランクまたはハイブリッドポートのみ、RSPAN 送信元ポートとして設定することができます。アクセスポートには設定できません。詳細は、switchport mode コマンドを参照してください。
- 送信元ポートと宛先ポートは、同じスイッチ上で設定することはできません。

例

次の例は、ポート 2 とポート 3 からの受信パケットをミラーリングするようにスイッチを設定しています。

```
Console(config)#rspan session 1 source interface ethernet 1/2
Console(config)#rspan session 1 source interface ethernet 1/3
Console(config)#
```

14.2.2 rspan destination

ミラーリングしたトラフィックを監視するための宛先ポートを指定するために、このコマンドを使用します。指定したポート上で RSPAN を無効にするには、no 形式を使用してください。

構文

rspan session *session-id* destination interface *interface* [tagged | untagged]

no rspan session *session-id* destination interface *interface*

session-id - この RSPAN セッションを識別する番号です。(範囲: 1 から 3)

RSPAN セッションに対して異なる VLAN を使用して、ローカルおよびリモート監視を含む、3 つのセッションが許容されています。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

tagged - 宛先ポートから出るトラフィックには、RSPAN VLAN タグが付いています。

untagged - 宛先ポートから出るトラフィックにタグが付いていません。

デフォルト設定

宛先ポートから出るトラフィックには、タグが付いていません。

コマンドモード

Global Configuration

コマンドの使用方法

- セッションごとに同じスイッチに設定できる宛先ポートは 1 つだけですが、同じセッションで複数のスイッチに宛先ポートを設定することができます。
- 802.1Q トランクまたはハイブリッド(例; 一般使用)ポートのみ、RSPAN 宛先ポートとして設定することができます - アクセスポートは許容されません。詳細は、switchport mode コマンドを参照してください。
- RSPAN 宛先としてポートだけを設定することができます - 静的および動的トランクは許可されません。
- 送信元ポートと宛先ポートは、同じスイッチ上で設定することはできません。

例

以下の例では、ミラーリングした RSPAN トラフィックを受信するために、ポート 2 を設定します。

```
Console(config)#rspan session 1 destination interface ethernet 1/2
```

```
Console(config)#
```

14.2.3 rspan remote vlan

RSPAN VLAN、スイッチの役割(送信元スイッチ、中間スイッチまたは宛先スイッチ)およびアップリンクポートを指定するために、このコマンドを使用します。指定した VLAN 上の RSPAN を無効にするには、no 形式を使用してください。

構文

[no] rspan session *session-id* remote vlan *vlan-id*

{source | intermediate | destination} uplink *interface*

session-id - この RSPAN セッションを識別する番号です。(範囲: 1 から 3)

RSPAN セッションに対して異なる VLAN を使用して、ローカルおよびリモート監視を含む、3 つのセッションが許容されています。

vlan-id - 設定した RSPAN VLAN の ID です。(範囲: 1 から 4094)

vlan rspan コマンドを使用して、このコマンドで RSPAN を有効化する前に RSPAN ミラーリングの VLAN をリザーブします。

source - このデバイスを、ミラーリングされたトラフィックの送信元スイッチに指定します。

intermediate - このデバイスを、中間スイッチとして指定し、ミラーリングされたトラフィックを 1 つ以上のソース（アップリンクポート）から 1 つ以上の宛先（アップリンクポート）に透過的に渡します。

destination - このデバイスを、セッションのミラーリングされたトラフィックを受信する宛先ポートで構成された宛先スイッチとして指定します。

uplink - ミラーリングされたトラフィックを送受信するために、設定するポートです。

interface - ethernet *unit*/*port*

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- アップリンクポートは、802.1Q トランクまたはハイブリッド(例; 一般使用)ポートのみ設定することができます - アクセスポートは許容されません。詳細は、switchport mode コマンドを参照してください。
- 送信元スイッチには 1 つのアップリンクポートのみ設定することができますが、中間または宛先スイッチでは設定するアップリンクポート数の制限はありません。
- 宛先ポートおよびアップリンクポートだけが、RSPAN VLAN のメンバーとしてスイッチに割り当てら

れます。switchport allowed vlan コマンドを使用して、任意のポートに RSPAN VLAN を手動で割り当てることはできません。　また、show vlan コマンドでは RSPAN VLAN のメンバーは表示されませんが、設定された RSPAN VLAN ID 表示はされます。

例

以下の例では、VLAN 2 で RSPAN を有効にし、RSPAN 宛先スイッチとして、アップリンクインタフェースをポート 3 として指定します。

```
Console(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3
Console(config)#
```

14.2.4 no rspan session

本コマンドを、設定した RSPAN セッションを削除するために使用します。

構文

no rspan session *session-id*

session-id - この RSPAN セッションを識別する番号です。(範囲: 1 から 3)

RSPAN セッションに対して異なる VLAN を使用して、ローカルおよびリモート監視を含む、3 つのセッションが許容されています。

コマンドモード

Global Configuration

コマンドの使用方法

VLAN データベースから RSPAN VLAN を削除する前に、RSPAN VLAN を無効にするために no rspan session コマンドを使用します(vlan コマンドを参照)。

例

```
Console(config)#no rspan session 1
Console(config)#
```

14.2.5 show rspan

RSPAN セッションのコンフィグレーションを表示するために、このコマンドを使用します。

構文

show rspan session [*session-id*]

session-id - この RSPAN セッションを識別する番号です。(範囲: 1 から 3):

RSPAN セッションに対して異なる VLAN を使用して、ローカルおよびリモート監視を含む、3 つのセッションが許容されています。

コマンドモード

Privileged Exec

例

```
Console#show rspan session
RSPAN Session ID                : 1
Source Ports (mirrored ports)   : None
  RX Only                       : None
  TX Only                       : None
  BOTH                          : None
Destination Port (monitor port) : Eth 1/2
Destination Tagged Mode         : Untagged
Switch Role                     : Destination
RSPAN VLAN                      : 2
RSPAN Uplink Ports              : Eth 1/3
Operation Status                : Up
Console#
```

15 輻輳制御コマンド

スイッチでは、すべてのポートに対して、トラフィックの転送レートを設定することができます。ブロードキャストトラフィックまたはマルチキャストトラフィックの最大閾値を設定することにより、トラフィックストームを制御することができます。また、ブロードキャストおよびマルチキャストストームの境界閾値を設定して、自動的にレート制限をおこなうか、ポートをシャットダウンすることもできます。

表 15-1　輻輳制御コマンド

コマンドグループ	機能
レート制御コマンド	ポートに対して入力および出力レート制限を設定します。
ストームコントロールコマンド	各ポートのトラフィックストーム閾値を設定します。

15.1 レート制限コマンド

レート制限コマンドにより、インタフェース上でのトラフィック送受信の最大レートを制御ができるようになります。

レート制限は各ポートまたはトランクに適用することができます。この機能をインタフェースに設定することにより、トラフィックレートはハードウェアによって監視され、レート制限を超えたトラフィックは破棄されます。

表 15-2　レート制限コマンド

コマンド	機能	モード
rate-limit	インタフェースに対して最大入力または出力レートを設定します。	IC

15.1.1 rate-limit

本コマンドにより、特定インタフェースのレート制限を定義します。レートを指定せずにこのコマンドを使用した場合には、各ポートの最大値でレート制限が有効になります。レート制限を無効にするには、no 形式を使用してください。

構文

rate-limit {input | output} [*rate*]

no rate-limit {input | output}

input - 特定インタフェースの入力レートです。

output - 特定インタフェースの出力レートです。

rate - kbps の最小値です。

(範囲: 64 - 1,000,000 kbits/秒)

レートを設定できる粒度は 16 kbits /秒です。

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- レート制限とストーム制御を同じインタフェースで使用すると、期待と異なる動作となる場合があります。そのため、これらのコマンドを同一インタフェースで使用しないでください。
- コマンドの no 形式を使うとインタフェースのレート制限を無効にできます。コマンド”show interfaces swithcport”を実行すると、パラメータ”Ingress Rate Limit”と”Egress Rate Limit”が無効状態で表示され、ポートの最大スピードが表示されます。例にある出力側レート制限を無効にしたときの表示を参照してください。
- レート制限が適用されると、コマンドが running-config に表示されます。しかし、コマンドの no 形式を入力すると、元々のレート制限コマンドはそのまま残り、直下に no 形式のコマンドが表示されます。下記のコンソール出力画面を参照してください。

```
Console#config
Console(config)#interface ethernet 1/4
Console(config-if)#rate-limit output 200
Console(config-if)#end
Console#show running-config
~
interface ethernet 1/3
!
interface ethernet 1/4
 rate-limit output 200
!
interface ethernet 1/5
~
Console#config
Console(config)#interface ethernet 1/4
Console(config-if)#no rate-limit output
Console(config-if)#end
Console#show running-config
~
interface ethernet 1/3
!
interface ethernet 1/4
 rate-limit output 200
 no rate-limit output
!
interface ethernet 1/5
~
```

- running-config に、レート制限コマンドとコマンドの no 形式が同時に表示される場合、レート制限機能は無効になっています。
- running-config からレート制限の表示を削除するためには、下記の手順を実施してください。
  - 1.ポートの最大帯域でレート制限を設定します。(e.g. rate-limit input 1000000)
  - 2.コマンドの no 形式を入力します。(e.g. no rate-limit input)

例

この例では、イーサネットポート 1 の受信側レート制限を 64kbits/s に設定し、送信側レート制限を無効にします。

```
Console(config)#interface ethernet 1/1
```

```
Console(config-if)#rate-limit input 64
Console(config-if)#no rate-limit output
Console(config-if)#end
Console#show interfaces switchport ethernet 1/1
 Information of Eth 1/1
 Broadcast Threshold : Disabled
 Multicast Threshold : Disabled
 Unknown Unicast Threshold : Disabled
 Storm Threshold Resolution : 1 packets/second
 LACP Status : Disabled
 Ingress Rate Limit : Enabled, 64 kbits/second
 Egress Rate Limit : Disabled, 1000000 kbits/second
 Rate Limit Resolution : 16 kbits/second
 VLAN Membership Mode : Hybrid
 Ingress Rule : Enabled
 Acceptable Frame Type : All frames
 Native VLAN : 1
 Priority for Untagged Traffic : 0
 Allowed VLAN : 1(u)
 Forbidden VLAN :
 802.1Q Tunnel Status : Disabled
 802.1Q Tunnel Mode : Normal
 802.1Q Tunnel TPID : 8100 (Hex)
Console#
```

関連コマンド

show interfaces switchport

15.2 ストームコントロールコマンド

ストームコントロールコマンドは、ブロードキャスト、マルチキャスト、および未知のユニキャストトラフィックに対して、ストームコントロールの閾値を設定するために使用します。ネットワーク構成間違いや、ネットワーク上のデバイス、もしくはユーザが使用するアプリケーションプログラムが誤動作した場合、トラフィックストームが発生する場合があります。ネットワークに意図しないトラフィックが多すぎると、ユーザトラフィックのパフォーマンスが著しく低下するか、あるいは停止する可能性があります。

ブロードキャスト、マルチキャストまたは未知のユニキャストトラフィックに閾値を設定することにより、ネットワークをトラフィックストームから防御することができます。指定した閾値を超えるパケットについては破棄されます。

表 15-3 レート制限コマンド

コマンド	機能	モード
switchport packet-rate	ブロードキャスト、マルチキャスト、および未知のユニキャストストームの制御閾値を設定します。	IC

15.2.1 switchport packet-rate

本コマンドにより、ブロードキャスト、マルチキャストおよび未知のユニキャストストームコントロールを設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

switchport {broadcast | multicast | unknown-unicast} packet-rate *rate*

no switchport {broadcast | multicast | unknown-unicast}

broadcast - ブロードキャストトラフィックをストームコントロールの対象とします。

multicast - マルチキャストトラフィックをストームコントロールの対象とします。

unknown-unicast - 未知のユニキャストトラフィックをストームコントロールの対象とします。

rate - レートとしての閾値レベルです; 例. (範囲: 500 から 262142 pps)

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- トラフィックがブロードキャストおよびマルチキャストまたは未知のユニキャストトラフィックの指定された閾値を超えた場合、閾値を超えるパケットは、通信レートが閾値を下回るまで廃棄されます。
- レート制限とストームコントロールを同じインタフェースで使用すると、期待と異なる動作となる場合があります。そのため、これらのコマンドを同一インタフェースで使用しないでください。

例

以下の例では、ブロードキャストストームコントロールを 600 パケット/秒で設定する方法を示します:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

関連コマンド

show interfaces switchport

16 ループ検知コマンド

スイッチは、ハードウェア問題や工場出荷時のプロトコル設定が原因の一般的なループバック状態を検出するよう、設定することができます。有効にした場合、参加するポートで制御フレームが送信され、スイッチはインバウンドトラフィックを監視して、フレームがループバックされているかどうかを確認します。

表 16-1　ループバック検出コマンド

コマンド	機能	モード
loopback-detection	スイッチまたは特定のインタフェース上で、ループバック検出を有効にします。	GC, IC
loopback-detection action	検出されたループバック条件に対して行う応答を指定します。	GC
loopback-detection recover-time	シャットダウン状態からインタフェースを解放する前の待機する間隔を特定します。	GC
loopback-detection transmit-interval	ループバック検出制御フレームを送信する間隔を指定します。	GC
loopback detection trap	ループバック状態が検出時、またはスイッチがループバックから回復した時にトラップを送信するようにスイッチを設定します。	GC
loopback-detection release	ループバック検出機能を使用して現在シャットダウンされている、すべてのインタフェースを手動で解放します。	PE
show loopback-detection	スイッチまたは特定インタフェースの、ループバック検出コンフィグレーションを表示します。	PE

16.1 使用上のガイドライン

- 制御フレームの送信間隔をデフォルト設定に調整し、特定の環境のパフォーマンスを向上させることができます。ループバックされているパケットの種類を判断する場合、シャットダウンモードも変更する必要があります。
- 本章で説明するコマンドによって提供される一般的なループバック検出と、スパニングツリープロトコルによって提供されるループバック検出の両方を同時に有効にすることはできません。スパニングツリープロトコルでループバック検出が有効になっている場合には、同じインタフェース上で一般ループバック検出を有効にすることはできません。インタフェース上で一般的なループバック検出を有効にしたい場合は、同じインタフェース上でのスパニングツリープロトコルを無効(spanning-tree spanning-disabled を設定)にしてください。
- インタフェースでループバックイベントが検出された場合、または、インタフェースがループバックイベントに起因するシャットダウン状態から解放された場合、トラップメッセージが送信され、システムログにイベントが記録されます。
- ループバック検出を有効にするには、ループバック検出をグローバルでもインタフェース上でも有効にする必要があります。
- インタフェースでループバックイベントが検出された後、自動的にインタフェースをシャットダウン状態から解放する設定が有効である場合、その監視タイマは装置起動もしくは loopback-detection recover-time コマンド実行を契機に装置共通で実行されます。そのため、ループバックイベント検出後の 1 回目の解放までの時間は設定値より短くなります。

16.2 コマンド説明

16.2.1 loopback-detection

本コマンドにより、スイッチまたは特定インタフェースにおいてループバック検出をグローバルに有効にします。ループバック検出を無効にするには、no 形式を使用してください。

構文

[no] loopback-detection

デフォルト設定

有効

コマンドモード

Global Configuration

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- ループバック検出は、このコマンドによってスイッチに対してグローバルに有効にする必要があり、そしてこの機能を有効にする特定のインタフェースに対して有効にする必要があります。
- スパニングツリーがグローバルに有効になり、かつインタフェース上でスパニングツリーが有効(spanning-tree spanning-disabled を設定していない）の場合、ループバック検出は無効となります。スパニングツリーがグローバルで有効時に特定インタフェースにてループバック検出を有効にしたい場合は、該当インタフェースにおけるスパニングツリーアルゴリズムを無効(spanning-tree spanning-tree-disable を設定)にしてください。

例

この例では、スイッチ上で一般的なループバック検出を有効にし、ポート 1 でスパニングツリープロトコルに提供されたループバック検出を無効にしてから、そのポートに対して一般的なループバック検出を有効にします。

```
Console(config)#loopback-detection
Console(config)#interface ethernet 1/1
Console(config-if)#no spanning-tree loopback-detection
Console(config-if)#spanning-tree spanning-disable
Console(config-if)#loopback-detection
Console(config)#
```

16.2.2 loopback-detection action

本コマンドは、ループバック状態が検出されたときにスイッチが行う保護動作を指定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

loopback-detection action {none | shutdown}

no loopback-detection action

none - 何もアクションしません。

shutdown - インタフェースをシャットダウンします。

デフォルト設定

シャットダウン

コマンドモード

Global Configuration

コマンドの使用方法

- 自ポートから送信した制御フレームを受信した場合、ポートがループ状態にあり、フレームペイロード内の VLAN も、間違った VLAN タグでループ状態になっていることを意味します。したがって、ループしたポートはシャットダウンする必要があります。
- loopback-detection recover-time コマンドを使用して、ループバック検出処理でインタフェースシャットダウンを再有効化する前に、待機時間を設定します。
- ループバック検出時の動作を変更すると、ループバック検出処理によってシャットダウン状態に置かれたポートは、残存の回復時間にかかわらず直ちにシャットダウン状態が解除されます。

例

この例では、ループバック検出モードを設定して、ユーザトラフィックをシャットダウンします。

```
Console(config)#loopback-detection action shutdown
Console(config)#
```

16.2.3 loopback-detection recover-time

本コマンドにより、スイッチが自動的にインタフェースをシャットダウン状態から解放するまで待機する間隔を指定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

loopback-detection recover-time *seconds*

no loopback-detection recover-time

seconds - シャットダウン状態からの回復時間です。(範囲: 60 から 1,000,000 秒、または 0(自動回復を無効にします)

デフォルト設定

60 秒

コマンドモード

Global Configuration

コマンドの使用方法

- 自動回復時間を変更すると、ループバック検出処理によってシャットダウン状態に置かれたポートは、残存の回復時間にかかわらず直ちに動作状態に復元されます。
- 回復時間を 0 に設定すると、ループ検知でシャットダウンしたポートを自動で開放しません。loopback-detection release コマンドを使用して、シャットダウン状態に置かれているすべてのポートを動作状態に復元することができます。
- 自動回復時間のタイマは装置単位で制御しているため、ループ検知でシャットダウンしたポートが設定した回復時間より早くシャットダウン状態から解放される場合があります。ループ状態が継続していた場合、再度ループ検知でシャットダウンし、その後は設定した回復時間でポートの動作状態を復元します。

例

```
Console(config)#loopback-detection recover-time 120
Console(config-if)#
```

16.2.4 loopback-detection transmit-interval

本コマンドにより、ループバック検出制御フレームを送信する間隔を指定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

loopback-detection transmit-interval *seconds*

no loopback-detection transmit-interval

seconds - ループバック検出制御フレームの送信間隔です。(範囲: 1 から 32767 秒)

デフォルト設定

10 秒

コマンドモード

Global Configuration

例

```
Console(config)#loopback-detection transmit-interval 60
Console(config)#
```

16.2.5 loopback-detection trap

本コマンドでは、ループバック状態の検出時や、スイッチがループバック状態から回復した際にトラップ

を送信します。デフォルト状態を復元するには、no 形式を使用してください。

構文

loopback-detection trap [both | detect | none | recover]

no loopback-detection trap

both - ループバック状態の検出時や、スイッチがループバック状態から回復した際に SNMP トラップメッセージを送信します。

detect - ループバック状態の検出時に SNMP トラップメッセージを送信します。

none - ループバック検出または回復時に SNMP トラップメッセージを送信しません。

recover - スイッチがループバック状態から回復した際に、SNMP トラップメッセージを送信します。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

ループバック回復を構成する条件に関する情報については、loopback-detection recover-time コマンドを参照してください。

例

```
Console(config)#loopback-detection trap both
Console(config)#
```

16.2.6 loopback-detection release

本コマンドは、ループバック検出機能によって現在シャットダウンされている、すべてのインタフェースを解放します。

構文

loopback-detection release

コマンドモード

Privileged Exec

例

```
Console#loopback-detection release
Console(config)#
```

16.2.7 show loopback-detection

本コマンドにより、スイッチまたは指定されたインタフェースのループバック検出設定を表示します。

構文

show loopback-detection [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

```
Console#show loopback-detection
Loopback Detection Global Information
 Global Status     : Enabled
 Transmit Interval : 10
 Recover Time      : 60
 Action            : Shutdown
 Trap              : None
Loopback Detection Port Information
 Port      Admin State  Oper State
 --------  -----------  ----------
 Eth 1/ 1  Enabled      Normal
 Eth 1/ 2  Disabled     Disabled
 Eth 1/ 3  Disabled     Disabled
.
.
.
Console#show loopback-detection ethernet 1/1
Loopback Detection Information of Eth 1/1
 Admin State : Enabled
 Oper State  : Normal
 Looped VLAN : None
Console#
```

17 MAC アドレステーブルコマンド

これらのコマンドは指定のアドレスのフィルタリングや、現在のエントリの表示、テーブルのクリア、およびエージングタイムなどの、アドレステーブルに関する設定に使用されます。

表 17-1　MAC アドレステーブルコマンド

コマンド	機能	モード
mac-address-table aging-time	アドレステーブルのエージングタイムを設定します。	GC
mac-address-table static	静的アドレスを、VLAN のポートにマップします。	GC
clear mac-address-table dynamic	学習したエントリを転送データベースから削除します。	PE
show mac-address-table	ブリッジ転送データベースのエントリを表示します。	PE
show mac-address-table aging-time	アドレステーブルのエージングタイムを表示します。	PE
show mac-address-table count	使用された MAC アドレス数と使用可能な MAC アドレス数を表示します。	PE

17.1 コマンド説明

17.1.1 mac-address-table aging-time

本コマンドでは、アドレステーブル内のエントリのエージングタイムを設定します。デフォルトのエージングタイムを復元するには、no 形式を使用してください。

構文

mac-address-table aging-time *seconds*

no mac-address-table aging-time

seconds - エージングタイム(範囲: 6 から 7200 秒; エージングを無効にするには 0)

デフォルト設定

300 秒

コマンドモード

Global Configuration

コマンドの使用方法

エージングタイムは、動的に学習された転送情報のエージングに使用されます。

例

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

17.1.2 mac-address-table static

本コマンドでは、静的アドレスを VLAN の宛先ポートにマップします。アドレスを削除するには、no 形式を使用してください。

構文

mac-address-table static *mac-address* interface *interface* vlan *vlan-id* [*action*]

no mac-address-table static *mac-address* vlan *vlan-id*

mac-address - MAC アドレス

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

action -

delete-on-reset - 割当てはスイッチがリセットされるまで継続します。

permanent - 割当ては永久的です。

デフォルト設定

静的アドレスは定義されていません。デフォルトモードは、permanent です。

コマンドモード

Global Configuration

コマンドの使用方法

ホストデバイスの静的アドレスは、特定 VLAN 内の指定ポートへ割り当てることができます。このコマンドを使用して、静的アドレスを MAC Address Table に追加します。静的アドレスには、以下の特徴があります:

- 付与されたインタフェースリンクがダウンしている場合、静的アドレスはアドレステーブルから削除されません。
- 静的アドレスは割り当てられたインタフェースにバインディングし、削除されません。静的アドレスが他のインタフェース上に見られる場合、アドレスは無視されアドレステーブルには書き込まれません。
- 静的アドレスは、アドレスがコマンドの no 形式で削除されるまで、他のポートで学習することができません。
- 静的 MAC エントリの最大数は 1024 です。

  最大数はポートセキュリティ機能で学習したセキュア MAC アドレス数との合算になります。

例

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet 1/1 vlan 1
delete-on-reset
Console(config)#
```

17.1.3 clear mac-address-table dynamic

本コマンドでは、転送データベースからすべての学習したエントリを削除します。

構文

clear mac-address-table dynamic [address *mac-address* | interface *interface* | vlan *vlan-id* | all]

mac-address - MAC ハードウェアアドレスです。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

all - 学習した全てのエントリです。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

MAC アドレスのハッシュコリジョンが解決した場合でも、このコマンドでテーブルをリセットするか、またはシステムをリセットするまで、MAC アドレステーブルは削除されません。

例

```
Console#clear mac-address-table dynamic
Console#
```

17.1.4 show mac-address-table

本コマンドでは、ブリッジ転送データベース内のエントリのクラスを表示します。

構文

show mac-address-table [address *mac-address* [*mask*]] [interface *interface*] [vlan *vlan-id*] [sort {address | vlan | interface}]

mac-address - MAC アドレス

mask - アドレス内で合致するビットです。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

sort - アドレス、vlan またはインタフェースでソートします。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

◆ MAC Address Table には、各インタフェースに関連する MAC アドレスが含まれています。フィールド

Type には、以下のタイプが含まれることに留意してください:

- Learn - 動的アドレスエントリです。
- Config - 静的エントリです。
- Security - ポートセキュリティです。

フィールド Life Time には、該当 MAC アドレスが以下の契機に削除されるかを意味します。

- Delete on Reset - 装置再起動で削除されるエントリです。
- Delete on Timeout - エージングタイムアウトにより削除されるエントリです。
- Permanent - 削除されることはないエントリです。

◆ マスクは、指定された MAC アドレスに適用される xx-xx-xx-xx-xx-xx という形式の 16 進数(等価ビットマスクを表す)である必要があります。等価なバイナリビット 0 はビットが有効であることを意味し、 1 はビットを無視することを意味する 16 進数を入力してください。たとえば、00-00-00-00-00-00 のマスクは完全一致を意味し、FF-FF-FF-FF-FF-FF のマスクは「任意」を意味します。

◆ アドレスエントリの最大数は、8K です。

例

```
Console#show mac-address-table
 Interface MAC Address       VLAN Type     Life Time
 --------- ----------------- ---- -------- -----------------
  CPU      00-12-E2-00-00-01    1 CPU      Delete on Reset
  Eth 1/ 1 00-12-E2-10-90-09    1 Learn    Delete on Timeout
  Eth 1/ 1 00-12-E2-94-34-64    1 Learn    Delete on Timeout
Console#
```

17.1.5 show mac-address-table aging-time

本コマンドでは、アドレステーブル内のエントリのエージングタイムを表示します。

デフォルト設定

無し

コマンドモード

Privileged Exec

例

```
Console#show mac-address-table aging-time
 Aging Status : Enabled
 Aging Time: 300 sec.
Console#
```

17.1.6 show mac-address-table count

本コマンドでは、システム全体またはインタフェースで使用される MAC アドレス数と利用可能な MAC アドレスを表示します。

構文

show mac-address-table count [interface *interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Privileged Exec

例

```
Console#show mac-address-table count interface ethernet 1/1

MAC Entries for Eth 1/1
Total Address Count      :0
Static Address Count     :0
Dynamic Address Count    :0

Console#show mac-address-table count

Compute the number of MAC Address...

Maximum number of MAC Address which can be created in the system:
Total Number of MAC Address      : 16384
Number of Static MAC Address     : 1024

Current number of entries which have been created in the system:
Total Number of MAC Address      : 3
Number of Static MAC Address     : 1
Number of Dynamic MAC Address    : 2
Console#
```

18 スパニングツリーコマンド

本章には、スイッチのスパニングツリーアルゴリズム(STA)をグローバルに設定するコマンド、および選択したインタフェースに対してスパニングツリーアルゴリズムを設定するコマンドが含まれています。

表 18-1　スパニングツリーコマンド

コマンド	機能	モード
spanning-tree	スパニングツリープロトコルを有効にします。	GC
spanning-tree forward-time	スパニングツリーブリッジの転送期間を設定します。	GC
spanning-tree hello-time	スパニングツリーブリッジのハロータイムを設定します。	GC
spanning-tree max-age	スパニングツリーブリッジの最大有効期間を設定します。	GC
spanning-tree mode	STP、RSTP または MSTP モードを設定します。	GC
spanning-tree mst configuration	MSTP 設定モードに変更します。	GC
spanning-tree pathcost method	RSTP/MSTP のパスコスト方式を設定します。	GC
spanning-tree priority	スパニングツリーブリッジの優先度を設定します。	GC
spanning-tree system-bpdu-flooding	グローバルスパニングツリーが無効の場合、他のすべてのポートまたは同じ VLAN 内の他のすべてのポートに BPDU（ブリッジプロトコルデータユニット）をフラッディングします。	GC
spanning-tree transmission-limit	RSTP/MSTP の送信間隔を設定します。	GC
max-hops	BPDU が破棄される前に、領域内で許可されているホップの最大数を設定します。	MST
mst priority	スパニングツリーインスタンスの優先度を設定します。	MST
mst vlan	スパニングツリーインスタンスに VLAN を追加します。	MST
name	マルチプルスパニングツリーの名称を設定します。	MST
revision	マルチプルスパニングツリーのリビジョン番号を設定します。	MST
spanning-tree bpdu-filter	エッジポートの BPDU をフィルタリングします。	IC
spanning-tree bpdu-guard	BPDU を受信した場合、エッジポートをシャットダウンします。	IC
spanning-tree cost	インタフェースのスパニングツリーパスコストを設定します。	IC
spanning-tree edge-port	インタフェースをエッジポートに指定します。	IC
spanning-tree link-type	RSTP/MSTP のリンクタイプを設定します。	IC
spanning-tree loopback-detection	ポートの BPDU ループバック検出を有効にします。	IC
spanning-tree loopback-detection action	ユーザトラフィックをブロック、またはインタフェースをシャットダウンするために、ループバック検出の応答を設定し	IC

コマンド	機能	モード
	ます。	
spanning-tree loopback-detection release-mode	ポートのループバック解放モードを設定します。	IC
spanning-tree loopback-detection trap	ポートの BPDU ループバック SNMP トラップ通知を有効にします。	IC
spanning-tree mst cost	MST でインスタンスのパスコストを設定します。	IC
spanning-tree mst port-priority	MST のインスタンスの優先度を設定します。	IC
spanning-tree port-bpdu-flooding	グローバルスパニングツリーが無効の場合、BPDU を他のポートにフラッディングします。	IC
spanning-tree port-priority	インタフェースのスパニングツリー優先度を設定します。	IC
spanning-tree root-guard	指定されたポートが上位 BPDU を通過するのを防ぎます。	IC
spanning-tree spanning-disabled	インタフェースのスパニングツリーを無効にします。	IC
spanning-tree tc-prop-stop	トポロジ変更情報の伝播を停止します。	IC
spanning-tree loopback-detection release	ループバック検出によって Discarding 状態のポートを、手動で解放します。	PE
spanning-tree protocol-migration	適切な BPDU フォーマットを再確認します。	PE
show spanning-tree	共通スパニングツリー(例; ブリッジ全体)、選択されたインタフェース、またはマルチプルスパニングツリー内のインスタンスのスパニングツリー構成を表示します。	PE
show spanning-tree mst configuration	マルチプルスパニングツリー構成を表示します。	PE

18.1 コマンド説明

18.1.1 spanning-tree

本コマンドでは、スイッチのスパニングツリーアルゴリズムをグローバルに有効にします。無効にするには、no 形式を使用してください。

構文

[no] spanning-tree

デフォルト設定

スパニングツリーは無効です。

コマンドモード

Global Configuration

コマンドの使用方法

- スパニングツリーアルゴリズムは、ネットワークループの検出と無効化、スイッチ、ブリッジ、ルータ間のバックアップリンクを提供することができます。これにより、スイッチはネットワーク内の他のブリッジングデバイス(STA 準拠のスイッチ、ブリッジ、またはルータ)と連携して、ネットワーク上の 2 つのステーション間で通信経路の冗長化を可能とし、 プライマリリンクがダウンするとバックアップリンクに通信経路を切り替えることができます。
- 本コマンドにより、スパニングツリーがグローバルに有効になり、かつインタフェース上でスパニングツリーが有効(spanning-tree spanning-disabled を設定していない）の場合、ループバック検出は無効となります。

例

この例では、スイッチのスパニングツリーアルゴリズムを有効にする方法を表示します。

```
Console(config)#spanning-tree
Console(config)#
```

18.1.2 spanning-tree forward-time

本コマンドにより、スイッチのスパニングツリーブリッジの転送時間をグローバルに設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds - 秒単位の時間です。(範囲: 4 から 30 秒)

最小値は 4 以上または[(max-age / 2) + 1]です。

デフォルト設定

15 秒

コマンドモード

Global Configuration

コマンドの使用方法

本コマンドにより、スパニングツリーの状態が変わる前に(例; discarding → learning → forwarding)、ポートが待機する最長時間(秒単位)を設定します。この遅延は、すべてのデバイスがフレーム転送を開始する前にトポロジの変更に関する情報を受信する必要があるためにあります。

例

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

18.1.3 spanning-tree hello-time

本コマンドでは、スイッチがスパニングツリーブリッジのルートブリッジデバイスである場合、ハロータイムをグローバルに設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree hello-time *time*

no spanning-tree hello-time

time - 秒単位の時間です。(範囲: 1 から 10 秒)

最大値は 10 秒、または[(max-age / 2) - 1]の低いほうです。

デフォルト設定

2 秒

コマンドモード

Global Configuration

コマンドの使用方法

本コマンドにより、ルートブリッジデバイスのみ有効で、設定メッセージを送信する間隔(秒単位で)を設定します。

例

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

18.1.4 spanning-tree max-age

本コマンドでは、スイッチのスパニングツリーブリッジ最大エージングタイムをグローバルに設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree max-age *seconds*

no spanning-tree max-age

seconds - 秒単位の時間です。(範囲: 6 から 40 秒)

最低値は 6 以上か、または[2 x (hello-time + 1)]です。

最大値は 40 以下、または[2 x (forward-time - 1)].です。

デフォルト設定

20 秒

コマンドモード

Global Configuration

コマンドの使用方法

本コマンドでは、ルートブリッジデバイスから設定メッセージを受信しなかったとき、デバイスがスパニングツリーの再構成を試みるまでの最大エージングタイム（秒）を設定します。すべてのデバイスポート(指定されたポートを除く)は、定期的に設定メッセージを受信する必要があります。タイムアウトを検出した場合、STA 情報を最後に使用したポート(最後の設定メッセージで提供)は、接続された LAN の指定ポートになります。ルートポートの場合は、ネットワークに接続されているデバイスポートの中から新しいルートポートが選択されます。

例

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

関連コマンド

spanning-tree forward-time

spanning-tree hello-time

18.1.5 spanning-tree mode

本コマンドにより、スイッチのスパニングツリーモードを選択します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree mode {stp | rstp | mstp}

no spanning-tree mode

stp - スパニングツリープロトコルです。(IEEE 802.1D)

rstp - 高速スパニングツリープロトコルです。(IEEE 802.1w)

mstp - 複数のスパニングツリーです。(IEEE 802.1s)

デフォルト設定

rstp

コマンドモード

Global Configuration

コマンドの使用方法

◆ スパニングツリープロトコル
このオプションは、STP 強制互換モードに設定された RSTP を使用します。内部ステートマシンには RSTP を使用しますが、802.1D BPDU だけを送信します。これにより、ネットワーク全体に対して 1 つのスパニングツリーインスタンスが作成されます。ネットワーク上に複数の VLAN が実装されている場合には、特定の VLAN メンバー間のパスはネットワークループを防止するために無効になる場合があります。このため、複数の VLAN を操作する場合には、MSTP オプションを選択することを推奨します。

◆ 高速スパニングツリープロトコル
RSTP では、受信プロトコルメッセージを監視することにより、STP または RSTP のいずれかへの接続をサポートします。スイッチが送信する BPDU のプロトコルメッセージタイプを動的に調整します。:

- STP モード -ポートが 802.1D BPDU を受信し、移行遅延タイマ（migration delay timer）満了後、も 802.1D BPDU を受信した場合、スイッチは 802.1D BPDU を送信する STP モードで動作します。
- RSTP モード -ポート上で RSTP BPDU を受信した場合、あるいは RSTP で 802.1D BPDU を使用しているときに RSTP BPDU を受信し、移行遅延タイマ（migration delay timer）満了後、RSTP BPDU を受信した場合、スイッチは RSTP BPDU を送信する RSTP モードで動作します。

◆ マルチプルスパニングツリープロトコル

- マルチプルスパニングツリーでは、各スイッチがブリッジ関連の設定を合わせることにより、特定のスパニングツリーインスタンス上で動作するできるようになります。
- スパニングツリーインスタンスは、対応する VLAN インスタンス割当てを持つブリッジ上でのみ存在することができます。
- スパニングツリーモードを切り替える場合は注意してください。モードを変更すると、以前のモードのすべてのスパニングツリーインスタンスが停止し、新しいモードでシステムが再起動され、一時的にユーザトラフィックが中断されます。

例

以下の例では、高速スパニングツリーを使用するためにスイッチを設定します:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

18.1.6 spanning-tree mst configuration

本コマンドで、マルチプルスパニングツリー(MST)設定モードに変更します。

デフォルト設定

VLAN はどの MST インスタンスにもマップされていません。

MST 領域の名称にはスイッチの MAC アドレスが設定されています。

コマンドモード

Global Configuration

例

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

関連コマンド

mst vlan

mst priority

name

revision

max-hops

18.1.7 spanning-tree pathcost method

本コマンドでは、高速スパニングツリーとマルチプルスパニングツリーに使用されるパスコスト方式を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

long - 1 から 200,000,000 の 32 ビットベースの値を指定します。この方式は、IEEE 802.1w 高速スパニングツリープロトコルをベースにしています。

short - 1 から 65535 の 16 ビットベースの値を指定します。

この方式は、IEEE 802.1D スパニングツリープロトコルをベースにしています。

デフォルト設定

Long 方式

コマンドモード

Global Configuration

コマンドの使用方法

- デバイス間の最良なパスを決定するために、パスコスト方式が使用されます。したがって、より低い値は、より高速のメディアに接続されたポートに割り当てられ、より高い値は、より低速のメディアに割り当てられます。　パスコストがポートプライオリティよりも優先されることに留意してください。
- パスコスト方式は、すべてのスパニングツリーモード(STP、RSTP、および MSTP)に適用されます。具体的には、このモードは RSTP の下位互換モードでサポートされているため、long 方式を STP に適用することができます。

例

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

18.1.8 spanning-tree priority

本コマンドでは、スイッチのスパニングツリー優先度をグローバルに設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

spanning-tree priority *priority*

no spanning-tree priority

priority - ブリッジの優先度です。(範囲 - 0 から 61440、4096 ステップ単位(0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440))

デフォルト設定

32768

コマンドモード

Global Configuration

コマンドの使用方法

ブリッジ優先度は、ルートブリッジデバイス、ルートポートおよび指定ポートを選択するために使用されます。最高優先度(数値が小さい)のデバイスが STA ルートブリッジデバイスになります。ただし、すべてのデバイスの優先度が同じ場合、MAC アドレスが最も小さいデバイスがルートブリッジデバイスになります。

例

```
Console(config)#spanning-tree priority 40960
Console(config)#
```

18.1.9 spanning-tree system-bpdu-flooding

本コマンドでは、スパニングツリーがスイッチ上でグローバルに無効になっている場合、または特定のポートで無効になっている場合に、BPDU をスイッチ上の他のすべてのポートまたは同じ VLAN 内の他のポートにフラッディングさせるように設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree system-bpdu-flooding {to-all | to-vlan}

no spanning-tree system-bpdu-flooding

to-all - BPDU をスイッチ上の全ポートにフラッディングさせます。

to-vlan - 受信ポートのネイティブ VLAN 内の他のすべてのポートに BPDU をフラッディングします。

デフォルト設定

同じ VLAN 内のすべてのポートにフラッディングします。

コマンドモード

Global Configuration

コマンドの使用方法

ポート上で BPDU フラッディングが無効な場合、spanning-tree system-bpdu-flooding コマンドには効果はありません(spanning-tree port-bpdu-flooding コマンドを参照)。

例

```
Console(config)#spanning-tree system-bpdu-flooding
Console(config)#
```

18.1.10 spanning-tree transmission-limit

本コマンドでは、連続した RSTP / MSTP BPDU の最小送信間隔を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

count - 秒単位の送信間隔です。(範囲: 1 から 10)

デフォルト設定

3

コマンドモード

Global Configuration

コマンドの使用方法

本コマンドにより、BPDU の最大送信レートを制限します。

例

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

18.1.11 max-hops

本コマンドでは、マルチプルスパニングツリーの BPDU の最大ホップ数を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

max-hops *hop-number*

hop-number - マルチプルスパニングツリーの最大ホップ数です。(範囲: 1 から 40)

デフォルト設定

20

コマンドモード

MST Configuration

コマンドの使用方法

マルチプルスパニングツリーインスタンス（MSTI）領域は、STP および RSTP プロトコルにより、単一ノードとして取り扱われます。故に、MSTI 領域内に伝播される BPDU メッセージの経過時間は変更されません。　ただし、領域内の各スパニングツリーインスタンスと、これらのインスタンスを接続する内部スパニングツリー（IST）はホップカウントを使用して、BPDU を伝播するブリッジの最大数を指定するようにします。各ブリッジは、BPDU を通過する前にホップカウントを 1 減らします。　ホップカウントが 0 になると、メッセージは廃棄されます。

例

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

18.1.12 mst priority

本コマンドにより、スパニングツリーインスタンスの優先度を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

mst *instance-id* priority *priority*

no mst *instance-id* priority

instance-id - スパニングツリーのインスタンス識別子です。(範囲: 0 から 4094)

priority - スパニングツリーインスタンスの優先度です。

(範囲: 0 から 61440(4096 ステップ単位(0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440))

デフォルト設定

32768

コマンドモード

MST Configuration

コマンドの使用方法

- MST 優先度は、ルートブリッジと特定インスタンスの代替ブリッジの選択で使用されます。最優先度(数値が小さい)のデバイスが MSTI ルートブリッジデバイスになります。ただし、すべてのデバイスの優先度が同じ場合、MAC アドレスが最も小さいデバイスがルートブリッジデバイスになります。
- 優先度 0 を指定することにより、このスイッチを MSTI ルートブリッジデバイスとして動くように設定したり、または優先度 16384 を指定することで、MSTI 代替デバイスとして設定することができます。

例

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

18.1.13 mst vlan

本コマンドは、VLAN をスパニングツリーインスタンスに追加します。指定した VLAN を削除するためには、no 形式を使用します。VLAN パラメータ無しで no 形式を使用すると、すべての VLAN が削除されます。

構文

[no] mst *instance-id* vlan *vlan-range*

instance-id - スパニングツリーのインスタンス識別子です。(範囲: 0 から 4094)

vlan-range - VLAN の範囲です。(範囲: 1 から 4094)

デフォルト設定

無し

コマンドモード

MST Configuration

コマンドの使用方法

- 本コマンドを使用して、VLAN をスパニングツリーインスタンスにグループ化します。MSTP は、インスタンスごとに一意のスパニングツリーを生成します。これにより、ネットワーク全体で複数の経路が提供されるため、単一インスタンス内のブリッジノードに障害が発生した場合の大規模な中断を防ぎ、障害の発生したインスタンスに対して新しいトポロジのコンバージェンスを高速化できます。
- デフォルトでは、すべての VLAN は MST 領域内のすべてのブリッジと LAN を接続する内部スパニングツリー(MSTI 0)に割り当てられています。このスイッチは、最大 16 のインスタンスをサポートします。　ネットワークの同じ一般的な領域をカバーする VLAN をグループ化するようにしてください。ただし、同じ MSTI 領域内のすべてのブリッジを同じインスタンスセットで構成し、同じインスタンス(各ブリッジ上)を同じ VLAN セットで構成する必要があることに留意してください。また、RSTP は各 MSTI 領域を単一のノードとして取り扱い、すべての領域を共通スパニングツリーに接続します。

例

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

18.1.14 name

本コマンドでは、スイッチがある MST 領域の名称を設定します。名称をクリアするには、no 形式を使用してください。

構文

name *name*

name - マルチプルツリー領域の名称です。(範囲: 1 から 32 の英数字)

デフォルト設定

スイッチの MAC アドレス

コマンドモード

MST Configuration

コマンドの使用方法

MST 領域の名称とレビジョン番号は、一意の MST 領域を決定するために使用されます。ブリッジ(スパニングツリーで一意のインスタンスを構成する、スイッチなどのスパニングツリー対応デバイス)は、1 つの MST 領域にしか属しません。同じ領域内のすべてのブリッジは、同じ MST インスタンスで構成する必要があります。

例

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

関連コマンド

revision

18.1.15 revision

本コマンドにより、スイッチのマルチプルスパニングツリー構成のレビジョン番号を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

revision *number*

number - スパニングツリーのレビジョン番号です。(範囲: 0 から 65535)

デフォルト設定

0

コマンドモード

MST Configuration

コマンドの使用方法

MST 領域の名称とレビジョン番号は、一意の MST 領域を決定するために使用されます。ブリッジ(このスイッチなどのスパニングツリー対応デバイス)は、1 つの MST 領域にしか属しません。同じ領域内のすべてのブリッジは、同じ MST インスタンスで構成する必要があります。

例

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

関連コマンド

name

18.1.16 spanning-tree bpdu-filter

本コマンドを使用すると、エンドノードに接続されている設定済みのエッジポートで BPDU を送信しないようにできます。この機能を無効にするには、no 形式を使用してください。

構文

[no] spanning-tree bpdu-filter

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- 本コマンドは、すべての BPDU が設定済みのエッジポートで送信されるのを停止し、CPU 処理時間を節約します。本機能は、エンドステーションをスイッチに接続するだけのエッジポートと連携して動作するように設計されているため、BPDU を処理する必要はありません。ただし、別のスイッチまたはブリッジデバイスに接続されたトランキングポートを誤ってエッジポートとして設定し、このポートで BPDU フィルタリングをイネーブルにすると、スパニングツリーにループが発生する可能性があります。
- BPDU フィルタは、spanning-tree edge-port コマンドで有効または自動に設定されているインタフェース上で設定できます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-filter
Console(config-if)#
```

