TD61-7250

Apresia3400/5400 シリーズ

AEOS Ver. 7.44

コマンドリファレンス L2 編

APRESIA Systems 株式会社

制 定 ・ 改 訂 来 歴 表

No.	年　　月　　日	内　　容
-	2020年9月1日	• TD61-7164 AEOS Ver. 7.43 コマンドリファレンス L2編より作成 • 全章を対象に誤字・脱字・体裁を修正 • 適用機種一覧表を修正 • 表 3-3 設定項目一覧を修正 • 表 3-5 リンクアグリゲーション最大グループ数を修正 • 表 3-64 コマンドにより収集可能な装置情報を修正 • 1. パラメーター設定手順 章の説明を修正 • 1.3 パラメーター設定手順 節を修正 • 2.3 コマンド入力モード 節の説明を修正 • 3.7.16 show interface counters 項の注意事項を修正 • 3.15.1 flush-fdb rp-e port 項に注意事項を追加 • 3.15.2 flush-fdb rp-g port 項に注意事項を追加 • 3.33.1 line 項の説明を修正 • 3.33.2 exec-timeout 項を修正 • 3.33.3 terminal length 項の説明、及びコマンドモードを修正 • 3.42.1 mmrp-plus switch hello-cycle 項の説明を修正 • 3.42.3 mmrp-plus switch polling-rate 項の説明を修正 • 3.45.1 ssl gencsr rsakey 項に注意事項を追加 • 3.45.6 show ssl csr 項の使用例を変更 • 3.45.7 show ssl https-certificate 項の使用例を変更 • 3.47 AccessDefender 節の注意事項を修正 • 3.47.22 mac-authentication enable 項に注意事項を追加 • 3.47.10 web-authentication https-port 項に注意事項を追加 • 3.47.25 mac-authentication password-mac-address 項を追加 • 3.47.59 packet-filter2 max-rule 項に注意事項を追加 • 3.47.60 packet-filter2 group 項の注意事項を修正 • 3.48.6 snmp-server traps 項の注意事項を修正 • 3.48.16 show snmp-server 項の注意事項を修正 • 3.61.17 show hardware 項を修正 • 3.61.19 show tech-support 項の注意事項を修正

はじめに

本書には、スイッチングハブの L2、認証、運用・管理機能のコマンド説明、及び操作方法を記述しています。それ以外のコマンドの説明、及び操作方法については、TD61-7251 AEOS Ver. 7.44 コマンドリファレンス L3 編を参照願います。それ以外のハードウェアに関する説明、及び操作方法については、各適用機種のハードウェアマニュアルを参照してください。

適用機種一覧表

シリーズ名称		製品名称
Apresia 3400 シリーズ	Apresia 3424 シリーズ	Apresia3424GT-SS
		Apresia3424GT-SS2
		Apresia3424GT-HiPoE
	Apresia 3448 シリーズ	Apresia3448GT
		Apresia3448G-PSR
		Apresia3448G-PSR2
Apresia 5400 シリーズ	Apresia 5412 シリーズ	Apresia5412GT-PoE
		Apresia5412GT-HRSS
		Apresia5412GT-HRSS-DC48V
		Apresia5412GT-HRSS-DC110V
		Apresia5412GT-HRSS2
	Apresia 5428 シリーズ	Apresia5428GT

本書の使用例などに用いている IP アドレス、MAC アドレスは他組織所有である場合があるため、ご使用時に留意してください。また、IP アドレスにおいては、運用時に適切な IP アドレスとなるよう変更してください。

この注意シンボルは、そこに記述されている事項が人身の安全と直接関係しない注意書きに関するものであることを示し、注目させるために用います。

輸出する際のご注意

本製品や本資料を輸出、または再輸出する際には、日本国ならびに輸出先に適用される法令、規制に従い必要な手続きをお取りください。
ご不明な点がございましたら、販売店、または当社の営業担当にお問い合わせください。

使用条件と免責事項

ユーザーは、本製品を使用することにより、本ハードウェア内部で動作するルーティングソフトウェアを含むすべてのソフトウェア(以下、本ソフトウェアといいます)に関して、以下の諸条件に同意したものといたします。

本ソフトウェアの使用に起因する、または本ソフトウェアの使用不能によって生じたいかなる直接的、または間接的な損失・損害等(人の生命・身体に対する被害、事業の中断、事業情報の損失、またはその他の金銭的損害を含み、これに限定されない)については、その責を負わないものとします。

(a) 本ソフトウェアを逆コンパイル、リバースエンジニアリング、逆アセンブルすることはできません。

(b) 本ソフトウェアを本ハードウェアから分離すること、または本ハードウェアに組み込まれた状態以外で本ソフトウェアを使用すること、または本ハードウェアでの使用を目的とせず本ソフトウェアを移動することはできません。

APRESIA は、APRESIA Systems 株式会社の登録商標です。
AEOS は、APRESIA Systems 株式会社の登録商標です。
MMRP は、APRESIA Systems 株式会社の登録商標です。
AccessDefender は、APRESIA Systems 株式会社の登録商標です。
Ethernet/イーサネットは、富士ゼロックス株式会社の登録商標です。
GSRP は、アラクサラネットワークス株式会社の登録商標です。
sFlow は、米国 InMon Corp.の登録商標です。
その他ブランド名は、各所有者の商標、または登録商標です。

目次

制定・改訂来歴表 1
はじめに 2
1. パラメーター設定手順 23
1.1 設定項目と出荷時の設定値 23
1.2 L2 モデルの制限事項 25
1.3 パラメーター設定手順 26
1.4 パラメーター設定端末の準備 28
1.5 パラメーター設定端末の接続 29
2. コマンドラインインターフェースの基本操作 31
2.1 コマンドの表記規則 31
2.2 概要 32
2.2.1 ログイン 32
2.2.2 コマンド入力 32
2.3 コマンド入力モード 35
2.4 参照アカウント「user」 37
2.5 初期化アカウント「ap_recovery」 37
3. コマンドの詳細 39
3.1 LOGIN 39
3.1.1 username 39
3.1.2 password 40
3.1.3 show username 41
3.1.4 show users 42
3.2 factory-default 43
3.2.1 factory-default 43
3.3 ホスト名 46
3.3.1 hostname 46
3.4 ログインメッセージ 47
3.4.1 login-message 47
3.4.2 show login-message 48
3.5 IP アドレス 49
3.5.1 ip address 49
3.5.2 show ip address 50
3.6 IP ルート情報 52
3.6.1 ip route 52
3.6.2 show ip route 53
3.6.3 show ip route database 54
3.6.4 show ip route cache 55
3.6.5 show ip route summary 56

3.7 インターフェース 57
3.7.1 shutdown 58
3.7.2 auto-shutdown port 59
3.7.3 auto-shutdown timer 59
3.7.4 auto-negotiation 60
3.7.5 link-speed-duplex 61
3.7.6 advertise delete 62
3.7.7 auto-mdi-x 63
3.7.8 mdi-x 64
3.7.9 mdi 65
3.7.10 pause 65
3.7.11 media 66
3.7.12 description 67
3.7.13 counter-mode txdiscard only-buffer-overflow 68
3.7.14 show auto-shutdown 69
3.7.15 show interface status 69
3.7.16 show interface counters 74
3.7.17 clear interface counters 77
3.8 リンクアグリゲーション 79
3.8.1 link-aggregation 80
3.8.2 link-aggregation algorithm 81
3.8.3 link-aggregation lacp 83
3.8.4 lacp system-priority 84
3.8.5 lacp port-priority 84
3.8.6 lacp timeout short 85
3.8.7 show link-aggregation 86
3.8.8 show lacp 87
3.8.9 show lacp-counter 89
3.8.10 show lacp sys-id 90
3.8.11 show lacp port 90
3.8.12 show tech-support link-aggregation 92
3.8.13 clear lacp counters 93
3.9 ポートリダンダント 94
3.9.1 redundant group-number 94
3.9.2 redundant port-priority 95
3.9.3 redundant mac-address-table update 96
3.9.4 show redundant 97
3.9.5 show redundant portbase 97
3.10 ポートミラーリング 99
3.10.1 mirroring 99

3.10.2 show mirroring 101
3.11 VLAN 102
3.11.1 vlan database 102
3.11.2 vlan name 102
3.11.3 vlan state 103
3.11.4 switchport mode 104
3.11.5 switchport access 104
3.11.6 switchport trunk 106
3.11.7 vlan add protocol 107
3.11.8 tag-type 108
3.11.9 ignore-tag 109
3.11.10 snap-nonzero-oui 110
3.11.11 show vlan 111
3.11.12 show tag-type 112
3.11.13 show ignore-tag 112
3.12 LLDP 114
3.12.1 lldp enable 114
3.12.2 lldp mode 115
3.12.3 lldp msg-tx-interval 116
3.12.4 lldp msg-tx-hold 116
3.12.5 lldp reinit-delay 117
3.12.6 lldp tx-delay 118
3.12.7 lldp management-address 119
3.12.8 lldp err-disable-mode 119
3.12.9 show lldp port 120
3.12.10 show lldp port detail 122
3.12.11 show lldp configuration 123
3.12.12 show lldp statistics 124
3.13 MTU 126
3.13.1 mtu 126
3.13.2 show mtu 126
3.14 Forwarding Data Base(FDB) 128
3.14.1 mac-address-table static 128
3.14.2 mac-address-table aging-time 128
3.14.3 show mac-address-table 129
3.14.4 show mac-address-table aging-time 130
3.14.5 clear mac-address-table 131
3.15 Flush FDB 132
3.15.1 flush-fdb rp-e port 132
3.15.2 flush-fdb rp-g port 133

3.15.3 show flush-fdb rp-e 133
3.15.4 show flush-fdb rp-g 134
3.16 ARP テーブル 136
3.16.1 arp static 136
3.16.2 show arp 137
3.16.3 clear arp 137
3.17 スパニングツリープロトコル(STP/RSTP/MSTP) 139
3.17.1 spanning-tree mode 139
3.17.2 spanning-tree enable 141
3.17.3 spanning-tree disable 142
3.17.4 spanning-tree forward-time 143
3.17.5 spanning-tree hello-time 144
3.17.6 spanning-tree link-type 144
3.17.7 spanning-tree max-age 145
3.17.8 spanning-tree priority 146
3.17.9 spanning-tree portfast 147
3.17.10 spanning-tree port-priority 148
3.17.11 spanning-tree cost 149
3.17.12 spanning-tree force-version 150
3.17.13 spanning-tree mst configuration 150
3.17.14 spanning-tree mst max-hops 151
3.17.15 instance priority 152
3.17.16 instance vlan 153
3.17.17 name 153
3.17.18 revision 154
3.17.19 spanning-tree mst instance 155
3.17.20 spanning-tree mst instance port-priority 155
3.17.21 spanning-tree mst instance cost 156
3.17.22 spanning-tree interconnection-mode 157
3.17.23 show spanning-tree configuration 158
3.17.24 show spanning-tree port 158
3.17.25 show spanning-tree switch 159
3.17.26 show spanning-tree statistics 160
3.17.27 show spanning-tree rst 161
3.17.28 show spanning-tree mst 163
3.17.29 show spanning-tree mst config 164
3.17.30 show spanning-tree mst detail 165
3.17.31 show spanning-tree mst instance 169
3.17.32 show spanning-tree mst port 170
3.17.33 show tech-support spanning-tree 171

3.17.34 clear spanning-tree detected protocols 172
3.18 BPDU 転送制限 173
3.18.1 bpdu-forward 173
3.18.2 show bpdu-forward 173
3.19 マルチキャストフィルタリング 175
3.19.1 multicast-filtering 175
3.19.2 show multicast-filtering 176
3.20 フラッディング制限 178
3.20.1 no flooding 178
3.20.2 flooding enable 178
3.20.3 flooding limit 179
3.20.4 show flooding 180
3.21 フラッディング制御 181
3.21.1 no flooding control 181
3.21.2 flooding control action 182
3.21.3 flooding control enable 183
3.21.4 flooding control pps-hi 183
3.21.5 flooding control pps-low 184
3.21.6 flooding control shutdown pps-hi 185
3.21.7 flooding control interval 186
3.21.8 show flooding control 186
3.21.9 show flooding control port 188
3.22 Ingress フィルタ 190
3.22.1 ingress-filter disable 190
3.22.2 show ingress-filter 190
3.23 Egress フィルタリング 192
3.23.1 egress-filtering 192
3.23.2 show egress-filtering 193
3.24 Egress シェーピング 195
3.24.1 egress shape 195
3.24.2 egress-shape count-mode include-ifg-pa 196
3.24.3 show egress-shape 197
3.25 中継パス制限 198
3.25.1 forwarding 198
3.25.2 forwarding enable 198
3.25.3 show forwarding 199
3.26 ポートブリッジ 201
3.26.1 port-bridge enable 201
3.26.2 show port-bridge 201
3.27 ポートセキュリティー 203

3.27.1 port-security enable 203
3.27.2 switchport port-security enable 203
3.27.3 switchport port-security aging-time 204
3.27.4 switchport port-security maximum 205
3.27.5 port-security delete port 206
3.27.6 port-security delete mac 206
3.27.7 show port-security 207
3.28 パケットフィルター2 209
3.28.1 packet-filter2 210
3.28.2 state 210
3.28.3 assign 211
3.28.4 condition 216
3.28.5 action 222
3.28.6 exceeded-action 229
3.28.7 multi 229
3.28.8 block-cpu-control 232
3.28.9 wide-mode 233
3.28.10 show packet-filter2 235
3.28.11 show packet-filter2 brief 239
3.28.12 show packet-filter2 counter 241
3.28.13 show packet-filter2 tcp/udp-range 242
3.28.14 show packet-filter2 reserved-group 243
3.28.15 show tech-support packet-filter2 244
3.28.16 clear packet-filter2 counter 244
3.28.17 ポリシング 245
3.28.18 policing cbs 246
3.28.19 policing cir 246
3.28.20 action policing group 247
3.28.21 action policing cbs 248
3.28.22 action policing cir 249
3.28.23 ポリシーベースルーティング 250
3.28.24 action routing 250
3.28.25 pbr arp-interval 250
3.28.26 pbr icmp 250
3.28.27 show packet-filter2 policing 250
3.29 ユーザーループ検知 252
3.29.1 no loop-watch 252
3.29.2 loop-watch enable 253
3.29.3 loop-watch interval 254
3.29.4 loop-watch threshold 254

3.29.5 loop-watch auto-recovery timer 255
3.29.6 loop-watch group 256
3.29.7 loop-watch port 257
3.29.8 loop-watch vlan add 258
3.29.9 clear loop-watch information 259
3.29.10 show loop-watch configuration 260
3.29.11 show loop-watch status 261
3.30 QoS 263
3.30.1 qos enable 263
3.30.2 qos min-bandwidth 264
3.30.3 qos max-bandwidth 265
3.30.4 qos weight 266
3.30.5 qos algorithm 267
3.30.6 qos burst-size 268
3.30.7 qos mapping 269
3.30.8 show qos 270
3.31 NTP 273
3.31.1 ntp server 273
3.31.2 ntp enable 273
3.31.3 ntp interval 274
3.31.4 show ntp 275
3.32 時刻、タイムゾーン 276
3.32.1 clock set 276
3.32.2 timezone 276
3.32.3 show clock 277
3.32.4 show timezone 278
3.33 ターミナル設定 279
3.33.1 line 279
3.33.2 exec-timeout 279
3.33.3 terminal length 281
3.33.4 terminal monitor 281
3.34 TELNET 283
3.34.1 telnet mode deny 283
3.34.2 telnet server 283
3.34.3 telnet ip 284
3.34.4 telnet subnet 285
3.34.5 telnet disconnect 285
3.34.6 show telnet server 286
3.34.7 show telnet list 287
3.35 SSH 288

3.35.1 sshd keygen rsa 288
3.35.2 sshd keygen rsa1 289
3.35.3 sshd server 289
3.35.4 sshd keepalive disable 290
3.35.5 sshd port 291
3.35.6 sshd server-keybits 291
3.35.7 sshd mode deny 292
3.35.8 sshd ip 293
3.35.9 sshd subnet 293
3.35.10 sshd disconnect 294
3.35.11 copy file ssh-key 295
3.35.12 copy ssh-key file 295
3.35.13 show sshd server 297
3.35.14 show sshd list 297
3.35.15 show sshd key rsa 298
3.35.16 show sshd key rsa1 299
3.36 IGMP Snooping 300
3.36.1 ip igmp snooping enable 300
3.36.2 ip igmp snooping immediate-leave 301
3.36.3 ip igmp snooping max-member 301
3.36.4 ip igmp snooping member aging-time 302
3.36.5 ip igmp snooping member leave-time 302
3.36.6 ip igmp snooping mrouter aging-time 303
3.36.7 ip igmp snooping mrouter vlan 304
3.36.8 ip igmp snooping mrouter filter 304
3.36.9 ip igmp snooping group filter 305
3.36.10 ip igmp snooping send report-leave disable 306
3.36.11 ip igmp snooping report-message-proxy enable 306
3.36.12 ip igmp snooping leave-message-proxy enable 307
3.36.13 ip igmp snooping unregistered-filter 308
3.36.14 ip igmp snooping unregistered-filter pf2-group 309
3.36.15 clear ip igmp snooping cpu-counter 310
3.36.16 show ip igmp snooping cpu-counter 310
3.36.17 show ip igmp snooping configuration 311
3.36.18 show ip igmp snooping status 312
3.36.19 show tech-support igmp 313
3.37 IGMP クエリア 315
3.37.1 ip igmp querier enable 315
3.37.2 ip igmp querier vlan 315
3.37.3 ip igmp querier query-interval 316

3.37.4 ip igmp querier query-max-response-time 317
3.37.5 ip igmp querier query-timeout 317
3.37.6 ip igmp querier robustness 318
3.37.7 show ip igmp querier configuration 318
3.38 ロギング 320
3.38.1 logging buffered 320
3.38.2 logging sram 321
3.38.3 logging console 321
3.38.4 logging monitor 322
3.38.5 logging ip 323
3.38.6 logging source 324
3.38.7 logging on 324
3.38.8 logging flash 325
3.38.9 logging error-frame-received port disable 325
3.38.10 show logging 326
3.38.11 clear logging 327
3.39 MLD Snooping 328
3.39.1 ipv6 mld snooping enable 328
3.39.2 ipv6 mld snooping immediate-leave 328
3.39.3 ipv6 mld snooping max-member 329
3.39.4 ipv6 mld snooping member aging-time 330
3.39.5 ipv6 mld snooping member leave-time 330
3.39.6 ipv6 mld snooping mrouter aging-time 331
3.39.7 ipv6 mld snooping mrouter vlan 331
3.39.8 ipv6 mld snooping mrouter filter 332
3.39.9 ipv6 mld snooping group filter 333
3.39.10 ipv6 mld snooping unregistered-filter 333
3.39.11 ipv6 mld snooping unregistered-filter pf2-group 334
3.39.12 show ipv6 mld snooping configuration 335
3.39.13 show ipv6 mld snooping status 336
3.40 DHCP サーバー 338
3.40.1 dhcp policy 338
3.40.2 dhcp policy enable 339
3.40.3 dhcp server enable 339
3.40.4 dhcp server restart 340
3.40.5 dhcp server address-check arp 341
3.40.6 dhcp port max-lease-num 341
3.40.7 clear dhcp leases 342
3.40.8 network 342
3.40.9 range 343

3.40.10 domain-name 344
3.40.11 dns-server 345
3.40.12 wins-server 346
3.40.13 router 347
3.40.14 lease 348
3.40.15 renewing 348
3.40.16 rebinding 349
3.40.17 logs 350
3.40.18 merit 351
3.40.19 next-server 351
3.40.20 root-path 352
3.40.21 ntp-server 353
3.40.22 static-entry 354
3.40.23 show dhcp current 355
3.40.24 show dhcp policy 356
3.41 MMRP 357
3.41.1 mmrp switch hello-interval 357
3.41.2 mmrp group 358
3.41.3 mmrp enable 359
3.41.4 no mmrp ring 360
3.41.5 mmrp ring master master-port slave-port 361
3.41.6 mmrp ring master master-vid 362
3.41.7 mmrp ring master slave-vid 363
3.41.8 mmrp ring aware port 364
3.41.9 mmrp ring divided-master master-port 365
3.41.10 mmrp ring divided-master master-vid 365
3.41.11 mmrp ring divided-master uplink-forcedown-method 366
3.41.12 mmrp ring divided-master uplink-forcedown-time 367
3.41.13 mmrp ring divided-master uplink-port 368
3.41.14 mmrp ring divided-master uplink-up-wait 369
3.41.15 mmrp ring divided-shadow slave-port 369
3.41.16 mmrp ring divided-shadow slave-vid 370
3.41.17 mmrp ring divided-shadow uplink-forcedown-method 371
3.41.18 mmrp ring divided-shadow uplink-forcedown-time 372
3.41.19 mmrp ring divided-shadow uplink-port 373
3.41.20 mmrp ring divided-shadow uplink-up-wait 373
3.41.21 mmrp ring fdb-flush-timer 374
3.41.22 mmrp ring listening-timer 375
3.41.23 mmrp ring bidirectional-check disable 376
3.41.24 mmrp ring bidirectional-check error-disabled-timer 376

3.41.25 mmrp ring bidirectional-check revertive-timer 377
3.41.26 show mmrp status 378
3.41.27 show mmrp status port 379
3.41.28 show mmrp configuration 380
3.41.29 show mmrp configuration ring 381
3.41.30 show tech-support mmrp 382
3.41.31 clear mmrp error-disabled 383
3.42 MMRP-Plus 384
3.42.1 mmrp-plus switch hello-cycle 385
3.42.2 mmrp-plus switch hello-interval 387
3.42.3 mmrp-plus switch polling-rate 387
3.42.4 mmrp-plus group 388
3.42.5 mmrp-plus enable 390
3.42.6 no mmrp-plus ring 391
3.42.7 mmrp-plus ring name 391
3.42.8 mmrp-plus ring vid 392
3.42.9 mmrp-plus vlangroup slave-vid 393
3.42.10 mmrp-plus vlangroup master-vid 394
3.42.11 mmrp-plus ring vlangroup 396
3.42.12 mmrp-plus ring master master-port slave-port 396
3.42.13 mmrp-plus ring aware port 398
3.42.14 mmrp-plus ring revertive 399
3.42.15 mmrp-plus ring divided-master master-port 400
3.42.16 mmrp-plus ring divided-master uplink-forcedown-method 400
3.42.17 mmrp-plus ring divided-master uplink-forcedown-time 402
3.42.18 mmrp-plus ring divided-master uplink-port 402
3.42.19 mmrp-plus ring divided-master uplink-up-wait 403
3.42.20 mmrp-plus ring divided-master uplink-fdbflush-transmit 404
3.42.21 mmrp-plus ring divided-shadow slave-port 405
3.42.22 mmrp-plus ring divided-shadow uplink-forcedown-method 406
3.42.23 mmrp-plus ring divided-shadow uplink-forcedown-time 407
3.42.24 mmrp-plus ring divided-shadow uplink-port 408
3.42.25 mmrp-plus ring divided-shadow uplink-up-wait 409
3.42.26 mmrp-plus ring divided-shadow uplink-fdbflush-transmit 409
3.42.27 mmrp-plus ring fdb-flush-timer 410
3.42.28 mmrp-plus ring listening-timer 411
3.42.29 mmrp-plus ring hello-timeout 412
3.42.30 mmrp-plus ring port-restart enable 413
3.42.31 mmrp-plus ring port-restart forcedown-time 414
3.42.32 mmrp-plus ring port-restart linkup-wait 414

3.42.33 show mmrp-plus configuration 415
3.42.34 show mmrp-plus configuration ring 417
3.42.35 show mmrp-plus vlangroup 419
3.42.36 show mmrp-plus status 420
3.42.37 show mmrp-plus status port 421
3.42.38 show tech-support mmrp-plus 422
3.42.39 clear mmrp-plus failure ring 423
3.43 MMRP2 aware 424
3.43.1 mmrp2 group 424
3.43.2 mmrp2 enable 426
3.43.3 mmrp2 aware port 427
3.43.4 no mmrp2 428
3.43.5 mmrp2 vid 428
3.43.6 mmrp2 name 429
3.43.7 mmrp2 listening-timeout 429
3.43.8 mmrp2 revertive 430
3.43.9 mmrp2 enable 431
3.43.10 show mmrp2 432
3.43.11 show mmrp2 detail 432
3.43.12 clear mmrp2 failure 434
3.44 RADIUS ログイン認証機能 436
3.44.1 radius login enable 437
3.44.2 radius login local-authentication disable 437
3.44.3 radius login ip 438
3.44.4 radius login secret-key 439
3.44.5 radius login max-request 440
3.44.6 radius login request-interval 440
3.44.7 show radius login configuration 441
3.44.8 RADIUS 属性 442
3.45 SSL 機能 443
3.45.1 ssl gencsr rsakey 443
3.45.2 copy csr tftp 444
3.45.3 copy file https-file 445
3.45.4 copy https-file file 446
3.45.5 erase ssl-files 447
3.45.6 show ssl csr 448
3.45.7 show ssl https-certificate 449
3.45.8 show ssl https-private-key 450
3.46 NA 機能 452
3.46.1 ライセンスキー追加 452

3.46.2 na enable 453
3.46.3 na radius ip 454
3.46.4 na radius port 454
3.46.5 na radius secret 455
3.46.6 na radius max-req 456
3.46.7 na radius request-interval 456
3.46.8 na httpd name radius 457
3.46.9 na httpd ip 459
3.46.10 na httpd port 460
3.46.11 na httpd url 461
3.46.12 na httpd ssl enable 461
3.46.13 na httpd sslv2 enable 463
3.46.14 na httpd sslv3 enable 463
3.46.15 na httpd english-language enable 464
3.46.16 na port shared mode 465
3.46.17 na port designated mode 466
3.46.18 na port shared-dynamic-vlan mode 468
3.46.19 na filter permit-ttl 469
3.46.20 na force-authorized port 470
3.46.21 na local-authorized port 471
3.46.22 na logout aging 472
3.46.23 na logout ping ttl 473
3.46.24 na logout ping dest-ip 474
3.46.25 na logout timeout 474
3.46.26 na logout polling interval 475
3.46.27 na logout polling count 476
3.46.28 na logout clock 477
3.46.29 na mac-base passwd 478
3.46.30 na arp-relay-port 478
3.46.31 na arp-relay-port vid 479
3.46.32 na dhcp-relay-port 480
3.46.33 na roaming enable 481
3.46.34 na disc-mac-delete interval 481
3.46.35 na clear 482
3.46.36 na custom-relay-port port 483
3.46.37 na custom-relay-port ip 484
3.46.38 na custom-relay-port tcp 485
3.46.39 na custom-relay-port udp 486
3.46.40 na auth-page redirect 487
3.46.41 na auth-page redirect proxy-port 489

3.46.42 na auth-page redirect vid 490
3.46.43 na auth-page redirect url 491
3.46.44 na success-url 493
3.46.45 na success-url timeout 494
3.46.46 copy tftp local-db 494
3.46.47 copy local-db tftp 495
3.46.48 erase local-db 496
3.46.49 show na aging 497
3.46.50 show na configuration 497
3.46.51 show na local-db 501
3.46.52 show na client 501
3.46.53 show tech-support na 502
3.46.54 RADIUS サーバー設定例 503
3.47 AccessDefender 504
3.47.1 access-defender 506
3.47.2 aaa authentication 507
3.47.3 aaa authentication control 508
3.47.4 aaa radius host 509
3.47.5 aaa radius client-ip 510
3.47.6 aaa radius deadtime 511
3.47.7 web-authentication enable 512
3.47.8 web-authentication port 514
3.47.9 web-authentication http-port 517
3.47.10 web-authentication https-port 518
3.47.11 web-authentication http-session-timeout 519
3.47.12 web-authentication ip 520
3.47.13 web-authentication redirect url 521
3.47.14 web-authentication redirect http 521
3.47.15 web-authentication redirect https 523
3.47.16 web-authentication redirect proxy-port 524
3.47.17 web-authentication snooping proxy-port 525
3.47.18 web-authentication mac-authentication-password 526
3.47.19 web-authentication ttl 527
3.47.20 web-authentication sslv2 enable 528
3.47.21 web-authentication sslv3 enable 528
3.47.22 mac-authentication enable 529
3.47.23 mac-authentication port 531
3.47.24 mac-authentication password 531
3.47.25 mac-authentication password-mac-address 532
3.47.26 mac-authentication ignore-dhcp 533

3.47.27 dot1x enable 534
3.47.28 dot1x port 534
3.47.29 dot1x mac-authentication-password 535
3.47.30 dot1x port ignore-eapol-start 536
3.47.31 dot1x port initialize 537
3.47.32 dot1x port max-req 537
3.47.33 dot1x port reauthentication 538
3.47.34 dot1x port re-authenticate 539
3.47.35 dot1x port timeout quiet-period 539
3.47.36 dot1x port timeout re-authperiod 540
3.47.37 dot1x port timeout supp-timeout 540
3.47.38 dot1x port timeout tx-period 541
3.47.39 dhcp-snooping enable 542
3.47.40 dhcp-snooping port 543
3.47.41 dhcp-snooping mode deny 544
3.47.42 dhcp-snooping mode mac-authentication 544
3.47.43 dhcp-snooping mode timer 545
3.47.44 dhcp-snooping static-entry port 546
3.47.45 dhcp-snooping internal-dhcp-vlan 547
3.47.46 logout aging-time 548
3.47.47 logout timeout 549
3.47.48 logout linkdown port disable 550
3.47.49 logout linkdown time port enable 550
3.47.50 logout linkdown time 551
3.47.51 logout ping dst-ip 552
3.47.52 logout ping ttl 552
3.47.53 logout clock 553
3.47.54 access-defender-deny 554
3.47.55 access-defender-logout ip 554
3.47.56 access-defender-logout mac 555
3.47.57 access-defender-logout user 556
3.47.58 port max-client 556
3.47.59 packet-filter2 max-rule 557
3.47.60 packet-filter2 group 559
3.47.61 roaming port enable 560
3.47.62 vlan mode dynamic port-base 561
3.47.63 vlan mode static 563
3.47.64 logging access-defender web-access on 564
3.47.65 copy file WEB-PAGE 564
3.47.66 copy WEB-PAGE file 566

3.47.67 copy file aaa-local-db 567
3.47.68 copy aaa-local-db file 569
3.47.69 aaa-local-db add user 570
3.47.70 aaa-local-db del user 571
3.47.71 show access-defender aaa-local-db 572
3.47.72 show access-defender client 572
3.47.73 show access-defender deny 574
3.47.74 show access-defender dot1x 574
3.47.75 show access-defender dot1x statistics port 577
3.47.76 show access-defender dhcp-snooping configuration 578
3.47.77 show access-defender dhcp-snooping mode-status 579
3.47.78 show access-defender dhcp-snooping status 580
3.47.79 show access-defender packet-filter2 rule-statistics 581
3.47.80 show access-defender port-configuration 583
3.47.81 show tech-support access-defender 584
3.47.82 認証ページ 584
3.47.83 RADIUS 属性 587
3.48 SNMP 589
3.48.1 snmp-server disable 589
3.48.2 snmp-server community 589
3.48.3 snmp-server access-disable 591
3.48.4 snmp-server host 591
3.48.5 snmp-server trap source 593
3.48.6 snmp-server traps 594
3.48.7 snmp-server contact 596
3.48.8 snmp-server location 597
3.48.9 snmp-server name 597
3.48.10 snmp-server trap-source 598
3.48.11 snmp-server traps boot-time-delay 599
3.48.12 snmp-server traps transmit-delay 600
3.48.13 snmp-server traps transmit-gap disable 601
3.48.14 snmp-server rmon-history 601
3.48.15 snmp-server counter ifinerrors-exclude-oversize 602
3.48.16 show snmp-server 603
3.49 構成情報の表示 606
3.49.1 show running-config 606
3.49.2 show flash-config 607
3.50 構成情報のチェックと保存 609
3.50.1 check config 609
3.50.2 copy running-config flash-config, write memory 609

3.50.3 copy tftp server file flash-config 611
3.50.4 copy flash-config tftp server file 612
3.50.5 copy running-config file 612
3.51 構成情報の初期化 614
3.51.1 erase flash-config 614
3.52 Default disable 615
3.52.1 default disable 615
3.53 構成情報自動ダウンロード 616
3.53.1 auto-download 616
3.53.2 show auto-download 617
3.54 メモリーカード 618
3.54.1 copy memory-card software 618
3.54.2 copy memory-card flash-config 619
3.54.3 copy tftp memory-card 619
3.54.4 copy flash-config memory-card 620
3.54.5 copy log memory-card 621
3.54.6 cat memory-card 622
3.54.7 erase memory-card 623
3.54.8 rename memory-card 623
3.54.9 show memory-card files 624
3.55 ブートスクリプト 625
3.55.1 boot-script system primary 626
3.55.2 boot-script system secondary 626
3.55.3 boot-script configuration primary 627
3.55.4 boot-script configuration secondary 628
3.55.5 copy configured-script 628
3.55.6 copy default-script configured-script 629
3.55.7 erase boot-script 629
3.55.8 show boot-script configured 630
3.55.9 show boot-script flash 631
3.55.10 show boot-script memory-card 631
3.56 再起動 633
3.56.1 reboot 633
3.56.2 reboot timer 633
3.56.3 show reboot timer 634
3.57 ファームウェアの管理 635
3.57.1 archive download-sw 635
3.57.2 archive download-loader 637
3.57.3 archive upload-sw 638
3.57.4 archive upload-loader 639

3.58 AEOS6へのダウングレード(Apresia4348シリーズ) 641
3.58.1 archive downgrade-aeos6 641
3.59 CPU使用率通知 643
3.59.1 cpu-utilization-notify threshold polling 643
3.59.2 clear cpu-utilization history 643
3.60 メモリー使用容量通知 645
3.60.1 memory-used-notify threshold polling 645
3.61 保守/運用コマンド 646
3.61.1 ping 646
3.61.2 traceroute 647
3.61.3 telnet 647
3.61.4 debug 648
3.61.5 backup tftp, backup memory-card 649
3.61.6 backup clone 651
3.61.7 restore 652
3.61.8 tftp source 654
3.61.9 memory-error auto-recovery-mode enable 655
3.61.10 memory-error auto-recovery-mode notify disable 656
3.61.11 error-frame threshold polling-rate 657
3.61.12 power-down-notify enable 658
3.61.13 show debugging 659
3.61.14 show version 660
3.61.15 show version flash 661
3.61.16 show system 662
3.61.17 show hardware 664
3.61.18 show history 667
3.61.19 show tech-support 668
3.61.20 show netstat 670
3.61.21 show ps 670
3.61.22 show vmstat 671
3.61.23 clear memory-error 672
3.62 PoE 674
3.62.1 poe threshold power(最大値設定) 674
3.62.2 poe threshold power(ポート設定) 675
3.62.3 poe disable 676
3.62.4 poe priority 676
3.62.5 poe power management class-based 678
3.62.6 poe other-fault retry-interval 679
3.62.7 show poe status 679
3.62.8 show poe power status 681

3.63 sFlow 684
3.63.1 sflow enable 684
3.63.2 sflow destination 684
3.63.3 sflow forwarding 685
3.63.4 sflow mode 686
3.63.5 sflow polling-interval 687
3.63.6 sflow sample 688
3.63.7 sflow source 689
3.63.8 sflow max-header-size 690
3.63.9 show sflow 690
4. トラブルシューティング 692
4.1 表示 LED に関連する現象と対策 692
4.2 コンソール端末に関連する現象と対策 692
4.3 SNMP マネージャーに関連する現象と対策 693
4.4 TELNET に関連する現象と対策 693
4.5 スイッチングハブ機能に関連する現象と対策 693
4.6 VLAN に関連する現象と対策 693
4.7 リンクアグリゲーションに関連する現象と対策 694
4.8 内蔵冷却ファンに関連する現象と対策 694
4.9 XENPAK に関連する現象と対策 694
4.10 装置の表示、エラーログに関連する現象と対策 694
5. 準拠規格 696

1. パラメーター設定手順

パラメーターの設定は以下の方式により行うことができます。パラメーター設定手順については 1.3 節を参照してください。

コマンドライン方式(パラメーター設定端末、または TELNET/SSH(最大 8 セッション)による)は 3 章で詳述します。

1.1 設定項目と出荷時の設定値

各パラメーターの内容と出荷時の設定値を表 1-1 に示します。L3 機能の各パラメーターの内容と出荷時の設定値については、TD61-7251 AEOS Ver. 7.44 コマンドリファレンス L3 編を参照してください。

設定したパラメーターは、設定後即時に反映されます。ただし、設定後保存コマンド(3.50.2 項参照)を実行せずにリセットした場合、消去されます。リセット後も設定値を保持する場合は、設定保存コマンドを実行してください。

表 1-1 設定項目一覧

	設定項目	内容	出荷時の設定値
1	username password	user の登録・削除 user の password 設定	なし なし
2	ip address	管理ポートの IP アドレス	なし
3	ip route	経路情報	なし
4	ip icmp redirect accept disable ip icmp redirect send disable	ICMP の送受信動作	送受信共に ENABLE
5	shutdown	ポートの状態(活性/非活性)	活性(no shutdown)
6	auto-negotiation	通信速度/通信方式	ENABLE(自動認識)
7	link-speed-duplex	自動認識モード OFF 時の 通信速度/通信方式	100M/半二重
8	advertise delete	自動認識時の通信速度/通信方式の広告設定	Delete 設定なし (すべて広告設定)
9	auto-mdi-x	MDI/MDI-X の自動認識	ENABLE(自動認識)
10	mdi-x mdi	MDI-X/MDI の設定	MDI：管理ポート、UTP ポート (10/100/1000 Mbps)、GBIC ポート (SFP-T 使用時) MDI-X ： UTP ポート (10/100 Mbps)
11	pause	ポートごとのフロー制御機能の動作状態	DISABLE(非動作)
12	media	GigabitEthernet ポートのメディアタイプ	GBIC
13	link-aggregation	リンクアグリゲーショングループ	なし(非動作)
14	redundant group-number	ポートリダンダントグループ番号	設定なし

	設定項目	内容	出荷時の設定値
15	mirroring	ポートミラーリング	設定なし
16	vlan name	VLAN 名	Default(VID=1)
17	vlan state	VLAN の動作状態	ENABLE(工場出荷時は default vlan のみ動作)
18	switchport mode	ポートの VLAN モード	アクセスポート
19	switchport access	アクセスポートの VLAN 所属	VID=1 の VLAN に所属
20	switchport trunk	トランクポートの VLAN 所属	なし
21	mac-address-table static	static FDB 登録	なし
22	mac-address-table aging-time	自動アドレス学習機能による エージング時間	300(秒)
23	arp static	ARP 固定エントリー	設定無し
24	multicast-filtering	マルチキャストフィルタリング	フィルタリングなし
25	spanning-tree enable	スパニングツリープロトコル	スパニングツリー プロトコル非動作
26	flooding	フラッディングフレームの制限	DISABLE(非動作)
27	ingress-filter	タグ付きフレームの受信動作	ENABLE(動作)
28	egress-filtering	フラッディングフレームの 出力ポート設定	OFF(非動作)
29	port-security enable	ポートセキュリティー機能	非動作
30	packet-filter2	パケットフィルター2	ENABLE(工場出荷時は エントリーなし)
31	egress shape	送信するトラフィック量の制限	制限なし
32	qos enable	QoS 機能の動作状態	DISABLE(非動作)
33	ntp server	NTP サーバーの設定	なし
34	clock set	日付と時刻の設定	現在時刻
35	exec-timeout	自動ログアウトまでの時間 ※1	300(秒)
36	telnet mode deny	TELNET 禁止モード	設定なし(TELNET 許可)
37	telnet server	TELNET サーバーの起動	ENABLE(有効)
38	ip igmp snooping enable	IGMP Snooping 機能	設定なし(IGMP Snooping 非動作)
39	logging buffered	ログメッセージの優先度設定	info
40	logging console	ログメッセージのコンソール出力	alert
41	logging ip	ログ転送先 SYSLOG サーバーの設定	なし
42	snmp-server disable ※2	SNMP の動作状態	ENABLE(SNMP 動作)
43	snmp-server community	コミュニティー名	Read Only ：public Read/Write：private
44	snmp-server host	トラップ送信先	宛先ホスト：なし コミュニティー名：public

	設定項目	内容	出荷時の設定値
45	snmp-server traps	トラップ送信機能の動作状態	NA、MMRP 以外： トラップ送信有効 NA、MMRP： トラップ送信無効
46	snmp-server contact	システムコンタクト	なし
47	snmp-server location	システムロケーション	なし
48	snmp-server name	システムネーム	なし
49	snmp-server rmon-history ※3	RMON historyControlGroup のデフォルトエントリーの設定	デフォルトエントリーを追加しない
50	dhcp policy	DHCP サーバーのポリシー	ポリシー設定なし(DHCP 非動作)
51	poe power management class-based	給電モード	なし(dynamic)

※1 自動ログアウトまでの時間の設定変更時は、すでに成立しているログインセッションには反映されません。

※2 工場出荷時の設定状態においては、コミュニティー名が一致するすべての SNMP マネージャーからのアクセスが許可されます。SNMP 機能を使用しない場合、"snmp-server disable"設定を行う必要があります。

※3 この項目は、設定では即時動作反映しません。装置を再起動するか、"snmp-server disable"コマンド、及び"no snmp-server disable"コマンドで、SNMP サーバーの起動をやり直す必要があります。

1.2 L2 モデルの制限事項

L2 モデル(Apresia4300 シリーズ)では、TD61-7251 AEOS Ver. 7.44 コマンドリファレンス L3 編で述べるコマンドのうち、以下に述べる各節のコマンドは使用できません。

- IP フォワーディング
- ICMP リダイレクト
- IP ブロードキャストルーティング
- PIM-SM
- IGMP
- IGMP Proxy
- アクセスリスト
- prefix-list
- OSPF
- RIP
- RIP 認証
- BGP
- ルートマップ
- VRRP
- DHCP リレー
- ポリシーベースルーティング

1.3 パラメーター設定手順

(1) パラメーター設定端末を用いたパラメーター設定の手順

パラメーター設定端末の準備(1.4 節参照)

↓

パラメーター設定端末の接続(1.5 節参照)

↓

パラメーター設定端末の電源 ON

↓

本装置の電源 ON

↓

LED 表示ランプの確認
POWER 表示 LED が点灯し、FAULT LED が消灯していることを確認してください。

↓

パラメーター設定端末の表示画面の確認
以下のような表示がされていることを確認してください。
＜表示例＞
Ethernet Switch Apresia13000-48X

login:

↓

システムログイン(2.2.1 項参照)

↓

システムパラメーターの設定(2 章参照)

↓

パラメーター設定端末を電源 OFF とし、本装置から取り外します。

↓

セットアップ完了

(2) TELNET を用いたパラメーター設定の手順

TELNET を用いたパラメーターの設定は、本装置が LAN に接続され IP アドレスが設定されている場合のみ可能です。

本装置に割り当てられた IP アドレスに Telnet コマンドでアクセスしてください。
　例)telnet 192.168.1.10
プロンプト(login:)が表示されることを確認してください。

↓

システムログイン(2.2.1 項参照)

↓

システムパラメーターの設定(2 章参照)

↓

セットアップ完了

(3) SSH を用いたパラメーター設定の手順

SSH を用いたパラメーターの設定は、本装置が LAN に接続され IP アドレスが設定されている場合のみ可能です。

本装置に割り当てられた IP アドレスに SSH コマンドでアクセスしてください。
例)ssh -l adpro 192.168.1.10
プロンプト(>)が表示されることを確認してください。