関連コマンド

spanning-tree edge-port

18.1.17 spanning-tree bpdu-guard

本コマンドは、BPDU を受信すると、エッジポートをシャットダウンします。　この機能を無効にするには、キーワードなしの no 形式を使用するか、デフォルト設定を復元するキーワードを使用します。

構文

spanning-tree bpdu-guard [auto-recovery [interval *interval*]]

no spanning-tree bpdu-guard [auto-recovery [interval]]

auto-recovery - 指定した間隔の後にインタフェースを自動的に再び有効にします。

interval - インタフェースを再度有効にするまで待機する時間です。(範囲: 30 から 86400 秒)

デフォルト設定

BPDU ガード: 無効

自動回復: 無効

自動回復間隔: 300 秒

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- エッジポートは、BPDU を生成しないエンドノードにのみ接続する必要があります。BPDU がエッジポートで受信された場合、これは無効なネットワーク構成を示しているか、またはスイッチがハッカーの攻撃を受けている可能性があります。
- BPDU ガードによってインタフェースがシャットダウンした後、自動回復が指定されていない場合には、インタフェースに shutdown コマンドを一旦設定してから、no shutdown コマンドを使用して、手動で復旧させてください。
- BPDU ガードは、spanning-tree edge-port コマンドで有効または自動に設定されているインタフェース上で設定できます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-guard
Console(config-if)#
```

関連コマンド

spanning-tree edge-port

spanning-tree spanning-disabled

18.1.18 spanning-tree cost

本コマンドは、指定されたインタフェースのスパニングツリーパスコストを設定します。　デフォルトの自動設定モードを復元するには、no 形式を使用してください。

構文

spanning-tree cost *cost*

no spanning-tree cost

cost - ポートのパスコストです。(範囲: 自動構成の場合は 0、短パスコスト方式の場合は 1 から 65535、長パスコスト方式の場合は 1 から 200,000,000）※

注※ spanning-tree pathcost method コマンドを使用して、パスコスト方式を設定します。

表 18-2　推奨 STA パスコスト範囲

ポートタイプ	short パスコスト (IEEE 802.1D-1998)	long パスコスト (IEEE 802.1D-2004)
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

デフォルト設定

デフォルトでは、各ポートで使用される速度とデュプレックスモードが自動的に検出され、以下に示す値

に従ってパスコストが設定されます。パスコスト「0」は、自動構成モードを示すために使用されます。short パスコスト方式が選択され、かつ IEEE802.1w 標準で推奨されるデフォルトパスコストが 65,535 を超える場合、デフォルトは 65,535 に設定されます。

表 18-3 デフォルト STA パスコスト

ポートタイプ	short パスコスト (IEEE 802.1D-1998)	long パスコスト (IEEE 802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- 本コマンドは、デバイス間の最適なパスを決定するためにスパニングツリーアルゴリズムによって使用されます。したがって、より低い値は、より高速のメディアに接続されたポートに割り当てられ、より高い値は、より低速のメディアに割り当てられます。
- パスコストはポートの優先度よりも優先されます。
- spanning-tree pathcost method コマンドが short に設定されている場合、パスコストの最大値は 65,535 です。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

18.1.19 spanning-tree edge-port

本コマンドは、インタフェースをエッジポートとして指定します。

構文

spanning-tree edge-port auto

no spanning-tree edge-port

auto - インタフェースがエッジポートであるかどうかを自動的に判断します。

デフォルト設定

auto

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- エッジポートは auto 設定のみサポートします。
- ブリッジされた LAN の終端にある LAN セグメントまたはエンドノードにインタフェースが接続されている場合、このオプションを有効にすることができます。このオプションを有効にすることで、再構成の際に、アドレステーブルを再構築するために必要となるフレームのフラッディング量を削減できます。ただし、エッジポートは、エンドノードデバイスに接続されたポートに対してのみ有効にする必要があります。
- エッジポートが auto に設定されている場合、動作状態は 802.1D-2004 に記載されているブリッジ検出ステートマシンによって自動的に決定されます。エッジポートの状態は、環境の変化に基づいて動的に変化します（BPDU の受信や、 間隔）。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port auto
Console(config-if)#
```

18.1.20 spanning-tree link-type

本コマンドは、RSTP および MSTP のリンクタイプを設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

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

no spanning-tree link-type

auto - デュプレックスモードの設定から自動的に引き出されます。

point-to-point - Point-to-point リンク

shared - 共有媒体。

デフォルト設定

auto

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- インタフェースが他の 1 つのブリッジにのみ接続できる場合は、ポイントツーポイントリンクを指定し、2 つ以上のブリッジに接続できる場合は共有リンクを指定します。
- auto が選択されている場合、スイッチはデュプレックスモードからリンクタイプを取得します。全二重インタフェースはポイントツーポイントリンクと見なされますが、半二重インタフェースは共有リンク上にあるとみなされます。
- RSTP は、2 つのブリッジ間のポイントツーポイントリンク上でのみ機能します。ポートを共有リンクとして指定すると、RSTP は禁止されます。MSTP は RSTP の拡張版なので、同じ制限が適用されま

す。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

18.1.21 spanning-tree loopback-detection

本コマンドは、ポート上のスパニングツリーループバック BPDU パケットの検出と応答を有効にします。この機能を無効にするには、no 形式を使用してください。

構文

[no] spanning-tree loopback-detection

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- スパニングツリーループバック検出が有効ではなく、ポートが自身の BPDU を受信すると、ポートは IEEE 標準 802.1W-2001 9.3.4（Note1）に従ってループバック BPDU を廃棄します。
- スイッチ上でスパニングツリーが無効になっている場合、スパニングツリーループバック検出は有効になりません。
- スパニングツリーループバックを使用する場合、spanning-tree loopback-detection release-mode コマンドでリリースモードを必ず manual に設定してください。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

18.1.22 spanning-tree loopback-detection action

本コマンドは、インタフェースをシャットダウンするループバック検出の応答を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree loopback-detection action shutdown *duration*

no spanning-tree loopback-detection action

shutdown - インタフェースをシャットダウンします。

duration - インタフェースをシャットダウンする時間です。

(範囲: 60 から 86400 秒)

デフォルト設定

シャットダウン、60 秒

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- 本コマンドでインタフェースがシャットダウンされ、spanning-tree loopback-detection release-mode コマンドでリリースモードが auto に設定されている場合、選択したインタフェースはシャットダウン間隔が経過すると自動的にシャットダウン解除となります。
- 本コマンドによってインタフェースがシャットダウンされ、リリースモードが「手動」に設定されている場合、インタフェースは spanning-tree loopback-detection release コマンドを使用して再度有効にすることができます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection action shutdown 600
Console(config-if)#
```

18.1.23 spanning-tree loopback-detection release-mode

本コマンドは、ループバック BPDU を受信したため discarding 状態にあったポートのリリースモードを設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree loopback-detection release-mode manual

no spanning-tree loopback-detection release-mode

manual - ポートは discarding 状態から手動でのみ解放することができます。

デフォルト設定

auto

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- ポートループバック検出が有効ではなく、ポートが自身の BPDU を受信すると、ポートは IEEE 標準 802.1W-2001 9.3.4（Note1）に従ってループバック BPDU を廃棄します。
- スイッチ上でスパニングツリーが無効になっている場合、ポートループバック検出は有効になりませ

ん。

◆ スパニングツリーループバックを使用する場合、spanning-tree loopback-detection release-mode コマンドでリリースモードを必ず manual(手動解除)に設定してください。手動解除モードに設定されている場合、リンクダウン/アップイベントはポートを破棄状態から解放しません。spanning-tree loopback-detection release コマンドを使用してのみ解放することができます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
Console(config-if)#
```

18.1.24 spanning-tree loopback-detection trap

本コマンドは、スパニングツリーループバック BPDU 検出の SNMP トラップ通知をイネーブルにします。デフォルトの状態に復元するには、no 形式を使用してください。

構文

[no] spanning-tree loopback-detection trap

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

18.1.25 spanning-tree mst cost

本コマンドは、MST 内の MSTI のパスコストを設定します。デフォルトの自動設定モードを復元するには、no 形式を使用してください。

構文

spanning-tree mst *instance-id* cost *cost*

no spanning-tree mst *instance-id* cost

instance-id - スパニングツリーのインスタンス識別子です。(範囲: 0 から 4094)

cost - インタフェースのパスコストです。(範囲: 自動構成の場合は 0、short パスコスト方式の場合は 1 から 65535※、long パスコストの場合は 1 から 200,000,000)

推奨されるパスコストの範囲は、「表 18-2　推奨 STA パスコスト範囲」を参照してください。

注※ spanning-tree pathcost method コマンドを使用して、パスコスト方式を設定します。

デフォルト設定

デフォルトでは、各ポートで使用される速度とデュプレックスモードが自動的に検出され、以下に示す値に従ってパスコストが設定されます。パスコスト「0」は、自動構成モードを示すために使用されます。short パスコスト方式が選択され、IEEE8021w 標準で推奨されるデフォルトパスコストが 65,535 を超える場合、デフォルトは 65,535 に設定されます。デフォルトのパスコストは、「表 18-3　デフォルト STA パスコスト」を参照してください。

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- ◆ 各スパニングツリーインスタンスは、一意の VLAN ID のセットに関連付けられています。
- ◆ 本コマンドは、複数の STA によって、デバイス間の最適なパスを判断するために使用されます。したがって、より高速なメディアに接続されたインタフェースには低い値を割り当て、遅いメディアには高い値を割り当てます。
- ◆ 自動設定モードを指定するには、no spanning-tree mst cost コマンドを使用します。
- ◆ パスコストはインタフェースの優先度よりも優先されます。

例

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

関連コマンド

spanning-tree mst port-priority

18.1.26 spanning-tree mst port-priority

本コマンドは、MST 内の MSTI 上のインタフェースプライオリティを設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree mst *instance-id* port-priority *priority*

no spanning-tree mst *instance-id* port-priority

instance-id - スパニングツリーのインスタンス識別子です。(範囲: 0 から 4094)

priority - インタフェースの優先度です。(範囲: 0 から 240、ステップは 16）

デフォルト設定

128

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- 本コマンドは、マルチプルスパニングツリーにおけるインタフェースの使用の優先順位を定義します。スイッチ上のすべてのインタフェースのパスコストが同じである場合、最高のプライオリティ（最小値）のインタフェースがスパニングツリーのアクティブリンクとして設定されます。
- 複数のインタフェースに最高の優先度が割り当てられている場合、最も小さい番号を持つインタフェースが有効になります。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

関連コマンド

spanning-tree mst cost

18.1.27 spanning-tree port-bpdu-flooding

本コマンドは、スパニングツリーがスイッチ上でグローバルに無効になっている場合、または特定のポートで無効になっている場合に、BPDU を他のポートにフラッディングします。デフォルト設定を復元するには、no 形式を使用してください。

構文

[no] spanning-tree port-bpdu-flooding

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- 有効にすると、BPDU は、スイッチ上の他のすべてのポートまたは spanning-tree system-bpdu-flooding コマンドで指定された受信ポートのネイティブ VLAN 内の他のすべてのポートにフラッディングされます。
- spanning-tree port-bpdu-flooding コマンドで、ポート上において BPDU フラッディングが無効の場合、spanning-tree system-bpdu-flooding コマンドは無効です。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-bpdu-flooding
Console(config-if)#
```

18.1.28 spanning-tree port-priority

本コマンドは、指定されたインタフェースのプライオリティを設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

spanning-tree port-priority *priority*

no spanning-tree port-priority

priority - ポートの優先順位です。(範囲: 0 から 240、ステップは 16)

デフォルト設定

128

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- 本コマンドは、STA でポートを使用するための優先順位を定義します。スイッチ上のすべてのポートのパスコストが同じ場合、最も優先度の高いポート（最小値）がスパニングツリーのアクティブリンクとして設定されます。
- 複数のポートに最高の優先度が割り当てられている場合は、最も小さい番号のポートが有効になります。
- ポートの役割を決定するために使用される基準は、ルートブリッジ ID、ルートパスコスト、指定ブリッジ、指定ポート、ポートプライオリティ、およびポート番号に基づいております。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

関連コマンド

spanning-tree cost

18.1.29 spanning-tree root-guard

本コマンドは、指定されたポートが上位 BPDU を考慮するのを防ぎ、新しい STP ルートポートを選択できるようにします。この機能を無効にするには、no 形式を使用してください。

構文

[no] spanning-tree root-guard

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- ブリッジ識別子が小さい値（または同じ識別子で小さい値の MAC アドレス）を持つブリッジは、いつでもルートブリッジとして引き継ぐことができます。
- ルートガードが有効の場合、スイッチがこのポートで上位 BPDU を受信すると、一定の回復期間の間、上位 BPDU の受信を停止するまで、Discarding 状態に設定されます。Discarding 状態では、トラフィックはポートを介して転送されません。
- ルートガードを使用して、最適な位置にルートブリッジが形成されないようにすることができます。低速ブリッジに接続されている指定ポートではルートガードを有効にする必要があります。ルートポートとして引き継ぎ、新しいスパニングツリートポロジを形成することにより、低速リンクに過負荷をかける可能性があります。ルートブリッジが許可されているネットワークの一部の周りに境界線を形成するために使用することもできます。
- スパニングツリーがスイッチまたはインタフェース上でグローバルに初期化されると、スイッチはルートガードを有効にする前にスパニングツリーが収束していることを確認するために 20 秒間待機します。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

18.1.30 spanning-tree spanning-disabled

本コマンドは、指定されたインタフェースのスパニングツリーアルゴリズムを無効にします。特定のインタフェースに対してスパニングツリーアルゴリズムを再度有効にするには、no 形式を使用してください。

構文

[no] spanning-tree spanning-disabled

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

スイッチのスパニングツリーが有効（spanning-tree コマンド）であり、かつインタフェースでスパニングツリーが有効（本コマンドを設定）とした場合、スパニングツリーのループバック検知は無効となります。

例

この例では、ポート 5 のスパニングツリーアルゴリズムを無効にします。

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

18.1.31 spanning-tree tc-prop-stop

本コマンドは、トポロジ変更通知（TCN）の伝播を停止します。TCN メッセージの伝播を許可するには、no 形式を使用してください。

構文

[no] spanning-tree tc-prop-stop

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

本コマンドがインタフェースで有効になっている場合、インタフェースから発信されるトポロジ変更情報は引き続き伝播されます。

本コマンドは、リングトポロジで意図的に設定されたインタフェースでは使用しないでください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#spanning-tree tc-prop-stop
Console(config-if)#
```

18.1.32 spanning-tree loopback-detection release

本コマンドは、ループバック検出によって Discarding 状態になったポートを手動で解放します。

構文

spanning-tree loopback-detection release *interface*

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1):

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

コマンドモード

Privileged Exec

コマンドの使用方法

spanning-tree loopback-detection release-mode コマンドでループバック検出リリースモードを手動に設定し、BPDU ループバックが発生した場合は、本コマンドを使用して Discarding 状態からインタフェースを解放します。

例

```
Console#spanning-tree loopback-detection release ethernet 1/1
Console#
```

18.1.33 spanning-tree protocol-migration

本コマンドは、選択したインタフェースで送信する適切な BPDU 形式を再チェックします。

構文

spanning-tree protocol-migration *interface*

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1):

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

コマンドモード

Privileged Exec

コマンドの使用方法

スイッチが設定またはトポロジ変更通知 BPDU を含む STP BPDU を検出すると、いつでも、選択されたインタフェースが強制 STP 互換モードに自動的に設定されます。ただし、いつでも spanning-tree protocol-migration コマンドを使用して、選択したインタフェース（RSTP または STP 互換）で送信する適切な BPDU 形式を手動で再確認することもできます。

例

```
Console#spanning-tree protocol-migration ethernet 1/5
Console#
```

18.1.34 show spanning-tree

本コマンドは、共通スパニングツリー（CST）、マルチプルスパニングツリー（MST）内のすべてのインスタンス、または MST 内の特定のインスタンスの設定を表示します。

構文

show spanning-tree [*interface* | mst *instance-id* | brief | stp-enabled-only]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1):

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

instance-id - 複数のスパニングツリーのインスタンス識別子です。

(範囲: 0 から 4094)

brief - グローバル設定とインタフェース設定の概要を表示します。

stp-enabled-only - STP が有効になっているインタフェースの設定を表示します。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

- 共通スパニングツリー（CST）のスイッチおよびツリー内のすべてのインタフェースのスパニングツリー設定を表示するには、パラメータなしで show spanning-tree コマンドを使用します。
- 共通スパニングツリー（CST）内のインタフェースのスパニングツリー設定を表示するには、show spanning-tree interface コマンドを使用します。
- show spanning-tree mst コマンドを使用して、アクティブなインタフェースのグローバル設定やインタフェース設定など、MST 内のすべてのインスタンスのスパニングツリー設定を表示します。
- show spanning-tree mst instance-id コマンドを使用して、すべてのインタフェースのグローバル設定およびインタフェース設定など、MST 内のインスタンスのスパニングツリー設定を表示します。

例

```
Console#show spanning-tree
Spanning Tree Information
```

```
------------------------------------------------------------
 Spanning Tree Mode              : MSTP
 Spanning Tree Enabled/Disabled  : Enabled
 Instance                        : 0
 VLANs Configured                : 1-4094
 Priority                        : 32768
 Bridge Hello Time (sec.)        : 2
 Bridge Max. Age (sec.)          : 20
 Bridge Forward Delay (sec.)     : 15
 Root Hello Time (sec.)          : 2
 Root Max. Age (sec.)            : 20
 Root Forward Delay (sec.)       : 15
 Max. Hops                       : 20
 Remaining Hops                  : 20
 Designated Root                 : 32768.0.0001ECF8D8C6
 Current Root Port               : 21
 Current Root Cost               : 100000
 Number of Topology Changes      : 5
 Last Topology Change Time (sec.): 11409
 Transmission Limit              : 3
 Path Cost Method                : Long
 Flooding Behavior               : To VLAN
 Cisco Prestandard               : Disabled
------------------------------------------------------------
Eth  1/ 1 Information
------------------------------------------------------------
 Admin Status                      : Enabled
 Role                              : Disabled
 State                             : Discarding
 External Admin Path Cost          : 0
 Internal Admin Path Cost          : 0
 External Oper Path Cost           : 100000
 Internal Oper Path Cost           : 100000
 Priority                          : 128
 Designated Cost                   : 100000
 Designated Port                   : 128.1
 Designated Root                   : 32768.0.0001ECF8D8C6
 Designated Bridge                 : 32768.0.123412341234
 Forward Transitions               : 4
 Admin Edge Port                   : Disabled
 Oper Edge Port                    : Disabled
 Admin Link Type                   : Auto
 Oper Link Type                    : Point-to-point
 Flooding Behavior                 : Enabled
 Spanning-Tree Status              : Enabled
 Loopback Detection Status         : Enabled
 Loopback Detection Release Mode   : Auto
 Loopback Detection Trap           : Disabled
 Loopback Detection Action         : Block
```

```
 Root Guard Status                 : Disabled
 BPDU Guard Status                 : Disabled
 BPDU Guard Auto Recovery          : Disabled
 BPDU Guard Auto Recovery Interval : 300
 BPDU Filter Status                : Disabled
 TC Propagate Stop                 : Disabled
```

.
.
.

この例は、スパニングツリーのグローバル設定とインタフェース設定の概要を示しています。

```
Console#show spanning-tree brief
Spanning Tree Mode             : RSTP
Spanning Tree Enabled/Disabled : Enabled
Designated Root                : 32768.0000E8944000
Current Root Port (Eth)        : 1/24
Current Root Cost              : 10000

Interface Pri Designated           Designated Oper     STP    Role State Oper
              Bridge ID            Port ID    Cost     Status            Edge
--------- --- -------------------- ---------- -------- ------ ---- ----- ---
Eth 1/ 1  128 32768.0000E89382A0   128.1        100000 EN     DESG FWD   No
Eth 1/ 2  128 32768.0000E89382A0   128.2         10000 EN     DISB BLK   No
Eth 1/ 3  128 32768.0000E89382A0   128.3         10000 EN     DISB BLK   No
Eth 1/ 4  128 32768.0000E89382A0   128.4         10000 EN     DISB BLK   No
Eth 1/ 5  128 32768.0000E89382A0   128.5         10000 EN     DISB BLK   No
.
.
.
```

18.1.35 show spanning-tree mst configuration

本コマンドは、マルチプルスパニングツリーの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-------------------------------------------------------------
 Configuration Name : R&D
```

```
 Revision Level     :0

 Instance VLANs
------------------------------------------------------------
     0    1-4094
Console#
```

19 VLAN コマンド

VLAN は、ネットワーク内のどこにでも配置できるポートのグループですが、同じ物理セグメントに属しているかのように通信します。本章では、VLAN グループの作成、ポートメンバーの追加、VLAN タギングの使用方法の指定、および選択したインタフェースの自動 VLAN 登録を有効にするコマンドについて説明します

表 19-1 VLAN コマンド

コマンドグループ	機能
VLAN グループの設定	名称、VID および状態を含む、VLAN グループをセットアップします。
VLAN インタフェースの設定	入力および出力のタグ付けモード、入力フィルタリング、および PVID を含む VLAN インタフェースパラメータを設定します。
VLAN 情報の表示	VLAN グループ、ステータス、ポートメンバー、および MAC アドレスを表示します。
IEEE 802.1Q トンネリングの設定	802.1Q トンネリング（QinQ トンネリング）を設定します
プロトコルベースの VLAN の設定※	フレームタイプとプロトコルに基づいてプロトコルベースの VLAN を設定します。
MAC ベースの VLAN の設定※	MAC ベースの VLAN を設定します。

注※ パケットがこれらの機能の複数で定義されたルールと一致する場合には、そのうちの 1 つだけが適用され優先順位は MAC ベース、プロトコルベース、ネイティブポートベースとなります(switchport priority default コマンドを参照)。

19.1 VLAN グループの設定

表 19-2　VLAN グループ編集コマンド

コマンド	機能	モード
vlan database	VLAN データベースモードを開始し、VLAN を追加、変更、および削除します。	GC
vlan	VID、名称および状態を含む、VLAN を設定します。	VC

19.1.1 vlan database

本コマンドにより、VLAN データベースモードを開始します。本コマンドのすべてのモードは直ちに実施されます。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- VLAN を追加、変更、および削除するために VLAN database コマンドを使用します。設定変更完了後、show vlan コマンドを入力することにより VLAN 設定を表示することができます。
- interface vlan コマンドを使って、ポートメンバーシップモードの定義と VLAN からポートを追加および削除します。これらのコマンド結果はランニングコンフィグレーションファイルに書き込まれ、show running-config コマンドを入力してこのファイルを表示することができます。

例

```
Console(config)#vlan database
Console(config-vlan)#
```

関連コマンド

show vlan

19.1.2 vlan

本コマンドにより、VLAN を設定します。デフォルト設定を復元や VLAN を削除するには、no 形式を使用してください。VLAN 状態の変更はサポートしてません。

構文

vlan *vlan-id* [name *vlan-name*] [media ethernet [state {active | suspend}] | [rspan]]

no vlan *vlan-id* [name | state]

vlan-id - 単一の番号として指定された VLAN ID、ハイフンで区切られた連続した番号の範囲、またはコンマで区切られた複数の番号です。(範囲: 1 から 4094)

name - VLAN 名の後に続くキーワードです。

vlan-name - 1 から 32 文字の ASCII 文字列です。

media ethernet - イーサネットメディアタイプです。

state - VLAN 状態の後に続くキーワードです。 ※将来サポート予定

active - VLAN の状態を enable にし，全フレームの送受信を開始します。

suspend - VLAN の状態を disable にし，全フレームの送受信を停止します。

rspan - リモートスイッチからのトラフィックをミラーリングするために使用する VLAN を作成するキーワードです。RSPAN に使用される VLAN には、VLAN 1(スイッチのデフォルト VLAN)は含まれません。他の目的で VLAN 4093 を設定すると、クラスタリング操作(未サポート)で問題が発生する可能性があります。CLI を使用して RSPAN を設定する方法の詳細については、「14.2　RSPAN ミラーリングコマンド」を参照してください。 RSPAN VLAN は VLAN リストの対象外となります。

デフォルト設定

デフォルトでは VLAN1 のみが存在し、アクティブな状態になっています。

コマンドモード

VLAN Database Configuration

コマンドの使用方法

- no vlan *vlan-id* VLAN を削除します。
- no vlan *vlan-id* name VLAN 名を削除します。
- no vlan *vlan-id* state VLAN をデフォルト状態に戻します(例；アクティブ)
- スイッチでは、最大 4094VLAN を設定することができます。

例

以下の例では、VLAN ID 105 と名称 RDS を使って VLAN を追加します。デフォルトでは VLAN をアクティベートしています。

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

関連コマンド

show vlan

19.2 VLAN インタフェースの設定

表 19-3 VLAN インタフェース設定のコマンド

コマンド	機能	モード
interface vlan	特定 VLAN のインタフェース設定モードを開始します。	GC
switchport acceptable-frame-types	インタフェースに受け入れられるための、フレームタイプを設定します。	IC
switchport allowed vlan	インタフェースに関連した VLAN を設定します。	IC
switchport forbidden vlan	インターフェイスの禁止リストに VLAN を追加します。	IC
switchport mode	インタフェースの VLAN メンバーシップモードを設定します。	IC
switchport native vlan	インタフェースの PVID(ネイティブ VLAN)を設定します。	IC
switchport priority default	受信タグ無しフレームのポート優先度を設定します。	IC

19.2.1 interface vlan

本コマンドでは、物理インタフェースの VLAN パラメータを設定するために使用される、インタフェース設定コマンドを入力します。レイヤ 3 インタフェースをレイヤ 2 インタフェースに戻すには、no 形式を使用してください。

構文

[no] interface vlan *vlan-id*

vlan-id - 設定済み VLAN の ID です。(範囲: 1 から 4094)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- vlan コマンドで VLAN を作成することにより、レイヤ 2 インタフェースを初期化します。レイヤ 3 インタフェースに変更するには、interface コマンドを使って必要な VLAN のインタフェース設定を入力し、レイヤ 3 設定コマンドを入力後、コンフィグレーションを保存します。
- レイヤ 3 インタフェースをレイヤ 2 に戻すには、no interface コマンドを使用してください。
- vlan-id に 4094 を指定した場合、VLAN4094 のインタフェースに ipv6 nd dad attempts 0 のコンフィグレーションが自動生成されることがありますが、動作や通信に影響はありません。

例

以下の例では、インタフェース設定モードを VLAN1 に設定し、IP アドレスを VLAN に割当てる方法を表示します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

関連コマンド

shutdown

interface

vlan

19.2.2 switchport acceptable-frame-types

本コマンドでは、ポートの受け入れ可能フレームタイプを設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

switchport acceptable-frame-types {all | tagged}

no switchport acceptable-frame-types

all - ポートは、タグ付きまたはタグ無しのすべてのフレームを受け入れます。

tagged - ポートはタグ付きフレームのみ受け入れます。

デフォルト設定

全フレームタイプ

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

全フレームタイプを受け入れるよう設定した際、受け入れたすべてのタグ無しフレームは、デフォルト VLAN に割当てられます。

例

以下の例では、ポート 1 で受信したトラフィックをタグ付きフレームに制限する例を示します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

関連コマンド

switchport mode

19.2.3 switchport allowed vlan

本コマンドでは、選択したインタフェースで VLAN グループを設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

switchport allowed vlan {*vlan-list* | add *vlan-list* [tagged | untagged] | remove *vlan-list*}

no switchport allowed vlan

vlan-list - add オプション無しで VLAN リストを入力した場合、インタフェースは特定 VLAN に割当てられ、以前の VLAN の中のメンバーシップは削除されます。

非連続な VLAN 識別子はカンマで区切り、スペースは使用しないでください。ハイフンを使用して ID の範囲を指定します(範囲: 1 から 4094)。

add *vlan-list* - 追加する VLAN 識別子の一覧です。add オプションを使用した際、インタフェースは特定 VLAN に割当てられ、以前の VLAN の中のメンバーシップは保持されます。

remove *vlan-list* - 削除する VLAN 識別子の一覧です。

デフォルト設定

デフォルトでは全ポートは VLAN 1 に割当てられます。

デフォルトフレームタイプはタグ付けされていません。

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- ポートまたはトランクの switchport mode が access に設定されている場合、本コマンドでは 1 つの VLAN だけを追加できます。　VLAN リストを指定すると、リストの最後の VLAN だけがインタフェースに追加されます。
- ポートまたはトランクの switchport mode が hybrid に設定されている場合、最低 1 つの VLAN はタグ無しで割当てられる必要があります。
- トランクの switchport mode が trunk に設定されている場合(例； 1Q トランク)、インタフェースを VLAN グループにタグ付きメンバーとしてのみ、割当てることができます。
- スイッチでは、フレームは常にタグ付きとなります。VLAN をインタフェースに追加する際に使用されるタグ付き/タグ無しパラメータは、スイッチに出口でタグを保持するか維持するかについて通知します。
- 接続の相手側の中間ネットワークデバイスもホストも VLAN をサポートしていない場合は、これらの VLAN にタグ無しメンバーとしてインタフェースを追加する必要があります。それ以外の場合は、最大で 1 つの VLAN をタグ無しとして追加するだけで済みます。これはインタフェースのネイティブ VLAN に対応する必要があります。
- インタフェースの禁止リストに設定された VLAN を switchport allowed vlan コマンドでインタフェースに追加した場合、VLANはインタフェースの禁止リストから自動的に削除されます。

例

以下の例では、VLAN 1、 2、 5 および 6 をポート 1 のタグ付き VLAN として、許可されたリストへ追加する方法を示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

19.2.4 switchport forbidden vlan

動的に VLAN に参加するポートを防ぐために、このコマンドを使用します。 すべての制限を無効にするには、このコマンドの no 形式を使用します。

構文

switchport forbidden vlan {vlan-list | add vlan-list | remove vlan-list}

no switchport forbidden vlan

vlan-list - 禁止リストに追加する VLAN 識別子のリストです。非連続な VLAN 識別子はカンマで区切り、スペースは使用しないでください。ハイフンを使用して ID の範囲を指定します(範囲: 1 から 4094)。

add *vlan-list* - 禁止リストに追加する VLAN 識別子のリストです。add オプションを使用すると、指定された VLAN にインターフェイスが動的に追加されなくなります。

remove *vlan-list* - 禁止リストから削除する VLAN 識別子のリストです。

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

インターフェイスの許可リストにある VLAN をインターフェイスの禁止リストに手動で追加すると、そのインターフェイスの許可リストから VLAN が自動的に削除されます。

例

以下の例では、インタフェースのポート 2 の禁止リストに VLAN 300 および 600 を追加する例を示します。

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport forbidden vlan add 300,600
Console(config-if)#
```

19.2.5 switchport mode

本コマンドでは、ポートの VLAN メンバーシップを設定します。デフォルトの状態に復元するには、no 形式を使用します。

構文

switchport mode {access | hybrid | trunk}

no switchport mode

access - アクセス VLAN インタフェースを指定します。ポートはタグ無しフレームを単一 VLAN でのみ送受信します。

hybrid - ハイブリッド VLAN インタフェースを指定します。ポートはタグ付きまたはタグ無しフレームを送信します。

trunk - ポートを VLAN トランクのエンドポイントとして指定します。トランクは 2 つのスイッチ間の直接リンクなので、ポートは送信元 VLAN を識別するタグ付きフレームを送信します。ポートのデフォルト VLAN に属する(例; PVID に関連付けられた)フレームも、タグ付きフレームとして送信されることに留意してください。

デフォルト設定

PVID が VLAN 1 に設定されたハイブリッドモード。

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

例

以下の例では、設定モードをポート 1 に設定する方法と、その際に switchport mode をハイブリッドに設定する方法を示します。:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

関連コマンド

switchport acceptable-frame-types

19.2.6 switchport native vlan

本コマンドでは、ポートの PVID を設定します(例; デフォルト VLAN ID)。デフォルトの状態に復元するには、no 形式を使用してください。

構文

switchport native vlan *vlan-id*

no switchport native vlan

vlan-id - ポートのデフォルト VLAN ID です。(範囲: 1 から 4094)

デフォルト設定

VLAN 1

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- アクセスモードを使用してインタフェースが新しい VLAN に割当てられると、その VLAN の PVID が自動的にその VLAN の識別子に設定されます。ハイブリッドモードを使用する場合、インタフェースの PVID はタグ無しメンバーである任意の VLAN に設定できます。
- 受け入れ可能なフレーム対応が all に設定、または switchport mode が hybrid に設定されると、PVID は入力ポートに入るすべてのタグ無しフレームに挿入されます。

例

以下の例では、ポート 1 の PVOD の VLAN3 への設定方法について示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

19.3 VLAN 情報の表示

本章では、VLAN 情報を表示するために使用するコマンドについて説明します。

表 19-4 VLAN 情報表示のコマンド

コマンド	機能	モード
show interfaces status vlan	特定 VLAN インタフェースの状態を表示します。	NE, PE
show interfaces switchport	インタフェースの管理ステータスと動作ステータスを表示します。	NE, PE
show vlan	VLAN 情報を表示します。	NE, PE

19.3.1 show vlan

本コマンドでは、VLAN 情報を表示します。

構文

show vlan [id *vlan-id* | name *vlan-name*]

id - VLAN ID の後に続くキーワードです。

vlan-id - 設定済み VLAN の ID です。(範囲: 1 から 4094)

name - VLAN 名の後に続くキーワードです。

vlan-name - 1 から 32 文字の ASCII 文字列です。

デフォルト設定

全 VLAN を表示します。

コマンドモード

Normal Exec, Privileged Exec

例

以下の例では、VLAN 1 情報の表示方法について示します。

```
Console#show vlan id 1

VLAN ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channels : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                      Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
Console#
```

19.4 IEEE 802.1Q トンネリングの設定

IEEE 802.1Q トンネリング(QinQ トンネリング)では、複数の VLAN を持つ顧客に対して単一の SPVLAN(Service Provider VLAN)を使用します。同じ顧客固有の VLAN ID を使用している場合でも、カスタマーVLAN ID は保持され、異なる顧客からのトラフィックはサービスプロバイダのネットワーク内で分離されます。QinQ トンネリングは、VLAN-in-VLAN 階層を使用し、顧客の元のタグ付きパケットを保存し、各フレームに SPVLAN タグを追加することによって VLAN スペースを拡張します(ダブルタギングとも呼ばれます)。

本章では、QinQ トンネリングの設定に使用されるコマンドについて説明します。

表 19-5 802.1Q トンネリングコマンド

コマンド	機能	モード
dot1q-tunnel system-tunnel-control	通常モードまたは QinQ モードで動作するスイッチを設定します。	GC
dot1q-tunnel tpid	トンネルポートのタグプロトコル識別子（TPID）値を設定します。	GC
switchport dot1q-tunnel mode	QinQ トンネルポートとしてインタフェースを設定します。	IC
show dot1q-tunnel	QinQ トンネルポートの設定を表示します。	PE
show interfaces switchport	ポート QinQ 動作状態を表示します。	PE

QinQ の一般設定ガイドライン

1. スイッチを QinQ モードに設定します(dot1q-tunnel system-tunnel-control)。
2. SPVLAN（vlan）を作成します。
3. QinQ トンネルアクセスポートを dot1Q トンネルアクセスモード（switchport dot1q-tunnel mode）に設定します。
4. トンネルアクセスポートの TPID（Tag Protocol Identifier）値を設定します。この手順は、接続されたクライアントが 802.1Q タグ付きフレームを識別するために非標準の 2 バイトの ethertype を使用している場合に必要です。標準の ethertype 値は 0x8100 です。（dot1q-tunnel tpid を参照してください。）
5. タグ無しメンバーとして SPVLAN に参加するように QinQ トンネルアクセスポートを設定します(switchport allowed vlan)。
6. SPVLAN ID を QinQ トンネルアクセスポートのネイティブ VID として設定します(switchport native vlan)。
7. QinQ トンネルアップリンクポートを dot1Q トンネルアップリンクモードに設定します(switchport dot1q-tunnel mode)。
8. QinQ トンネルアップリンクポートを設定して、SPVLAN をタグ付きメンバーとして参加させます(switchport allowed vlan)。

QinQ の制限

- トンネルアップリンクポートとトンネルアクセスポートのネイティブ VLAN は同じにすることはできません。ただし、両方のトンネルポートタイプで同じサービス VLAN を設定することができます。
- トンネルアクセスポートで IGMP スヌーピングを有効にするべきではありません。
- スパニングツリープロトコルが有効の場合、スパニングツリー構造が自動的に再構成されて通信が復旧すると、トンネルアクセスまたはトンネルアップリンクポートがディセーブルになる可能性があることに注意してください。したがって、これらのポートでスパニングツリーを無効にすることをお勧めします。

19.4.1 dot1q-tunnel system-tunnel-control

本コマンドは、QinQ モードで動作するようにスイッチを設定します。QinQ の動作モードを無効にするには、no 形式を使用します。

構文

[no] dot1q-tunnel system-tunnel-control

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

スイッチで QinQ トンネルモードを有効にして、QinQ インタフェース設定を機能させる必要があります。

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

関連コマンド

show dot1q-tunnel

show interfaces switchport

19.4.2 dot1q-tunnel tpid

本コマンドは、トンネルポートの TPID（Tag Protocol Identifier）値をグローバルに設定します。デフォルトの TPID 値に戻すには、no 形式を使用してください。

構文

[no] dot1q-tunnel tpid *ethertype*

ethertype - 802.1Q カプセル化の ethertype 値を設定します。この識別子は、802.1Q タグ付きフレームを識別するために非標準の 2 バイトの ethertype を選択するために使用されます。標準の ethertype 値は 0x8100 です。(範囲: 0800 から FFFF 16 進)

デフォルト設定

0x8100

コマンドモード

Global Configuration

コマンドの使用方法

- dot1q-tunnel tpid コマンドを使用して、カスタム 802.1Q イーサタイプのグローバル設定を行います。この機能により、スイッチは 802.1Q タグ付きフレームを識別するために標準の 0x8100 イーサネットタイプを使用しないサードパーティのスイッチと相互運用できます。 たとえば、0x1234 がグローバル 802.1Q イーサタイプとして設定されている場合、その ethertype を含むトランクポート上の受信フレームは、ethertype フィールドに続くタグに含まれる VLAN に割り当てられます。 他の ethertype を含むトランクポートに到着したフレームは、タグなしフレームとみなされ、ポートのネイティブ VLAN に割り当てられます。
- 指定された ethertype は、switchport dot1q-tunnel mode コマンドを使用してアップリンクモードで設定されたポートにのみ適用されます。 ポートが通常モード（すなわち、指定されていない）である場合、TPID は常に 0x8100 である。 ポートがアクセスモードの場合、受信パケットはタグなしパケットとして処理されます。

例

```
Console(config)#dot1q-tunnel tpid 0x88A8
Console(config)#
```

関連コマンド

show interfaces switchport

19.4.3 switchport dot1q-tunnel mode

本コマンドは、インタフェースを QinQ トンネルポートとして設定します。インタフェース上で QinQ を無効にするには、no 形式を使用します。

構文

switchport dot1q-tunnel mode {access | uplink}

no switchport dot1q-tunnel mode

access - ポートを 802.1Q トンネルアクセスポートとして設定します。

uplink - ポートを 802.1Q トンネルアップリンクポートとして設定します。

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- switchport dot1q-tunnel mode interface コマンドを有効にするには、dot1q-tunnel system-tunnel-control コマンドを使用してスイッチ上で QinQ トンネリングを有効にする必要があります。
- トンネルアクセスポートがカスタマーからパケットを受信すると、カスタマータグ（1 つ以上のタグレイヤーがあるかどうかに関係なく）が内部タグに保持され、サービスプロバイダのタグが外部タグ

に追加されます。

◆ トンネルアップリンクポートがサービスプロバイダからパケットを受信すると、外部サービスプロバイダのタグは取り除かれ、パケットは内部タグが示す VLAN に渡されます。内部タグが見つからない場合、パケットはアップリンクポート用に定義されたネイティブ VLAN に渡されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

関連コマンド

show dot1q-tunnel

show interfaces switchport

19.4.4 show dot1q-tunnel

本コマンドは、QinQ トンネルポートに関する情報を表示します。

構文

show dot1q-tunnel

コマンドモード

Privileged Exec

例

```
Console#show dot1q-tunnel
802.1Q Tunnel Status : Enabled
802.1Q Tunnel TPID : FFFF (Hex)

Port     Mode   Priority Mapping
-------- ------ ----------------
Eth 1/ 1 Normal Disabled
Eth 1/ 2 Uplink Enabled
Eth 1/ 3 Normal Disabled
Eth 1/ 4 Normal Disabled
Eth 1/ 5 Normal Disabled
Eth 1/ 6 Normal Disabled
Eth 1/ 7 Normal Disabled
Eth 1/ 8 Normal Disabled
Eth 1/ 9 Normal Disabled
Eth 1/10 Normal Disabled
Console#
```

19.5 プロトコルベースの VLAN の設定

複数のプロトコルをサポートするために必要なネットワークデバイスは、共通の VLAN に簡単にグループ化することはできません。これは、特定のプロトコルに参加するすべてのデバイスを包含するために、非標準デバイスが異なる VLAN 間でトラフィックを通過することを必要とする場合があります。この種の設定では、セキュリティと簡単なアクセシビリティを含め、VLAN の基本的な利点がユーザに奪われます。

これらの問題を回避するには、物理ネットワークを必要なプロトコルごとに論理 VLAN グループに分割するプロトコルベースの VLAN でこのスイッチを構成します。フレームがポートで受信されると、その VLAN メンバーシップは、受信パケットによって使用されているプロトコルタイプにもとづいて決定されます。

表 19-6 プロトコルベース VLAN コマンド

コマンド	機能	モード
protocol-vlan protocol-group	サポートされているプロトコルを指定してプロトコルグループを作成します	GC
protocol-vlan protocol-group	プロトコルグループを VLAN にマッピングします。	IC
show protocol-vlan protocol-group	プロトコルグループの構成を表示します。	PE
show interfaces protocol-vlan protocol-group	プロトコルグループと対応する VLAN にマップされたインタフェースを表示します。	PE

プロトコルベースの VLAN を設定する手順は、以下のとおりです。:

1. 最初に、使用するプロトコルの VLAN グループを設定します。必須ではありませんが、ネットワーク上で動作する主要なプロトコルごとに別々の VLAN を設定することを推奨します。この段階でポートメンバーを追加しないでください。
2. protocol-vlan protocol-group コマンド（グローバルコンフィグレーションモード）を使用して、VLAN に割当てる各プロトコルのプロトコルグループを作成します。
3. 次に、protocol-vlan protocol-group コマンド（インタフェースコンフィグレーションモード）を使用して、各インタフェースのプロトコルを適切な VLAN にマッピングします。

19.5.1 protocol-vlan protocol-group (Configuring Groups)

本コマンドは、プロトコルグループを作成したり、特定のプロトコルをグループに追加したりします。プロトコルグループを削除するには、no 形式を使用してください。

構文

protocol-vlan protocol-group *group-id* [{add | remove} frame-type *frame* protocol-type *protocol*]

no protocol-vlan protocol-group *group-id*

group-id - このプロトコルグループのグループ識別子です。(範囲: 1 から 2147483647)

frame※ - このプロトコルで使用されるフレームタイプです。（オプション：ethernet、rfc_1042、llc_other）

protocol - プロトコルタイプです。llc_other フレームタイプの唯一のオプションは ipx_raw です。他のすべてのフレームタイプのオプションには、arp、ip、ipv6、rarp、pppoe-dis、pppoe-ses があります。

注※ SNAP フレームタイプは、ハードウェアの制限によりこのスイッチではサポートされていません。

デフォルト設定

プロトコルグループは構成されていません。

コマンドモード

Global Configuration

例

以下は、プロトコルグループ 1 を作成し、IP および ARP プロトコルタイプのイーサネットフレームを指定します。

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet protocol-type arp
Console(config)#
```

19.5.2 protocol-vlan protocol-group (Configuring Interfaces)

本コマンドは、プロトコルグループを現在のインタフェースの VLAN にマッピングします。このインタフェースのプロトコルマッピングを削除するには、no 形式を使用してください。

構文

protocol-vlan protocol-group *group-id* vlan *vlan-id* priority *priority*

no protocol-vlan protocol-group *group-id* vlan

group-id - このプロトコルグループのグループ識別子です。。(範囲: 1 から 2147483647):

vlan-id - 一致するプロトコルトラフィックが転送される VLAN です。(範囲: 1 から 4094)

priority - タグ無し入力トラフィックに割当てられた優先順位です。

(範囲: 0 から 7、7 が最も高い優先順位です)

デフォルト設定

どのインタフェースにもマッピングされているプロトコルグループはありません。

Priority: 0

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- プロトコルベースの VLAN を作成する場合は、本コマンドでインタフェースを割当てるだけです。他の VLAN コマンド（vlan コマンドなど）を使用してインタフェースを割当てる場合、これらのインタフェースは、関連する VLAN に任意のプロトコルタイプのトラフィックを許可します。
- MAC ベース VLAN、およびプロトコルベース VLAN が同時にサポートされている場合、このシーケンスで優先順位が適用され、ポートベースの VLAN が最後に適用されます。
- フレームがプロトコル VLAN に割当てられたポートに入ると、次のように処理されます。
  - フレームにタグが付いている場合は、タグ付きフレームに適用されている標準規則に従って処理

されます。

- フレームがタグなしでプロトコルタイプが一致する場合、フレームは適切な VLAN に転送されます。
- フレームがタグなしでプロトコルタイプが一致しない場合、フレームはこのインタフェースのデフォルト VLAN に転送されます。

例

次の例では、プロトコル 1 で指定されたプロトコルタイプと一致するポート 1 に入力されるトラフィックを VLAN 2 にマッピングします。

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2 priority 0
Console(config-if)#
```

19.5.3 show protocol-vlan protocol-group

本コマンドは、プロトコルグループに関連付けられたフレームとプロトコルタイプを表示します。

構文

show protocol-vlan protocol-group [*group-id*]

group-id - プロトコルグループのグループ識別子です。 (範囲: 1 から 2147483647):

デフォルト設定

すべてのプロトコルグループが表示されます。

コマンドモード

Privileged Exec

例

これは、IP over Ethernet で設定されたプロトコルグループ 1 を示しています。

```
Console#show protocol-vlan protocol-group

 Protocol Group ID   Frame Type    Protocol Type
------------------ ------------- ---------------
                1      ethernet     08 00
Console#
```

19.5.4 show interfaces protocol-vlan protocol-group

本コマンドは、選択したインタフェースのプロトコルグループから VLAN へのマッピングを表示します。

構文

show interfaces protocol-vlan protocol-group [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

すべてのインタフェースのマッピングが表示されます。

コマンドモード

Privileged Exec

例

これは、プロトコル 1 の仕様と一致するポート 1 に入るトラフィックが VLAN 2 にマッピングされることを示しています。

```
Console#show interfaces protocol-vlan protocol-group
Port     Protocol Group ID VLAN ID Priority
-------- ----------------- ------- --------
 Eth 1/1                 1   vlan2        0
Console#
```

19.6 MAC ベースの VLAN の設定

IEEE 802.1Q ポートベースの VLAN 設定を使用する場合、ポートによって受信されたすべてのタグなしフレームは、VID（PVID）がそのポートに関連付けられている VLAN に属するものとして分類されます。

MAC ベースの VLAN 設定が有効の場合、タグなしの入力フレームの送信元アドレスが MAC アドレスと VLAN のマッピングテーブルと照合されます。そのアドレスのエントリが見つかった場合、これらのフレームはエントリに示されている VLAN に割当てられます。MAC アドレスが一致しない場合、タグなしフレームは受信ポートの VLAN ID（PVID）に属するものとして分類されます。

表 19-7 MAC ベース VLAN コマンド

コマンド	機能	モード
mac-vlan	MAC ベース VLAN を定義します。	GC
show mac-vlan	MAC ベース VLAN 設定を表示します。	PE

19.6.1 mac-vlan

このコマンドは、MAC アドレスと VLAN のマッピングを設定します。割当てを削除するには、no 形式を使用してください。

構文

mac-vlan mac-address *mac-address* [mask *mask-address*] vlan *vlan-id* [priority *priority*]

no mac-vlan mac-address {*mac-address* [mask *mask-address*] | all}

mac-address - 一致させる送信元 MAC アドレスです。設定された MAC アドレスは、ユニキャストアドレスのみにすることができます。MAC アドレスは、xx-xx-xx-xx-xx-xx または xxxxxxxxxxxx の形式で指定する必要があります。

mask-address - MAC アドレスの範囲を指定します。マスクは、xx-xx-xx-xx-xx-xx または xxxxxxxxxxxx の形式で指定できます。ここで、同等のバイナリ値 "1"は関連性があり、 "0"は無視されます。

vlan-id -一致する送信元 MAC アドレストラフィックが転送される VLAN です。(範囲: 1 から 4094)

priority - タグなし入力トラフィックに割当てられた優先順位です。(範囲: 0 から 7、7 が最も高い優先順位です)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- MAC から VLAN へのマッピングは、スイッチ上のすべてのポートに適用されます。
- 送信元 MAC アドレスは、1 つの VLAN ID にのみマッピングできます。
- 設定された MAC アドレスはブロードキャストまたはマルチキャストアドレスにすることはできません。
- MAC ベース VLAN、およびプロトコルベース VLAN が同時にサポートされている場合、このシーケンスで優先順位が適用され、ポートベースの VLAN が最後に適用されます。

◆ 最初の非ゼロ文字の前にある文字と一致するバイナリ相当マスクは、すべて 1 でなければなりません（たとえば、111、つまり 101 または 001 にすることはできません）。MAC アドレスのマスク：00-12-E2-8F-2C-A7 バイナリに変換：
MAC: 00000000-00010010-11100010-10001111-00101100-10100111
になり得る：11111111-1111xxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx
したがって、この例の 16 進数のマスクは次のようになります。
ff-f0-00-00-00-00

例

以下の例では、送信元 MAC アドレス 00-12-E2-8F-2C-A7 から VLAN 10 にトラフィックを割当てます。

```
Console(config)#mac-vlan mac-address 00-12-E2-8F-2C-A7 mask FF-F0-00-00-00-00  vlan 10
Console(config)#
```

19.6.2 show mac-vlan

本コマンドは、MAC アドレスと VLAN の割当てを表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドは MAC アドレスと VLAN の割当を表示します。

例

次の例では、設定されたすべての MAC アドレスベース VLAN を表示します。

```
Console#show mac-vlan
MAC Address        Mask               VLAN ID  Priority
-----------------  -----------------  -------  --------
00-12-E2-8F-2C-A7  FF-FF-FF-FF-FF-FF        10         0
Console#
```

20 CoS コマンド

本章で説明するコマンドを使用すると、トラフィックが輻輳によるスイッチでバッファリングされたときに、データパケットの優先度を指定することができます。このスイッチは、ポートごとに 8 つのプライオリティキューを持つ CoS をサポートしています。ポートの高優先度キューのデータパケットは、低優先度キューのデータパケットの前に送信されます。デフォルトのプライオリティは各インタフェースに設定できます。また、キューサービスモードおよびフレーム優先度タグのスイッチのプライオリティキューへのマッピングも設定できます

表 20-1 優先制御コマンド

コマンドグループ	機能
優先制御コマンド(レイヤ 2)	キューモード、キューの重み付け、タグ無しフレームのデフォルト優先度を設定します。
優先制御コマンド(レイヤ 3 および 4)	デフォルトの優先処理方式（CoS または DSCP）を設定します。内部処理の優先度タグをマッピングし、内部プライオリティテーブルの値をレイヤ 2 インタフェースのタグ付き出力パケットで使用される CoS 値にマッピングし、ホップごとの動作をハードウェアキューにマッピングします

20.1 優先制御コマンド（レイヤ 2）

本章では、スイッチ上でレイヤ 2 トラフィックプライオリティを設定するために使用されるコマンドについて説明します。

表 20-2 優先制御コマンド（レイヤ 2）

コマンド	機能	モード
queue mode	キューモードを Weighted Round-Robin（WRR;重み付けラウンドロビン）、完全優先、または完全優先キューイングと重み付けキューイングの組み合わせに設定します。	IC
queue weight	優先制御キューにラウンドロビン重み付けをします。	IC
switchport priority default	受信タグ無しフレームのポート優先度を設定します。	IC
show queue mode	現在のキューモードを表示します。	PE
show queue weight	重み付きキューに割当てられた重みを表示します。	PE

20.1.1 queue mode

本コマンドは、各サービスクラス（CoS）プライオリティキューの処理に使用されるスケジューリングモードを設定します。オプションには、完全優先、WRR（Weighted Round Robin）、または完全優先キューイングと重み付けキューイングの組み合わせが含まれます。デフォルト値を復元するには、no 形式を使用してください。

構文

queue mode {strict | wrr | strict-wrr [*queue-type-list*]}

no queue mode

strict - 順番に送信キューを処理し、優先度の低いキューを処理する前に、より高い優先度のキューのすべてのトラフィックを送信します。これにより、最も優先順位の高いパケットが、他のすべてのトラフィックよりも常に先にサービスされます。

wrr - Weighted Round-Robin は、スケジューリングの重み（queue weight コマンドに基づく）を使用し、各キューをラウンドロビン方式で処理することにより、送信ポートでの帯域幅を共有します。

strict-wrr - 各キューに指定された完全優先サービスまたは重み付けされたサービスを使用します。

queue-type-list - キューが重み付けタイプか完全優先タイプかを示します。キュー番号 0～7 の順番でキュータイプを指定します。(オプション: 0 は重み付けキューを示し、1 は完全優先キューを示します)

デフォルト設定

WRR

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

◆ スイッチは、完全優先、WRR、または完全優先キューイングと重み付けキューイングの組み合わせに基づいてポートキューを処理するように設定できます。

- 完全優先では、優先順位の低いキューが処理される前に、優先順位の高いキューのすべてのトラフィックを処理する必要があります。
- Weighted Round-Robin（WRR）は、キューごとに事前に定義された相対的な重みを使用して、スイッチが次のキューに移動する前に各キューにサービスするサービス時間のパーセンテージを決定します。これにより、完全優先キューイングで発生する可能性のある HOL ブロッキングが防止されます。WRR キューイングの重みを 8 つのプライオリティキューに割当てるには、queue weight コマンドを使用します。
- 完全優先モードと WRR モードが選択されている場合、各キューに指定されているように、完全優先サービスと重み付けサービスの組み合わせが使用されます。　完全優先または WRR 優先順位を使用するように割当てられたキューは、queue-type-list パラメータを使用して指定する必要があります。
- 重み付け各キューに（したがって、対応するトラフィック優先度に）重みを割当てることができます。この重みは、各キューがサービスのためにポーリングされる頻度を設定し、その後、特定の優先度値が割当てられたソフトウェアアプリケーションの応答時間に影響します。
- サービス時間は、WRR のスケジューリング重み、または完全優先キューイングと重み付けキューイングの組み合わせを使用するキューイングモードを定義して、送信ポートで共有されます。　各ラウンドで処理される正確なバイト/秒数を計算することにより、各キューにサービス時間が割当てられます。
- トランクポートとなるインタフェースでは、全てのインタフェースで同じキューモードを使用してください。

例

次の例では、キューモードを完全優先サービスモードに設定しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue mode strict
Console(config-ip)#
```

関連コマンド

queue weight

show queue mode

20.1.2 queue weight

本コマンドは、重み付けキューイングを使用する場合は 8 つの CoS（Class of Service）優先キューに、または完全優先キューイングと重み付けキューイングの組み合わせを使用する場合はキューのいずれかに重みを割当てます。デフォルトの重みを復元するには、no 形式を使用してください。

構文

queue weight *weight0...weight7*

no queue weight

weight0...weight7 - キュー0 から 7 の重みの比率によって、WRR スケジューラが使用する重みが決まります。(範囲: 1 から 255)

デフォルト設定

重み 1,2,4,6,8,10,12,14 はそれぞれキュー0-7 に割当てられます。

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- 本コマンドは、Weighted Round-Robin または完全優先キューイングと重み付けキューイングの組み合わせを使用するキューイングモードのスケジューリング重みを定義することによって、送信ポートで帯域幅を共有します。
- 各ラウンドで処理される正確なバイト/秒数を計算することによって、各キューに帯域幅が割当てられます。
- トランクポートとなるインタフェースでは、全てのインタフェースで同じキューモードを使用してください。

例

次の例は、CoS プライオリティキュー0 から 7 に 1 から 8 のラウンドロビン重みを割当てる方法を示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue weight 1 2 3 4 5 6 7 8
Console(config-if)#
```

関連コマンド

queue mode

show queue weight

20.1.3 switchport priority default

本コマンドは、タグの付いていないフレームの受信に優先度を設定します。デフォルト値を復元するには、no 形式を使用してください。

構文

switchport priority default *default-priority-id*

no switchport priority default

default-priority-id - タグなし入力トラフィックの優先順位番号です。優先順位は 0 から 7 の数字です。7 が最優先です。

デフォルト設定

優先度は設定されず、インタフェースで受信されたタグなしフレームのデフォルト値はゼロです。

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- プライオリティマッピングの優先順位は、IP DSCP、次にデフォルトのスイッチポートプライオリティです。
- デフォルトの優先度は、すべてのフレームタイプを受け入れる（つまり、タグなしフレームとタグ付きフレームの両方を受信する）ポートセットで受信したタグなしフレームに適用されます。この優先順位は、IEEE 802.1Q VLAN タグ付きフレームには適用されません。受信フレームが IEEE 802.1Q VLAN タグ付きフレームである場合、IEEE 802.1p ユーザ優先度ビットが使用されます。
- スイッチは各ポートに 8 つのプライオリティキューを提供します。queue mode コマンドを使用して、完全優先キューイング、WRR（Weighted Round Robin）、または完全優先および重み付けキューイングの組み合わせを使用するように設定できます。VLAN タグを持たない受信フレームには、受信ポートのデフォルトの受信ユーザ優先度でタグ付けされ、送信ポートで適切な優先度キューに配置されます。すべての受信ポートのデフォルトの優先順位はゼロです。したがって、優先度タグを持たない受信フレームは、送信ポートのキュー2 に配置されます。(送信ポートが関連 VLAN のタグなしメンバーである場合、これらのフレームは送信前にすべての VLAN タグが削除されます。)

例

次に、ポート 3 のデフォルトプライオリティを 5 に設定する例を示します。

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
Console(config-if)#
```

関連コマンド

show interfaces switchport

20.1.4 show queue mode

本コマンドは、現在のキューモードを表示します。

構文

show queue mode [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

```
Console#show queue mode
Unit   Port   queue mode
----   ----   ---------------
   1      1   Weighted Round Robin
...
```

20.1.5 show queue weight

本コマンドは、重み付きキューに使用されている重みを表示します。

構文

show queue weight [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

```
Console#show queue weight
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
        0       1
        1       2
        2       4
        3       6
        4       8
        5      10
        6      12
        7      14
...
```

20.2 優先制御コマンド（レイヤ 3 および 4）

本章では、スイッチ上でレイヤ 3 および 4 のトラフィックプライオリティマッピングを設定するために使用されるコマンドについて説明します。

表 20-3 優先制御コマンド（レイヤ 3 および 4）

コマンド	機能	モード
qos map cos-queue	受信パケットの CoS / CFI 値をホップ単位の動作、またはこのルータホップに使用されるキューにマッピングします。	IC
qos map dscp-queue	受信パケットの DSCP 値をホップ単位の動作、またはこのルータホップに使用されるキューにマッピングします。	IC
qos map trust-mode	QoS マッピングを DSCP または CoS に設定します。	IC
show qos map cos-queue	受信 CoS から送信キューへのマッピングを表示します。	PE
show qos map dscp-queue	受信 DSCP から送信キューへのマッピングを表示します。	PE
show qos map trust-mode	QoS マッピングモードを示します。	PE

注 プライオリティ値を内部 DSCP 値にマッピングしてハードウェアキューに戻すために使用されるデフォルト設定は、大多数のネットワークアプリケーションの優先サービスを最適化するように設計されています。特定のアプリケーションでキューイングの問題が発生しない限り、デフォルト設定を変更する必要はありません。

20.2.1 qos map cos-queue

本コマンドは、受信パケットの CoS / CFI 値を優先処理のためのホップ単位の動作にマッピングします。デフォルト設定に復元するには、no 形式を使用してください。

構文

qos map cos-queue *queue* from *cos0 cfi0...cos7 cfi7*

no qos map cos-dscp *cos0 cfi0...cos7 cfi7*

queue - ホップごとの動作、またはこのルータホップに使用されるプライオリティです。

(範囲: 0 から 7)

cos - 受信パケットの CoS 値です。(範囲: 0 から 7)

cfi - 正規フォーマットインジケータです。このパラメータを "0"に設定すると、フレームで搬送される MAC アドレス情報が正規フォーマットになっていることを示します。(範囲: 0 から 1)

デフォルト設定

表 20-4 CoS/CFI 値の Queue/CFI へのデフォルトマッピング

CFI CoS	0	1
0	2	2
1	0	0
2	1	1
3	3	3
4	4	4
5	5	5

CFI CoS	0	1
6	6	6
7	7	7

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- ◆ 前の表「CoS/CFI 値の Queue/CFI へのデフォルトマッピング」は、CoS 値を送信キューにマッピングするための IEEE 802.1p の推奨設定に基づいています。
- ◆ ホップ単位の動作の後にキーワード「from」を入力し、最大 8 つの CoS / CFI ペア値をスペースで区切って入力します。
- ◆ パケットが 802.1Q ヘッダーと共に到着するが IP パケットでない場合、
処理の優先順位を生成するために CoS / CFI から Queue へのマッピングテーブルが使用されます。元のパケットの優先度タグは、本コマンドで変更されないことに注意してください。
- ◆ 設定ははすべてのインタフェースに適用されます。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#qos map cos-dscp 0 0 from 0 1
Console(config-if)#
```

20.2.2 qos map dscp-queue

本コマンドは、受信パケットの DSCP 値を優先処理のためのホップ単位の動作にマッピングします。デフォルト設定に復元するには、no 形式を使用してください。

構文

qos map dscp-queue *dscp-queue* from *dscp0 ...dscp7*

no qos map dscp-queue *dscp0 ...dscp7*

dscp-queue - ホップごとの動作、またはこのルータホップに使用されるプライオリティです。(範囲: 0 から 7)

dscp - 受信パケットの DSCP 値です。(範囲: 0 から 63)

デフォルト設定

表 20-5 Queue への DSCP/CFI l 値のデフォルトマッピング

ingress-dscp1 ingress-dscp10	0	1	2	3	4	5	6	7	8	9
0	2	2	2	2	2	2	2	2	0	0
1	0	0	0	0	0	0	1	1	1	1
2	1	1	1	1	3	3	3	3	3	3
3	3	3	4	4	4	4	4	4	4	4
4	5	5	5	5	5	5	5	5	6	6
5	6	6	6	6	6	6	7	7	7	7
6	7	7	7	7						

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- ホップ単位の動作の値を入力し、その後にキーワード "from"を入力し、最大 8 個の DSCP 値をスペースで区切って入力します。
- このマップは、QoS マッピングモードが qos map trust-mode コマンドによって「DSCP」に設定され、受信パケットタイプが IPv4 の場合にのみ使用されます。
- 2 つの QoS ドメインは異なる DSCP 定義を持つことができるため、DSCP から Queue へのマップを使用して、別のドメインの定義に一致する 1 組の DSCP 値を変更できます。このマップは、QoS 管理ドメインの境界にある受信ポートで適用する必要があります。
- 設定ははすべてのインタフェースに適用されます。

例

この例では、DSCP 値が 1 で、ホップごとの動作が 3 であるポート 1 に入るすべてのパケットのプライオリティを変更します。

```
Console(config)#interface ethernet 1/2
Console(config-if)#qos map dscp-queue 3 from 1
Console(config-if)#
```

20.2.3 qos map trust-mode

本コマンドは、QoS マッピングを DSCP または CoS に設定します。デフォルト設定に戻すには、no 形式を使用してください。

構文

qos map trust-mode {dscp | cos}

no qos map trust-mode

dscp - QoS マッピングモードを DSCP に設定します。

cos - QoS マッピングモードを CoS に設定します。

デフォルト設定

CoS

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- 本コマンドで QoS マッピングモードが DSCP に設定され、受信パケットタイプが IPv4 または IPv6 の場合、優先処理は受信パケットの DSCP 値に基づいて行われます。
- QoS マッピングモードが DSCP に設定され、非 IP パケットが受信された場合、パケットにタグが付けられている場合、パケットの CoS および CFI（Canonical Format Indicator）値が優先処理に使用されます。タグなしパケットの場合、優先処理にはデフォルトのポート優先度が使用されます。
- 本コマンドで QoS マッピングモードが CoS に設定され、受信パケットタイプが IPv4 の場合、優先処理は受信パケットの CoS 値と CFI 値に基づいて行われます。
  タグなしパケットの場合、優先処理にはデフォルトのポート優先度が使用されます。

例

この例では、コマンドの使用方法のセクションで説明した条件に基づいて、DSCP を使用するように QoS プライオリティマッピングモードを設定します。

```
Console(config)#interface 1/1
Console(config-if)#qos map trust-mode cos
Console(config-if)#
```

20.2.4 show qos map cos-queue

本コマンドは、受信 CoS から送信キューへのマップを表示します。

構文

show qos map cos-queue interface *interface*

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

```
Console#show qos map cos-queue interface ethernet 1/1
CoS Information of Eth 1/1
 CoS-Queue map.
 CoS  : CFI  0          1
---------------------------------
 0           2          2
 1           0          0
 2           1          1
 3           3          3
 4           4          4
 5           5          5
 6           6          6
 7           7          7

Console#
```

20.2.5 show qos map dscp-queue

本コマンドは、受信 DSCP から送信キューへのマップを表示します。

構文

show qos map dscp-queue interface *interface*

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

入力 DSCP は、ingress-dscp10（左桁の最上位桁）と ingress-dscp1（最下桁の最上位桁（つまり、ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1）で構成されます。対応する dscp が表の交差セルに表示されます。

```
Console#show qos map dscp-queue interface ethernet 1/1
Information of Eth 1/1
 DSCP to queue map.
 d1:d2   0   1   2   3   4   5   6   7   8   9
 -----------------------------------------
 0   :   2   2   2   2   2   2   2   2   0   0
 1   :   0   0   0   0   0   0   1   1   1   1
 2   :   1   1   1   1   3   3   3   3   3   3
```

```
 3   :   3   3   4   4   4   4   4   4   4   4
 4   :   5   5   5   5   5   5   5   5   6   6
 5   :   6   6   6   6   6   6   7   7   7   7
 6   :   7   7   7   7

Console#
```

20.2.6 show qos map trust-mode

本コマンドは、QoS マッピングモードを示します。

構文

show qos map trust-mode interface *interface*

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

以下は、信頼モードが CoS に設定されていることを示しています。

```
Console#show qos map trust-mode interface ethernet 1/5
Information of Eth 1/5
  CoS Map Mode:          CoS mode
Console#
```

21 QoS コマンド

本章で説明するコマンドは、Differentiated Services（DiffServ）分類基準とサービスポリシーを設定するために使用されます。アクセスリスト、IP Precedence または DSCP 値、または VLAN にもとづいてトラフィックを分類できます。アクセスリストを使用すると、各パケットに含まれるレイヤ 2、レイヤ 3、またはレイヤ 4 の情報をもとにトラフィックを選択することができます。

表 21-1 QoS コマンド

コマンド	機能	モード
class-map	トラフィックタイプのクラスマップを作成します。	GC
description	クラスマップの説明を指定します。	CM
match	トラフィックを分類するために使用される基準を定義します。	CM
rename	クラスマップの名前を再定義します。	CM
policy-map	複数のインタフェースのポリシーマップを作成します。	GC
description	ポリシーマップの説明を指定します。	PM
class	ポリシーが動作するトラフィックの分類を定義します。	PM
rename	ポリシーマップの名前を再定義します。	PM
police rate	設定したフローレートに基づいて分類されたトラフィックの帯域制限を定義します。	PM-C
set cos	内部処理のために一致するパケットの CoS 値を書き換えます。	PM-C
set ip dscp	内部処理のために一致するパケットの IP DSCP 値を書き換えます。	PM-C
service-policy	policy-map コマンドで定義されたポリシーマップを特定のインタフェースに適用します。	IC
show class-map	トラフィックの分類に使用される一致基準を定義する QoS クラスマップを表示します。	PE
show policy-map	受信トラフィックの分類基準を定義する QoS ポリシーマップを表示し、帯域制限のポリサーを含めることができます。	PE
show policy-map interface	指定されたインタフェース上のすべてのサービスポリシーに対して設定されたすべてのクラスの設定を表示します。	PE

特定のカテゴリの受信トラフィックのサービスポリシーを作成するには、次の手順を実行します。

1. class-map コマンドを使用して、特定のトラフィックカテゴリのクラス名を指定し、クラスマップコンフィグレーションモードに移行します。
2. match コマンドを使用して、アクセスリスト、IPv4 DSCP 値、IPv4 Precedence 値、IPv6 DSCP 値、VLAN、または CoS 値に基づいて、特定のタイプのトラフィックを選択します。 クラスマップには、IP 値と VLAN の両方の一致設定を含めることができます。
3. policy-map コマンドを使用して、受信トラフィックを処理する特定の方法のポリシー名を指定し、ポリシーマップコンフィグレーションモードに移行します。
4. class コマンドを使用してクラスマップを識別し、ポリシーマップクラスコンフィグレーションモード

を開始します。 ポリシーマップには、最大 16 のクラスマップを含めることができます。

5. set cos コマンドを使用して、ホップ単位の動作、一致するトラフィッククラスの VLAN タグ内の CoS 値を変更し、police rate コマンドを使用して指定されたレートを超えるトラフィックを廃棄します。
6. 特定のインタフェースにポリシーマップを割当てるには、service-policy コマンドを使用します。

Note: ポリシーマップを作成する前に、クラスマップを作成します。

21.1 コマンド説明

21.1.1 class-map

本コマンドは、指定されたクラスにパケットを一致させるために使用されるクラスマップを作成し、クラスマップコンフィグレーションモードを開始します。クラスマップを削除するには、no 形式を使用してください。

構文

[no] class-map *class-map-name* [match-any]

class-map-name - クラスマップの名前です。(範囲: 1 から 32 文字)

match-any - クラスマップを全てのパケットに適用します。

デフォルト設定

match-any

コマンドモード

Global Configuration

コマンドの使用方法

- はじめに本コマンドを入力してクラスマップを指定し、クラスマップコンフィグレーションモードに移行します。次に、match コマンドを使用して、このクラスマップで分類される受信トラフィックの基準を指定します。
- 1 つまたは複数のクラスマップをポリシーマップに割当てることができます。ポリシーマップは、サービスポリシーによってインタフェースに割り当てられます。サービスポリシーは、パケット分類、サービスタグ付け、および帯域幅ポリシングを定義します。ポリシーマップがインタフェースにバインドされると、クラスマップをポリシーマップに追加することも、match コマンドで割当てられたクラスマップに変更を加えることもできません。

例

この例では、「rd-class」というクラスマップを作成し、DSCP サービス値 3 のパケットに一致するように設定します。

```
Console(config)#class-map rd-class
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

関連コマンド

show class-map

21.1.2 description

本コマンドは、クラスマップまたはポリシーマップの説明を指定します。

構文

description *string*

no description

string - クラスマップまたはポリシーマップの説明です。(範囲: 1 から 64 文字)

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description “matches packets marked for DSCP service value 3”
Console(config-cmap)#
```

21.1.3 match

本コマンドは、トラフィックを分類するために使用される基準を定義します。一致する基準を削除するには、no 形式を使用してください。

構文

[no] match {access-list *acl-name* | cos *cos* | ip dscp *dscp* |

ip precedence *ip-precedence* | ipv6 dscp *dscp* | vlan *vlan*}

acl-name - アクセス制御リストの名前です。標準または拡張 IPv4 / IPv6 ACL および MAC ACL を含む、任意のタイプの ACL を指定できます。(範囲: 1 から 32 文字)

cos - CoS の値です。(範囲: 0 から 7)

dscp - DSCP 値です。(範囲: 0 から 63)

ip-precedence - IP Precedence 値です。(範囲: 0 から 7)

vlan - VLAN 値です。（範囲:1 から 4094）

デフォルト設定

無し

コマンドモード

Class Map Configuration

コマンドの使用方法

- まず、class-map コマンドを入力してクラスマップを指定し、クラスマップコンフィグレーションモードを開始します。次に、match コマンドを使用して、このクラスマップに適合する条件を指定します。
- 受信パケットが本コマンドで指定された ACL と一致する場合、ACL に含まれるすべての deny ルールは無視されます。
- 一致基準に IP ACL または IP 優先順位ルールが含まれている場合、VLAN ルールを同じクラスマップ

に含めることはできません。

- ◆ 一致条件に MAC ACL または VLAN ルールが含まれている場合、IP ACL も IP 優先順位ルールも同じクラスマップに含めることはできません。
- ◆ クラスマップには、最大 16 の一致エントリを含めることができます。

例

この例では、「rd-class＃1」というクラスマップを作成し、DSCP サービス値 3 とマークされたパケットに一致するように設定します。

```
Console(config)#class-map rd-class#1
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

この例では、「rd-class＃2」というクラスマップを作成し、IP Precedence サービス値 5 とマークされたパケットに一致するように設定します。

```
Console(config)#class-map rd-class#2
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

この例では、「rd-class＃3」というクラスマップを作成し、VLAN 1 にマークされたパケットに一致するように設定します。

```
Console(config)#class-map rd-class#3
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

21.1.4 rename

本コマンドは、クラスマップまたはポリシーマップの名前を再定義します。なお、既に設定済みのクラスマップまたはポリシーマップの名前を再定義した場合、設定済みの名称も再定義されます。

構文

rename *map-name*

map-name - クラスマップまたはポリシーマップの名前です。(範囲: 1 から 32 文字)

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
```

```
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

21.1.5 policy-map

本コマンドは、複数のインタフェースに割り当てることができるポリシーマップを作成し、ポリシーマップコンフィグレーションモードに移行します。ポリシーマップを削除するには、no 形式を使用してください。

構文

[no] policy-map *policy-map-name*

policy-map-name - ポリシーマップの名前です。(範囲: 1 から 32 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- policy-map コマンドを使用してポリシーマップの名前を指定し、class コマンドを使用して、クラスマップで定義された基準に一致するトラフィックのポリシーを設定します。
- ポリシーマップには、service-policy コマンドを使用して同じインタフェースに適用できる複数のクラスステートメントを含めることができます。
- クラスマップをポリシーマップに割当てる前に、クラスマップを作成してください。

例

この例では、 "rd-policy"というポリシーを作成し、class コマンドを使用して以前に定義された "rd-class"を指定し、set コマンドを使用して受信パケットに実施するサービスを設定します。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 0
Console(config-pmap-c)#
```

21.1.6 class

本コマンドは、ポリシーが動作するトラフィック分類を定義し、ポリシーマップクラスコンフィグレーションモードに移行します。クラスマップを削除するには、no 形式を使用してください。

構文

[no] class *class-map-name*

class-map-name - クラスマップの名前です。(範囲: 1 から 32 文字)

デフォルト設定

無し

コマンドモード

Policy Map Configuration

コマンドの使用方法

- policy-map コマンドを使用して、ポリシーマップを指定し、ポリシーマップコンフィグレーションモードに移行します。次に、class コマンドを使用して、ポリシーマップクラスコンフィグレーションモードに移行します。最後に、set コマンドと police コマンドを使用して一致基準を指定します。
  - set cos コマンドは、一致するパケットの CoS 値を設定します。（これにより、VLAN タグのパケット優先度が変更されます。）
  - set ip dscp コマンドは、一致するパケットの DSCP 値を設定します。
  - police rate コマンドは、帯域制限のレートを定義します。
- ポリシーマップには、最大 16 のクラスを含めることができます。

例

この例では、 "rd-policy"というポリシーを作成し、class コマンドを使用して以前定義した "rd-class"を指定し、set cos コマンドを使用して受信パケットに実施するサービスを設定します。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#
```

21.1.7 police rate

本コマンドは、設定したフローレートに基づいて、分類されたトラフィックの帯域制限を定義します。ポリサーを削除するには、no 形式を使用してください。

構文

[no] police rate *committed-rate*

committed-rate - コミットされた情報速度をキロビット/秒で表します。(範囲: 16 から 1000000 kbps、64 kbps または最大ポート速度のいずれか小さい方です。)

デフォルト設定

無し

コマンドモード

Policy Map Class Configuration

コマンドの使用方法

- 受信ポート用に最大 16 のポリサー（クラスマップ）を設定できます。
- committed-rate は、設定されたインタフェース速度を超えることはできません。
- ポリシングはトークンバケットに基づいており、バケットの深さはバケットがオーバーフローする前の最大バーストであり、バケットに追加される平均レートトークンは committed-rate によって指定されます。トークンバケットは、RFC 2697 および RFC 2698 で説明されているものと同様の機能を持つことに注意してください。
- メーターの動作は、1 つのトークンバケット（C)、トークンがインクリメントされるレート（CIR - Committed Information Rate)、およびトークンバケットの最大サイズ（BC - Committed Burst Size）によって指定されます。
  トークンバケット C は、最初は満杯であり、すなわちトークンカウント Tc（0）= BC です。その後、トークンカウント Tc は、以下のように秒当たり CIR 回更新されます。
  - Tc が BC よりも小さい場合、Tc は 1 だけインクリメントされ、そうでなければ
  - Tc はインクリメントされません。

  サイズ B バイトのパケットが時刻 t に到着すると、次のようになります。
  - Tc（t）-B ≧ 0 の場合、パケットは緑色であり、Tc は B だけ減少して最小値の 0 まで減少し、
  - それ以外のパケットは赤で、Tc はデクリメントされません。

例

この例では、"rd-policy"というポリシーマップを作成し、class コマンドにて以前定義した"rd-class"に指定し、police rate コマンドを使用して平均帯域幅を 100,000Kbps に制限します。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#police rate 100000
Console(config-pmap-c)#
```

21.1.8 set cos

本コマンドは、一致するパケット（match コマンドで指定されたもの）の VLAN タグ内のサービスクラス（CoS）値を変更します。　この設定を削除するには、no 形式を使用してください。

構文

[no] set cos *cos-value*

cos-value - CoS の値です。(範囲: 0 から 7)

デフォルト設定

無し

コマンドモード

Policy Map Class Configuration

コマンドの使用方法

- set cos コマンドは、一致するパケットの VLAN タグに CoS 値を設定するために使用します。
- set cos コマンドと set ip dscp コマンドは同時に設定できません。

例

この例では、 "rd-policy"というポリシーを作成し、class コマンドを使用して以前定義した "rd-class"を指定し、set cos コマンドを使用して受信パケットの cos 値を 3 に変更するサービスを設定します。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#
```

21.1.9 set ip dscp

本コマンドは、IPv4 ヘッダの TOS フィールドまたは IPv6 ヘッダの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 値を変更します。　この設定を削除するには、no 形式を使用してください。

構文

[no] set ip dscp *dscp*

dscp - DSCP の値です。(範囲: 0 から 63)

デフォルト設定

無し

コマンドモード

Policy Map Class Configuration

コマンドの使用方法

- set ip dscp コマンドは、一致するパケットの ToS フィールドの優先度の値を設定するために使用します。
- set cos コマンドと set ip dscp コマンドは同時に設定できません。

例

この例では、"rd-policy"というポリシーマップを作成し、class コマンドにて以前定義した"rd-class"に指定し、set ip dscp コマンドを使用して受信パケットの DSCP 値を 3 に変更するサービスを設定します。

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#
```

21.1.10 service-policy

本コマンドは、policy-map コマンドで定義された policy-map を特定のインタフェースの受信側に適用します。このマッピングを削除するには、no 形式を使用してください。

構文

[no] service-policy input *policy-map-name*

input - 受信トラフィックに適用します。

policy-map-name - このインタフェースに設定するポリシーマップの名前です。(範囲: 1 から 32 文字)

デフォルト設定

インタフェースにはポリシーマップは関連付けられていません。

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- インタフェースに割当てられるポリシーマップは 1 つだけです。
- 既にポリシーマップを適用しているインタフェースに別のポリシーマップを適用する場合には、適用済みのポリシーマップを削除してから適用してください。
- 最初にクラスマップを定義し、次にポリシーマップを定義し、最後に service-policy コマンドを使用してポリシーマップを必要なインタフェースに割り当てます。

例

この例では、サービスポリシーを受信インタフェースに適用します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd-policy
Console(config-if)#
```

21.1.11 show class-map

本コマンドは、トラフィックを分類するために使用される一致基準を定義する QoS クラスマップを表示します。

構文

show class-map [*class-map-name*]

class-map-name - クラスマップの名前です。(範囲: 1 から 32 文字)

デフォルト設定

すべてのクラスマップを表示します。

コマンドモード

Privileged Exec

例

```
Console#show class-map
Class Map match-any rd-class#1
Description:
 Match ip dscp 10
 Match access-list rd-access
 Match ip dscp 0

Class Map match-any rd-class#2
 Match ip precedence 5

Class Map match-any rd-class#3
 Match vlan 1

Console#
```

21.1.12 show policy-map

本コマンドは、受信トラフィックの分類基準を定義する QoS ポリシーマップを表示し、帯域制限のポリサーを含めることができます。

構文

show policy-map [*policy-map-name* [class *class-map-name*]]

policy-map-name - ポリシーマップの名前です。(範囲: 1 から 32 文字)

class-map-name - クラスマップの名前です。(範囲: 1 から 32 文字)

デフォルト設定

すべてのポリシーマップとすべてのクラスを表示します。

コマンドモード

Privileged Exec

例

```
Console#show policy-map
Policy Map rd-policy
Description:
 class rd-class
 class finance-class
  police rate 100 class rd-class
```

```
Policy Map rd-policy
 class rd-class
Console#
```

21.1.13 show policy-map interface

本コマンドは、指定されたインタフェースに割当てられたサービスポリシーを表示します。

構文

show policy-map interface *interface* input

interface

unit/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

コマンドモード

Privileged Exec

例

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#show policy-map interface
Interface ethernet 1/2
  service-policy input policy-map
Interface ethernet 1/3
  service-policy input policy-map
Interface ethernet 1/4
  service-policy input policy-map
Interface ethernet 1/5
  service-policy input policy-map
Console#
```

22 マルチキャストフィルタリングコマンド

このスイッチは IGMP（Internet Group Management Protocol）を使用して、VLAN 内にマルチキャストグループの受信者が存在するか確認し、受信者を接続するポートにのみマルチキャストパケットを中継します。また、受信者からの加入/離脱要求を隣接するマルチキャストスイッチ/ルータに中継することで、マルチキャストパケットの中継を制御します。

Note: IGMP snooping と MLD snooping を同時に使用する場合、最大エントリ数は IGMP snooping と MLD snooping の合計で 511 エントリになります。

Note: IGMPv3 snooping と MLDv2 snooping では ASM(any-source multicast)だけをサポートします(SSM (source-specific multicast)は未サポート)。そのため、送信元アドレスを指定した IGMPv3 Report メッセージおよび MLDv2 Report メッセージを受信した場合、当該 Report メッセージではエントリを生成しません。

表 22-1 マルチキャストフィルタリングコマンド

コマンドグループ	機能
IGMP Snooping	IGMP snooping の各機能について設定/表示します。
IGMP Filtering and Throttling	IGMP フィルタリングと IGMP スロットリングを設定します。
MLD Snooping	MLD snooping の各機能について設定/表示します。
MLD Filtering and Throttling	MLD フィルタリングと MLD スロットリングを設定します。