↓

システムログイン(2.2.1 項参照)

↓

システムパラメーターの設定(2 章参照)

↓

セットアップ完了

注意事項

コンソール、TELNET/SSH によりターミナル接続する場合は、改行コードとして CR を送信するようターミナルソフトを設定してください。CR+LF など異なる設定をした場合、表示、設定が正しく行われない場合があります。

コンソールによりターミナル接続した場合の表示画面には 80 文字固定で改行が入ります。"terminal length 0"を設定した場合は入りません。

1.4 パラメーター設定端末の準備

本装置のパラメーター設定に必要な端末の条件、及び通信条件を表 1-2、表 1-3 に示します。

表 1-2 パラメーター設定端末の条件

項番	項目	仕様
1	端末の設定	ANSI(VT100 互換)

表 1-3 通信条件

項番	項目	仕様
1	スクリーンサイズ	80 列×24 行/スクリーン以上
2	キャラクター	8 bit/キャラクター
3	ストップビット	1 bit
4	パリティー	なし
5	フロー制御	なし
6	ボー・レート	9600 bps
7	RS, ER	常時 ON とする
8	CD	監視しない
9	端末接続ケーブル	RS-232C ケーブル(クロス)、ただし、本装置側は DB-9 メス型コネクタを使用のこと

1.5 パラメーター設定端末の接続

パラメーター設定端末と本装置のコンソールポートを、表 1-3 の項番 9 の RS-232C ケーブル(クロス)を用いて接続します。

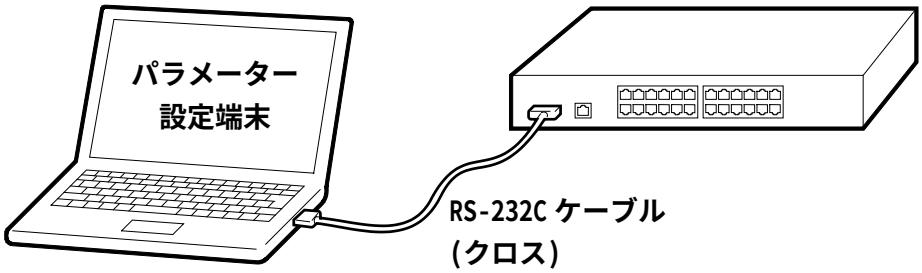


図 1-1 RS-232C ケーブルの接続

本装置のコンソールポートのピン仕様を表 1-4 に示します。コンソールポートは、DTE 仕様(オス)の DB-9 コネクタになっています。

表 1-4 コンソールポートのピン仕様

ピン No.	信号名	信号の内容	備考
1			未接続
2	RD	受信データ	入力
3	SD	送信データ	出力
4			ピン 6 に接続
5	SG	回路アース	
6			ピン 4 に接続
7			ピン 8 に接続
8			ピン 7 に接続
9			未接続

注意事項

コンソールポートには、パラメーター設定時のみに RS-232C ケーブルを接続し、通常の運用時には接続しないでください。

RS-232C ケーブルの接続結線例を表 1-5、表 1-6 に示します。

表 1-5 RS-232C ケーブル接続結線例(9 ピン-25 ピン D-SUB の場合)

本装置側 コネクタ 9 ピン D-SUB(メス)	接続	パラメーター設定端末側 コネクタ 25 ピン D-SUB(メス)
ピン番号		ピン番号
1		4
		5
2		2
3		3
4		6
5		7
6		20
7		8
8		
9		22

表 1-6 RS-232C ケーブル接続結線例(9 ピン-9 ピン D-SUB の場合)

本装置側 コネクタ 9 ピン D-SUB(メス)	接続	パラメーター設定用端末 コネクタ 9 ピン D-SUB(メス)
ピン番号		ピン番号
1		1
2		2
3		3
4		4
5		5
6		6
7		7
8		8

2. コマンドラインインターフェースの基本操作

コマンドライン方式によるパラメーターの表示/設定方法を説明します。

2.1 コマンドの表記規則

2 章、及び 3 章のコマンドの詳細にて記述される、各コマンドの引数の表記規則を表 2-1 に示します。

表 2-1 コマンド引数の表記規則

シンボル	説明
< >	文字列、または値の指定が必要
A | B	A、または B のどちらかを選択
[ ]	省略可能
( )	複数のパラメーターを 1 つの集合として扱う
ITALIC 体	複数のパラメーターに分割

2.2 概要

コマンドライン方式の概要を説明します。

2.2.1 ログイン

login 名：adpro によりシステムにログインします。初回立ち上げ時にはパスワードは設定されていないため、そのままリターンを入力してログインしてください。

```
Ethernet Switch Apresia13000-48X

login: adpro
>
```

TELNET で装置に接続した後、装置にログインせずに放置すると、300 秒後にセッションタイムアウトします。

SSH で装置に接続した後、装置にログインせずに放置すると、600 秒後にセッションタイムアウトします。

2.2.2 コマンド入力

2.2.2.1 コマンド入力文字

コマンドは小文字で入力してください。本コマンドライン方式は大文字/小文字を区別します。

2.2.2.2 入力補完機能

(1) コマンドの入力の際は、そのコマンドを認識可能な文字列のみ入力すればよく、すべての文字列の入力は必要ありません。

(例) "write memory"コマンドを省略して入力

```
# write memory
```

↓

```
# w m
```

(2) 使用可能なコマンドを知りたい場合には、[?]キーを入力してください。入力文字列から選択可能なコマンドを表示します。複数のコマンドが選択できる場合には、選択可能なすべてのコマンドが表示されます。また、パラメーターを設定するコマンドの場合に、[?]キーを入力すると、パラメーター設定範囲を表示することができます。[TAB]キーを入力すると、入力可能なコマンドがあればその文字列をコマンドラインに自動的に表示するため、すべての文字列を入力する必要がありません。例えば"con"という文字列から選択可能なコマンドは"configure"であることを知ることができます。

(例)

```
# con[TAB]キー
```

↓

```
# configure
```

2.2.2.3 設定の取り消し

パラメーターをデフォルト設定に戻す場合には"no"コマンドを用いてください。ただし、"clock set"コマンドは、"no"コマンドを使用できません。

(例) QoS をデフォルト設定(disable)に戻す

```
(config)# no qos enable
```

2.2.2.4 設定の保存

変更内容をフラッシュメモリーに書き込むには、"write memory"コマンドを使ってください。

(例)

```
# write memory
Current running-config is saved to flash-config.
Writing to flash memory...
[OK]
Writing to SD memory...
upload completed.(hc-flash-config)

#
```

2.2.2.5 画面のスクロール

コマンド実行時に表示できる内容が 1 画面に収まらない場合は画面下に"--more--"が表示されます。この状態で[スペース]キーを入力すると 1 画面スクロールし、[Enter]キーを入力すると 1 行、[0]キーを入力すると最後までスクロールします。[q]キーを入力すると、それ以降の表示は行わずにコマンドを終了します。

コンソールの行数が小さく設定されていると、1 画面スクロールの機能が正常に動作しない時があります。その時は、[q]キーなどで抜けた後、ご使用の端末のコンソール行数を大きい値に設定し直してください。

(例)

```
# show running-config
!
!
vlan database
vlan 3 name vlan3
!
interface port 1
!
interface port 2
!
interface port 3
!
interface port 4
!
```

```
interface port 5
!
interface port 6
!
interface port 7
--- more ---
```

2.2.2.6 表示コマンドとの併用コマンド

show コマンドにて設定内容を表示する際に、パイプ" | "を用いて次の 2 つの併用コマンドをつなぐことができます。

表 2-2 表示コマンドとの併用コマンド

併用コマンド	機能
include <WORD>	<WORD>と同一の文字列を含む行のみを表示 ※1、※2
exclude <WORD>	<WORD>と同一の文字列を含まない行のみを表示 ※1、※2

※1 .^$[]*+?|()¥は特殊文字扱いのため、取得できません。

※2 .^$[]*+?|()¥を検索対象とする場合は、これらの文字の前に¥を付けて指定してください。

(例) cli を含まない行のみを表示する。

```
# show logging | exclude cli
Date            Log messages
Mar  1 17:43:03  <system:emerg> Rebooting.
Apr 19 15:44:00  <system:warning> Power up. Start logging.
Apr 19 15:44:00  <device:warning> device rvn0: Initialize start.
Apr 19 15:44:00  <device:info> device rvn0: Initialize done.
Apr 19 15:44:04  <process:info> PtSec : Port Security start
Apr 19 15:44:04  <process:info> FldCtl : Flooding Control start
Apr 19 15:44:05  <process:info> igmpxyd: started.
May  9 12:56:26  <port:warning> Port 23 link up 100BASE-TX, full-duplex, MDI.
May  9 13:00:16  <port:err> Port 23 link down.
May  9 13:00:25  <port:warning> Port 23 link up 100BASE-TX, full-duplex, MDI-X.
May  9 13:02:02  <port:err> Port 23 link down.
May  9 13:03:47  <port:warning> Port 23 link up 100BASE-TX, full-duplex, MDI-X.
May  9 13:10:41  <port:err> Port 23 link down.
May  9 13:10:45  <port:warning> Port 23 link up 100BASE-TX, full-duplex, MDI.
May  9 13:13:27  <port:err> Port 23 link down.
```

2.3 コマンド入力モード

コマンドライン方式におけるコマンド入力モードの状態変移を図 2-1 に示します。基本的な 3 つのコマンドのモードの概要を表 2-3 に、CONFIG モードから図 2-1 の点線内の各コマンド入力モードに移動するために必要なコマンド、及び各モードでのプロンプトを表 2-4 に示します。

本コマンドインターフェースは、最大 8 つの TELNET/SSH セッションにて同時に使用することができます。ただし、複数のユーザーが同時に設定コマンドを発行することを避けるため、一度に CONFIG モードを使用できるのは 1 人のユーザーのみに限定されます。

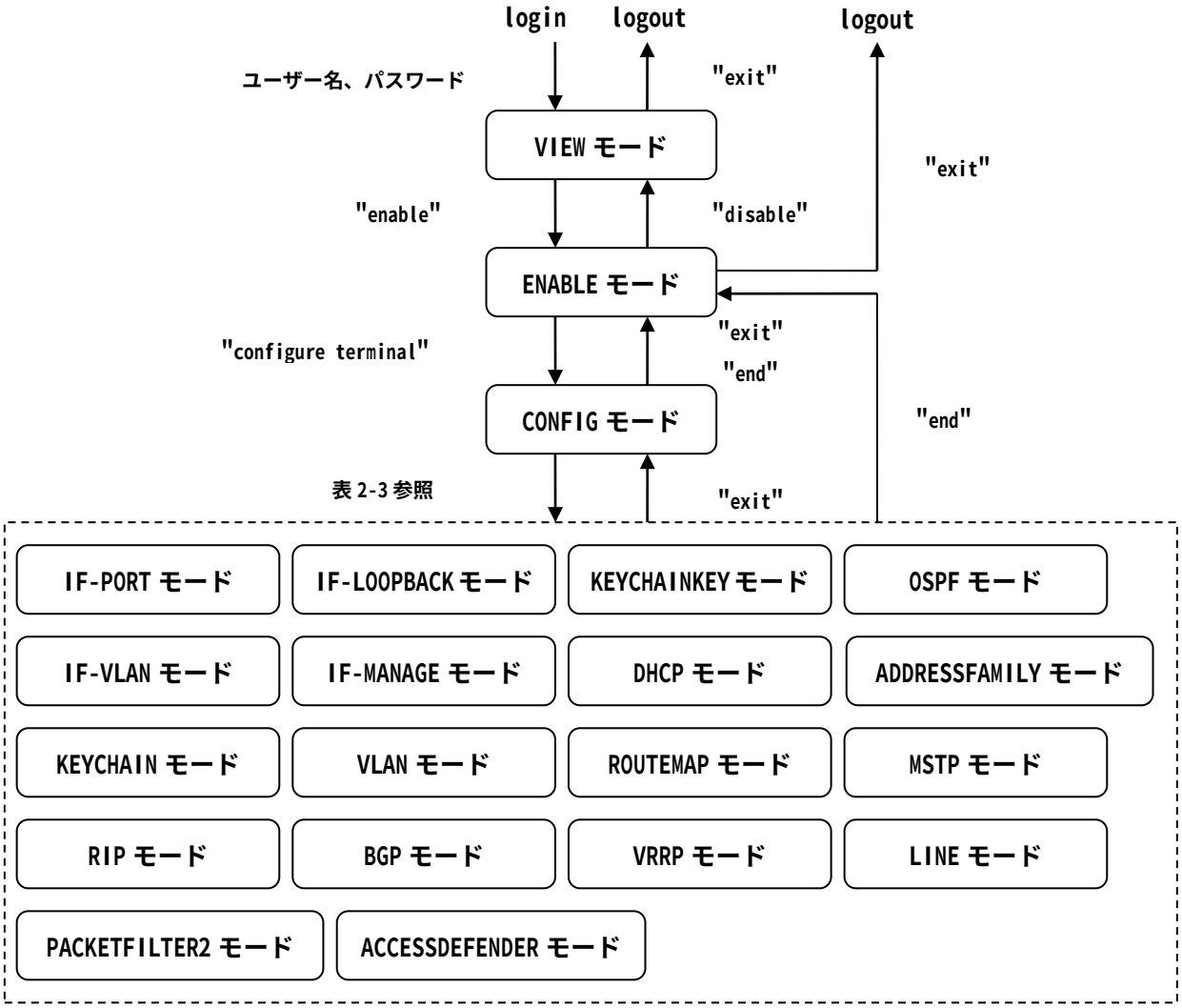


図 2-1 コマンド入力モードの状態変移

(1) CTRL+C、または CTRL+Z の入力で、"end"コマンドの入力と同等の動作をします。

(2) CTRL+D の入力で、"exit"コマンドの入力と同等の動作をします。

表 2-3 コマンド入力モードの概要

コマンド入力モード	概要	プロンプト
VIEW モード	ログイン後の最初に入るモードです。基本的な装置の監視コマンドなどが使用できます。	>
ENABLE モード	設定の変更以外のすべてのコマンド(監視コマンド、設定保存コマンドなど)が使用できるモードです。	#
CONFIG モード	設定の変更を行うモードです。設定する項目によっては、必要に応じてさらに表 2-4 に示すモードへ移行して設定を行います。	(config)#

表 2-4 コマンド入力モードの移動コマンド、及びプロンプト

コマンド入力モード	CONFIG モードからの移動コマンド	プロンプト
IF-PORT モード	interface port <PORT>	(config-if-port)#
IF-VLAN モード	interface vlan <VID>	(config-if)#
IF-MANAGE モード	interface manage	(config-if-mng)#
IF-LOOPBACK モード	interface loopback	(config-if)#
VLAN モード	vlan database	(config-vlan)#
LINE モード	line console line vty <LINENUMBER> [<ENDING_LINENUMBER>]	(config-line)#
PACKETFILTER2 モード	packet-filter2	(config-filter)#
OSPF モード	router ospf <PROCESSID>	(config-router)#
RIP モード	router rip	(config-router)#
BGP モード	router bgp <ASN>	(config-router)#
VRRP モード	router vrrp <VRID>	(config-router)#
ROUTEMAP モード	route-map <MAPNAME> (deny | permit) <SEQVALUE>	(config-route-map)#
KEYCHAIN モード	key chain <CHAINNAME>	(config-keychain)#
KEYCHAINKEY モード	(KEYCHAIN モードから) key <KEYID>	(config-keychain-key)#
DHCP モード	dhcp policy <POLICY_NAME>	(config-dhcp)#
MSTP モード	spanning-tree mst configuration	(config-mst)#
ACCESSDEFENDER モード	access-defender	(config-a-def)#
ADDRESSFAMILY モード	(BGP モードから) address-family ipv4 [multicast | unicast]	(config-router-af)#

※ 機種により、モードの有無、パラメーターの指定範囲が異なります。

2.4 参照アカウント「user」

「user」は本装置の設定を参照することができるアカウントです。本アカウントは本装置の設定を変更することはできませんが、(例)に示したコマンドを使用し、本装置の構成情報を参照することができます。アカウント「user」のパスワードは工場出荷時はなし、アカウント「adpro」でログイン後、変更することができます。

(例)

```
login: user
> ?
Exec commands:
  check       Check configuration
  disable     Turn off privileged mode command
  enable      Turn on privileged mode command
  exit        End current mode and down to previous mode
  ping        Send echo messages
  show        Show running system information
  telnet      user interface to the TELNET protocol
  traceroute  Trace route to destination

>
```

2.5 初期化アカウント「ap_recovery」

「ap_recovery」は装置のパスワード、設定を初期化することができる特別なアカウントです。ログインと同時に、ユーザーが設定したアカウント、パスワードの消去、SD メモリーカードに保存された運用情報(hc-flash-config、hc-software、hc-system-name.txt、hcloader.conf)、フラッシュメモリーに保存された設定の消去、ログの消去、再起動が行われます。アカウント「ap_recovery」のパスワードはありません。本アカウントはコンソールポートのみで有効です。

(例)

```
login: ap_recovery
Jul  6 16:58:01 <system:emerg> Configuration and logs were initialized.
Jul  6 16:58:02 <system:emerg> Rebooting.



HCBOOT   2.02.03
    DIMM slot 1: Not populated
    DIMM slot 0: DDR SDRAM detected
    Initializating ECC memory.  Please wait...
HCLoader 1.01.02
Boot from flash://primary
Expand system ... done

Loading configuration ...done.
```

```
  Firmware Version 7.06.01


Ethernet Switch Apresia13000-48X

login:
```

注意事項

PoE 機能対応機種(Apresia3424GT-PoE/3424GT-HiPoE/5412GT-PoE)では、装置を再起動すると PoE による電源供給は一時的に停止します。

本コマンドを実行しても、以下の情報は初期化されません。初期化コマンドを個別に実行してください。または、3.2.1 "factory-default"コマンドを実行してください。

「ap_recovery」で削除されない情報	初期化コマンド
(1)カスタマイズされた Web 認証ページ	erase login-page erase login-success-page erase login-failure-page erase logout-success-page erase logout-failure-page erase redirect-error-page
(2)証明書	erase ssl-files
(3)ローカルデータベース	erase local-db erase aaa-local-db
(4)ブートスクリプト	copy default-script configured-script copy configured-script flash-script ※1
(5)時刻設定	clock set <HH:MM:SS> [<YYYYMMDD>]

※1 再起動後にも初期化を反映させるために、デフォルトの設定をフラッシュメモリーに保存する必要があります。

3. コマンドの詳細

注意事項

本ファームウェア(AEOS Ver. 7.44)では、本章、及び TD61-7251 AEOS Ver. 7.44 コマンドリファレンス L3 編に記載しているコマンドのみサポートしております。未記載のコマンドを入力した場合の動作は保証されません。

3.1 LOGIN

3.1.1 username

ユーザーの登録・削除を行います。adpro 権限、user 権限合計で 20 ユーザーまで登録可能です。ユーザー名は 31 文字まで設定可能です。登録したユーザーを削除する場合は、no コマンドを使用してください。

コマンドシンタックス

username <USERNAME> adpro | user
no username <USERNAME>

USERNAME	ユーザー名(最大 31 文字)
adpro	adpro 権限
user	user 権限

デフォルト

adpro (adpro 権限)
user (user 権限)

コマンドモード

CONFIG

使用例

(1) adpro 権限のユーザー：tanaka を追加
(2) ユーザー：tanaka を削除

```
> enable
# configure terminal
(config)# username tanaka adpro
(config)# no username tanaka
```

関連コマンド

show running-config

注意事項

ユーザー名に設定できる文字は数字・英大文字・英小文字、.(dot)・_(under bar)・

-(hyphen)のみです。また、ユーザー名の先頭に.(dot)・_(under bar)・-(hyphen)を使用することはできません。

ユーザー追加、削除後に、設定保存コマンドを使用しない場合には、リブート後に元に戻ってしまいます。

一部予約されているユーザー名があり、予約ユーザー名を入力した場合は、エラーメッセージが表示され入力できません。

adpro 権限のユーザーを最低 1 つ残すため、adpro 権限のユーザーをすべて削除することはできません。

3.1.2 password

すでに登録されているユーザーのパスワードを設定します。パスワードは 31 文字まで設定可能です。設定したパスワードを削除する場合は、no コマンドを使用してください。

コマンドシンタックス

[no] password <USERNAME>

USERNAME　　パスワードを設定するすでに登録されているユーザー名

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ユーザー：tanaka のパスワードを変更します。

(2) ユーザー：tanaka のパスワードをデフォルト値に戻します。

```
> enable
# configure terminal
(config)# password tanaka
New password:
Retype new password:
(config)# no password tanaka
```

関連コマンド

show running-config

注意事項

ユーザー名に設定できる文字は数字・英大文字・英小文字、.(dot)・_(under bar)・-(hyphen)のみです。また、ユーザー名の先頭に-(hyphen)を使用することはできませ

ん。

パスワードに設定できる文字は空白、図形文字(0x21～0x7E)のみです。

パスワード変更後に設定保存コマンドを使用しない場合にはリブート後にパスワードが元に戻ってしまいます。

パスワードはシステム保護上非常に重要な情報となります。従って、他人に解読されないような複雑な文字列を入力ください。また、決して、忘れないでください。

3.49.1 "show running-config"、3.49.2 "show flash-config"では設定したパスワードが暗号化されて表示されます。

3.1.3 show username

登録されている全ユーザー、及びユーザーの権限を表示します。

コマンドシンタックス

show username

コマンドモード

VIEW, ENABLE

使用例

(1) 全ユーザー、及びユーザーの権限を表示します。

```
> enable
# show username
username                        authority
-----------------------------------------
adpro                           adpro
tanaka                          adpro
suzuki                          user
user                            user
```

username　　：ユーザー名
authority　　：権限
　adpro　　：管理者権限
　user　　：参照権限

関連コマンド

show running-config

注意事項

3.1.4 show users

現在ログインしているユーザー名を表示します。

コマンドシンタックス

show users

コマンドモード

ENABLE

使用例

(1) 現在ログインしているユーザー名を表示します。

```
# show users

User                            Login time      From
-------------------------------------------------------------
adpro                           Mar 21 14:22    console
```

User　　：ログインしているユーザー名
Login time　　：ログインした時間
From　　：ログイン元
　<IPADDR>　　：IP アドレス
　console　　：コンソール

関連コマンド

注意事項

3.2 factory-default

3.2.1 factory-default

フラッシュメモリーに設定されている構成情報を工場出荷状態へ初期化します。

include-license オプションをつけることにより、初期化対象にライセンスを含みます。本コマンド実行後は自動で再起動が行われます。本コマンドはコンソールポートでのみ実行可能です。

ap_recovery、factory-default、factory-default include-license コマンドの初期化対象ファイルを表 3-1 に示します。

表 3-1 初期化対象ファイル(○：初期化対象に含む)

ファイル	説明	ap_recovery	factory-default	factory-default include-license
flash-config	flash-config	○	○	○
aaa-local-db	ローカルデータベース	-	○	○
local-db	NA ローカルデータベース	-	○	○
login-page	ログイン認証ページ	-	○	○
login-success-page	認証成功ページ	-	○	○
login-failure-page	認証失敗ページ	-	○	○
logout-success-page	ログアウト成功ページ	-	○	○
logout-failure-page	ログアウト失敗ページ	-	○	○
redirect-error-page	リダイレクト失敗ページ	-	○	○
https-certificate, ssl-files	証明書	-	○	○
https-private-key, ssl-files	秘密鍵	-	○	○
ssh-rsa-key	RSA ホスト鍵対 (SSH プロトコルバージョン 1)	○	○	○
ssh-rsa1-key	RSA ホスト鍵対 (SSH プロトコルバージョン 2)	○	○	○
ライセンス(L3、NA)	ライセンス(L3、NA)	-	-	○
ログ (バッファメモリー)	ログ (バッファメモリー)	○	○	○
ログ(SRAM)	ログ(SRAM)	○	○	○
ブートスクリプト	ブートスクリプト	-	○	○
時刻設定	時刻設定	-	○	○
hc-flash-config (SD メモリーカード)	flash-config (SD メモリーカード)	○	○	○
hc-software (SD メモリーカード)	ファームウェア (SD メモリーカード)	○	○	○
hc-system-name.txt (SD メモリーカード)	ファームウェアのシステムバージョン (SD メモリーカード)	○	○	○
hcloader.conf (SD メモリーカード)	SD メモリーカード起動ブートスクリプト	○	○	○

ファイル	説明	ap_recovery	factory-default	factory-default include-license
	(SD メモリーカード)			

コマンドシンタックス

factory-default [include-license]

include-license　初期化対象にライセンスを含む

コマンドモード

ENABLE

使用例

(1) フラッシュメモリーに設定されている構成情報を工場出荷状態に初期化します。

```
# factory-default include-license
initialize factory-default? (y/n): y
Initializing ...
done.
erase backup-clone-files
hcloader.conf
done.
hc-flash-config
done.
hc-software
done.
hc-system-name.txt
done.
Jan  1 09:00:04  <system:emerg> Rebooting.
Write log messages to flash memory ... Done


HCBOOT   2.02.03
    DIMM slot 1: Not populated
    DIMM slot 0: DDR SDRAM detected
    Initializating ECC memory.  Please wait...
HCLoader 1.11.02
Boot from flash://primary
Expand system ... done

Loading configuration ...done.

  Firmware Version 7.32.01



Ethernet Switch Apresia13000-48X
```

```
login:
```

関連コマンド

注意事項

再起動後ループが発生する恐れがあるため本コマンドを実行する際は、装置をネットワークから切り離してください。

3.3 ホスト名

3.3.1 hostname

本装置のホスト名を設定します。ホスト名を設定すると、プロンプトにホスト名が表示されるようになります。ホスト名を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

hostname <NAME>
no hostname

NAME　　ホスト名 <1-254(文字)>
- ASCII コードの印字可能な文字のうち、[?]を除いた文字のみ使用可能
- 先頭文字はアルファベット・数字のみ使用可能

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ホスト名を Switch に設定します。

```
> enable
# configure terminal
(config)# hostname Switch
Switch(config)#
```

関連コマンド

show running-config

注意事項

本コマンドは、再ログインまたはロギング機能のコマンドを実行することで装置へ保存するログメッセージへも反映されます。ただしその場合でも、Syslog サーバーへ送信されるログメッセージには反映されません。

3.4 ログインメッセージ

装置にアクセスした際に、ユーザーが設定したメッセージを表示することによりログイン前に装置情報を表示し、誤アクセスを防止する機能です。

3.4.1 login-message

本装置へのログイン時に表示するログインメッセージを設定します。設定したログインメッセージを削除する場合は、no コマンドを使用してください。

設定したログインメッセージはコンソールログイン、TELNET/SSH ログインのいずれの場合でも有効です。ただし、SSH ログイン時に、SSH プロトコルバージョン 1 を使用している場合には表示されません。ログインメッセージは ASCII 文字を使用し最大 255 文字まで設定でき、"¥"を指定した場合は出力時に改行されて表示されます。

コマンドシンタックス

login-message <LINE>
no login-message
　　LINE　　表示する文字列 <1-255(文字)>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ログインメッセージを設定します。
(2) 実際のログインメッセージの出力例を示します。

```
> enable
# configure terminal
(config)# login-message Apresia ¥Apresia13000 ¥No1
(config)# exit
# exit
Apresia
Apresia13000
No1

Ethernet Switch Apresia13000-48X

login:
```

関連コマンド

show running-config

注意事項

3.4.2 show login-message

ログインメッセージを表示します。

コマンドシンタックス

show login-message

コマンドモード

VIEW, ENABLE

使用例

(1) ログインメッセージを表示します。

```
# show login-message
Login Message: Apresia ¥Apresia13000 ¥No1
```

関連コマンド

注意事項

3.5 IP アドレス

3.5.1 ip address

管理ポート、または VLAN に IP アドレスを設定します。IP アドレスを削除する場合は、no コマンドを使用してください。

VLAN には、インターフェース当たり、プライマリーIP アドレスが 1 つ、セカンダリーIP アドレスを 14 個まで、計 15 個の IP アドレスを設定できます。

管理ポートには、1 つのプライマリーIP アドレスを設定できます。

IF-LOOPBACK モードでは、プライマリーIP アドレス(secondary オプションをつけない設定)が 14 個まで設定できます。

セカンダリーIP アドレスは、プライマリーIP アドレスを設定していない状態では設定できません。また、プライマリーIP アドレスは、セカンダリーIP アドレスを設定した状態では削除できません。

IP アドレス最大設定数を表 3-2 に示します。

表 3-2 各 IP アドレス最大設定数

IP アドレス	最大設定数
プライマリー IP アドレス	255
セカンダリー IP アドレス	Apresia13000 シリーズ：1000 Apresia3400/4300/5400 シリーズ：100
ループバック IP アドレス	14

※ 装置に登録可能な IP アドレス総数(プライマリー/セカンダリー/ループバック)の最大設定数は、各 IP アドレスの設定数により変動します。

コマンドシンタックス

```
ip address <IPADDR/MASK> | ( <IPADDR> <NETMASK> ) [ secondary ]
no ip address [ <IPADDR/MASK> | ( <IPADDR> <NETMASK> ) [ secondary ] ]
```

IPADDR	IP アドレス
MASK	ネットマスク長
NETMASK	ネットマスク
secondary	セカンダリーIP アドレスを指定

デフォルト

なし(＝設定なし)

コマンドモード

IF-VLAN, IF-MANAGE, IF-LOOPBACK

使用例

(1) 管理ポートに IP アドレス：192.168.0.1、ネットマスク長：24 ビットを設定します。
(2) VLAN ID：1 に IP アドレス：10.1.1.1、ネットマスク長：8 ビットを設定します。
(3) VLAN ID：1 の IP アドレスを削除します。

```
> enable
# configure terminal
```

```
(config)# interface manage
(config-if-mng)# ip address 192.168.0.1/24
(config-if-mng)# exit
(config)# interface vlan 1
(config-if)# ip address 10.1.1.1/8
(config-if)# no ip address
```

関連コマンド

show ip address, show running-config

注意事項

VLAN インターフェースにセカンダリーIP アドレスを設定している状態で、プライマリーIP アドレスの削除はできません。プライマリーIP アドレスを変更する場合は、プライマリーIP アドレスの上書きを行ってください。

VLAN インターフェースにセカンダリーIP アドレスを 14 個設定している状態で、プライマリーIP アドレスの上書きはできません。プライマリーIP アドレスを変更する場合、セカンダリーIP アドレスを 1 つ以上削除してからプライマリーIP アドレスの上書きを行ってください。

セカンダリーIP アドレスを設定している VLAN の削除はできません。当該 VLAN を削除する場合、セカンダリーIP アドレスの消去後に行ってください。

IF-LOOPBACK モードでは、セカンダリーIP アドレスの設定はできません。

VLAN の IP アドレスを変更する場合は、DHCP 機能を無効にしてから行ってください。

IP アドレスの設定数に応じて、パケットフィルター2 のグループを使用します。詳しくは、表 3-20 各 IP アドレス最大設定数と使用するルール数、表 3-21 IP アドレスで使用するルール数とグループ数を参照してください。また、パケットフィルター2 のグループは昇番で使用されるため、IP アドレス設定に必要なグループがすでに使用されている場合、IP アドレスを設定できません。

セカンダリーIP アドレスを設定し、同一 VLAN インターフェース間でルーティングさせる場合は、"ip icmp redirect send disable"コマンドを設定してください。

3.5.2 show ip address

管理ポート、及び VLAN インターフェースに設定された IP アドレスを表示します。ループバックインターフェースの IP アドレスは表示されません。

コマンドシンタックス

show ip address

コマンドモード

VIEW, ENABLE

使用例

(1) IP アドレスを表示します。

```
# show ip address
  manage      172.17.51.177/24
  vlan 1      192.168.0.10/24
```

関連コマンド

注意事項

3.6 IP ルート情報

IP ルート情報を参照/設定します。ループバックインターフェース、VLAN インターフェース、管理ポートを一つのルーティングテーブルとして管理しています。ただし、管理ポートと VLAN インターフェース間の中継はできません。

例えば、管理ポートの IP アドレス宛、もしくは管理ポートの直接接続経路をネクストホップとする IP パケットが、VLAN インターフェースから届くような場合は、先の制限によって管理ポート側に中継できませんので、ネットワーク設計する際はご注意ください。

なお、L3 ライセンスが無効の場合、VLAN インターフェース間の中継もできません。VLAN インターフェース間を中継させる場合は、L3 ライセンスを別途購入する必要があります。ライセンスの購入方法については、弊社営業、または代理店にお問い合せください。

3.6.1 ip route

スタティックルートを設定します。最大設定数は、Apresia13000 シリーズが 12000 個、Apresia3400 シリーズ、Apresia5400 シリーズが 8000 個です。スタティックルートを削除する場合は、no コマンドを使用してください。

デフォルトゲートウェイを設定する場合は、宛先のネットワークアドレス、及びネットマスク長に 0 を指定してください。

コマンドシンタックス

[no] ip route (<DEST> <NETMASK>) | <DEST/MASK> <GATEWAY> | null [<DISTANCE>]

DEST	宛先ネットワークアドレス
NETMASK	ネットマスク
MASK	ネットマスク長
GATEWAY	ゲートウェイ IP アドレス
null	NULL インターフェース(パケットを破棄)
DISTANCE	管理距離 <1-255>

デフォルト

DISTANCE：1

コマンドモード

CONFIG

使用例

(1) ネットワークアドレスを 192.168.2.0、ネットマスク長を 24 ビット(255.255.255.0)、ゲートウェイアドレスを 192.168.1.2 に設定します。
(2) (1)の経路を削除します。
(3) デフォルトゲートウェイを 192.168.1.2 に設定します。

```
> enable
# configure terminal
(config)# ip route 192.168.2.0/24 192.168.1.2
(config)# no ip route 192.168.2.0/24 192.168.1.2
(config)# ip route 0.0.0.0/0 192.168.1.2
```

関連コマンド

show ip route, show running-config

注意事項

L3 ライセンスが設定されてない場合、<DISTANCE>、NULL インターフェースを指定できません。

他のルーティング機能(OSPF、RIP)の IPv4 ルートと管理距離が等しくならないように設定してください。

3.6.2 show ip route

IP フォワーダが実際にフォワーディング処理で使用しているルーティングテーブル(Forwarding Information Base：FIB)を表示します。オプションを指定すると指定したエントリーのみ表示します。

コマンドシンタックス

show ip route [<IPADDR> | <IPADDR/MASK> | bgp | connected | static | ospf | rip]

IPADDR	宛先 IP アドレス
IPADDR/MASK	宛先 IP アドレス/ネットマスク長
bgp	BGP 経路
connected	直接接続経路
static	スタティック経路
ospf	OSPF 経路
rip	RIP 経路

コマンドモード

VIEW, ENABLE

使用例

(1) ルーティングテーブル(Forwarding Information Base：FIB)を表示します。

```
# show ip route
Codes: K - kernel route, 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
       * - candidate default

C       127.0.0.0/8 is directly connected, loopback
C       172.21.30.0/24 is directly connected, vlan 2
```

関連コマンド

注意事項

L3 ライセンスが設定されてない場合、BGP 経路、OSPF 経路、RIP 経路を指定できません。

管理ポート("interface manage")に設定された IP アドレスの情報も反映されます。

3.6.3 show ip route database

装置が学習しているすべてのルーティングテーブルの情報を表示します。オプションを指定すると指定したエントリーのみ表示します。

本コマンドで表示するテーブルには、「宛先のインターフェース(VLAN、またはループバック)が決定できないエントリー」、「複数ある同一経路宛のエントリーで優先度が低いエントリー」などの FIB(Forwarding Information Base：FIB)に反映されないエントリーも含んでいます。FIB の表示は"show ip route"を参照してください。

優先度は、ルーティングエントリーの属性ごとに決められており、デフォルトでは以下の順で高優先度になっています。

1. 直接接続ネットワーク宛のエントリー
2. "ip route"コマンドで設定したエントリー
3. 外部 BGP(eBGP)で学習したエントリー
4. OSPF で学習したエントリー
5. RIP で学習したエントリー
6. 内部 BGP(iBGP)で学習したエントリー

同一ネットワーク宛エントリーが複数ある場合は最も高優先のエントリーが FIB に反映されます。static、OSPF、RIP、及び BGP の優先関係は、それぞれの"distance"の設定値("ip route"、OSPF "distance"、RIP "distance"(TD61-7251 AEOS Ver. 7.44 コマンドリファレンス L3 編)を参照)を変えることにより変更できます。

コマンドシンタックス

show ip route database [bgp | connected | ospf | rip | static]

bgp	BGP 経路
connected	直接接続経路
ospf	OSPF 経路
rip	RIP 経路
static	スタティック経路

コマンドモード

VIEW, ENABLE

使用例

(1) 装置のルーティングテーブルの情報を表示します。

```
# show ip route database
codes: K - kernel route, 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
        > - selected route, * - FIB route, p - stale info

S    *> 0.0.0.0/0 [1/0] via 172.21.30.1, vlan 2
C    *> 127.0.0.0/8 is directly connected, loopback
C    *> 172.21.30.0/24 is directly connected, vlan 2
```

関連コマンド

注意事項

L3 ライセンスが設定されてない場合、BGP、OSPF 経路、RIP 経路を指定できません。

3.6.4 show ip route cache

レイヤー3 スイッチングに使用するルーティングキャッシュテーブルを表示します。

動的に学習した ARP エントリーに対応する L3 キャッシュは、3.17 スパニングツリープロトコル(STP/RSTP/MSTP)、3.42 MMRP-Plus などの経路切り替えに伴う FDB フラッシュ(3.14.5 "clear mac-address-table"コマンド含む)によって、動的に学習した MAC アドレスの消去と連動して消去されます。その後、消去された宛先へ通信開始時(アドレス解決動作後)に再登録されます。

コマンドシンタックス

show ip route cache

コマンドモード

VIEW, ENABLE

使用例

(1) レイヤー3 スイッチングに用いるルーティングキャッシュテーブルを表示します。

```
# show ip route cache
Total layer 3 cache addresses : 3 (LPM = 2, cache = 1)

  destination          type   VID MAC address        port age
  0.0.0.0/0            LPM      1 00:40:66:11:a5:b2     7 --:--
  172.21.29.0/24       LPM   ---- --:--:--:--:--:--   CPU --:--
  172.21.29.1/32       cache    1 00:40:66:11:a5:b2     7 00:00:02
```

destination　：宛先の IP アドレス
type　：cache：L3 キャッシュ、または LPM：Longest Prefix Match
VID　：ネクストホップゲートウェイが属する VLAN ID
MAC address　：ネクストホップゲートウェイの MAC アドレス
port　：ネクストホップゲートウェイが接続されているポート
　BLOCK　：該当する IP アドレス宛のパケットを破棄
　CPU　：本装置に設定された IP ネットワーク
age　：この IP アドレスを宛先/送信元に持つ IP パケットが最後に
　レイヤー3 スイッチングされてからの経過時間

関連コマンド

注意事項

本コマンドは、L3 ライセンスが設定時のみ有効です。

3.6.5 show ip route summary

ルーティングテーブルの概略情報を表示します。

コマンドシンタックス

show ip route summary

コマンドモード

VIEW, ENABLE

使用例

(1) ルーティングテーブルの概略情報を表示します。

```
# show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 8
Route Source    Networks
connected       4
static          10
Total           59
FIB             45
```

関連コマンド

注意事項

3.7 インターフェース

表 3-3 に示すインターフェース、ループバック(装置内部の仮想ポート、DOWN しない性質を持つ)、及び管理ポート(10/100 Mbps ポート)の設定を行います。

表 3-3 設定項目一覧

	管理ポート 10/100 Mbps	UTP ポート 10/100 Mbps	UTP ポート 10/100/1000 Mbps	GBIC ポート (メディア SFP-T 使用) 1000 Mbps	GBIC ポート (メディア SFP-T 使用) 10/100/1000 Mbps	GBIC ポート (メディア SFP-SX、LXM、LX、LX40、ZX、BX10、BX20、BX40、BX80、CWDM 使用時) 1 Gbps	XENPAK ポート 10 Gbps
Apresia 3424GT-SS 3424GT-SS2 3424GT-PoE 3424GT-HiPoE 3448GT	-	○	○	-	○	○	-
Apresia 3448G-PSR 3448G-PSR2	-	○	-	-	○	○	-
Apresia 13000 シリーズ	○	-	○	○	-	○	○
Apresia 4328GT	○	-	○	○	-	○	-
Apresia 4348 シリーズ	○	-	○	-	-	○	-
Apresia 5400 シリーズ	○	-	○	-	○	○	-

注意事項

GigabitEthernet の UTP ポートは、自動 MDI-X 認識機能が無効な場合、mdi-x 設定に応じたモードとなります。

Apresia13000-48X の 41～44 ポートで SFP-T メディアを使用した場合、メディアを認識(挿抜時のログ出力、"show interface status"コマンドの表示)しますが、動作はしません。SFP-T メディアを使用する場合は、45～48 ポートで使用し、"media"コマンドで utp を設定してください。

Apresia13000-24GX の 21～24 ポートで SFP-T メディアを使用した場合、メディアを認識(挿抜時のログ出力、"show interface status"コマンドの表示)しますが、動作

はしません。SFP-T メディアを使用する場合は、1～20 ポートで使用し、"media"コマンドで utp を設定してください。

Apresia4300 シリーズ、及び Apresia5400 シリーズの管理ポートは MDI 固定です。

Apresia13000 シリーズの管理ポートは、自動認識機能("auto-negotiation")有効時に自動 MDI-X 認識機能("auto-mdi-x")が有効となります。自動認識機能無効時は MDI となります。

3.7.1 shutdown

各ポートを閉塞(shutdown)します。ポートの閉塞を解除する場合は、no コマンドを使用してください。

コマンドシンタックス

[no] shutdown

デフォルト

no shutdown(＝非閉塞状態)

コマンドモード

IF-PORT, IF-MANAGE, IF-LOOPBACK(a), IF-VLAN(b)

(a) ループバックインターフェースの閉塞はできません。IF-LOOPBACK モードにおいて、shutdown コマンドは、コマンド補完、Help のメニューに表示されますが、実際のコマンドの入力時にはエラーになります。

(b) VLAN を shutdown した場合は、該当する VLAN が関わる L3 の動作(自 IP アドレス宛てのパケットの送受信)が停止しますが、VLAN 内の L2 フォワーディングの動作は継続されます。L2 のフォワーディングを停止する場合は、vlan mode コマンドで VLAN を Disable に設定してください。

使用例

(1) ポート：1～5、及びポート：8 を閉塞状態にします。
(2) ポート：1～5、及びポート：8 の閉塞状態を解除します。

```
> enable
# configure terminal
(config)# interface port 1-5,8
(config-if-port)# shutdown
(config-if-port)# no shutdown
```

関連コマンド

show interface status(manage ポート vlan の状態を除く), show running-config

注意事項

3.7.2 auto-shutdown port

リンクダウン時の自動 shutdown 機能を設定します。設定を削除する場合は、no コマンドを使用してください。

指定ポートはリンクダウン後、保護時間("auto-shutdown timer"で設定)経過後に shutdown が自動的に設定されます。リンクダウン状態で本コマンドを入力すると、保護時間経過後に shutdown が自動的に設定されます。