22.1 IGMP snooping

本章では、スイッチ上で IGMP snooping を設定するために使用するコマンドについて説明します。

表 22-2　IGMP snooping コマンド

コマンド	機能	モード
ip igmp snooping	IGMP snooping を有効にします。	GC
ip igmp snooping mrouter-forward-mode dynamic	IGMP Report メッセージを受信したマルチキャストルータポートにだけマルチキャストパケットを中継します。	GC
ip igmp snooping proxy-reporting	IGMP snooping のプロキシ機能を有効にします。	GC
ip igmp snooping querier	IGMP snooping のクエリア機能を有効にします。	GC
ip igmp snooping router-alert-option-check	Router Alert オプションを含まない IGMPv2 / v3 メッセージを破棄します。	GC
ip igmp snooping router-port-expire-time	Dynamic のマルチキャストルータポートの有効時間を設定します。	GC
ip igmp snooping tcn-flood	スパニングツリーのトポロジの変更が発生したときにマルチキャストパケットをフラッディングします。	GC
ip igmp snooping tcn-query-solicit	スパニングツリーのトポロジの変更が発生したときに IGMP Query メッセージを送信します。	GC
ip igmp snooping unregistered-data-flood	未学習のマルチキャストパケットをフラッディングします。	GC
ip igmp snooping unsolicited-report-interval	プロキシ機能が有効の場合に、本装置が上流に送信する IGMP Report メッセージの送信周期を設定します。	GC
ip igmp snooping version	IGMP バージョンを設定します。	GC
ip igmp snooping version-exclusive	現在設定されている IGMP バージョンとは異なる IGMP バージョンの IGMP メッセージを受信した場合、当該メッセージを破棄します。	GC
ip igmp snooping vlan general-query-suppression	受信者が接続されていないポートへの General Query メッセージの中継を抑止します。	GC
ip igmp snooping vlan immediate-leave	即時離脱機能を設定します。	GC
ip igmp snooping vlan last-memb-query-count	クエリア機能使用時、マルチキャストグループ離脱時に送信する、Group-Specific Query メッセージの送信回数を設定します。	GC
ip igmp snooping vlan last-memb-query-intvl	クエリア機能使用時、マルチキャストグループ離脱時に送信する、Group-Specific Query メッセージの送信間隔を設定します。	GC
ip igmp snooping vlan mrouter	Static のマルチキャストルータポートを設定します。	GC
ip igmp snooping vlan proxy-address	プロキシ機能使用時に送信する IGMP Query メッセージ、IGMP Report メッセージおよび IGMP Leavet メッセージに設定するソースアドレスを設定します。	GC
ip igmp snooping vlan proxy-reporting	VLAN インタフェースでプロキシ機能を有効にします。	GC
ip igmp snooping vlan query-interval	IGMP General Query メッセージの送信間隔を設定します。	GC
ip igmp snooping vlan query-resp-intvl	IGMP General Query メッセージに対する受信者の最大応答時間を設定します。	GC
ip igmp snooping vlan static	Static の学習エントリを設定します。	GC

コマンド	機能	モード
clear ip igmp snooping groups dynamic	Dynamic の学習エントリを削除します。	PE
clear ip igmp snooping statistics	IGMP snooping の統計情報を消去します。	PE
show ip igmp snooping	IGMP snooping の設定を表示します。	PE
show ip igmp snooping group	IGMP snooping の学習エントリの情報を表示します。	PE
show ip igmp snooping mrouter	マルチキャストルータポートを表示します。	PE
show ip igmp snooping statistics	IGMP snooping の統計情報を表示します。	PE

22.1.1 ip igmp snooping

本コマンドは、グローバルまたは選択した VLAN インタフェースで IGMP snooping を有効にします。無効にするには、no 形式を使用してください。

構文

[no] ip igmp snooping [vlan *vlan-id*]

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- IGMP snooping がグローバルで有効の場合、VLAN インタフェースの設定が優先されます。
- IGMP snooping をグローバルで無効にすると、VLAN インタフェースごとに IGMP snooping を設定できますが、再びグローバルで IGMP snooping を有効にするまで、VLAN インタフェースの設定は有効になりません。

例

IGMP snooping をグローバルで有効にします。

```
Console(config)#ip igmp snooping
Console(config)#
```

22.1.2 ip igmp snooping mrouter-forward-mode dynamic

本コマンドは、IGMP Report メッセージを受信したマルチキャストルータポートにだけ、マルチキャストパケットを中継します。無効にするには、no 形式を使用してください。

構文

ip igmp snooping mrouter-forward-mode dynamic

no ip igmp snooping mrouter-forward-mode

デフォルト設定

無効

コマンドモード

Global Configuration

例

本機能をグローバルで有効にします。

Console(config)# ip igmp snooping mrouter-forward-mode dynamic

Console(config)#

22.1.3 ip igmp snooping proxy-reporting

本コマンドは、IGMP snooping のプロキシ機能を有効にします。デフォルト設定に戻すには、no 形式を使用してください。

構文

[no] ip igmp snooping proxy-reporting

ip igmp snooping vlan *vlan-id* proxy-reporting {enable | disable}

no ip igmp snooping vlan *vlan-id* proxy-reporting

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

enable - 指定した VLAN で有効にします。

disable - 指定した VLAN で無効にします。

デフォルト設定

Global: 無効

VLAN: グローバル設定に準じます

コマンドモード

Global Configuration

コマンドの使用方法

◆ 本コマンドを使用してプロキシ機能を有効にすると、本装置は最終 Leave と IGMP Query 抑制を含む「IGMP Snooping with Proxy Reporting」（DSL Forum TR-101、2006 年 4 月で定義）を実行します。最終 Leave は、最後の受信者がマルチキャストグループを離脱するときに IGMP Query メッセージを送信し、IGMP Query 抑制は、上流から送信された IGMP Query メッセージを受信者に転送しないことを意

味します。

◆ プロキシ機能が VLAN 上で設定されている場合、この設定はグローバル設定よりも優先されます。

例

プロキシ機能をグローバルで有効にします。

```
Console(config)#ip igmp snooping proxy-reporting
Console(config)#
```

22.1.4 ip igmp snooping querier

本コマンドは、本装置を IGMP クエリアとして有効にします。無効にするには、no 形式を使用してください。

構文

[no] ip igmp snooping querier

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

◆ IGMP クエリアを有効にした場合、本装置が代表クエリアに選出されれば、本装置がクエリアとして機能します。クエリアは、マルチキャストパケットを受信するかどうかを受信者に問い合わせます。

例

クエリア機能をグローバルで有効にします。

```
Console(config)#ip igmp snooping querier
Console(config)#
```

22.1.5 ip igmp snooping router-alert-option-check

本コマンドは、Router Alert オプションを含まない IGMPv2 / v3 メッセージを破棄します。IGMP メッセージを受信するときに、Router Alert オプションを無視するには、no 形式を使用してください。

構文

[no] ip igmp snooping router-alert-option-check

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

IGMP バージョン 3 の RFC 3376 のセクション 9.1 で説明されているように、Router Alert オプションを使用して DOS 攻撃から保護することができます。DOS 攻撃の一般的な方法の 1 つとして、クエリアに成りすました攻撃者が、大きなソースリストがあり、最大応答時間が大きな値に設定した多数の Group-and-Source Specific Query メッセージを送信して受信者に過負荷をかけます。

この種の攻撃から保護するために、(1) スイッチは IGMP Query メッセージを転送すべきではありません。クエリアが Router Alert オプションを持っている場合、これは簡単に実行できます。(2) また、スイッチが受信者の役割（プロキシ機能を使用している場合など）で動作している場合、Router Alert オプションを含まないバージョン 2 または 3 の IGMP Query メッセージは無視する必要があります。

例

Router Alert オプションチェックをグローバルで有効にします。

```
Console(config)#ip igmp snooping router-alert-option-check
Console(config)#
```

22.1.6 ip igmp snooping router-port-expire-time

本コマンドは、Dynamic に設定したマルチキャストルータポートの有効時間を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

seconds - Dynamic に学習したマルチキャストルータポートの有効時間を設定します。(範囲: 1 から 65535; 推奨範囲：300 から 500)

デフォルト設定

300 秒

コマンドモード

Global Configuration

例

有効時間を 400 秒に設定する方法を示します。

```
Console(config)#ip igmp snooping router-port-expire-time 400
```

```
Console(config)#
```

22.1.7 ip igmp snooping tcn-flood

本コマンドは、スパニングツリーのトポロジ変更通知（TCN）が発生した場合に、マルチキャストパケットのフラッディングを有効にします。フラッディングを無効にするには、no 形式を使用してください。

構文

[no] ip igmp snooping tcn-flood

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- スパニングツリーのトポロジ変更が発生すると、スイッチによって学習されたエントリ情報が古くなっている可能性があります。トポロジ変更時、すべての受信者にマルチキャストパケットが確実に配信されるようにするために、トポロジが安定してすべての受信者へのマルチキャストの中継経路が学習されるまでの間、マルチキャストパケットをフラッディングします。
- トポロジ変更通知（TCN）が受信され、その後すべてのアップリンクポートが削除されると、マルチキャストルータではすべてのマルチキャストグループがタイムアウトにより削除されます。
- 新しいアップリンクポートが起動すると、スイッチは新しいアップリンクポートに現在学習しているすべてのマルチキャストグループの IGMP Report メッセージを送信します。
- 本機能を有効にすると、トポロジの変更が発生した場合、スイッチはただちにマルチキャストパケットをフラッディングします。この場合、多くのマルチキャストグループに加入していると、フラッディングによってスイッチと受信者間の回線に過剰な負荷がかかる可能性があります。これを避けるために本機能を無効にして、マルチキャストパケットのフラッディングを抑制することができます。
- トポロジが変更されると、ルートブリッジは代理で IGMP Query メッセージを送信して、マルチキャストグループへの加入状況を迅速に再学習します。

例

TCN フラッディングを有効にします。

```
Console(config)#ip igmp snooping tcn-flood
Console(config)#
```

22.1.8 ip igmp snooping tcn-query-solicit

本コマンドは、スパニングツリーのトポロジ変更通知（TCN）が発生したときに IGMP General Query メッセージを送信するように設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip igmp snooping tcn-query-solicit

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- スパニングツリーのルートブリッジが、IGMP snooping が有効になっている VLAN のトポロジ変更通知を受信すると、IGMP General Query メッセージを要求するために、グローバルな IGMP Leave メッセージを送信します。スイッチはこのメッセージを受信すると、スパニングツリーの変更が発生した VLAN 内のすべてのポートにフラッディングします。上流のマルチキャストルータがこのメッセージを受信すると、IGMP General Query メッセージを即座に送信します。
- ip igmp snooping tcn query-solicit コマンドを使用すると、スイッチがスパニングツリーのルートブリッジでなくても、トポロジ変更に気付くたびに IGMP Query メッセージを送信します。

例

スパニングツリーのトポロジ変更通知を受信するたびに IGMP Query メッセージを送信するように設定します。

```
Console(config)#ip igmp snooping tcn query-solicit
Console(config)#
```

22.1.9 ip igmp snooping unregistered-data-flood

本コマンドは、未学習のマルチキャストパケットを、VLAN 内にフラッディングします。未学習のマルチキャストパケットを廃棄するには、no 形式を使用してください。

構文

[no] ip igmp snooping unregistered-data-flood

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

IGMP snooping およびマルチキャストルーティング用のマルチキャストエントリを格納するために使用されるテーブルがいっぱいになると、新しいエントリは学習されません。接続された VLAN にルータポートが設定されておらず、未登録のフラッディングがディセーブルの場合、テーブル内に見つからない後続のマ

ルチキャストトラフィックは廃棄され、それ以外の場合は VLAN 全体にフラッディングされます。

本コマンドを設定した場合、未学習のマルチキャストパケットは VLAN 内にフラッディングします。本コマンドを設定しない場合、VLAN にマルチキャストルータポートが設定されている場合はマルチキャストルータポートに中継し、マルチキャストルータポートが設定されていない場合は廃棄します。

例

未学習のマルチキャストパケットを、VLAN 内にフラッディングする設定をします。

```
Console(config)#ip igmp snooping unregistered-data-flood
Console(config)#
```

22.1.10 ip igmp snooping unsolicited-report-interval

本コマンドは、プロキシ機能が有効な場合に、本装置が上流に送信する IGMP Report メッセージの送信間隔を設定します。　デフォルト値に復元するには、no 形式を使用してください。

構文

ip igmp snooping unsolicited-report-interval *seconds*

no ip igmp snooping unsolicited-report-interval

seconds - 本装置が IGMP Report メッセージを送信する間隔です。(範囲: 1 から 65535 秒)

デフォルト設定

400 秒

コマンドモード

Global Configuration

コマンドの使用方法

- 新しいマルチキャストルータポートが追加されると、本装置は追加されたマルチキャストルータポートに現在学習しているすべてのマルチキャストグループの IGMP Report メッセージを送信します。
- 本コマンドは、プロキシ機能が有効になっている場合にのみ適用されます。

例

プロキシ機能有効時に送信する IGMP Report メッセージの送信間隔を 50 秒を設定します。

```
Console(config)#ip igmp snooping unsolicited-report-interval 50
Console(config)#
```

22.1.11 ip igmp snooping version

本コマンドは、IGMP snooping で使用する IGMP バージョンを設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ip igmp snooping [vlan *vlan-id*] version {1 | 2 | 3}

no ip igmp snooping [vlan *vlan-id*] version

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

1 - IGMP バージョン 1

2 - IGMP バージョン 2

3 - IGMP バージョン 3

デフォルト設定

Global: IGMP バージョン 2

VLAN: グローバル設定に準じます

コマンドモード

Global Configuration

コマンドの使用方法

- 本コマンドは、IGMP snooping で使用される IGMP Report/Query メッセージのバージョンを設定します。バージョン 1 から 3 はすべてサポートされており、バージョン 2 と 3 は下位互換性があるため、使用している IGMP バージョンに関係なく、本装置は他のデバイスと連携できます。
- IGMP バージョンが VLAN インタフェースで設定されている場合、この設定はグローバル設定よりも優先されます。

例

IGMP バージョン 1 をグローバルに設定します。

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

22.1.12 ip igmp snooping version-exclusive

本コマンドは、ip igmp snooping version コマンドで設定されているものとは異なる IGMP バージョンの IGMP メッセージ(マルチキャストパケットを除く)を受信した場合、すべて破棄します。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip igmp snooping [vlan *vlan-id*] version-exclusive

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

デフォルト設定

Global: 無効

VLAN: 無効

コマンドモード

Global Configuration

コマンドの使用方法

- VLAN インタフェースで本コマンドが無効の場合、本コマンドの設定はグローバルの設定に準じます。 VLAN インタフェースで有効の場合は、VLAN インタフェースの設定がグローバルの設定よりも優先されます。
- 本コマンドを無効にすると、現在設定している IGMP バージョンは下位互換性があります（ip igmp snooping version コマンドを参照）。

例

異なる IGMP バージョンの IGMP メッセージを破棄する設定をします。

```
Console(config)#ip igmp snooping version-exclusive
Console(config)#
```

22.1.13 ip igmp snooping vlan general-query-suppression

本コマンドは、送信者を接続していないポートへの IGMP General Query メッセージの中継を抑止します。IGMP General Query メッセージをフラッディングするには、no 形式を使用してください。

構文

[no] ip igmp snooping vlan *vlan-id* general-query-suppression

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- デフォルトでは、IGMP General Query メッセージは、VLAN 内にフラッディングされます。
- 本機能が有効の場合、IGMP General Query メッセージは受信者を説蔵しているポートにだけ中継されます。

例

IGMP General Query メッセージの中継を抑止する設定をします。

```
Console(config)#ip igmp snooping vlan 1 general-query-suppression
Console(config)#
```

22.1.14 ip igmp snooping vlan immediate-leave

本コマンドは、IGMP 即時離脱機能を設定します。IGMP 即時離脱機能は IGMP Leave メッセージを受信した場合、当該受信ポートをマルチキャストグループから即座に削除します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ip igmp snooping vlan *vlan-id* immediate-leave [by-host-ip]

no ip igmp snooping vlan *vlan-id* immediate-leave

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

by-host-ip - 当該マルチキャストグループに加入している最後の受信者から IGMP Leave メッセージを受信した場合に、当該マルチキャストグループから受信ポートを削除します。

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- 本機能を使用しない場合、マルチキャストルータまたはクエリアは、IGMP Leave / IGMPv3 Report(離脱要求)メッセージを受信すると、IGMP Group Specific Query メッセージを送信します。マルチキャストルータまたはクエリアは、IGMP Group Specific Query メッセージに対する受信者からの IGMP Report メッセージの応答がない場合にのみ、当該ポートへのマルチキャストパケットの中継を停止します。（この動作は、RFC 2236 で定義されている Last Member Query Interval（1 秒固定）* Robustness Variable（固定値 2）によって定義されています）
- 本機能を使用している場合、本装置は 1 台の受信者だけが当該ポートに接続されていると見なして削除処理を行います。したがって、同じマルチキャストグループに加入する複数の受信者が当該ポートに接続されている場合、1 台の受信者からの離脱要求で即座にエントリを削除するため、他の受信者へのマルチキャスト中継が停止します。
- 「by-host-ip」オプションを使用した場合、IGMP Leave メッセージ受信時に、当該マルチキャストグループに加入している受信者が他に存在しているか確認します。当該マルチキャストグループに加入している受信者が存在しなくなったときに、当該ポートをマルチキャストグループから削除します。
- 本コマンドは、IGMPv2 または IGMPv3 スヌーピングが使用されている場合にのみ有効です。

例

VLAN 1 に IGMP 即時離脱機能を有効にします。

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

22.1.15 ip igmp snooping vlan last-memb-query-count

本コマンドは、IGMP Leave メッセージ受信時に送信する IGMP Group Specific Query メッセージの送信回数

を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ip igmp snooping vlan *vlan-id* last-memb-query-count *count*

no ip igmp snooping vlan *vlan-id* last-memb-query-count

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

count - IGMP Group Specific Query メッセージの送信回数です。(範囲: 1 から 255)

デフォルト設定

2

コマンドモード

Global Configuration

コマンドの使用方法

本コマンドは、プロキシ機能または IGMP クエリアが有効の場合にのみ有効です.。

例

IGMP Group Specific Query メッセージの送信回数に 7 を設定します。

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7
Console(config)#
```

22.1.16 ip igmp snooping vlan last-memb-query-intvl

本コマンドは、IGMP Leave メッセージ受信時に送信する IGMP Group Specific Query メッセージの送信間隔を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ip igmp snooping vlan *vlan-id* last-memb-query-intvl *interval*

no ip igmp snooping vlan *vlan-id* last-memb-query-intvl

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

interval - IGMP Group Specific Query メッセージの送信間隔です。(範囲: 1 から 31744 秒）

デフォルト設定

10（1 秒）

コマンドモード

Global Configuration

コマンドの使用方法

◆ 受信者がマルチキャストグループから離脱する場合、IGMP Leave メッセージを送信します。IGMP

Leave メッセージを本装置賀が受信すると、IGMP Group Specific Query メッセージを送信して、この受信者が最後にマルチキャストグループから脱退したかどうかを確認ます。他の受信者から IGMP Report メッセージの応答が無い場合、当該 IGMP Leave メッセージが最後の受信者からのメッセージと見なし、当該ポートをマルチキャストグループから削除します。

- 値を小さくすると、グループまたはソースの最後のメンバーの損失を検出する時間が短縮されますが、バースト性の高いトラフィックが生成される可能性があります。
- 本コマンドは、プロキシ機能またはクエリア機能が有効になっている場合にのみ有効です。

例

IGMP Group Specific Query メッセージの送信回数に 5 秒を設定します。

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 50
Console(config)#
```

22.1.17 ip igmp snooping vlan mrouter

本コマンドは、指定された VLAN インタフェースにマルチキャストルータポートを Static に設定します。設定を削除するには、no 形式を使用してください。

構文

[no] ip igmp snooping vlan *vlan-id* mrouter *interface*

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

Static マルチキャストルータポートは設定されていません。

コマンドモード

Global Configuration

コマンドの使用方法

- ネットワークによっては、IGMP snooping が IGMP クエリアを検出できないことがあります。この場合、本コマンドで既知のマルチキャストルータまたはスイッチを接続しているポートまたはチャネルグループを Static にマルチキャストルータポートに設定することができます。
- マルチキャストルータポートを有効にするには、IGMP snooping をグローバルに有効にする必要があります（ip igmp snooping コマンドを使用）。

例

ポート 1/10 を VLAN 1 の Static マルチキャストルータポートに設定します。

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/10
Console(config)#
```

22.1.18 ip igmp snooping vlan proxy-address

本コマンドは、プロキシ機能使用時に送信する IGMP Query メッセージ、IGMP Report メッセージおよび IGMP Leave メッセージの送信元アドレスを設定します。送信元アドレスをデフォルトに復元するには、no 形式を使用してください。

構文

ip igmp snooping vlan *vlan-id* proxy-address *source-address*

no ip igmp snooping vlan *vlan-id* proxy-address

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

source-address - プロキシ機能で送信する IGMP ッセージで使用する送信元アドレスです。(任意の有効な IP ユニキャストアドレス)

デフォルト設定

0.0.0.0

コマンドモード

Global Configuration

コマンドの使用方法

プロキシ機能で送信する IGMP Query メッセージ、IGMP Report メッセージおよび IGMP Leave メッセージの送信元アドレスを、本コマンドで設定したユニキャストアドレスに置き換えることができます。

プロキシ機能に使用されるルール

プロキシ機能が有効な場合、送信元アドレスは次の基準で設定します。

- proxy-address が設定されている場合、設定されたアドレスを IGMP Query メッセージ、IGMP Report メッセージおよび IGMP Leave メッセージの送信元アドレスに使用します。
- proxy-address が設定されていない場合、VLAN の IP アドレスを IGMP Query メッセージに使用し、IGMP Report メッセージおよび IGMP Leave メッセージの送信元アドレスには受信者の IP アドレスを使用します。

例

プロキシ機能で送信する IGMP メッセージの送信元アドレスに 10.0.1.8 に設定します。

```
Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8
Console(config)#
```

22.1.19 ip igmp snooping vlan query-interval

本コマンドは、VLAN インタフェースに IGMP General Query メッセージを送信する間隔を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ip igmp snooping vlan *vlan-id* query-interval *interval*

no ip igmp snooping vlan *vlan-id* query-interval

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

interval - IGMP General Query メッセージを送信する間隔です。(範囲: 2 から 31744 秒)

デフォルト設定

125 秒

コマンドモード

Global Configuration

コマンドの使用方法

- 本コマンドで設定した間隔で IGMP General Query メッセージを送信します。このメッセージを受信者が受信すると、すべての受信者は、参加しているマルチキャストグループの IGMP Report メッセージを応答します。
- 本コマンドは、本装置がクエリアとして機能している場合に適用されます。
- 「IGMP General Query メッセージの送信間隔 > IGMP General Query メッセージの最大応答時間」となるように設定してください。

例

VLAN 1 の IGMP General Query メッセージの送信間隔を 150 秒に設定します。

```
Console(config)#ip igmp snooping vlan 1 query-interval 150
Console(config)#
```

関連コマンド

ip igmp snooping vlan query-resp-intvl

22.1.20 ip igmp snooping vlan query-resp-intvl

本コマンドは、本装置が送信する IGMP General Query メッセージの最大応答時間を設定します。受信者が当該 IGMP General Query メッセージを受信した場合、最大応答時間内でランダムに IGMP Report メッセージを応答します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ip igmp snooping vlan *vlan-id* query-resp-intvl *interval*

no ip igmp snooping vlan *vlan-id* query-resp-intvl

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

interval - 最大応答時間です。(範囲: 10 から 31740 の 10 分の 1 秒）

デフォルト設定

100（10 秒）

コマンドモード

Global Configuration

コマンドの使用方法

- 本コマンドは、本装置がクエリアとして機能している場合に適用されます。
- 「IGMP General Query メッセージの送信間隔 > IGMP General Query メッセージの最大応答時間」となるように設定してください。

例

VLAN 1 の IGMP General Query メッセージの最大応答時間に 20 秒を設定します。

```
Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20
Console(config)#
```

関連コマンド

ip igmp snooping vlan query-interval

22.1.21 ip igmp snooping vlan static

本コマンドは、IGMP snooping の学習エントリを Static に設定します。Static エントリを削除するには、no 形式を使用してください。

構文

[no] ip igmp snooping vlan *vlan-id* static *ip-address interface*

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

ip-address - マルチキャストグループの IP アドレスです

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- ◆ 静的エントリは決してタイムアウトしません。
- ◆ 静的エントリを VLAN インタフェースに設定すると、当該マルチキャストパケットは VLAN 内の静的エントリを設定したポートにのみ中継します。
- ◆ 静的エントリは最大 64 個まで設定できます。

例

vlan 1 の 1/5 にマルチキャストグループ(224.0.0.12)の Static エントリを設定します。

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

22.1.22 clear ip igmp snooping groups dynamic

本コマンドは、IGMP snooping によって Dynamic に学習したエントリ情報を消去します。

構文

clear ip igmp snooping groups dynamic

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドは、IGMP snooping によって Dynamic に学習したエントリだけを消去します。Static に設定したエントリは消去しません。

例

Dynamic に学習したエントリを消去します。

```
Console#clear ip igmp snooping groups dynamic
Console#
```

22.1.23 clear ip igmp snooping statistics

本コマンドは、IGMP snooping の統計情報を消去します。

構文

clear ip igmp snooping statistics [interface *interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

コマンドモード

Privileged Exec

例

IGMP snooping の統計情報を消去します。

```
Console#clear ip igmp snooping statistics
Console#
```

22.1.24 show ip igmp snooping

本コマンドは、IGMP snooping の設定値を表示します。

構文

show ip igmp snooping [vlan *vlan-id*]

vlan-id - VLAN ID (1-4094)

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドは、グローバルおよび VLAN インタフェースの IGMP snooping の設定値を表示します。

例

IGMP snooping の設定値を表示します。

```
Console#show ip igmp snooping
 IGMP Snooping                    : Enabled
 Router Port Expire Time          : 300 s
```

```
Router Alert Check                : Disabled
Router Port Mode                  : Forward
TCN Flood                         : Disabled
TCN Query Solicit                 : Disabled
Unregistered Data Flood           : Disabled
802.1p Forwarding Priority        : Disabled
Unsolicited Report Interval       : 400 s
Version Exclusive                 : Disabled
Version                           : 2
Proxy Reporting                   : Disabled
Querier                           : Disabled

VLAN 1:
--------
IGMP Snooping                     : Enabled
IGMP Snooping Running Status      : Inactive
Version                           : Using global Version (2)
Version Exclusive                 : Using global status (Disabled)
Immediate Leave                   : Disabled
Last Member Query Interval        : 10 (unit: 1/10s)
Last Member Query Count           : 2
General Query Suppression         : Disabled
Query Interval                    : 125
Query Response Interval           : 100 (unit: 1/10s)
Proxy Query Address               : 0.0.0.0
Proxy Reporting                   : Using global status (Disabled)
Multicast Router Discovery        : Disabled

VLAN Static Group    Port
---- --------------- --------
1    224.1.1.1       Eth 1/ 1
.
.
.
```

22.1.25 show ip igmp snooping group

本コマンドは、指定された VLAN インタフェース、または指定されていない場合はすべてのインタフェースのエントリ情報を表示します。

構文

show ip igmp snooping group [host-ip-addr [*ip-address* | *interface* [*ip-address*] | vlan *vlan-id* [*ip-address* | *interface* [*ip-address*]] | igmpsnp | sort-by-port [*ip-address* | *interface* [*ip-address*] | vlan *vlan-id* [*ip-address* | *interface* [*ip-address*]] | user | vlan *vlan-id* [user | igmpsnp]]

ip-address - マルチキャストグループの IP アドレスです

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

igmpsnp - IGMP snooping で学習したエントリだけを表示します。

sort-by-port - エントリをポート単位で並べ替えます。

user - ユーザが設定したマルチキャストエントリのみを表示します。

host-ip-addr - エントリの受信者情報を表示します。

vlan-id - VLAN ID です（1 から 4094）。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

選択されたオプションに応じて、エントリ情報を表示します。

例

VLAN 1 のエントリ情報を表示します。

```
Console#show ip igmp snooping group vlan 1
Bridge Multicast Forwarding Entry Count:1
Flag: R - Router port, M - Group member port
      H - Host counts (number of hosts join the group on this port).
      P - Port counts (number of ports join the group).
 Up time: Group elapsed time (d:h:m:s).
 Expire : Group remaining time (m:s).

VLAN Group           Port        Up time     Expire Count
---- --------------- ----------- ----------- ------ --------
   1 224.1.1.1                   00:00:00:37           2(P)
                     Eth 1/ 1(R)
                     Eth 1/ 2(M)                       0(H)
Console#
```

22.1.26 show ip igmp snooping mrouter

本コマンドは、IGMP snooping のマルチキャストルータポートの情報を表示します。

構文

show ip igmp snooping mrouter [vlan *vlan-id*]

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

デフォルト設定

すべての VLAN のマルチキャストルータポートを表示します。

コマンドモード

Privileged Exec

コマンドの使用方法

表示するマルチキャストルータポートには、静的および動的が含まれます。

例

VLAN 1 のマルチキャストルータポートを表示します。

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Port Type    Expire
 ---- ----------------- ------- --------
 1    Eth 1/4            Dynamic 0:4:28
 1    Eth 1/10           Static
Console#
```

22.1.27 show ip igmp snooping statistics

本コマンドは、IGMP snooping の統計情報を表示します。

構文

show ip igmp snooping statistics

{input [interface *interface*] |

output [interface *interface*] |

query [vlan *vlan-id*]}

input - IGMP snooping の入力に関する統計情報を表示します。

output - IGMP snooping の出力に関する統計情報を表示します。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan *vlan-id* - VLAN ID です。 (範囲: 1 から 4094)

query - IGMP Query メッセージに関する統計情報を表示します。

デフォルト設定

無し

コマンドモード

Privileged Exec

例

1/1 で受信した IGMP メッセージの統計情報を表示します。

```
Console#show ip igmp snooping statistics input interface ethernet 1/1
 Input Statistics:
 Interface Report   Leave    G Query  G(-S)-S Query Drop     Join Succ Group
 --------- -------- -------- -------- ------------- -------- --------- ------
 Eth 1/ 1        23       11        4            10        5        14      5
Console#
```

表 22-3 show ip igmp snooping statistics input - 表示の説明

フィールド	説明
Interface	インタフェースを表示します。
Report	このインタフェースで受信した IGMP Report メッセージの数です。
Leave	このインタフェースで受信した IGMP Leave メッセージの数です。
G Query	このインタフェースで受信した IGMP General Query メッセージの数です。
G(-S)-S Query	このインタフェースで受信した IGMP Group Specific Query メッセージまたは IGMP Group and Source Specific Query メッセージの数です。
Drop	IGMP Query/Report/Leave メッセージが廃棄された回数です。無効なフォーマット、レート制限、またはパケットコンテンツが許可されていないため、メッセージが廃棄される可能性があります。
Join Succ	正常にマルチキャストグループに加入した回数です。
Group	このインタフェースでアクティブなマルチキャストグループの数です。

次に、1/1 から送信した IGMP メッセージの統計情報を表示します。

```
Console#show ip igmp snooping statistics output interface ethernet 1/1
 Output Statistics:
 Interface  Report   Leave    G Query  G(-S)-S Query Drop     Group
 ---------- -------- -------- -------- ------------- -------- ------
 Eth 1/ 1        12        0        1             0        0      0
Console#
```

表 22-4 show ip igmp snooping statistics output - 表示の説明

フィールド	説明
Interface	インタフェースを表示します。
Report	このインタフェースから送信した IGMP Report メッセージの数です。
Leave	このインタフェースから送信した IGMP Leave メッセージの数です。
G Query	このインタフェースから送信した IGMP General Query メッセージの数です。
G(-S)-S Query	このインタフェースから送信した IGMP Group Specific Query メッセージまたは IGMP Group and Source Specific Query メッセージの数です。

フィールド	説明
Drop	IGMP Query/Report/Leave メッセージが廃棄された回数です。無効なフォーマット、レート制限、またはパケットコンテンツが許可されていないため、メッセージが廃棄される可能性があります。
Group	このインタフェースでアクティブなマルチキャストグループの数です。

次に、VLAN 1 の IGMP Query メッセージに関する統計情報を表示します。

```
Console#show ip igmp snooping statistics query vlan 1
 Other Querier             : None
 Other Querier Expire      : 0(m):0(s)
 Other Querier Uptime      : 0(h):0(m):0(s)
 Self Querier              : 192.168.2.12
 Self Querier Expire       : 0(m):0(s)
 Self Querier Uptime       : 0(h):0(m):0(s)
 General Query Received    : 0
 General Query Sent        : 0
 Specific Query Received   : 0
 Specific Query Sent       : 0
 Warn Rate Limit           : 0 sec.
 V1 Warning Count          : 0
 V2 Warning Count          : 0
 V3 Warning Count          : 0
Console#
```

表 22-5　show ip igmp snooping statistics vlan query - 表示の説明

フィールド	説明
Other Querier	このインタフェース上の他装置のクエリアの IP アドレスです。
Other Querier Expire	他装置のクエリアがタイムアウトするまでの時間です。
Other Querier Uptime	他装置のクエリアを検出してからの経過時間です。
Self Querier	本装置の IP アドレスです。
Self Querier Expire	本装置がクエリアの場合、IGMP General Query メッセージを送信するまでの残時間です。
Self Querier Uptime	本装置のクエリア機能が有効になってからの経過時間です。
General Query Received	このインタフェースで受信した IGMP General Query メッセージの数です。
General Query Sent	このインタフェースから送信した IGMP General Query メッセージの数です。
Specific Query Received	このインタフェースで受信した IGMP Group Specific Query メッセージの数です。
Specific Query Sent	このインタフェースから送信した IGMP Group Specific Query メッセージの数です。
Warn Rate Limit	誤ったバージョンの IGMP Query メッセージを受信した場合、「Vx Warning Count」に加算するときの基準となる秒数を表示します。表示している時間内であれば、当該 IGMP Query メッセージを複数受信したとしても、1 を加算します。したがって、秒数が「0 sec.」の場合、当該 IGMP Query メッセージの受信数だけ「Vx Warning Count」にカウントします。
V1 Warning Count	このインタフェースに設定したバージョンと一致しない、バージョン 1 の IGMP Query メッセージの数です。

フィールド	説明
V2 Warning Count	このインタフェースに設定したバージョンと一致しない、バージョン 2 の IGMP Query メッセージの数です。
V3 Warning Count	このインタフェースに設定したバージョンと一致しない、バージョン 3 の IGMP Query メッセージの数です。

22.2 IGMP フィルタリングおよびスロットリング

◆ 受信者が加入できるマルチキャストグループを制御する機能として、IGMP フィルタリングと IGMP スロットリングをサポートします。IGMP フィルタリングでは指定されたマルチキャストグループへの加入を制限し、IGMP スロットリングでは参加できるマルチキャストグループの加入数を制限します。IGMP フィルタリングおよび IGMP スロットリングはイーサネットまたはポートチャネルに設定します。IGMP フィルタリングと IGMP スロットリング処理は、動的に学習したエントリにのみ適用され、静的に設定したエントリには適用されません。IGMP スロットリング処理は無効することはできません。

表 22-6　IGMP フィルタリングおよび IGMP スロットリングコマンド

コマンド	機能	モード
ip igmp filter	IGMP フィルタリングを有効にします。	GC
ip igmp profile	プロファイル番号を設定し、IGMP フィルタプロファイルコンフィグレーションモードに移行します。	GC
permit, deny	プロファイルアクセスモードを permit(許可)または deny(拒否)に設定します。	IPC
range	プロファイルのマルチキャストアドレスを範囲指定します。	IPC
ip igmp filter	インタフェースに IGMP フィルタプロファイルを割当てます。	IC
ip igmp max-groups	インタフェースにマルチキャストグループの最大加入数を設定します。	IC
ip igmp max-groups action	インタフェースにマルチキャストグループの最大加入数を超過したときのアクションを設定します。	IC
ip igmp query-drop	受信した IGMP Query メッセージをすべて削除します。	IC
ip multicast-data-drop	すべての UDP マルチキャストパケットを廃棄します。	IC
show ip igmp filter	IGMP フィルタリングの情報を表示します。	PE
show ip igmp profile	IGMP プロファイルの情報を表示します。	PE
show ip igmp query-drop	IGMP Query メッセージの廃棄状態を表示します。	PE
show ip igmp throttle interface	インタフェースの IGMP スロットリング情報を表示します。	PE
show ip multicast-data-drop	マルチキャストパケット廃棄状態を表示します。	PE

22.2.1 ip igmp filter (Global Configuration)

本コマンドは、IGMP フィルタリングをグローバルに有効にします。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip igmp filter

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

◆ IGMP フィルタリングを使用すると、スイッチポートに許可または拒否されるマルチキャストグループを指定するプロファイルを割当てることができます。プロファイルには、1 つまたは複数のマルチキャストアドレスを設定することができます。 ポートに割当てられるプロファイルは 1 つだけです。有効にすると、ポートで受信した IGMP Report メッセージをプロファイルと照合します。IGMP Report メッセージで加入要求されたマルチキャストグループがプロファイルで許可されている場合、IGMP Report メッセージは通常どおり受信します。加入要求されたマルチキャストグループが拒否された場合、IGMP Report メッセージは破棄します。

例

IGMP フィルタリングをグローバルに有効にします。

```
Console(config)#ip igmp filter
Console(config)#
```

22.2.2 ip igmp profile

本コマンドは、IGMP フィルタプロファイル番号を作成し、IGMP プロファイルコンフィグレーションモードに移行します。プロファイル番号を削除するには、no 形式を使用してください。

構文

[no] ip igmp profile *profile-number*

profile-number - IGMP フィルタプロファイル番号です。(範囲: 1 から 60)

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

プロファイルは、受信者が加入を許可または拒否するマルチキャストグループを設定します。同じプロファイルを多くのインタフェースに適用できますが、1 つのインタフェースに割当てるプロファイルは 1 つだけです。各プロファイルには 1 つのアクセスモードしかありません。 許可または拒否のいずれかです。

例

IGMP フィルタプロファイルの 19 番を作成し IGMP プロファイルコンフィグレーションモードに移行します。

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

22.2.3 permit, deny

本コマンドは、IGMP フィルタプロファイルのアクセスモードを設定します。

構文

{permit | deny}

デフォルト設定

deny

コマンドモード

IGMP Profile Configuration

コマンドの使用方法

- ◆ 各プロファイルには 1 つのアクセスモードしかありません。 permit または deny のいずれかです。
- ◆ アクセスモードが permit に設定されている場合、マルチキャストグループが制御された範囲内に入ると、IGMP Report メッセージが処理されます。アクセスモードが deny に設定されている場合、IGMP Report メッセージは、設定された範囲外のマルチキャストグループの場合にのみ処理されます。

例

IGMP フィルタプロファイルの 19 番に permit を設定します。

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

22.2.4 range

本コマンドは、プロファイルのマルチキャストグループアドレスを範囲設定します。プロファイルからアドレスを削除するには、no 形式を使用してください。

構文

[no] range *low-ip-address high-ip-address*

low-ip-address - マルチキャストグループ範囲の開始となる IP アドレスです。

high-ip-address - マルチキャストグループ範囲の終了となる IP アドレスです。対象となるマルチキャストアドレスが 1 つの場合(範囲指定ではない場合)は、*low-ip-address* と同じ IP アドレスを設定してください。

デフォルト設定

無し

コマンドモード

IGMP プロファイルの設定

コマンドの使用方法

本コマンドを複数入力することで、複数のマルチキャストアドレス範囲を設定できます。

例

IGMP フィルタプロファイルの 19 番にマルチキャストアドレスを設定します。

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

22.2.5 ip igmp filter (Interface Configuration)

本コマンドは、IGMP フィルタリングプロファイルをスイッチのインタフェースに割当てます。インタフェースからプロファイルを削除するには、no 形式を使用してください。

構文

[no] ip igmp filter *profile-number*

profile-number - IGMP フィルタプロファイル番号です。(範囲: 1 から 60)

デフォルト設定

無し

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- IGMP フィルタリングプロファイルは、インタフェースに割当てる前に、ip igmp profile コマンドを使用して作成しておく必要があります。
- 1 つのインタフェースに割当てることができるプロファイルは 1 つだけです。
- プロファイルをトランクインタフェースに割当てることもできます。ポートがトランクメンバーとして設定されている場合、トランクはトランクの最初のポートメンバーに割当てられたフィルタリングプロファイルを使用します。

例

1/1 に IGMP フィルタプロファイルの 19 番を割り当てます。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

22.2.6 ip igmp max-groups

本コマンドは、インタフェースで同時に参加できるマルチキャストグループの最大数を設定します。デフォルト設定に戻すには、no 形式を使用してください。

構文

ip igmp max-groups *number*

no ip igmp max-groups

number - インタフェースで同時に参加できるマルチキャストグループの最大数です。(範囲: 1 から 511)

デフォルト設定

511

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- IGMP スロットリングは、ポートが同時に参加できるマルチキャストグループの最大数を設定します。1 つのポートで最大グループ数に達すると、スイッチは 2 つのアクションのいずれかをとることができます。(ip igmp max-group action コマンドを参照してください)。
- IGMP スロットリングは、トランクインタフェースでも設定できます。ポートがトランクメンバーとして設定されている場合、トランクはトランク内の最初のポートメンバーの IGMP スロットリング設定を使用します。
- マルチキャストグループの最大数は IGMP snooping と MLD snooping のエントリの合算値となります。

例

ポート 1/1 の最大加入数に 10 を設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

22.2.7 ip igmp max-groups action

本コマンドは、IGMP スロットリングで設定したマルチキャストグループの最大数を超過した場合の動作を指定します。

構文

ip igmp max-groups action {deny | replace}

no ip igmp max-groups action

deny - マルチキャストグループの最大数超過後に受信した IGMP Report メッセージを破棄します。

replace - マルチキャストグループの最大数超過後に受信した IGMP Report メッセージで、既存のエントリを置き換えます。

デフォルト設定

deny

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

1 つのポートで最大グループ数に達すると、deny または replace のいずれかのアクションを実行できます。アクションが deny に設定されている場合、超過後に受信した IGMP Report メッセージはすべて廃棄されます。アクションが replace に設定されている場合、既存のエントリをランダムに削除し、超過後に受信した IGMP Report メッセージのエントリを学習します。

例

ポート 1/1 の最大数超過時の動作に Replace を設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

22.2.8 ip igmp query-drop

本コマンドは、受信した IGMP Query メッセージをすべて廃棄します。デフォルト設定を復元するには、no 形式を使用してください。

構文

[no] ip igmp query-drop [vlan *vlan id*]

vlan id - IGMP クエリーパケットを廃棄する VLAN を指定します。

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

本コマンドを使用すると、指定したインタフェースで受信したすべての IGMP Query メッセージを廃棄します。本装置がクエリアとして動作している場合、別のクエリアから受信した IGMP Query メッセージの影響を受けません。

例

ポート 1/1 に IGMP Query メッセージを廃棄する設定をします。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

22.2.9 ip multicast-data-drop

本コマンドは、すべての UDP マルチキャストパケットを廃棄します。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip multicast-data-drop

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

本コマンドを使用することで、当該インタフェースで受信した UDP マルチキャストパケットを廃棄することができます。

例

ポート 1/1 に UDP マルチキャストパケットを廃棄する設定をします。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip multicast-data-drop
Console(config-if)#
```

22.2.10 show ip igmp filter

本コマンドは、IGMP フィルタリングのグローバル設定とインタフェース設定を表示します。

構文

show ip igmp filter [interface *interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Privileged Exec

例

IGMP フィルタリングの情報を表示します。

```
Console#show ip igmp filter
IGMP Filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
--------------------------------
 IGMP Profile 19
  Deny
  Range 239.1.1.1 239.1.1.1
  Range 239.2.3.1 239.2.3.100
Console#
```

22.2.11 show ip igmp profile

本コマンドは、IGMP フィルタリングプロファイルの情報を表示します。

構文

show ip igmp profile [*profile-number*]

profile-number - 既存の IGMP フィルタプロファイル番号です。

(範囲: 1 から 60)

デフォルト設定

無し

コマンドモード

Privileged Exec

例

IGMP フィルタリングプロファイルの情報を表示します。

```
Console#show ip igmp profile
  IGMP Profile 19
  Deny
```

```
  Range 239.1.1.1 239.1.1.1
  Range 239.2.3.1 239.2.3.100
  IGMP Profile 50
  Deny
Console#show ip igmp profile 19
  IGMP Profile 19
  Deny
  Range 239.1.1.1 239.1.1.1
  Range 239.2.3.1 239.2.3.100
Console#
```

22.2.12 show ip igmp query-drop

本コマンドは、インタフェースの IGMP Query メッセージの廃棄状態を表示します。

構文

show ip igmp query-drop [interface [*interface*]]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

インタフェースを指定せずに本コマンドを使用すると、すべてのインタフェースが表示されます。

例

ポート 1/1 の IGMP Query メッセージの廃棄状態を表示します。