コマンドシンタックス

auto-shutdown port <PORTRANGE>
no auto-shutdown port [<PORTRANGE>]
　　PORTRANGE　　ポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1～5 に自動 shutdown 機能を設定します。
(2) ポート：1～5 の自動 shutdown 機能を削除します。

```
> enable
# configure terminal
(config)# auto-shutdown port 1-5
(config)# no auto-shutdown port 1-5
```

関連コマンド

show auto-shutdown, show running-config

注意事項

3.7.3 auto-shutdown timer

自動 shutdown 機能の保護時間を設定します。デフォルトに戻す場合は、no コマンドを使用してください。

"auto-shutdown port"の指定ポートは、リンクダウン後の保護時間経過後に shutdown が自動的に設定されます。実際の保護時間は設定値＋500 ミリ秒です。

"no shutdown"実施直後、及び装置起動直後の保護時間は設定値＋10 秒です。

コマンドシンタックス

auto-shutdown timer <TIME>
no auto-shutdown timer
　　TIME　　保護時間 <500-10000(ミリ秒)>
　　• 任意の数値を設定可能だが、実際の動作時は 500 ミリ秒単位で切り上げ

デフォルト
0(ミリ秒)

コマンドモード
CONFIG

使用例
(1) 自動 shutdown 機能の保護時間を 1000 ミリ秒に設定します。
(2) 自動 shutdown 機能の保護時間をデフォルトに戻します。

```
> enable
# configure terminal
(config)# auto-shutdown timer 1000
(config)# no auto-shutdown timer
```

関連コマンド
show auto-shutdown, show running-config

注意事項

再リンク処理が発生するコマンド実行時に自動 shutdown 機能が動作する場合があります。

3.7.4 auto-negotiation

自動認識機能を無効に設定します。有効にする場合は、no コマンドを使用してください。設定は使用しているメディアタイプを指定して行います。utp、gbic の指定をメディアタイプの対象ポート外で行っても、装置の動作に影響はありません。

コマンドシンタックス
IF-MANAGE モード
[no] auto-negotiation disable
IF-PORT モード
[no] utp | gbic auto-negotiation disable

utp	UTP メディアを指定
gbic	GBIC(SFP)メディアを選択

デフォルト
no disable(＝自動認識機能有効)

コマンドモード
IF-PORT, IF-MANAGE

使用例
(1) ポート：1 の自動認識機能を無効に設定します。

(2) ポート：41～42 の GBIC ポートの自動認識機能を無効に設定します。
(3) ポート：41～42 の GBIC ポートの自動認識機能を有効に設定します。

```
> enable
# configure terminal
(config)# interface port 1
(config-if-port)# utp auto-negotiation disable
(config-if-port)# exit
(config)# interface port 41-42
(config-if-port)# gbic auto-negotiation disable
(config-if-port)# no gbic auto-negotiation disable
```

関連コマンド

show interface status, show running-config

注意事項

1G ポートにて SFP-FX モジュールを使用した場合、自動認識機能("auto-negotiation")を使用できません。

接続対向ポートの自動認識機能("auto-negotiation")は、共に有効状態、あるいは共に無効状態に設定してお使いください。

UTP ポートは規格上、自動認識機能(auto-negotiation)無効時に 1Gbps がサポートされません。

3.7.5 link-speed-duplex

各ポートの通信速度、及び全二重/半二重の設定をします。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

IF-MANAGE モード

link-speed-duplex 10m/half | 10m/full | 100m/half | 100m/full
no link-speed-duplex

IF-PORT モード

utp link-speed-duplex 10m/half | 10m/full | 100m/half | 100m/full
no utp link-speed-duplex

10m/half	10M/半二重を設定
10m/full	10M/全二重を設定
100m/half	100M/半二重を設定
100m/full	100M/全二重を設定

デフォルト

100m/half(＝100M/半二重)

コマンドモード

IF-PORT, IF-MANAGE

使用例

(1) ポート：1～8 を 10M/半二重に設定します。

```
> enable
# configure terminal
(config)# interface port 1-8
(config-if-port)# utp link-speed-duplex 10m/half
```

関連コマンド

show interface status, show running-config

注意事項

設定を有効にするには、自動認識機能("auto-negotiation")を無効状態にする必要があります。

3.7.6 advertise delete

各ポートの自動認識において advertise する通信速度、及び全二重/半二重(通信モード)を削除します。追加する場合は、no コマンドを使用してください。デフォルトでは、設定可能なすべての通信モードが advertise されます。

コマンドシンタックス

utp advertise delete <*10M*> | <*100M*> | <*1G*> | <*HALF*> | <*FULL*>
no utp advertise delete [<*10M*> | <*100M*> | <*1G*> | <*HALF*> | <*FULL*>]
10M = 10m-speed | 10m/half | 10m/full
100M = 100m-speed | 100m/half | 100m/full
1G = 1g/full
HALF = half-duplex
FULL = full-duplex

10m-speed	10M/半二重、及び 10M/全二重を削除
100m-speed	100M/半二重、及び 100M/全二重を削除
10m/half	10M/半二重を削除
10m/full	10M/全二重を削除
100m/half	100M/半二重を削除
100m/full	100M/全二重を削除
1g/full	1G/全二重を削除
half-duplex	10M/半二重、及び 100M/半二重を削除
full-duplex	10M/全二重、100M/全二重、及び 1G/全二重を削除

デフォルト

なし(＝インターフェースに設定可能なすべての通信モードが有効)

コマンドモード
IF-PORT

使用例
(1) ポート：1～8 の advertise を 1G/全二重のみに設定します。
(2) ポート：1～8 の advertise をデフォルト値に戻します。

```
> enable
# configure terminal
(config)# interface port 1-8
(config-if-port)# utp advertise delete 10m-speed
(config-if-port)# utp advertise delete 100m-speed
(config-if-port)# no utp advertise delete
(config-if-port)# exit
```

関連コマンド
show interface status, show running-config

注意事項

自動認識においては、リンクパートナーが advertise によって互いに設定可能な通信モードを通知し合うことにより、最適な通信モードを決定します。リンクパートナー間で通信モードが一致しない場合、リンクは確立しません。

3.7.7 auto-mdi-x

自動 MDI-X 認識機能を無効に設定します。有効にする場合は、no コマンドを使用してください。自動 MDI-X 認識機能を有効に設定すると、UTP クロス/ストレートケーブルのどちらでも使用できるようになります。

コマンドシンタックス
[no] utp auto-mdi-x disable

デフォルト
no disable(＝自動 MDI-X 認識機能有効)

コマンドモード
IF-PORT

使用例
(1) ポート：1 の自動 MDI-X 認識機能を無効に設定します。
(2) ポート：1 の自動 MDI-X 認識機能を有効に設定します。

```
> enable
# configure terminal
(config)# interface port 1
```

```
(config-if-port)# utp auto-mdi-x disable
(config-if-port)# no utp auto-mdi-x disable
```

関連コマンド

show interface status, show running-config

注意事項

自動認識機能("auto-negotiation")が無効な場合、自動 MDI-X 認識機能が有効であっても、MDI、MDI-X の自動選択は行われず、管理ポート、UTP ポート(10/100/1000 Mbps)、及び GBIC ポート(SFP-T 使用時)では MDI、UTP ポート(10/100 Mbps)では MDI-X で動作します。

3.7.8 mdi-x

各ポートを MDI-X に設定します。設定をデフォルト状態に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

[no] utp mdi-x enable

デフォルト

no enable

コマンドモード

IF-PORT

使用例

(1) ポート：1 を MDI-X に設定します。
(2) ポート：1 をデフォルトに設定します。

```
> enable
# configure terminal
(config)# interface port 1
(config-if-port)# utp mdi-x enable
(config-if-port)# no utp mdi-x enable
```

関連コマンド

show interface status, show running-config

注意事項

自動 MDI-X 認識機能("auto-mdi-x")が有効な場合、MDI、MDI-X の自動選択が行われ、本設定は反映されません。

自動認識機能("auto-negotiation")が無効な場合のデフォルト値は、管理ポート、UTP ポート(10/100/1000 Mbps)、及び GBIC ポート(SFP-T 使用時)では MDI、UTP ポート(10/100 Mbps)では MDI-X となります。

3.7.9 mdi

各ポートをMDIに設定します。設定をデフォルト状態に戻す場合は、noコマンドを使用してください。

コマンドシンタックス

[no] utp mdi enable

デフォルト

no enable

コマンドモード

IF-PORT

使用例

(1) ポート：1をMDIに設定します。
(2) ポート：1をデフォルトに設定します。

```
> enable
# configure terminal
(config)# interface port 1
(config-if-port)# utp mdi enable
(config-if-port)# no utp mdi enable
```

関連コマンド

show interface status, show running-config

注意事項

自動 MDI-X 認識機能("auto-mdi-x")が有効な場合、MDI、MDI-X の自動選択が行われ、本設定は反映されません。

自動認識機能("auto-negotiation")が無効な場合のデフォルト値は、管理ポート、UTP ポート(10/100/1000 Mbps)、及び GBIC ポート(SFP-T 使用時)では MDI、UTP ポート(10/100 Mbps)では MDI-X となります。

3.7.10 pause

各ポートの 802.3x フロー制御を有効にします。無効にする場合は、no コマンドを使用してください。802.3x フロー制御有効時も pause フレームは送信されません。

コマンドシンタックス

[no] pause enable

デフォルト
no enable(＝フロー制御無効)

コマンドモード
IF-PORT

使用例
(1) ポート：1～5 の 802.3x フロー制御を有効にします。
(2) ポート：1～5 の 802.3x フロー制御を無効にします。

```
> enable
# configure terminal
(config)# interface port 1-5
(config-if-port)# pause enable
(config-if-port)# no pause enable
```

関連コマンド
show interface status, show running-config

注意事項

リンクアップした状態で"pause enable"/"no pause enable"を行うとリンクダウンが発生します。

3.7.11 media

ポートのメディアタイプを設定します。UTP 専用ポート、XENPAK 専用ポートには設定できません。
SFP-T メディアを使用する場合は、メディアタイプに utp を選択してください。各機種のサポートメディアタイプは各機種の標準仕様書、及び TD61-3584 Apresia2000/3000/4000/5000/13000 シリーズ適合トランシーバー対応表を参照ください。

コマンドシンタックス
media gbic | utp
no media

gbic	GBIC(SFP)メディア
utp	UTP メディア

デフォルト
gbic

コマンドモード
IF-PORT

使用例

(1) GigabitEthernet ポート：41～42 のメディアタイプを UTP に設定します。

```
> enable
# configure terminal
(config)# interface port 41-42
(config-if-port)# media utp
```

関連コマンド

show interface status, show running-config

注意事項

Apresia13000-48X の 41～44 ポートは、SFP-T のメディアを認識(挿抜時のログ出力、"show interface status"の表示)しますが、SFP-T をサポートしていません。SFP-T を使用する場合は、45～48 ポートで使用してください。

Apresia13000-24GX の 21～24 ポートは、SFP-T のメディアを認識(挿抜時のログ出力、"show interface status"の表示)しますが、SFP-T をサポートしていません。SFP-T を使用する場合は、1～20 ポートで使用してください。

Apresia4348 の 45～48 ポートは、SFP-T のメディアを認識(挿抜時のログ出力、"show interface status"の表示)しますが、SFP-T をサポートしていません。SFP-T を使用する場合は、1～44 ポートで使用してください。

3.7.12 description

各ポートの識別を容易にするためのポート名を設定します。設定されたポート名は"show interface status"コマンドで表示されます。

コマンドシンタックス

description <LINE>
no description

LINE	ポート名 <1-64(文字)> (空白文字を含む)

デフォルト

なし(＝設定なし)

コマンドモード

IF-PORT

使用例

(1) ポート：1～2 のポート名を apresia に設定します。

```
> enable
# configure terminal
(config)# interface port 1-2
```

```
(config-if-port)# description apresia
```

関連コマンド

show interface status, show running-config

注意事項

3.7.13 counter-mode txdiscard only-buffer-overflow

TxDiscard のカウンターモードをバッファオーバーカウントモードに設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

本モードの設定により、"show interface counters"における TxDiscard のカウント条件が変更されます。TxDiscard のカウント条件を表 3-4 に示します。

表 3-4 TxDiscard のカウント条件

カウンターモード	TxDiscard のカウント条件
バッファオーバーカウントモード未設定時(デフォルト)	カウントアップしません(0 固定)。
バッファオーバーカウントモード設定時	送信ポートのバッファが溢れた場合 ※ show interface counters における BfOverflow の値をカウントします。

コマンドシンタックス

counter-mode txdiscard only-buffer-overflow
no counter-mode txdiscard

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) TxDiscard のカウンターモードをバッファオーバーカウントモードに設定します。
(2) TxDiscard のカウンターモードをデフォルトに戻します。

```
(config)# counter-mode txdiscard only-buffer-overflow
The counter value will be correct after rebooting.
(config)# no counter-mode txdiscard
The counter value will be correct after rebooting.
```

関連コマンド

show interface counters, show running-config

注意事項

カウンターモードを変更した場合は、必ず、装置を再起動してください。再起動するまでは、カウンターの値が正常に表示されません。

3.7.14 show auto-shutdown

リンクダウン時の自動 shutdown 機能の構成情報を表示します。

コマンドシンタックス

show auto-shutdown

コマンドモード

VIEW, ENABLE

使用例

(1) リンクダウン時の自動 shutdown 機能の構成情報を表示します。

```
# show auto-shutdown
 Timer :  1000 msec

--- port information ---
     *=Enable
     1    6 7   12
     +----+ +----+
     *****. ......
```

関連コマンド

注意事項

3.7.15 show interface status

各ポートの構成情報、及び状態を表示します。

コマンドシンタックス

show interface status [<PORTRANGE>] [detail]

PORTRANGE	構成情報、及び状態を表示するポート番号(複数指定可能)
detail	詳細情報を表示

コマンドモード

VIEW, ENABLE

使用例

(1) ポートの簡易情報を表示します。

```
# show interface status
Pt. [Description]
    Link    Flow   Auto Advertise         Fix     Pause MDIX        Media
```

```
    Status  Status Neg  Spd/Dpx           Spd/Dpx
-----------------------------------------------------------------------------
  1 [ ]
    Down    OFF    OFF  1G/F,100M,10M     100M/F  OFF   OFF(MDI-X)  UTP
  2 [ ]
    Down    OFF    ON   1G/F,100M,10M     100M/H  OFF   ON(---)     UTP
  3 [ ]
    Down    OFF    ON   1G/F,100M,10M     100M/H  OFF   ON(---)     UTP
                              (中略)
47 [ ]
    Down                                                            SFP-NONE
      +---  OFF    ON   1G/F,100M,10M     100M/H  OFF   ON(---)     (UTP)
   *  +---  OFF    ON   1G/F               1G/F   OFF   OFF         (FIBER)
 48 [ ]
    Down                                                            SFP-NONE
   *  +---  OFF    ON   1G/F,100M,10M     100M/H  OFF   ON(---)     (UTP)
      +---  OFF    ON   1G/F               1G/F   OFF   OFF         (FIBER)
 49 [ ]
    Down    OFF    OFF  10G/F              10G/F  OFF   OFF         XENPAK-NONE
 50 [ ]
    Down    OFF    OFF  10G/F              10G/F  OFF   OFF         XENPAK-NONE
```

(2) ポートの詳細情報を表示します。

```
# show interface status detail
Port                    : 1
Description             :
Link status             : Down
Flow status             : OFF
Auto negotiation        : ON
Advertise speed/duplex  : 1G/F,100M,10M
Fix speed/duplex        : 100M/H
Pause                   : OFF
MDIX                    : ON(---)
Media                   : UTP
Media part number       : -
Media serial number     : -
Tx/Rx power [dBm]
 Port                   : - / -

Port                    : 2
Description             :
Link status             : Down
Flow status             : OFF
Auto negotiation        : ON
Advertise speed/duplex  : 1G/F,100M,10M
Fix speed/duplex        : 100M/H
```

```
Pause                   : OFF
MDIX                    : ON(---)
Media                   : UTP
Media part number       : -
Media serial number     : -
Tx/Rx power [dBm]
 Port                   : - / -
                       (中略)
Port                    : 49
Description             :
Link status             : Down
Flow status             : OFF
Auto negotiation        : OFF
Advertise speed/duplex  : 10G/F
Fix speed/duplex        : 10G/F
Pause                   : OFF
MDIX                    : OFF
Media                   : XENPAK-LR
Media part number       : TXN174312013FYA
Media serial number     : CRTN84301G
Tx/Rx power [dBm]
 Port                   : -40.00 / -33.98

Port                    : 50
Description             :
Link status             : Down
Flow status             : OFF
Auto negotiation        : OFF
Advertise speed/duplex  : 10G/F
Fix speed/duplex        : 10G/F
Pause                   : OFF
MDIX                    : OFF
Media                   : XENPAK-LR
Media part number       : TXN174312013F27
Media serial number     : MYBG67784B
Tx/Rx power [dBm]
 Port                   : -40.00 / -40.00
```

Pt. [Description]　　：ポート番号、及びポート名
GBIC ポート/UTP ポートを選択可能なポートでは、選択されているポートに"*"を表示

(※ detail 指定時：Port　　：ポート番号
Description　：ポート名)

Link Status　　：ポートのリンク状態(ポートの状態)
10G/F　　：10 Gbps 全二重でリンクアップ
1G/F　　：1 Gbps 全二重でリンクアップ

100M/F	：100 Mbps 全二重でリンクアップ
100M/H	：100 Mbps 半二重でリンクアップ
10M/F	：10 Mbps 全二重でリンクアップ
10M/H	：10 Mbps 半二重でリンクアップ
Down	：リンクダウン状態
Disable	：ポート非活性(shutdown)状態
errDis	：LLDP による疑似リンクダウン状態
Flow Status	：ポートのフロー制御状態
ON	：フロー制御 ON(pause フレーム受信のみ)
OFF	：フロー制御 OFF
Auto Neg	：自動認識の設定状態
ON	：自動認識モード ON
OFF	：自動認識モード OFF
Advertise Spd/Dpx	：自動認識における Advertise 設定状態 (※ detail 指定時：Advertise speed/duplex)
10G/F	：10 Gbps 全二重
1G/F	：1 Gbps 全二重
100M	：100 Mbps 全二重、100 Mbps 半二重
100M/F	：100 Mbps 全二重
100M/H	：100 Mbps 半二重
10M	：10 Mbps 全二重、10 Mbps 半二重
10M/F	：10 Mbps 全二重
10M/H	：10 Mbps 半二重
none	：Advertise 設定をすべて削除
Fix Spd/Dpx	：自動認識 OFF 時の Speed/Duplex 設定状態 (※ detail 指定時：Fix speed/duplex)
100M/F	：100 Mbps 全二重
100M/H	：100 Mbps 半二重
10M/F	：10 Mbps 全二重
10M/H	：10 Mbps 半二重
Pause	：802.3x フロー制御モード設定状態
ON	：フロー制御モード ON
OFF	：フロー制御モード OFF
MDIX	：自動 MDI 切り替え設定状態
ON(---)	：自動認識モード ON、自動 MDI 切り替え ON、かつリンクダウン
ON(MDI-X)	：自動認識モード ON、自動 MDI 切り替え ON、かつ MDI-X 状態で リンクアップ
ON(MDI)	：自動認識モード ON、自動 MDI 切り替え ON、かつ MDI 状態で リンクアップ
OFF	：自動認識モード OFF、または自動 MDI 切り替え OFF、UTP 接続以外
OFF(MDI-X)	：自動認識モード OFF、または自動 MDI 切り替え OFF、MDI-X モード 固定
OFF(MDI)	：自動認識モード OFF、または自動 MDI 切り替え OFF、MDI モード 固定
Media	：Media の種類

UTP　　：1000BASE-T、100BASE-TX、10BASE-T
SFP-SX　　：1000BASE-SX
SFP-LXM　　：マルチモード光ファイバー用 SFP(2 km 仕様)
SFP-LX　　：1000BASE-LX
SFP-LX40　　：1000BASE-LX(40 km 仕様)
SFP-LX80　　：1000BASE-LX(80 km 仕様)
SFP-ZX　　：1000BASE-ZX
SFP-T　　：1000BASE-T
SFP-FX　　：100BASE-FX
SFP-BX10D　　：一芯 SFP(送信波長：1.490 μm 10 km 仕様)
SFP-BX10U　　：一芯 SFP(送信波長：1.310 μm 10 km 仕様)
SFP-BX20D　　：一芯 SFP(送信波長：1.490 μm 20 km 仕様)
SFP-BX20U　　：一芯 SFP(送信波長：1.310 μm 20 km 仕様)
SFP-BX40D　　：一芯 SFP(送信波長：1.490 μm 40 km 仕様)
SFP-BX40U　　：一芯 SFP(送信波長：1.310 μm 40 km 仕様)
SFP-BX80D　　：一芯 SFP(送信波長：1.490 μm 80 km 仕様)
SFP-BX80U　　：一芯 SFP(送信波長：1.310 μm 80 km 仕様)
C-1470　　：CWDM SFP(波長：1.470 μm)
C-1490　　：CWDM SFP(波長：1.490 μm)
C-1510　　：CWDM SFP(波長：1.510 μm)
C-1530　　：CWDM SFP(波長：1.530 μm)
C-1550　　：CWDM SFP(波長：1.550 μm)
C-1570　　：CWDM SFP(波長：1.570 μm)
C-1590　　：CWDM SFP(波長：1.590 μm)
C-1610　　：CWDM SFP(波長：1.610 μm)
SFP-NONE　　：認識不能な SFP、または SFP モジュール未挿入
XENPAK-CX4　　：10GBASE-CX4
XENPAK-LR　　：10GBASE-LR
XENPAK-SR　　：10GBASE-SR
XENPAK-ER　　：10GBASE-ER
XENPAK-ZR　　：10GBASE-ZR
XENPAK-LX4　　：10GBASE-LX4
XENPAK-NONE　　：認識不能な XENPAK、または XENPAK モジュール未挿入

※ detail 指定時、以下が追加で表示される
Media part number　　：Media の型式情報
　　Media 未挿入、または UTP ポートの場合、"-"表示
Media serial number　　：Media のシリアル番号
　　Media 未挿入、または UTP ポートの場合、"-"表示
Tx/Rx power [dBm]　　：光送信パワー/光受信パワー(単位：dBm)
　Port　　：ポートの単位値
　　Media 未挿入、Tx/Rx power が未対応、または UTP ポートの場合、"-"表示
　　モジュールが光出力していない場合、光送信パワーは"-"表示

関連コマンド

注意事項

100BASE-FX SFP を使用した場合、Advertise Spd/Dpx、及び Fix Spd/Dpx の表示は 1G/F となります。

3.7.16 show interface counters

各ポートの送受信フレームの統計情報を表示します。matrix オプションを指定することにより、表示するカウンター種別を指定することができます。

コマンドシンタックス

show interface counters [<PORTRANGE>] [matrix [<MATRIXRANGE>]]

PORTRANGE　統計情報を表示するポートの番号(複数指定可能)

MATRIXRANGE　統計情報を表示するカウンター種別 <1-4>(複数指定可能)

1：RxOctet, TxOctet, RxUnicast, TxUnicast, RxNUnicast, TxNUnicast, RxBC

2：RxDiscard, TxDiscard, BfOverflow, RxBitRate, TxBitRate, RxPktRate, TxPktRate

3：Collision, AlignError, FCS Error, Undersize, Oversize, Fragments, Jabbers

4：64Octet, 65-127, 128-255, 256-511, 512-1023, 1024-1518

コマンドモード

VIEW, ENABLE

使用例

(1) ポート：6 の送受信フレームの統計情報を表示します。

```
# show interface counters 6
port 6
RxOctet    :        0  TxOctet    :        0  Single Coll:        0
RxUnicast  :        0  TxUnicast  :        0  Multi Coll :        0
RxNUnicast :        0  TxNUnicast :        0  Late Coll  :        0
RxBroadcast:        0  TxDiscard  :        0  Excess Coll:        0
RxDiscard  :        0  Collision  :        0  BfOverflow :        0
64Octet    :        0  AlignError :        0  CarSenseErr:        0
65-127     :        0  FCS Error  :        0  RxBitRate  :        0
128-255    :        0  Undersize  :        0  RxPktRate  :        0
256-511    :        0  Oversize   :        0  TxBitRate  :        0
512-1023   :        0  Fragments  :        0  TxPktRate  :        0
1024-1518  :        0  Jabbers    :        0
```

RxOctet　：受信オクテット数

RxUnicast　：受信ユニキャストパケット数

RxNUnicast　：受信非ユニキャスト(マルチキャスト、及びブロードキャスト)パケット数

RxBroadcast　：受信ブロードキャストパケット数
RxDiscard　：受信廃棄パケット数(受信フレームを転送しない(パケットフィルター2 での deny などを含む)場合にカウント。Mirror などで転送した場合はカウントしない)
64Octet　：64 オクテット長の送受信パケット数
65-127　：65 以上 127 オクテット長以下の送受信パケット数
128-255　：128 以上 255 オクテット長以下の送受信パケット数
256-511　：256 以上 511 オクテット長以下の送受信パケット数
512-1023　：512 以上 1023 オクテット長以下の送受信パケット数
1024-1518　：1024 以上 1518 オクテット長以下の送受信パケット数
TxOctet　：送信オクテット数
TxUnicast　：送信ユニキャストパケット数
TxNUnicast　：送信非ユニキャスト(マルチキャスト、及びブロードキャスト)パケット数
TxDiscard　：送信廃棄パケット数
"counter-mode txdiscard only-buffer-overflow"項参照
Collision　：コリジョン発生回数
AlignError　：アライメントエラーパケット(フレーム長がオクテットの整数倍ではなく、かつ FCS エラー)受信回数
FCS Error　：FCS エラーパケット受信回数
Undersize　：アンダーサイズ(63 オクテット以下)パケット受信回数
Oversize　：1519～MTU オクテットパケット受信回数
VLAN タグ付きフレーム受信時は 4 バイト加算された範囲(1523～MTU+4)でカウント
Fragments　：フラグメントエラーパケット(63 オクテット以下、かつ FCS エラー)受信回数
Jabbers　：ジャバーパケット(1519～MTU オクテット、かつ FCS エラー)受信回数
VLAN タグ付きフレーム受信時は 4 バイト加算された範囲(1523～MTU+4)でカウント
Single Coll　：シングルコリジョン発生回数(半二重通信において送信中に 1 度だけ衝突(送信と受信が同時に行われた))
Multi Coll　：マルチコリジョン発生回数(送信中に 2～15 回の衝突)
Late Coll　：レイトコリジョン発生回数(フレームの 512 番目のビット送信後の衝突)
Excess Coll　：エクセシブコリジョン発生回数(16 回連続で衝突し送信停止)
BfOverflow　：送信バッファオーバーフローパケット数
CarSenseErr　：キャリアセンスエラー発生回数
RxBitRate　：過去 5 分間の平均受信ビットレート(bps) ※1
- フレーム間ギャップ、及びプリアンブル部を除くデータ部分のみが対象

RxPktRate　：過去 5 分間の平均受信パケット数(pps) ※1
TxBitRate　：過去 5 分間の平均送信ビットレート(bps) ※1
- フレーム間ギャップ、及びプリアンブル部を除くデータ部分のみが対象

TxPktRate　：過去 5 分間の平均送信パケット数(pps) ※1

※1 "clear interface counters"コマンド実行後の 5 分間は、"clear interface counters"コマンド実行時刻から"show interface counters"コマンド実行時刻までの平均レートとなります。

関連コマンド

注意事項

- キャリアセンスエラーは、ケーブルの抜き差しでカウントすることがあります。

- Apresia3400シリーズでは、10/100Mと1Gポート(Apresia3424シリーズはport 25-28、Apresia3448シリーズはport 49-52)でAlignErrorフレームを受信した場合のカウンターの動作が異なります。
  10/100MポートではAlignError、FCS Errorが増加し、1GポートではFCS Errorのみが増加します。

- 1519～MTU オクテットのフレームを受信した場合、Oversize、RxOctet、RxUnicastがカウントアップし、RxNUnicast、及びRxBroadcastはカウントアップしません。ただし、Apresia3400/5400シリーズではRxUnicastもカウントアップしません。

- 63オクテット以下のフレームを受信した場合、Undersize、RxOctetがカウントアップし、RxUnicast、RxNUnicast、及びRxBroadcastはカウントアップしません。

- 1519～MTUオクテットのフレームを送信した場合、TxUnicastのみがカウントアップし、TxNUnicastはカウントアップしません。

- Apresia3400シリーズの10MリンクではRxDiscardがカウントアップしない場合があります。

- Apresia4348 シリーズと Apresia13000 シリーズではミラーリングポートで 1G から 100M へ転送した場合に、BfOverflowがカウントされません。

- RxDiscardは以下の要因でカウントアップします。
  (1) パケットフィルター2のdeny等による受信フレーム破棄 ※1
  (2) 転送先ポートの帯域オーバーによるフレーム破棄 ※2、※3、※4
  (3) MMRP-Plus Master/SlaveポートでのMMRP-Plusハローフレーム受信
  (4) トランクポートでのVLAN ID不一致フレーム受信
  (5) 中継先がないフレーム ※5、※6
  ※1 3.47 AccessDefender機能での未認証パケットも含みます。
  ※2 ポートブロックが2個存在する以下の機種では、ポートブロックを跨ぐパケットはカウントアップしません。
  - Apresia3448シリーズ(port 1～24、49～50とport 25～48、51～52)
  - Apresia4348シリーズ(port 1～24とport 25～48)
  - Apresia13000-48X(port 1～24、50とport 25～49)

※3 ポートブロックが 2 個存在する以下の機種では、UC 以外の BC、MC、DLF パケットはカウントアップしません。

- **Apresia3448 シリーズ(port 1～24、49～50 と port 25～48、51～52)**
- **Apresia4348 シリーズ(port 1～24 と port 25～48)**
- **Apresia13000-48X(port 1～24、50 と port 25～49)**

※4 (2)の要因には 3.24 Egress シェーピング機能での破棄も含みます。

※5 フレームの受信ポートと宛先ポートが同一の場合も含みます(ポートブリッジ有効ポートは除く)。

※6 以下の機種では、VLAN 内で 1 ポートのみリンクアップし、中継先がない状態でのフレーム受信ではカウントアップしません。

- **Apresia3448 シリーズ**
- **Apresia4348 シリーズ**
- **Apresia13000-48X**

RxDiscard は以下の要因ではカウントアップしません。

(1) ポートミラーリングなどで転送したフレーム(mirroring、action mirror)

(2) CPU 宛フレーム ※1

(3) パケットフィルター2 の CPU 宛フィルター機能(action block-cpu-control)で CPU 転送を抑止した場合の以下フレーム

- **sFlow フレーム**
- **ICMP リダイレクトフレーム**

※1 パケットフィルター2 の action deny では CPU への転送を抑止できないため、カウントアップしません。

3.7.17 clear interface counters

各ポートの送受信フレームの統計情報を消去します。

コマンドシンタックス

clear interface counters <PORTRANGE>

PORTRANGE　　統計情報を消去するポートの番号(複数指定可能)

コマンドモード

ENABLE

使用例

(1) ポート：1、及び 2 の統計情報を消去します。

```
> enable
# clear interface counters 1,2
```

関連コマンド

注意事項

3.8 リンクアグリゲーション

IEEE 802.3ad 静的リンクアグリゲーションと LACP(Link Aggregation Control Protocol)による動的リンクアグリゲーションが可能です。スイッチングハブ間に複数のリンクを設定することができ、複数のポートで同時にフレームの中継を行うことにより帯域の拡張と縮退による冗長化ができます。リンクアグリゲーション可能なポート数は最大 8 ポート/グループです。最大グループ数は表 3-5 に示します。LACP の場合、8 ポート/グループ以上の設定が可能ですが、9 ポート以上はスタンバイポートとなります。また、ポートリダンダント機能と同一ポートでの併用が可能です。

表 3-5 リンクアグリゲーション最大グループ数

製品名	最大グループ数
Apresia5412GT-PoE	6 グループ
Apresia5412GT-HRSS	
Apresia5412GT-HRSS-DC48V	
Apresia5412GT-HRSS-DC110V	
Apresia5412GT-HRSS2	
Apresia3424GT-SS	14 グループ
Apresia3424GT-SS2	
Apresia3424GT-PoE	
Apresia3424GT-HiPoE	
Apresia4328GT	
Apresia5428GT	
Apresia13000-24GX-PSR	
Apresia13000-48X	24 グループ
Apresia3448GT	26 グループ
Apresia3448G-PSR	
Apresia3448G-PSR2	
Apresia4348GT	
Apresia4348GT-PSR	

注意事項

LAG(リンクアグリゲーショングループ)のメンバーポートは、以下の条件を満たしている必要があります。

(1) VLAN、インターフェースなどのポートに関するすべての設定が同じであること。

(2) グループ全部のポートにおいて自動認識機能(3.7.4 "auto-negotiation")の設定が等しいこと(有効、または無効に統一)。

(3) 自動認識機能("auto-negotiation")が有効の場合、advertise する通信モードは、10M/Full、100M/Full、1G/Full のいずれか 1 つのみに統一されていること。

(4) 自動認識機能("auto-negotiation")が無効の場合、link-speed-duplex 設定が 10M/Full、100M/Full のいずれかで統一されていること。

※ UTP ポート(10/100/1000 Mbps)で 1G/Full に固定する場合は、(3)の方法で設定し

ます。
advertise する通信速度/通信モードから 10M、100M の設定を削除してください。
例：no utp auto-negotiation disable
utp advertise delete 10m-speed
utp advertise delete 100m-speed

一つのポートを複数の LAG でメンバーポートとして定義することはできません。

Apresia4348 シリーズでは、12 ポートごとの境界(1～12、13～24、25～36、37～48)を超えて LAG を定義することはできません。

Apresia3448 シリーズでは、24 ポートごとの境界(1～24、25～48、49～50、51～52)を超えて LAG を定義することはできません。

LAG のメンバーポートに、3.20 フラッディング制限を設定することはできません。

マルチキャストルーティング("ip multicast-routing")有効時、動的リンクアグリゲーション(LACP 機能)は有効にすることはできません。

LACP を使用する場合、ログが LACP Key 番号で出力されます。運用上の混乱を避けるため、LAG ID と LACP Key は同じ数字を使用することを推奨します。

3.8.1 link-aggregation

LAG(リンクアグリゲーショングループ)を設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

設定可能なポート数は 1 グループにつき最大 8 ポート、設定可能グループ数は最大 24 グループです。

コマンドシンタックス

link-aggregation <GROUP>
no link-aggregation [<GROUP>]
GROUP　　LAG ID

デフォルト

なし(＝設定なし)

コマンドモード

IF-PORT

使用例

(1) ポート：1～8 までを LAG ID：1 に設定します。
(2) LAG ID：1 を削除します。
(3) すべての LAG を削除します。

```
> enable
# configure terminal
(config)# interface port 1-8
(config-if-port)# link-aggregation 1
(config-if-port)# no link-aggregation 1
(config-if-port)# exit
(config)# interface port 1-48
(config-if-port)# no link-aggregation
```

関連コマンド

show link-aggregation, show running-config

注意事項

Apresia13000-48X において、ポートブロック(port 1-24、50 と port 25-49)を跨いだリンクアグリゲーションを行う場合、端末の送信ポートと受信ポートがポートブロックを跨がないような接続をしてください。

3.8.2 link-aggregation algorithm

静的リンクアグリゲーションにおいて、出力ポートの選択アルゴリズムを変更することができます。

アルゴリズムに、dst-ip-base、mac-base、ip-base のいずれかを設定し、さらにそのオプションとして non-uc-dst-only の設定を追加することによって、以下の表 3-6 のように中継するフレームの宛先、送信元 MAC アドレス、または宛先、送信元 IP アドレスなどに基づき、中継ポートの選択(振り分け)をすることができます。表 3-6 には各設定をした際の中継ポート(振り分け)の選択に使用される要素を示します。

なお、表 3-6 の ip-base の設定に対する動作は IP パケットの場合で、非 IP パケットについては mac-base に準じる動作をします。

表 3-6 中継ポート選択(振り分け)ルール対応表

中継対象フレームの種類 / コマンド	ユニキャスト		マルチキャスト		ブロードキャスト
	MAC アドレス既学習	MAC アドレス未学習	マルチキャストグループに IP アドレス既登録(注 1、注 2)	マルチキャストグループに IP アドレス未登録	
dst-ip-base	※4	※1	※2、※7	※1	※5
dst-ip-base non-uc-dst-only	※4	※3	※4、※8	※3	※6
mac-base	※9	※1	※2、※7	※1	※5
mac-base non-uc-dst-only	※9	※3	※4、※8	※3	※6
ip-base	※2	※1	※2、※7	※1	※5
ip-base	※2	※3	※4、※8	※3	※6

中継対象フレームの種類 / コマンド	ユニキャスト		マルチキャスト		ブロードキャスト
	MAC アドレス既学習	MAC アドレス未学習	マルチキャストグループに IP アドレス既登録(注 1、注 2)	マルチキャストグループに IP アドレス未登録	
non-uc-dst-only					

※1：送信元、宛先 MAC アドレス
※2：送信元、宛先 IP アドレス
※3：宛先 MAC アドレス
※4：宛先 IP アドレス
※5：送信元 MAC アドレス
※6：振り分けない
※7：送信元、宛先 MAC アドレス(Apresia4328GT のみ)
※8：宛先 MAC アドレス(Apresia4328GT のみ)
※9：送信元、宛先 MAC アドレス、VLAN ID、ether_type

注 1：宛先 IP アドレスがマルチキャストグループに登録済のものと一致(Apresia4348 シリーズ、Apresia13000-48X)
注 2：宛先 MAC アドレス、宛先 IP アドレスがマルチキャストグループに登録済のものと一致(Apresia3400/5400 シリーズ、Apresia13000-24GX)

コマンドシンタックス

link-aggregation algorithm dst-ip-base | mac-base | ip-base [non-uc-dst-only]

dst-ip-base	宛先 IP アドレスベース
mac-base	送信元/宛先 MAC アドレスベース(デフォルト)
ip-base	送信元/宛先 IP アドレスベース
non-uc-dst-only	宛先 MAC、または IP アドレスに基づき振り分ける

デフォルト

mac-base

コマンドモード

CONFIG

使用例

(1) リンクアグリゲーションを IP アドレスで振り分ける設定にします。

```
(config)# link-aggregation algorithm ip-base
```

関連コマンド

show link-aggregation, show running-config

注意事項

動的リンクアグリゲーション(LACP 機能)では、分散アルゴリズムの設定に関係なく、

常に mac-base で中継ポート選択(振り分け)を行います。
ただし、non-uc-dst-only を設定した場合、"mac-base | ip-base"どちらを設定しても mac-base non-uc-dst-only として動作します。

マルチキャストフィルタリングで指定した IP アドレス宛のマルチキャストフレームは学習済みマルチキャストフレームとして扱われます。

3.8.3 link-aggregation lacp

LACP(Link Aggregation Control Protocol)による動的リンクアグリゲーションを設定します。キー番号を、対向装置と同じにする必要はありません。

コマンドシンタックス

link-aggregation <GROUP> lacp mode active | passive key <KEY>
no link-aggregation [<GROUP>]

GROUP	LAG(リンクアグリゲーショングループ) ID
KEY	キー番号 <1-12>
active	アクティブモード • 定期的に LACPDU を送信し対向装置とネゴシエーションを行う
passive	パッシブモード • LACPDU を受信した場合、ネゴシエーションを開始 • 対向装置がパッシブモードの場合、LACP は動作しない

デフォルト

なし(＝設定なし)

コマンドモード

IF-PORT

使用例

(1) ポート：1～8 までを LACP の LAG ID：1 に設定します。
(2) LAG ID：1 を削除します。
(3) すべての LAG を削除します。

```
> enable
# configure terminal
(config)# interface port 1-8
(config-if-port)# link-aggregation 1 lacp mode active key 1
(config-if-port)# no link-aggregation 1
(config-if-port)# exit
(config)# interface port 1-26
(config-if-port)# no link-aggregation
```

関連コマンド

show link-aggregation, show lacp, show running-config

注意事項

同じ LAG に属するポートのキー番号は同一に設定する必要があります。

LACP と 3.42 MMRP-Plus を装置で同時に使用できません。

3.8.4 lacp system-priority

LACP の装置優先度を設定します。値が小さいほど優先度が高くなります。

コマンドシンタックス

lacp system-priority <PRIORITY>
no lacp system-priority
PRIORITY　　プライオリティ <1-65535>

デフォルト

32768

コマンドモード

CONFIG

使用例

(1) プライオリティを 100 に設定します。

```
> enable
# configure terminal
(config)# lacp system-priority 100
```

関連コマンド

show lacp sys-id, show running-config

注意事項

3.8.5 lacp port-priority

LACP のポート優先度を設定します。値が小さいほど優先度が高くなります。

コマンドシンタックス

lacp port-priority <PRIORITY>
no lacp port-priority
PRIORITY　　プライオリティ <1-65535>

デフォルト

32768

コマンドモード
IF-PORT

使用例
(1) ポート：1～8 のプライオリティを 100 に設定します。

```
> enable
# configure terminal
(config)# interface port 1-8
(config-if-port)# lacp port-priority 100
```

関連コマンド
show lacp, show running-config

注意事項

3.8.6 lacp timeout short

LACPDU の受信タイムアウト時間を Short(3 秒)に設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

対向装置から本装置へ送信される LACPDU の間隔は、本装置の受信タイムアウト時間の設定が Short の場合は 1 秒、Long の場合は 30 秒になります。

コマンドシンタックス
[no] lacp timeout short

デフォルト
なし(＝Long(90 秒))

コマンドモード
IF-PORT

使用例
(1) ポート：1～8 の送信間隔を 1 秒に設定します。

```
> enable
# configure terminal
(config)# interface port 1-8
(config-if-port)# lacp timeout short
```

関連コマンド
show lacp, show running-config

注意事項

本設定を Short に設定した場合、障害検知までの時間は短縮されますが、代わりに LACPDU を大量に受信するため CPU 負荷が増加します。本設定を Short に設定したこ

とで LACP の受信タイムアウトによるポートダウンが頻発する場合は、本設定を Long に変更するか、または静的リンクアグリゲーションを使用してください。

LACPDU の送信間隔は、対向装置の受信タイムアウト時間に依存するため、対向装置と本装置において本設定を統一してください。

3.8.7 show link-aggregation

リンクアグリゲーションの構成情報を表示します。

コマンドシンタックス

show link-aggregation

コマンドモード

VIEW, ENABLE

使用例

(1) リンクアグリゲーションの構成情報を表示します。

```
# show link-aggregation
algorithm: mac-base
Static LAG        O: Link Up  o: Link Down
LACP active mode  A: Collecting/Distributing a: not Collecting/Distributing
LACP passive mode P: Collecting/Distributing p: not Collecting/Distributing
      Port
      1      8 9     16 17    24 25    32 33    40 41    48 49
GrpNo +------+ +------+ +------+ +------+ +------+ +------+ +-
  1   Aa...... ........ ........ ........ ........ ........ ..
  2   ........ ....Pppp ........ ........ ........ ........ ..
  3   ........ ........ Oooo.... ........ ........ ........ ..
```

Static LAG	：静的 LAG の状態
O	：リンクアップ中
o	：リンクダウン中
LACP active mode	：動的 LAG の状態(LACP アクティブモード)
A	：LACP 冗長化接続中
a	：LACP 冗長化接続中以外
LACP passive mode	：動的 LAG の状態(LACP パッシブモード)
P	：LACP 冗長化接続中
p	：LACP 冗長化接続中以外
GrpNo	：LAG ID
Port	：ポート番号