```
Console#show ip igmp query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

22.2.13 show ip igmp throttle interface

本コマンドは、インタフェースに設定した IGMP スロットリングの情報を表示します。

構文

show ip igmp throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

インタフェースを指定せずに本コマンドを使用すると、すべてのインタフェースの情報が表示されます。

例

ポート 1/1 の IGMP スロットリングの情報を表示します。

```
Console#show ip igmp throttle interface ethernet 1/1
Eth  1/1 Information
                  Status : FALSE
                  Action : Deny
     Max Multicast Groups : 300
 Current Multicast Groups : 0

Console#
```

22.2.14 show ip multicast-data-drop

本コマンドは、インタフェースのマルチキャストパケットの廃棄状態を表示します。

構文

show ip multicast-data-drop [interface [*interface*]]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

インタフェースを指定せずに本コマンドを使用すると、すべてのインタフェースが表示されます。

例

ポート 1/1 のマルチキャストパケットの廃棄状態を表示します。

```
Console#show ip multicast-data-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

22.3 MLD snooping

MLD snooping は IPv6 トラフィックで動作し、IPv4 の IGMP snooping と同様の機能を実行します。つまり、MLD snooping では、マルチキャストグループを学習して IPv6 マルチキャストパケットを制限し、受信者が存在するポートにのみ転送します。これにより、指定した VLAN 内の IPv6 マルチキャストパケットのフラッディングを軽減します。

MLD には、バージョン 1 とバージョン 2 の 2 つのバージョンがあります。MLDv1 制御パケットには、MLD Query、MLD Report、および MLD Done メッセージ（IGMPv2 Query、IGMP Report、および IGMP Leave メッセージに相当）が含まれます。MLDv2 制御パケットには、MLDv2 Query および MLDv2 Report メッセージ、および MLDv1 Report および MLD Done メッセージが含まれます。

IGMP snooping と MLD snooping は独立した機能なので、同時に使用することができます。

表 22-7　MLD snooping コマンド

コマンド	機能	モード
ipv6 mld snooping	MLD snooping をグローバルに有効にします。	GC
ipv6 mld snooping proxy-reporting	プロキシ機能を有効にします。	GC
ipv6 mld snooping querier	本装置が MLD snooping のクエリアとして動作します。	GC
ipv6 mld snooping query-interval	MLD General Query メッセージの送信間隔を設定します。	GC
ipv6 mld snooping query-max-response-time	MLD General Query メッセージの最大応答時間を設定します。	GC
ipv6 mld snooping robustness	ロバストネス値を設定します。	GC
ipv6 mld snooping router-port-expire-time	Dynamic のマルチキャストルータポートの有効時間を設定します。	GC
ipv6 mld snooping unknown-multicast mode	未学習のマルチキャストパケットに対するアクションを設定します。	GC
ipv6 mld snooping unsolicited-report-interval	プロキシ機能が有効な場合に、上流に送信する MLD Report メッセージの送信間隔を設定します。	GC
ipv6 mld snooping version	MLD バージョンを設定します。	GC
ipv6 mld snooping vlan immediate-leave	MLD 即時離脱機能を設定します。	GC
ipv6 mld snooping vlan mrouter	マルチキャストルータポートを設定します。	GC
ipv6 mld snooping vlan static	static エントリを設定します。	GC
clear ipv6 mld snooping groups dynamic	Dynamic に学習したエントリを消去します。	PE
clear ipv6 mld snooping statistics	MLD snooping の統計情報を消去します。	PE
show ipv6 mld snooping	MLD snooping の設定を表示します。	PE
show ipv6 mld snooping group	学習したエントリの情報を表示します。	PE
show ipv6 mld snooping mrouter	マルチキャストルータポートの情報を表示します。	PE
show ipv6 mld snooping	MLD snooping の統計情報を表示します。	PE

コマンド	機能	モード
statistics		

22.3.1 ipv6 mld snooping

本コマンドは、MLD snooping をグローバルに有効にします。MLD snooping を無効にするには、no 形式を使用してください。

構文

[no] ipv6 mld snooping

デフォルト設定

無効

コマンドモード

Global Configuration

例

MLD snooping をグローバルで有効にします。

```
Console(config)#ipv6 mld snooping
Console(config)#
```

22.3.2 ipv6 mld snooping proxy-reporting

本コマンドは、MLD snooping のプロキシ機能を有効にします。デフォルト設定に戻すには、no 形式を使用してください。

構文

[no] ipv6 mld snooping proxy-reporting

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

◆ 本コマンドでプロキシ機能を有効にすると、受信者から受信した MLD Report メッセージを集計して、エントリを学習します。集計した MLD Report メッセージを要約して上流に送信する場合、当該 MLD Report メッセージの送信元アドレスにオールゼロを使用することがあります。このため、上流のスイッチは送信元アドレスがオールゼロの MLD Report メッセージを拒否しないようにしてください。

例

プロキシ機能をグローバルで有効にします。

```
Console(config)#ipv6 mld snooping proxy-reporting
Console(config)#
```

22.3.3 ipv6 mld snooping querier

本コマンドを使用すると、本装置は MLD クエリアとして動作します。この機能を無効にするには、no 形式を使用してください。

構文

[no] ipv6 mld snooping querier

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- ◆ クエリア機能を有効にした場合、本装置が代表クエリアに選出されればクエリアとして動作します。クエリアは、マルチキャストパケットを受信するかどうかを受信者に問い合わせます。
- ◆ クエリアを有効にする場合、VLAN インタフェースに IPv6 アドレスを設定する必要があります。設定した IPv6 アドレスを、クエリア機能で送信する MLD メッセージの送信元アドレスに使用します。
- ◆ ネットワーク上の IPv6 マルチキャストルータが検出された場合、クエリア機能は起動せず、起動後も自動的に無効になります。

例

クエリア機能をグローバルで有効にします。

```
Console(config)#ipv6 mld snooping querier
Console(config)#
```

22.3.4 ipv6 mld snooping query-interval

本コマンドは、MLD General Query メッセージの送信間隔を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ipv6 mld snooping query-interval *interval*

no ipv6 mld snooping query-interval

interval - MLD General Query メッセージの送信間隔です。(範囲: 60 から 125 秒)

デフォルト設定

125 秒

コマンドモード

Global Configuration

コマンドの使用方法

- 本コマンドは、本装置がクエリアとして動作している場合に適用されます。
- MLD General Query メッセージは、本コマンドで指定された間隔で送信されます。このメッセージを受信者が受信すると、すべての受信者は、加入しているマルチキャストグループの MLD Report メッセージを応答します。
- 「MLD General Query メッセージの送信間隔 > MLD General Query メッセージの最大応答時間」となるように設定してください。

例

MLD General Query メッセージの送信間隔に 150 秒を設定します。

```
Console(config)#ipv6 mld snooping query-interval 150
Console(config)#
```

関連コマンド

ipv6 mld snooping query-max-response-time

22.3.5 ipv6 mld snooping query-max-response-time

本コマンドは、本装置が送信する MLD General Query メッセージの最大応答時間を設定します。受信者が当該 MLD General Query メッセージを受信した場合、設定された最大応答時間内でランダムに MLD Report メッセージを応答します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ipv6 mld snooping query-max-response-time *seconds*

no ipv6 mld snooping query-max-response-time

seconds - 最大応答時間です。(範囲: 5 から 25 秒)

デフォルト設定

10 秒

コマンドモード

Global Configuration

コマンドの使用方法

- ◆ 本コマンドは、受信者が MLD General Query メッセージに応答する時間を制御します。
- ◆ 「MLD General Query メッセージの送信間隔 > MLD General Query メッセージの最大応答時間」となるように設定してください。

例

MLD General Query メッセージの最大応答時間に 20 秒を設定します。

```
Console(config)#ipv6 mld snooping query-max-response-time seconds 15
Console(config)#
```

関連コマンド

ipv6 mld snooping query-interval

22.3.6 ipv6 mld snooping robustness

本コマンドは、MLD snooping で使用するロバストネス値を設定します。デフォルト値を復元するには、no 形式を使用してください。

構文

ipv6 mld snooping robustness *value*

no ipv6 mld snooping robustness

value - ロバストネス変数の数です。(範囲: 2 から 10)

デフォルト設定

2

コマンドモード

Global Configuration

コマンドの使用方法

MLD General Query メッセージに多数の受信者が応答して、すべての MLD Report メッセージを受信できなかった場合、当該ポートがエントリから削除されて受信者へのマルチキャスト中継が停止する可能性があります。この場合、ロバストネス値を大きくすることで、エントリを保持する期間(MLD General Query メッセージの送信回数)を延長できるため、マルチキャスト中継停止の可能性を軽減できます。

例

ロバストネス値に 3 を設定します。

```
Console(config)#ipv6 mld snooping robustness 3
Console(config)#
```

22.3.7 ipv6 mld snooping router-port-expire-time

本コマンドは、Dynamic に設定したマルチキャストルータポートの有効時間を設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ipv6 mld snooping router-port-expire-time *time*

no ipv6 mld snooping router-port-expire-time

time - Dynamic に学習したマルチキャストルータポートの有効時間を設定します。(範囲: 300 から 500 秒)

デフォルト設定

300 秒

コマンドモード

Global Configuration

コマンドの使用方法

マルチキャストルータポートのタイムアウト時間は、本装置が他装置のクエリアが停止したと判定するまでの時間です。他装置から MLD Query メッセージを受信してから、本コマンドのタイムアウト時間内に MLD Query メッセージを受信しない場合、他装置のクエリアが停止したと判定します。

例

マルチキャストルータポートの有効時間に 300 秒を設定します。

```
Console(config)#ipv6 mld snooping router-port-expire-time 300
Console(config)#
```

22.3.8 ipv6 mld snooping unknown-multicast mode

本コマンドは、未学習のマルチキャストパケットを処理するためのアクションを設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ipv6 mld snooping unknown-multicast mode {flood | to-router-port}

no ipv6 mld snooping unknown-multicast mode

flood - 未学習のマルチキャストパケットをフラッディングします。

to-router-port - 未学習のマルチキャストパケットをマルチキャストルータポートに中継します。

デフォルト設定

to-router-port

コマンドモード

Global Configuration

コマンドの使用方法

- flood に設定した場合、未学習のマルチキャストパケットはフラッディングされるため、受信者が要求していないマルチキャストパケットも中継されます。
- to-router-port に設定した場合、未学習のマルチキャストパケットは、マルチキャストルータポートに中継されます。

例

未学習のマルチキャストパケットの処理をフラッディングにします。

```
Console(config)#ipv6 mld snooping unknown-multicast mode flood
Console(config)#
```

22.3.9 ipv6 mld snooping unsolicited-report-interval

本コマンドは、プロキシ機能が有効な場合に、本装置が上流に MLD Report メッセージを送信する間隔を設定します。デフォルト値を復元するには、no 形式を使用してください。

構文

ipv6 mld snooping unsolicited-report-interval *seconds*

no ipv6 mld snooping unsolicited-report-interval

seconds - MLD Report メッセージを送信する間隔です。(範囲: 1 から 65535 秒)

デフォルト設定

400 秒

コマンドモード

Global Configuration

コマンドの使用方法

- マルチキャストルータポートが追加されると、本装置は追加されたマルチキャストルータポートに対して、現在学習しているすべてのマルチキャストグループの MLD Report メッセージを送信します。
- 本コマンドは、プロキシ機能が有効な場合にのみ適用されます。

例

プロキシ機能有効時に送信する MLD Report メッセージの送信間隔を 50 秒を設定します。

```
Console(config)#ipv6 mld snooping unsolicited-report-interval 50
Console(config)#
```

22.3.10 ipv6 mld snooping version

本コマンドは、MLD バージョンを設定します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ipv6 mld snooping version {1 | 2}

no ipv6 mld snooping version

1 - MLD バージョン 1.

2 - MLD バージョン 2.

デフォルト設定

バージョン 2 :

コマンドモード

Global Configuration

例

MLD バージョンを 1 に設定します。

```
Console(config)#ipv6 mld snooping version 1
Console(config)#
```

22.3.11 ipv6 mld snooping vlan immediate-leave

本コマンドは、MLD 即時離脱機能を有効にします。MLD 即時離脱機能は MLD Done メッセージを受信した場合、当該受信ポートをマルチキャストグループから即座に削除します。デフォルトの状態に復元するには、no 形式を使用してください。

構文

ipv6 mld snooping vlan *vlan-id* immediate-leave [by-host-ip]

no ipv6 mld snooping vlan *vlan-id* immediate-leave

vlan-id - VLAN ID です。(範囲: 1 から 4094)

by-host-ip - 当該マルチキャストグループに加入している最後の受信者から MLD Done メッセージを受信した場合に、当該マルチキャストグループから受信ポートを削除します。

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- 本機能を使用しない場合、マルチキャストルータまたはクエリアは、MLD Done / MLDv2 Report(離脱要求)メッセージを受信すると、MLD Group Specific Query メッセージを送信します。マルチキャストルータまたはクエリアは、MLD Group Specific Query メッセージに対する受信者からの MLD Report メッセージの応答がない場合にのみ、当該ポートへのマルチキャストパケットの中継を停止します。
- 本機能を使用している場合、本装置は 1 台の受信者だけが当該ポートに接続されていると見なして削除処理を行います。したがって、同じマルチキャストグループに加入する複数の受信者が当該ポートに接続されている場合、1 台の受信者からの離脱要求で即座にエントリを削除するため、他の受信者へのマルチキャスト中継が停止します。

例

MLD 即時離脱機能を有効にします。

```
Console(config)#ipv6 mld snooping immediate-leave
Console(config)#
```

22.3.12 ipv6 mld snooping vlan mrouter

本コマンドは、マルチキャストルータポートを Static に設定します。設定を削除するには、no 形式を使用してください。

構文

[no] ipv6 mld snooping vlan *vlan-id* mrouter *interface*

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

Static のマルチキャストルータポートは設定されていません。

コマンドモード

Global Configuration

コマンドの使用方法

ネットワークによっては、MLD snooping が MLD クエリアを検出できないことがあります。この場合、本コマンドで既知のマルチキャストルータまたはスイッチを接続しているポートまたはチャネルグループを Static にマルチキャストルータポートに設定することができます。

例

1/1 を VLAN 1 の Static マルチキャストルータポートに設定します。

```
Console(config)#ipv6 mld snooping vlan 1 mrouter ethernet 1/1
Console(config)#
```

22.3.13 ipv6 mld snooping vlan static

本コマンドは、MLD snooping の学習エントリを Static に設定します。Static エントリを削除するには、no 形式を使用してください。

構文

[no] ipv6 mld snooping vlan *vlan-id* static *ipv6-address interface*

vlan - VLAN ID です。 (範囲: 1 から 4094)

ipv6-address - マルチキャストグループの IPv6 アドレスです。(書式: X:X:X:X::X)

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Global Configuration

例

vlan 1 の 1/6 にマルチキャストグループ(ff05:0:1:2:3:4:5:6)の Static エントリを設定します。

```
Console(config)#ipv6 mld snooping vlan 1 static ff05:0:1:2:3:4:5:6 ethernet 1/6
Console(config)#
```

22.3.14 clear ipv6 mld snooping groups dynamic

本コマンドは、MLD snooping によって Dynamic に学習したエントリ情報を消去します。

構文

clear ipv6 mld snooping groups dynamic

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドは、MLD snooping によって Dynamic に学習したエントリだけを消去します。Static に設定したエントリは消去しません。

例

Dynamic に学習したエントリを消去します。

```
Console#clear ipv6 mld snooping groups dynamic
Console#
```

22.3.15 clear ipv6 mld snooping statistics

本コマンドは、MLD snooping の統計情報を消去します。

構文

clear ipv6 mld snooping statistics [interface *interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

コマンドモード

Privileged Exec

例

MLD snooping の統計情報を消去します。

```
Console#clear ipv6 mld snooping statistics
Console#
```

22.3.16 show ipv6 mld snooping

本コマンドは、MLD snooping の設定値を表示します。

構文

show ipv6 mld snooping [vlan [*vlan-id*]]

vlan-id - VLAN ID です（1 から 4094）。

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドは、グローバルおよび VLAN インタフェースの MLD snooping の設定値を表示します。

例

MLD snooping の設定値を表示します。

```
Console#show ipv6 mld snooping
 Service Status              : Disabled
 Proxy Reporting             : Disabled
 Querier Status              : Disabled
 Robustness                  : 2
 Query Interval              : 125 sec
 Query Max Response Time     : 10 sec
 Router Port Expiry Time     : 300 sec
 Unsolicit Report Interval   : 400 sec
 Immediate Leave             : Disabled on all VLAN
 Immediate Leave By Host     : Disabled on all VLAN
 Unknown Flood Behavior      : To Router Port
 MLD Snooping Version        : Version 2

VLAN Group IPv6 Address                     Port
---- ------------------------------------ ---------
   1                     ff05:0:1:2:3:4:5:6 Eth 1/1

Console#show ipv6 mld snooping vlan
VLAN 1
 Immediate Leave        : Disabled
 Unknown Flood Behavior : To Router Port
Console#
```

22.3.17 show ipv6 mld snooping group

本コマンドは、MLD snooping のエントリ情報を表示します。

構文

show ipv6 mld snooping group [*ip-address* | host-ip-addr [*interface*] | sort-by-port [*interface*] | source-list {*ip-address* | vlan *vlan-id*] | vlan *vlan-id*]

ip-address - マルチキャストグループの IP アドレスです

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

sort-by-port - エントリをポート単位で並べ替えます。

host-ip-addr - エントリの受信者情報を表示します。

source-list - エントリの送信元情報を表示します。

vlan-id - VLAN ID です（1 から 4094）。

コマンドモード

Privileged Exec

例

MLD snooping のエントリ情報を表示します。

```
Console#show ipv6 mld snooping group

Total Entries 3, limit 255

VLAN Multicast IPv6 Address                  Member Port Type
---- --------------------------------------- ----------- ---------------
   1                      FF02::01:01:01:01 Eth 1/1     MLD Snooping
   1                      FF02::01:01:01:02 Eth 1/1     Multicast Data
   1                      FF02::01:01:01:02 Eth 1/1     User

Console#
```

次に、host-ip-addr パラメータを指定してエントリ情報を表示します。

```
Console#show ipv6 mld snooping group host-ip-addr ethernet 1/10
Port      VLAN Group
               Host
--------- ---- ---------------------------------------
Eth 1/10  1    ff02::fb
               fe80::f0a3:ea46:d9f2:90d5
Eth 1/10  1    ff02::1:fff2:90d5
               fe80::f0a3:ea46:d9f2:90d5
Eth 1/10  1    ff12::1:3

Console#
```

次に、sort-by-port パラメータを指定してエントリ情報を表示します。

```
Console#show ipv6 mld snooping group sort-by-port ethernet 1/10
Expire: H:M:S; Uptime: H:M:S; T: Dynamic/Static; Q: Unreply query
Port      VLAN Group                                   Expire Uptime     T Q
--------- ---- --------------------------------------- ------ ---------- - --
Eth 1/10  1    ff02::fb                                2:28   0:1:59     D  0
Eth 1/10  1    ff02::1:fff2:90d5                       2:20   0:1:59     D  0
Eth 1/10  1    ff12::1:3                               2:23   0:1:56     D  0
Eth 1/10  1    ff17::101                               2:22   0:1:57     D  0
Eth 1/10  2    ff12::1:3                               2:54   0:1:25     D  0
Eth 1/10  2    ff17::101                               2:53   0:1:26     D  0

Console#
```

次に、vlan パラメータを指定してエントリ情報を表示します。

```
Console#show ipv6 mld snooping group vlan 2
VLAN Multicast IPv6 Address                  Member Port     Type
---- --------------------------------------- -------------- ---------------
   2                              ff12::1:3 Eth 1/10(M)     MLD Snooping
   2                              ff17::101 Eth 1/10(M)     MLD Snooping

Console#
```

次に、source-list パラメータを指定してエントリ情報を表示します。

```
onsole#show ipv6 mld snooping group source-list
VLAN ID                    : 1
Mutlicast IPv6 Address     : FF02::01:01:01:01
Member Port                : Eth 1/1
MLD Snooping               : Multicast Data
Filter Mode                : Include
(if exclude filter mode)
Filter Timer Elapse        : 10 sec.
Request List               : ::01:02:03:04, ::01:02:03:05, ::01:02:03:06,
                             ::01:02:03:07
Exclude List               : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                             ::02:02:03:07
```

```
(if include filter mode)
Include List                : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                              ::02:02:03:06
Option:
 Filter Mode: Include, Exclude

Console#
```

22.3.18 show ipv6 mld snooping mrouter

本コマンドは、MLD snooping のマルチキャストルータポートの情報を表示します。

構文

show ipv6 mld snooping mrouter vlan *vlan-id*

vlan-id - VLAN ID です。(範囲: 1 から 4094)

コマンドモード

Privileged Exec

例

VLAN 1 のマルチキャストルータポートを表示します。

```
Console#show ipv6 mld snooping mrouter vlan 1
 VLAN Multicast Router Port Type      Expire
 ---- --------------------- --------- ------
    1 Eth 1/ 2              Static
Console#
```

22.3.19 show ipv6 mld snooping statistics

本コマンドは、MLD snooping の統計情報を表示します。

構文

show ipv6 mld snooping statistics

{input [interface *interface*] |

output [interface *interface*] |

query [vlan [*vlan-id*]] |

summary interface *interface*}

input - MLD snooping の入力に関する統計情報を表示します。

output - MLD snooping の出力に関する統計情報を表示します。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

vlan *vlan-id* - VLAN ID です。 (範囲: 1 から 4094)

query - MLD Query メッセージに関する統計情報を表示します。

summary - MLD snooping の統計情報の summary を表示します。

デフォルト設定

無し

コマンドモード

Privileged Exec

例

MLD snooping の入力に関する統計情報を表示します。

```
Console#show ipv6 mld snooping statistics input interface ethernet 1/1
 Input Statistics:
 Interface Report   Leave    G Query  G(-S)-S Query Drop     Join Succ Group
 --------- -------- -------- -------- ------------- -------- --------- ------
 Eth 1/ 1         4        0        0             0        0         0      2
Console#
```

表 22-8 show ipv6 mld snooping statistics input - 表示の説明

フィールド	説明
Interface	インタフェースを表示します。
Report	このインタフェースで受信した MLD Report メッセージの数です。
Leave	このインタフェースで受信した MLD Done メッセージの数です。
G Query	このインタフェースで受信した MLD General Query メッセージの数です。
G(-S)-S Query	このインタフェースで受信した MLD Group Specific Query メッセージまたは MLD Group and Source Specific Query メッセージの数です。
Drop	MLD Query/Report/Done メッセージが廃棄された回数です。無効なフォーマット、レート制限、またはパケットコンテンツが許可されていないため、メッセージが廃棄される可能性があります。
Join Succ	正常にマルチキャストグループに加入した回数です。
Group	このインタフェースでアクティブなマルチキャストグループの数です。

次に、1/1 から送信した MLD メッセージの統計情報を表示します。

```
Console#show ipv6 mld snooping statistics output interface ethernet 1/1
 Output Statistics:
 Interface Report   Leave    G Query  G(-S)-S Query Drop     Group
 --------- -------- -------- -------- ------------- -------- ------
```

```
 Eth 1/ 1          0         0         5                 0         0       2

Console#
```

表 22-9 show ipv6 mld snooping statistics output - 表示の説明

フィールド	説明
Interface	インタフェースを表示します。
Report	このインタフェースから送信した MLD Report メッセージの数です。
Leave	このインタフェースから送信した MLD Done メッセージの数です。
G Query	このインタフェースから送信した MLD General Query メッセージの数です。
G(-S)-S Query	このインタフェースから送信した MLD Group Specific Query メッセージまたは MLD Group and Source Specific Query メッセージの数です。
Drop	MLD Query/Report/Done メッセージが廃棄された回数です。無効なフォーマット、レート制限、またはパケットコンテンツが許可されていないため、メッセージが廃棄される可能性があります。
Group	このインタフェースでアクティブなマルチキャストグループの数です。

次に、VLAN 1 の MLD Query メッセージに関する統計情報を表示します。

```
Console#show ipv6 mld snooping statistics query vlan 1
 Other Querier Address     : 無し
 Other Querier Expire      : 0(m):0(s)
 Other Querier Uptime      : 0(h):0(m):0(s)
 Self Querier Address      : ::
 Self Querier Expire Time  : 1(m):49(s)
 Self Querier UpTime       : 0(h):9(m):6(s)
 General Query Received    : 0
 General Query Sent        : 6
 Specific Query Received   : 0
 Specific Query Sent       : 0
Console#
```

表 22-10 show ipv6 mld snooping statistics query - 表示の説明

フィールド	説明
Other Querier Address	このインタフェース上の他装置のクエリアの IP アドレスです。
Other Querier Expire	他装置のクエリアがタイムアウトするまでの時間です。
Other Querier Uptime	他装置のクエリアを検出してからの経過時間です。
Self Querier	本装置の IP アドレスです。
Self Querier Expire	本装置がクエリアの場合、MLD General Query メッセージを送信するまでの残時間です。
Self Querier Uptime	本装置のクエリア機能が有効になってからの経過時間です。
General Query Received	このインタフェースで受信した MLD General Query メッセージの数です。
General Query Sent	このインタフェースから送信した MLD General Query メッセージの数です。
Specific Query Received	このインタフェースで受信した MLD Group Specific Query メッセージの数です。

フィールド	説明
Specific Query Sent	このインタフェースから送信した MLD Group Specific Query メッセージの数です。

次に、MLD snooping の統計情報の summary を表示します。

```
Console#show ipv6 mld snooping statistics summary interface e 1/1
Number of Groups:  1
 Querier:         :                    Report & Leave:    :
  Transmit        :                     Transmit          :
   General        : 6                    Report          : 0
   Group Specific: 0                     Leave           : 0
  Recieved        :                     Recieved          :
   General        : 0                    Report          : 4
   Group Specific: 0                     Leave           : 0
                                         join Success    : 0
                                         Filter Drop     : 0
                                         Source Port Drop: 0
                                         Others Drop     : 0
Console#show ipv6 mld snooping statistics summary interface vlan 1
Number of Groups:  1
 Querier:         :                    Report & Leave:    :
  Other Querier   : None
                                         Host Addr         : None
  Other Uptime    : 0(h):0(m):0(s)       Unsolicit Expire : 0 sec
  Other Expire    : 0(m):0(s)
  Self Addr       : None
  Self Expire     :  2(m): 3(s)
  Self Uptime     : 0(h):10(m):58(s)
  Transmit        :                     Transmit          :
   General        : 7                    Report          : 0
   Group Specific: 0                     Leave           : 0
  Recieved        :                     Recieved          :
   General        : 0                    Report          : 4
   Group Specific: 0                     Leave           : 0
                                         join Success    : 0
                                         Filter Drop     : 0
                                         Source Port Drop: 0
                                         Others Drop     : 0
Console#
```

表 22-11　show ipv6 mld snooping statistics summary - 表示の説明

フィールド	説明
Number of Groups	指定されたインタフェース上でアクティブなマルチキャストグループの数です。
Physical Interface (Port/Trunk)	
Querier:	
Transmit	

フィールド	説明
General	このインタフェースから送信した MLD General Query メッセージの数です。
Group Specific	このインタフェースから送信した MLD Group Specific Query メッセージの数です。
Recieved	
General	このインタフェースで受信した MLD General Query メッセージの数です。
Group Specific	このインタフェースで受信した MLD Group Specific Query メッセージの数です。
Report & Leave	
Transmit	
Report	このインタフェースから送信した MLD Report メッセージの数です。
Leave	このインタフェースから送信した MLD Done メッセージの数です。
Recieved	
Report	このインタフェースで受信した MLD Report メッセージの数です。
Leave	このインタフェースで受信した MLD Done メッセージの数です。
join Success	正常にマルチキャストグループに加入した回数です。
Filter Drop	MLD フィルタリングによって廃棄された MLD Report メッセージの数です。
Source Port Drop	マルチキャストルータポートで廃棄された MLD メッセージの数です。
Others Drop	受信した無効な MLD メッセージの数です。
Logical Interface (VLAN)	VLAN インタフェースには、次の追加パラメータが含まれています。
Querier:	
Other Querier	このインタフェース上の他装置のクエリアの IP アドレスです。
Other Uptime	他装置のクエリアがタイムアウトするまでの時間です。
Other Expire	他装置のクエリアを検出してからの経過時間です。
Self Addr	本装置の IP アドレスです。
Self Expire	本装置がクエリアの場合、MLD General Query メッセージを送信するまでの残時間です。
Self Uptime	本装置のクエリア機能が有効になってからの経過時間です。
Report & Leave	
Host Addr	その VLAN に割当てられているリンクローカルまたはグローバル IPv6 アドレスです。
Unsolicit Expire	プロキシ機能有効時、本装置が MLD Report メッセージを送信するまでの残時間です。

22.4 MLD フィルタリングおよびスロットリング

受信者が加入できるマルチキャストグループを制御する機能として、MLD フィルタリングと MLD スロットリングをサポートします。MLD フィルタリングでは指定されたマルチキャストグループへの加入を制限し、MLD スロットリングでは参加できるマルチキャストグループの加入数を制限します。MLD フィルタリングおよび MLD スロットリングはイーサネットまたはポートチャネルに設定します。MLD フィルタリングと MLD スロットリング処理は、動的に学習したエントリにのみ適用され、静的に設定したエントリには適用されません。MLD スロットリング処理は無効することはできません。

表 22-12　MLD フィルタリングおよび MLD スロットリングコマンド

コマンド	機能	モード
ipv6 mld filter	MLD フィルタリングを有効にします。	GC
ipv6 mld profile	プロファイル番号を設定し、MLD フィルタプロファイルコンフィグレーションモードに移行します。	GC
permit, deny	プロファイルアクセスモードを permit(許可)または deny(拒否)に設定します。	IPC
range	プロファイルのマルチキャストアドレスを範囲指定します。	IPC
ipv6 mld filter	インタフェースに MLD フィルタプロファイルを割当てます。	IC
ipv6 mld max-groups	インタフェースにマルチキャストグループの最大加入数を設定します。	IC
ipv6 mld max-groups action	インタフェースにマルチキャストグループの最大加入数を超過したときのアクションを設定します。	IC
ipv6 mld query-drop	受信した MLD Query メッセージをすべて削除します。	IC
show ipv6 mld filter	MLD フィルタリングの情報を表示します。	PE
show ipv6 mld profile	MLD プロファイルの情報を表示します。	PE
show ipv6 mld query-drop	MLD Query メッセージの廃棄状態を表示します。	PE
show ipv6 mld throttle interface	インタフェースの MLD スロットリング情報を表示します。	PE

22.4.1 ipv6 mld filter (Global Configuration)

本コマンドは、MLD フィルタリングをグローバルに有効にします。この機能を無効にするには、no 形式を使用してください。

構文

[no] ipv6 mld filter

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

◆ MLD フィルタリングを使用すると、スイッチポートに許可または拒否されるマルチキャストグループを指定するプロファイルを割当てることができます。プロファイルには、1 つまたは複数のマルチキャストアドレスを設定することができます。 ポートに割当てられるプロファイルは 1 つだけです。有効にすると、ポートで受信した MLD Report メッセージをプロファイルと照合します。MLD Report メッセージで加入要求されたマルチキャストグループがプロファイルで許可されている場合、MLD Report メッセージは通常どおり受信します。加入要求されたマルチキャストグループが拒否された場合、MLD Report メッセージは破棄します。

例

MLD フィルタリングをグローバルに有効にします。

```
Console(config)#ipv6 mld filter
Console(config)#
```

関連コマンド

show ipv6 mld filter

22.4.2 ipv6 mld profile

本コマンドは、MLD フィルタプロファイル番号を作成し、MLD プロファイルコンフィグレーションモードに移行します。プロファイル番号を削除するには、no 形式を使用してください。

構文

[no] ipv6 mld profile *profile-number*

profile-number - MLD フィルタプロファイル番号です。(範囲: 1 から 40)

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

プロファイルは、受信者が加入を許可または拒否するマルチキャストグループを設定します。同じプロファイルを多くのインタフェースに適用できますが、1 つのインタフェースに割当てるプロファイルは 1 つだけです。各プロファイルには 1 つのアクセスモードしかありません。 許可または拒否のいずれかです。

例

MLD フィルタプロファイルの 19 番を作成し MLD プロファイルコンフィグレーションモードに移行します。

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#
```

関連コマンド

show ipv6 mld profile

22.4.3 permit, deny

本コマンドは、MLD フィルタプロファイルのアクセスモードを設定します。

構文

{permit | deny}

デフォルト設定

deny

コマンドモード

MLD Profile Configuration

コマンドの使用方法

- ◆ 各プロファイルには 1 つのアクセスモードしかありません。 permit または deny のいずれかです。
- ◆ アクセスモードが permit に設定されている場合、マルチキャストグループが制御された範囲内に入ると、MLD Report メッセージが処理されます。アクセスモードが拒否に設定されている場合、MLD Report メッセージは、設定された範囲外のマルチキャストグループの場合にのみ処理されます。

例

MLD フィルタプロファイルの 19 番に permit を設定します。

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#permit
Console(config-mld-profile)#
```

22.4.4 range

本コマンドは、プロファイルのマルチキャストグループアドレスを範囲設定します。プロファイルからアドレスを削除するには、no 形式を使用してください。

構文

[no] range *low-ipv6-address high-ipv6-address*

low-ipv6-address - マルチキャストグループ範囲の開始となる IP アドレスです。

high-ipv6-address - マルチキャストグループ範囲の終了となる IP アドレスです。対象となるマルチキャストアドレスが 1 つの場合(範囲指定ではない場合)は、*low-ip-address* と同じ IP アドレスを設定してください。

デフォルト設定

無し

コマンドモード

MLD Profile Configuration

コマンドの使用方法

本コマンドを複数入力することで、複数のマルチキャストアドレス範囲を設定できます。

例

MLD フィルタプロファイルの 19 番にマルチキャストアドレスを設定します。

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#range ff01::0101 ff01::0202
Console(config-mld-profile)#
```

22.4.5 ipv6 mld filter (Interface Configuration)

本コマンドは、MLD フィルタリングプロファイルをスイッチのインタフェースに割当てます。インタフェースからプロファイルを削除するには、no 形式を使用してください。

構文

[no] ipv6 mld filter *profile-number*

profile-number - MLD フィルタプロファイル番号です。(範囲: 1 から 40)

デフォルト設定

無し

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- MLD フィルタリングプロファイルは、インタフェースに割当てる前に、ipv6 mld profile コマンドを使用して作成しておく必要があります。
- 1 つのインタフェースに割当てることができるプロファイルは 1 つだけです。
- プロファイルをトランクインタフェースに割当てることもできます。ポートがトランクメンバーとして設定されている場合、トランクはトランクの最初のポートメンバーに割当てられたフィルタリングプロファイルを使用します。

例

ポート 1/1 に MLD フィルタプロファイルの 19 番を割り当てます。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld filter 19
Console(config-if)#
```

22.4.6 ipv6 mld max-groups

本コマンドは、インタフェースで同時に参加できるマルチキャストグループの最大数を設定します。デフォルト設定に戻すには、no 形式を使用してください。

構文

ipv6 mld max-groups *number*

no ipv6 mld max-groups

number - インタフェースで同時に参加できるマルチキャストグループの最大数です。(範囲: 1 から 255)

デフォルト設定

255

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- MLD スロットリングは、ポートが同時に参加できるマルチキャストグループの最大数を設定します。1 つのポートで最大グループ数に達すると、スイッチは 2 つのアクションのいずれかをとることができます。(ipv6 mld max-group action コマンドを参照してください)。
- MLD スロットリングはトランクインタフェースで設定できます。ポートがトランクメンバーとして設定されている場合、トランクはトランク内の最初のポートメンバーの MLD スロットリング設定を使用します。
- マルチキャストグループの最大数がデフォルト値に設定されている場合、MLD スロットリングの実行ステータスは FALSE で表示されます。つまり、最大数をデフォルト値以外に設定されるまで、MLD スロットリングの設定は無効になります。
- マルチキャストグループの最大数は IGMP snooping と MLD snooping のエントリの合算値が 511 になるように設定してください。

例

ポート 1/1 の最大加入数に 10 を設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups 10
Console(config-if)#
```

22.4.7 ipv6 mld max-groups action

本コマンドは、MLD スロットリングで設定したマルチキャストグループの最大数を超過した場合の動作を指定します。 デフォルト設定を戻すには、no 形式を使用してください。

構文

ipv6 mld max-groups action {deny | replace}

no ipv6 mld max-groups action

deny - マルチキャストグループの最大数超過後に受信した MLD Report メッセージを破棄します。

replace - マルチキャストグループの最大数超過後に受信した MLD Report メッセージで、既存のエントリを置き換えます。

デフォルト設定

deny

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

1 つのポートで最大グループ数に達すると、deny または replace のいずれかのアクションを実行できます。アクションが deny に設定されている場合、超過後に受信した MLD Report メッセージはすべて廃棄されます。アクションが replace に設定されている場合、既存のエントリをランダムに削除し、超過後に受信した MLD Report メッセージのエントリを学習します。

例

ポート 1/1 の最大数超過時の動作に Replace を設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups action replace
Console(config-if)#
```

22.4.8 ipv6 mld query-drop

本コマンドは、受信した MLD Query メッセージをすべて破棄します。デフォルト設定を復元するには、no 形式を使用してください。

構文

[no] ipv6 mld query-drop

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

本コマンドを使用すると、指定したインタフェースで受信したすべての MLD Query メッセージを廃棄します。本装置がクエリアとして動作している場合、別のクエリアから受信した MLD Query メッセージの影響を受けません。

例

ポート 1/1 に MLD Query メッセージを廃棄する設定をします。

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld query-drop
Console(config-if)#
```

22.4.9 show ipv6 mld filter

本コマンドは、MLD フィルタリングのグローバル設定とインタフェース設定を表示します。

構文

show ipv6 mld filter [interface *interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Privileged Exec

例

MLD フィルタリングの情報を表示します。

```
Console#show ipv6 mld filter
 MLD filter Enabled
Console#show ipv6 mld filter interface ethernet 1/3
Ethernet 1/3 information
--------------------------------
 MLD  Profile 19
 Deny
```

```
 Range  ff01::101          ff01::faa
Console#
```

22.4.10 show ipv6 mld profile

本コマンドは、MLD フィルタリングプロファイルの情報を表示します。

構文

show ipv6 mld profile [*profile-number*]

profile-number - 既存の MLD フィルタプロファイル番号です。

(範囲: 1 から 40)

デフォルト設定

無し

コマンドモード

Privileged Exec

例

MLD フィルタリングプロファイルの情報を表示します。

```
Console#show ipv6 mld profile
 MLD Profile 19
 MLD Profile 40
Console#show ipv6 mld profile 19
 MLD  Profile 19
 Deny
 Range  ff01::101          ff01::faa
Console#
```

22.4.11 show ipv6 mld query-drop

本コマンドは、インタフェースの MLD Query メッセージの廃棄状態を表示します。

構文

show ipv6 mld query-drop interface [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

インタフェースを指定せずに本コマンドを使用すると、すべてのインタフェースが表示されます。

例

ポート 1/1 の MLD Query メッセージの廃棄状態を表示します。

```
Console#show ipv6 mld query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

22.4.12 show ipv6 mld throttle interface

本コマンドは、インタフェースに設定した MLD スロットリングの情報を表示します。

構文

show ipv6 mld throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

インタフェースを指定せずに本コマンドを使用すると、すべてのインタフェースの情報が表示されます。

例

ポート 1/1 の MLD スロットリングの情報を表示します。

```
Console#show ipv6 mld throttle interface ethernet 1/3
```

```
Eth  1/3 Information
 Status                   : TRUE
 Action                   : Replace
 Max Multicast Groups     : 10
 Current Multicast Groups : 0

Console#
```

23 LLDP コマンド

LLDP(Link Layer Discovery Protocol)は、ローカルブロードキャストドメイン上の隣接デバイスに関する基本情報を検出するために使用されます。LLDP は、定期的なブロードキャストを使用して送信デバイスに関する情報を広告するレイヤ 2 プロトコルです。広告された情報は、IEEE 802.1AB 規格に準拠した TLV(Type Length Value)形式で表示され、デバイスの識別、機能、および設定などの詳細を含めることができます。LLDP では、検出された隣接ネットワークノードについて収集された情報を保存および維持する方法も定義します。

表 23-1 LLDP コマンド

コマンド	機能	モード
lldp	スイッチで LLDP をグローバルに有効にします	GC
lldp holdtime-multiplier	LLDP 広告に送信される、time-to-live (TTL)値を設定します。	GC
lldp med-fast-start-count	medFastStart パケットを送信する数を設定します。	GC
lldp notification-interval	LLDP の変更に関する SNMP 通知を送信するための定期間隔の時間を設定します。	GC
lldp refresh-interval	LLDP 広告の定期送信間隔の時間を設定します。	GC
lldp reinit-delay	LLDP ポートが無効になったとき、またはポートがリンクがダウンしたときに再初期化を試みる際の待ち合わせ時間を設定します。	GC
lldp tx-delay	ローカル LLDP MIB 変数の変更によっておこなわれる、広告の連続送信の遅延時間を設定します。	GC
lldp admin-status	特定ポートで、LLDP PDU(Protocol Data Unit)を送信のみ、受信のみ、または送受信のモードを有効にします。	IC
lldp basic-tlv management-ip-address	デバイスの Management Address（管理アドレス）を広告するかどうかを設定します。	IC
lldp basic-tlv port-description	Port Description（ポートの説明）を広告するかどうかを設定します。	IC
lldp basic-tlv system-capabilities	System Capabilities（システム機能）を広告するかどうかを設定します。	IC
lldp basic-tlv system-description	System Description（システム説明）を広告するかどうかを設定します。	IC
lldp basic-tlv system-name	System Name（システム名）を広告するかどうかを設定します。	IC
lldp dot1-tlv proto-ident※	Protocol Identity（サポートされているプロトコル）を広告するかどうかを設定します。	IC
lldp dot1-tlv proto-vid※	Port Protocol VLAN ID（ポートベースのプロトコル VLAN 情報）を広告するかどうかを設定します。	IC
lldp dot1-tlv pvid※	Port VLAN ID（デフォルト VLAN ID）を広告するかどうかを設定します。	IC

コマンド	機能	モード
lldp dot1-tlv vlan-name※	VLAN Name（VLAN 名称）を広告するかどうかを設定します。	IC
lldp dot3-tlv link-agg	Link Aggregation（リンクアグリゲーション機能）を広告するかどうかを設定します。	IC
lldp dot3-tlv max-frame	Maximum Frame Size（最大フレームサイズ）を広告するかどうかを設定します。	IC
lldp dot3-tlv poe	Power-over-Ethernet(PoE)機能を広告するかどうかを設定します。	IC
lldp med-notification	LLDP-MED 変更に関する SNMP トラップ通知の送信を有効にします。	IC
lldp med-tlv ext-poe	LLDP Media Endpoint Discovery（LLDP-MED）有効化ポートを拡張 Power-over-Ethernet 設定と使用状況を通知して受け入れるように設定します。	IC
lldp med-tlv inventory	LLDP-MED 対応ポートがインベントリ識別情報を通知するように設定します。	IC
lldp med-tlv location	LLDP-MED 対応ポートがロケーション識別の詳細を通知するように設定します。	IC
lldp med-tlv med-cap	LLDP-MED 対応ポートが Media Endpoint Device 機能を通知するように設定します。	IC
lldp med-tlv network-policy	LLDP-MED 対応ポートがネットワークポリシー設定を通知するように設定します。	IC
lldp notification	LLDP 変更に関する SNMP トラップ通知の送信を有効にします。	IC
show lldp config	全ポートの LLDP コンフィグレーションを示します。	PE
show lldp info local-device	デバイスの LLDP グローバル、およびインタフェース特有のコンフィグレーションを示します。	PE
show lldp info remote-device	リモートデバイスの LLDP グローバル、およびインタフェース特有コンフィグレーションを示します。	PE
show lldp info statistics	すべての LLDP 対応インタフェースの統計カウンタを表示します。	PE

注※ ベンダー固有のオプションは、近隣のデバイスによってアドバタイズされる場合と、されない場合があります。

23.1 コマンド説明

23.1.1 lldp

本コマンドでは、スイッチ上で LLDP をグローバルに有効にします。LLDP を無効にするには、no 形式を使用してください。

構文

[no] lldp

デフォルト設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#lldp
Console(config)#
```

23.1.2 lldp holdtime-multiplier

本コマンドでは、LLDP 広告に送信した time-to-live (TTL)値を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

value - 以下のルールに従って TTL を秒で計算します。

((送信間隔 * ホールドタイム乗数)、または 65536)の最小値

(範囲: 2 から 10)

デフォルト設定

ホールドタイム乗数: 4

TTL: 4*30 = 120 秒

コマンドモード

Global Configuration

コマンドの使用方法

TTL は、受信側の LLDP エージェントに対して、送信側の LLDP エージェントが適時に更新を送信しない

場合に、受信側の LLDP エージェントが送信側の LLDP エージェントに関するすべての情報をどのくらい保持するかの保持時間を示します。

例

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

23.1.3 lldp med-fast-start-count

本コマンドでは、LLDP-MED Fast Start メカニズムが動作している期間に送信する MED Fast Start LLDPDU の数を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

lldp med-fast-start-count *packet-number*

no lldp med-fast-start-count

packet-number - パケット数です。(範囲: 1 から 10 パケット)

デフォルト設定

4 パケット

コマンドモード

Global Configuration

コマンドの使用方法

このパラメータは、LLDP-MED Fast Start メカニズムがポートで有効であることを保障するタイマーの一部です。LLDP-MED Fast Start は LLDP の素早い通知に重要であるため、Emergency Call Service の高可用に必要です。

例

```
Console(config)#lldp med-fast-start-count 6
Console(config)#
```

23.1.4 lldp notification-interval

本コマンドでは、LLDP 変更に関する SNMP 通知の送信のための定期間隔の時間を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

lldp notification-interval *seconds*

no lldp notification-interval

seconds - SNMP 通知が送信される定期間隔を特定します。(範囲: 5 から 3600 秒)

デフォルト設定

5 秒

コマンドモード

Global Configuration

コマンドの使用方法

- このパラメータは、ネットワーク監視または管理のために LLDP MIB に格納されたデータを使用する SNMP アプリケーションにのみ適用されます。
- SNMP 通知の間に発生した LLDP 隣接の変更に関する情報は送信されません。通知時に存在した状態変更のみが送信に含まれます。したがって SNMP エージェントは、lldpStatsRemTableLastChangeTime の値を定期的にチェックして、伝送損失などのために lldpRemTablesChange 通知イベントが検知されなかったことを検出する必要があります。

例

```
Console(config)#lldp notification-interval 30
Console(config)#
```

23.1.5 lldp refresh-interval

本コマンドでは、LLDP 広告の定期送信間隔の時間を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

lldp refresh-interval *seconds*

no lldp refresh-delay

seconds -LLDP 通知が送信される、定期間隔を指定します。(範囲: 5 から 32768 秒)

デフォルト設定

30 seconds

コマンドモード

Global Configuration

例

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

23.1.6 lldp reinit-delay

本コマンドでは、LLDP ポートを無効にしたとき、ポートまたはリンクがダウンしたときに LLDP の後に再初期化を試みる際の待ち合わせ時間を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

lldp reinit-delay *seconds*

no lldp reinit-delay

seconds - LLDP を再初期化する前に、遅延を特定します。(範囲: 1 から 10 秒)

デフォルト設定

2 秒

コマンドモード

Global Configuration

コマンドの使用方法

ポートで LLDP が再初期化される際、このポートに関連する LLDP MIB で取得する情報は削除されます。

例

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

23.1.7 lldp tx-delay

本コマンドでは、ローカル LLDP MIB 変数の変更によっておこなわれる、広告の連続送信の遅延時間を設定します。デフォルト設定を復元するには、no 形式を使用してください。

構文

lldp tx-delay *seconds*

no lldp tx-delay

seconds - 送信遅延時間(範囲: 1 から 8192 秒)

デフォルト設定

2 秒

コマンドモード

Global Configuration

コマンドの使用方法

◆ 送信遅延時間は、ローカル LLDP MIB オブジェクトの短期間の急激な変化における一連の連続する

LLDP 送信を防止し、単一の変更ではなく複数の変更が各送信で報告される確率を高めるために使用します。

◆ 属性は、以下のルールに従う必要があります:
(4 * tx-delay) ≦ リフレッシュ間隔

例

```
Console(config)#lldp tx-delay 10
Console(config)#
```

23.1.8 lldp admin-status

本コマンドでは、特定ポートで LLDP プロトコルデータユニット（PDU）を送信のみ、受信のみ、または送受信のモードを有効にします。この機能を無効にするには、no 形式を使用してください。

構文

lldp admin-status {rx-only | tx-only | tx-rx}

no lldp admin-status

rx-only - LLDP PDU を受信だけします。

tx-only - LLDP PDU を送信だけします。

tx-rx - LLDP PDU を送受信します。

デフォルト設定

tx-rx

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

23.1.9 lldp basic-tlv management-ip-address

本コマンドでは、デバイスの Management Address（管理アドレス）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp basic-tlv management-ip-address

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

◆ 管理アドレスには、スイッチの IPv4 アドレスが含まれます。管理アドレスを設定していない場合には、アドレスは CPU、またはこの広告を送信するポートの MAC アドレスが入ります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

23.1.10 lldp basic-tlv port-description

本コマンドでは、Port Description（ポートの説明）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp basic-tlv port-description

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

ポートの説明は、製造元、製品名、およびインタフェースハードウェア/ソフトウェアバージョンなど RFC 2863 の ifDescr の MIB オブジェクトで取得できる情報が入ります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

23.1.11 lldp basic-tlv system-capabilities

本コマンドでは、特定ポートで System Capabilities（システム機能）を広告するかどうかを設定します。こ

の機能を無効にするには、no 形式を使用してください。

構文

[no] lldp basic-tlv system-capabilities

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

システム機能では、システムの主機能とこれらの主機能が有効かどうかを識別します。この TLV によって広告される情報は、IEEE 802.1AB に記載されています。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

23.1.12 lldp basic-tlv system-description

本コマンドでは、System Description（システム説明）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp basic-tlv system-description

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

システムの説明は、システムのハードウェアタイプ、ソフトウェアオペレーティングシステム、およびネットワーキングソフトウェアのフルネームとバージョン ID を含みます。RFC 3418 の sysDescr の MIB オブジェクトで取得できる情報が入ります。

例

```
Console(config)#interface ethernet 1/1
```

```
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

23.1.13 lldp basic-tlv system-name

本コマンドでは、System Name（システム名）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp basic-tlv system-name

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

システム名は、システムの管理上割り当てられた名前（hostname コマンドで設定する内容）を含む RFC 3418 の sysName の MIB オブジェクトで取得できる情報が入ります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

23.1.14 lldp dot1-tlv proto-ident

本コマンドでは、Protocol Identity（サポートされているプロトコル）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp dot1-tlv proto-ident

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

本オプションでは、インタフェースを通じてアクセス可能なプロトコルについて広告します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

23.1.15 lldp dot1-tlv proto-vid

本コマンドでは、Port Protocol VLAN ID（ポートベースのプロトコル VLAN 情報）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp dot1-tlv proto-vid

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

本オプションにより、このインタフェースで設定したポートベースのプロトコル VLAN を広告します（「19.5　プロトコルベースの VLAN の設定」を参照してください)。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

23.1.16 lldp dot1-tlv pvid

本コマンドでは、Port VLAN ID（デフォルト VLAN ID）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp dot1-tlv pvid

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

ポートのデフォルト VLAN 識別子(PVID)は、タグ無しフレームまたは優先タグ付きフレームが関連付けられている VLAN を示します(switchport native vlan コマンドを参照)。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

23.1.17 lldp dot1-tlv vlan-name

本コマンドでは、VLAN Name（VLAN 名称）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp dot1-tlv vlan-name

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

このオプションでは、インタフェースが割り当てられているすべての VLAN の名称を広告します。
switchport allowed vlan コマンドおよび protocol-vlan protocol-group (Configuring Interfaces)コマンドを参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

23.1.18 lldp dot3-tlv link-agg

本コマンドでは、Link Aggregation（リンクアグリゲーション機能）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp dot3-tlv link-agg

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

本オプションでは、インタフェースがリンクアグリゲーションメンバーの場合、リンクのアグリゲーションステータス、およびポート識別子を広告します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

23.1.19 lldp dot3-tlv max-frame

本コマンドでは、Maximum Frame Size（最大フレームサイズ）を広告するかどうかを設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp dot3-tlv max-frame

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

スイッチの最大フレームサイズ設定に関する情報については、「4.3　フレームサイズ」を参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

23.1.20 lldp dot3-tlv poe

本コマンドでは、Power-over-Ethernet (PoE)機能を広告するかどうかを設定します。この機能を無効にする

には、no 形式を使用してください。

構文

[no] lldp dot3-tlv poe

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット)

コマンドの使用方法

- 本コマンドは、PoE モデルにのみ適用されます。
- 本オプションでは、PoE がサポートされているか、現在有効になっているか、電力が供給されるポートピンを制御することができるか、ポートピンは電力および電力クラスを供給するように選択されているかを含む、Power-over-Ethernet 機能を広告します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv poe
Console(config-if)#
```

23.1.21 lldp med-notification

本コマンドでは、LLDP-MED 変更に関する SNMP トラップ通知の送信を有効にします。LLDE-MED 通知を無効にするには、no 形式を使用してください。

構文

[no] lldp med-notification

デフォルト設定

無効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- このオプションは、”lldp notification-interval”コマンドによって設定された間隔で指定された目標に SNMP トラップ通知を送信します。トラップ通知には LLDP MIB(IEEE802.1AB)の状態変更、LLDP-MED MIB(ANSI/TIA1057)、組織特有の LLDP-EXT-DOT1 と LLDP-EXT-DOT3 MIB が含まれます。
- SNMP トラップの宛先は、”snmp-server host”コマンドで設定されます。
- SNMP 通知と通知の間で起こる隣接 LLDP の変化の情報は送信されません。トラップ通知と同時に発

生する状態変化のみが送信されます。そのため、SNMP エージェントはスロットリングや送信ロスによって起こる lldpRemTablesChange 通知イベントの失敗を検出するために、定期的に lldpStatsRemTableLastChangeTime の値を確認するべきです。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-notification
Console(config-if)#
```

23.1.22 lldp med-tlv ext-poe

本コマンドでは、LLDP Media Endpoint Discovery（LLDP-MED）有効化ポートを拡張 Power-over-Ethernet 設定と使用状況を通知して受け入れるように設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp med-tlv ext-poe

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

本コマンドは、PoE モデルにのみ適用されます。

本オプションでは、スイッチから入手可能な電力、およびスイッチがプライマリまたはバックアップ電力のどちらから作動しているかを含む、スイッチの電力状態等の拡張 Power-over-Ethernet 機能詳細を広告します(エンドポイントデバイスは、この情報を使用して省電力モードに入ることを決定することができます)。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv ext-poe
Console(config-if)#
```

23.1.23 lldp med-tlv inventory

本コマンドでは、LLDP-MED が有効なポートでインベントリ識別の詳細情報を通知する設定をします。この機能を無効にするためには、no 形式を使用してください。

構文

[no] lldp med-tlv inventory

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

このオプションは、製造者、モデル、ソフトウェアバージョンなどの管理に役立つデバイスの詳細情報を通知します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv inventory
Console(config-if)#
```

23.1.24 lldp med-tlv location

本コマンドでは、LLDP-MED が有効なポートでその位置を識別する詳細情報の通知を設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp med-tlv location

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

このオプションは、位置を識別する詳細情報を通知します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv location
Console(config-if)#
```

23.1.25 lldp med-tlv med-cap

本コマンドでは、LLDP-MED が有効なポートで MED 対応であることの通知を設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp med-tlv med-cap

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

このオプションは、LLDP-MED TLV 対応であることを通知します。それにより、Media Endpoint and Connectivity Devices は TLV に関連した LLDP-MED にスイッチが対応していることを効率的に知ることができます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv med-cap
Console(config-if)#
```

23.1.26 lldp med-tlv network-policy

本コマンドでは、LLDP-MED が有効なポートでネットワークポリシー設定の通知を設定します。この機能を無効にするには、no 形式を使用してください。

構文

[no] lldp med-tlv network-policy

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

このオプションは、VLAN 設定とポートの不適切な組み合わせの発見と診断を目的とした、ネットワーク

ポリシー設定の情報を通知します。不適切なネットワークポリシー設定は、しばしば音声品質の低下やサービスの完全な停止を引き起こします。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv network-policy
Console(config-if)#
```

23.1.27 lldp notification

本コマンドでは、LLDP 変更の SNMP トラップ通知の送信を有効にします。この LLDP 通知を無効にするには、no 形式を使用してください。

構文

[no] lldp notification

デフォルト設定

有効

コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

コマンドの使用方法

- 本オプションでは、lldp notification-interval コマンドを使用して指定した間隔で、指定されたターゲットステーションに SNMP トラップ通知を送信します。このトラップ通知には、LLDP MIB(IEEE 802.1AB)、または LLDP-EXT-DOT1 および LLDP-EXT-DOT3 MIB の状態変化に関する情報が含まれています。
- snmp-server host コマンドを使用して、SNMP トラップ宛先を設定してください。
- SNMP 通知の間に発生した LLDP 隣接追加の変更に関する情報は送信されません。トラップ通知の時点で存在する状態変化のみが送信されます。したがって SNMP エージェントは、lldpStatsRemTableLastChangeTime の値を定期的にチェックして、伝送損失などのために lldpRemTablesChange 通知イベントが検知されなかったことを検出する必要があります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

23.1.28 show lldp config

本コマンドでは、全ポートの LLDP コンフィグレーションを表示します。

構文

show lldp config [detail *interface*]

detail - 設定サマリを表示します。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

コマンドモード

Privileged Exec

例

以下の例では、ポート 1 ですべての基本 LLDP パラメータが有効になっています。

```
Console#show lldp config
LLDP Global Configuation
 LLDP Enabled                 : Yes
 LLDP Transmit Interval       : 30 seconds
 LLDP Hold Time Multiplier    : 4
 LLDP Delay Interval          : 2 seconds
 LLDP Re-initialization Delay : 2 seconds
 LLDP Notification Interval   : 5 seconds
 LLDP MED Fast Start Count    : 4

LLDP Port Configuration
 Port     Admin Status Notification Enabled
 -------- ------------ --------------------
 Eth 1/1  Tx-Rx        True
 Eth 1/2  Tx-Rx        True
 Eth 1/3  Tx-Rx        True
 Eth 1/4  Tx-Rx        True
 Eth 1/5  Tx-Rx        True
.
.
.
Console#show lldp config detail ethernet 1/1
LLDP Port Configuration Detail
 Port                         : Eth 1/1
 Admin Status                 : Tx-Rx
 Notification Enabled         : True
 Basic TLVs Advertised        : port-description
                                system-name
                                system-description
                                system-capabilities
```

```
                                  management-ip-address
 802.1 specific TLVs Advertised : port-vid
                                  vlan-name
                                  proto-vlan
                                  proto-ident
 802.3 specific TLVs Advertised : mac-phy
                                  link-agg
                                  max-frame
 MED Notification Status        : Enabled
 MED Enabled TLVs Advertised    : med-cap
                                  network-policy
                                  location
                                  ext-poe
                                  inventory

Console#
```

23.1.29 show lldp info local-device

本コマンドでは、デバイスの LLDP グローバルおよびインタフェース固有のコンフィグレーションを表示します。

構文

show lldp info local-device [detail *interface*]

detail - 設定サマリを表示します。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

コマンドモード

Privileged Exec

例

```
Console#show lldp info local-device
 LLDP Local Global Information
  Chassis Type : MAC Address
  Chassis ID   : 00-01-02-03-04-05
  System Name  :
  System Description : AXprimoM210-08T
  System Capabilities Support : Bridge
  System Capabilities Enabled : Bridge
  Management Address : 192.168.0.101 (IPv4)
```

```
 LLDP Port Information
  Port    Port ID Type     Port ID           Port Description
 -------- ---------------- ----------------- ------------------------------
 Eth 1/1  MAC Address      00-12-E2-DA-FC-E9 Ethernet Port on unit 0, port 1
 Eth 1/2  MAC Address      00-12-E2-DA-FC-EA Ethernet Port on unit 0, port 2
 Eth 1/3  MAC Address      00-12-E2-DA-FC-EB Ethernet Port on unit 0, port 3
 Eth 1/4  MAC Address      00-12-E2-DA-FC-EC Ethernet Port on unit 0, port 4
.
.
.
Console#show lldp info local-device detail ethernet 1/1
LLDP Local Port Information Detail
 Port             : Eth 1/1
 Port ID Type     : MAC Address
 Port ID          : 00-12-E2-DA-FC-E9
 Port Description : Ethernet Port on unit 1, port 1

Console#
```

23.1.30 show lldp info remote-device

本コマンドでは、LLDP 有効化ポートに接続しているリモートデバイスの LLDP グローバル、およびインタフェース特有コンフィグレーションを示します。

構文

show lldp info remote-device [detail *interface*]

detail - 詳細説明を表示します。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

コマンドモード

Privileged Exec

例

LLDP-MED 機能を広告する IP 電話またはその他のエンドノードデバイスは、「LLDP-MED 機能」およびその他の関連フィールドに表示される情報のためにスイッチに接続する必要があります。

```
Console#show lldp info remote-device
LLDP Remote Devices Information
 Local Port Chassis ID        Port ID           System Name
 ---------- ----------------- ----------------- ------------------------------
```

```
 Eth 1/2    00-12-E2-03-01-30 00-12-E2-03-01-32

Console#show lldp info remote-device detail ethernet 1/2
LLDP Remote Devices Information Detail
------------------------------------------------------------------------------
 Index               : 1
 Chassis Type        : MAC Address
 Chassis ID          : 00-12-E2-03-01-30
 Port ID Type        : MAC Address
 Port ID             : 00-12-E2-03-01-32
 Time To Live        : 120 seconds
 Port Description    : Ethernet Port on unit 1, port 2
 System Description  : AXprimoM210-08P
 System Capabilities : Bridge
 Enabled Capabilities : Bridge

 Management Address : 192.168.13.226 (IPv4)

 Port VLAN ID : 1

 Port and Protocol VLAN ID : supported, disabled

 VLAN Name : VLAN    1 - DefaultVlan
             VLAN   13 -

 Protocol Identity (Hex) : 00-27-42-42-03-00-00-02
                           88-09-01
                           88-8E

 MAC/PHY Configuration/Status
  Port Auto-neg Supported            : Yes
  Port Auto-neg Enabled              : Yes
  Port Auto-neg Advertised Cap (Hex) : 6C01
  Port MAU Type                      : 30

 Power via MDI
  Power Class             : PSE
  Power MDI Supported     : Yes
  Power MDI Enabled       : Yes
  Power Pair Controllable : No
  Power Pairs             : Spare
  Power Classification    : Class 1

 Link Aggregation
  Link Aggregation Capable : Yes
  Link Aggregation Enable  : No
  Link Aggregation Port ID : 0

 Max Frame Size : 1522
```

```
Console#
```

以下の例では、LLDP-MED TLV を広告するエンドノードデバイスに表示される情報について示します。

```
...
  LLDP-MED Capability :
    Device Class                  : Network Connectivity
    Supported Capabilities        : LLDP-MED Capabilities
                                    Network Policy
                                    Location Identification
                                    Extended Power via MDI - PSE
                                    Inventory
    Current Capabilities          : LLDP-MED Capabilities
                                    Location Identification
                                    Extended Power via MDI - PSE
                                    Inventory
  Location Identification :
    Location Data Format          : Civic Address LCI
    Country Name                  : JP
    What                          : 2
  Extended Power via MDI :
    Power Type                    : PSE
    Power Source                  : Unknown
    Power Priority                : Unknown
    Power Value                   : 0 Watts
  Inventory          :
    Hardware Revision             : ROA
    Firmware Revision             : 1.2.6.0
    Software Revision             : 1.2.6.0
    Serial Number                 : S123456
    Manufacture Name              : Prye
    Model Name                    : VP101
    Asset ID                      : 340937
Console#
```

23.1.31 show lldp info statistics

本コマンドでは、すべての接続 LLDP 有効化インタフェースを通じて受信したトラフィックをベースにした、統計を示します。

構文

show lldp info statistics [detail *interface*]

detail - 設定サマリを表示します。

interface

ethernet *unit*/*port*

unit - ユニット識別子です。(範囲: 1)

port - ポート番号です。(範囲: 1 から 10)

port-channel *channel-id* (範囲: 1-8)

コマンドモード

Privileged Exec

例

```
Console#show lldp info statistics
LLDP Global Statistics
 Neighbor Entries List Last Updated : 485 seconds
 New Neighbor Entries Count         : 2
 Neighbor Entries Deleted Count     : 1
 Neighbor Entries Dropped Count     : 0
 Neighbor Entries Ageout Count      : 1

LLDP Port Statistics
 Port     NumFramesRecvd NumFramesSent NumFramesDiscarded
 -------- -------------- ------------ -----------------
 Eth 1/1              12           12                 0
 Eth 1/2              17           17                 0
 Eth 1/3               0            0                 0
 Eth 1/4               0            0                 0
 Eth 1/5               0            0                 0
.
.
.
Console#show lldp info statistics detail ethernet 1/1
LLDP Port Statistics Detail
 Port Name         : Eth 1/1
 Frames Discarded  : 0
 Frames Invalid    : 0
 Frames Received   : 12
 Frames Sent       : 12
 TLVs Unrecognized : 0
 TLVs Discarded    : 0
 Neighbor Ageouts  : 1
Console#
```

24 ドメインネームサービスコマンド

これらのコマンドは、ドメインネームシステム(DNS)サービスを構成するために使用されます。エントリは、DNS ドメイン名から IP アドレスへのマッピングテーブル、構成されたデフォルトのドメイン名、またはドメイン名から変換に使用するために指定された 1 つ以上のネームサーバで、手動で構成することができます。

ドメインネームサービスは、最低一つのネームサーバを ip name-server コマンドで指定して、ドメインルックアップを ip domain-lookup コマンドで有効にするまで、有効になりません。

表 24-1 アドレステーブルコマンド

コマンド	機能	モード
DNS コマンド		
ip domain-list	不完全なホスト名のデフォルトのドメイン名のリストを定義します。	GC
ip domain-lookup	DNS ベースのホスト名からアドレスへの変換を有効にします。	GC
ip domain-name	不完全なホスト名のデフォルトドメイン名を定義します。	GC
ip host	静的 IPv4 ホストの名前からアドレスへのマッピングを作成します。	GC
ip name-server	ホスト名からアドレスへの変換に使用するための、1 つまたは複数のネームサーバのアドレスを指定します。	GC
ipv6 host	静的 IPv6 ホストの名前からアドレスへのマッピングを作成します。	GC
clear dns cache	DNS キャッシュからのすべてのエントリをクリアします。	PE
clear host	ホスト名からアドレスへのエントリを削除します。	PE
show dns	DNS サービスの設定を表示します。	PE
show dns cache	DNS キャッシュのエントリを表示します。	PE
show hosts	静的ホストの名前からアドレスへのマッピングテーブルを表示します。	PE
マルチキャスト DNS コマンド		
ip mdns	マルチキャスト DNS を有効にします。	GC
show ip mdns	マルチキャスト DNS の設定状態を表示します。	GC

24.1 DNS コマンド

24.1.1 ip domain-list

本コマンドでは、不完全なホスト名に追加するドメイン名のリストを定義します(例; クライアントから渡された、ドット区切りの書式でフォーマットされていないホスト名)。リストから名前を削除するには、no 形式を使用してください。

構文

[no] ip domain-list *name*

name - ホスト名です。ドメイン名からホスト名を区切る最初のドットは含めないでください。(範囲: 1 から 127 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

- ドメイン名は、一度に 1 つずつリストの末尾に追加されます。
- スイッチ上で DNS サービスによって、不完全なホスト名を受信した際、ドメインリストを介して動作し、リスト内の各ドメイン名をホスト名に追加して、指定されたネームサーバで一致するかどうかをチェックします。
- ドメインリストが無い場合、ip domain-name コマンドで特定されたドメイン名が使用されます。ドメインリストがある場合には、デフォルトドメイン名は使用されません。

例

この例では、現在のリストに 2 つのドメイン名を追加して、リストを表示します。

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
Console#
```

関連コマンド

ip domain-name

24.1.2 ip domain-lookup

本コマンドでは、DNS ホストの名前からアドレスへの変換を有効にします。DNS を無効にするには、no 形式を使用してください。

構文

[no] ip domain-lookup

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用方法

- DNS を有効にする前に、最低 1 つのネームサーバを指定する必要があります。
- 1 つ以上のネームサーバが設定されていても DNS がまだ有効になっておらず、スイッチが DNS サーバのリストを含む DNS フィールドを含む DHCP パケットを受信すると、スイッチは自動的に DNS ホストの名前からアドレスへの変換を有効にします。
- すべてのネームサーバが削除された場合、DNS は自動的に無効になります。

例

この例では DNS を有効にし、その次に設定を表示します。

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

関連コマンド

ip domain-name

ip name-server

24.1.3 ip domain-name

本コマンドでは、不完全なホスト名に追加するドメイン名のリストを定義します(例; クライアントから渡された、ドット区切りの書式でフォーマットされていないホスト名)。現在のドメイン名から削除するには、no 形式を使用してください。

構文

ip domain-name *name*

no ip domain-name

name - ホスト名です。ドメイン名からホスト名を区切る最初のドットは含めないでください。(範囲: 1 から 127 文字)

デフォルト設定

無し

コマンドモード

Global Configuration

例

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Disabled
Default Domain Name:
    sample.com
Domain Name List:
Name Server List:
Console#
```

関連コマンド

ip domain-list

ip name-server

ip domain-lookup

24.1.4 ip host

本コマンドでは、ホスト名を IPv4 アドレスにマップする DNS テーブルの中で、静的エントリを作成します。エントリを削除するには、no 形式を使用してください。

構文

[no] ip host *name address*

name - IPv4 ホスト名です。(範囲: 1 から 127 文字)

address - 対応する IPv4 アドレスです。

デフォルト設定

静的エントリはありません。

コマンドモード

Global Configuration

コマンドの使用方法

no ip host コマンドを使って、静的エントリをクリアするか、または clear host コマンドで動的エントリをクリアします。

例

この例では、IPv4 アドレスをホスト名にマッピングします。

```
Console(config)#ip host rd5 192.168.1.55
Console(config)#end
Console#show hosts
No.  Flag Type    IP Address            TTL   Domain
---- ---- ------- --------------------  ----- ------------------------------
   0    2 Address 192.168.1.55                rd5
Console#
```

24.1.5 ip name-server

本コマンドでは、名前からアドレスへの解決に使用する 1 つまたは複数のドメインネームサーバのアドレスを指定します。リストからネームサーバを削除するには、no 形式を使用してください。

構文

[no] ip name-server *server-address1* [*server-address2* …

server-address6]

server-address1 - ドメインネームサーバの IPv4 または IPv6 アドレスです。

server-address2 … *server-address6* - 追加ドメインネームサーバの IPv4 または IPv6 アドレスです。

デフォルト設定

無し

コマンドモード

Global Configuration

コマンドの使用方法

一覧化されたネームサーバは、応答が受信されるか、または応答無しでリストの終わりに達するまで、指

定されたシーケンスで照会されます。

例

この例では、リストに 2 つのドメインネームサーバを追加し、その次にリストを表示します。

```
Console(config)#ip name-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

関連コマンド

ip domain-name

ip domain-lookup

24.1.6 ipv6 host

本コマンドでは、ホスト名を IPv6 アドレスにマップする DNS テーブルの中で、静的エントリを作成します。エントリを削除するには、no 形式を使用してください。

構文

[no] ipv6 host *name ipv6-address*

name - IPv6 ホスト名です。(範囲: 1 から 127 文字)

ipv6-address - 対応する IPv6 アドレスです。このアドレスは、RFC 2373 の「IPv6 アドレッシングアーキテクチャ」に従って、コロンで区切られた 8 つの 16 ビットの 16 進数を使用して入力する必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。

デフォルト設定

静的エントリはありません。

コマンドモード

Global Configuration

例

この例では、IPv6 アドレスをホスト名にマッピングします。

```
Console(config)#ipv6 host rd6 2001:0db8:1::12
Console(config)#end
Console#show hosts
No.  Flag Type    IP Address            TTL   Domain
---- ---- ------- --------------------  ----- ------------------------------
   0    2 Address 192.168.1.55                rd5
   1    2 Address 2001:DB8:1::12              rd6
Console#
```

24.1.7 clear dns cache

本コマンドでは、DNS キャッシュですべてのエントリをクリアします。

コマンドモード

Privileged Exec

例

```
Console#clear dns cache
Console#show dns cache
No.     Flag    Type    IP Address      TTL     Host
------- ------- ------- --------------- ------- --------

Console#
```

24.1.8 clear host

本コマンドでは、DNS テーブルから動的エントリを削除します。

構文

clear host {*name* | *}

name - ホスト名です。(範囲: 1 から 127 文字)

* - すべてのエントリを削除します。

デフォルト設定

None

コマンドモード

Privileged Exec

コマンドの使用方法

clear host コマンドを使って、動的エントリをクリアするか、または no ip host コマンドを使用して静的エントリをクリアします。

例

この例では、DNS テーブルからすべての動的エントリをクリアします。

```
Console#clear host *
Console#
```

24.1.9 show dns

本コマンドでは、DNS サービスの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

24.1.10 show dns cache

本コマンドでは、DNS キャッシュのエントリを表示します。

コマンドモード

Privileged Exec

例

```
Console#show dns cache
No.     Flag    Type    IP Address      TTL     Host
------- ------- ------- --------------- ------- --------
```

```
      3        4 Host     192.168.36.158       115 www.example1.com
      4        4 CNAME    POINTER TO:3         115 www.example2.com
Console#
```

表 24-2 show dns cache - 表示の説明

フィールド	説明
No.	各リソースレコードのエントリ番号です。
Flag	フラグは常にキャッシュエントリを示す 「4」であるため、信頼できません。
Type	このフィールドには、所有者のプライマリ名を指定する「ホスト」と、既存のエントリと同じ IP アドレスにマップされる複数のドメイン名（またはエイリアス）を指定する「CNAME」が含まれます。
IP Address	このレコードに関連する IP アドレスです。
TTL	ネームサーバによって報告された生存時間です。
Host	このレコードに関連するホスト名です。

24.1.11 show hosts

本コマンドでは、静的ホストの名前からアドレスへのマッピングテーブルを表示します。

コマンドモード

Privileged Exec

例

以前に設定されたエントリと同じアドレスにマッピングされている場合、ホスト名はエイリアスとして表示されることに留意してください。

```
Console#show hosts
No.  Flag Type    IP Address            TTL   Host
---- ---- ------- --------------------  ----- ------------------------------
   0    2 Address 192.168.1.55                rd5
   1    2 Address 2001:DB8:1::12              rd6
   3    4 Address 192.168.36.158            65 www.example1.com
   4    4 CNAME   POINTER TO:3              65 www.example2.com
Console#
```

表 24-3 show hosts - 表示の説明

フィールド	説明
No.	各リソースレコードのエントリ番号です。
Flag	フィールドには、静的エントリの場合は「2」、キャッシュに格納されている動的エントリの場合は「4」が表示されます。
Type	このフィールドには、所有者のプライマリ名を指定する「アドレス」と、既存のエントリと同じ IP アドレスにマップされる複数のドメイン名（またはエイリアス）を指定する「CNAME」が含まれます。
IP Address	このレコードに関連する IP アドレスです。
TTL	ネームサーバによって報告された生存時間です。静的エントリの場合は、このフィールド

フィールド	説明
	は常に空白です。
Host	このレコードに関連するホスト名です。

24.2 マルチキャスト DNS コマンド

24.2.1 ip mdns

本コマンドでは、マルチキャスト DNS を有効にします。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip mdns

デフォルト設定

有効

コマンドモード

Global Configuration

コマンドの使用方法

このコマンドを使用して、専用 DNS サーバを必要とせずに、ローカルネットワーク上でマルチキャスト DNS ホストの名前からアドレスへのマッピングを有効にします。このコマンドの詳細については、Web 管理ガイドを参照してください。

例

```
Console(config)#ip mdns
Console(config)#
```

24.2.2 show ip mdns

本コマンドでは、設定状態のマルチキャスト DNS サービスを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip mdns
Multicast DNS Status : Enabled
Console#
```

25 DHCP コマンド

これらのコマンドは、DHCP(Dynamic Host Configuration Protocol)クライアント機能を設定するために使用されます。

表 25-1　DHCP コマンド

コマンドグループ	機能
DHCP Client	インタフェースに、IP アドレス情報の動的取得を許可します。

25.1 DHCP クライアント

本章に記載されているコマンドを使用して、スイッチの VLAN インタフェースに IP アドレスの動的取得を許可します。

表 25-2　DHCP クライアントコマンド

コマンド	機能	モード
IPv4 の DHCP		
ip dhcp dynamic-provision	DHCP を通じてダイナミックプロビジョニングを有効にします。	GC
ip dhcp client class-id	インタフェースの DHCP クライント識別子を指定します。	IC
ip dhcp restart client	BOOTP または DHCP クライアント要求を通知します。	PE
show ip dhcp dynamic-provision	DHCP によるダイナミックプロビジョニングのステータスを表示します。	PE
IPv6 の DHCP		
ipv6 dhcp client rapid-commit vlan	DHCPv6 メッセージの Rapid Commit オプションを指定します。	GC
ipv6 dhcp restart client vlan	DHCPv6 クライアント要求を通知します。	PE
show ipv6 dhcp duid	スイッチの DHCP ユニーク識別子を表示します。	PE
show ipv6 dhcp vlan	特定インタフェースの DHCPv6 情報を表示します。	PE

25.1.1 ip dhcp dynamic-provision

本コマンドでは、DHCP を通じたダイナミックプロビジョニングを有効にします。この機能を無効にするには、no 形式を使用してください。

構文

[no] ip dhcp dynamic-provision

デフォルト設定

有効

コマンドモード

Global Configuration

コマンドの使用方法

DHCP デーモンは、Linux がクライアントシステムの TCP / IP 情報を動的に設定するために使用するデーモンです。DHCP オプション 66/67 をサポートするには、対応するステートメントを DHCP デーモンの構成ファイルに追加する必要があります。このプロセスの完了方法については、「1.6　DHCP サーバからのコンフィグレーションおよびその他パラメータのダウンロード」を参照してください。

以下は、ダイナミックプロビジョニングプロセスを完了するために DHCP デーモンに追加できる、いくつかの代替コマンドです。

デフォルトでは、DHCP オプション 66/67 のパラメータは DHCP サーバから送られた応答から伝播されません。オプション 66/67 で DHCP 応答を要求するには、クライアントは、「parameter request list」オプションを含む DHCP 要求を送信して、オプション 66/67 に関心があることをサーバに通知できます。これに加

えて、クライアントは DHCP サーバがデバイスを識別し、要求するデバイスにどの情報を与えるべきかを決定するために、「vendor class identifier」オプションを含む DHCP 要求をサーバに送信することもできます。

次に示すのは、サーババージョン dhcp-3.0.4rc1 用の dhcpd.conf ファイルの 2 つの追加の構成例です。いずれか 1 つを選択することができます。

1. サブネットセクションで条件を定義します:

```
shared-network Sample1 {
    subnet 192.168.1.0 netmask 255.255.255.0 {
# option 55
    option dhcp-parameter-request-list 1,66,67;
# option 66
    option tftp-server-name "192.168.1.1";
# option 67
    option bootfile-name "dhcp_config.cfg ";
      }
   }
```

2. クラスセクションで条件を定義します:

```
class "OPT66_67" { # for option 66/67
# option 124
    match if option vendor-class-identifier = "AXprimoM210-08P";
# option 55
    option dhcp-parameter-request-list 1,66,67;
# option 66
    option tftp-server-name "192.168.1.1";
# option 67
    option bootfile-name "dhcp_config.cfg";
}

shared-network Sample2 {
subnet 192.168.1.0 netmask 255.255.255.0 {
    }
    pool {
        allow members of "OPT66_67";
        range 192.168.1.10 192.168.1.20;
    }
}
```

◆ 自動アップグレードとダイナミックプロビジョニングの両方が有効である場合、まずダイナミックプロビジョニングが動作し、その後に自動アップグレードが動作します。

例

以下の例では、ダイナミックプロビジョニングを有効にします。

```
Console(config)#ip dhcp dynamic provisioning
Console(config)#
```

25.1.2 ip dhcp client class-id

本コマンドでは、現在のインタフェースの DHCP クライアントベンダクラス識別子を指定します。DHCP パケットからクラス識別子を削除するには、no 形式を使用してください。

構文

ip dhcp client class-id [text *text* | hex *hex*]

no ip dhcp client class-id

text - テキスト文字列です。(範囲: 1 から 32 文字)

hex - 16 進数(ascii コード表記)の値です。(範囲: 1 から 64 文字)

デフォルト設定

モデル番号を文字列として、使用するクラス識別子オプションが有効になっています。

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- デフォルト設定を復元するために、キーワード無しで本コマンドを使用します。
- 本コマンドは、DHCP サーバへのスイッチのベンダクラスと構成を識別するために使用され、DHCP サーバはこの情報を使用して、クライアントへのサービス方法または返される情報の種類を決定します。
- この DHCP オプションの一般的なフレームワークは、RFC 2132(オプション 60)に規定されています。この情報は、クライアントに関するコンフィグレーションやその他の識別情報を伝えるために使用されますが、使用する特定の文字列は、サービスプロバイダまたはネットワーク管理者が提供する必要があります。オプション 60,66 および 67 のステートメントをサーバデーモンの構成ファイルに追加することができます。

表 25-3 オプション 60、66 および 67 ステートメント

オプション	ステートメント	
	キーワード	パラメータ
60	vendor-class-identifier	ベンダクラス識別子を示す文字列
66	tftp-server-name	tftp サーバ名を示す文字列
67	bootfile-name	bootfile 名を示す文字列

- デフォルトでは、DHCP オプション 66/67 のパラメータは DHCP サーバの応答には含まれません。オプション 66/67 情報で DHCP 応答を要求するには、このスイッチから送信された DHCP クライアント要求に、この情報を要求する“parameter request list”が含まれています。さらにクライアント要求には、DHCP サーバがデバイスを識別しダウンロードに適した構成ファイルを選択できるようにする ip dhcp client class-id コマンドで設定された「ベンダクラス識別子」も含まれています。この情報はオプション 55 および 124 に含まれています。

表 25-4 オプション 55 および 124 ステートメント

オプション	ステートメント	
	キーワード	パラメータ
55	dhcp-parameter-request-list	','で分割されているパラメータリストです。
124	vendor-class-identifier	ベンダクラス識別子を示す文字列です。

- サーバは、TFTP サーバ名とブートファイル名を含む、オプション 66 属性で返信する必要があります。
- ベンダクラス識別子は、ip dhcp client class-id コマンドを使用して、テキストまたは 16 進数のいずれかでフォーマットすることができます。しかしながら、クライアントとサーバの両方で使用されたフォーマットは同一である必要があることに、留意してください。

例

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

関連コマンド

ip dhcp restart client

25.1.3 ip dhcp restart client

本コマンドでは、BOOTP または DHCP クライアント要求を通知します。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

- 本コマンドでは、ip address コマンドによって BOOTP または DHCP モードに設定されているすべての IP インタフェースに対して、BOOTP または DHCP クライアント要求を発行します。
- クライアントのホストアドレスの再設定を DHCP サーバに要求します。
- BOOTP または DHCP サーバが異なるドメインに移動している場合、クライアントに提供したアドレスのネットワークポーションは新規ドメインをベースとします。

例

以下の例では、デバイスは同じアドレスを再割当てします。

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
```

```
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-12-E2-00-00-01
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
  Proxy ARP is disabled
  DHCP Client Vendor Class ID (text): AXprimoM210-08P
  DHCP Relay Server:
Console#
```

関連コマンド

ip address

25.1.4 show ip dhcp dynamic-provision

本コマンドでは、DHCP を通じてダイナミックプロビジョンのステータスを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp dynamic provisioning
Dynamic Provision via DHCP Status:   Disabled
Console#
```

25.1.5 ipv6 dhcp client rapid-commit

このコマンドは、DHCPv6 メッセージ交換の Rapid Commit オプションを指定します。

指定されたインタフェースから送信されたすべての DHCPv6 クライアント要求に対して適用されます。このオプションを無効するには、no 形式を使用します。

構文

[no] ipv6 dhcp client rapid-commit vlan *vlan-id*

vlan-id - 単一の番号として指定された VLAN ID、ハイフンで区切られた連続する番号の範囲、またはコンマで区切られた複数の数字

（範囲：1～4094、最大コマンド長：300 文字）

デフォルト設定

無効

コマンドモード

Global Configuration

コマンドの使用法

- DHCPv6 クライアントは、通常の 4 メッセージ交換（要請、アドバタイズ、要求、応答)、または迅速な 2 メッセージ交換（要請、応答）を通じて、サーバから設定パラメータを取得できます。 2 メッセージ交換を使用するには、クライアントとサーバの両方で迅速コミットオプションを有効にする必要があります。
- このコマンドは、プレフィックス委任のための 2 メッセージ交換方式を可能にします。
  イネーブルにすると、指定されたインタフェースから送信された DHCPv6 クライアント要求では、すべての要請メッセージに迅速コミットオプションが含まれます。
- このコマンドを使用してスイッチ上で迅速コミットオプションが有効になっている場合は、DHCPv6 サーバでは、メッセージ交換を通常の 4 段階のプロセスから要請メッセージと返信メッセージの 2 段階の交換に減らすことができます。

例

```
Console(config)#ipv6 dhcp client rapid-commit vlan 2
Console(config)#
```

25.1.6 ipv6 dhcp restart client vlan

本コマンドでは、DHCPv6 クライアント要求を通知します。

構文

ipv6 dhcp restart client vlan *vlan-id*

vlan-id - 単一の番号として指定された VLAN ID、ハイフンで区切られた連続した番号の範囲、またはコンマで区切られた複数の番号です。(範囲: 1 から 4094; 最長コマンド長: 300 文字)

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

- 本コマンドは、DHCPv6 クライアントプロセスがまだ実行されていない場合は、指定されたインタフェースを介して構成情報の要求を送信して起動します。DHCPv6 が再起動されると、スイッチはステートフルアドレス自動設定によって IP アドレスプレフィックスを取得しようとする可能性があります。ルータアドバタイズメントに「その他のステートフルコンフィグレーション」フラグが設定されている場合、スイッチは DHCPv6 が再起動されたときに他の非アドレス設定情報(デフォルトゲートウェイまたは DNS サーバ等)を取得しようとする場合もあります。
  クライアント要求を DHCPv6 サーバに送信する前に、スイッチに ipv6 address autoconfig コマンドを使用してリンクローカルアドレスを設定する必要があります。ルータ通知メッセージで受信した管理ア