関連コマンド

注意事項

3.8.8 show lacp

LACP の状態を表示します。

コマンドシンタックス

show lacp <KEY> | summary | detail

KEY	キー番号 <1-12>
summary	簡易情報を表示
detail	詳細情報を表示

コマンドモード

VIEW, ENABLE

使用例

(1) キー番号：1 の LACP 簡易情報を表示します。

```
# show lacp 1
% Aggregator 1 Admin Key: 0001 - Oper Key 0001 Partner LAG:
0x8000,00-40-66-45-b5-c7 Partner Oper Key 0001
%   Link: port1 (1) sync: 1
%   Link: port2 (2) sync: 1
%   Link: port3 (3) sync: 1
%   Link: port4 (4) sync: 1
%   Link: port5 (5) sync: 1
%   Link: port6 (6) sync: 1
%   Link: port7 (7) sync: 1
%   Link: port8 (8) sync: 1
#
```

(2) LACP 簡易情報を表示します。

```
# show lacp summary
% Aggregator 1
%  Admin Key: 0001 - Oper Key 0001
%   Link: port1 (1) sync: 1
%   Link: port2 (2) sync: 1
%   Link: port3 (3) sync: 1
%   Link: port4 (4) sync: 1
%   Link: port5 (5) sync: 1
%   Link: port6 (6) sync: 1
%   Link: port7 (7) sync: 1
%   Link: port8 (8) sync: 1
#
```

Aggregator	：登録 LACP 数の ifIndex 値
Admin Key, Oper Key	："link-aggregation lacp"コマンドで設定したキー値
Partner LAG	：対向の装置優先度とシステム ID
Partner Oper Key	：対向の LAG ID のキー値

Link　　：本 LAG ID で定義されるポート番号と LACP 状態
　　• 括弧内は ifIndex 値
　sync：1　　：LACP 冗長化接続中状態(Collecting/Distributing)
　sync：0　　：LACP 接続可能状態(Attached)

(3) LACP 詳細情報を表示します。

```
# show lacp detail
% Aggregator 1
%  Mac address: 00:40:66:11:67:da
%  Admin Key: 0001 - Oper Key 0001
%  Receive link count: 2 - Transmit link count: 2
%  Individual: 0 - Ready: 1
%  Actor LAG  - 0x8000,00-40-66-11-67-da
%  Partner LAG- 0x8000,00-40-66-33-1d-bc
%   Link: port41 (41) Collecting/Distributing
%   Link: port42 (42) Collecting/Distributing
```

Aggregator　　：登録 LACP 数の ifIndex 値
Mac address　　：本装置の MAC アドレス
Admin Key, Oper Key　　："link-aggregation lacp"コマンドで設定したキー値
Receive link count　　：本 LAG ID で、動的リンク接続中のポート数
Transmit link count　　：本 LAG ID で、動的リンク接続中のポート数
Individual　　：本装置では常に 0
Ready　　：動的リンク可能状態(1)、動的リンク可能ポートなし(0)
Actor LAG　　：本装置の装置優先度とシステム ID
Partner LAG　　：対向の装置優先度とシステム ID
　　※ 本装置と対向装置で、装置優先度とシステム ID が同一の場合、各設定が対向装置と重複していることを示すメッセージ(system-id is overlapping)が出力されます。
Link　　：本 LAG ID で定義されるポート番号と LACP 状態
　　• 括弧内は ifIndex 値
　Collecting/Distributing　　：LACP 冗長化接続中状態
　　LACP リンク(ポートが対向と同期)し、正常に、帯域の拡張と縮退による冗長化接続を行っている状態
　Attached　　：LACP 接続可能状態
　　LACP リンク可能な状態であるが、対向ポートと動的リンク接続を行っていない状態
　　• 対向ポートがリンクダウンしている場合
　　• 対向ポートが LACP リンク動作不可の場合
　　• 対向ポートが動的 LAG ではない場合など
　Waiting　　：LACP ポート選択状態
　　LACP リンク可能な状態ではない、LACP リンク動作待ちの状態
　　• 9 ポート以上の構成によるスタンバイポートなど、LACP リンクポートとして選択されていない場合
　　• 同一 LAG ID における他のポートで、すでに別のグル

ープ番号と LACP リンク接続している場合など

Detached　：LACP 離脱状態
ポート未接続による、LACP 未動作の状態
※ 正常動作時は、LACP リンクするまでに、以下の順で遷移します。
Detached -> Waiting -> Attached -> Collecting/Distributing

関連コマンド

注意事項

3.8.9 show lacp-counter

LACP 統計情報を表示します。キー番号を指定しない場合はすべての統計情報を表示します。

コマンドシンタックス

show lacp-counter [<KEY>]

KEY　キー番号 <1-12>

コマンドモード

VIEW, ENABLE

使用例

(1) LACP 統計情報を表示します。

```
# show lacp-counter 1
% Traffic statistics
Port      LACPDUs        Marker         Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
% Aggregator po1 1
port1   549     537     0       0       0       0
port2   521     514     0       0       0       0
port3   516     512     0       0       0       0
port4   513     512     0       0       0       0
port5   517     512     0       0       0       0
port6   515     514     0       0       0       0
port7   527     525     0       0       0       0
port8   530     524     0       0       0       0
```

LACPDUs(Sent/Recv)　：LACP フレーム数
Marker(Sent/Recv)　：LACP マーカーフレーム数
Pckt err(Sent/Recv)　：不正、または不明なフレーム数

関連コマンド

注意事項

3.8.10 show lacp sys-id

LACP のシステム ID と優先度を表示します。

コマンドシンタックス

show lacp sys-id

コマンドモード

VIEW, ENABLE

使用例

(1) LACP のシステム ID と装置優先度を表示します。

```
# show lacp sys-id
% System 8000,00-40-66-11-cd-6f
```

System　　：装置優先度とシステム ID

関連コマンド

注意事項

3.8.11 show lacp port

ポートごとに LACP の動作状態を表示します。

コマンドシンタックス

show lacp port <PORT>

PORT　　ポート番号

コマンドモード

VIEW, ENABLE

使用例

(1) ポート：8 に関する LACP の動作状態を表示します。

```
# show lacp port 8
% LACP link info: port8 - 8
% LAG ID: 0x8000,00-40-66-13-09-77
% Partner oper LAG ID: 0x8000,00-40-66-34-48-35
% Actor priority: 0x8000 (32768)
% Admin key: 0x0001 (1) Oper key: 0x0001 (1)
% Physical admin key:(0)
% Receive machine state : Current
% Periodic Transmission machine state : Fast periodic
% Mux machine state : Collecting/Distributing
% Oper state:          ACT:1 TIM:1 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
```

```
% Partner oper state:  ACT:1 TIM:1 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner link info: admin port 0
% Partner oper port: 32
% Partner admin LAG ID: 0x0000-00:00:00:00:00:00
% Admin state:         ACT:1 TIM:1 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner admin state: ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner system priority - admin:0x8000 - oper:0x03e8
% Aggregator ID: 1
```

LACP link info	：本ポート番号と ifIndex 値
LAG ID	：本ポート優先度とシステム ID
Partner oper LAG ID	：対向のポート優先度とシステム ID
Actor priority	：本ポート優先度
Admin Key, Oper Key	："link-aggregation lacp"コマンドで設定したキー値
Physical admin key	：管理キー値(固定値)
Receive machine state	：LACPDU 受信状態
Invalid	：LACP 未動作
Port disabled	：対向ポートリンクダウンなどによる LACPDU 受信不可
LACP disabled	：LACP 動作停止
Expired	：LACPDU 受信タイムアウト
Defaulted	：LACPDU 未受信
Current	：LACPDU 正常受信中
Periodic Transmission machine state	：LACPDU 送信状態
Invalid	：LACP 未動作
No periodic	：LACPDU 未送信
Fast periodic	：送信間隔 Short(1 秒)による LACPDU 送信中
Slow periodic	：送信間隔 Long(30 秒)による LACPDU 送信中
Mux machine state	：LACP 状態("show lacp"項参照)
Collecting/Distributing	：LACP 冗長化接続中状態
Attached	：LACP 接続可能状態
Waiting	：LACP ポート選択状態
Detached	：LACP 離脱状態
Oper state	：本ポート状態
Partner oper state	：対向ポート状態
ACT	：アクティブモード(1)、パッシブモード(0)
TIM	：LACPDU 送信間隔 Short(1)、LACPDU 送信間隔 Long(0)
AGG	：LAG(1)、それ以外(0)
SYN(本ポート状態の場合)	：LACP リンク可能(1)、それ以外(0)
SYN(対向ポート状態の場合)	：本ポートの情報で LACP リンク中(1)、それ以外(0) ※ Oper state、Partner oper state ともに、SYN：1 の場合に、LACP リンク動作します。
COL	：LACP リンク接続中(1)、それ以外(0)

DIS　　：LACP リンク接続中(1)、それ以外(0)
DEF　　：LACPDU 未受信(1)、それ以外(0)
EXP　　：LACPDU 受信タイムアウト(1)、それ以外(0)
Partner link info　　：対向から LACPDU を受信していない場合に使用される対向のデフォルト値(固定、変更不可)
Partner oper port　　：対向ポート番号
Partner admin LAG ID　　：対向から LACPDU を受信していない場合に使用される対向のデフォルト値(固定、変更不可)
Admin state　　：本ポートの管理状態
Partner admin state　　：対向ポートの管理状態
Partner system priority　　：対向の装置優先度
Aggregator ID　　：本ポートが動作している、動的 LAG ID

関連コマンド

注意事項

3.8.12 show tech-support link-aggregation

リンクアグリゲーションの各種情報を収集し表示します。本コマンドで表示する内容は、表 3-7 に示すコマンドが収集している情報です。system-dump オプションを指定した場合、装置内部のダンプ情報(独自形式で表示)を含めて取得し表示します。

表 3-7 コマンドにより収集可能なリンクアグリゲーション情報

show system
show version
show link-aggregation
show lacp detail
show lacp port
show lacp-counter ※1
show interface counters ※1

※1 1 秒おきに 3 回情報を取得

コマンドシンタックス

show tech-support link-aggregation [system-dump]
　　system-dump　　装置内部のダンプ情報を出力

コマンドモード

ENABLE

関連コマンド

注意事項

system-dump オプションを指定した場合、装置の性能、及び通信に対して影響を及ぼ

す可能性があります。使用する場合には、必ず事前にサポート対応窓口へご相談のうえ、指示に従ってください。

3.8.13 clear lacp counters

LACP 統計情報を消去します。キー番号を指定しない場合は、すべての LACP 統計情報を消去します。

コマンドシンタックス

clear lacp [<KEY>] counters

KEY　　キー番号 <1-12>

コマンドモード

ENABLE

使用例

(1) LACP 統計情報を消去します。

```
> enable
# clear lacp 1 counters
```

関連コマンド

注意事項

3.9 ポートリダンダント

注意事項

Apresia13000-48X、及び Apresia4348 シリーズにおいて、本機能を使用し、かつリダンダント設定ポートで BPDU を受信する場合は、リダンダント設定ポートをトランクポート(3.11.4 "switchport mode")に設定してください。ただし、ネイティブ VLAN の設定(3.11.6 "switchport trunk native <VID>")は行わないでください。

3.9.1 redundant group-number

ポートリダンダントのグループ番号を設定します。設定を削除する場合は、no コマンドを使用してください。

グループ番号は 1～64 の範囲で設定可能です。ポートリダンダントは複数のポートをグループ化し、グループ内で優先順位の高いポートでフレームの中継を行う機能です。中継を行うポートはグループ内で１つのみです。優先順位はポートリダンダントプライオリティが小さいものほど高くなり、ポートリダンダントプライオリティが同じ場合には、帯域速度が大きいほど優先順位は高くなり(リンクアグリゲーション機能併用時はリンクアップしているポートの合計帯域)、帯域速度が同じ場合は、ポート番号の小さいものほど高くなります。また、リンクアグリゲーション機能と同一ポートでの併用が可能です。

コマンドシンタックス

redundant group-number <GROUP>
no redundant group-number [<GROUP>]
GROUP　　ポートリダンダントグループ <1-64>

デフォルト

なし(＝設定なし)

コマンドモード

IF-PORT

使用例

(1) ポート：1～8 までをポートリダンダントグループ：1 に設定します。
(2) ポートリダンダントグループ：1 を削除します。
(3) すべてのポートリダンダントグループを削除します。

```
> enable
# configure terminal
(config)# interface port 1-8
(config-if-port)# redundant group-number 1
(config-if-port)# no redundant group-number 1
(config-if-port)# exit
(config)# interface port 1-26
```

```
(config-if-port)# no redundant group-number
```

関連コマンド

show redundant, show running-config

注意事項

ポートリダンダントグループのメンバーポートは、すべて同じ VLAN に所属させる必要があります。

ポートリダンダントグループのメンバーポートに対して、以下の設定を行うことはできません。

(1) ポートミラーリングの To ポート
(2) static FDB 登録
(3) パケットフィルター2
(4) ユーザーループ検知(notify-only のみ可)
(5) マルチキャストフィルタリング
(6) ポートセキュリティー
(7) MMRP、MMRP-Plus、MMRP2 aware
(8) LLDP

3.9.2 redundant port-priority

ポートリダンダントプライオリティを設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。プライオリティは 0～255 の範囲で設定可能です。

コマンドシンタックス

redundant port-priority <PRIORITY>
no redundant port-priority
PRIORITY　　ポートリダンダントプライオリティ <0-255>

デフォルト

10/100M ポート　　：19
1G ポート　　：4
10G ポート　　：2

コマンドモード

IF-PORT

使用例

(1) ポート：1～8 のポートリダンダントプライオリティを 5 に設定します。
(2) ポート：1～8 のポートリダンダントプライオリティをデフォルト値に戻します。

```
> enable
```

```
# configure terminal
(config)# interface port 1-8
(config-if-port)# redundant port-priority 5
(config-if-port)# no redundant port-priority
```

関連コマンド

show redundant portbase, show running-config

注意事項

3.9.3 redundant mac-address-table update

アクティブポート切り替わり時の MAC アドレス再学習フレーム送信回数を設定します。送信回数が 2 回以上の場合、MAC アドレス再学習フレームはおよそ 1 秒間隔で送信されますが、エントリー数や CPU 負荷によっては 1 秒以上間隔が空くことがあります。設定を削除する場合は、no コマンドを使用してください。

本コマンドで指定したポートリダンダントグループはアクティブポートの切り替わり時に MAC アドレス再学習フレームを指定回数送信します。MAC アドレス再学習フレームにより、対向スイッチの MAC アドレステーブルを更新し、通信を速やかに復旧させます。送信 MAC アドレスエントリーの最大数は 1024 エントリーです。

以下の条件をすべて満たす MAC アドレスが送信対象です。

- 3.14.3 "show mac-address-table"に表示される MAC アドレス
- 該当ポートリダンダントグループのメンバーポートが属する VLAN で学習した MAC アドレス
- 該当ポートリダンダントグループのメンバーポート以外で学習した MAC アドレス

コマンドシンタックス

redundant group-number <GROUP> mac-address-table update transmit count <COUNT>
no redundant group-number <GROUP> mac-address-table update transmit

GROUP	ポートリダンダントグループ <1-64>
COUNT	送信回数 <1-3>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポートリダンダントグループ：1 において MAC アドレス再学習フレームを 3 回送信します。
(2) ポートリダンダントグループ：1 において MAC アドレス再学習フレーム送信を無効にします。

```
> enable
# configure terminal
(config)# redundant group-number 1 mac-address-table update transmit count 3
(config)# no redundant group-number 1 mac-address-table update transmit
```

関連コマンド

show redundant, show running-config

注意事項

3.9.4 show redundant

ポートリダンダントグループの情報をグループ番号ベースで表示します。

コマンドシンタックス

show redundant

コマンドモード

VIEW, ENABLE

使用例

(1) ポートリダンダントグループの情報を表示します。

```
# show redundant
 A: Active       a: Active (LAG)
 R: Ready        r: Ready (LAG)
 D: Link Down    d: Link Down (LAG)
      Port
      1      8 9     16 17    24 25    32 33    40 41    48 49
GrpNo +------+ +------+ +------+ +------+ +------+ +------+ +-  TxCount
  1   ARD..... ........ ........ ........ ........ ........ ..        3
  2   ........ aarr.... ........ ........ ........ ........ ..        -
```

GrpNo　：ポートリダンダントグループ番号
Port　：ポート番号
A　：Active 状態
R　：Ready 状態
D　：リンクダウン状態
a　：Active 状態(リンクアグリゲーション併用時)
r　：Ready 状態(リンクアグリゲーション併用時)
d　：リンクダウン状態(リンクアグリゲーション併用時)
.　：ポートリダンダント非設定ポート

関連コマンド

注意事項

3.9.5 show redundant portbase

ポートリダンダントグループの情報をポート番号ベースで表示します。

コマンドシンタックス

show redundant portbase

コマンドモード

VIEW, ENABLE

使用例

(1) ポートリダンダントグループの情報を表示します。

```
# show redundant portbase
Pt.  Status       GrpNo  Priority  LAG-ID
 15  Active         1       4        1
 19  Ready          1       4        2
 41  Ready          1       4        3
 45  Ready          1       4        4
 47  Active         1       4        1
```

関連コマンド

注意事項

3.10 ポートミラーリング

3.10.1 mirroring

ポートミラーリングの設定を行います。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

mirroring rx | tx <FROMPORT> <TOPORT>
no mirroring rx | tx

rx	<FROMPORT>で指定したポートから受信したフレームを <TOPORT>で指定したポートにミラーリング
tx	<FROMPORT>で指定したポートから送信したフレームを <TOPORT>で指定したポートにミラーリング
FROMPORT	フレームの転送元のポート(複数指定可能)を指定
TOPORT	フレームの転送先のポートを指定

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1 で受信したフレームをポート：8 にミラーリングします。
(2) ポート：1 で送信したフレームをポート：10 にミラーリングします。

```
> enable
# configure terminal
(config)# mirroring rx 1 8
(config)# mirroring tx 1 10
```

関連コマンド

show mirroring, show running-config

注意事項

To ポートの所属 VLAN でフラッディングフレームが発生しても To ポートには転送されません。

本装置の CPU から送信されるフレームや中継時に CPU 処理が行われるフレーム(※)は、From ポートから送信されてもミラーリングは行われません(To ポートに転送されません)。
※ 中継時に CPU 処理が行われるフレームには、BPDU、DHCP パケットなどがあります。

本機能は、From ポートとして設定したポートで送受信されたフレームを解析するための機能です。従って、To ポートとして設定したポートでは他機能を動作させず、

アナライザーなどのネットワーク解析装置以外は接続しないでください。

LAG(リンクアグリゲーショングループ)のメンバーポート、及びポートリダンダントグループのメンバーポートに対して、ポートミラーリングの To ポートの設定はできません。

送信フレームのミラーリングでは、From ポートから送信したフレームのタグ有無に関わらず、タグ付きフレームでミラーリングされます。

rx、tx の指定に関係なく、To ポートで指定するポートが From ポートで指定されている場合は、コマンドがエラーとなります。また、From ポートで指定するポートが To ポートで指定されている場合もエラーとなります。

STP/RSTP 機能を使用している場合、To ポートのスパニングツリー機能を停止(3.17.3 "spanning-tree disable")してください。

MSTP 機能を利用している場合、To ポートに instance を割り当てないでください。

ポートミラーリング rx 指定の From ポートと 3.28 パケットフィルター2 機能"action mirror"の assign port を同一ポートに設定している場合、"action mirror"が優先的に動作します。

エラーパケットはミラーリングされません。

ポートミラーリングの From ポートに設定時、該当するポートで受信、送信したフレームの、各ポート状態におけるミラーリング動作について以下の表 3-8 各ポート状態における From ポートに設定時のミラーリング動作に示します。

表 3-8 各ポート状態における From ポートに設定時のミラーリング動作

		mirroring 設定	
機能	ポート状態	mirroring rx	mirroring tx
ポートリダンダント	Ready ポート	○	×
スパニングツリープロトコル	ブロッキング状態	○	×
MMRP-Plus	Blocking ポート	○	○

○：ミラーリングする
×：ミラーリングしない

ミラーリングの To ポートでフレームを受信した場合、宛先 MAC アドレスが表 3-9 である制御フレームは、To ポートでフレームの送信元 MAC アドレスを学習します。
※ 以上の動作は、ミラーリングの To ポートに限らずすべてのポートで共通です。

表 3-9 送信元 MAC アドレスを学習する予約アドレス種別

機種	バージョン	宛先 MAC アドレス
Apresia3400/5400 シリーズ、 Apresia13000-24GX-PSR	AEOS7.29.01 より前	01:80:c2:00:00:00-01:80:c2:00:00:0f 01:80:c2:00:00:20-01:80:c2:00:00:2f
	AEOS7.29.01 以降	01:80:c2:00:00:03
Apresia4300 シリーズ、 Apresia13000-48X	-	01:80:c2:00:00:00-01:80:c2:00:00:0f 01:80:c2:00:00:20-01:80:c2:00:00:2f

3.10.2 show mirroring

ポートミラーリングの構成情報を表示します。

コマンドシンタックス

show mirroring

コマンドモード

VIEW, ENABLE

使用例

(1) ポートミラーリングの構成情報を表示します。

```
# show mirroring
          f = From   t = To
          Port
          1     6 7    12 13   18 19   24 25   30 31   36 37   42 43   48 49
          +----+ +----+ +----+ +----+ +----+ +----+ +----+ +----+ +-
Rx        f..... .t.... ...... ...... ...... ...... ...... ...... ..
Tx        f..... ...t.. ...... ...... ...... ...... ...... ...... ..
```

関連コマンド

注意事項

3.11 VLAN

VLAN は論理的にネットワークセグメントを分割する機能です。最大 4094 個の VLAN 設定が可能です。

3.11.1 vlan database

VLAN モードへ移行します。VLAN モードは VLAN の作成・削除、VLAN の動作状態の設定が行えます。

VLAN モードから CONFIG モードへ移行したい場合は exit コマンド、ENABLE モードへ移行したい場合は end コマンドを使用してください。

コマンドシンタックス

vlan database

デフォルト

なし

コマンドモード

CONFIG

使用例

(1) VLAN モードへ移行します。

(2) CONFIG モードへ移行します。

```
> enable
# configure terminal
(config)# vlan database
(config-vlan)# exit
(config)#
```

関連コマンド

vlan name, vlan state

注意事項

セカンダリーIP アドレスを設定している VLAN は削除できません。VLAN の削除はセカンダリーIP アドレスの消去後に行う必要があります。

3.11.2 vlan name

VLAN の作成、または削除します。工場出荷時は VLAN 名：default、VLAN ID：1 のデフォルト VLAN が作成されています。デフォルト VLAN は削除できません。

コマンドシンタックス

vlan <VID> name <NAME>

no vlan <VID>

VID　　作成、または削除する VLAN ID <2-4094>

NAME　　作成、または削除する VLAN の名称 <1-32(文字)>
- ASCII 文字
- ダブルクォーテーションで囲めば、空白文字を使用可能

デフォルト

デフォルト VLAN(VLAN 名：default、VLAN ID：1)

コマンドモード

VLAN

使用例

(1) VLAN ID：4094、VLAN 名：V4094 の VLAN を作成します。
(2) VLAN ID：4094 の VLAN を削除します。

```
> enable
# configure terminal
(config)# vlan database
(config-vlan)# vlan 4094 name V4094
(config-vlan)# no vlan 4094
```

関連コマンド

show vlan, show running-config

注意事項

3.11.3 vlan state

VLAN の動作状態を無効にします。有効にする場合は、no コマンドを使用してください。デフォルト VLAN(VLAN ID：1)の動作状態は変更できません。

コマンドシンタックス

[no] vlan <VID> state disable

VID　　状態を変更する VLAN ID <2-4094>

デフォルト

enable(＝有効)

コマンドモード

VLAN

使用例

(1) VLAN ID：4094 の VLAN を無効にします。
(2) VLAN ID：4094 の VLAN を有効にします。

```
> enable
# configure terminal
(config)# vlan database
```

```
(config-vlan)# vlan 4094 state disable
(config-vlan)# no vlan 4094 state disable
```

関連コマンド

show vlan, show running-config

注意事項

3.11.4 switchport mode

各ポートの VLAN モードを設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

switchport mode access | trunk
no switchport mode

access	アクセスポート(ポートベース VLAN モード)
trunk	トランクポート(802.1Q タグ付き VLAN モード)

デフォルト

access(＝アクセスポート)

コマンドモード

IF-PORT

使用例

(1) ポート：1～26 をアクセスポートに設定します。
(2) ポート：1～5 とポート：25、26 をトランクポートに設定します。

```
# configure terminal
(config)# interface port 1-26
(config-if-port)# switchport mode access
(config-if-port)# exit
(config)# interface port 1-5,25-26
(config-if-port)# switchport mode trunk
```

関連コマンド

show vlan, show running-config

注意事項

3.11.5 switchport access

アクセスポートが所属する VLAN を設定します。デフォルトの VLAN に設定する場合は、no コマンドを使用してください。

アクセスポートは 1 つの VLAN にのみ所属することができます。複数の VLAN に所属させる場合は、ト

ランクポートに設定する必要があります("vlan state"項、"switchport trunk"項参照)。
　アクセスポートで受信したVLANタグ無しフレームは、設定したVLANに属するフレームであると認識して当該VLANに中継します。

コマンドシンタックス

switchport access vlan <VID>
no switchport access
　　VID　　アクセスポートが所属するVLAN ID <1-4094>

デフォルト

VLAN ID：1

コマンドモード

IF-PORT

使用例

(1) ポート：1～12をVLAN ID：1のVLANに所属するアクセスポートに設定します。
(2) ポート：13～26をVLAN ID：2のVLANに所属するアクセスポートに設定します。

```
# configure terminal
(config)# interface port 1-12
(config-if-port)# switchport access vlan 1
(config-if-port)# exit
(config)# interface port 13-26
(config-if-port)# switchport access vlan 2
```

関連コマンド

show vlan, show running-config

注意事項

本コマンドを実行するには、指定するVLANをあらかじめ生成しておく必要があります("vlan name"項参照)。

本コマンドを実行するには、指定するポートをあらかじめアクセスポートに設定しておく必要があります("switchport mode"項参照)。

アクセスポートでVLANタグ付きフレームを受信した場合、そのVLAN IDがアクセスポートに登録されているVLAN IDと等しければ、本装置は受信したフレームを中継します(IEEE 802.1Q準拠)。

アクセスポートでVLAN ID：0のタグ付きフレーム(プライオリティタグフレーム)を受信した場合、タグ無しフレームと同様に処理されます。なお、ソフトウェア中継されるフレームは、タグプライオリティが0固定で中継されます。

3.11.6 switchport trunk

トランクポートが所属する VLAN を設定します。設定をデフォルトに戻す場合、no コマンドを使用してください。

トランクポートで受信した VLAN タグ無しフレームは、ネイティブ VLAN に属するフレームであると認識して当該 VLAN に中継します。トランクポートで受信した VLAN タグ付きフレームは、タグ内の VLAN ID がトランクポートに設定されていれば中継します。

コマンドシンタックス

```
switchport trunk add <VLANRANGE>
switchport trunk native | remove | protocol <VID>
switchport trunk remove
no switchport trunk
```

add	タグ付きフレームを中継
native	タグ無しフレームを中継
remove	タグ付き、またはタグ無しフレームを中継する VLAN を削除
protocol	プロトコル VLAN を登録
VLANRANGE	VLAN ID <1-4094> (複数指定可能)
VID	VLAN ID • native：<1-4094> • remove：<1-4094> • protocol：<2-4094>

デフォルト

なし(＝所属する VLAN なし)

コマンドモード

IF-PORT

使用例

(1) ポート：1～26 で受信したタグ無しフレームを VLAN ID：10 の VLAN に中継します。
(2) ポート：9～26 で受信した VLAN ID：2、VLAN ID：3 のタグ付きフレームの中継を許可します。
(3) ポート：9～26 で受信した VLAN ID：3 のタグ付きフレームの中継を禁止します。
(4) ポート：20～24 で受信した ipv4 プロトコルフレームを VLAN ID：20 の VLAN に中継します。

```
> enable
# configure terminal
(config)# interface port 1-26
(config-if-port)# switchport trunk native 10
(config-if-port)# exit
(config)# interface port 9-26
(config-if-port)# switchport trunk add 2
(config-if-port)# switchport trunk add 3
(config-if-port)# switchport trunk remove 3
(config-if-port)# exit
(config)# vlan database
```

```
(config-vlan)# vlan 20 add protocol ipv4
(config-vlan)# exit
(config)# interface port 20-24
(config-if-port)# switchport trunk protocol 20
```

関連コマンド

show vlan, show running-config

注意事項

本コマンドを実行するには、指定する VLAN をあらかじめ生成しておく必要があります("vlan name"項参照)。

本コマンドを実行するには、指定するポートをあらかじめトランクポートに設定しておく必要があります("switchport mode"項参照)。

トランクポートで VLAN ID：0 のタグ付きフレーム(プライオリティタグフレーム)を受信した場合、タグ無しフレームと同様に処理されます。なお、ソフトウェア中継されるフレームは、タグプライオリティが 0 固定で中継されます。

3.11.7 vlan add protocol

VLAN データベースにプロトコル VLAN を追加します。設定をデフォルトに戻す場合は、no コマンドをしようしてください。プロトコルの指定は、フレームタイプとタイプ値を組み合わせる設定方法と、プリセットプロトコルを指定する設定方法があります。

コマンドシンタックス

[no] vlan <VID> add protocol ether | llc | snap <TYPE>

[no] vlan <VID> add protocol appletalk | ipv4 | ipv6 | ipx | ipx_8022 | ipx_snap | netbios

VID	VLAN ID <2-4094>
ether	EthernetV2 形式フレーム
llc	802.3 LLC 形式フレーム
snap	802.3 LLC/SNAP 形式フレーム
TYPE	タイプを 16 進数で設定 (llc、snap は 0x0000～0xffff、ether は 0x0600～0xffff)
appletalk	appletalk (snap 0x809b + snap 0x80f3 と同等)
ipv4	ipv4 (ether 0x0800 + ether 0x0806 と同等)
ipv6	ipv6 (ether 0x86dd と同等)
ipx	ipx (ether 0x8137 と同等)
ipx_8022	ipx_802.2 (llc 0xe0e0 と同等)
ipx_snap	ipx_snap (snap 0x8137 と同等)
netbios	netbios (llc 0xf0f0 + llc 0xf0f1 と同等)

デフォルト

なし(＝設定無し)

コマンドモード

VLAN

使用例

(1) VLAN ID：4094 の VLAN にフレームタイプ ether、タイプ値：0x0800 のプロトコルを追加します。

(2) VLAN ID：4094 の VLAN に ipv6 プロトコルを追加します。

```
> enable
# configure terminal
(config)# vlan database
(config-vlan)# vlan 4094 add protocol ether 0x0800
(config-vlan)# vlan 4094 add protocol ipv6
```

関連コマンド

show vlan, show running-config

注意事項

VLAN タグ付きフレームはプロトコル VLAN の対象になりません。

ingress filter が有効の場合、プロトコル VLAN で設定した VLAN をポートに設定する必要があります。

同一 VLAN、及び 1 ポートに設定可能なプロトコル数は最大 7 個です。また装置全体で設定可能なプロトコルの種類は最大 16 個です。
設定可能な個数は、16 進数で設定した場合の数になります。ipv4 のように 2 つの ether type に展開される場合、2 つと数える必要があります。

ignore-tag を設定した VLAN ではプロトコル VLAN を使用できません。

3.11.8 tag-type

装置が VLAN タグ付きフレームとして認識する 802.1Q タグタイプを変更します。本機能により、802.1Q の VLAN タグ付きフレームを VLAN タグ無しフレームとみなすことができ、VLAN のトンネリングが可能になります(802.1ad Stacked VLAN 機能)。

コマンドシンタックス

tag-type <TAG-TYPE>
no tag-type

TAG-TYPE	802.1Q タグタイプ(16 進数表記) <0x0-0xffff>

デフォルト

0x8100(＝802.1Q VLAN タグフレーム)

コマンドモード

VLAN

使用例

(1) 802.1Q タグタイプを 0x9100 に変更します。

```
> enable
# configure terminal
(config)# vlan database
(config-vlan)# tag-type 0x9100
```

関連コマンド

show tag-type, show running-config

注意事項

正常に通信させるためには対向接続する装置の VLAN タグタイプを同じ値に設定してください。

0x0000～0x05DC の値は IEEE 802.3 の Length Field(0～1500)として予約されています。これらの値をタグタイプとして設定した場合、対向接続する装置によっては廃棄される可能性があります。

タグタイプを設定した場合、VLAN タグ付きフレームによる装置に対する通信、監視、その他の機能(3.36 IGMP Snooping、3.29 ユーザーループ検知、3.42 MMRP-Plus など)は使用できません。

0x8808 は IEEE 制御(3.7.10 "pause"コマンドなど)用に予約されています。この値をタグタイプとして設定した場合、VLAN トンネリングは構成できません。

3.11.9 ignore-tag

本機能を有効にすると、アクセスポートが受信した 802.1Q VLAN タグフレームをタグ無しフレームとして処理し、VLAN のトンネリングが可能になります(802.1ad Stacked VLAN 機能)。トランクポートで受信した 802.1Q VLAN タグフレームの VLAN タグは無視されません。

コマンドシンタックス

[no] ignore-tag enable

デフォルト

no enable(＝無効)

コマンドモード

VLAN

使用例

(1) 受信フレームの VLAN タグを無視するよう設定します。

```
> enable
# configure terminal
(config)# vlan database
(config-vlan)# ignore-tag enable
```

関連コマンド

show ignore-tag, show running-config

注意事項

本機能を有効にすると VLAN タグ付きフレームによる装置に対する通信、監視、その他の機能(3.36 IGMP Snooping、3.29 ユーザーループ検知など)は使用できません。

3.11.10 snap-nonzero-oui

本機能を有効にすると、SNAP OUI(SNAP Organization code)が 00 00 00 以外も SNAP 形式のフレームとして認識するようにします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] snap-nonzero-oui enable

デフォルト

no enable(＝無効)

コマンドモード

VLAN

使用例

(1) SNAP の Organization code が 00 00 00 以外のフレームも SNAP として認識するようにします。

(2) SNAP の Organization code が 00 00 00 のフレームのみ SNAP として認識するようにします。

```
> enable
# configure terminal
(config)# vlan database
(config-vlan)# snap-nonzero-oui enable
(config-vlan)# no snap-nonzero-oui enable
```

関連コマンド

show vlan, show running-config

注意事項

3.11.11 show vlan

VLAN ステータス情報を表示します。

コマンドシンタックス

show vlan [<VID>]

VID　　表示する VLAN ID

コマンドモード

VIEW, ENABLE

使用例

(1) VLAN ステータス情報を表示します。

```
# show vlan

--- vlan port information ---
                 a = access-port  t = trunk-port
                 Port
                 1      8 9     16 17    24 25    32 33    40 41    48 49
                 +------+ +------+ +------+ +------+ +------+ +------+ +-
 Port Mode       aaatttaa atttaaaa aaattaaa aaaaaaaa aaaaaaaa aaaaaaaa aa

--- vlan mapping information ---
                 St = Status  En = Enable  Dis = Disable
                 u = untag  t = tag  p = protocol vlan  d = dynamic port vlan
                 Port
                 1      8 9     16 17    24 25    32 33    40 41    48 49
 Name     VID St  +------+ +------+ +------+ +------+ +------+ +------+ +-
default     1 En  ......uu u...uuuu .....uuu uuuuuuuu uuuuuuuu uuuuuuuu uu
v2          2 En  uuu..... ........ ........ ........ ........ ........ ..
v3          3 En  ........ .ttt.... ........ ........ ........ ........ ..
v4          4 En  ........ ........ uuupp... ........ ........ ........ ..

--- protocol vlan information ---
 VID  protocol   type
---------------------
   2    ether   0x0800
   3    snap    0x0806
   4    llc     0x0800

SNAP nonzero OUI: Disable
#
```

PORT Mode　　：ポートの VLAN 属性

a　　：アクセスポート(ポートベース VLAN モード)

t　　：トランクポート(802.1Q タグ付き VLAN モード)

Name　　：VLAN 名

VID　　：VLAN ID
Port　　：VLAN メンバー
　u　　：タグ無しフレーム中継ポート(untagged メンバー)
　t　　：タグ付きフレーム中継ポート(tagged メンバー)
　p　　：プロトコル VLAN 中継ポート
　d　　：Dynamic Port VLAN 中継ポート
protocol　　：フレームタイプ
　ether　　：Ethernet-II
　llc　　：802.3 LLC
　snap　　：802.3 LLC/SNAP
type　　：タイプ値
SNAP nonzero OUI　　：SNAP Organization code 00 00 00 以外のフレームの扱い
　Enable　　：プロトコル VLAN(SNAP)の対象とする
　Disable　　：プロトコル VLAN(SNAP)の対象としない

関連コマンド

注意事項

3.11.12 show tag-type

タグタイプ情報を表示します。

コマンドシンタックス

show tag-type

コマンドモード

VIEW, ENABLE

使用例

(1) 802.1Q タグタイプ情報を表示します。

```
# show tag-type
  VLAN Tag Type: 0x8100
#
```

関連コマンド

注意事項

3.11.13 show ignore-tag

ignore-tag の構成情報を表示します。

コマンドシンタックス

show ignore-tag

コマンドモード

VIEW, ENABLE

使用例

(1) ignore-tag の構成情報を表示します。

```
# show ignore-tag
  VLAN Ignore Tag: enable
#
```

関連コマンド

注意事項

3.12 LLDP

LLDP(Link Layer Discovery Protocol)は、LLDP フレームを送受信することにより定期的に隣接する装置情報を収集するプロトコルです。

注意事項

LLDP とポートリダンダントを同一ポートで使用しないでください。同一のポートで使用した場合の動作は保証されません。

Apresia3400/4300/5400 シリーズで LLDP タイムアウト時間(msg-tx-interval × msg-tx-hold)を 4 秒以下に設定し、かつ疑似リンクダウン機能を使用する場合は、以下の設定範囲内で使用するようにしてください。

- **IP アドレス数：装置全体で 8 個以内**
- **疑似リンクダウン使用ポート数：16 ポート以内**

上記範囲を超える設定でも動作はしますが、上記の設定数が多い場合は装置への過負荷により以下の事象が発生することがあります。

- **多数ポートの一斉リンクアップ時に、疑似リンクダウン状態がばたつく**
- **多数ポートの一斉リンクダウン時に、LLDP 設定ポートからの LLDPDU の送信に遅延が発生し、対向の疑似リンクダウン設定ポートで通信断が発生する**

3.12.1 lldp enable

LLDP 機能を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] lldp enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) LLDP 機能を有効にします。
(2) LLDP 機能を無効にします。

```
# configure terminal
(config)# lldp enable
(config)# no lldp enable
```

関連コマンド

show running-config, show lldp configuration

注意事項

ポートリダンダントと本機能を、同一のポートで使用しないでください。同一のポートで使用した場合の動作は保証されません。

マルチキャストルーティング("ip multicast-routing")有効時、本機能を有効にすることはできません。

3.12.2 lldp mode

LLDP 機能の動作モードを設定します。動作モードをデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

lldp mode tx-rx | tx-only | rx-only | tx-rx-err-disable
no lldp mode

tx-rx	LLDP フレームを送受信
tx-only	LLDP フレームを送信のみ行い、受信した LLDP フレームを破棄
rx-only	LLDP フレームの受信のみ
tx-rx-err-disable	疑似リンクダウン情報(独自 TLV(Type Length Value))付き LLDP フレームを送受信

デフォルト

なし(＝設定なし)

コマンドモード

IF-PORT

使用例

(1) 動作モードを tx-rx に設定します。
(2) 動作モードを disable に設定します。

```
# configure terminal
(config)# interface port 1
(config-if-port)# lldp mode tx-rx
(config-if-port)# no lldp mode
```

関連コマンド

show running-config, show lldp configuration

注意事項

3.12.3 lldp msg-tx-interval

LLDP フレームの送信間隔を設定します。送信間隔をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

lldp msg-tx-interval <INTERVAL>
no lldp msg-tx-interval
　　INTERVAL　　送信間隔を指定 <1-32768(秒)>

デフォルト

30(秒)

コマンドモード

CONFIG

使用例

(1) LLDP フレームの送信間隔を 10 秒に設定します。
(2) LLDP フレームの送信間隔をデフォルト値に戻します。

```
# configure terminal
(config)# lldp msg-tx-interval 10
(config)# no lldp msg-tx-interval
```

関連コマンド

show running-config, show lldp configuration

注意事項

LLDP フレームの送信間隔("lldp msg-tx-interval")は送信遅延間隔("lldp tx-delay")と次の条件を満たす必要があります。
送信遅延間隔 ≦ 0.25 × 送信間隔
ただし、1 ≦ 送信間隔 ≦ 4 の場合、上記条件は適用されず設定した値で動作します。

3.12.4 lldp msg-tx-hold

送信する LLDP フレームの TTL TLV(Type Length Value)のパラメーター(隣接機の情報保持時間)を msg-tx-interval の倍数で設定します。TTL TLV をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

lldp msg-tx-hold <TTL-TLV>
no lldp msg-tx-hold
　　TTL-TLV　　TTL TLV パラメーター <2-10>

デフォルト
4

コマンドモード
CONFIG

使用例
(1) LLDP フレームの TTL TLV を 5 に設定します。
(2) LLDP フレームの設定をデフォルト値に戻します。

```
# configure terminal
(config)# lldp msg-tx-hold 5
(config)# no lldp msg-tx-hold
```

関連コマンド
show running-config, show lldp configuration

注意事項

3.12.5 lldp reinit-delay

"lldp mode"コマンドにより LLDPDU の動作モードを変更した場合、LLDP フレーム送信再開までの遅延時間を設定します。本設定をデフォルト値に戻す場合は、no コマンドを使用してください。遅延時間が満了する前に、"lldp mode"コマンドによる動作モードの再変更や本コマンドによる遅延時間の再設定は、LLDP フレーム送信再開までの遅延時間満了後に反映されます。

なお、"no lldp enable"コマンドを用いて LLDP フレームの送信を無効にし、"lldp enable"コマンドで再度有効化した場合、"lldp tx-delay"コマンドによる遅延のみとなり、本コマンドの遅延時間は加算されません。

コマンドシンタックス
lldp reinit-delay <DELAY>
no lldp reinit-delay
DELAY　　LLDPDU 送信再開までの遅延時間 <1-10(秒)>

デフォルト
2(秒)

コマンドモード
CONFIG

使用例
(1) LLDPDU 送信再開までの遅延時間を 10 秒に設定します。
(2) LLDPDU 送信再開までの遅延時間をデフォルト値に戻します。

```
# configure terminal
(config)# lldp reinit-delay 10
(config)# no lldp reinit-delay
```

関連コマンド

show running-config, show lldp configuration

注意事項

3.12.6 lldp tx-delay

LLDP フレーム送信遅延間隔を設定します。送信遅延間隔をデフォルト値に戻す場合は、no コマンドを使用してください。

LLDP フレームは、"lldp msg-tx-interval"コマンドで設定した送信間隔、または LLDP フレームの内容が変更された場合に送信されます。本コマンドによる送信遅延間隔は、以下の契機に反映されます。

- LLDP 機能の有効化("lldp enable")
- 動作モードの変更("lldp mode")
- 当該ポートの有効化(3.7.1 "no shutdown")

また、以下のコマンドの設定値は、本コマンドの送信遅延間隔経過前は満了まで待ってから反映され、送信遅延間隔経過満了後は即時反映されます。

- "lldp msg-tx-hold"
- "lldp msg-tx-interval"
- "lldp management-address"

コマンドシンタックス

lldp tx-delay <DELAY>
no lldp tx-delay

DELAY	LLDP フレーム送信遅延間隔 <1-8192(秒)>

デフォルト

2(秒)

コマンドモード

CONFIG

使用例

(1) LLDP 送信遅延間隔を 10 秒に設定します。
(2) LLDP 送信遅延間隔をデフォルト値に戻します。

```
# configure terminal
(config)# lldp tx-delay 10
(config)# no lldp tx-delay
```

関連コマンド

show running-config, show lldp configuration

注意事項

LLDP フレーム送信遅延間隔("lldp tx-delay")は、送信間隔("lldp

msg-tx-interval")と次の条件を満たす必要があります。
送信遅延間隔 ≦ 0.25 × 送信間隔
ただし、1 ≦ 送信間隔 ≦ 4 の場合、上記条件は適用されず設定した値で動作します。

3.12.7 lldp management-address

本装置に設定した VLAN の IP アドレスを管理用 IP アドレスとしてリモートシステムに送信します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

本コマンドで管理用 IP アドレスの設定を行わない場合、管理ポートの IP アドレス、もしくは VLAN インターフェース 1 の IP アドレスが送信されます(デフォルト)。管理ポート、VLAN インターフェース 1 に IP アドレスが設定されていない場合、0.0.0.0 を管理用 IP アドレスとして送信します。

コマンドシンタックス

```
lldp management-address vlan <VID>
no lldp management-address vlan
```

VID　　VLAN ID

デフォルト

管理ポートがある装置	管理ポートの IP アドレス
管理ポートがない装置	VLAN インターフェース 1 の IP アドレス

コマンドモード

CONFIG

使用例

(1) 管理用 IP アドレスとして VLAN ID：10 を設定します。
(2) 管理用 IP アドレスの設定をデフォルトに戻します。

```
# configure terminal
(config)# lldp management-address vlan 10
(config)# no lldp management-address vlan
```

関連コマンド

show running-config, show lldp configuration

注意事項

3.12.8 lldp err-disable-mode

LLDP による疑似リンクダウン機能を有効にします。LLDP フレームにより自局ポートのリンク情報を対向装置に通知することにより、LLDP フレームの受信状態や受信した内容により隣接スイッチの状態を確認し、障害発生/復旧時にポートを閉塞/復旧させます。

コマンドシンタックス

[no] lldp err-disable-mode enable

デフォルト
no enable(＝無効)

コマンドモード
CONFIG

使用例
(1) LLDP による疑似リンクダウン機能を有効にします。
(2) LLDP による疑似リンクダウン機能を無効にします。

```
# configure terminal
(config)# lldp err-disable-mode enable
(config)# no lldp err-disable-mode enable
```

関連コマンド
show running-config, show lldp, show interface status

注意事項

LLDP 機能が無効("no lldp enable")の場合、本機能を有効("lldp err-disable-mode enable")にすることはできません。また、本機能が動作中は、LLDP 機能を無効にすることはできません。

本機能と 3.42 MMRP-Plus 機能を併用する場合の各種タイマー値は 3.42.29 "mmrp-plus ring hello-timeout"を参照ください。

本機能を有効にする場合、必ず接続対向装置にも本機能を設定してください。

3.12.9 show lldp port

ポートに格納されている受信した LLDP フレームの情報を表示します。

本コマンドで表示される項目のうち、Chassis ID と Port ID は、それぞれの subtype の値に応じて、表 3-10、表 3-11 に示す形式で表記されます。表示例は、Chassis ID に文字列"chas-1"が、また、Port ID に文字列"port-9"が格納されていた場合を示します。

表 3-10 Chassis ID の表示形式

Chassis ID の subtype	Chassis ID の表示形式	表示例
4	MAC アドレス形式	63:68:61:73:2D:31
2、6	文字列	chas-1
上記以外	16 進数表記	636861732D31

表 3-11 Port ID の表示形式

Port ID の subtype	Port ID の表示形式	表示例
3	MAC アドレス形式	70:6F:72:74:2D:39
1、5	文字列	port-9
上記以外	16 進数表記	706F72742D39

コマンドシンタックス

show lldp port <PORTRANGE>

PORTRANGE　　ポート番号(複数指定可能)

コマンドモード

VIEW, ENABLE

使用例

(1) ポート：24 で受信した LLDP フレームを表示します(疑似リンクダウン機能が無効("no lldp err-disable-mode enable"))。

```
# show lldp port 24
Port               : 24
Chassis ID         : 00:40:66:13:09:4e
Port ID            : Gigaether-24
TTL                : 120
Port Description   : Apresia13000-48X-24
System Name        :
System Description : Hitachi Cable Ethernet Switch Apresia13000-48X Ver.7.15.01
Mgmt. Address      : 192.168.1.65
```

(2) ポート：24 で受信した LLDP フレームを表示します(疑似リンクダウン機能が有効("lldp err-disable-mode enable"))。

```
# show lldp port 24
Port               : 24
Chassis ID         : 00:40:66:13:09:4e
Port ID            : Gigaether-24
TTL                : 120
Port Description   : Apresia13000-48X-24
System Name        :
System Description : Hitachi Cable Ethernet Switch Apresia13000-48X Ver.7.15.01
Mgmt. Address      : 192.168.1.65
Link Status        : Normal
```

Link Status　　：受信した LLDPDU の未受信フラグ状態

Normal　　：通常時、または LLDPDU 受信不可(InfoTTL expire)時

Fault　　：未受信フラグ付きの LLDPDU 受信時

- 対向装置が LLDPDU 未受信時に、未受信フラグ付き LLDPDU を受信

関連コマンド

注意事項

System Name にはシステムグループ MIB のシステムネームが表示されます(3.3.1 "hostname"コマンドで指定したホスト名ではありません)。System Name を変更する場合、3.48.9 "snmp-server name"コマンドを使用してください。

InfoTTL expire は msg-tx-interval × msg-tx-hold 時間、LLDP フレームを受信しなかったことを示します。

3.12.10 show lldp port detail

ポートに格納されている受信した LLDP フレームの詳細な情報を表示します。

本コマンドで表示される項目のうち、Chassis ID と Port ID は、それぞれの subtype の値に応じて、表 3-12、表 3-13 に示す形式で表記されます。表示例は、Chassis ID に文字列"chas-1"が、また、Port ID に文字列"port-9"が格納されていた場合を示します。

表 3-12 Chassis ID の表示形式

Chassis ID の subtype	Chassis ID の表示形式	表示例
4	MAC アドレス形式	63:68:61:73:2D:31
2、6	文字列	chas-1
上記以外	16 進数表記	636861732D31

表 3-13 Port ID の表示形式

Port ID の subtype	Port ID の表示形式	表示例
3	MAC アドレス形式	70:6F:72:74:2D:39
1、5	文字列	port-9
上記以外	16 進数表記	706F72742D39

コマンドシンタックス

show lldp port detail <PORTRANGE>

PORTRANGE　　ポート番号(複数指定可能)

コマンドモード

VIEW, ENABLE

使用例

(1) ポート：1 で受信した LLDP フレームの詳細を表示します。

```
# show lldp port detail 1
Port                : 1
Chassis ID          : 00:40:66:11:66:fd
Port ID             : Gigaether-1
TTL                 : 120
Port Description    : Apresia13000-48X-24
System Name         : ap13000
```

```
System Description : Hitachi Cable Ethernet Switch Apresia 13000-48X Ver.7.14.02
Mgmt. Address      : 192.168.1.65
Vendor TLVs:
```

関連コマンド

注意事項

3.12.11 show lldp configuration

ローカルシステムの LLDP 構成情報を表示します。

コマンドシンタックス

show lldp configuration

コマンドモード

VIEW, ENABLE

使用例

(1) LLDP 構成情報を表示します。

```
# show lldp configuration
Mode            : Enable
Msg Tx Hold     : 4
Msg Tx Interval : 30
Reinit Delay    : 2
Tx Delay        : 2
Mgmt. VID       : 0
PseudoLinkdown  : Enabled

port    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
mode   tr tr tr tr tr tr tr tr tr tr tr tr  t  t  t  t  t  t  t  r

port   21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
mode    r  r  d  d  d  d  d  d  d  d  d  d  d  d  d  d  d  d  d ed

port   41 42 43 44 45 46 47 48 49 50
mode   ed ed ed ed ed ed ed ed ed ed
```

MODE　　：LLDP 機能(Enable/Disable)
Msg Tx Hold　　：LLDP フレームの TTL TLV
Msg Tx Interval　　：LLDP フレームの送信間隔
Reinit Delay　　：LLDPDU 送信再開までの遅延時間
Tx Delay　　：LLDP フレーム送信遅延間隔
Mgmt. VID　　：管理用 IP アドレス
PseudoLinkdown　　：LLDP 疑似リンクダウン機能(Enable/Disable)

mode　　：動作モード
　tr　　：LLDP フレームを送受信
　t　　：LLDP フレームを送信のみ
　r　　：LLDP フレームを受信のみ
　d　　：動作モードが非設定
　ed　　：リンク情報が載った LLDP フレームを送受信

関連コマンド

注意事項

3.12.12 show lldp statistics

ローカルシステムの LLDP の統計情報を表示します。

コマンドシンタックス

show lldp statistics

コマンドモード

VIEW, ENABLE

使用例

(1) LLDP の統計情報を表示します。

```
# show lldp statistics
Port    InTotal   OutTotal    Discard    Ageouts   Inerrors TLVDiscard UnknownTLV
  1         239        243          0          0          0          0          0
  2           0          0          0          0          0          0          0
  3         239        241          0          0          0          0          0
  4           0          0          0          0          0          0          0
  5         239        241          0          0          0          0          0
  6           0          0          0          0          0          0          0
  7           0          0          0          0          0          0          0
  8           0          0          0          0          0          0          0
  9         239        240          0          0          0          0          0
 10           0          0          0          0          0          0          0
 11           0          0          0          0          0          0          0
 12           0          0          0          0          0          0          0
 13         239        239          0          0          0          0          0
 14           0          0          0          0          0          0          0
 15           0          0          0          0          0          0          0
 16           0          0          0          0          0          0          0
 17           0          0          0          0          0          0          0
                                   (省略)
 49           0          0          0          0          0          0          0
 50           0          0          0          0          0          0          0
```

```
#
```

関連コマンド

注意事項

3.13 MTU

3.13.1 mtu

中継可能なフレームサイズ(MTU)を指定します。イーサネットフレームの MAC ヘッダー(宛先 MAC アドレス、送信元 MAC アドレス、Length/Type)、データ、FCS が MTU の対象になります。設定値はタグ無しフレーム(FCS 含む)の場合の値です。UTP ポート、もしくは GBIC ポートで 802.1q タグ付きフレームを中継する場合、中継可能なフレームサイズは設定値より 4 オクテット大きくなります。設定値は 4 の整数倍となるように切り捨てられます(ただし 1518 の場合を除く)。XENPAK ポートでは、フレームのタグ付の有無に関係なく設定した MTU 値で制限されます。

コマンドシンタックス

mtu <MTU>
no mtu
MTU　　MTU <1518-9044(オクテット)>

デフォルト

1544(オクテット)

コマンドモード

CONFIG

使用例

(1) 中継可能なフレームサイズ(MTU)を設定します。

```
> enable
# configure terminal
(config)# mtu 1518
```

関連コマンド

show mtu, show running-config

注意事項

3.13.2 show mtu

MTU 情報を表示します。本コマンドでは 4 の整数倍が切り捨てられた値が表示され、"show running-config"コマンドでは"mtu"コマンドで実際に入力した値が表示されます。

コマンドシンタックス

show mtu

コマンドモード

VIEW, ENABLE

使用例

(1) MTU 情報を表示します。

```
# show mtu
  MTU: 1544 byte
#
```

関連コマンド

注意事項

3.14 Forwarding Data Base(FDB)

3.14.1 mac-address-table static

FDB にスタティックエントリーを登録します。登録できるエントリーは最大 256 個です。登録したユニキャスト MAC アドレスを宛先に持つフレームは設定したポートにのみ中継されます。

コマンドシンタックス

mac-address-table static <MACADDR> vlan <VID> interface <PORT>
no mac-address-table static <MACADDR> vlan <VID>

MACADDR	MAC アドレス
VID	VLAN ID
PORT	ポート番号

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) VLAN ID：1、ポート：10 に MAC アドレス：00:40:66:00:00:01 のエントリーを登録します。
(2) (1)のエントリーを削除します。

```
> enable
# configure terminal
(config)# mac-address-table static 00:40:66:00:00:01 vlan 1 interface 10
(config)# no mac-address-table static 00:40:66:00:00:01 vlan 1
```

関連コマンド

show mac-address-table, show running-config

注意事項

ミラーリング To ポートに設定されているポート、及びポートリダンダントグループのメンバーポートに対して、スタティック FDB エントリーのポートの設定はできません。

I/G ビットが 1 である MAC アドレス(マルチキャスト MAC アドレス)は登録できません。

3.14.2 mac-address-table aging-time

本装置が動的に学習した MAC アドレスを削除する時間(秒)を設定します。値は 0(エージング OFF)、及び 10 から 1000000 まで設定可能です。

コマンドシンタックス

mac-address-table aging-time <AGINGTIME>
no mac-address-table aging-time
AGINGTIME　　エージング時間 <0、10-1000000(秒)>

デフォルト
300(秒)

コマンドモード
CONFIG

使用例
(1) エージング時間を 600 秒に設定します。
(2) エージング OFF を設定します。

```
> enable
# configure terminal
(config)# mac-address-table aging-time 600
(config)# mac-address-table aging-time 0
```

関連コマンド
show mac-address-table aging-time, show running-config

注意事項

実際に FDB のエントリーが削除されるのは、<AGINGTIME>～<AGINGTIME> × 2 までの時間幅があります。

3.17.1 "spanning-tree mode"コマンドを設定時、及び削除時に、エージング時間がデフォルト値に戻るため再度設定してください。

3.14.3 show mac-address-table

FDB の情報を表示します。ポートごと、または VLAN ごとに表示することもできます。

コマンドシンタックス
show mac-address-table [(port <PORTRANGE>) | (vlan <VLANRANGE>)]
PORTRANGE　　ポート番号(複数指定可能)
VLANRANGE　　VLAN ID <1-4094> (複数指定可能)

コマンドモード
VIEW, ENABLE

使用例
(1) FDB の情報を表示します。

```
# show mac-address-table
```

```
Total MAC addresses : 3

  MAC address          port VID  status
  00:40:66:11:12:4a    CPU  1    static
  00:b0:d0:d3:c6:be    7    1    dynamic
  00:12:11:f1:aa:12    8    1    dynamic
```

Total MAC addresses　：登録されている MAC アドレスエントリー数
MAC addresses　：登録されている MAC アドレス
port　：MAC アドレスが学習されているポート
　(VLAN インターフェースは CPU と表示)
VID　：MAC アドレスが学習されている VLAN ID
status　：エントリー種別
　static　：スタティック登録エントリー、
　　または VLAN インターフェースエントリー
　dynamic　：動的に学習されたエントリー

関連コマンド

注意事項

管理ポートで学習されたエントリーは表示されません。

リンクアグリゲーションを構成した場合のポート番号表示は、フレームを受信したポートに関係なくリンクアグリゲーションを構成したポートの最小番号が表示されます。

宛先 MAC アドレスが表 3-9 である制御フレームは、受信ポートにおいてフレームの送信元 MAC アドレスを学習します。

3.14.4 show mac-address-table aging-time

エージング時間の構成情報を表示します。

コマンドシンタックス

show mac-address-table aging-time

コマンドモード

VIEW, ENABLE

使用例

(1) エージング時間の構成情報を表示します。

```
# show mac-address-table aging-time
Aging Time: 300 seconds
```

関連コマンド

注意事項

3.14.5 clear mac-address-table

FDB に動的に登録された MAC アドレスを消去します。

コマンドシンタックス

clear mac-address-table dynamic [(interface port <PORT>) | (vlan <VID>)]

PORT	指定されたポートに登録された MAC アドレスを削除
VID	指定された VLAN に登録された MAC アドレスを削除

コマンドモード

ENABLE

使用例

(1) FDB のポート：7 に登録されている MAC アドレスを削除します。

```
# clear mac-address-table dynamic interface port 7
```

関連コマンド

注意事項

3.15 Flush FDB

3.15.1 flush-fdb rp-e port

Flush FDB 機能をポートごとに有効にします。無効にする場合は、no コマンドを使用してください。有効にすると同じハローパケットを別のポートより受信した場合に FDB を消去します。検出するハローパケットの宛先 MAC アドレスは 00:E0:2B:00:00:02、送信元 MAC アドレスは 00:E0:2B:00:00:80～9F です。

コマンドシンタックス

flush-fdb rp-e port <PORTRANGE> enable
no flush-fdb rp-e enable
PORTRANGE　　ポート番号(複数指定可能)

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) Flush FDB 機能を有効にします。

```
# configure terminal
(config)# flush-fdb rp-e port 1-26 enable
```

関連コマンド

show flush-fdb rp-e, show running-config

注意事項

本装置では、ハローパケットを受信するポートが切り替わった場合だけではなく、ハローパケットを初めて検出した場合にも、自動的に FDB が消去されます。

本装置の時刻を戻す変更を行った場合、Flush FDB が動作しない場合があります。本コマンドで再設定を行ってください。

本コマンドを有効にするとパケットフィルター2 のグループを 1 つ使用します。

本コマンドはパケットフィルター2 のグループ番号を指定できず、自動的にまだ他の機能で使用されていない最老番のグループから確保します。

本装置再起動後は構成情報の記載順にパケットフィルター2 のグループが確保されます。他機能とグループ番号が重複しないよう、表 3-19 をご確認ください。

3.15.2 flush-fdb rp-g port

Flush FDB 機能(GSRP aware)をポートごとに有効にします。無効にする場合は、no コマンドを使用してください。有効にすると GSRP Flush Request フレームを受信した場合に FDB を消去します。検出する GSRP Flush Request フレームの宛先 MAC アドレスは 00:00:87:58:13:00 です。

コマンドシンタックス

flush-fdb rp-g port <PORTRANGE> enable
no flush-fdb rp-g enable
PORTRANGE　　ポート番号(複数指定可能)

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) Flush FDB 機能(GSRP aware)を有効にします。

```
# configure terminal
(config)# flush-fdb rp-g port 1-26 enable
```

関連コマンド

show flush-fdb rp-g, show running-config

注意事項

本装置の時刻を戻す変更を行った場合、Flush FDB が動作しない場合があります。本コマンドで再設定を行ってください。

本コマンドを有効にするとパケットフィルター2 のグループを 1 つ使用します。

本コマンドはパケットフィルター2 のグループ番号を指定できず、自動的にまだ他の機能で使用されていない最老番のグループから確保します。

本装置再起動後は構成情報の記載順にパケットフィルター2 のグループが確保されます。他機能とグループ番号が重複しないよう、表 3-19 をご確認ください。

3.15.3 show flush-fdb rp-e

本装置に設定されている Flush FDB 機能の情報を表示します。

コマンドシンタックス

show flush-fdb rp-e

コマンドモード

VIEW, ENABLE

使用例

(1) Flush FDB 機能の情報を表示します。

```
# show flush-fdb rp-e
Enable port : 1-26
Total entry : 3

  VID  group port Last-HelloPacket     Last-Fdb-Flushed     Total-Fdb-Flushes
  1    0     18   2006/02/02 14:32:13  2006/02/02 14:32:10  272
  1    1     18   2006/02/02 14:32:13  2006/02/02 14:32:10  272
  1    2     18   2006/02/02 14:32:13  2006/02/02 14:32:10  272
```

Enable port　　：Flush FDB 機能が有効になっているポート
Total entry　　：現在のエントリー数
VID　　：VLAN ID
group　　：グループ番号
port　　：ハローパケットを受信したポートの番号
Last-HelloPacket　　：ハローパケットを最後に受信した時刻
Last-Fdb-Flushed　　：最後に FDB を自動的に消去した時刻
Total-Fdb-Flushes　　：FDB を自動的に消去した回数

関連コマンド

注意事項

3.15.4 show flush-fdb rp-g

本装置に設定されている Flush FDB 機能(GSRP aware)の情報を表示します。

コマンドシンタックス

show flush-fdb rp-g

コマンドモード

VIEW, ENABLE

使用例

(1) Flush FDB 機能(GSRP aware)の情報を表示します。

```
# show flush-fdb rp-g
Enable port : 1-26
Total entry : 3

  port Last-Fdb-Flushed     Total-Fdb-Flushes
  14   2006/07/01 12:40:00  1
  16   2006/07/01 12:45:53  2
```

```
  18    2006/07/01 12:40:00   1
```

Enable port　　：Flush FDB 機能(GSRP aware)が有効になっているポート
Total entry　　：現在のエントリー数
Port　　：GSRP Flush Request フレームを受信したポートの番号
Last-Fdb-Flushed　　：最後に FDB を自動的に消去した時刻
Total-Fdb-Flushes　　：FDB を自動的に消去した回数

関連コマンド

注意事項

3.16 ARP テーブル

ARP(Address Resolution Protocol)テーブルの情報を参照/設定します。通信がない場合 ARP テーブルのエントリーは 20～25 分で更新されます。登録された ARP 情報の更新には ARP パケットの受信が必要です。

注意事項

Apresia13000 シリーズ/4348 シリーズはユニキャスト MAC アドレス宛の ARP に応答しません。

ARP テーブルに登録された端末の交換が行われた後も、古い ARP テーブルを保持し続けていた場合、交換後の ARP パケットを受け取るまでは、古い MAC アドレス宛にパケットを送信し続けてしまいます。

3.16.1 arp static

ARP テーブルにスタティックエントリーを登録します。スタティックエントリーは最大 256 個登録可能です。スタティックエントリーを削除する場合は、no コマンドを使用してください。all を指定すると全スタティックエントリーを削除します。

本機能を動作させるには、FDB テーブルに同一 MAC アドレスを登録する必要があります(3.14.1 "mac-address-table static")。

コマンドシンタックス

arp static <IPADDR> <MACADDR>
no arp <IPADDR> | all

IPADDR	IP アドレス
MACADDR	MAC アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) IP アドレス：10.74.8.5、MAC アドレス：00:40:66:11:ba:58 の端末を ARP テーブルに登録します。

```
(config)# arp static 10.74.8.5 00:40:66:11:ba:58
```

関連コマンド

mac-address-table static, show arp, show running-config

注意事項

3.16.2 show arp

ARP テーブル内に登録されている情報を表示します。

コマンドシンタックス

show arp

コマンドモード

VIEW, ENABLE

使用例

(1) ARP 情報を表示します。

```
# show arp
Total : 5

(172.17.51.1) at 08:00:2b:22:70:7b on manage (age 00:23:26)
(172.17.51.176) at 00:40:66:a3:57:90 on manage permanent
(172.17.51.221) at 00:40:66:10:fb:e7 on manage (age 00:12:53)
(192.168.0.15) at 00:b0:d0:d3:c6:be on vlan 1 (age 00:03:44)
(192.168.0.16) at 00:b0:d1:d4:c7:cc on vlan 1 (age 00:05:19)
```

Total　：ARP エントリー数
permanent　：静的エントリー
age　：ARP エントリーが生成されてからの経過時間(permanent の場合は非表示)
出力形式　：([IP アドレス]) at [MAC アドレス] on [登録インターフェース] (age [HH:MM:SS])
本装置のインターフェースに設定された IP アドレスに対する ARP エントリー、及び ARP テーブルのスタティックエントリーについては、登録インターフェースの後ろに"permanent"が表示されます。

関連コマンド

注意事項

ARP 登録上限数は Apresia3400/4300/5400 シリーズが 5000、Apresia13000 シリーズが 10000 です。

3.16.3 clear arp

動的に学習した ARP エントリーを消去します。

コマンドシンタックス

clear arp <IPADDR> | all

IPADDR　ARP エントリーの IP アドレス
all　動的に学習した全 ARP エントリーの消去

コマンドモード

ENABLE

使用例

(1) 動的に学習した 192.168.0.100 の ARP エントリーを消去します。

(2) 動的に学習した全 ARP エントリーを削除します。

```
> enable
# clear arp 192.168.1.100
# clear arp all
```

関連コマンド

注意事項

3.17 スパニングツリープロトコル(STP/RSTP/MSTP)

注意事項

MSTP を使用される場合には、リージョン数 1 個、インスタンス数 2 個以内に設定してください。

スパニングツリー動作中にスパニングツリーの各種設定変更を行うと、装置にトポロジーチェンジが発生します。

スパニングツリープロトコル(STP/RSTP/MSTP)と 3.42 MMRP-Plus を装置で同時に使用できません。

スパニングツリープロトコル(STP/RSTP/MSTP)と LACP は併用できません。

Apresia13000-48X、及び Apresia4348 シリーズの場合は、各スパニングツリープロトコルのポートをトランクポート(3.11.4 "switchport mode")に設定してください。ただし、ネイティブ VLAN の設定(3.11.6 "switchport trunk native <VID>")は行わないでください。

3.17.1 spanning-tree mode

スパニングツリープロトコルの動作モードを設定します。動作モードの設定を削除する場合は、no コマンドを使用してください。RSTP、STP、MSTP の切り替えは、一度 no コマンドで設定を削除してから行う必要があります。

スパニングツリープロトコル関連のコマンド(後述)を使用するには、あらかじめ本コマンドでスパニングツリーのモードを設定しておく必要があります。

"no spanning-tree mode"コマンドで本コマンドの設定を削除する時は、その他のスパニングツリーの設定も同時に削除されます。また、スパニングツリーが動作中("spanning-tree enable"コマンドが設定されている間)は、"no spanning-tree mode"コマンドは実行できません。

(1) "spanning-tree mode"コマンドで、STP/RSTP/MSTP いずれかの設定が必要となるコマンド

```
spanning-tree enable
spanning-tree priority
spanning-tree disable
spanning-tree port-priority
spanning-tree cost
spanning-tree forward-time
spanning-tree hello-time
spanning-tree max-age
```

(2) "spanning-tree mode"コマンドで、RSTP/MSTP の設定が必要となるコマンド(RSTP/MSTP モードの時のみ設定可能)

```
spanning-tree link-type
spanning-tree portfast
clear spanning-tree detected protocols
spanning-tree force-version
spanning-tree interconnection-mode
```

(3) "spanning-tree mode"コマンドで、MSTP の設定が必要となるコマンド(MSTP モードの時のみ設定可能)

```
spanning-tree mst configuration
spanning-tree mst max-hops
instance priority
instance vlan
name
revision
spanning-tree mst instance
spanning-tree mst instance port-priority
spanning-tree mst instance cost
```

コマンドシンタックス

spanning-tree mode stp | rst | mst
no spanning-tree mode

stp	IEEE 802.1D 仕様の Spanning Tree
rst	IEEE 802.1w 仕様の Rapid Spanning Tree
mst	IEEE 802.1s 仕様の Multiple Spanning Tree

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) スパニングツリープロトコルのモードを IEEE 802.1D 仕様に設定します。
(2) スパニングツリープロトコルのモード設定を解除します。この時、STP の設定がすべてクリアされる旨の確認に答える必要があります。

```
> enable
# configure terminal
(config)# spanning-tree mode stp
(config)# no spanning-tree mode
Current STP parameters will be cleared. Proceed anyway? (y/n): y
(config)#
```

関連コマンド

show spanning-tree switch, show running-config

注意事項

1 台の装置に STP、RSTP、MSTP を同時に設定することはできません。いずれかの 1 つのモードでご使用ください。

動作モード、及び"spanning-tree enable"設定時は全ポートにおいて BPDU を中継しません。

本コマンド設定時、及び削除時に FDB のエージング時間がデフォルト値に戻るため、3.14.2 "mac-address-table aging-time"コマンドにて再度設定してください。

3.17.2 spanning-tree enable

スパニングツリープロトコルを有効にし、動作を開始させます。動作を停止させる場合は、no コマンドを使用してください。

コマンドシンタックス

[no] spanning-tree enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) スパニングツリープロトコルを IEEE 802.1D 仕様で開始します。
(2) スパニングツリープロトコルを停止します。

```
> enable
# configure terminal
(config)# spanning-tree mode stp
(config)# spanning-tree enable
(config)# no spanning-tree enable
```

関連コマンド

show spanning-tree switch, show running-config

注意事項

STP、RSTP、MSTP の各設定値は、デフォルト値でのご使用を推奨します。この場合推奨 diameter 数(任意の 2 つのエンドステーション間の最大スイッチ数)は 7 台となります。

リンクアグリゲーションとスパニングツリープロトコルを同時に使用した場合、以下

のような動作となります。

(1) LAG(リンクアグリゲーショングループ)内の最小ポート以外のポート状態は、STP モードの場合は DISABLED("show spanning-tree port")、RSTP/MSTP モードの場合は Discarding("show spanning-tree rst"/"show spanning-tree mst detail") と表示されますが、リンクアグリゲーションの帯域拡張は有効であり、通信に影響はありません。

(2) STP モードでは、port 別の STP 設定が異なる場合、それらのポートを同一グループとしたポートリダンダントの設定を行うことはできません。

(3) RSTP、MSTP モードでは、port 別の STP 設定が異なっていてもリンクアグリゲーションの設定を行うことはできますが、port 別の STP の設定値は LAG 中で最も番号の小さいポートの設定がグループ全体の設定として採用されます。他のポートの設定は動作に反映されません。

ポートリダンダントとスパニングツリープロトコルを同時に使用した場合、以下のような動作となります。
ポートリダンダントグループ内の最小ポート以外のポート状態は、STP モードの場合は DISABLED("show spanning-tree port")、RSTP/MSTP モードの場合は Discarding("show spanning-tree rst"/"show spanning-tree mst detail")と表示されますが、ポートリダンダントのプライオリティ指定は有効であり、通信に影響はありません。

(1) STP モードでは、port 別の STP 設定が異なる場合、それらのポートを同一グループとしたポートリダンダントの設定を行うことはできません。

(2) RSTP、MSTP モードでは、port 別の STP 設定が異なっていてもポートリダンダントの設定を行うことはできますが、port 別の STP の設定値はポートリダンダントグループ中で最も番号の小さいポートの設定がグループ全体の設定として採用されます。他のポートの設定は動作に反映されません。

STP、RSTP、MSTP のいずれかを有効にした場合、自動的に 3.18.1 "bpdu-forward disable"が設定されます。無効にした場合にも設定が残ります。

3.17.3 spanning-tree disable

任意のポートをスパニングツリープロトコルの動作対象からはずします。動作対象に戻す場合は、no コマンドを使用してください。

STP/RSTP モードでは、デフォルトですべてのポートがスパニングツリープロトコルの動作対象になります。ポートによりスパニングツリープロトコルを動作させたくない場合は、本コマンドで動作対象からはずしてください。

コマンドシンタックス

[no] spanning-tree disable

デフォルト

no disable(＝動作対象)

コマンドモード

IF-PORT

使用例

(1) ポート：1～3 ではスパニングツリープロトコルが動作しないようにします。

```
> enable
# configure terminal
(config)# interface port 1-3
(config-if-port)# spanning-tree disable
```

関連コマンド

show spanning-tree port, show running-config

注意事項

MSTP 機能使用時に本機能(disable)を設定するとすべてのフレーム中継が停止するため、他機能との併用ができません。MSTP 機能をポート単位で停止させ他機能と併用する場合は、MSTP インスタンスを設定しない方法で対応してください。

3.17.4 spanning-tree forward-time

スパニングツリープロトコルのフォワードディレイ時間を設定します。設定を削除する場合は、no コマンドを使用してください。

フォワードディレイ時間は、ルートブリッジになったときに送信するコンフィグレーション BPDU 内に含まれる LISTENING、LEARNING ステータスのタイムアウト値です。したがって、ルートブリッジにならなかった場合には使用されません。

MSTP モード選択時、複数のインスタンスを設定し、インスタンスごとにルートブリッジが異なる場合は、インスタンス 0 のルートブリッジに設定されているフォワードディレイ時間が有効となります。

コマンドシンタックス

spanning-tree forward-time <SECONDS>
no spanning-tree forward-time
　SECONDS　　フォワードディレイ時間 <4-30(秒)>

デフォルト

15(秒)

コマンドモード

CONFIG

使用例

(1) フォワードディレイ時間を 30 秒に設定します。

```
> enable
```

```
# configure terminal
(config)# spanning-tree forward-time 30
```

関連コマンド

show spanning-tree switch, show running-config

注意事項

フォワードディレイを変更する場合はカスケード接続段数に注意してください。IEEE 802.1D ではフォワードディレイが 15 の場合は最大カスケード接続数 7 を推奨しています。

3.17.5 spanning-tree hello-time

スパニングツリープロトコルのハロー間隔を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

ハロー間隔は、ルートブリッジがコンフィグレーション BPDU を送信する間隔です。

MSTP モード選択時、複数のインスタンスを設定し、インスタンスごとにルートブリッジが異なる場合は、インスタンス 0 のルートブリッジに設定されているハロー間隔が有効となります。

コマンドシンタックス

spanning-tree hello-time <SECONDS>
no spanning-tree hello-time
SECONDS　　ハロー間隔 <1-10(秒)>

デフォルト

2(秒)

コマンドモード

CONFIG

使用例

(1) スパニングツリープロトコルのハロー間隔を 9 秒に設定します。

```
> enable
# configure terminal
(config)# spanning-tree hello-time 9
```

関連コマンド

show spanning-tree switch, show running-config

注意事項

3.17.6 spanning-tree link-type

RSTP モード/MSTP モード時に、ポートのリンクタイプを設定します。設定を削除する場合は、no コマ

ンドを使用してください。

コマンドシンタックス

spanning-tree link-type point-to-point | shared
no spanning-tree link-type
　　point-to-point　　1対1のリンク時
　　shared　　3以上のノードの帯域共有時

デフォルト

point-to-point

コマンドモード

IF-PORT
(ただし、RSTP、またはMSTPモードを指定した時のみ設定可能)

使用例

(1) RSTPモードでポート：1～4までのリンクタイプをsharedに設定します。

```
> enable
# configure terminal
(config)# spanning-tree mode rst
(config)# interface port 1-4
(config-if-port)# spanning-tree link-type shared
```

関連コマンド

show running-config

注意事項

3.17.7 spanning-tree max-age

スパニングツリープロトコルのコンフィグレーション BPDU の最大経過時間を設定します。値は 6 から 40 までの設定が可能です。

最大経過時間は、本装置がルートブリッジになったときに送信するコンフィグレーション BPDU の最大経過時間です。したがってルートブリッジにならなかったときには使用されません。

MSTPモード選択時、複数のインスタンスを設定し、インスタンスごとにルートブリッジが異なる場合は、インスタンス0のルートブリッジに設定されている最大経過時間が有効となります。

コマンドシンタックス

spanning-tree max-age <SECONDS>
no spanning-tree max-age
　　SECONDS　　BPDUの最大経過時間 <6-40(秒)>

デフォルト

20(秒)

コマンドモード
CONFIG

使用例
(1) コンフィグレーション BPDU の最大経過時間を 25 秒に設定します。

```
> enable
# configure terminal
(config)# spanning-tree max-age 25
```

関連コマンド
show spanning-tree switch, show running-config

注意事項

3.17.8 spanning-tree priority

スパニングツリープロトコルのプライオリティを設定します。設定を削除する場合は、no コマンドを使用してください。

プライオリティは、STP モードを選択している場合は 0 から 65535 まで、RSTP/MSTP モードを選択している場合は、0 から 61440 まで設定が可能です。プライオリティが小さいほどルートブリッジになる可能性が高くなります。

コマンドシンタックス
spanning-tree priority <PRIORITY>
no spanning-tree priority

PRIORITY	プライオリティ • STP モード ：<0-65535> • RSTP モード：<0-61440> • MSTP モード：<0-61440>

デフォルト
32768

コマンドモード
CONFIG

使用例
(1) プライオリティを 10000 に設定します。

```
> enable
# configure terminal
(config)# spanning-tree priority 10000
```

関連コマンド
show spanning-tree switch, show running-config

注意事項

MSTP モードの場合、設定値はインスタンス 0 にのみ反映されます。

RSTP モード、MSTP モードの場合、0-61440 の範囲の任意の数値を設定できますが、実際の数値は 4096 の整数倍に切り捨てられます。構成情報に保存される値も切り捨てた値となります。

プライオリティ変更などトポロジーチェンジを伴う設定作業時には、不慮のループ発生回避のため、必ずポートの shutdown などで物理ループ構成を解除してから実施してください。

3.17.9 spanning-tree portfast

RSTP モード、または MSTP モード選択時、ポートに Port Fast 機能を設定します。設定を解除する場合は、no コマンドを使用してください。

Port Fast が設定されたポートは、リンクアップ時に即座に、Blocking ステータスから Forwarding ステータスに遷移します。

コマンドシンタックス

[no] spanning-tree portfast

デフォルト

なし(＝設定なし)

コマンドモード

IF-PORT

(ただし、RSTP、または MSTP モードを指定時のみ設定可能)

使用例

(1) RSTP モードでポート：1～4 まで Port Fast を有効に設定します。

```
> enable
# configure terminal
(config)# spanning-tree mode rst
(config)# interface port 1-4
(config-if-port)# spanning-tree portfast
```

関連コマンド

show spanning-tree mst port, show running-config

注意事項

エッジポート(RSTP、MSTP が動作しない端末を接続するポート)以外には Port Fast を設定しないでください。

3.17.10 spanning-tree port-priority

各ポートのスパニングツリープロトコルの優先度を設定します。設定を削除する場合は、no コマンドを使用してください。

STP モードを選択している場合は 0～255 まで、RSTP/MSTP モードを選択している場合は、0～240 までの設定が可能です。

本コマンドは、非ルートブリッジの装置が同一セグメントに複数のポートを接続している場合に使用します。設定値が小さいほど優先度が高くなり、ルートポートになる可能性が高くなります。値が同じ場合、ポート番号が小さいほうがルートポートになる可能性が高くなります。

コマンドシンタックス

spanning-tree port-priority <PRIORITY>
no spanning-tree port-priority

PRIORITY　各ポートの優先度
- STP モード　：<0-255>
- RSTP モード：<0-240>
- MSTP モード：<0-240>

デフォルト

128

コマンドモード

IF-PORT

使用例

(1) ポート：1～4 までの優先度を 100 に設定します。

```
> enable
# configure terminal
(config)# interface port 1-4
(config-if-port)# spanning-tree port-priority 100
```

関連コマンド

show spanning-tree port, show running-config

注意事項

RSTP モード、MSTP モードの場合、0-240 の範囲の任意の数値を設定できますが、実際の数値は 16 の整数倍に切り捨てられます。構成情報に保存される値も切り捨てた値となります。

MSTP モードの場合、設定値はインスタンス 0 にのみ反映されます。

3.17.11 spanning-tree cost

各ポートのスパニングツリープロトコルのパスコストを設定します。設定を削除する場合は、no コマンドを使用してください。

パスコストは、ルートブリッジまでの近さを判断する基準となります。小さいパスコストがルートブリッジまで近いことを表します。

BPDU を受信した装置は、受信したインターフェースに設定されているパスコストを加算して、他の装置へ転送します。パスコストを変更することによって、経路を変更することができるようになります。

パスコストは、STP モードの時は 0 から 1000000、RSTP/MSTP モードの時は 0 から 200000000 までの設定が可能です。デフォルトは 0(パスコスト自動設定)です。デフォルト状態では、リンクスピードによりパスコスト値が切り替わります。

コマンドシンタックス

spanning-tree cost <COST>
no spanning-tree cost

COST	各ポートのパスコスト • STP モード ：<0-1000000> • RSTP モード：<0-200000000> • MSTP モード：<0-200000000>

デフォルト

0(＝自動設定)

自動設定時のパスコストの値は、以下のようになります。

(1) STP モード時

```
10G リンク ：2
1G リンク  ：4
100M リンク：19
10M リンク ：100
```

(2) RSTP/MSTP モード時

```
10G リンク ：2000
1G リンク  ：20000
100M リンク：200000
10M リンク ：2000000
```

コマンドモード

IF-PORT

使用例

(1) ポート：1～4 までのスパニングツリープロトコルのパスコストを 100 に設定します。

```
> enable
# configure terminal
(config)# interface port 1-4
(config-if-port)# spanning-tree cost 100
```

関連コマンド

show spanning-tree port, show running-config

注意事項

MSTP モードの場合、設定値はインスタンス 0 にのみ反映されます。

3.17.12 spanning-tree force-version

RSTP/MSTP モードの時に、BPDU バージョンフィールド値を強制的に変更します。設定を削除する場合は、no コマンドを使用してください。

通常、BPDU のバージョンは RSTP が 2、MSTP が 3 ですが、本コマンドで 0 を指定することにより 802.1D 仕様のブリッジとの相互接続が確保されます。802.1w 仕様のブリッジのみで RSTP の機能をフルに使用するには、本コマンドを設定しないか、2 を指定して設定するようにしてください。802.1s 仕様のブリッジのみで MSTP の機能をフルに使用するには、本コマンドを設定しないか、3 を指定して設定するようにしてください。

コマンドシンタックス

spanning-tree force-version <VERSION>
no spanning-tree force-version
　VERSION　　BPDU のバージョンフィールド値 <0-3>

デフォルト

RSTP：2
MSTP：3

コマンドモード

IF-PORT
(ただし、RSTP、または MSTP モードを指定時のみ設定可能)

使用例

(1) RSTP モードでポート：1～4 までの BPDU バージョンフィールド値を 0 に設定します。

```
> enable
# configure terminal
(config)# spanning-tree mode rst
(config)# interface port 1-4
(config-if-port)# spanning-tree force-version 0
```

関連コマンド

show running-config

注意事項

3.17.13 spanning-tree mst configuration

MSTP に必要な情報を設定するための、MSTP モードに移行します。設定を削除した場合、すでに設定されているすべての情報が削除されます。

コマンドシンタックス
spanning-tree mst configuration

デフォルト
なし

コマンドモード
CONFIG
(ただし、MSTP モードを指定時のみ移行可能)

使用例
(1) MSTP モードに移行します。

```
> enable
# configure terminal
(config)# spanning-tree mode mst
(config)# spanning-tree mst configuration
```

関連コマンド
show spanning-tree mst config, show running-config

注意事項

3.17.14 spanning-tree mst max-hops

BPDU の最大ホップ数を指定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

MSTP モードの時に、不要な BPDU の送信を防ぐため、MST リージョン中で許される最大のホップ数を指定します。本設定値は装置がルートブリッジの場合に送信する BPDU の最大ホップ数です。ルートブリッジでない場合は適用されません。また、本設定はすべてのインスタンスで共通です。

コマンドシンタックス
spanning-tree mst max-hops <HOP_COUNT>
no spanning-tree mst max-hops
HOP_COUNT 最大ホップ数 <7-127>

デフォルト
20

コマンドモード
CONFIG

使用例
(1) max-hops を 10 に設定します。

```
> enable
```

```
# configure terminal
(config)# spanning-tree mode mst
(config)# spanning-tree mst max-hops 10
```

関連コマンド

show spanning-tree mst, show running-config

注意事項

3.17.15 instance priority

MSTP モードの時に、指定したインスタンスにプライオリティを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

プライオリティは 0 から 61440 までの設定が可能です。プライオリティが小さいほどルートブリッジか指定ブリッジ(Designated Bridge)になる可能性が高くなります。