ドレス設定フラグ(M フラグ)およびその他のステートフル設定フラグ(O フラグ)の状態によって、このスイッチが DHCPv6 サーバから取得しようとする情報が、以下のように決定されます:

- M および O フラグの両方が 1 に設定されます:
  DHCPv6 が、アドレスとその他のコンフィグレーションの両方に使用されます。
  この組み合わせは、DHCPv6 ステートフルと呼ばれ、DHCPv6 サーバがステートフルアドレスを IPv6 ホストに割当てます。
- M フラグが 0 に設定され、O フラグが 1 に設定されます:
  DHCPv6 は、他のコンフィグレーションに対してのみ使用されます。
  隣接ルータは、IPv6 ホストがステートレスアドレスを取得する非リンクローカルアドレスプレフィックスを広告するように設定されています。
  この組み合わせは、DHCPv6 ステートレスと呼ばれ、DHCPv6 サーバは IPv6 ホストにステートフルアドレスを割り当てず、ステートレスな設定を割り当てます。

◆ DHCPv6 クライアントは、送信請求メッセージを送信し、通知されたメッセージ応答を収集することによって、サーバリストを作成します。これらのサーバは、広告されたプリファレンス値にもとづいてランク付けされます。クライアントがサーバからプレフィックスを取得する必要がある場合には、プレフィックスを通知したサーバのみが考慮されます。

◆ ipv6 dhcp client rapid-commit vlan コマンドと DHCPv6 サーバを使用して、スイッチ上で高速コミットオプションが有効になっている場合、メッセージ交換を通常の 4 ステッププロセスから送信請求と応答メッセージのみの 2 ステップ交換に減らすことができます。

例

以下の例では、VLAN 1 においてクライアント要求を通知します。

```
Console#ipv6 dhcp restart client vlan 1
Console#
```

関連コマンド

ipv6 address autoconfig

25.1.7 show ipv6 dhcp duid

本コマンドでは、このスイッチの DHCP 固有識別子を示します。

コマンドモード

Privileged Exec

コマンドの使用方法

DHCPv6 クライアントとサーバは、クライアント識別子とサーバ識別子オプションに含まれる、DHCP 固有識別子(DUID)によって、識別されます。静的または動的プレフィックスは、クライアントの DUID にもとづいて割当てられる可能性があります。

例

```
Console#show ipv6 dhcp duid
```

```
DHCPv6 Unique Identifier (DUID): 0001-0001-4A8158B4-00E00C0000FD
Console#
```

25.1.8 show ipv6 dhcp vlan

本コマンドでは、特定インタフェースの DHCPv6 情報を示します。

構文

show ipv6 dhcp vlan *vlan-list*

vlan-list - 単一の番号として指定された VLAN ID、ハイフンで区切られた連続した番号の範囲、またはコンマで区切られた複数の番号です。(範囲: 1 から 4094; 最長コマンド長: 300 文字)

コマンドの使用方法

DHCPv6 サーバの中の各割当ては、DUID と IAID によって識別されます。IAID とは、インタフェース関連付け識別子(Interface Association Identifier)の意味で、インタフェースと 1 つ以上のアドレスをバインドします。

コマンドモード

Privileged Exec

例

```
Console#show ipv6 dhcp vlan 1
VLAN 1 is in DHCP client mode, Rapid-Commit
  IAID:                          C0000F0
List of known servers:
  Server address : FE80::250:FCFF:FEF9:A494
  DUID           : 0001-0001-48CFB0D5-F48F2A006801

  Server address : FE80::250:FCFF:FEF9:A405
  DUID           : 0001-0001-38CF5AB0-F48F2A003917
Console#
```

関連コマンド

ipv6 address

26 IP インタフェースコマンド

IP バージョン 4 とバージョン 6 アドレスは、ネットワーク経由でのスイッチへの管理アクセスに使用することができます。また、IPv4 または IPv6 の両方のアドレスを同時に使用してスイッチにアクセスすることができます。特定の IPv4 または IPv6 アドレスを手動で設定するか、BOOTP または DHCP サーバの電源が入っているときにスイッチから IPv4 アドレスを取得するように指示できます。IPv6 アドレスは、手動で構成することも動的に生成することもできます。

VLAN 1 のスイッチの IPv4 アドレスは、デフォルトでは DHCP を介して取得されます。また、このデバイスと別のネットワークセグメントに存在する管理ステーションとの間に、IPv4 または IPv6 のデフォルトゲートウェイを確立する必要があります。

表 26-1 IP インタフェースコマンド

コマンドグループ	機能
IPv4 インタフェース	スイッチの IPv4 アドレスを設定します。
IPv6 インタフェース	スイッチの IPv6 アドレスを設定します。

26.1 IPv4 インタフェース

デフォルトでは、このスイッチに割当てられた IP アドレスはありません。ネットワークを通じて、あるいはスイッチを既存の IP サブネットに接続して、スイッチを管理するために新規のアドレスを手動で設定する必要があります。また(ルーティングが有効になっていない場合)、本デバイスと管理ステーション、または他のネットワークセグメントに存在する他のデバイス間で、デフォルトゲートウェイを確立する必要があります。

本章では、IP インタフェース、アドレス解決プロトコル(ARP)とプロキシ ARP を設定するコマンドが含まれます。

表 26-2 IPv4 インタフェースコマンド

コマンドグループ	機能
基本的な IPv4 のコマンド	インタフェースおよびゲートウェイルータの IP アドレスを設定します。
ARP のコマンド	静的、動的およびプロキシ ARP サービスを設定します。

26.1.1 基本的な IPv4 のコマンド

本章では、スイッチ上で VLAN インタフェースの IP アドレスを設定するために使用されるコマンドについて説明します。

表 26-3 基本 IP 設定コマンド

コマンド	機能	モード
ip address	現在のインタフェースの IP アドレスを設定します。	IC
show ip interface	本デバイスの IP 設定を表示します。	PE
show ip traffic	IP、ICMP。 UDP、 TCP および ARP プロトコルの統計を表示します。	PE
traceroute	特定ホストに通るルートパケットを表示します。	PE
ping	ネットワーク上で ICMP エコー要求パケットを他のノードへ送信します。	NE, PE

26.1.2 ip address

本コマンドでは、現在選択されている VLAN インタフェースの IPv4 アドレスを設定します。IP アドレスを削除するには、no 形式を使用してください。

構文

ip address {*ip-address netmask* [secondary]

[default-gateway *ip-address*] | bootp | dhcp}

no ip address [*ip-address netmask* [secondary] | dhcp]

ip-address - IIP アドレスです。

netmask - 関連 IP サブネットのネットワークマスクです。このマスクは、特定のサブネットへのルーティングに使用されるホストアドレスビットを識別します。ネットワークマスクは、伝統的なフォーマット xxx.xxx.xxx.xxx または/ 5 から/ 32 の範囲のクラスレスフォーマットを使用してください。たとえば、サブネット 255.255.224.0 は、/19 となります。

secondary - 二次 IP アドレスを特定します。

default-gateway - デフォルトゲートウェイです。

bootp - BOOTP から IP アドレスを取得します。

dhcp - DHCP から IP アドレスを取得します。

デフォルト設定

dhcp

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- ネットワーク経由での管理アクセスを取得するため、または既存の IP サブネットにルータを接続するには、このデバイスに IP アドレスを割当てる必要があります。特定の IP アドレスを手動で設定することも、ルータを BOOTP または DHCP サーバからアドレスを取得するように指示することもできます。有効な IP アドレスは、ピリオドで区切られた 0 から 255 の 4 つの数字で構成されます。このフォーマット以外のものは、設定プログラムによって受け入れられません。
- インタフェースでは 1 つの一次 IP アドレスしか持たないものの、多くの二次 IP アドレスを持つことができます。つまり、複数の IP サブネットにこのインタフェースでアクセスできる場合は、二次アドレスを指定する必要があります。一次 IP アドレスを設定する前に二次アドレスを設定することは出来ず、二次アドレスがまだ存在する場合は一次アドレスを削除できないことに留意してください。また、ネットワークセグメント内のルータ/スイッチが二次アドレスを使用する場合、そのセグメント内の他のすべてのルータ/スイッチも同じネットワークまたはサブネットアドレス空間の二次リアドレスを使用する必要があります。
- bootp または dhcp オプションを選択した場合、システムは BOOTP または DHCP を介してアドレス割当てを取得するように設定されたすべての VLAN のブロードキャストサービス要求を、直ちに開始します。IP は有効ですが、BOOTP または DHCP 応答が受信されるまで機能しません。要求は、IP アドレスを知るためにルータによって定期的にブロードキャストされます。(BOOTP および DHCP 値には、IP アドレス、デフォルトゲートウェイ、およびサブネットマスクを含めることができます) 。DHCP / BOOTP サーバの応答が遅い場合には、サービス要求のブロードキャストを再開するために ip dhcp restart client コマンドを使用するか、スイッチをリブートする必要があります。

Note: 各 VLAN グループは、それぞれの IP インタフェースアドレスに割当てることができます。スイッチをこれらの IP アドレスのいずれかを通じて、管理することができます。

例

以下の例では、デバイスに VLAN 1 のアドレスが割当てられています。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

この例では、クラスレスネットワークマスクを使用して、VLAN 2 に IP アドレスを割当てます。

```
Console(config)#interface vlan 2
Console(config-if)#ip address 10.2.2.1/24
Console(config-if)#
```

関連コマンド

ip dhcp restart client

ipv6 address

26.1.3 show ip interface

本コマンドでは、IPv4 インタフェースの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-12-E2-00-00-01
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
  Proxy ARP is disabled
  DHCP Client Vendor Class ID (text): AXprimoM210-08P
Console#
```

関連コマンド

ip address

show ipv6 interface

26.1.4 show ip traffic

本コマンドでは、IP、ICMP、 UDP、 TCP プロトコルの統計を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip traffic
IP Statistics:
```

```
IP received
               7845 total received
                    header errors
                    unknown protocols
                    address errors
                    discards
               7845 delivers
                    reassembly request datagrams
                    reassembly succeeded
                    reassembly failed
IP sent
                    forwards datagrams
               9903 requests
                    discards
                    no routes
                    generated fragments
                    fragment succeeded
                    fragment failed
ICMP Statistics:
ICMP received
                    input
                    errors
                    destination unreachable messages
                    time exceeded messages
                    parameter problem message
                    echo request messages
                    echo reply messages
                    redirect messages
                    timestamp request messages
                    timestamp reply messages
                    source quench messages
                    address mask request messages
                    address mask reply messages
ICMP sent
                    output
                    errors
                    destination unreachable messages
                    time exceeded messages
                    parameter problem message
                    echo request messages
                    echo reply messages
                    redirect messages
                    timestamp request messages
                    timestamp reply messages
                    source quench messages
                    address mask request messages
                    address mask reply messages
UDP Statistics:
                    input
```

```
                    no port errors
                    other errors
                    output
TCP Statistics:
                7841 input
                     input errors
                9897 output
Console#
```

26.1.5 traceroute

本コマンドでは、指定された宛先へのパケットのルートを表示します。

構文

traceroute *host*

host - ホストの IP アドレスまたはエイリアスです。

デフォルト設定

無し

コマンドモード

Privileged Exec

コマンドの使用方法

- traceroute コマンドを使用して、指定された宛先に到達するために必要なパスを特定します。
- 宛先が応答した際、最大タイムアウト(TTL)を超過した時、または最大ホップ数を超えた時にトレースが終了します。
- traceroute コマンドは、最初に TTL 値が 1 に設定されたプローブデータグラムを送信します。これにより、最初のルータはデータグラムを破棄しエラーメッセージを返します。トレース機能は、その後の各 TTL レベルでいくつかのプローブメッセージを送信し、各メッセージのラウンドトリップ時間を表示します。「ICMP port unreachable」メッセージを返すことによって、すべてのデバイスがプローブに正しく応答するわけではありません。応答が返される前にタイマーがオフになると、トレース機能は一連のアスタリスクと「Request Timed Out」メッセージを出力します。最大タイムアウトに達したときに終了するこれらのメッセージの長いシーケンスは、ターゲットデバイスでこの問題が発生している可能性があります。
- 対象デバイスが応答しない、またはその他のエラーが検出された場合には、スイッチは以下のいずれかのメッセージで示します:
  - * - 応答無し
  - H - ホストに到達できません
  - N - ネットワークに到達できません
  - P - プロトコルに到達しません。
  - O -その他

例

```
Console#traceroute 192.168.0.1
Press "ESC" to abort.
Traceroute to 192.168.0.99, 30 hops max, timeout is 3 seconds
Hop Packet 1 Packet 2 Packet 3 IP Address
--- -------- -------- -------- ---------------
  1    20 ms   <10 ms   <10 ms 192.168.0.99

Trace completed.
Console#
```

26.1.6 ping

本コマンドでは、(IPv4) ICMP エコー要求パケットをネットワーク上の他のノードへ送信します。

構文

ping *host* [count *count*] [size *size*]

host - ホストの IP アドレスまたはエイリアスです。

count - 送信するパケット数です。(範囲: 1 から 16)

size - パケット内でのバイト数です。(範囲: 32 から 512)

実際のパケットサイズは、スイッチがヘッダー情報を追加するため、指定されたサイズより 8 バイト大きくなります。

デフォルト設定

カウント: 5

サイズ: 32 バイト

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

- ping コマンドを使用して、ネットワーク上の他のサイトがネットワークに到達できるかを確認します。
- 以下は、ping コマンドのいくつかの結果です:
  - Normal response - 通常応答がネットワークのトラフィック状態に応じて、0 秒から 10 秒以内に発生します。
  - Destination does not respond - ホストが応答しない場合、“timeout”が 10 秒以内に表示されます。
  - Destination unreachable - 宛先のゲートウェイが、宛先に到達できないことを示しています。
  - Network or host unreachable - ゲートウェイは、ルートテーブルに対応するエントリが見つかりませんでした。
- ホスト名に ping を実行するときは、DNS サーバが定義されていて、ホスト名からアドレスへの変換が有効であることを確認してください。 必要に応じて、ローカルデバイスを DNS スタティックホスト

テーブルで指定することもできます。

例

```
Console#ping 10.1.0.9
Press ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

関連コマンド

interface

26.1.7 ARP のコマンド

本章では、アドレス解決プロトコル(ARP)をスイッチ上で設定するために使用するコマンドについて説明します。

表 26-4 アドレス解決プロトコルコマンド

コマンド	機能	モード
arp	ARP キャッシュ内で静的エントリを追加します。	GC
ip proxy-arp	プロキシ ARP サービスを有効にします。	IC
clear arp-cache	ARP キャッシュからすべての動的エントリを削除します。	PE
show arp	ARP キャッシュ内でエントリを表示します。	NE, PE

26.1.8 arp

本コマンドでは、アドレス解決プロトコル(ARP)キャッシュの中の静的エントリに追加します。キャッシュからエントリを削除するには、no 形式を使用してください。

構文

arp *ip-address hardware-address*

no arp *ip-address*

ip-address - 特定ハードウェアアドレスにマップするための IP アドレスです。

hardware-address - 特定 IP アドレスにマップするためのハードウェアアドレスです。(このアドレスのフォーマットは、xx-xx-xx-xx-xx-xx です。)

デフォルト設定

デフォルトエントリはありません。

コマンドモード

Global Configuration

コマンドの使用方法

- ARP キャッシュは、48 ビットハードウェア(例; メディアアクセスコントロール)に 32 ビット IP アドレスをマップするために使用されます。このキャッシュには、ルータ上で定義されたローカルネットワークインタフェースのホストおよび他のルータのエントリが含まれます。
- ARP キャッシュ内で許容された静的エントリの最大数は、8 です。
- ARP ブロードキャストメッセージに対して応答が無い場合、静的エントリの使用が必要になる場合があります。たとえば、アプリケーションのいくつかが ARP 要求に応答しない場合や、応答が極端に遅く、その結果ネットワーク操作がタイムアウトになってしまう場合です。
- 電源がリセットされた際、静的エントリはエージアウトも削除もされません。静的エントリは設定インタフェースを通じてのみ、削除されます。

例

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

関連コマンド

clear arp-cache

show arp

26.1.9 ip proxy-arp

本コマンドでは、プロキシアドレス解決プロトコル(ARP)を有効にします。プロキシ ARP を削除するには、no 形式を使用してください。

構文

[no] ip proxy-arp

デフォルト設定

無効

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- プロキシ ARP を使用すると、ルーティングしていないデバイスは別のサブネットまたはネットワーク

上のホストの MAC アドレスを判別することができます。

- プロキシ ARP を必要とするエンドステーションは、ネットワーク全体を単一のネットワークとして表示する必要があります。したがって、これらのノードは、ルータまたは他の関連ネットワークデバイスによって使用されるよりも小さなサブネットマスクを使用する必要があります。
- プロキシ ARP を広範囲に使用すると、ルータのパフォーマンスが低下する可能性があります。これは ARP トラフィックが増加し、大きな ARP アドレステーブルの検索時間が長くなるためです。

例

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

26.1.10 clear arp-cache

本コマンドでは、アドレス解決プロトコル(ARP)キャッシュから、すべての動的エントリを削除します。

コマンドモード

Privileged Exec

例

この例では、ARP キャッシュ内のすべての動的エントリをクリアします。

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Do you want to continue this operation (y/n)?
Console#
```

26.1.11 show arp

本コマンドでは、アドレス解決プロトコル(ARP)キャッシュ内のエントリを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンドの使用方法

- このコマンドでは、IP アドレス、MAC アドレス、タイプ(静的、動的、その他)、VLAN インタフェースなどの各 ARP キャッシュエントリが表示されます。エントリタイプ "other"は、このルータのローカルアドレスを示します。
- 静的エントリは、アップ状態の VLAN に対してのみ表示されます。つまり、既存の VLAN の IP サブネット用に設定されている場合にのみ静的エントリが表示され、その VLAN はリンクアップされています。
- ARP エントリの最大数は 64 です。静的エントリは最大 8 個、ダイナミックエントリは最大 48 個となります。また、タイプがその他のエントリに 8 個が予約されています。

◆ このテーブルは IPV6 ND と共有されているため、ARP の使用可能なエントリの合計が制限される可能性があります

例

この例では、ARP キャッシュ内のすべてのエントリを表示します。

```
Console#show arp

IP Address      MAC Address       Type      Interface
--------------- ----------------- --------- -----------
192.168.1.1     00-12-E2-93-82-A0 other     VLAN1
192.168.1.2     00-E0-4C-68-14-79 dynamic   VLAN1
145.30.20.23    09-50-40-30-20-10 dynamic   VLAN3

Total entry : 3
Console#
```

26.2 IPv6 インタフェース

本スイッチでは、次の IPv6 インタフェースコマンドをサポートします。

表 26-5 IPv6 設定コマンド

コマンド	機能	モード
インタフェースアドレス設定およびユーティリティ		
ipv6 default-gateway	既知のネクストホップが無いトラフィックに、IPv6 のデフォルトゲートウェイを設定します。	GC
ipv6 address	IPv6 グローバルユニキャストアドレスを設定し、インタフェースで IPv6 を有効にします。	IC
ipv6 address autoconfig	インタフェースで IPv6 アドレスの自動設定を有効にし、インタフェースで IPv6 を有効にします。	IC
ipv6 address eui-64	下位 64 ビットの中の EUI-64 インタフェースを使用して、インタフェースの IPv6 グローバルユニキャストアドレスを設定し、インタフェース上の IPv6 を有効にします。	IC
ipv6 address link-local	インタフェースの IPv6 リンクローカルアドレスを設定し、インタフェース上の IPv6 を有効にします。	IC
ipv6 enable	明示的な IPv6 アドレスで設定されていないインタフェースで、IPv6 を有効にします。	IC
ipv6 mtu	インタフェース上で送信される IPv6 パケットの最大伝送ユニット(MTU)のサイズを設定します。	IC
show ipv6 default-gateway	現在の IPv6 デフォルトゲートウェイを表示します。	PE
show ipv6 interface	IPv6 インタフェースの可用性と、構成された設定を表示します。	PE
show ipv6 mtu	IPv6 インタフェースの最大伝送ユニット(MTU)情報を表示します。	PE
show ipv6 traffic	IPv6 トラフィックに関する統計を表示します。	PE
clear ipv6 traffic	IPv6 トラフィックカウンタをリセットします。	PE
ping6	IPv6 ICMP エコー要求パケットをネットワーク上の他のノードに送信します。	PE
traceroute6	特定ホストに通るルートパケットを表示します。	PE
近隣探索		
ipv6 nd dad attempts	重複アドレス検出中にインタフェース上で送信される連続する近隣送信要求メッセージの数を設定します。	IC
ipv6 nd ns-interval	インタフェース上の IPv6 近隣送信要求の再送信間隔を設定します。	IC
ipv6 nd reachable-time	到達可能性の確認イベントが発生した後に、リモート IPv6 ノードが到達可能であるとみなされる時間を設定します。	IC
clear ipv6 neighbors	IPv6 近隣探索キャッシュ内のすべての動的エントリを削除します。	PE
show ipv6 neighbors	IPv6 近隣探索キャッシュ内の情報を表示します。	PE

26.2.1 ipv6 default-gateway

本コマンドでは、既知のネクストホップがない宛先に使用する IPv6 デフォルトゲートウェイを設定します。以前に設定されたデフォルトゲートウェイを削除するには、no 形式を使用してください。

構文

ipv6 default-gateway *ipv6-address*

no ipv6 address

ipv6-address - 既知のネクストホップがない宛先に使用する、デフォルトネクストホップルータの IPv6 アドレスです。

デフォルト設定

デフォルトゲートウェイは定義されていません。

コマンドモード

Global Configuration

コマンドの使用方法

- すべての IPv6 アドレスは、コロンで区切られた 16 ビットの 16 進数値を使用して、RFC 2373「IPv6 アドレッシングアーキテクチャ」に準拠している必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。
- 同じリンクローカルアドレスは、異なるゾーン(RFC 4007)の異なるインタフェース/ノードによって使用されます。したがって、リンクローカルアドレスを指定する場合は、%デリミタの後に VLAN 識別子を示す zone-id 情報を含めます。たとえば、FE80::7272%1 は VLAN 1 をインタフェースとして識別します。
- 異なる IP セグメントにある IPv6 アドレスを宛先が割当てている場合には、IPv6 デフォルトゲートウェイを定義する必要があります。
- スイッチ上で設定されているゲートウェイに、ネットワークインタフェースが直接接続されている場合のみ、IPv6 デフォルトゲートウェイは正常に設定することができます。

例

以下の例では、本デバイスのデフォルトゲートウェイを定義します。

```
Console(config)#ipv6 default-gateway FE80::269:3EF9:FE19:6780%1
Console(config)#
```

関連コマンド

show ipv6 default gateway

26.2.2 ipv6 address

本コマンドでは、IPv6 グローバルユニキャストアドレスを設定し、インタフェース上で IPv6 を有効にします。すべての IPv6 アドレスをインタフェースから削除するには、引数なしで no 形式を使用するか、インタフェースからそのアドレスを削除するには、特定の IPv6 アドレスとともに no 形式を使用してください。

構文

[no] ipv6 address *ipv6-address*/*prefix-length*

ipv6-address - ネットワークプレフィックスおよびホストアドレスビットを含む、完全 IPv6 アドレスです。

prefix-length - アドレスのいくつの連続ビット(左から)がプレフィックス(例; アドレスのネットワーク部分)を構成するかを示す 10 進数です。

デフォルト設定

IPv6 アドレスは定義されていません。

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- すべての IPv6 アドレスは、コロンで区切られた 16 ビットの 16 進数値を使用して、RFC 2373「IPv6 アドレッシングアーキテクチャ」に準拠している必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。
- 複数のサブネットを持つ大規模なネットワークに接続するには、グローバルユニキャストアドレスを設定する必要があります。　このアドレスは、このコマンドを使用して手動で設定することも、また ipv6 address auto config コマンドを使用して自動的に設定することもできます。
- リンクローカルアドレスがこのインタフェースにまだ割当てられていない場合、このコマンドは指定された静的グローバルユニキャストアドレスを割当て、インタフェースのリンクローカルユニキャストアドレスも動的に生成します。(リンクローカルアドレスは、FE80 のアドレスプレフィックスと、変更された EUI-64 形式のスイッチの MAC アドレスにもとづくホスト部分で作成されます)。
- 重複したアドレスが検出された場合、コンソールに警告メッセージが送信されます。

例

この例では、完全な IPv6 アドレスとプレフィックス長を指定します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::72/96
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  fe80::7272:cfff:fe83:3466%1/64
Global unicast address(es):
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
ff02::1:ff00:72
ff02::1:ff83:3466
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
```

```
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

関連コマンド

ipv6 address eui-64

ipv6 address autoconfig

show ipv6 interface

ip address

26.2.3 ipv6 address autoconfig

本コマンドにより、インタフェース上で IPv6 アドレスのステートレス自動設定を有効にし、インタフェース上で IPv6 を有効にします。アドレスのネットワーク部分は、IPv6 ルータ通知メッセージで受信されたプレフィックスにもとづいています。ホスト部分は、インタフェース識別子(例; スイッチの MAC アドレス)が変更された EUI-64 形式にもとづいています。このコマンドで生成されたアドレスを削除するには、no 形式を使用してください。

構文

[no] ipv6 address autoconfig

デフォルト設定

IPv6 アドレスは定義されていません。

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- リンクローカルアドレスがこのインタフェースに割当てられていない場合、このコマンドはインタフェースの動的にグローバルユニキャストアドレス(グローバルプレフィックスが受信したルータアドバタイズメントに含まれている場合)とリンクローカルアドレスを生成します。(リンクローカルアドレスは、FE80 のアドレスプレフィックスと、変更された EUI-64 形式のスイッチの MAC アドレスにもとづくホスト部分で作成されます)。
- 重複したアドレスが検出された場合、コンソールに警告メッセージが送信されます。
- DHCPv6 を再起動すると、スイッチはステートフルアドレス自動設定によって IP アドレスプレフィックスを取得しようとします。ルータアドバタイズメントに「その他のステートフルコンフィグレーション」フラグが設定されている場合、スイッチは DHCPv6 が再起動された際に、DHCPv6 サーバから他の非アドレス設定情報(デフォルトゲートウェイ等)を取得しようとする場合もあります

例

この例では、動的グローバルユニキャストアドレスをスイッチに割当てます。

```
Console(config-if)#ipv6 address autoconfig
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale
Link-local address:
  fe80::7272:cfff:fe83:3466%1/64
Global unicast address(es):
  2001:db8:2222:7272:7272:cfff:fe83:3466/64, subnet is 2001:db8:2222:7272::/64
    valid lifetime 2591531 preferred lifetime 604331
Joined group address(es):
ff02::1:ff83:3466
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

関連コマンド

ipv6 address

show ipv6 interface

26.2.4 ipv6 address eui-64

本コマンドでは、下位 64 ビットの EUI-64 インタフェース ID を使用してインタフェースの IPv6 アドレスを設定し、インタフェースで IPv6 を有効にします。すべての手動設定済み IPv6 アドレスをインタフェースから削除するには、引数無しで no 形式を使用します。インタフェースから削除するには、特定のアドレスの no 形式を使用してください。

構文

ipv6 address *ipv6-prefix*/*prefix-length* eui-64

no ipv6 address [*ipv6-prefix*/*prefix-length* eui-64]

ipv6-prefix - インタフェースに割当てられているアドレスの IPv6 ネットワーク部分です。

prefix-length - アドレスのいくつの連続ビット(左から)がプレフィックス(例; アドレスのネットワーク部分)を構成するかを示す 10 進数です。

デフォルト設定

IPv6 アドレスは定義されていません。

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- プレフィックスは、コロンで区切られた 16 ビットの 16 進数値を使用して RFC 2373「IPv6 アドレス指定アーキテクチャ」に従ってフォーマットする必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。
- リンクローカルアドレスがこのインタフェースに未だ割当てられていない場合、コマンドがインタフェースの動的にグローバルユニキャストアドレスとリンクローカルアドレスを生成します。(リンクローカルアドレスは、アドレスプレフィックスが FE80 でスイッチの MAC アドレスにもとづくホスト部分が変更された EUI-64 フォーマットで作成されます)
- 指定されたプレフィックス長が 64 ビット未満の場合、ipv6-prefix に指定された値に高次ホストビットの一部が含まれることに留意してください。指定されたプレフィックス長が 64 ビットを超える場合、アドレスのネットワーク部分がインタフェース識別子よりも優先されます。
- 重複したアドレスが検出された場合、コンソールに警告メッセージが送信されます。
- IPv6 アドレスは 16 バイト長で、そのうちの 8 バイトは通常デバイスの MAC アドレスにもとづいて一意のホスト識別子を形成します。EUI-64 仕様は、拡張 8 バイトの MAC アドレスを使用するデバイス向けに設計されています。6 バイトの MAC アドレス(EUI-48 フォーマットとも呼ばれます)を使用するデバイスの場合は、アドレスのユニバーサル/ローカルビットを反転し、16 進数の FFFE を MAC アドレスの上位と下位 3 バイトの間に挿入して、EUI-64 フォーマットに変換する必要があります。
- たとえば、デバイスの EUI-48 アドレスが 28-9F-18-1C-82-35 の場合、EUI-64 要件を満たすためにグローバル/ローカルビットを最初に反転する必要があります(例; グローバルに定義されている場合には、1 アドレスは 0、ローカル定義アドレスは 0)、28 を 2A に変更します。次に、2 バイトの FFFE が OUI(例; 企業 id)と残りのアドレスとの間に挿入され、修正された EUI-64 インタフェース識別子が 2A-9F-18-FF-FE-1C-82-35 となります。
- このホストアドレス方式では、これらのインタフェースが異なるサブネットに接続されている場合、同じインタフェース識別子を 1 つのデバイスの複数の IP インタフェースで使用することができます。

例

この例では、ネットワークプレフィックス 2001：0DB8：0：1::/64 を使用し、アドレスの下位 64 ビットで使用される EUI-64 インタフェース識別子を指定します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  fe80::7272:cfff:fe83:3466%1/64
Global unicast address(es):
  2001:db8:0:1:7272:cfff:fe83:3466/64, subnet is 2001:db8:0:1::/64[EUI]
```

```
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
ff02::1:ff00:72
ff02::1:ff83:3466
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

関連コマンド

ipv6 address autoconfig

show ipv6 interface

26.2.5 ipv6 address link-local

本コマンドでは、インタフェースの IPv6 リンクローカルアドレスを設定し、インタフェースで IPv6 を有効にします。すべての手動設定済み IPv6 アドレスをインタフェースから削除するには、引数無しで no 形式を使用します。インタフェースから削除するには、特定のアドレスの no 形式を使用してください。

構文

ipv6 address *ipv6-address* link-local

no ipv6 address [*ipv6-address* link-local]

ipv6-address - インタフェースに割当てられた IPv6 アドレスです。

デフォルト設定

IPv6 アドレスは定義されていません。

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- 指定されたアドレスは、RFC 2373「IPv6 アドレッシングアーキテクチャ」に準拠して、コロンで区切られた 8 つの 16 ビット 16 進数を使用してフォーマットする必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。また、アドレスプレフィックスは FE80 から FEBF の範囲内になければなりません。
- このコマンドで特定されたアドレスは、インタフェースで自動的に生成されたリンクローカルアドレスを置換します。
- インタフェースごとに複数の IPv6 グローバルユニキャストアドレスを設定することができます。しか

しながら、1 つのインタフェースに対し 1 つのリンクローカルアドレスのみとなります。

◆ 重複したアドレスが検出された場合、コンソールに警告メッセージが送信されます。

例

この例では、リンクローカルアドレス FE80 :: 269：3EF9：FE19：6779 を VLAN 1 に割当てます。リンクローカルアドレスには、FE80 から FEBF の範囲内のプレフィックスが必要となります。 0269 の形式でホストアドレスの最初の 16 ビットグループに 0 が埋め込まれます。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
  2001:db8:0:1:7272:cfff:fe83:3466/64, subnet is 2001:db8:0:1::/64[EUI]
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
ff02::1:ff19:6779
ff02::1:ff00:72
ff02::1:ff83:3466
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

関連コマンド

ipv6 enable

show ipv6 interface

26.2.6 ipv6 enable

本コマンドでは、IPv6 アドレスが明示的に設定されていないインタフェースで IPv6 を有効にします。明示的な IPv6 アドレスを設定されていないインタフェースで IPv6 を無効にするには、no 形式を使用してください。

構文

[no] ipv6 enable

デフォルト設定

IPv6 は無効です。

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- このコマンドでは、現在の VLAN インタフェースで IPv6 を有効にし、自動的にリンクローカルのユニキャストアドレスを生成します。アドレスプレフィックスは FE80 を使用し、アドレスのホスト部分は、スイッチの MAC アドレスを変更された EUI-64 フォーマットに変換することによって生成されます(ipv6 address eui-64 を参照)。このアドレスタイプを使用すると、同じローカルサブネットに接続されているすべてのデバイスのスイッチが、IPv6 経由でアクセス可能になります。
- ローカルセグメントにおいて重複したアドレスが検出された場合、インタフェースは無効となり、コンソールに警告メッセージが表示されます。
- no ipv6 enable コマンドは、IPv6 アドレスで明示的に設定されているインタフェースの IPv6 を無効にしません。

例

この例では、IPv6 は VLAN 1 で有効にされ、リンクローカルアドレス FE80::2E0:CFF:FE00:FD/64 は、スイッチで自動的に生成されます。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
  2001:db8:0:1:7272:cfff:fe83:3466/64, subnet is 2001:db8:0:1::/64[EUI]
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
ff02::1:ff19:6779
ff02::1:ff00:72
ff02::1:ff83:3466
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

関連コマンド

ipv6 address link-local

show ipv6 interface

26.2.7 ipv6 mtu

本コマンドでは、インタフェース上で送信された IPv6 パケットの最大伝送ユニット(MTU)サイズを設定します。デフォルト設定を復元するには、デフォルト値を設定してください、

構文

ipv6 mtu *size*

size - MTU サイズを指定します。(範囲: 1280 から 65535 バイト)

デフォルト設定

1500 バイト

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- 非デフォルト値が設定された場合、MTU オプションがデバイスから送信されたルータアドバタイズメントに含まれます。
- コマンドによって設定された最大値は、現在 1500 バイトで固定されている物理インタフェースの MTU を超過することはできません。
- IPv6 ルータは、他のルータから転送された IPv6 パケットを断片化しません。ただし、IPv6 ルータに接続されたエンドステーションから発信されるトラフィックは断片化する可能性があります。
- 同じ物理メディアのすべてのデバイスは、正確に作動させるために同じ MTU を使用する必要があります。
- IPv6 は、MTU を設定する前にインタフェース上で有効にする必要があります。

例

以下の例では、VLAN 1 用の MTU を 1280 バイトに設定します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mtu 1280
Console(config-if)#
```

関連コマンド

show ipv6 mtu

jumbo frame

26.2.8 show ipv6 default-gateway

本コマンドでは、現在の IPv6 デフォルトゲートウェイを表示します。

コマンドモード

Normal Exec, Privileged Exec

例

以下では、デバイスのために設定したデフォルトゲートウェイを表示します。

```
Console#show ipv6 default-gateway
IPv6 default gateway 2001:DB8:2222:7272::254

Console#
```

26.2.9 show ipv6 interface

本コマンドでは、IPv6 インタフェースの可用性とコンフィグレーションを表示します。

構文

show ipv6 interface [brief [vlan *vlan-id* [*ipv6-prefix*/*prefix-length*]]]

brief - IPv6 の動作ステータスと、各インタフェースに設定されているアドレスの概要を表示します。

vlan-id - VLAN ID です。 (範囲: 1 から 4093)

ipv6-prefix - インタフェースに割当てられているアドレスの IPv6 ネットワーク部分です。プレフィックスは、コロンで区切られた 16 ビットの 16 進数値を使用して RFC 2373「IPv6 アドレス指定アーキテクチャ」に従ってフォーマットする必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。

prefix-length - アドレスの連続したビット(左から)が、プレフィックス(例; アドレスのネットワーク部分)を何個含んでいるかを示す 10 進数です。

コマンドモード

Privileged Exec

例

この例では、スイッチのために設定したすべての IPv6 アドレスを表示します。

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
  2001:db8:0:1:7272:cfff:fe83:3466/64, subnet is 2001:db8:0:1::/64[EUI]
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
```

```
Joined group address(es):
ff02::1:ff19:6779
ff02::1:ff00:72
ff02::1:ff83:3466
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

表 26-6 show ipv6 interface - 表示の説明

フィールド	説明
VLAN	VLAN がこのインタフェースでパケットを送受信できる場合は「up」、回線信号がない場合は「down」、管理者がインタフェースを無効にしている場合には「administratively down」と表示されます。
IPv6	スイッチがこのインタフェースで IP トラフィックを送受信できる場合、IPv6 は「有効」、このインタフェースで IP トラフィックを送受信できない場合には「無効」、あるいはインタフェースで重複するリンクローカルアドレスが検出された場合は「停止」とマークされます。
Link-local address	インタフェースに割当てられた、リンクローカルアドレスが表示されます。
Global unicast address(es)	インタフェースに割当てられた、グローバルユニキャストアドレスが表示されます。
Joined group address(es)	スコープ 1(インタフェースローカル）とスコープ 2(リンクローカル)のすべての IPv6 ノードに対して、ノードはマルチキャストアドレス FF01::1 と FF02::1 をすべて参加させる必要があります。 FF01::1/16 は、接続されたすべての IPv6 ノードの一時的なインタフェースローカルマルチキャストアドレスであり、FF02::1/16 は、接続されたすべての IPv6 ノードのリンクローカルマルチキャストアドレスです。インタフェースローカルマルチキャストアドレスは、マルチキャストトラフィックのループバック送信にのみ使用されます。リンクローカルマルチキャストアドレスは以下に説明するように、すべてのノード（FF02::1）、すべてのルータ（FF02::2）、および要請されたノード（FF02::1:FFXX:XXXX）を含むリンクローカルユニキャストアドレスで使用されるのと同じタイプをカバーします。 またノードは、それが割当てられているすべてのユニキャストおよびエニキャストアドレスについて、関連する要求ノードマルチキャストアドレスを計算して参加させる必要があります。上位ビットのみが異なる IPv6 アドレスとなります。 異なるアグリゲーションに関連付けられた複数の上位プレフィックスが同じ要請ノードアドレスにマッピングされるため、ノードが参加する必要があるマルチキャストアドレスの数が減少します。この例では、FF02::1:FF90:0/104 はアドレスの下位 24 ビットを取り、それらのビットをプレフィックスに付加することによって形成される要請ノードマルチキャストアドレスです。
ND DAD	(近隣探索)重複アドレス検出が有効になっているかを示します。
number of DAD attempts	重複アドレス検出中にインタフェース上で送信された、連続する近隣送信

フィールド	説明
	メッセージの数です。
ND retransmit interval	重複アドレス検出中にインタフェース上で送信された、IPv6 近隣送信要請の再送信間隔です。
ND advertised retransmit interval	再送信間隔は、同じリンク上のノードが同じ時刻値を使用するように、インタフェースから送信されたすべてのルータアドバタイズメントに含まれます。
ND reachable time	到達可能性確認イベントが発生した後に、リモート IPv6 ノードが到達可能であるとみなされる時間です。
ND advertised reachable time	到達可能時間は、同じリンク上のノードが同じ時間値を使用するように、インタフェースから送信されたすべてのルータ通知に含まれます。
ND advertised router lifetime	プレフィックスがオンリンク判定に有効である時間の長さです。

この例では、スイッチ上で設定された IPv6 の概要が表示されます。

```
Console#show ipv6 interface brief
Interface       VLAN       IPv6       IPv6 Address
--------------- ---------- ---------- ------------------------------------
VLAN 1          Up         Up         2001:DB8:2222:7273::72/96
VLAN 1          Up         Up         FE80::2E0:CFF:FE00:FD%1/64
Console#
```

関連コマンド

show ip interface

26.2.10 show ipv6 mtu

本コマンドでは、このスイッチに受け入れ可能な MTU と共に ICMP パケットが大きすぎるメッセージを返す宛先の最大伝送ユニット(MTU)キャッシュを表示します。

コマンドモード

Normal Exec, Privileged Exec

例

以下の例ではこのデバイスの MTU キャッシュを表示します。

```
Console#show ipv6 mtu
MTU     Since   Destination Address
1400    00:04:21  5000:1::3
1280    00:04:50  FE80::203:A0FF:FED6:141D
Console#
```

表 26-7 show ipv6 mtu - 表示の説明※

フィールド	説明
MTU	この宛先から返された ICMP パケットの大きすぎるメッセージに含まれる調整済みの MTU です。このパスに沿って送信されたすべてのトラフィックに使用されるようになりました。
Since	この宛先から ICMP パケットが大きすぎるメッセージを受信してからの経過時間です。
Destination Address	ICMP パケットが大きすぎるメッセージを送信したアドレスです。

注※ このスイッチに IPv6 が割当てられていない場合には、情報が表示されません。

26.2.11 show ipv6 traffic

本コマンドでは、スイッチを介して通過する IPv6 トラフィックの統計を表示します。

コマンドモード

Privileged Exec

例

以下の例では、すべての IPv6 ユニキャストトラフィック、マルチキャストトラフィック、および ICMP、UDP、および TCP 統計情報を表示します。

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received
                  3 total received
                    header errors
                    too big errors
                    no routes
                    address errors
                    unknown protocols
                    truncated packets
                    discards
                    delivers
                    reassembly request datagrams
                    reassembly succeeded
                    reassembly failed
IPv6 sent
                    forwards datagrams
                  6 requests
                    discards
                    no routes
                    generated fragments
                    fragment succeeded
                    fragment failed
ICMPv6 Statistics:
ICMPv6 received
                    input
```