コマンドシンタックス

instance <INSTANCE_ID> priority <PRIORITY>
no instance <INSTANCE_ID> priority

INSTANCE_ID	インスタンス ID <1-15>
PRIORITY	プライオリティ <0-61440>

デフォルト

32768

コマンドモード

MSTP

使用例

(1) プライオリティを 4096 に設定します。

```
> enable
# configure terminal
(config)# spanning-tree mode mst
(config)# spanning-tree mst configuration
(config-mst)# instance 2 vlan 30
(config-mst)# instance 2 priority 4096
```

関連コマンド

show spanning-tree mst instance, show running-config

注意事項

インスタンス 0 のプライオリティは"spanning-tree priority"コマンドで設定します。

プライオリティは、0-61440 の範囲の任意の数値を設定できますが、実際の数値は

4096 の整数倍に切り捨てられます。

3.17.16 instance vlan

MSTP モードの時に、インスタンスに VLAN を割り当てます。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

[no] instance <INSTANCE_ID> vlan <VID>

INSTANCE_ID　　インスタンス ID <0-15>

VID　　VLAN ID <1-4094>

デフォルト

全 VLAN がインスタンス 0 に割り当て

コマンドモード

MSTP

使用例

(1) インスタンス：2 を作成し VLAN ID：30 と VLAN ID：31 を割り当てます。

```
> enable
# configure terminal
(config)# spanning-tree mode mst
(config)# spanning-tree mst configuration
(config-mst)# instance 2 vlan 30
(config-mst)# instance 2 vlan 31
```

関連コマンド

show spanning-tree mst instance, show running-config

注意事項

MST インスタンスに VLAN を追加する前にあらかじめ VLAN コマンドにて VLAN を作成しておく必要があります。

3.17.17 name

MSTP モードの時に、MST リージョンの名前を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

name <REGION_NAME>

no name

REGION_NAME　　リージョン名 <32(文字)>

デフォルト
なし(＝設定なし)

コマンドモード
MSTP

使用例
(1) リージョン名を b1 に設定します。

```
> enable
# configure terminal
(config)# spanning-tree mode mst
(config)# spanning-tree mst configuration
(config-mst)# name b1
```

関連コマンド
show spanning-tree mst config, show running-config

注意事項

3.17.18 revision

MSTP モードの時に、MST リージョンを識別するためのリビジョン番号を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス
revision <REVISION_NUM>
no revision
REVISION_NUM　　リビジョン番号 <0-65535>

デフォルト
0

コマンドモード
MSTP

使用例
(1) リビジョン番号を 1 に設定します。

```
> enable
# configure terminal
(config)# spanning-tree mode mst
(config)# spanning-tree mst configuration
(config-mst)# revision 1
```

関連コマンド
show spanning-tree mst config, show running-config

注意事項

3.17.19 spanning-tree mst instance

MSTP モードの時に、指定したポートにインスタンスを割り当てます。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

[no] spanning-tree mst instance <INSTANCE_ID>

INSTANCE_ID　　インスタンス ID <0-15>

デフォルト

なし(＝設定なし)

コマンドモード

IF-PORT

使用例

(1) ポート：1～4 までにインスタンス：1 を割り当てます。

```
> enable
# configure terminal
(config)# interface port 1-4
(config-if-port)# spanning-tree mst instance 1
```

関連コマンド

show spanning-tree mst instance, show running-config

注意事項

3.17.20 spanning-tree mst instance port-priority

MSTP モードの時に、インスタンスごとにポートの優先度を設定します。設定を削除する場合は、no コマンドを使用してください。

本コマンドは、非ルートブリッジの装置が同一セグメントに複数のポートを接続している場合に使用します。設定値が小さいほど優先度が高くなり、ルートポートになる可能性が高くなります。値が同じ場合、ポート番号が小さいほうがルートポートになる可能性が高くなります。

コマンドシンタックス

spanning-tree mst instance <INSTANCE_ID> port-priority <PRIORITY>

no spanning-tree mst instance <INSTANCE_ID> port-priority

INSTANCE_ID　　インスタンス ID <0-15>

PRIORITY　　プライオリティ <0-240>

デフォルト

コマンドモード

IF-PORT

使用例

(1) ポート：1～4 までのインスタンス：1 のポート優先度を 100 に設定します。

```
> enable
# configure terminal
(config)# interface port 1-4
(config-if-port)# spanning-tree mst instance 1
(config-if-port)# spanning-tree mst instance 1 port-priority 100
```

関連コマンド

show spanning-tree mst instance, show running-config

注意事項

優先度は、0-240 の範囲の任意の数値を設定できますが、実際の数値は 16 の整数倍に切り詰められます。

3.17.21 spanning-tree mst instance cost

MSTP モードの時に、インスタンスのパスコストを設定します。設定を削除する場合は、no コマンドを使用してください。

MSTP は各インスタンスでループが発生した場合、低いパスコストのインターフェースを選んで、Forwarding ステータスに、他のインターフェースを Blocking ステータスにします。デフォルトは 0(パスコスト自動設定)です。パスコスト自動設定では、リンクスピードによりパスコスト値が切り替わります。

コマンドシンタックス

spanning-tree mst instance <INSTANCE_ID> cost <COST>
no spanning-tree mst instance <INSTANCE_ID> cost

INSTANCE_ID	インスタンス ID <0-15>
COST	パスコスト <0-200000000>

デフォルト

0(＝自動設定)

自動設定時のパスコスト値は、以下のようになります。

```
10G リンク  ：2000
1G リンク   ：20000
100M リンク：200000
10M リンク  ：2000000
```

コマンドモード

IF-PORT

使用例

(1) ポート：1～4 までのインスタンス：1 のパスコストを 200000 に設定します。

```
> enable
# configure terminal
(config)# interface port 1-4
(config-if-port)# spanning-tree mst instance 1
(config-if-port)# spanning-tree mst instance 1 cost 200000
```

関連コマンド

show spanning-tree mst instance, show running-config

注意事項

3.17.22 spanning-tree interconnection-mode

RSTP/MSTP において、他社製装置との相互接続性を改善します。設定を削除する場合は、no コマンドを使用してください。MSTP モードに設定する場合、あらかじめ、ポートをインスタンスに割り当てる必要があります。本コマンドを有効とすることにより agreement BPDU の設定値が以下に変更されます。

- root path cost：対向装置より受信した internal root path cost に port cost を加算した値
- remaining hops：対向装置より受信した remaining hops の値

コマンドシンタックス

[no] spanning-tree interconnection-mode

デフォルト

なし(＝設定なし)

コマンドモード

IF-PORT

使用例

(1) ポート：1 において他社製装置との相互接続性を改善します。

```
> enable
# configure terminal
(config)# interface port 1
(config-if-port)# spanning-tree interconnection-mode
```

関連コマンド

show running-config

注意事項

3.17.23 show spanning-tree configuration

スパニングツリープロトコルの構成情報を表示します。

コマンドシンタックス

show spanning-tree configuration

コマンドモード

VIEW, ENABLE

使用例

(1) スパニングツリープロトコルの構成情報を表示します。

```
# show spanning-tree configuration
STP Switch configuration:
     STP state           : enable
     Switch priority     : 32768
     Switch max age      : 20 seconds
     Switch hello time   : 2 seconds
     Switch forward delay : 15 seconds

STP Port configuration:
Port Priority Path cost STP state
1    128      0        disable
2    128      0        disable
(中略)
50   128      0        enable
```

関連コマンド

注意事項

3.17.24 show spanning-tree port

各ポートのスパニングツリープロトコルのパラメーターなどの情報を表示します。ただし、スパニングツリープロトコルが無効の場合は何も表示されません。

コマンドシンタックス

show spanning-tree port

コマンドモード

VIEW, ENABLE

使用例

(1) ポートのスパニングツリープロトコルのパラメーター情報を表示します。

```
# show spanning-tree port
========================= SpanningTree port parameters =======================
```

```
pt   port          pt      path cost   designated switch    des.  designated
no   state         prt                 (priority/mac)       port  cost
 1   STP OFF       128            0    ----/------ ------   ----          -
 2   STP OFF       128            0    ----/------ ------   ----          -
 3   STP OFF       128            0    ----/------ ------   ----          -
 4   DISABLED      128            0    8000/004066-7dc853   8004          0
 5   LISTENING     128            0    8000/004066-7dc853   8005          0
(中略)
50   DISABLED      128            0    8000/004066-7dc853   801a          0
```

pt no　　：ポート番号(10 進数表示)
port state　　：ポートステータス
　STP OFF
　LISTENING
　LEARNING
　FORWARDING
　BLOCKING
　DISABLED
　BROKEN
pt prt　　：ポート優先度(10 進数表示)
path cost　　：ポートパスコスト(10 進数表示)
designated switch　　：本装置から見て、スパニングツリーとして
　　ルート側に隣接した装置の ID
des.port　　：designated ポートの優先度とポート番号(16 進数表示)
　上位二桁の値　　：designated ポートの優先度
　下位二桁の値　　：designated ポート番号
des.cost　　：designated コスト(10 進数表示)

関連コマンド

注意事項

リンクアグリゲーションとスパニングツリープロトコル(STP)、及びポートリダンダントとスパニングツリープロトコル(STP)を同時に使用した場合、各グループ中最も番号の小さいポートのポート状態(port state)のみが変化し、他のポートは DISABLED と表示されます。

3.17.25 show spanning-tree switch

スパニングツリープロトコルの動作状態が表示されます。ただし、STP が Disabled に設定されている時には何も表示されません。

コマンドシンタックス

show spanning-tree switch

コマンドモード

VIEW, ENABLE

使用例

(1) スパニングツリープロトコルの動作状態を表示します。

```
# show spanning-tree switch
================ SpanningTree switch running parameters ================
   switch profile         : root switch
   desi root              : 8000/004066-7cf6d2 (priority/mac address)
   root port              : 0
   root path cost         : 0
   hello time             :  2 sec.
   max age                : 20 sec.
   forward delay          : 15 sec.
   aging time             : 300
================== SpanningTree switch static parameters ===============
   switch id              : 8000/004066-7cf6d2 (priority/mac address)
   switch hello time      :  2 sec.
   switch max age         : 20 sec.
   switch forward delay   : 15 sec.
```

switch profile　　：ルートスイッチかどうかを示す
desi root　　：ルートスイッチのプライオリティと MAC アドレス
root port　　：ルートと接続されているポート
root path cost　　：ルートまでのパスコスト
hello time　　：ハロー間隔
max age　　：コンフィグレーション BPDU の最大経過時間
forward delay　　：フォワードディレイ時間
aging time　　：エージング時間
switch id　　：スイッチ自身のプライオリティと MAC アドレス
switch hello time　　：スイッチ自身のハロー間隔
switch max age　　：スイッチ自身の BPDU 最大経過時間
switch forward delay　　：スイッチ自身のフォワードディレイ時間

関連コマンド

注意事項

3.17.26 show spanning-tree statistics

起動後から現在までのスパニングツリープロトコルに関する統計情報を表示します。

コマンドシンタックス

show spanning-tree statistics

コマンドモード

VIEW, ENABLE

使用例

(1) スパニングツリープロトコルに関する統計情報を表示します。

```
# show spanning-tree statistics
========= SpanningTree statistics information ==========
port  fwdCnt  blkCnt  rxCBPDU  rxTBPDU  txCBPDU  txTBPDU
   1       0       0        0        0        0        0
   2       0       0        0        0        0        0
(中略)
  50       0       2        0        0        2        0
```

fwdCnt　　：FORWARDING ステータスに遷移した回数(10 進数表示)
blkCnt　　：BLOCKING ステータスに遷移した回数(10 進数表示)
rxCBPDU　　：Configuration BPDU の受信回数(10 進数表示)
rxTBPDU　　：TCN(Topology Change Notification) BPDU の受信回数(10 進数表示)
txCBPDU　　：Configuration BPDU の送信回数(10 進数表示)
txTBPDU　　：TCN BPDU の送信回数(10 進数表示)

関連コマンド

注意事項

リンクアグリゲーションとスパニングツリープロトコル(STP)、及びポートリダンダントとスパニングツリープロトコル(STP)を同時に使用した場合、各グループ中最も番号の小さいポートのカウントのみ増加します。

3.17.27 show spanning-tree rst

RSTP に関する情報を表示します。

コマンドシンタックス

show spanning-tree rst [port <PORT>]
　PORT　　ポート番号

コマンドモード

VIEW, ENABLE

使用例

(1) RSTP に関する情報を表示します。

```
# show spanning-tree rst
% brg: Spanning Tree Enabled - Learning Enabled
% brg: Aging Time 300 - Root Path Cost 0 - Priority 32768
% brg: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% brg: Root Id 8000004066130973
% brg: Bridge Id 8000004066130973
```

```
% brg: 55 topology changes - last topology change Thu Apr 19 12:52:30 2007
%
%   port1: Port 1 - Id 8001 - Role Disabled - State Discarding
%   port1: Configured path cost 20000000 - Designated path cost 0
%   port1: Designated port id 8001 - Priority 128
%   port1: Designated Root 8000004066130973
%   port1: Designated Bridge 8000004066130973
%   port1: Message Age 0 - Max Age 20
%   port1: Hello Time 2 - Forward Delay 15
%   port1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   port1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   port1: No portfast configured - Current  portfast off
%   port1: Configured Link Type point-to-point - Current point-to-point
%   port1: No interconnection mode configured
%
%   port2: Port 2 - Id 8002 - Role Disabled - State Discarding
%   port2: Configured path cost 20000000 - Designated path cost 0
%   port2: Designated port id 8002 - Priority 128
%   port2: Designated Root 8000004066130973

(以下略)
```

Brg ステータス

Spanning Tree Enabled	：スパニングツリーの動作状況
Learning Enabled	：有効
Learning Disabled	：無効
Aging Time	：エージング時間(10 進数表示)
Root Path Cost	：ルートまでのパスコスト(10 進数表示)
Priority	：スイッチ自身のプライオリティ(10 進数表示)
Forward Delay	：フォワードディレイ時間(10 進数表示)
Hello Time	：ハロー間隔(10 進数表示)
Max Age	：BPDU の最大経過時間(10 進数表示)
Root Port	：ルートポート(10 進数表示)
Root Id	：ルートブリッジのプライオリティと MAC アドレス(16 進数表示)
Bridge Id	：スイッチ自身のプライオリティと MAC アドレス(16 進数表示)
** topology changes	：トポロジーチェンジした回数(10 進数表示)
last topology change	：最後にトポロジーチェンジが起きた時間

port ステータス

Id	：ポートの ID 番号(16 進数表示)
Role	：ポート役割
Root	
Designated	
Alternate	

```
  Backup
State                          ：ポートステータス
  Discarding
  Learning
  Forwarding
  Disabled
Configured path cost           ：ポートが接続したリンクのパスコスト(10 進数表示)
Designated path cost           ：ルートブリッジまでのパスコスト(10 進数表示)
Designated port id             ：接続した指定ポートの ID 番号
                                 (16 進数表示、自身が指定ポートの場合は自身の値)
Priority                       ：ポートプライオリティ(10 進数表示)
Designated Root                ：ルートブリッジのプライオリティと MAC アドレス
                                 (16 進数表示)
Designated Bridge              ：指定ブリッジプライオリティと MAC アドレス
                                 (16 進数表示、自身が指定ポートの場合は自身の値)
Message Age                    ：受信した BPDU の有効時間(10 進数表示)
Max Age                        ：BPDU の最大経過時間(10 進数表示)
Hello Time                     ：ハロー間隔(10 進数表示)
Forward Delay                  ：フォワードディレイ時間(10 進数表示)
Version                        ：スパニングツリーのバージョン
  RSTP
  STP
Portfast configured            ：Port Fast の設定
  No portfast configured
  Portfast configured
Configured Link Type           ：リンクタイプ
  point-to-point
  shared
Interconnection mode configured ：他社製装置との相互接続性
  No interconnection mode configured
  Interconnection mode configured
```

関連コマンド

注意事項

リンクアグリゲーションとスパニングツリープロトコル(RSTP)、及びポートリダンダントとスパニングツリープロトコル(RSTP)を同時に使用した場合、各グループ中最も番号の小さいポートのポート状態(port state)のみが変化し、他のポートは Discarding と表示されます。

3.17.28 show spanning-tree mst

MSTP に関する情報を表示します。作成したインスタンスとそれに関連づけられた VLAN を表示します。

コマンドシンタックス

show spanning-tree mst

コマンドモード

VIEW, ENABLE

使用例

(1) MSTP に関する情報を表示します。

```
# show spanning-tree mst
% brg: Bridge up - Spanning Tree Enabled
% brg: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% brg: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% brg: CIST Root Id 8000004066119001
% brg: CIST Reg Root Id 8000004066119001
% brg: CST Bridge Id 8000004066119001
%
%   Instance        VLAN
%   0:              1
%   1:              11
%   2:              21
```

関連コマンド

注意事項

3.17.29 show spanning-tree mst config

MSTP に関する構成情報を表示します。

コマンドシンタックス

show spanning-tree mst config

コマンドモード

VIEW, ENABLE

使用例

(1) MSTP に関する構成情報を表示します。

```
# show spanning-tree mst config
%
%  MSTP Configuration Information for bridge brg :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : b1
%  Revision Level : 0
%  Digest         : 0xC11059A55216D1A689741811D49765CC
```

```
%-----------------------------------------------------
```

関連コマンド

注意事項

3.17.30 show spanning-tree mst detail

MSTP に関する情報を表示します。すべてのインスタンスとポートに関する詳細情報を表示します。

コマンドシンタックス

show spanning-tree mst detail

コマンドモード

VIEW, ENABLE

使用例

(1) MSTP に関する詳細情報を表示します。

```
# show spanning-tree mst detail
% brg: Bridge up - Spanning Tree Enabled
% brg: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 0
% brg: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% brg: CIST Root Id 00000040661274dd
% brg: CIST Reg Root Id 00000040661274dd
% brg: CST Bridge Id 00000040661274dd
%   port12: Port 12 - Id 800c - Role Designated - State Forwarding
%   port12: Designated External Path Cost 0 -Internal Path Cost 0
%   port12: Configured Path Cost 20000  - Add type Implicit ref count 1
%   port12: Designated Port Id 800c - CST Priority 128  -
%   port12: CIST Root 00000040661274dd
%   port12: Regional Root 00000040661274dd
%   port12: Designated Bridge 00000040661274dd
%   port12: Message Age 0 - Max Age 20
%   port12: CIST Hello Time 2 - Forward Delay 15
%   port12: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   port12: CIST Remaining Hops 20
%   port12: Version Multiple Spanning Tree Protocol - Received RSTP - Send RSTP
%   port12: No portfast configured - Current  portfast off
%   port12: Configured Link Type point-to-point - Current point-to-point
%   port12: No interconnection mode configured
%
%   port13: Port 13 - Id 800d - Role Designated - State Forwarding
%   port13: Designated External Path Cost 0 -Internal Path Cost 0
%   port13: Configured Path Cost 20000  - Add type Implicit ref count 1
%   port13: Designated Port Id 800d - CST Priority 128  -
```

```
%   port13: CIST Root 00000040661274dd
%   port13: Regional Root 00000040661274dd
%   port13: Designated Bridge 00000040661274dd
%   port13: Message Age 0 - Max Age 20
%   port13: CIST Hello Time 2 - Forward Delay 15
%   port13: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   port13: CIST Remaining Hops 20
%   port13: Version Multiple Spanning Tree Protocol - Received RSTP - Send RSTP
%   port13: No portfast configured - Current  portfast off
%   port13: Configured Link Type point-to-point - Current point-to-point
%   port13: No interconnection mode configured
%
% Instance  1:  Vlans: 10
% brg: MSTI Root Path Cost 40000 - MSTI Root Port 13 - MSTI Bridge Priority 122
88
% brg: MSTI Root Id 0001004066114312
% brg: MSTI Bridge Id 30010040661274dd
%   port12: Port 12 - Id 800c - Role Alternate - State Discarding
%   port12: Configured Internal Path Cost 20000 -External Path cost 20000
%   port12: Designated Internal Path Cost 20000  - Designated Port Id 800c
%   port12: CST Priority 128  - MSTI Priority 128
%   port12: Designated Root 0001004066114312
%   port12: Designated Bridge 200100406612bd10
%   port12: Message Age 0 - Max Age 0
%   port12: Hello Time 2 - Forward Delay 15
%   port12: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0
%   port12: MSTI Remaining Hops 18
%
%   port13: Port 13 - Id 800d - Role Rootport - State Forwarding
%   port13: Configured Internal Path Cost 20000 -External Path cost 20000
%   port13: Designated Internal Path Cost 20000  - Designated Port Id 800d
%   port13: CST Priority 128  - MSTI Priority 128
%   port13: Designated Root 0001004066114312
%   port13: Designated Bridge 10010040661276ce
%   port13: Message Age 0 - Max Age 0
%   port13: Hello Time 2 - Forward Delay 15
%   port13: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0
%   port13: MSTI Remaining Hops 18
```

Brg ステータス

Bridge up	：スパニングツリーの動作状況
Learning Enabled	：有効
Learning Disabled	：無効
CIST Root Path Cost	：CIST ルートブリッジまでのパスコスト(10 進数表示)
CIST Root Port	：CIST ルートポートのポート番号
CIST Bridge Priority	：CIST スイッチ自身のプライオリティ(10 進数表示)

Forward Delay　　：フォワードディレイ時間(10 進数表示)
Hello Time　　：ハロー間隔(10 進数表示)
Max Age　　：BPDU の最大経過時間(10 進数表示)
Max Hops　　：BPDU 最大ホップ数(10 進数表示)
CIST Root Id　　：CIST ルートブリッジのプライオリティと MAC アドレス
(16 進数表示)
CST Bridge Id　　：CIST スイッチ自身のプライオリティと MAC アドレス
(16 進数表示)
Instance　　：インスタンス番号
Vlans　　：インスタンスに所属する VLAN ID
MSTI Root Path Cost　　：MSTI ルートまでのパスコスト(10 進数表示)
MSTI Root Port　　：MSTI ルートポートのポート番号
MSTI Bridge Priority　　：MSTI スイッチ自身のプライオリティ(10 進数表示)

port ステータス(CIST インスタンス 0)
Id　　：ポートの ID 番号(16 進数表示)
Role　　：ポート役割
Root
Designated
Alternate
Backup
State　　：ポートステータス
Discarding
Learning
Forwarding
Disabled
Designated External Path Cost　　：CIST 外部ルートパスコスト(10 進数表示)
Internal Path Cost　　：CIST 内部ルートパスコスト(10 進数表示)
Configured Path Cost　　：ポートが接続したリンクのパスコスト(10 進数表示)
Designated Port Id　　：接続した指定ポートの ID 番号
(16 進数表示、自身が指定ポートの場合は自身の値)
CST Priority　　：CST ポートプライオリティ
CIST Root　　：CIST ルートブリッジのプライオリティと MAC アドレス
(16 進数表示)
Regional Root　　：リージョン内のルートブリッジのプライオリティと
MAC アドレス(16 進数表示)
Designated Bridge　　：指定ブリッジプライオリティと MAC アドレス
(16 進数表示、自身が指定ポートの場合は自身の値)
CIST Message Age　　：受信した BPDU の有効時間(10 進数表示)
Max Age　　：BPDU の最大経過時間(10 進数表示)
Hello Time　　：CIST ハロー間隔(10 進数表示)
CIST Forward Delay　　：CIST フォワードディレイ時間(10 進数表示)
CIST Forward Timer　　：CIST フォワードタイマー(10 進数表示)
CIST Msg Age Timer　　：CIST BPDU メッセージ有効タイマー(10 進数表示)
CIST Hello Timer　　：CIST ハロータイマー(10 進数表示)

```
    CIST Remaining Hops             : CIST BPDU 残り有効ホップ数
    Version Multiple Spanning Tree Protocol
                                    : 送受信プロトコル
      Received                      : 受信プロトコル
        RSTP                        : RSTP、または MSTP
        STP                         : STP
        None                        : 未確定
      Send                          : 送信プロトコル
        RSTP                        : RSTP、または MSTP
        STP                         : STP
        None                        : 未確定
    Portfast configured             : Port Fast の設定
      No portfast configured
      Portfast configured
    Configured Link Type            : リンクタイプ
      point-to-point
      shared
    Interconnection mode configured : 他社製装置との相互接続性
      No interconnection mode configured
      Interconnection mode configured

port ステータス(MSTI)
    Id                              : ポートの ID 番号(16 進数表示)
    Role                            : ポート役割
      Root
      Designated
      Alternate
      Backup
    State                           : ポートステータス
      Discarding
      Learning
      Forwarding
      Disabled
    Configured Internal Path Cost   : ポートが接続したリンクの内部パスコスト
                                      (10 進数表示)
    External Path cost              : ポートが接続したリンクの外部パスコスト
                                      (10 進数表示)
    Designated Internal Path Cost   : 内部パスコスト
    Designated Port Id              : 接続した指定ポートの ID 番号
                                      (16 進数表示、自身が指定ポートの場合は自身の値)
    CST Priority                    : CST ポートプライオリティ(10 進数表示)
    MSTI Priority                   : MSTI ポートプライオリティ(10 進数表示)
    Designated Root                 : ルートブリッジのプライオリティと MAC アドレス
                                      (16 進数表示)
    Designated Bridge               : 指定ブリッジプライオリティと MAC アドレス
```

(16 進数表示、自身が指定ポートの場合は自身の値)

Message Age	：受信した BPDU の有効時間(10 進数表示)
Max Age	：BPDU の最大経過時間(10 進数表示)
Hello Time	：ハロー間隔(10 進数表示)
Forward Delay	：フォワードディレイ時間(10 進数表示)
MSTI Forward Timer	：MSTI フォワードタイマー(10 進数表示)
CIST Msg Age Timer	：CIST BPDU メッセージ有効タイマー(10 進数表示)
CIST Hello Timer	：CIST ハロータイマー(10 進数表示)
MSTI Remaining Hops	：MSTI BPDU 残り有効ホップ数

関連コマンド

注意事項

リンクアグリゲーションとスパニングツリープロトコル(MSTP)、及びポートリダンダントとスパニングツリープロトコル(MSTP)を同時に使用した場合、各グループ中最も番号の小さいポートのポート状態(port state)のみが変化し、他のポートは Discarding と表示されます。

RSTP と接続するポートの場合、受信プロトコルの表示は、BPDU 送信する度に未確定(None)となります。

3.17.31 show spanning-tree mst instance

MSTP に関する情報を表示します。指定したインスタンスの指定したポートに関する詳細情報を表示します。ポート番号を省略すると指定したインスタンスに関する全ポートの情報が表示されます。

コマンドシンタックス

show spanning-tree mst instance <INSTANCE_ID> [port <PORT>]

INSTANCE_ID	インスタンス ID <0-15>
PORT	ポート番号

コマンドモード

VIEW, ENABLE

使用例

(1) インスタンス ID：1 のポート：2 に関する MSTP 情報を表示します。

```
# show spanning-tree mst instance 1 port 2
% brg: Bridge up - Spanning Tree Enabled
% brg: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% brg: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% brg: CIST Root Id 8000004066119001
% brg: CIST Reg Root Id 8000004066119001
% brg: CST Bridge Id 8000004066119001
```

```
%
%   port2: Port 2 - Id 8002 - Role Designated - State Forwarding
%   port2: Configured Internal Path Cost 200000 -External Path cost 200000
%   port2: Designated Internal Path Cost 0  - Designated Port Id 8002
%   port2: CST Priority 128  - MSTI Priority 128
%   port2: Designated Root 8001004066119001
%   port2: Designated Bridge 8001004066119001
%   port2: Message Age 0 - Max Age 0
%   port2: Hello Time 2 - Forward Delay 15
%   port2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%
```

関連コマンド

注意事項

3.17.32 show spanning-tree mst port

MSTP に関する情報を表示します。指定したポートに関する詳細情報を表示します。

コマンドシンタックス

show spanning-tree mst port <PORT>

PORT　　ポート番号

コマンドモード

VIEW, ENABLE

使用例

(1) ポート：2 の MSTP 詳細情報を表示します。

```
# show spanning-tree mst port 2
% brg: Bridge up - Spanning Tree Enabled
% brg: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% brg: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% brg: CIST Root Id 8000004066119001
% brg: CIST Reg Root Id 8000004066119001
% brg: CST Bridge Id 8000004066119001
%
%   port2: Port 2 - Id 8002 - Role Designated - State Forwarding
%   port2: Designated External Path Cost 0 -Internal Path Cost 0
%   port2: Configured Path Cost 200000  - Add type Implicit ref count 2
(中略)
%   port2: Configured Link Type point-to-point - Current point-to-point
%
% Instance  1:  Vlans: 11
%   port2: Port 2 - Id 8002 - Role Designated - State Forwarding
```

```
%   port2: Configured Internal Path Cost 200000 -External Path cost 200000
(中略)
%   port2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%
% Instance  2:  Vlans: 21
%   port2: Port 2 - Id 8002 - Role Designated - State Forwarding
%   port2: Configured Internal Path Cost 200000 -External Path cost 200000
(以下略)
```

関連コマンド

注意事項

3.17.33 show tech-support spanning-tree

スパニングツリーの各種情報を収集し表示します。本コマンドで表示する内容は、表 3-14 に示すコマンドが収集している情報です。system-dump オプションを指定した場合、装置内部のダンプ情報(独自形式で表示)を含めて取得し表示します。

表 3-14 コマンドにより収集可能なスパニングツリー情報

show system
show version
show spanning-tree configuration
show spanning-tree port
show spanning-tree switch
show spanning-tree statistics
show spanning-tree rst
show spanning-tree mst config
show spanning-tree mst detail
show interface counters ※1

※1 1 秒おきに 3 回情報を取得

コマンドシンタックス

show tech-support spanning-tree [system-dump]

system-dump　　装置内部のダンプ情報を出力

コマンドモード

ENABLE

関連コマンド

注意事項

system-dump オプションを指定した場合、装置の性能、及び通信に対して影響を及ぼす可能性があります。使用する場合には、必ず事前にサポート対応窓口へご相談のう

え、指示に従ってください。

3.17.34 clear spanning-tree detected protocols

RSTP モード使用時、または MSTP モードの時に、検出したプロトコルをクリアして、検出を再度実施します。

コマンドシンタックス

clear spanning-tree detected protocols

デフォルト

プロトコル検出前のデフォルトは、バージョン 0 を認識

コマンドモード

ENABLE
(ただし、RSTP、または MSTP モードを指定時のみ実行可能)

使用例

(1) プロトコルの検出を再度実施します。

```
> enable
# clear spanning-tree detected protocols
```

関連コマンド

注意事項

3.18 BPDU 転送制限

3.18.1 bpdu-forward

スパニングツリープロトコル(STP/RSTP/MSTP)が稼動していない装置において、BPDU の転送を禁止します。設定を無効に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

[no] bpdu-forward disable

デフォルト

no disable(＝転送許可)

コマンドモード

CONFIG

使用例

(1) BPDU の転送を禁止します。

```
> enable
# configure terminal
(config)# bpdu-forward disable
```

関連コマンド

show bpdu-forward, show running-config

注意事項

3.17 スパニングツリープロトコル(STP/RSTP/MSTP)のいずれかを有効(3.17.2 "spanning-tree enable")にした場合、自動的に"bpdu-forward disable"が設定されます。また、スパニングツリープロトコル(STP/RSTP/MSTP)を無効にした場合、本設定は継続されるので、無効(転送許可)にする場合は、no コマンドを使用してください。

BPDU 転送制限機能無効時の BPDU はソフトウェア中継されます。ハードウェア中継ではありません。

3.18.2 show bpdu-forward

BPDU 転送制限機能の設定状態を表示します。

コマンドシンタックス

show bpdu-forward

コマンドモード

VIEW, ENABLE

使用例

(1) BPDU 転送制限機能の設定状態を表示します。

```
# show bpdu-forward
BPDU Forward state : Disabled
```

関連コマンド

注意事項

3.19 マルチキャストフィルタリング

マルチキャストフレームの中継を、宛先 MAC アドレス、または宛先 IP アドレスにより制限します。登録できるマルチキャストアドレスは最大 128 個です。登録したマルチキャスト MAC アドレスを持つフレームは設定したポートには中継されず、それ以外のポートには中継されます。また、未登録のマルチキャスト MAC アドレスを持つフレームは全ポートに中継されます。

IP アドレスを設定した場合、その IP アドレスは RFC 1112 の定義に従って、IP アドレスの下位 23 ビットを取り出し、上位に 01:00:5e を付けてマルチキャスト MAC アドレスを構成します。

3.19.1 multicast-filtering

マルチキャストのグループを作成します。作成したグループへ、対象ポートでフィルターするマルチキャストアドレス、及び VLAN を設定します。

コマンドシンタックス

```
[ no ] multicast-filtering <GROUP> state disable
multicast-filtering <GROUP> vid <VID> ip <IPADDR> <PORTRANGE>
multicast-filtering <GROUP> vid <VID> mac <MACADDR> <PORTRANGE>
no multicast-filtering [ <GROUP> vid ]
```

GROUP	マルチキャストグループ番号 <1-128>
VID	VLAN ID
IPADDR	マルチキャスト IP アドレス
MACADDR	マルチキャスト MAC アドレス
PORTRANGE	ポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) VLAN ID：10 のマルチキャスト MAC アドレス：01:00:10:00:00:01 宛てフレームをポート：1～10 に中継しないようにします。

(2) VLAN ID：10 のマルチキャスト IP アドレス：224.0.0.100 宛てフレームをポート：1～10 に中継しないようにします。

(3) マルチキャストフィルタに関する全設定をデフォルトに戻します。

```
> enable
# configure terminal
(config)# multicast-filtering 1 vid 10 mac 01:00:10:00:00:01 1-10
(config)# multicast-filtering 1 vid 10 ip 224.0.0.100 1-10
(config)# no multicast-filtering
```

関連コマンド

show multicast-filtering, show running-config

注意事項

マルチキャストフィルタリングと IGMP Snooping を同時に使用することはできません。用途に応じていずれかの機能を設定してください。

Apresia3400/4348/5400/13000 シリーズでは、以下に示す特定の MAC アドレス形式を指定した場合、フィルタリングは行われません。IP アドレス形式で指定してください。

表 3-15 マルチキャストフィルタリング設定時のアドレス形式

フィルタリング対象フレーム	MAC アドレス指定不可形式	IP アドレス指定形式
マルチキャストアドレス	01:00:5E:00:00:00～ 01:00:5E:7F:FF:FF	224.0.0.0～ 239.255.255.255

MAC アドレス指定形式のブロードキャストアドレス(ff:ff:ff:ff:ff:ff)は設定可能ですが、フィルタリングされません。

Apresia3400/4348/5400/13000 シリーズでは、マルチキャストフィルタリングは、IP ヘッダー内の宛先 IP アドレスを対象に行われます。

IP アドレス形式指定でのマルチキャストフィルタリングと umc(宛先不明マルチキャストフレーム)指定による Egress フィルタリングを併用時、マルチキャストフィルタリングにて指定されたグループについては、Egress フィルタリングの対象外となります。

LAG(リンクアグリゲーショングループ)のメンバーポートを指定する場合は、同一の LAG に所属するすべてのメンバーポートを指定してください。

3.19.2 show multicast-filtering

マルチキャストフレームに関する情報を表示します。

コマンドシンタックス

show multicast-filtering

コマンドモード

VIEW, ENABLE

使用例

(1) マルチキャストフレームに関する情報を表示します。

```
# show multicast-filtering
```

```
No VID   Multicast MAC Address (rfc1112 IP Address)  State
         Port
1  1     01:00:5e:00:00:01 (224.0.0.1)               Enabled
          1       8 9      16 17     24 25     32 33     40 41     48 49
          +------+ +------+ +------+ +------+ +------+ +------+ +-
          00000000 00...... ........ ........ ........ ........ ..
```

0　　：multicast-filtering 有効ポート

.　　：multicast-filtering 無効ポート

- 設定された宛先マルチキャストアドレスを持つフレームは、"."と表示されているポートからのみ出力

関連コマンド

注意事項

3.20 フラッディング制限

フラッディング制限機能は、フラッディングフレームの帯域を制限する機能です。

フラッディングフレームとは、ブロードキャスト(BC)、マルチキャスト(MC)、宛先不明ユニキャスト(DLF)のことです。

フラッディング制限は入力ポート単位での制限となります。

注意事項

フラッディング制限の対象ポートに、LAG(リンクアグリゲーショングループ)のメンバーポートを設定することはできません。

3.20.1 no flooding

フラッディング制限機能の設定をすべて削除します。

コマンドシンタックス

no flooding

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) フラッディング制限機能の設定を削除します。

```
# configure terminal
(config)# no flooding
```

関連コマンド

show flooding, show running-config

注意事項

3.20.2 flooding enable

フラッディング制限をブロードキャスト、マルチキャスト、宛先不明の各フレームについて有効にします。各設定はポートごとで行います。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] flooding bc | mc | dlf port <PORTRANGE> enable

bc	ブロードキャストフレームの制限
mc	マルチキャストフレームの制限
dlf	宛先不明フレームの制限

PORTRANGE　　ポート番号(複数指定可能)

デフォルト

no enable(＝フラッディング制限無効)

コマンドモード

CONFIG

使用例

(1) ポート：1で受信したブロードキャストフレームを制限します。
(2) ポート：1のフラッディングフレーム制限値を1000 frames/secに設定します。

```
> enable
# configure terminal
(config)# flooding bc port 1 enable
(config)# flooding limit port 1 1000
```

関連コマンド

show flooding, show running-config

注意事項

3.20.3 flooding limit

フラッディングフレームの制限値を1秒間のフレーム数で設定します。各設定はポートごとで行います。

コマンドシンタックス

flooding limit port <PORTRANGE> <FRAMECOUNT>
no flooding limit port <PORTRANGE>

PORTRANGE　　ポート番号(複数指定可能)
FRAMECOUNT　　1秒当たりに中継するフラッディングフレーム数
　　<0-14880952(frames/sec)>

デフォルト

14880952(frames/sec)

コマンドモード

CONFIG

使用例

(1) ポート：1で受信したブロードキャストフレームを制限します。
(2) ポート：1のフラッディングフレーム制限値を1000 frames/secに設定します。

```
> enable
# configure terminal
(config)# flooding bc port 1 enable
```

```
(config)# flooding limit port 1 1000
```

関連コマンド

show flooding, show running-config

注意事項

3.20.4 show flooding

フラッディング制限機能の設定を表示します。

コマンドシンタックス

show flooding

コマンドモード

VIEW, ENABLE

使用例

(1) フラッディング制限機能の設定を表示します。

```
# show flooding
port   BC   MC   DLF  limit(frames/sec)
    1  OFF  OFF  OFF  14880952
    2  OFF  OFF  OFF  14880952
    3  OFF  OFF  OFF  14880952
    4  OFF  OFF  OFF  14880952
    5  OFF  OFF  OFF  14880952
```

port　　：ポート番号
BC　　：ブロードキャストフレームの制限
MC　　：マルチキャストフレームの制限
DLF　　：宛先不明フレームの制限
limit　　：1秒当たりに中継するフラッディングフレーム数

関連コマンド

注意事項

3.21 フラッディング制御

ブロードキャストフレーム、またはマルチキャストフレームのトラフィックを監視し、閾値を上回るか下回る変化を検出した場合にログの記録、トラップの送信、フラッディング制限、またはポートの閉塞(3.7.1 "shutdown")を動的に行います。

フラッディング制限、もしくはポート閉塞の動作モードの選択はコマンドにより装置単位で行います。

フラッディング制御機能では、フラッディング制御を開始/終了(注)する 1 秒当たりのフレーム数(frames/sec：PPS)を閾値として設定することにより以下の動作を行います。

- フラッディング制御の開始、または終了(注)を示すログの記録
- フラッディング制御の開始、または終了(注)を示すトラップの送信
- フラッディング制限を実行する(3.20.2 "flooding enable")コマンドの発行、またはポートの閉塞を実行する("shutdown")コマンドの発行
  (注)：ポート閉塞モードの場合は開始の動作のみになります。

"flooding enable"コマンドの発行を実際に効力のあるものとするためには、あらかじめ 3.20.3 "flooding limit"コマンドでフラッディング制限の値を設定しておく必要があります。また、上記アクションで発行された"flooding enable"コマンドは、CLI からのユーザー入力と同等であり、ユーザー入力による"flooding enable"の設定を上書きします(running-config に反映されます)。

注意事項

フラッディング制御が動作している状態で、3.50.2 "write memory"("copy running-config flash-config"を含む)を行うと発行された"flooding enable"コマンドが flash-config に反映されます。

フラッディング制御が動作している状態で、"no flooding control enable"(フラッディング制御機能を無効)を行うと発行された"flooding enable"コマンドの設定は残ったままとなります。

フラッディング制御機能を、スパニングツリーのブロッキング状態のポート、MMRP-Plus の Blocking ポートで動作させた場合、ブロッキング状態のポート、または VLAN に対してもフラッディング制御が動作します。

3.21.1 no flooding control

フラッディング制御機能の設定をすべて削除します。

コマンドシンタックス

no flooding control

デフォルト

なし

コマンドモード
CONFIG

使用例
(1) フラッディング制御機能の設定を削除します。

```
# configure terminal
(config)# no flooding control
```

関連コマンド
show flooding control, show running-config

注意事項

3.21.2 flooding control action

フラッディング制御機能により閾値を跨いだ際にフラッディング制限を行うか、ポートの閉塞("shutdown")を行うかの動作モードを選択します。フラッディング制限モードでは"flooding control pps-hi"、"flooding control pps-low"の設定が、ポート閉塞モードでは"flooding control shutdown pps-hi"の設定が必要です。

コマンドシンタックス
flooding control action limit | shutdown
no flooding control action

limit	フラッディング制限モード
shutdown	ポート閉塞モード

デフォルト
limit

コマンドモード
CONFIG

使用例
(1) フラッディング制限モードを選択します。
(2) ポート閉塞モードを選択します。
(3) 設定をデフォルト値(フラッディング制限モード)に戻します。

```
# configure terminal
(config)# flooding control action limit
(config)# flooding control action shutdown
(config)# no flooding control action
```

関連コマンド
show flooding control, show running-config

注意事項

本設定を変更した場合、フラッディング制御機能の他の設定が削除されるため、再設定の必要があります。

フラッディング制御機能("flooding control enable")が有効の場合は、本設定を変更することはできません。

3.21.3 flooding control enable

フラッディング制御機能を有効にします。

コマンドシンタックス

[no] flooding control enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

ポート：1でのブロードキャストパケットが200 ppsを超えた際に、フラッディング制限を100 ppsで開始し、20 ppsを下回るとフラッディング制限を解除します。

(1) 本機能で動的に制御されるフラッディング制限の対象ポートと制限値を設定します。
(2) フラッディング制御開始の閾値を設定します。
(3) フラッディング制御終了の閾値を設定します。
(4) フラッディング制御機能を有効にします。

```
# configure terminal
(config)# flooding limit port 1 100
(config)# flooding control bc port 1 pps-hi 200
(config)# flooding control bc port 1 pps-low 20
(config)# flooding control enable
```

関連コマンド

show flooding control, show running-config

注意事項

一定量の対象フレーム検出後、フラッディング制御を開始するまで1～数秒かかります。また、開始までの時間は、設定や使用条件によって変動します。

3.21.4 flooding control pps-hi

フラッディング制御を開始する1秒当たりのフレーム数を閾値として設定します。指定はポートごと

に行います。指定したポートのうち１ポート以上で、ブロードキャストフレーム、またはマルチキャストフレームの受信量が設定した値を上回ると、フラッディング制御が開始します。

コマンドシンタックス

```
flooding control bc | mc port <PORTRANGE> pps-hi <PPS_HI>
no flooding control bc | mc [ port <PORTRANGE> [ pps-hi ] ]
```

bc	ブロードキャストフレーム
mc	マルチキャストフレーム
PORTRANGE	監視するポート番号(複数指定可能)
PPS_HI	１秒当たりのフレーム数 <1-4294967295(frames/sec：pps)>

デフォルト

4294967295(pps)

コマンドモード

CONFIG

使用例

(1) ポート：5 の pps-hi の値を、10000 pps に設定します。

```
# configure terminal
(config)# flooding control bc port 5 pps-hi 10000
```

関連コマンド

show flooding control, show running-config

注意事項

pps-hi ≦ pps-low となる値は設定できません。

"flooding control action"で動作モードに shutdown を選択した場合、本設定はできません。

3.21.5 flooding control pps-low

pps-hi を超えたフレーム数を検出してフラッディング制御が開始された後、フラッディング制御を終了するフレーム数を閾値として設定します。指定したすべてのポートで、ブロードキャストフレーム、またはマルチキャストフレームの受信量がこの値を下回ると、フラッディング制御を終了します。

コマンドシンタックス

```
flooding control bc | mc port <PORTRANGE> pps-low <PPS_LOW>
no flooding control bc | mc [ port <PORTRANGE> [ pps-low ] ]
```

bc	ブロードキャストフレーム
mc	マルチキャストフレーム
PORTRANGE	監視するポート番号(複数指定可能)
PPS_LOW	１秒当たりのフレーム数 <0-4294967294(frames/sec：pps)>

デフォルト
0(pps)

コマンドモード
CONFIG

使用例
(1) ポート：5 の pps-low の値を、5000 pps に設定します。

```
# configure terminal
(config)# flooding control bc port 5 pps-low 5000
```

関連コマンド
show flooding control, show running-config

注意事項

pps-hi ≦ pps-low となる値は設定できません。

"flooding control action"で動作モードに shutdown を選択した場合、本設定はできません。

3.21.6 flooding control shutdown pps-hi

フラッディング制御を開始する 1 秒当たりのフレーム数を閾値として設定します。指定はポートごとに行います。指定したポートで、ブロードキャストフレーム、またはマルチキャストフレームの受信量が設定値を上回ると、ポートの閉塞("shutdown")を行います。

コマンドシンタックス
flooding control shutdown bc | mc port <PORTRANGE> pps-hi <PPS_HI>
no flooding control shutdown [bc | mc [port <PORTRANGE>]]

bc	ブロードキャストフレーム
mc	マルチキャストフレーム
PORTRANGE	監視するポート番号(複数指定可能)
PPS_HI	1 秒当たりのフレーム数 <1-4294967295(frames/sec：pps)>

デフォルト
4294967295(pps)

コマンドモード
CONFIG

使用例
(1) ポート：5 の pps-hi の値を、10000 pps に設定します。

```
# configure terminal
```

```
(config)# flooding control shutdown bc port 5 pps-hi 10000
```

関連コマンド

show flooding control, show running-config

注意事項

"flooding control action"で動作モードに shutdown を選択した場合のみ、設定が可能です。

3.21.7 flooding control interval

フラッディング制御のためにフレーム数を監視する時間を設定します。監視するインターバルを大きくすることにより、事象発生からフラッディング制御を開始するまでの時間が長くなりますが、フラッディング制御による監視のため生じる定常的な CPU 負荷を軽減する効果があります。

コマンドシンタックス

flooding control interval <INTERVAL>
no flooding control interval
　　INTERVAL　　フレーム数を監視する単位時間 <1-15(秒)>

デフォルト

1(秒)

コマンドモード

CONFIG

使用例

(1) インターバルの値を 5 秒に設定します。

```
# configure terminal
(config)# flooding control interval 5
```

関連コマンド

show flooding control, show running-config

注意事項

3.21.8 show flooding control

フラッディング制御の設定内容を表示します。オプションを指定することによりブロードキャストフレーム、マルチキャストフレームごとに表示することが可能です。

コマンドシンタックス

show flooding control [bc | mc]
　　bc　　ブロードキャストフレーム

mc　　マルチキャストフレーム

コマンドモード

VIEW, ENABLE

使用例

(1) フラッディング制御の設定内容を表示します(フラッディング制限モード時)。

```
# show flooding control
Flooding Control action: limit
Flooding Control state : Enabled
Polling interval time  : 1

Multicast configuration :
port   State    pps-hi      pps-low
-------------------------------------
   1   Normal   4294967295  0
   2   Normal   4294967295  0
   3   Normal   4294967295  0
   4   Normal   4294967295  0
   5   Normal   4294967295  0
              .
              .
              .

Broadcast configuration :
port   State    pps-hi      pps-low
-------------------------------------
   1   Normal   4294967295  0
   2   Normal   4294967295  0
   3   Normal   4294967295  0
   4   Normal   4294967295  0
   5   Normal   4294967295  0
              .
              .
              .
```

port　　：ポート番号

State　　：フラッディング制御の動作状態

Normal　　：フラッディング制御機能有効、かつ閾値(pps-hi)を上回っていない状態(フラッディング制御非動作)

Act　　：フラッディング制御機能有効、かつ閾値(pps-low)を下回っていない状態(フラッディング制御動作中)

Disable　　：フラッディング制御機能無効状態

pps-hi　　：フラッディング制御を開始する１秒当たりのフレーム数

pps-low　　：フラッディング制御が開始された後、フラッディング制御を終了する１秒当たりのフレーム数

(2) フラッディング制御の設定内容を表示します(閉塞モード時)。

```
# show flooding control
Flooding Control action: shutdown
Flooding Control state : Enabled
Polling interval time  : 1

Port   BCThreshold  MCThreshold
--------------------------------
   1   4294967295   4294967295
   2   4294967295   4294967295
   3   4294967295   4294967295
   4   4294967295   4294967295
              ・
              ・
              ・
```

Port　　：ポート番号
BCThreshold　　：ブロードキャストフレームの閾値
MCThreshold　　：マルチキャストフレームの閾値

関連コマンド

注意事項

3.21.9 show flooding control port

フラッディング制御の設定内容をフレーム種別ごと、ポートごとに表示します。

コマンドシンタックス

show flooding control bc | mc port <PORTRANGE>

bc　　ブロードキャストフレーム
mc　　マルチキャストフレーム
PORTRANGE　　ポート番号(複数指定可能)

コマンドモード

VIEW, ENABLE

使用例

(1) 動作モードが limit の場合
(2) 動作モードが shutdown の場合

```
# show flooding control bc port 1
Flooding Control action : limit
Flooding Control state : Enabled
Polling interval time  : 1

Broadcast configuration :
```

```
port   State    pps-hi      pps-low
-------------------------------------
   1   Normal   4294967295  0


# show flooding control bc port 1
Flooding Control action : shutdown
Flooding Control state : Disabled
Polling interval time  : 1

Port   BCThreshold
-------------------
   1   4294967295
```

関連コマンド

注意事項

3.22 Ingress フィルタ

Ingress フィルタは、受信するフレームの VLAN ID と受信ポートの VLAN ID が異なる場合に、フレーム中継を制限(破棄)する機能です(デフォルト状態で動作)。

3.22.1 ingress-filter disable

Ingress フィルタ機能を無効にします。有効にする場合は、no コマンドを使用してください。

Ingress フィルタ機能を無効にしたポートは、受信ポートと異なる VLAN ID を持つフレームの中継が可能となります。本機能は IEEE 802.1Q タグ付きフレームにのみ有効です。

コマンドシンタックス

[no] ingress-filter disable

デフォルト

no disable(＝VLAN ID が異なるフレームを制限(破棄))

コマンドモード

IF-PORT

使用例

(1) ポート：1～5 の ingress filter を無効にします。

(2) ポート：3 の ingress filter を有効にします。

```
> enable
# configure terminal
(config)# interface port 1-5
(config-if-port)# ingress-filter disable
(config-if-port)# exit
(config)# interface port 3
(config-if-port)# no ingress-filter disable
```

関連コマンド

show ingress-filter, show running-config

注意事項

3.22.2 show ingress-filter

ingress-filter の構成情報を表示します。

コマンドシンタックス

show ingress-filter

コマンドモード

VIEW, ENABLE

使用例

(1) ingress-filter の構成情報を表示します。

```
# show ingress-filter
0 : Enable  . : Disable
Port
1       8 9      16 17     24 25     32 33     40 41     48 49
+------+ +------+ +------+ +------+ +------+ +------+ +-
..0..000 00000000 00000000 00000000 00000000 00000000 00
```

0　　：ingress-filter 有効ポート

.　　：ingress-filter 無効ポート

関連コマンド

注意事項

3.23 Egress フィルタリング

Egress フィルタリングは、出力ポートごとにフレーム中継の制限(破棄)を行う機能です。対象となるフレームは次の 3 種類です。

(1) ブロードキャスト
(2) 宛先不明ユニキャスト
(3) 宛先不明マルチキャスト

注意事項

PIM-SM などにより(S,G)エントリーとして認識されたマルチキャストフレームは、宛先不明マルチキャスト(umc)では無いため、Egress フィルタリングの対象外となります。

3.23.1 egress-filtering

フレーム制限(破棄)を行う出力ポート、対象フレームを指定します。設定をデフォルトに戻す場合は、no コマンド使用してください。

umc オプション(宛先不明マルチキャストフレーム)では、3.36 IGMP Snooping、3.37 IGMP クエリア、3.39 MLD Snooping、PIM-SM、IGMP で登録されたマルチキャストグループアドレスは、フレーム制限(破棄)の対象外になります。

コマンドシンタックス

```
egress-filtering bc | umc | dlf port <PORTRANGE>
no egress-filtering [ bc | umc | dlf ]
```

bc	ブロードキャストフレーム
umc	宛先不明マルチキャストフレーム
dlf	宛先不明ユニキャストフレーム
PORTRANGE	フレームを制限する出力先ポート番号(複数指定可能)

デフォルト

なし(＝すべてのフレームを中継)

コマンドモード

CONFIG

使用例

(1) ポート：1～24 に宛先不明マルチキャストフレームを出力しないようにします。
(2) (1)の設定を削除します。
(3) Egress フィルタリングに関するすべての設定をデフォルトに戻します。

```
> enable
# configure terminal
(config)# egress-filtering umc port 1-24
(config)# no egress-filtering umc
(config)# no egress-filtering
```

関連コマンド

show egress-filtering, show running-config

注意事項

IP アドレス形式指定での 3.19 マルチキャストフィルタリングと umc オプション(宛先不明マルチキャストフレーム)指定による Egress フィルタリングを併用時、マルチキャストフィルタリングにて指定されたグループについては、Egress フィルタリングの対象外となります。

umc オプション(宛先不明マルチキャストフレーム)を設定すると、表 3-16 に示す予約マルチキャストアドレスも破棄されます。透過させた状態で IGMP Snooping、MLD Snooping にて未登録のマルチキャストフレームを破棄させたい場合は、"ip igmp snooping unregistered-filter"、"ipv6 mld snooping unregistered-filter"を使用してください。

表 3-16 破棄される予約マルチキャストアドレス

IPv4	224.0.0.0/24
IPv6	FF02::/111、FF02::1:FFXX:XXXX/104、FF05::/111

3.23.2 show egress-filtering

egress-filtering の設定状態を表示します。

コマンドシンタックス

show egress-filtering bc | umc | dlf

bc	ブロードキャストフレーム
umc	宛先不明マルチキャストフレーム
dlf	宛先不明ユニキャストフレーム

コマンドモード

VIEW, ENABLE

使用例

(1) egress-filtering の設定状態を表示します。

```
# show egress-filtering bc
Broadcast Egress Filtering
  e:egress filtering
      Port
      1       8 9      16 17     24 25     32 33     40 41     48 49
      +------+ +------+ +------+ +------+ +------+ +------+ +-
      eeeeeeee ee...... ........ ........ ........ ........ ..
```

```
# show egress-filtering umc
Unknown Multicast Egress Filtering
  e:egress filtering
      Port
      1       8 9      16 17     24 25     32 33     40 41     48 49
      +------+ +------+ +------+ +------+ +------+ +------+ +-
      ........ ........ ........ ........ ........ ........ ..

# show egress-filtering dlf
Unknown Destination Egress Filtering
  e:egress filtering
      Port
      1       8 9      16 17     24 25     32 33     40 41     48 49
      +------+ +------+ +------+ +------+ +------+ +------+ +-
      ........ ........ ........ ........ ........ ........ ..
```

e　　：受信した各フレームについて、"e"と表示されているポートからの出力を禁止

関連コマンド

注意事項

3.24 Egress シェーピング

注意事項

3.30 QoS 機能の WRR(Weighted Round Robin)/DRR(Deficit Round Robin)と Egress シェーピング機能の併用は Apresia3400/5400 シリーズのみ可能です。これ以外の機種では併用できません。

3.24.1 egress shape

指定したポートから送信されるフレームのトラフィック量を指定した値に制限します。各ポートの設定をデフォルトに戻す場合は、no コマンドを使用してください。<BURST_SIZE>の設定を省略した場合は、デフォルト値が設定されます。

コマンドシンタックス

egress-shape <RATE_LIMIT> [<BURST_SIZE>]
no egress-shape

RATE_LIMIT　制限するトラフィック量 <64～10000000(Kbps)>

BURST_SIZE　トラフィック量を測る際に使用するバーストサイズ <32-131072(Kbit)>

- 任意の数値を設定できるが、実際の動作時には表 3-17 で示す値に切り捨て(2^n Kbps 単位、n=5～17)

表 3-17 実際設定されるバーストサイズ

バーストサイズ設定値
32
64
128
256
512
1024
2048
4096
8192
16384
32768
65536
131072

デフォルト

バーストサイズ：128(Kbit)

コマンドモード

IF-PORT

使用例

(1) ポート：1～8 に Egress シェーピングを帯域制限値：5000 Kbps、バーストサイズ：100 Kbit に設定します。

```
> enable
# configure terminal
(config)# interface port 1-8
(config-if-port)# egress-shape 5000 100
```

関連コマンド

show egress-shape, show running-config

注意事項

ポートに対して帯域以上の<RATE_LIMIT>を超過した値に設定可能ですが、動作に影響はありません(ポートの帯域が適用されます)。

3.24.2 egress-shape count-mode include-ifg-pa

"egress shape"で対象とする中継フレームの帯域を InterFrame Gap(12 オクテット)と Preamble(8 オクテット)を含めた形式で算出します。設定を解除する場合は、no コマンドを使用してください。

コマンドシンタックス

egress-shape count-mode include-ifg-pa
no egress-shape count-mode

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) egress-shape count-mode include-ifg-pa を設定します。
(2) 設定を解除します。

```
> enable
# configure terminal
(config)# egress-shape count-mode include-ifg-pa
(config)# no egress-shape count-mode
```

関連コマンド

show egress-shape, show running-config

注意事項

3.24.3 show egress-shape

Egress シェーピングの設定状態を表示します。

コマンドシンタックス

show egress-shape

コマンドモード

VIEW, ENABLE

使用例

(1) ポート：1～8 の Egress シェーピングの設定状態を表示します(帯域制限値：5000 Kbps、バーストサイズ：1000 Kbit に設定した場合)。

```
# show egress-shape
 Port | Rate Limit(Kbps) | Burst Size(Kbit)
------+------------------+-----------------
    1 |           4992   |          512
    2 |           4992   |          512
    3 |           4992   |          512
    4 |           4992   |          512
    5 |           4992   |          512
    6 |           4992   |          512
    7 |           4992   |          512
    8 |           4992   |          512

count-mode: normal
```

Port　：送信ポート番号
Rate Limit(Kbps)　：帯域制限値(Kbps 単位)
Burst Size(Kbit)　：バーストサイズ(Kbit 単位)

関連コマンド

注意事項

3.25 中継パス制限

3.25.1 forwarding

指定したポートにおいて受信したフレームを、中継可能とするポートを設定します。設定をデフォルトに戻す場合は、no コマンド使用してください。

コマンドシンタックス

forwarding <PORTRANGE1> <PORTRANGE2>
no forwarding <PORTRANGE1>

PORTRANGE1	受信ポート(複数指定可能)
PORTRANGE2	中継ポート(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1 において受信したフレームをポート：1～18 に中継するように設定します。

```
> enable
# configure terminal
(config)# forwarding 1 1-18
```

関連コマンド

show forwarding, show running-config

注意事項

Apresia13000 シリーズ/4348 シリーズは LAG(リンクアグリゲーショングループ)のメンバーポートを受信ポートに設定できません。

3.25.2 forwarding enable

中継パス機能を有効に設定します。設定を無効にする場合は、no コマンド使用してください。

コマンドシンタックス

[no] forwarding enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) ポート：1 において受信したフレームをポート：1～18 に中継するように設定します。
(2) 中継パス機能を有効にします。
(3) 中継パス機能を無効にします。

```
> enable
# configure terminal
(config)# forwarding 1 1-18
(config)# forwarding enable
(config)# no forwarding enable
```

関連コマンド

show forwarding, show running-config

注意事項

3.25.3 show forwarding

中継パス機能の設定状態を表示します。

コマンドシンタックス

show forwarding

コマンドモード

VIEW, ENABLE

使用例

(1) 中継パス制限機能の設定状態を表示します。

```
# show forwarding
  Forwarding: Disabled
  f:forward  .:not forward
      Port
      1      8 9     16 17    24 25    32 33    40 41    48 49
Port  +------+ +------+ +------+ +------+ +------+ +------+ +-
  1   ........ ...f.... ........ ........ ........ ........ ..
  2   ........ ...f.... ........ ........ ........ ........ ..
  3   ........ ...f.... ........ ........ ........ ........ ..
  4   ........ ...f.... ........ ........ ........ ........ ..
  5   ........ ...f.... ........ ........ ........ ........ ..
  6   ........ ...f.... ........ ........ ........ ........ ..
  7   ........ ...f.... ........ ........ ........ ........ ..
  8   ........ ...f.... ........ ........ ........ ........ ..
  9   ........ ...f.... ........ ........ ........ ........ ..
 10   ........ ...f.... ........ ........ ........ ........ ..
 11   ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ff
(以下略)
```

f	：中継
.	：中継しない

関連コマンド

注意事項

3.26 ポートブリッジ

3.26.1 port-bridge enable

ポートブリッジを有効にします。無効にする場合は、no コマンドを使用してください。

ポートブリッジを有効にしたポートから入力されたフレームは、L2 中継の宛先ポートが入力ポートと同じ場合についても中継されます(入力ポートが宛先のユニキャストフレーム、フラッディングフレームなどを入力されたポートに対して折り返します)。

コマンドシンタックス

[no] port-bridge enable

デフォルト

no enable(＝無効)

コマンドモード

IF-PORT

使用例

(1) ポート：1 のポートブリッジを有効にします。

(2) ポート：1 のポートブリッジを無効にします。

```
> enable
# configure terminal
(config)# interface port 1
(config-if-port)# port-bridge enable
(config-if-port)# no port-bridge enable
```

関連コマンド

show port-bridge, show running-config

注意事項

本コマンドは Apresia4348 シリーズでのみ有効です。

3.26.2 show port-bridge

ポートブリッジの設定状態を表示します。

コマンドシンタックス

show port-bridge

コマンドモード

VIEW, ENABLE

使用例

(1) ポートブリッジの設定状態を表示します。

```
# show port-bridge
                x = Port Bridge Enable
                1     6 7    12 13   18 19   24 25   30 31   36 37   42 43   48
                +----+ +----+ +----+ +----+ +----+ +----+ +----+ +----+
Port Bridge     x..... ...... ...... ...... ...... ...... ...... ..x...
```

関連コマンド

注意事項

本コマンドは Apresia4348 シリーズでのみ有効です。

3.27 ポートセキュリティー

ポートセキュリティー設定では、ポートで接続可能な端末台数を、設定した台数に制限します。ポート単位で接続端末数量を 1～256 台まで設定可能です。

3.27.1 port-security enable

ポートセキュリティー機能を有効にし、動作を開始させます。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] port-security enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) ポートセキュリティー機能を開始します。
(2) ポートセキュリティー機能を停止します。

```
> enable
# configure terminal
(config)# port-security enable
(config)# no port-security enable
```

関連コマンド

show port-security, show running-config

注意事項

3.27.2 switchport port-security enable

ポートごとにポートセキュリティー機能を有効にし、動作を開始させます。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] switchport port-security enable

デフォルト

no enable(＝無効)

コマンドモード

IF-PORT

使用例

(1) ポート：1をポートセキュリティーの動作対象に設定します。

(2) ポート：2、4～6をポートセキュリティーの動作対象から外します。

```
> enable
# configure terminal
(config)# interface port 1
(config-if-port)# switchport port-security enable
(config-if-port)# exit
(config)# interface port 2,4-6
(config-if-port)# no switchport port-security enable
```

関連コマンド

show port-security, show running-config

注意事項

STP 管理対象となっているポートではポートセキュリティー機能は使用できません。本機能を設定する場合は、該当するポートを 3.17.3 "spanning-tree disable"コマンドで disable に設定してください。

ポートセキュリティーと 3.46 NA 機能を同一のポートで使用しないでください。同一のポートで使用した場合の動作は保証されません。

リンクアグリゲーション、ポートリダンダント、3.47 AccessDefender が設定されているポートではポートセキュリティー機能は使用できません。本機能を設定する場合は、該当するポートのリンクアグリゲーション、ポートリダンダント、AccessDefender の各設定を解除してください。

FDB にすでに対象端末の MAC アドレスが登録されている場合、ポートセキュリティーの対象になりません。すでに MAC アドレスが登録されている場合は 3.14.5 "clear mac-address-table"コマンドを使用して動的に学習した MAC アドレス削除してください。

3.27.3 switchport port-security aging-time

ポートごとにポートセキュリティーのエージング時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。値は 0(エージング OFF)、及び 30 から 86400 まで設定可能です。

コマンドシンタックス

switchport port-security aging-time <AGINGTIME>

no switchport port-security aging-time

AGINGTIME　　エージング時間 <0、30-86400(秒)>

デフォルト
300(秒)

コマンドモード
IF-PORT

使用例
(1) ポート：1のポートセキュリティーのエージング時間を600秒に設定します。
(2) ポート：1にポートセキュリティーのエージングOFFを設定します。
(3) ポート：1のポートセキュリティーのエージング時間をデフォルト値に戻します。

```
> enable
# configure terminal
(config)# interface port 1
(config-if-port)# switchport port-security aging-time 600
(config-if-port)# switchport port-security aging-time 0
(config-if-port)# no switchport port-security aging-time
```

関連コマンド
show port-security, show running-config

注意事項

3.27.4 switchport port-security maximum

ポートごとに接続可能な端末台数を設定します。設定をデフォルト値に戻す場合は、noコマンドを使用してください。

コマンドシンタックス
switchport port-security maximum <MAXIMUM_NUMBER>
no switchport port-security maximum
MAXIMUM_NUMBER　接続可能な端末台数 <1-256(台)>

デフォルト
1(台)

コマンドモード
IF-PORT

使用例
(1) ポート：1に接続可能な端末台数を5台に設定します。
(2) ポート：1に接続可能な端末台数をデフォルト値に戻します。

```
> enable
# configure terminal
(config)# interface port 1
```

```
(config-if-port)# switchport port-security maximum 5
(config-if-port)# no switchport port-security maximum
```

関連コマンド

show port-security, show running-config

注意事項

接続可能な端末台数には、3.14.1 "mac-address-table static"コマンドで設定するFDB のスタティックエントリーを含みません。

3.27.5 port-security delete port

指定されたポートのすべての登録端末を削除します。

コマンドシンタックス

port-security delete port <PORTRANGE>

PORTRANGE　　ポート番号(複数指定可能)

デフォルト

なし

コマンドモード

CONFIG

使用例

(1) ポート：1 に登録されている端末をすべて削除します。

(2) ポート：2、4～6 に登録されている端末をすべて削除します。

```
> enable
# configure terminal
(config)# port-security delete port 1
(config)# port-security delete port 2,4-6
```

関連コマンド

show port-security

注意事項

3.27.6 port-security delete mac

登録端末から指定された MAC アドレスの端末を削除します。

コマンドシンタックス

port-security delete mac <MACADDR>

MACADDR　　MAC アドレス

デフォルト
なし

コマンドモード
CONFIG

使用例
(1) 登録端末から MAC アドレス：00:08:0c:13:9d:e6 を削除します。

```
> enable
# configure terminal
(config)# port-security delete mac 00:08:0c:13:9d:e6
```

関連コマンド
show port-security

注意事項

3.27.7 show port-security

ポートセキュリティー機能の動作状態が表示されます。

コマンドシンタックス
show port-security [<PORTRANGE>]
PORTRANGE　　ポート番号(複数指定可能)

コマンドモード
VIEW, ENABLE

使用例
(1) ポートセキュリティー機能の動作状態が表示されます。

```
# show port-security
Port Security state : Enabled

Port configuration :
 Pt.  State     Max            Aging-Time
  1   Enabled   256            86400
  2   Enabled   5              1000
  3   Enabled   10             5000
  (省略)
 50   Disabled  1              300
#
# show port-security 1
Port configuration :
 Pt.  State     Max            Aging-Time
```

```
-----------------------------------------
  1   Enabled   256            86400

Port Status :
 Pt.  Learn  MAC address        Link Time
-------------------------------------------------------
  1   0      --:--:--:--:--:--
#
```

State　　：ポートセキュリティー動作ポート状態
Max　　：接続可能端末台数
Aging-Time　　：ポートセキュリティーのエージング時間
Port status　　：ポートの状態
Learn　　：接続端末数
MAC address　　：学習した端末の MAC アドレス
Link Time　　：端末が接続された時間

関連コマンド

注意事項

3.28 パケットフィルター2

パケットフィルター2では、受信フレームに対する識別条件(アサイン)、フィルター条件(コンディション)を満たしたフレームに対して行う動作(アクション)を設定します。保証帯域を超過したフレームに対して行う動作にはEXCEEDEDアクション("exceeded-action"項参照)を設定します。

識別条件によって、装置の受信フレームからフィルター対象フレームを識別し、フィルター対象フレームとフィルター条件を比較し、フィルター条件を満たしたフレームに対して処理を行います。帯域制限を設定した場合は、フィルター条件を満たしたフレームが使用する帯域を計測し、帯域制限を満たしたフレームと帯域制限を満たさないフレームの、それぞれに対して処理を行います。

注意事項

パケットフィルター2とアクセスリストは動作が異なりますのでご注意ください。パケットフィルター2はハードウェアによる中継フレームの制限、アクセスリストはソフトウェアによるルーティング情報の制限を行います。

管理ポートの受信フレームはフィルタリングできません。

ルールを有効にするためには、必ず識別条件("assign")の設定が必要です。

ポートリダンダントグループのメンバーポートに対して、パケットフィルター2の設定は使用しないでください。同一のポートで使用した場合の動作は保証されません。

識別条件だけを設定してフィルター条件を設定しない場合、グループの対象フレームのトラフィックがアクション対象になります。

ダブルタグ付きフレームをパケットフィルター2の対象とする場合、以下の両方を満たす必要があります。

- **受信ポートをトランクポートに設定(3.11.4 "switchport mode"項参照)**
- **3.11.9 "ignore-tag enable"コマンドを設定**

3.47 AccessDefender機能併用時に、AccessDefender機能で使用しているグループ番号よりも小さいグループ番号でパケットフィルター2機能を設定する場合、DHCPパケットや未認証端末からのパケットが、action permitによって意図せず中継されないように、次のどちらかの設定を行ってください。

- **DHCP パケット、または未認証端末からのパケットをフィルター対象外となるようにconditionを設定する**
- **DHCP パケット、または未認証端末からのパケットに対して action none を設定する**

3.29 ユーザーループ検知機能、3.41 MMRP機能、3.42 MMRP-Plus機能のいずれかと併用時に、各機能で使用しているグループ番号よりも小さいグループ番号でパケット

フィルター2 機能を設定する場合、以下に示す各制御フレームがフィルター対象とならないように設定してください。

- **ethertype 0x8820 のユーザーループ検知フレーム、MMRP 制御フレーム、MMRP-Plus 制御フレーム**

3.28.1 packet-filter2

PACKETFILTER2 モードへ移行します。PACKETFILTER2 モードにおいてパケットフィルター2 の設定を行います。PACKETFILTER2 モードから CONFIG モードへ移行する場合は exit コマンド、ENABLE モードへ移行する場合は end コマンドを使用してください。

no コマンドを使用すると、パケットフィルター2 の全設定を削除することができます。

コマンドシンタックス

[no] packet-filter2

デフォルト

なし

コマンドモード

CONFIG

使用例

(1) PACKETFILTER2 モードへ移行します。

(2) パケットフィルター2 の全設定を削除します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# exit
(config)# no packet-filter2
```

関連コマンド

show packet-filter2, show running-config

注意事項

3.28.2 state

ルールを無効に設定します。有効に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

[no] <GROUP> <RULE> state disable

GROUP　　グループ番号

- Apresia3400/4348/5400/13000 シリーズ：<1-14>
- Apresia4328 シリーズ：<1-7>

RULE　　ルール番号
- Apresia3400/4300/5400 シリーズ/13000-48X：<1-128>
- Apresia13000-24GX：<1-256>

デフォルト
no disable(＝有効)

コマンドモード
PACKETFILTER2

使用例
(1) グループ：1、ルール：1 のフィルターの状態を無効に設定します。
(2) グループ：1、ルール：1 のフィルターの状態を有効に設定します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 1 state disable
(config-filter)# no 1 1 state disable
```

関連コマンド
show packet-filter2, show running-config

注意事項

"action mirror <PORT>"が設定済みのルールを DISABLE 状態にした場合、指定<PORT>ではフレーム中継を行いません。

3.28.3 assign

受信フレームのフィルタリングを行うポート番号、もしくは VLAN を設定(アサイン)します。設定を削除する場合は、no コマンドを使用してください。no コマンドと共にポート番号を指定した場合、該当ポート番号の設定が削除されます。指定を省略した場合は、ルール、もしくはグループに設定されているすべてのポート番号が削除されます。

パケットフィルター2 を動作させるには、必ず本コマンドを設定してください。ポート番号を指定した場合は対象ポートでの受信フレーム、VLAN ID を指定した場合は対象 VLAN での受信フレームがフィルター対象となります。ポート番号と VLAN ID の双方を指定した場合、受信ポート番号と受信 VLAN ID が適合したフレームがフィルタリングされます。また、ルール番号を省略して設定を行った場合、該当するグループ全体でポート番号、もしくは VLAN が設定されます。

コマンドシンタックス
<GROUP> [<RULE>] assign (port <PORTRANGE>) | (vlan <VID> [mask <MASK>])
no <GROUP> [<RULE>] assign [port | vlan]

GROUP　　グループ番号
- Apresia3400/4348/5400/13000 シリーズ：<1-14>
- Apresia4328 シリーズ：<1-7>

RULE　　ルール番号
- Apresia3400/4300/5400 シリーズ/13000-48X：<1-128>
- Apresia13000-24GX：<1-256>

PORTRANGE　　ポート番号(複数指定可能)
VID　　VLAN ID
MASK　　VLAN ID に対するマスク(0x0-0xfff、「0x」は省略可)
- <MASK>省略時は 0xfff を自動設定

表 3-18 組み合わせの制限

組み合わせ	内容
<GROUP> assign port と <GROUP> <RULE> assign port	同一グループでは同時に設定不可
<GROUP> assign vlan と <GROUP> <RULE> assign vlan	

デフォルト
なし(＝設定なし)

コマンドモード
PACKETFILTER2

使用例
(1) グループ：1、ルール：1 のフィルターをポート：1～3 とポート：5 に割り当てます。
(2) グループ：1、ルール：1 のフィルターのポート割り当てを削除します。
(3) グループ：1、ルール：1 のフィルターを VLAN ID：1 に割り当てます。
(4) グループ：1、ルール：1 のフィルターの VLAN 割り当てを削除します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 1 assign port 1-3,5
(config-filter)# no 1 1 assign port
(config-filter)# 1 1 assign vlan 1
(config-filter)# no 1 1 assign vlan
```

関連コマンド
show packet-filter2, show packet-filter2 group brief, show running-config

注意事項

表 3-19 の各コマンドは、パケットフィルター2 のグループを使用するため、これらの機能設定がある場合、使用するグループが重複し、設定できない場合があります。その場合は、指定するグループ番号を変更し再度設定を行ってください。

表 3-19 パケットフィルター2 のグループを使用するコマンド

コマンド	グループ予約の条件	使用するグループ数
3.5.1 ip address	-	Apresia13000-24GX：0～4 Apresia3400/5400 シリーズ/4348：0～5 Apresia4328：0～6 Apresia13000-48X：0～9
3.15.1 flush-fdb rp-e port	-	1
3.15.2 flush-fdb rp-g port	-	1
3.29.2 loop-watch enable	-	1
3.41.3 mmrp enable	-	左記コマンドが一つでもあれば､以下のグループ数を使用する。 Apresia5412 シリーズ/13000-24GX：1 Apresia3424/4300 シリーズ/5428GT/13000-48X：1～2 Apresia3448 シリーズ：1～3 "mmrp group"コマンドでどのグループを予約するかの指定ができる。
3.42.5 mmrp-plus enable	-	左記コマンドが一つでもあれば､以下のグループ数を使用する。 Apresia5412 シリーズ/13000-24GX：1 Apresia3424/4300 シリーズ/5428GT/13000-48X：1～2 Apresia3448 シリーズ：1～3 複数ある場合も上記グループ数しか使用しない。 "mmrp-plus group"コマンドでどのグループを予約するかの指定ができる。
3.43.2 mmrp2 enable	-	左記コマンドが一つでもあれば､以下のグループ数を使用する。 Apresia13000-24GX：1 Apresia13000-48X：1～2 "mmrp2 group"コマンドでどのグループを予約するかの指定ができる。
3.46.9 na httpd ip	na enable、ユーザー認証ポート、na httpd ip の設定あり	1(Apresia13000-48X のみ) 左記コマンドはすべて､1 つのグループを共有して使用する。 左記コマンドで一番先にグループ予約の条件を満たした場合にグループを予約する。 左記すべてのコマンドを設定しても 1 つのグループしか使用しない。
3.46.10 na httpd port		
3.46.23 na logout ping ttl	na enable	
3.46.24 na logout ping dest-ip		
3.46.32 na dhcp-relay-port		
3.46.40 na auth-page redirect http	na enable、ユーザー認証ポートの設定あり	
3.46.40 na auth-page redirect https		
3.46.41 na auth-page redirect		

<table>
<tr><th>コマンド</th><th>グループ予約の条件</th><th>使用するグループ数</th></tr>
<tr><td>proxy-port</td><td></td><td></td></tr>
<tr><td>3.46.36 na custom-relay-port port</td><td>na enable、na custom-relay-port ip/tcp/udp のいずれかの設定あり</td><td rowspan="5">1(Apresia13000-48X のみ)
左記コマンドはすべて、1 つのグループを共有して使用する。
左記コマンドで一番先にグループ予約の条件を満たした場合にグループを予約する。
左記すべてのコマンドを設定しても 1 つのグループしか使用しない。</td></tr>
<tr><td>3.46.37 na custom-relay-port ip</td><td rowspan="3">na enable、na custom-relay-port port dual-mac-user-base 、 na auth-page redirect http/https /proxy-port</td></tr>
<tr><td>3.46.38 na custom-relay-port tcp</td></tr>
<tr><td>3.46.39 na custom-relay-port udp</td></tr>
<tr><td>3.46.42 na auth-page redirect vid</td><td>na enable、shared-dynamic-vlan モードのユーザー認証ポートの設定あり</td></tr>
<tr><td>3.46.30 na arp-relay-port</td><td>na enable</td><td>1(Apresia13000-48X のみ)</td></tr>
<tr><td>3.47.59 packet-filter2 max-rule</td><td>-</td><td>4～11 ※1</td></tr>
</table>

※1 AccessDefender 機能では、設定ルール(認証端末)数により使用グループ数が増減します。詳細は表 3-22 を参照ください。

表 3-20 各 IP アドレス最大設定数と使用するルール数

IP アドレス	最大設定数	IP アドレス 1 個につき使用するルール数
プライマリーIP アドレス	255	3
セカンダリーIP アドレス	Apresia13000 シリーズ：1000 Apresia3400/4300/5400 シリーズ：100	1
ループバック IP アドレス	14	1

表 3-21 IP アドレスで使用するルール数とグループ数

<table>
<tr><th rowspan="2">使用するグループ数</th><th colspan="5">使用ルール数</th></tr>
<tr><th>Apresia3400/5400 シリーズ</th><th>Apresia4328GT</th><th>Apresia4348 シリーズ</th><th>Apresia13000-24GX-PSR</th><th>Apresia13000-48X</th></tr>
<tr><td>0</td><td>251 以下</td><td>128 以下</td><td>256 以下</td><td>507 以下</td><td>256 以下</td></tr>
<tr><td>1</td><td>252-379</td><td>129-256</td><td>257-384</td><td>508-763</td><td>257-384</td></tr>
<tr><td>2</td><td>380-507</td><td>257-384</td><td>385-512</td><td>764-1019</td><td>385-512</td></tr>
<tr><td>3</td><td>508-635</td><td>385-512</td><td>513-640</td><td>1020-1275</td><td>513-640</td></tr>
<tr><td>4</td><td>636-763</td><td>513-640</td><td>641-768</td><td>1276-1531</td><td>641-768</td></tr>
<tr><td>5</td><td>764-891</td><td>641-768</td><td>769-896</td><td>1532-1787</td><td>769-896</td></tr>
<tr><td>6</td><td>-</td><td>769-896</td><td>-</td><td>-</td><td>897-1024</td></tr>
<tr><td>7</td><td>-</td><td>897-1024</td><td>-</td><td>-</td><td>1025-1152</td></tr>
<tr><td>8</td><td>-</td><td>-</td><td>-</td><td>-</td><td>1153-1280</td></tr>
<tr><td>9</td><td>-</td><td>-</td><td>-</td><td>-</td><td>1281-1408</td></tr>
</table>

表 3-22 AccessDefender で使用するルール数とグループ数

使用するグループ数	使用ルール数				
	Apresia3400/5400 シリーズ	Apresia4328GT	Apresia4348 シリーズ	Apresia13000-24GX-PSR	Apresia13000-48X
4	1-128	1-128	1-128	1-256	1-128
5	129-256	129-256	129-256	257-512	129-256
6	257-384	257-384	257-384	513-768	257-384
7	385-512	385-512	385-512	769-1024	385-512
8	513-640	-	513-640	1025-1280	513-640
9	641-768	-	641-768	1281-1536	641-768
10	769-896	-	769-896	1537-1792	769-896
11	897-1024	-	897-1024	1793-2048	897-1024
12	1025-1152	-	1025-1152	2049-2304	1025-1152
13	1153-1280	-	1153-1280	2305-2560	1153-1280
14	1281-1408	-	1281-1408	2561-2816	1281-1408

使用する総ルール数は、プライマリー/セカンダリー/ループバックの各 IP アドレス数に、各々対応するルール数を乗じ、これらの総和をとった値となります。
例：プライマリーIP アドレスを 100 個、セカンダリーIP アドレスを 500 個、ループバックアドレスを 1 個設定している場合、使用するルール数は 801 個、使用するグループ数は 5 個になります。

(ルール数の計算式)
100 * 3 + 500 * 1 + 1 * 1 = 801(個)

使用する総ルール数は、IP アドレスの設定数によっては、パケットフィルター2 のグループを別途使用する場合があります。表 3-21 を参照してください。
例：Apresia13000-48X で 801 個のルールを使う場合、表 3-21 の項目ルール数の 769～896 に該当するので、使用するグループ数は 5 個になります。

"show packet-filter2 reserved-group"により使用しているグループ数を確認できます。

3.36 IGMP/3.39 MLD 機能を併用した場合、両機能合わせて使用できるルール数は Apresia4328GT が 256 個、それ以外の機種では 1024 個となります。

表 3-23 MMRP、MMRP-Plus、MMRP2 のパケットフィルター2 利用グループと使用可能ポート数

パケットフィルター2 の利用グループ	Apresia3400/4300/5400/13000-48X 使用可能ポート数	Apresia13000-24GX 使用可能ポート数
1	25	28
2	50	-
3	52	-

MMRP として使用できるポート数が 25 の場合、以下のリング数をサポートすることが可能です。なお論理ポート(リンクアグリゲーション機能)も 1 つのポートとして認識します。

- **シングルマスター構成(マスタースイッチ)：12 リング**
- **分散マスター構成(マスタースイッチ)：25 リング**
- **MMRP アウェアスイッチ：12 リング**

本コマンドにて port 番号や VLAN といった識別条件のみ設定して、フィルター条件を設定しない場合は、グループの対象フレームのトラフィックがアクション対象になります。

同一グループ内の各ルールは若番から順にチェックされ、一致した場合はそれ以降のルールはチェックされません。

3.28.4 condition

フィルター条件(コンディション)を設定します。設定を削除するには、no コマンドを使用してください。no コマンドと共に特定のコンディションを指定した場合、該当コンディションのみが削除されます。コンディションの指定を省略した場合は、ルールに設定されているすべてのコンディションが削除されます。

コンディションは、宛先/送信元アドレス、ポート番号などフィルター対象フレームの該当する領域とのマッチングに使用されます。

コマンドシンタックス

<GROUP> <RULE> condition <*CONDITIONS*>
no <GROUP> <RULE> condition [<*CONDITIONS*>]

GROUP　グループ番号
- Apresia3400/4348/5400/13000 シリーズ：<1-14>
- Apresia4328 シリーズ：<1-7>

RULE　ルール番号
- Apresia3400/4300/5400 シリーズ/13000-48X：<1-128>
- Apresia13000-24GX：<1-256>

CONDITIONS　表 3-24 に示す condition を指定
- no コマンドを使用する場合、パラメーター範囲は指定不可

表 3-24 フィルター条件

condition		内容
dst	ip <IPADDR> | <IPADDR/NETMASK>	宛先 IPv4 アドレス • <NETMASK>入力省略時のマスクは自動設定
	mac <MACADDR> [mask <MASK>]	宛先 MAC アドレス • マスクの指定は MAC アドレス形式
	type <ETHERTYPE> [mask <MASK>]	Ether Type(16 進数設定) <0x0000-0xffff> • 0～0x5ff、0x8100、0x8808 はフィルターの対象とならないため、指定不可

condition		内容
	vid <VID> [mask <MASK>]	受信 VLAN の IEEE 802.1Q VID <1-4094>
src	ip <IPADDR> | <IPADDR/NETMASK>	送信元 IPv4 アドレス • <NETMASK>入力省略時のマスクは自動設定
	mac <MACADDR> [mask <MASK>]	送信元 MAC アドレス • マスクの指定は MAC アドレス形式
	type <ETHERTYPE> [mask <MASK>]	Ether Type(16 進数設定) <0x0000-0xffff> • 0～0x5ff、0x8100、0x8808 はフィルターの対象とならないため、指定不可
	vid <VID> [mask <MASK>]	受信 VLAN の IEEE 802.1Q VID <1-4094>
	arp-sender-ip <IPADDR> | <IPADDR/NETMASK>	ARP 送信元 IPv4 アドレス • <NETMASK>入力省略時のマスクは自動設定
ethernet	dst mac <MACADDR> [mask <MASK>]	宛先 MAC アドレス • マスクの指定は MAC アドレス形式
	src mac <MACADDR> [mask <MASK>]	送信元 MAC アドレス • マスクの指定は MAC アドレス形式
	type <ETHERTYPE> [mask <MASK>]	Ether Type(16 進数設定) <0x0000-0xffff> • 0～0x5ff、0x8100、0x8808 はフィルターの対象とならないため、指定不可
	vid <VID> [mask <MASK>]	受信 VLAN の IEEE 802.1Q VID <1-4094>
ipv4	dst ip <IPADDR> | <IPADDR/NETMASK>	宛先 IP アドレス • <NETMASK>入力省略時のマスクは自動設定
	dst tcp/udp <TCP/UDPPORT> [tcp | udp]	宛先 TCP/UDP ポート番号 <0-65535> • 範囲指定可 • tcp|udp オプションを使用することにより、特定のプロトコルのみを指定可能 • 範囲指定時は、異なる指定パターンにつき、range-id を 1 つ使用 ※range-id は装置全体で 16 個までです("show packet-filter2 tcp/udp-range"項参照)。 • tcp | udp オプションを使用せず、TCP、UDP ではない IP パケットを受信すると「TCP、UDP の宛先ポート番号に当たるデータ部分の 3～4byte 目」が設定した宛先 TCP/UDP ポート番号の 16 進数値と同じ場合フィルターの対象となる
	src ip <IPADDR> | <IPADDR/NETMASK>	送信元 IP アドレス • <NETMASK>入力省略時のマスクは自動設定
	src tcp/udp <TCP/UDPPORT> [tcp | udp]	送信元 TCP/UDP ポート番号 <0-65535> • 範囲指定可 • tcp|udp オプションを使用することにより、特定のプロトコルのみを指定可能 • 範囲指定時は、異なる指定パターンにつき、range-id を 1 つ使用

condition		内容
		※range-id は装置全体で 16 個までです("show packet-filter2 tcp/udp-range"項参照)。 • tcp | udp オプションを使用せず、TCP、UDP ではない IP パケットを受信すると「TCP、UDP の送信元ポート番号に当たるデータ部分の 1～2byte 目」が設定した送信元 TCP/UDP ポート番号の 16 進数値と同じ場合フィルターの対象となる
	tos <TOS> [mask <MASK>]	IPv4 ヘッダーの ToS フィールドの 1 オクテットを(16 進数設定) <0x00-0xff>
	tos-dscp <DSCP> [mask <MASK>]	IPv4 ヘッダーの DSCP 値 <0-63>
	tos-precedence <PRECEDENCE> [mask <MASK>]	IPv4 ヘッダーの Precedence 値 <0-7>
	protocol <PROTOCOL> [mask <MASK>]	IPv4 ヘッダーのプロトコル値 <0-255>
	tcp-flag fin | syn | rst | psh | ack | urg <FLAG>	TCP ヘッダーの各 Flag の値
ipv6	dst ip <IPv6ADDR/LENGTH>	宛先 IPv6 アドレス
	dst tcp/udp <TCP/UDPPORT> [tcp | udp]	宛先 TCP/UDP ポート番号 <0-65535> • 範囲指定可 • tcp | udp オプションを使用することにより、特定のプロトコルのみを指定可能 • "wide-mode"使用時のみ指定可能 • 範囲指定時は、異なる指定パターンにつき、range-id を 1 つ使用 ※range-id は装置全体で 16 個までです("show packet-filter2 tcp/udp-range"項参照)。 • tcp | udp オプションを使用せず、TCP、UDP ではない IP パケットを受信すると「TCP、UDP の宛先ポート番号に当たるデータ部分の 3～4byte 目」が設定した宛先 TCP/UDP ポート番号の 16 進数値と同じ場合フィルターの対象となる
	src ip <IPv6ADDR/LENGTH>	送信元 IPv6 アドレス
	src tcp/udp <TCP/UDPPORT> [tcp | udp]	送信元 TCP/UDP ポート番号 <0-65535> • 範囲指定可 • tcp | udp オプションを使用することにより、特定のプロトコルのみを指定可能 • "wide-mode"使用時のみ指定可能 • 範囲指定時は、異なる指定パターンにつき、range-id を 1 つ使用 ※range-id は装置全体で 16 個までです("show packet-filter2 tcp/udp-range"項参

condition		内容
		照)。 • tcp | udp オプションを使用せず、TCP、UDP ではない IP パケットを受信すると「TCP、UDP の送信元ポート番号に当たるデータ部分の 1～2byte 目」が設定した送信元 TCP/UDP ポート番号の 16 進数値と同じ場合フィルターの対象となる
	flow-label <FLOWLABEL> [mask <MASK>]	IPv6 ヘッダーの Flow Label 値 <0-1048575>
	hop-limit <HOPLIMIT> [mask <MASK>]	IPv6 ヘッダーの Hop Limit 値 <0-255>
	next-header <NEXTHEADER> [mask <MASK>]	IPv6 ヘッダーの Next Header 値 <0-255>
	traffic-class <TRAFFICCLASS> [mask <MASK>]	IPv6 ヘッダーの Traffic Class 値 <0-255>
	icmp type<TYPE> [mask <MASK>]	ICMPv6 ヘッダーの Type 値 <0-255> • "wide-mode"使用時のみ指定可能

デフォルト

なし(＝設定なし)

コマンドモード

PACKETFILTER2

使用例

(1) グループ:1、ルール:1 のフィルターに送信元 IP アドレス:172.15.51.0 の条件を追加します。
(2) グループ：4、ルール：1 のフィルターから送信元 MAC アドレスの条件を削除します。
(3) グループ：5、ルール：2 のすべてのフィルター条件を削除します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 1 condition src ip 172.17.51.0/24
(config-filter)# no 4 1 condition ethernet src mac
(config-filter)# no 5 2 condition
```