```
                    errors
                    destination unreachable messages
                    packet too big messages
                    time exceeded messages
                    parameter problem message
                    echo request messages
                    echo reply messages
                    router solicit messages
                    router advertisement messages
                    neighbor solicit messages
                    neighbor advertisement messages
                    redirect messages
                    group membership query messages
                    group membership response messages
                    group membership reduction messages
ICMPv6 sent
                  6 output
                    destination unreachable messages
                    packet too big messages
                    time exceeded messages
                    parameter problem message
                    echo request messages
                    echo reply messages
                  3 router solicit messages
                    router advertisement messages
                  3 neighbor solicit messages
                    neighbor advertisement messages
                    redirect messages
                    group membership query messages
                    group membership response messages
                    group membership reduction messages
UDP Statistics:
                    input
                    no port errors
                    other errors
                    output
Console#
```

表 26-8 show ipv6 traffic - 表示の説明

フィールド	説明
IPv6 Statistics	
IPv6 received	
total received	エラーで受信したデータグラムを含む、インタフェースによって受信された入力データグラムの総数です。
header errors	バージョン番号の不一致、その他のフォーマットエラー、ホップ数超過、IPv6 オプション等、IPv6 ヘッダーエラーのために破棄された入力データグラムの数です。

フィールド	説明
too big errors	サイズが送信インタフェースのリンク MTU を超過したために転送できなかった、入力データグラムの数です。
no routes	送信先に送信する経路が見つからなかったために破棄された、入力データグラムの数です。
address errors	IPv6 ヘッダーの宛先フィールドの IPv6 アドレスがこのエンティティで受信される有効なアドレスでなかったために廃棄された入力データグラムの数です。このカウントには、無効なアドレス（例：:: 0）とサポートされていないアドレス(未割当てのプレフィックスを持つアドレス等)が含まれます。IPv6 ルータではないため、データグラムを転送しないエンティティの場合、このカウンタには宛先アドレスがローカルアドレスではないため、廃棄されたデータグラムが含まれます。
unknown protocols	正常に受信されたものの未知、またはサポートされていないプロトコルのために破棄された、ローカルにアドレス指定されたデータグラムの数です。このカウンタは、これらのデータグラムがアドレス指定されたインタフェースで増分されます。これらのデータグラムは、必ずしもデータグラムの一部の入力インタフェースではない可能性があります。
truncated packets	データグラムフレームに十分なデータが格納されていないために破棄された、入力データグラムの数です。
discards	継続的な処理を妨げるような問題は発生しなかったものの、廃棄された(例; バッファスペースが不足している)入力 IPv6 データグラムの数です。このカウンタには、再組み立てを待つ間に破棄されたデータグラムは含まれないことに留意してください。
delivers	IPv6 ユーザプロトコル(ICMP を含む)に正常に配信されたデータグラムの総数です。このカウンタは、これらのデータグラムがアドレス指定されたインタフェースで増分されます。これらのデータグラムは、必ずしもデータグラムの一部の入力インタフェースではない可能性があります。
reassembly request datagrams	受信した IPv6 フラグメントの数です。このインタフェースで再構成する必要があります。このカウンタはこれらのフラグメントがアドレス指定されたインタフェースで増分されます。これらのフラグメントは、必ずしも一部のフラグメントの入力インタフェースではない可能性があります。
reassembly succeeded	IPv6 データグラムの数が正常に再構成されています。このカウンタは、これらのデータグラムがアドレス指定されたインタフェースで増分されます。これらのデータグラムは、必ずしも一部のフラグメントの入力インタフェースではない可能性があります。
reassembly failed	IPv6 再構成アルゴリズムによって検出された障害の数です(何らかの理由でタイムアウト、エラー等)。これは、一部のアルゴリズム(特に RFC 815 のアルゴリズム)がフラグメントの数を受信時に組み合わせて追跡できなくなるため、必ずしも廃棄された IPv6 フラグメントの数ではありません。このカウンタは、これらのフラグメントがアドレス指定されたインタフェースで増分されるものの、一部のフラグメントの入力インタフェースではない可能性があります。
IPv6 sent	
forwards datagrams	このエンティティが受信し最終宛先に転送した出力データグラムの数です。IPv6 ルータとして機能しないエンティティでは、このカウンタにはこのエンティティ経由で送信元ルーティングされたパケットのみが含まれ、送信元ルート処理は成功しています。転送されたデータグラムが正常に転送された場合、発信インタフェースのカウンタが増分されることに留意してください。
requests	ローカル IPv6 ユーザプロトコル(ICMP を含む)が送信要求で IPv6 に提供された IPv6 データグラムの総数です。このカウンタには、ipv6IfStatsOutForwDatagrams でカウントされたデータグラムは含まれません。
discards	送信先への送信を妨げるような問題は発生しなかったものの、廃棄された(例; バッファスペースが不足している)出力 IPv6 データグラムの数です。このカウンタは、このようなパケットがこの(任意の)破棄基準を満たしていれば、

フィールド	説明
	ipv6IfStatsOutForwDatagrams でカウントされたデータグラムを含むことに留意してください。
no routes	送信先に送信する経路が見つからなかったために破棄された、入力データグラムの数です。
generated fragments	この出力インタフェースでフラグメンテーションの結果生成された、出力データグラムフラグメントの数です。
fragment succeeded	この出力インタフェースで正常に断片化された、IPv6 データグラムの数です。
fragment failed	この出力インタフェースでフラグメント化する必要があったものの、破棄できなかったために破棄された IPv6 データグラムの数です。
ICMPv6 Statistics	
ICMPv6 received	
input	ipv6IfIcmpInErrors でカウントされたすべての ICMP メッセージを含むインタフェースによって受信された ICMP メッセージの総数です。このインタフェースは ICMP メッセージがアドレス指定されたインタフェースであり、必ずしもメッセージの入力インタフェースではない可能性があることに注意してください。
errors	インタフェースが受信したが ICMP 固有のエラー(不良 ICMP チェックサム、長さの不良等)があると判断した、ICMP メッセージの数です。
destination unreachable messages	インタフェースによって受信された、ICMP Destination Unreachable メッセージの数です。
packet too big messages	インタフェースによって受信された、ICMP Packet Too Big メッセージの数です。
time exceeded messages	インタフェースによって受信された、ICMP Time Exceeded メッセージの数です。
parameter problem message	インタフェースによって受信された、ICMP Parameter Problem メッセージの数です。
echo request messages	インタフェースによって受信された、ICMP Echo (要求)メッセージの数です。
echo reply messages	インタフェースによって受信された、ICMP Echo Reply メッセージの数です。
router solicit messages	インタフェースによって受信された、ICMP Router Solicit メッセージの数です、
router advertisement messages	インタフェースによって受信された、ICMP Router Advertisement メッセージの数です。
neighbor solicit messages	インタフェースによって受信された、ICMP Neighbor Solicit メッセージの数です。
neighbor advertisement messages	インタフェースによって受信された、ICMP Neighbor Advertisement メッセージの数です。
redirect messages	インタフェースによって受信された、Redirect メッセージの数です。このインタフェースで受信した休暇メッセージの数です。
group membership query messages	インタフェースによって受信された、ICMPv6 Group Membership Query メッセージの数です。
group membership response messages	インタフェースによって受信された、ICMPv6 Group Membership Response メッセージの数です。
group membership reduction messages	インタフェースによって受信された、ICMPv6 Group Membership Reduction メッセージの数です。
multicast listener discovery version 2	インタフェースによって受信された、MLDv2 レポートの数です。

フィールド	説明
reports	
ICMPv6 sent	
output	このインタフェースが送信しようとした ICMP メッセージの総数です。このカウンタには、icmpOutErrors でカウントされたすべてのカウンタが含まれていることに留意してください。
destination unreachable messages	インタフェースによって送信された、ICMP Destination Unreachable、メッセージの数です。
packet too big messages	インタフェースによって送信された、ICMP Packet Too Big メッセージの数です。
time exceeded messages	インタフェースによって送信された、ICMP Time Exceeded メッセージの数です。
parameter problem message	インタフェースによって送信された、ICMP Parameter Problem メッセージの数です。
echo request messages	インタフェースによって送信された、ICMP Echo (要求)メッセージの数です。
echo reply messages	インタフェースによって送信された、ICMP Echo Reply メッセージの数です。
router solicit messages	インタフェースによって送信された、ICMP Router Solicitation メッセージの数です。
router advertisement messages	インタフェースによって送信された、ICMP Router Advertisement メッセージの数です。
neighbor solicit messages	インタフェースによって送信された、ICMP Neighbor Solicit メッセージの数です。
neighbor advertisement messages	インタフェースによって送信された、ICMP Router Advertisement メッセージの数です。
redirect messages	送信された Redirect メッセージの数です。ホストについては、ホストはリダイレクトを送信しないため、このオブジェクトは常に 0 となります。
group membership query messages	インタフェースによって送信された、ICMPv6 Group Membership Query メッセージの数です。
group membership response messages	送信された ICMPv6 Group Membership Response メッセージの数です。
group membership reduction messages	送信された ICMPv6 Group Membership Reduction メッセージの数です。
multicast listener discovery version 2 reports	インタフェースによって送信された、MLDv2 レポートの数です。
UDP Statistics	
input	UDP ユーザに運ばれた UDP データグラムの総数です。
no port errors	宛先ポートにアプリケーションが無かった受信 UDP データグラムの総数です。
other errors	宛先ポートでのアプリケーションの不足以外の理由で配信できなかった、受信 UDP データグラムの数です。
output	エンティティから送信された UDP データグラムの総数です。

26.2.12 clear ipv6 traffic

本コマンドでは、IPv6 トラフィックカウンタをリセットします。

コマンドモード

Privileged Exec

コマンドの使用方法

本コマンドでは、show ipv6 traffic コマンドで表示されたすべてのカウンタをリセットします。

例

```
Console#clear ipv6 traffic
Console#
```

26.2.13 ping6

本コマンドでは、(IPv6) ICMP エコ要求パケットをネットワーク上の他のノードへ送信します。

構文

ping6 {*ipv6-address* | *host-name*} [count *count*] [size *size*]

ipv6-address - 近隣デバイスの IPv6 アドレスです。コロンで区切られた 16 ビットの 16 進数の 8 つの値を使用して、RFC 2373「IPv6 アドレッシングアーキテクチャ」に準拠してフォーマットされたリンクローカル、またはグローバルのユニキャストアドレスを指定することができます。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。

host-name - ドメイン名で IPv6 アドレスに解決できるホスト名文字列です。

count - 送信するパケット数です。(範囲: 1 から 16)

size - パケット内でのバイト数です。(範囲: 0 から 1500 バイト)

実際のパケットサイズはルータがヘッダー情報を追加するため、指定されたサイズより 8 バイト大きくなります。

デフォルト設定

カウント: 5

サイズ: 32 バイト

コマンドモード

Privileged Exec

コマンドの使用方法

- ping6 コマンドを使用して、ネットワーク上の他のサイトが到達可能かを確認します。または、パスを介して遅延を評価します。
- 同一のリンクローカルアドレスは、異なるゾーン(RFC4007)の違ったインタフェース/ノードによって使用される可能性があります。したがって、リンクローカルアドレスを指定する場合は、%デリミタの後に VLAN 識別子を示す zone-id 情報を含めます。たとえば、FE80 :: 7272%1 は、ping が送信されるインタフェースとして VLAN 1 を識別します。

- ホスト名に ping を実行する場合は、DNS サーバが有効になっていることを確認してください。必要に応じて、ローカルデバイスを DNS スタティックホストテーブルで指定することもできます。
- ホスト名と一緒に ping6 を使用する際、スイッチは最初に IPv4 アドレスに解決する前にエイリアスを IPv6 アドレスに解決しようとします。

例

```
Console#ping6 FE80::2E0:CFF:FE00:FC%1
Press ESC to abort.
PING to FE80::2E0:CFF:FE00:FC%1/64, by 5 32-byte payload ICMP packets, timeout is 3 seconds
response time: 20 ms    [FE80::2E0:CFF:FE00:FC] seq_no: 1
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 2
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 3
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 4
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 5
Ping statistics for FE80::2E0:CFF:FE00:FC%1/64:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 20 ms, Average = 4 ms
Console#
```

26.2.14 traceroute6

本コマンドでは、パケットが指定された宛先に送信されるルートを表示します。

構文

traceroute6 *ipv6-address* [max-failures *failure-count*]

ipv6-address - 近隣デバイスの IPv6 アドレスです。コロンで区切られた 16 ビットの 16 進数の 8 つの値を使用して、RFC 2373「IPv6 アドレッシングアーキテクチャ」に準拠してフォーマットされたリンクローカル、またはグローバルのユニキャストアドレスを指定することができます。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。

failure-count - トレースルートが終了するまでの最大失敗回数です。(範囲: 1 から 255)

デフォルト設定

最大失敗数: 5

コマンドモード

Privileged Exec

コマンドの使用方法

- traceroute6 コマンドを使用して、指定された宛先に到達するために必要なパスを判別します。
- 同じリンクローカルアドレスは、異なるゾーン(RFC 4007)の異なるインタフェース/ノードによって使用されます。したがって、リンクローカルアドレスを指定する場合は、%デリミタの後に VLAN 識別子を示す zone-id 情報を含めます。たとえば、FE80 :: 7272%1 は、ping が送信されるインタフェースと

して VLAN 1 を識別します。

- 宛先が応答した際、最大タイムアウト(TTL)を超過した時、または最大ホップ数を超えた時にトレースが終了します。
- traceroute コマンドは、最初に TTL 値が 1 に設定されたプローブデータグラムを送信します。これにより、最初のルータはデータグラムを破棄しエラーメッセージを返します。トレース機能は、その後の各 TTL レベルでいくつかのプローブメッセージを送信し、各メッセージのラウンドトリップ時間を表示します。「ICMP port unreachable」メッセージを返すことによって、すべてのデバイスがプローブに正しく応答するわけではありません。応答が返される前にタイマーがオフになると、トレース機能は一連のアスタリスクと「Request Timed Out」メッセージを出力します。最大タイムアウトに達したときに終了するこれらのメッセージの長いシーケンスは、ターゲットデバイスでこの問題が発生している可能性があります。

例

```
Console#traceroute6 FE80::2E0:CFF:FE9C:CA10%1
Press "ESC" to abort.

Traceroute to FE80::2E0:CFF:FE9C:CA10%1/64, 30 hops max, timeout is 3 seconds, 5 max failure(s)
before termination.

Hop Packet 1 Packet 2 Packet 3 IPv6 Address
--- -------- -------- -------- ---------------------------------------
  1   <10 ms   <10 ms   <10 ms FE80::2E0:CFF:FE9C:CA10%1/64

Trace completed.
Console#
```

26.2.15 ipv6 nd dad attempts

本コマンドでは、重複アドレス検出中にインタフェース上で送信された連続する近隣送信要求メッセージの数を設定します。デフォルト設定を復元するには、no 形式を使用してください、

構文

ipv6 nd dad attempts *count*

no ipv6 nd dad attempts

count - このインタフェース上に重複アドレスが存在するかどうかを判断するために送信された、近隣送信要求メッセージの数です(範囲: 0 から 600)

デフォルト設定

3

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

- 値を 0 に設定すると、重複アドレス検出が無効になります。
- 重複アドレス検出は、新しいユニキャスト IPv6 アドレスがネットワークにすでに存在していて、それがインタフェースに割当てられているかどうかを判断します。
- 重複アドレス検出は、中断されているすべてのインタフェースで停止します（vlan コマンドを参照）。インタフェースが中断されている間は、そのインタフェースに割当てられているすべてのユニキャスト IPv6 アドレスが「保留中」の状態になります。インタフェースが管理上再起動されると、重複アドレス検出が自動的に再開されます。
- 再アクティブ化されたインタフェースは、インタフェース上のすべてのユニキャスト IPv6 アドレスに対して重複アドレス検出を再開します。重複したアドレス検出がインタフェースのリンクローカルアドレスで実行されている間、他の IPv6 アドレスは「仮の」状態のままとなります。重複したリンクローカルアドレスが見つからない場合には、残りの IPv6 アドレスに対して重複アドレス検出が開始されます。
- 重複アドレスが検出された場合には、重複状態に設定され警告メッセージがコンソールに送信されます。重複したリンクローカルアドレスが検出されると、IPv6 プロセスはインタフェース上で無効となります。重複するグローバルユニキャストアドレスが検出された場合には使用されません。重複アドレスに関連するすべての設定コマンドは、アドレスが「重複」状態の間は設定されたままとなります。
- インタフェースのリンクローカルアドレスが変更された場合には、重複したアドレス検出が新規のリンクローカルアドレスで実行されますが、インタフェースにすでに関連付けられている IPv6 グローバルユニキャストアドレスのいずれに対しても実施されません。

例

以下の例では、VLAN 1 で設定されたアドレスに対して試みる 5 回の近傍要請を設定します。show ipv6 interface コマンドで、重複アドレス検出処理が続行されていることを示します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  fe80::200:e8ff:fe90:0/64
Global unicast address(es):
  2009:db9:2229::79, subnet is 2009:db9:2229:0::/64
Joined group address(es):
  ff01::1/16
  ff02::1/16
  ff02::1:ff00:79/104
  ff02::1:ff90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
```

```
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
Console#
```

関連コマンド

ipv6 nd ns-interval

show ipv6 neighbors

26.2.16 ipv6 nd ns-interval

本コマンドでは、インタフェース上で IPv6 近接送信要求メッセージを送信する間隔を設定します。デフォルト値を復元するには、no 形式を使用します。

構文

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

milliseconds - 送信する IPv6 近接送信要求メッセージの送信間隔です。(範囲: 1000 から 3600000)

デフォルト設定

近隣探索操作には、1000 ミリセコンドが使用されます。

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

◆ このコマンドでは、アドレスを解決する時、または近隣の到達可能性をプロービングする場合に、近隣送信要求メッセージを送信する間隔を指定します。したがって、通常の IPv6 操作には極端に短い間隔を使用しないでください。

例

以下では、近隣送信要求メッセージの送信間隔を 30000 ミリ秒に設定します。

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  fe80::200:e8ff:FE90:0/64
Global unicast address(es):
  2009:db9:2229::79, subnet is 2009:db9:2229:0::/64
Joined group address(es):
  ff01::1/16
```

```
  ff02::1/16
  ff02::1:ff00:79/104
  ff02::1:ff90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
Console#
```

関連コマンド

show running-config

26.2.17 ipv6 nd reachable-time

本コマンドでは、到達可能性の確認イベントの発生後、リモート IPv6 ノードが到達可能であるとみなされる時間を設定します。デフォルト設定を復元するには、no 形式を使用してください、

構文

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

milliseconds - 到達可能性の確認を受信後に、ノードが到達可能とみなせる時間です。(範囲: 0 から 3600000）

デフォルト設定

近隣探索操作には、30000 ミリセコンドが使用されます。

コマンドモード

Interface Configuration (VLAN)

コマンドの使用方法

◆ このパラメータで設定された制限時間は、ルータが使用できない近隣を検出できるようにします。近隣検出処理中に、IPv6 ノードは近隣送信要求メッセージをマルチキャストして隣接ノードを検索します。隣接ノードが到達可能であると見なされるためには、隣接ノードに隣接ノード通知メッセージで応答して、確認された隣接ノードになる必要がありその後到達可能タイマーは後続のユニキャスト IPv6 レイヤ通信のために有効とみなされます。

例

以下では、リモートノードの到達可能時間を 1000 ミリセコンドに設定します。

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd reachable-time 1000
```

```
Console(config)#
```

26.2.18 clear ipv6 neighbors

本コマンドでは、IPv6 近隣探索キャッシュ内のすべての動的エントリを削除します。

コマンドモード

Privileged Exec

例

以下では、IPv6 近隣探索キャッシュ内のすべての動的エントリを削除します。

```
Console#clear ipv6 neighbors
Console#
```

26.2.19 show ipv6 neighbors

本コマンドでは、IPv6 近隣探索キャッシュ内の情報を表示します。

構文

show ipv6 neighbors [vlan *vlan-id* | *ipv6-address*]

vlan-id - VLAN ID です。 (範囲: 1 から 4094)

ipv6-address - 近隣デバイスの IPv6 アドレスです。コロンで区切られた 16 ビットの 16 進数の 8 つの値を使用して、RFC 2373「IPv6 アドレッシングアーキテクチャ」に準拠してフォーマットされたリンクローカル、またはグローバルのユニキャストアドレスを指定することができます。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。

デフォルト設定

すべての IPv6 近隣探索キャッシュエントリが表示されます。

コマンドモード

Privileged Exec

例

以下では、スイッチのすべての既知の IPv6 近隣を示しています。

```
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
       P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address                          Age  Link-layer Addr   State Interface
------------------------------------ ---- ----------------- ----- ---------
FE80::2E0:CFF:FE9C:CA10               4    00-12-E2-9C-CA-10 R     1
```

```
Console#
```

表 26-9 show ipv6 neighbors - 表示の説明

フィールド	説明
IPv6 Address	近隣の IPv6 アドレスです。
Age	アドレスが到達可能（秒単位）として確認されてからの時間です。静的エントリは、値 "Permanent"によって示されます。
Link-layer Addr	物理レイヤ MAC アドレスです。
State	以下のステートが動的エントリに対して使用されます: I1 (Incomplete) - エントリのアドレス解決が実行されています。近隣送信要求メッセージは、ターゲットのマルチキャストアドレスに送信されていますが、近隣アドバタイズメッセージをまだ返していません。 I2 (Invalid) - 無効マッピングです。状態を無効に設定すると、このエントリで指定されたインタフェースが示されたマッピング(RFC 4293)と関連付けられなくなります。 R (Reachable) - 近隣の ReachableTime 間隔内に、近隣へのフォワードパスが機能していることが確認されています。REACH 状態の間、デバイスはパケットを送信するときに特別な動作を実施しません。 S (Stale) - フォワードパスが機能していた最後の肯定的な確認が受信されているため、ReachableTime 間隔が経過しています。STALE 状態の間、デバイスはパケットが送信されるまで何の動作も実施しません。 D (Delay) - フォワードパスが機能していた最後の肯定的な確認が受信されているため、ReachableTime 間隔が経過しています。最後の DELAY_FIRST_PROBE_TIME 間隔内にパケットが送信されています。DELAY 状態に入った後にこの間隔内に到達可能性確認が受信されない場合、スイッチは近隣送信要求メッセージを送信し、状態を PROBE に変更します。 P1 (Probe) - 到達可能性の確認が受信されるまで、RetransTimer 間隔ごとに近隣要請メッセージを再送信することによって、到達可能性の確認が積極的に実施されます。 U (Unknown) - 未知の状態です。 以下のステートが静的エントリに対して使用されます: I1 (Incomplete)-エントリのインタフェースがダウンしています。 R (Reachable) - エントリのインタフェースがアップしています。IPv6 近隣探索キャッシュの静的エントリに到達可能性の検出は適用されません。 P2 (Permanent) - 静的エントリを示します。
VLAN	アドレスが到達した VLAN インタフェースです。

関連コマンド

show mac-address-table

27 IP ルーティングコマンド

スイッチのネットワークを設定後、異なるインタフェース間でトラフィックを送信するパスを設定する必要があります。トラフィックを他のサブネットワーク上のデバイスに転送するには、静的ルーティングコマンドで固定パスを設定します。本章には静的ルーティングのコマンドが含まれています。これらのコマンドは、異なるローカルサブネットワーク間の接続、またはルータの企業ネットワークへの接続に使用されます。

表 27-1 IP ルーティングコマンド

コマンドグループ	機能
グローバルルーティング設定	静的ルーティングに対してグローバルパラメータを設定し、ルーティングテーブルを表示します。

27.1 グローバルルーティング設定

.

表 27-2 グローバルルーティング設定コマンド

コマンド	機能	モード
IPv4 コマンド		
ip route	静的ルートを設定します。	GC
show ip route	ルーティングテーブルの中のエントリを表示します。	PE

27.1.1 ip route

本コマンドでは、静的ルートを設定します。静的ルートを削除するには、no 形式を使用してください。

構文

ip route *destination-ip netmask next-hop* [*distance*]

no ip route {*destination-ip netmask next-hop* | *}

destination-ip - 宛先ネットワーク、サブネットワーク、またはホストの IP アドレスです。

netmask - 関連 IP サブネットのネットワークマスクです。このマスクは、特定のサブネットへのルーティングに使用されるホストアドレスビットを識別します。

next-hop - ルートに使用される次のホップルータの IP アドレスです。

distance - このルートが他のルーティング情報によって上書きできることを示す管理ディスタンスです。 (範囲: 1 から 255、デフォルト: 1):

* - すべての静的ルーティングエントリを削除します。

デフォルト設定

静的ルートは設定されていません。

コマンドモード

Global Configuration

コマンドの使用方法

- 最大 32 の静的ルートを設定することができます。
- 静的ルートに対して管理距離が定義され、短い管理距離において動的ルートを通じて同じ距離が到達可能な場合には、動的ルートが使用されます。

例

この例では、デフォルトのメトリック 1 を使用してサブネット 192.168.1.0 のすべてのトラフィックをゲートウェイルータ 192.168.5.254 に転送します。

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

27.1.2 show ip route

本コマンドでは、転送情報ベース(FIB)内の情報を表示します。

構文

show ip route [connected | database | rip | static | summary]

connected - 現在の直結エントリをすべて表示します。

database - インアクティブルートを含む、すべての既知のルートです。

rip - ルーティング情報プロトコル(RIP)を通じて学習した、すべてのエントリを表示します。

static - すべての静的エントリを表示します。

summary - ルーティングテーブル内のエントリに関する要約情報の簡単なリストを表示します。直結ルート数、ルーティングテーブルに現在格納されているルート総数、および FIB 内のエントリ数等を含みます。

コマンドモード

Privileged Exec

コマンドの使用方法

- FIB には、IP トラフィックを転送するために必要な情報が含まれています。IP ルーティングテーブルにもとづいて、各到達可能な宛先ネットワークプレフィクスのインタフェース識別子と次のホップ情報を含んでいます。ネットワーク内でルーティングまたはトポロジの変更が発生すると、ルーティングテーブルが更新され、それらの変更はすぐに FIB に反映されます。
  FIB は、ルーティングピアから受信したすべてのルーティング情報を保持するルーティングテーブル(あるいは、ルーティング情報ベース）とは異なります。転送情報ベースには、一意のパスのみが含まれ、セカンダリパスは含まれません。FIB エントリは、特定のパケットの転送決定を行うために必要な最小限の情報で構成されます。転送情報ベースエントリ内の典型的な構成要素は、ネットワークプレフィックス、ルータポート識別子、および次のホップ情報です。
- 本コマンドでは、現在転送可能なルートのみを表示します。ルータは次のホップに直接到達できる必要があります。したがって、静的ルートエントリに関連付けられた VLAN インタフェースは up でなければなりません。

例

```
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       192.168.1.0/24 is directly connected, VLAN1
Console#
```

ルーティング情報ベース(RIB)には直接接続されたネットワークを介して学習された利用可能なすべての

ルートと、静的ルートなどの追加構成されたルートが含まれます。RIB には、転送情報ベースで使用するために最適なエントリが選択されているすべての使用可能なルートのセットが含まれています(show ip route コマンドの使用法を参照)。

```
Console#show ip route database
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

C    *> 192.168.1.0/24 is directly connected, VLAN1

Console#
```

以下の例では、ルーティングテーブル名(0)に続く数値識別子は、転送情報ベース識別子を示しています。

```
Console#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 1
Connected       2
Total           2
Console#
```

付録

付録A　トラブルシューティング

付録A.1　管理インタフェースへのアクセスに関する問題

表 A-1　トラブルシューティングチャート

現象	対処方法
Telnet または SNMP ソフトウェアを使用して接続できません。	・スイッチの電源が入っていることを確認してください。 ・管理ステーションとスイッチ間のネットワークケーブル接続を確認してください。両端が正しく接続され、ケーブルに損傷がないことを確認してください。必要に応じてケーブルをテストします。 ・スイッチとのネットワーク接続が有効で、使用しているポートが無効になっていないことを確認してください。 ・有効な IP アドレス、サブネットマスク、およびデフォルトゲートウェイで管理ステーションが接続されている VLAN インタフェースを設定していることを確認してください。 ・管理ステーションの IP アドレスは、スイッチの IP インタフェースと同じサブネット内にあることを確認してください。 ・タグ付き VLAN グループの IP アドレスを使用してスイッチに接続しようとする場合は、管理ステーションとネットワーク内の中間スイッチを接続するポートに適切なタグを設定する必要があります。 ・Telnet を使用して接続できない場合は、許可されている同時接続可能な Telnet / SSH セッションの最大数を超えている可能性があります。
SSH を使用して接続できません	・SSH を使用して接続できない場合は、許可されている同時接続可能な Telnet / SSH セッションの最大数を超えている可能性があります。 ・スイッチ上で SSH サーバの制御パラメータが正しく設定されていること、および SSH クライアントソフトウェアが管理ステーションで正しく設定されていることを確認してください。 ・スイッチに RSA 公開鍵と DSA 公開鍵の両方を生成し、この鍵を SSH クライアントにエクスポートし、SSH サービスを有効にしてください。別の SSH クライアントを使用するか、SSH クライアントアプリケーションの更新を確認してください。 ・ユーザ名、認証レベル、パスワードなど、各 SSH ユーザのスイッチにアカウントを設定してください。 ・クライアントの公開鍵をスイッチにインポートしたことを確認してください（公開鍵認証が使用されている場合）。
シリアルポート接続でアクセスできません。	・VT100 互換、8 データビット、1 ストップビット、パリティなし、およびボーレートを 115200bps に設定していることを確認してください。 ・RJ-45～DB-9 ヌルモデムシリアルケーブルを使用していることを確認してください。

付録A.2　システムログの使用

障害が発生した場合は、「ハードウェア取扱説明書」を参照して、発生した問題が実際にスイッチによって引き起こされていることを確認してください。スイッチによって問題が発生したように見える場合は、次

の手順を実行します。

1. ロギングを有効にします。
2. 報告されたエラーメッセージに、すべてのカテゴリを含めるように設定します。
3. SNMP を有効にします。
4. SNMP トラップを有効にします。
5. エラーメッセージを受信する SNMP ホストを指定します。
6. コマンドやエラーにつながる他の一連の動作を繰り返します。
7. 障害につながったコマンドや状況のリストを作成します。また、表示されるエラーメッセージのリストも作成します。
8. すべてのコンソール出力をファイルに取り込むことができるように、端末エミュレーションソフトウェアを設定します。次に、 "show tech-support"コマンドを入力して、このファイルにすべてのシステム設定を記録します。
9. 弊社窓口へご連絡下さい。

下記に例を示します。

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
.
.
.
```

付録B　用語集

ACL（Access Control List）

アクセス制御リスト（ACL）は、ネットワークトラフィックを制限し、特定の IP または MAC（即ち、レイヤ 2）については、各パケットをチェックすることにより、特定のユーザまたはデバイスへのアクセスを制限することができます。

ARP（Address Resolution Protocol）

アドレス解決プロトコル（ARP）は、IP アドレスと MAC アドレスを変換します。ARP は、特定の IP アドレスに対応する MAC アドレスの場所を特定するために使用されます。これにより、スイッチはルーティングの決定に IP アドレスを使用し、対応する MAC アドレスはパケットをあるホップから次のホップに転送します。

。

BOOTP（Boot Protocol）

ブートプロトコル（BOOTP）は、IP アドレス情報、デバイスのシステムファイルを含む TFTP サーバーのアドレス、ブートファイルの名前など、ネットワークデバイスのブートアップ情報を提供するために使用されます。

CoS（Class of Service）

サービスクラス（CoS）は、必要なサービスレベルに基づいてパケットに優先順位を付け、適切な出力キューにパケットを配置します。重み付けラウンドロビンサービスを使用してデータがキューから送信され、優先サービスが実行されることで、低レベルキューの閉塞が防止されます。プライオリティは、ポートのデフォルト、パケットのプライオリティビット（VLAN タグ内）、TCP / UDP ポート番号、IP Precedence ビット、または DSCP プライオリティビットに応じて設定できます。

DHCP（Dynamic Host Control Protocol）

動的ホスト制御プロトコル（DHCP）は、TCP / IP ネットワーク上のホストに構成情報を渡すためのフレームワークを提供します。DHCP は Bootstrap Protocol（BOOTP）に基づいており、再利用可能なネットワークアドレスと追加の設定オプションの自動割り当て機能が追加されています。

DHCP Option 82

スイッチによって転送された DHCP 要求パケットと DHCP サーバから返信された応答パケットの中で、要求元のクライアント（または中間リレーエージェント）に関する情報を送信するためのリレーオプションです。この情報は、固定 IP アドレスを割り当てるために DHCP サーバーによって使用されたり、クライアントに他のサービスまたはポリシーを設定したりできます。

DHCP Snooping

DHCP サーバーのメッセージをスヌーピングしてホストの物理的な位置を追跡し、ホストが割り当てられた IP アドレスのみを使用し、許可された DHCP サーバーのみがアクセス可能であることを確認することにより、DHCP サーバへのなりすましや、DHCP サーバへの攻撃を防げます。

DiffServ（Differentiated Services）

差別化サービス（DiffServ）は、さまざまな集約転送動作を構築するための明確に定義されたビルディングブロックを使用することによって、大規模ネットワーク上でサービス品質を提供します。各パケットは、各ホップによって使用される情報（DS バイト）を運び、各ネットワークノードで特定の転送処理またはホップごとの動作を実行します。DiffServ は、トラフィックメーター、シェイパー/ドロッパー、ネットワークの境界にあるパケットマーカーなどのメカニズムを使用して、ネットワーク上のユーザーにさまざまなレベルのサービスを割り当てます。

DNS（Domain Name Service）

ドメインネームサービス（DNS）は、ネットワークノードのホスト名を IP アドレスに変換するために使用されるシステムです。

DSCP（Differentiated Services Code Point）

差別化サービスコードポイント（DSCP）は、6 ビットタグを使用して最大 64 の異なる転送動作を提供します。ネットワークポリシーに基づいて、異なる種類のトラフィックを異なる種類の転送用にマークすることができます。DSCP ビットは、Class of Service カテゴリにマップされ、次に出力キューにマップされます。

EUI （Extended Universal Identifier）

拡張汎用識別子（EUI）は、ネットワークアドレスのホスト部分を識別するための IPv6 で使用されるアドレス形式です。EUI 互換アドレスのインタフェース識別子は、インタフェースのリンクレイヤ（MAC）アドレスに基づいています。グローバルユニキャストおよび他の IPv6 アドレスタイプで使用されるインタフェース識別子は 64 ビット長で、EUI-64 形式で構築できます。変更された EUI-64 形式のインタフェース ID は、リンクレイヤアドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することにより、48 ビットのリンクレイヤアドレスから導出されます。選択されたアドレスが固有のイーサネット MAC アドレスからのものであることを保証するため、上位バイトの 7 番目のビットは 1（IEEE Global / Local ビットに相当）に設定され、48 ビットアドレスの一意性を示します。

ICMP（Internet Control Message Protocol）

インターネット制御メッセージプロトコル（ICMP）は、IP パケットを処理する際にエラーを報告するネットワークレイヤプロトコルです。ICMP は、ルーターがより良いルーティング選択に関する情報をフィードバックするためにも使用されます。

IEEE 802.1D

スパニングツリープロトコルを含む MAC ブリッジの一般的な操作方法を指定します。

IEEE 802.1Q

VLAN Tagging - VLAN 情報を伝送するイーサネットフレームタグを定義します。これにより、スイッチは異なる仮想 LAN にエンドステーションを割り当てることができ、VLAN がスイッチドネットワークを介して通信するための標準的な方法を定義します。

IEEE 802.1p

イーサネットネットワークでサービス品質（QoS）を提供するための IEEE 標準です。この規格では、最大 8 つのトラフィッククラスを定義するパケットタグを使用し、スイッチがタグ付きプライオリティ値に基づいてパケットを送信できるようにしています。

IEEE 802.1s

マルチプルスパニングツリープロトコル（MSTP）の IEEE 標準は、VLAN グループに独立したスパニングツリーを提供します。

IEEE 802.1w

高速スパニングツリープロトコル（RSTP）の IEEE 標準では、ネットワークトポロジの変更の収束時間を、古い IEEE 802.1D STP 標準で必要とされるものの約 10%に低減します。（現在、IEEE 802.1D-2004 に組み込まれています）

IEEE 802.3ac

VLAN タグ付けのフレーム拡張を定義します。

IEEE 802.3x

全二重リンクのフロー制御に使用されるイーサネットフレームの開始/停止要求とタイマーを定義します。（現在、IEEE 802.3-2002 に組み込まれています）

IGMP（Internet Group Management Protocol）

インターネットグループ管理プロトコル（IGMP）は、ホストがマルチキャストサービスのためにローカルルータに登録するためのプロトコルです。特定のサブネットワーク上に複数のマルチキャストスイッチ/ルータが存在する場合、そのうちの 1 つが「クエリア」になり、グループメンバーシップの追跡を担当します。

IGMP Proxy

プロキシは、ダウンストリームインタフェースでモニタされる IGMP メッセージに基づいて、アップストリームインタフェースにグループメンバーシップ情報をマルチキャストし、その情報に基づいてマルチキャストトラフィックを転送します。IGMP プロキシを使用する単純なツリー内にマルチキャストルーティングプロトコルは必要ありません。

IGMP Query

各サブネットワーク上では、1 つの IGMP 対応デバイスがクエリアとして動作します。つまり、参加したい IP マルチキャストグループまたは既に属している IP マルチキャストグループをすべてのホストに報告するように要求するデバイスです。選択されたクエリアは、サブネットワーク内の IP アドレスが最も小さいデバイスになります。

IGMP Snooping

IP マルチキャストグループのメンバーを識別するために IP マルチキャストルータと IP マルチキャストホストグループとの間で転送される IGMP クエリーおよび IGMP レポートパケットを監視します。

IP Precedence

IPv4 ヘッダーのサービスタイプ（ToS）オクテットには、ネットワーク制御パケットの最高優先順位からルーチントラフィックの最低優先順位までの 8 つの異なる優先レベルを定義する 3 つの優先ビット（IP Precedence）が含まれています。8 つの値は、デフォルトでサービスクラスのカテゴリに 1 対 1 にマッピングされますが、特定のネットワークアプリケーションの要件に合わせて異なるように構成することもできます。

LACP（Link Aggregation Control Protocol）

LACP は、リンク集約制御プロトコルです。ポートが、別のデバイス上の LACP 設定ポートとのトランクリンクを自動的にネゴシエートできるようにします。

Layer 2

ISO 7 層データ通信プロトコルのデータリンク層です。これは、ネットワークデバイスのハードウェアインタフェースに直接関連し、MAC アドレスに基づくトラフィックを通過させます。

Layer 3

ISO 7 層データ通信プロトコルのネットワーク層です。このレイヤーは、1 つのオープンシステムから別のシステムに移動するデータのルーティング機能を処理します。

Link Aggregation

Port Trunk を参照してください。

LLDP（Link Layer Discovery Protocol）

リンク層検出プロトコル（LLDP）は、ローカルブロードキャストドメイン内の隣接デバイスに関する基本情報を検出するために定期的なブロードキャストを使用して、デバイスの識別、機能、および設定の設定などの情報をアドバタイズするために使用されます。

MD5（Message Digest Algorithm 5）

MD5 は、デジタル署名を作成するために使用されるアルゴリズムです。これは、32 ビットマシンでの使用を意図し、切断された MD4 アルゴリズムより安全です。MD5 は一方向ハッシュ関数です。つまり、メッセージを受け取り、メッセージダイジェストとも呼ばれる固定桁の数字に変換します。

MIB（Management Information Base）

管理情報ベース（MIB）は、特定のデバイスに関する情報を含む一連のデータベースオブジェクトです。

MSTP（Multiple Spanning Tree Protocol）

マルチプルスパニングツリープロトコル（MSTP）は、異なる VLAN に独立したスパニングツリーを提供できます。ネットワーク管理を簡素化し、各リージョンのサイズを制限して RSTP よりも高速なコンバージェンスを実現し、VLAN メンバーが他のグループからセグメント化されないようにします。

NTP（Network Time Protocol）

ネットワークタイムプロトコル（NTP）は、ネットワーク全体の時間を同期させるメカニズムを提供します。タイムサーバは、サブネット内のローカルクロックと有線または無線を介して各国の標準規格とを同期させるために、階層構造を持っております。

Port Mirroring

ロジックアナライザまたは RMON プローブによるトラブルシューティングのために、ターゲットポートのデータをモニタポートに反映させる方法です。

Port Trunk

いくつかの低速物理リンクを組み合わせた単一の高速論理リンクを作成する方法を指定するネットワークリンクアグリゲーションおよびトランキングメソッドを定義します。

QinQ

QinQ トンネリングは、ネットワークを介して複数の顧客にトラフィックを伝送するサービスプロバイダ向けに設計されています。これは、異なる顧客が同じ内部 VLAN ID を使用する場合でも、顧客固有の VLAN およびレイヤ 2 プロトコル設定を維持するために使用されます。

QoS（Quality of Service）

サービス品質（QoS）とは、データの優先順位付け、キューイング、輻輳回避、トラフィックシェーピングなどの機能を使用して、選択したトラフィックフローに優れたサービスを提供するネットワークの機能を指します。これらの機能は、1 つのフローの優先順位を上げることによって、または別のフローの優先順位を制限することによって、特定のフローに対して優先的な処理を効果的に提供します。

RADIUS（Remote Authentication Dial-in User Service）

リモート認証ダイヤルインユーザーサービス（RADIUS）は、ネットワーク上の RADIUS 準拠デバイスへのアクセスを制御するために中央サーバー上で実行されるソフトウェアを使用するログオン認証プロトコルです。

RMON（Remote Monitoring）

遠隔モニタリング（RMON）は、は包括的なネットワーク監視機能を提供します。標準の SNMP で必要とされるポーリングを排除し、特定のエラータイプを含むさまざまなトラフィック条件でアラームを設定できます。

RSTP（Rapid Spanning Tree Protocol）

高速スパニングツリープロトコル（RSTP）は、ネットワークトポロジ変更の収束時間を、古い IEEE 802.1D STP 標準で要求される収束時間の約 10%に短縮します。

SMTP（Simple Mail Transfer Protocol）

簡易メール転送プロトコル（SMTP）は、TCP（ポート 25）上で動作する標準のホストツーホストメール転送プロトコルです。

SNMP（Simple Network Management Protocol）

簡易ネットワーク管理プロトコル（SNMP）は、ネットワーク管理サービスを提供するインターネットスイートのアプリケーションプロトコルです。

SNTP（Simple Network Time Protocol）

シンプルネットワークタイムプロトコル（SNTP）は、NTP サーバーからの定期的な時刻更新に基づいて、デバイスの内部クロックを設定するプロトコルです。内部クロックの更新は、特定の NTP サーバーから要求することも、NTP サーバーから送信されたブロードキャストを介して受信することもできます。

SSH（Secure Shell）

セキュアシェル（SSH）は、Telnet を含むリモートアクセス機能を安全に置き換えるものです。SSH は暗号鍵でユーザーを認証し、管理クライアントとスイッチ間のデータ接続を暗号化できます。

STA（Spanning Tree Algorithm）

スパニングツリーアルゴリズム（STA）は、ネットワークにループがないかどうかをチェックするテクノロジです。ループは、複雑なまたはバックアップのために冗長化されたネットワークシステムで発生することがよくあります。スパニングツリーは、利用可能な最短経路に沿ってデータを検出して誘導し、ネットワークのパフォーマンスと効率を最大限に高めます。

TACACS+（Terminal Access Controller Access Control System Plus）

ターミナルアクセスコントローラアクセス制御システムプラス（TACACS +）は、ネットワーク上の TACACS 準拠デバイスへのアクセスを制御するために、中央サーバ上で動作するソフトウェアを使用するログオン認証プロトコルです。

TCP/IP（Transmission Control Protocol / Internet Protocol）

伝送制御プロトコル/インターネットプロトコル（TCP/IP）は、プライマリトランスポートプロトコルとして TCP、ネットワークレイヤプロトコルとして IP を含むプロトコルスイートです。

Telnet

TCP / IP を介して端末装置に接続するためのリモート通信機能を定義します。

TFTP（Trivial File Transfer Protocol）

トリビアルファイル転送プロトコル（TFTP）は、ソフトウェアのダウンロードによく使用される TCP / IP プロトコルです。

UDP（User Datagram Protocol）

ユーザデータグラムプロトコル（UDP）は、パケット交換通信のためのデータグラムモードを提供します。これは、IP のようなサービスへのアクセスを提供するための基礎となるトランスポートメカニズムとして IP を使用します。UDP パケットは、IP パケットと同様に配信されます。ターゲットに達する前に破棄されるコネクションレスのデータグラムです。UDP は、TCP が複雑すぎる、遅すぎる、または不必要な場合に便利です。

UTC（Universal Time Coordinate）

ユニバーサルタイムコーディネート（UTC）は、グリニッジ標準時（地球の回転速度のみに基づく）と非常に正確な原子時間を結合する時間スケールです。UTC 自体にはサマータイムがありません。

VLAN（Virtual LAN）

仮想 LAN（VLAN）は、ネットワーク内の物理的な場所または接続ポイントに関係なく、同じコリジョンドメインを共有するネットワークノードの集まりです。VLAN は物理的障壁のない論理的なワークグループとして機能し、ユーザーは同じ LAN 上にあるかのように情報とリソースを共有できます。