関連コマンド

show packet-filter2, show running-config

表 3-25 同一 condition-type での condition 組み合わせの制限

組み合わせ	内容
ipv4 protocol と ipv4 (src | dst) tcp/udp	グループ、ルールが同じ組み合わせでは、同時に設定不可
ipv4 (src | dst) tcp/udp tcp と ipv4 (src | dst) tcp/udp udp	
ipv4 protocol と tcp-flag	

組み合わせ	内容
tcp-flag と ipv4 (src | dst) tcp/udp [udp]	
src ip と src arp-sender-ip	
src type と src arp-sender-ip	
ipv6 (src | dst) tcp/udp tcp と ipv6 (src | dst) tcp/udp udp	
ipv6 next-header と ipv6 icmp type	

注意事項

グループで最初にコンディションを設定するとき、そのコンディションの属するコンディションタイプが自動的にグループのコンディションタイプとして設定されます。コンディションタイプごとに参照可能な領域が異なるため、異なるコンディションタイプに属するコンディションを同一グループ内に設定することはできません。デフォルトでは、グループにコンディションタイプは設定されていません。
dst tcp/udp(宛先 TCP/UDP ポート番号)、src tcp/udp(送信元 TCP/UDP ポート番号)を複数ポートで指定した場合は、condition-type が ipv4 から、ipv4-dst-tcp/udp-range、ipv4-src-tcp/udp-range に自動的に変更されます。

表 3-26 condition-type

condition-type	condition
dst	dst ip, dst mac, dst type, dst vid
src	src ip, src mac, src type, src vid, src arp-sender-ip
ethernet	ethernet dst, ethernet src, ethernet type, ethernet vid
ipv4	ipv4 dst ip, ipv4 dst tcp/udp (1), ipv4 src ip, ipv4 src tcp/udp (1), ipv4 tos, ipv4 tos-dscp, ipv4 tos-precedence, ipv4 protocol, ipv4 tcp-flag
ipv4-dst-tcp/udp-range	ipv4 dst ip, ipv4 dst tcp/udp (2), ipv4 src ip, ipv4 src tcp/udp (1), ipv4 tos, ipv4 tos-dscp, ipv4 tos-precedence, ipv4 protocol, ipv4 tcp-flag
ipv4-src-tcp/udp-range	ipv4 dst ip, ipv4 dst tcp/udp (1), ipv4 src ip, ipv4 src tcp/udp (2), ipv4 tos, ipv4 tos-dscp, ipv4 tos-precedence, ipv4 protocol, ipv4 tcp-flag
ipv6	ipv6 dst ip (3), ipv6 src ip (3)
ipv6-header	ipv6 flow-label, ipv6 hop-limit, ipv6 next-header, ipv6 traffic-class, icmp-type
ipv6-dst-ip	ipv6 dst ip (4)
ipv6-src-ip	ipv6 src ip (4)
ipv6-tcp/udp-range	ipv6 dst ip (5), ipv6 src ip (5), ipv6 dst tcp/udp, ipv6 src tcp/udp

(1) 単一の TCP/UDP ポート番号を指定する場合
(2) 複数の TCP/UDP ポート番号を指定する場合
(3) wide-mode を設定している場合

(4) wide-mode を設定していない場合
(5) ipv6 dst tcp/udp、または ipv6 dst tcp/udp と同一グループ内に設定する場合

<NETMASK>の指定を省略した場合は、<IPADDR>をクラスフルのアドレスとみなし、ホスト部がすべて 0 の場合はクラスに応じたマスク長、それ以外の場合は 32 がマスク長として自動で設定されます。
mask <MASK>オプションを使用したマスクの指定では、2 進数表記で 0 となるビットがマスキングされます。マスクの指定を省略した場合は、全ビットが 1 のマスクが自動で設定されます。

各フィルター条件設定の対象となるフレームは以下の通りです。

condition-type	condition	対象フレーム
ethernet	type	ethernet II
dst	type	
src	type	
ipv4, ipv4-dst-tcp/udp-range, ipv4-src-tcp/udp-range	ipv4 dst ip, ipv4 src ip, ipv4 tos, ipv4 tos-dscp, ipv4 tos-precedence, ipv4 protocol, ipv4 dst tcp/udp, ipv4 src tcp/udp, ipv4 tcp-flag	ethernet II(type = 0x800)
dst	ip	
src	ip	
ipv6-tcp/udp-range	ipv6 dst tcp/udp, ipv6 src tcp/udp	ethernet II(type = 0x86dd)
ipv6-header	ipv6 flow-label, ipv6 hop-limit, ipv6 next-header, ipv6 traffic-class, ipv6 icmp type	
ipv6, ipv6-dst-ip, ipv6-tcp/udp-range	ipv6 dst ip	
ipv6, ipv6-src-ip, ipv6-tcp/udp-range	ipv6 src ip	
src	arp-sender-ip	Ethernet II(type = 0x0806)

コンディションタイプが以下のグループの場合、コンディション未設定のルールでは、イーサネットタイプが 0x0800 以外のフレームをフィルターできません。

- **ipv4**
- **ipv4-dst-tcp/udp-range**
- **ipv4-src-tcp/udp-range**

コンディションタイプが以下のグループの場合、コンディション未設定のルールでは、イーサネットタイプが 0x86dd 以外のフレームをフィルターできません。

- **ipv6**
- **ipv6-header**
- **ipv6-dst-ip**
- **ipv6-src-ip**
- **ipv6-tcp/udp-range**

表 3-19 の機能設定がある場合、使用するグループが重複し、設定できない場合があります。その場合は、指定するグループ番号を変更し再度設定を行ってください。

condition の dst vid に関しては src vid と同じく「受信 VLAN ID」の指定となります。送信先の VLAN ID は指定できませんのでご注意ください。

3.28.5 action

ルールにアクションを設定します。設定したアクションを削除する場合は、no コマンドを使用してください。特定のアクションを指定した場合は、該当アクションのみ削除されます。アクションの指定を省略した場合は、ルールに設定されているすべてのアクションが削除されます。

アクションは、ルールに設定されているフィルター条件(コンディション)を満たすフレームに対して適用される処理です。ポリシング(ポリシング)を設定した場合、保証帯域を超過したフレームには EXCEEDED アクション("exceeded-action"項参照)が適用されます。

コマンドシンタックス

<GROUP> <RULE> action <*ACTIONS*>

no <GROUP> <RULE> action [<*ACTIONS*>]

GROUP	グループ番号 • Apresia3400/4348/5400/13000 シリーズ：<1-14> • Apresia4328 シリーズ：<1-7>
RULE	ルール番号 • Apresia3400/4300/5400 シリーズ/13000-48X：<1-128> • Apresia13000-24GX：<1-256>
ACTIONS	表 3-27 に示す処理方法を指定 • no コマンドを使用する場合、パラメーター範囲は指定不可

表 3-27 フレームの処理方法(アクション)

処理方法	内容
permit	フレームの中継を許可する • ルールのデフォルトアクション

処理方法	内容
	• deny、none、authentication-bypass 以外のアクションや、assign、condition、exceeded-action コマンドにより、ルールを新規作成する場合には、permit を自動設定 ※ AccessDefender の認証ポートにおいて、未認証端末からのフレームを中継する場合は、authentication-bypass を指定してください。
deny	フレームの中継を拒否する • 同一ルールに permit、none の同時設定は不可 • 同一ルールに対する authentication-bypass の設定は未サポート
none	対象フレームの中継動作に、permit、deny の影響を与えないようにする • 同一グループにおいて、none を設定しているルールの番号が、permit、deny が設定されているルールよりも若い場合に、none アクションが有効 • 同一ルールに permit、deny の同時設定は不可 • 同一ルールに対する authentication-bypass の設定は未サポート • block-cpu-control で指定したグループでは、action コマンドや、assign、condition コマンドにより、ルールを新規作成する場合には、none を自動設定 • 別グループで permit、deny、authentication-bypass が設定されている場合、別グループの permit、deny、authentication-bypass アクションが有効
authentication-bypass	認証バイパス(AccessDefender 認証ポートにおいて、未認証端末からのフレームを中継する) • 同一ルールに permit の同時設定は不可 • 同一ルールに対する、deny、none の設定は未サポート
block-cpu-control	対象フレームが CPU に転送されることを抑止する • 通常の転送フレームに対しては、none を適用 • block-cpu-control で指定したグループでのみ設定可能 • Apresia4348 シリーズ/Apresia13000-48X には設定不可
counter <INDEX>	対象となるフレームのフレーム数、またはバイト数をカウントする • <INDEX>は使用する index • カウンターはグループごとに複数個(注)用意されているため、複数ルールで個別にカウンターを使用することや、同じカウンターを複数ルール(グループ内)で共有することが可能 (注)：1 グループあたりの index 数 • Apresia3400/4300/5400 シリーズ/13000-48X：<1-64> • Apresia13000-24GX：<1-128>
counter unit byte	カウンターのカウント単位をバイト単位に変更する
qos <QOSPROFILE>	<QOSPROFILE>で指定した QoS プロファイルに従い、優先制御を行う <qp1 | qp2 | qp3 | qp4 | qp5 | qp6 | qp7 | qp8>
priority <PRIORITY>	IEEE 802.1Q Tag 内の User Priority を<PRIORITY>で指定した値に変更する <0-7> • TAG 付きで出力するフレームのみが対象
priority from ip-tos-precedence	IEEE 802.1Q Tag 内の User priority を IPv4 ヘッダーの Precedence から取得した値と同じ値に変更する

処理方法	内容
	• TAG 付きで出力する IPv4 パケットのみが対象
redirect <PORT>	フレームを指定したポートに転送する • フレームのタグの有無は転送先のポートに従う
policing group <INDEX>	<INDEX>で指定した帯域制限エントリーを使用する <1-64> • 「ポリシング」を参照
policing cbs <BURSTSIZE>	ルールごとにポリシングを設定する <4-16384> • 「ポリシング」を参照
policing cir <RATE>	ルールごとにポリシングを設定する <64-33554368> • 「ポリシング」を参照
mirror <PORT>	<PORT>で指定したポートにフレームをコピー(ミラーリング)する • To ポートとして 2 ポート指定可能 • 受信トラフィックを装置が Untag フレームと認識した場合にはその Untag フレーム形式のままミラーリングされ、受信トラフィックを Tag フレームと認識した場合にはその Tag フレーム形式のままミラーリングされる
ip-tos-precedence <PRECEDENCE>	Precedence を<PRECEDENCE>で指定した値に変更する <0-7>
ip-tos-dscp <DSCP>	DSCP(DiffServ Code Point)を<DSCP>で指定した値に変更する <0-63>
routing <NEXTHOP-IP> [tracking <IPADDR>] [drop]	<NEXTHOP-IP>で指定したネクストホップにパケットを中継する • 「TD61-7251 AEOS Ver. 7.44 コマンドリファレンス L3 編 ポリシーベースルーティング」を参照

デフォルト

permit

コマンドモード

PACKETFILTER2

使用例

(1) グループ：1、ルール：1 にフレーム中継拒否を追加し、インデックス番号：1 のカウンター条件を割り当てます。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 1 action deny
(config-filter)# 1 1 action counter 1
```

関連コマンド

show packet-filter2, show running-config

注意事項

1 つのフレームが複数のルールにヒットする場合や、ルールに複数のアクションが設

定されている場合、アクションが適用される前にアクションの調整が行われます。表3-29に、ルールに2つのアクションを設定した場合、表3-30に、1つのフレームが2つのルールにヒットした場合に適用されるアクションを示します。

ルールに"action permit"以外のコマンドが設定されている場合、"no action permit"コマンド、"no action"コマンドを使用しても"action permit"を削除することはできません。

ルールに"action deny"以外のコマンドが設定されている場合、"no action deny"コマンド、"no action"コマンドを使用すると"action deny"は削除され、"action permit"が設定されます。

none アクションを使用する場合、同一ルールに他のアクションは設定しないでください。

authentication-bypassは、AccessDefender認証ポートでのみ有効です。他の認証機能(3.46 NA機能)では使用しないでください。

authentication-bypass機能とrouting機能を併用する場合は、同一のグループ番号を指定しないでください。同一のグループ番号を指定した場合の動作は保証されません。

routing機能と"assign vlan"との併用はできません。

3.10 ポートミラーリング機能における rx 指定の From ポートと"action mirror"の assign port を同一ポートに設定している場合、"action mirror"が優先的に動作します。

AccessDefender 認証ポートで、認証を行わずにフレーム中継を許可する場合、authentication-bypass を使用してください。使用するグループ番号は、AccessDefender で使用するグループ番号(3.47.60 "packet-filter2 group"で指定)より小さい番号を使用してください。

<設定例>

```
packet-filter2
1 1 assign port 1-13
1 1 condition src mac 00:13:d3:08:da:68
1 1 action authentication-bypass
```

設定	内容
condition src mac 00:13:d3:08:da:68	端末のMACアドレスを指定

condition action authentication-bypass　action に authentication-bypass を指定

"action counter"は FCS エラーフレームについても、ルールの condition を満たす場合はカウントされます。

ユーザーループ検知機能が有効であるポートでは"action mirror"は設定できません。

同一グループに none と他アクション(permit、deny)を設定した場合、若番の none が適用されたフレームには老番の他アクションは適用されません。

表 3-19 の機能設定がある場合、使用するグループが重複し、設定できない場合があります。その場合は、指定するグループ番号を変更し再度設定を行ってください。

表 3-28 アクション組み合わせの制限

組み合わせ	内容
permit と deny と none と authentication-bypass	同一ルールでは同時に設定不可
ip-tos-dscp と ip-tos-precedence	
qos と priority と priority from ip-tos-precedence	

表 3-29 同一ルールに 2 つのアクションを設定する場合

action2 \ action1	permit	deny	none	authentication-bypass	block-cpu-control	ip-tos-dscp	ip-tos-precedence	priority	priority from ip-tos-precedence	qos	mirror ※2	redirect	counter	policing ※3	routing
permit	-	×	×	×	×	1,2	1,2	1,2	1,2	1,2	1,2	2,1	1,2	1,2	2,1
deny ※1	-	-	×	×	×	1,2	1,2	1,2	1,2	1,2	1,2	2	1,2	1,2	2
none	-	-	-	×	2,1	×	×	×	×	×	×	×	1,2	×	×
authentication-bypass	-	-	-	-	×	1,2	1,2	1,2	1,2	1,2	1,2	2,1	1,2	1,2	2,1
block-cpu-control	-	-	-	-	-	×	×	×	×	×	×	×	1,2	×	×
ip-tos-dscp	-	-	-	-	-	-	×	1,2	1,2	1,2	1,2	2,1	1,2	1,2	2,1
ip-tos-precedence	-	-	-	-	-	-	-	1,2	1,2	1,2	1,2	2,1	1,2	1,2	2,1
priority	-	-	-	-	-	-	-	-	×	×	1,2	2,1	1,2	2,1	2,1
priority from ip-tos-precedence	-	-	-	-	-	-	-	-	-	×	1,2	2,1	1,2	2,1	2,1
qos	-	-	-	-	-	-	-	-	-	-	2,1	2,1	1,2	2,1	2,1
mirror ※2	-	-	-	-	-	-	-	-	-	-	-	2,1	1,2	2,1	2,1
redirect	-	-	-	-	-	-	-	-	-	-	-	-	1,2	1,2	×
counter	-	-	-	-	-	-	-	-	-	-	-	-	-	2,1	2,1
policing ※3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2,1
routing	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

「2」：action2 のみ適用

「1,2」：action1、action2 の順で適用

「2,1」：action2、action1 の順で適用

「×」：組み合わせ設定不可、または組み合わせ設定未サポート

※1 deny が後に適用される場合、最終的に得られる結果は破棄

※2 mirror が先に適用される場合、後のアクションはミラーリングフレームに対しては適用対象外

※3 policing が先に適用される場合、後のアクションは保証帯域分が適用対象

保証帯域超過分に対しては、exceeded-action deny 設定時は破棄、未設定時は通常の中継処理

表 3-30 異なるグループのルールに 2 つのアクションを設定する場合

action2 \ action1 ※1	permit ※3	deny ※3、※4	none ※3	authentication-bypass ※3	block-cpu-control ※2	ip-tos-dscp	ip-tos-precedence	priority	priority from ip-tos-precedence	qos	mirror ※5	redirect	counter	policing ※6	routing
permit ※3	1	1	2	1	1,2	1	1	1	1	1	1	1	1	2,1	1
deny ※3、※4	1	1	2	1	1,2	1	1	1	1	1	1	1	1	2,1	1
none ※3	1	1	1,2	1	1,2	1	1	1	1	1	1	1	1	1	1
authentication-bypass ※3	1	1	2	1	1,2	1	1	1	1	1	1	1	1	2,1	1
block-cpu-control ※2	2,1	2,1	2,1	2,1	1,2	2,1	2,1	2,1	2,1	2,1	2,1	2,1	2,1	2,1	2,1
ip-tos-dscp	2,1	2,1	2	2,1	1,2	1	2	1,2	1,2	1,2	1,2	2,1	1,2	2,1	2,1
ip-tos-precedence	2,1	2,1	2	2,1	1,2	1	1	1,2	1,2	1,2	1,2	2,1	1,2	2,1	2,1
priority	2,1	2,1	2	2,1	1,2	2,1	2,1	1	1	1,2	1,2	2,1	1,2	2,1	2,1
priority from ip-tos-precedence	2,1	2,1	2	2,1	1,2	2,1	2,1	1	1	1,2	1,2	2,1	1,2	2,1	2,1
qos	2,1	2,1	2	2,1	1,2	2,1	2,1	2,1	2,1	1	2,1	2,1	1,2	2,1	2,1
mirror ※5	2,1	2,1	2	2,1	1,2	2,1	2,1	2,1	2,1	1,2	1	2,1	1,2	2,1	2,1
redirect	1,2	1	2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1	1,2	2,1	×
counter	2,1	2,1	2	2,1	1,2	2,1	2,1	2,1	2,1	2,1	2,1	2,1	1,2	2,1	2,1
policing ※6	1	1	1,2	1	1,2	1	1	1	1	1	1	1	1	1	1
routing	1,2	1	2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	×	1,2	2,1	1

「1」：action1 のみ適用
「2」：action2 のみ適用
「1,2」：action1、action2 の順で適用
「2,1」：action2、action1 の順で適用
「×」：組み合わせ設定不可、または組み合わせ設定未サポート

※1 action2 よりも小さいグループ番号のルールに action1 が設定されている場合を示す
※2 block-cpu-control はどのルールよりも先に適用
※3 permit、deny、authentication-bypass、none の競合関係は以下の通り
- permit、deny、authentication-bypass は action1 のみ適用(action2 を action1 に上書き)
- none は何もしないアクションのため、action1 に設定されていている場合においても、action2 に設定された permit、deny、authentication-bypass を適用(競合関係なし)
- 他アクション設定時に同一ルールに設定される permit との競合関係も同様

※4 deny が後に適用される場合、最終的に得られる結果は破棄
※5 mirror が先に適用される場合、後のアクションはミラーリングフレームに対しては適用対象外
※6 異なるグループに policing を設定した場合、policing は後に適用
block-cpu-control との組み合わせは、保証帯域に関わらず、全帯域が CPU 宛フィルター対象

3.28.6 exceeded-action

ルールに EXCEEDED アクションを設定します。設定を削除する場合は、no コマンドを使用してください。

EXCEEDED アクションは、ルールとして設定されている識別条件(及びフィルター条件)を満たし、かつ保証帯域を超過したフレームに対して適用される処理です。

帯域制限については「ポリシング」を参照してください。

コマンドシンタックス

[no] <GROUP> <RULE> exceeded-action <*ACTIONS*>

GROUP	グループ番号 • Apresia3400/4348/5400/13000 シリーズ：<1-14> • Apresia4328 シリーズ：<1-7>
RULE	ルール番号 • Apresia3400/4300/5400 シリーズ/13000-48X：<1-128> • Apresia13000-24GX：<1-256>
ACTIONS	表 3-31 に示す exceeded action を指定

表 3-31 フレームの処理方法(exceeded action)

処理方法	内容
deny	フレームの中継を拒否する

デフォルト

なし(＝設定なし)

コマンドモード

PACKETFILTER2

使用例

(1) グループ：1、ルール：1 に EXCEEDED アクションを追加します。

(2) グループ：1、ルール：1 から EXCEEDED アクションを削除します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 1 exceeded-action deny
(config-filter)# no 1 1 exceeded-action deny
```

関連コマンド

show packet-filter2, show running-config

注意事項

3.28.7 multi

パケットフィルター2 のフィルター条件(コンディション)、動作(アクション)を一括設定します。一括設定を解除する場合は、"no <GROUP> <RULE> multi"コマンドを使用してください。設定したコンデ

ィション、アクションのみを削除する場合は、no コマンド使用時にコンディション、アクションを指定してください。
block-cpu-control の指定グループでは設定できません。

コマンドシンタックス

[no] <GROUP> <RULE> multi [condition ipv4 <*CONDITIONS*> [<*CONDITIONS*>] [<*CONDITIONS*>] [<*CONDITIONS*>]] [action <*ACTIONS*> [<*ACTIONS*>]]
no <GROUP> <RULE> multi

GROUP　グループ番号
- Apresia3400/4348/5400/13000 シリーズ：<1-14>
- Apresia4328 シリーズ：<1-7>

RULE　ルール番号
- Apresia3400/4300/5400 シリーズ/13000-48X：<1-128>
- Apresia13000-24GX：<1-256>

CONDITIONS　表 3-32 に示すコンディションを指定
- no コマンドを使用する場合、パラメーター範囲は指定不可

ACTIONS　表 3-33 に示すアクションを指定
- no コマンドを使用する場合、パラメーター範囲は指定不可

表 3-32 multi コマンドの設定可能フィルター条件(コンディション)

condition		内容
ipv4	dst-ip <IPADDR> | <IPADDR/NETMASK>	宛先 IP アドレス • <NETMASK>入力省略時のマスクは自動設定
	src-ip <IPADDR> | <IPADDR/NETMASK>	送信元 IP アドレス • <NETMASK>入力省略時のマスクは自動設定
	protocol <PROTOCOL> [mask <MASK>]	IPv4 ヘッダーのプロトコル値 <0-255>
	dst-tcp <TCPPORT>	宛先 TCP ポート番号 <0-65535> • 範囲指定可 • 範囲指定時は、異なる指定パターンにつき、range-id を 1 つ使用 ※ range-id は装置全体で 16 個までです ("show packet-filter2 tcp/udp-range" 項参照)。
	src-tcp <TCPPORT>	送信元 TCP ポート番号 <0-65535> • 範囲指定可 • 範囲指定時は、異なる指定パターンにつき、range-id を 1 つ使用 ※ range-id は装置全体で 16 個までです ("show packet-filter2 tcp/udp-range" 項参照)。
	dst-udp <UDPPORT>	宛先 UDP ポート番号 <0-65535> • 範囲指定可 • 範囲指定時は、異なる指定パターンにつき、range-id を 1 つ使用 ※ range-id は装置全体で 16 個までです

condition		内容
		("show packet-filter2 tcp/udp-range" 項参照)。
	src-udp <UDPPORT>	送信元 UDP ポート番号 <0-65535> • 範囲指定可 • 範囲指定時に関わらず、異なる指定パターンにつき、range-id を 1 つ使用 ※ range-id は装置全体で 16 個までです ("show packet-filter2 tcp/udp-range" 項参照)。

表 3-33 multi コマンドの設定可能処理方法(アクション)

処理方法	内容
permit	フレームの中継を許可する • ルールのデフォルトアクション • アクションに counter を設定した場合、permit が自動設定 • アクションに counter が設定された状態で no コマンドを使用しても permit は削除不可
deny	フレームの中継を拒否する • 同一ルールに permit、none の同時設定は不可 • アクションに deny、及び counter が設定されている状態において no コマンドで deny を削除した場合、permit が自動設定
none	対象フレームの中継動作に、permit、deny の影響を与えないようにする • 同一グループにおいて、none を設定しているルールの番号が、permit、deny が設定されているルールよりも若い場合に、none アクションが有効 • 同一ルールに permit、deny の同時設定は不可 • アクションに none、及び counter が設定されている状態において no コマンドで none を削除した場合、permit が自動設定 • 別グループで permit、deny が設定されている場合、別グループの permit、deny アクションが有効
counter <INDEX>	対象となるフレームのフレーム数、またはバイト数をカウントする • <INDEX>は使用する index • カウンターはグループごとに複数個(注)用意されているため、複数ルールで個別にカウンターを使用することや、同じカウンターを複数ルール(グループ内)で共有することが可能 (注)：1 グループあたりの index 数 • Apresia3400/4300/5400 シリーズ/13000-48X：<1-64> • Apresia13000-24GX：<1-128>

デフォルト

なし(＝設定なし)

コマンドモード

PACKETFILTER2

使用例

(1) グループ：1、ルール：1 のフィルターに送信元 IP アドレス：192.168.1.100 のパケットを破棄するルールを設定します。

(2) グループ：1、ルール：1 から deny アクションを削除します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 1 multi condition ipv4 src-ip 192.168.1.100 action deny
(config-filter)# no 1 1 multi action deny
```

関連コマンド

show packet-filter2, show running-config

注意事項

フィルター条件(コンディション)を複数指定する場合、表 3-32 の順番に従って設定してください。
例：src-ip の後に dst-ip は設定できません。

3.28.8 block-cpu-control

CPU 宛フィルター機能で使用するパケットフィルター2 のグループを指定します。設定を削除する場合は、no コマンドを使用してください。指定グループにパケットフィルター2 関連の設定がある場合は、削除できません。

CPU 宛フィルター機能はパケットフィルター2 のグループを 2 個使用します。指定グループに"action block-cpu-control"を設定することにより、フィルター条件(コンディション)を満たした CPU 宛フレームをフィルターできます。指定グループで使用可能なアクションは none、block-cpu-control、counter です。指定グループへのパケットフィルター2 関連の設定/削除は、自動的にもう一方の指定グループへ設定/削除されます。

Apresia4348 シリーズ/Apresia13000-48X には設定できません。

コマンドシンタックス

[no] block-cpu-control <GROUP> <GROUP> enable

GROUP　グループ番号
- Apresia3400/5400 シリーズ：<1-14>
- Apresia13000-24GX-PSR：<1-14>
- Apresia4328 シリーズ：<1-7>

デフォルト

なし(＝設定なし)

コマンドモード

PACKETFILTER2

使用例

(1) パケットフィルター2 のグループ：1、2 を CPU 宛フィルター機能で使用するグループに指定します。
(2) グループ：1、2 の指定を削除します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# block-cpu-control 1 2 enable
(config-filter)# no block-cpu-control 1 2 enable
```

関連コマンド

show packet-filter2, show running-config

注意事項

CPU 宛フィルター機能はアクション設定前に必ずフィルター条件(コンディション)を設定してください。フィルター条件が設定されていない場合、CPU 宛ての全パケットがフィルターされます。

"no ip icmp redirect send disable"設定時の ICMP リダイレクト対象パケットはフィルターできません。

sFlow 有効時は sFlow パケットをフィルターできません。

Apresia3448 シリーズにおいて、以下の組み合わせ(*1、または*2)でアクション block-cpu-control を設定した場合、パケット数を 2 倍にカウントする可能性があるため、アクション counter を使用できません。
(*1)ポート 1～24、49～50 のいずれかを assign port で指定
ポート 25～48、51～52 のいずれかを assign port で指定
(*2)ポート 1～24、49～50 のいずれかの所属 vlan を assign vlan で指定
ポート 25～48、51～52 のいずれかの所属 vlan を assign vlan で指定

3.28.9 wide-mode

特定フィルター条件(コンディション)の同一ルール内複数設定を可能にするワイドモードを設定します。設定を削除する場合は、no コマンドを使用してください。

ワイドモードにより複数設定可能となるフィルター条件(コンディション)を表 3-34 に示します。これらのフィルター条件は、コンディションタイプが異なっていてもワイドモードにより同一ルール内に設定可能となります。

ワイドモードはグループを連番で 2 つ使用します。

コマンドシンタックス

[no] wide-mode <GROUP>

GROUP　　グループ番号

- Apresia3400/4348/5400/13000 シリーズ：<奇数グループ>
- Apresia4328 シリーズ：<偶数グループ>

表 3-34 ワイドモードで同一ルール内に複数設定可能なフィルター条件

condition		内容
ipv6	dst ip <IPv6ADDR/LENGTH>	宛先 IPv6 アドレス
	dst tcp/udp <TCP/UDPPORT> [tcp | udp]	宛先 TCP/UDP ポート番号 <0-65535> • 範囲指定可 • tcp | udp オプションを使用することにより、特定のプロトコルのみを指定可能 • "wide-mode"使用時のみ指定可能 • 範囲指定時に関わらず、異なる指定パターンにつき、range-id を 1 つ使用 ※ range-id は装置全体で 16 個までです("show packet-filter2 tcp/udp-range"項参照)。 • tcp | udp オプションを使用せず、TCP、UDP ではない IP パケットを受信すると「TCP、UDP の宛先ポート番号に当たるデータ部分の 3～4byte 目」が設定した宛先 TCP/UDP ポート番号の 16 進数値と同じ場合、フィルターの対象となる
	src ip <IPv6ADDR/LENGTH>	送信元 IPv6 アドレス
	src tcp/udp <TCP/UDPPORT> [tcp | udp]	送信元 TCP/UDP ポート番号 <0-65535> • 範囲指定可 • tcp | udp オプションを使用することにより、特定のプロトコルのみを指定可能 • "wide-mode"使用時のみ指定可能 • 範囲指定時に関わらず、異なる指定パターンにつき、range-id を 1 つ使用 ※ range-id は装置全体で 16 個までです("show packet-filter2 tcp/udp-range"項参照)。 • tcp | udp オプションを使用せず、TCP、UDP ではない IP パケットを受信すると「TCP、UDP の送信元ポート番号に当たるデータ部分の 1～2byte 目」が設定した送信元 TCP/UDP ポート番号の 16 進数値と同じ場合フィルターの対象となる

デフォルト

なし(＝設定なし)

コマンドモード

PACKETFILTER2

使用例

(1) グループ：1をワイドモードに設定します。
(2) グループ：1のワイドモード設定を削除します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# wide-mode 1
(config-filter)# no wide-mode 1
```

関連コマンド

show packet-filter2, show running-config

注意事項

3.28.10 show packet-filter2

パケットフィルター2 の設定状態を表示します。グループ番号、ルール番号を省略した場合、すべてのルールの設定状態を表示します。グループ番号を指定すると、そのグループの全ルールについての設定状態を表示します。ルール番号まで含めた場合は、特定のルールのみ表示します。

コマンドシンタックス

show packet-filter2 [<GROUP> [<RULE>]]

GROUP　グループ番号
- Apresia3400/4348/5400/13000 シリーズ：<1-14>
- Apresia4328 シリーズ：<1-7>

RULE　ルール番号
- Apresia3400/4300/5400 シリーズ/13000-48X：<1-128>
- Apresia13000-24GX：<1-256>

コマンドモード

VIEW, ENABLE

使用例

(1) パケットフィルター2 の設定状態を表示します。

```
# show packet-filter2
group rule  status        assign condition-type
--------------------------------------------------------------------------------
    1    1  Enable          port           dst

action    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
--------------------------------------------------------------------------------
action  Permit       -       -       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
--------------------------------------------------------------------------------
                     100.0.0.1       100.0.0.1     -
```

```
Exc-action    deny
-------------------------------------------------------------------------------
Exc-action       -

assign     port                                      vid vid-m
-------------------------------------------------------------------------------
port       1                                           -     -

condition     dst mac address   dst ip address     Type    vid
-------------------------------------------------------------------------------
dst                        -      192.168.1.0        -      -
dst-m                      -    255.255.255.0        -      -

group rule  status        assign condition-type
-------------------------------------------------------------------------------
    2    1  Enable          port          ipv4

action    deny     CPU  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
action    None   Block              -          -

Exc-action    deny     CPU
-------------------------------------------------------------------------------
Exc-action       -       -
   (中略)

E = exclusive  Prio = priority  QosProf = QoS profile  Mirr = mirror
Redir = Redirect  Polic = policing  Tos-pre = from ip-tos-precedence
(B) = unit byte  Exc-action = exceeded-action  G = group  R = rule
Prot = protocol  (D) = tos-dscp  (P) = tos-precedence  Flag = tcp flag
S-t/u-pt = source-tcp/udp-port  D-t/u-pt = destination-tcp/udp-port
#
```

group　　：パケットフィルター2 のグループ番号
rule　　：パケットフィルター2 のルール番号
status　　：パケットフィルター2 の動作状態
　Enable　　：有効
　Disable　　：無効
assign　　：識別条件のタイプの設定状態
　port　　：ポート番号設定
　vlan　　：VLAN ID 設定
　port/vlan　　：ポート番号、VLAN ID 設定
condition-type　　：フィルター条件のタイプの設定状態
　ipv4　　：IPv4 ヘッダー
　ipv4-src-tcp/udp-range　　：送信元 tcp/udp の port 番号の範囲

ipv4-dst-tcp/udp-range　：宛先 tcp/udp の port 番号の範囲
ethernet　：Ethernet ヘッダー
src　：送信元の情報
dst　：宛先の情報
ipv6　：IPv6 アドレス
ipv6-header　：IPv6 ヘッダー
ipv6-dst-ip　：宛先 IPv6 アドレス
ipv6-src-ip　：送信元 IPv6 アドレス
ipv6-tcp/udp-range　：TCP/UDP ポート番号
action　：action の設定状態
deny　：フレーム中継拒否動作の設定状態
Permit　：中継を許可
Deny　：中継を拒否
None　：アクションしない
ABypass　：認証バイパス
CPU　：CPU 宛フィルター設定
Block　：CPU への転送を抑止
tos　：TOS 値変更指定の設定状態
pre-x　：Precedence 値を x に変更
dscp-x　：DSCP 値を x に変更
QoSProf　：QoS Profile 値変更指定の設定状態
qp1～qp8　：QoS profile 値を qp1～qp8 に変更
Prio　：IEEE 802.3Q Priority 値変更指定の設定状態
0～7　：Priority 値を表示値に変更
tos-pr　：Priority 値を IPv4 ヘッダーの TOS 優先度の値に変更
Mirr　：ミラーリングの設定状態
ポート番号　：ミラーリング先のポート
Redir　：フレーム転送動作の設定状態
ポート番号　：フレーム転送先ポート
Polic(grp-id)　：帯域制限エントリーの設定状態
group の値　：帯域制限エントリーのインデックス値
Polic(cir-cbs)　：帯域制限条件の設定状態
CIR 値-CBS 値　：帯域制限条件の設定値
counter(U)　：カウンターの設定状態
グループ値-1～64　：カウンターのインデックス値
• Byte カウントモード時は末尾に(B)
routing　：ポリシーベースルーティングの設定状態
Nexthop　：ネクストホップの IP アドレス
Tracking　：ICMP エコーによる監視先の IP アドレス
drop　：ネクストホップ喪失時の設定状態
drop　：ネクストホップ喪失時に強制破棄
Exc-action　：exceeded-action の設定状態
deny　：保証帯域超過フレームの中継拒否動作の設定状態
Deny　：中継を拒否
assign　：assign の設定状態

port	：ポート番号設定
vid	：VLAN ID 設定
port/vlan	：ポート番号、VLAN ID 設定
port	：受信ポート番号の設定状態
ポート番号	：受信ポート番号
vid	：受信 VLAN ID の設定状態
VID	：受信 VLAN ID
vid-m	：受信 VLAN ID マスクの設定状態
マスク値	：受信 VLAN ID マスク値
condition	：condition の設定状態
ipv4、ipv4-m	：IPv4 指定
src address	：送信元 IP アドレス/プレフィックス長
dst address	：宛先 IP アドレス/プレフィックス長
Prot	：IP ヘッダーのプロトコル値/マスク
tos(P/D)	：IP ヘッダーの TOS 値/マスク
ipv4-t/u、ipv4-t/u-m	：IPv4 TCP/UDP ポート範囲指定
tcp-flag	：TCP フラグ/マスク
S-t/u-p	：送信元 TCP/UDP ポート/マスク
D-t/u-p	：宛先 TCP/UDP ポート/マスク
tcp/udp-ranges(src/dst)	：送信元/宛先 TCP/UDP ポート範囲
ether、ether-m	：Ether Type 指定
dst mac address	：宛先 MAC アドレス/マスク
src mac address	：送信元 MAC アドレス/マスク
Type	：Ether Type/マスク
vid	：VLAN ID/マスク
dst、dst-m	：宛先情報指定
dst mac address	：宛先 MAC アドレス/マスク
dst ip address	：宛先 IP アドレス/プレフィックス長
Type	：Ether Type/マスク
vid	：VLAN ID/マスク
src、src-m	：送信元情報指定
src mac address	：送信元 MAC アドレス/マスク
src ip address	：送信元 IP アドレス/プレフィックス長
Type	：Ether Type/マスク
vid	：VLAN ID/マスク
ipv6、ipv6-m	：IPv6 指定
next-header	：IPv6 ネクストヘッダー/マスク
traffic-class	：IPv6 トラフィッククラス/マスク
flow-label	：IPv6 フローラベル/マスク
hop-limit	：IPv6 ホップリミット/マスク
icmp type	：ICMPv6 Type/マスク
ipv6-dst	：IPv6 宛先指定
ip address	：宛先 IP アドレス/プレフィックス長
ipv6-src	：IPv6 送信元指定
ip address	：送信元 IP アドレス/プレフィックス長

ipv6-t/u　　：IPv6 TCP/UDP ポート(範囲)指定
tcp/udp-ranges(src/dst)　　：送信元/宛先 TCP/UDP ポート(範囲)

関連コマンド

注意事項

3.28.11 show packet-filter2 brief

パケットフィルター2 の設定状態を簡易表示します。

コマンドシンタックス

show packet-filter2 brief
show packet-filter2 group brief
show packet-filter2 <GROUP> brief

GROUP　　グループ番号
- Apresia3400/4348/5400/13000 シリーズ：<1-14>
- Apresia4328 シリーズ：<1-7>

コマンドモード

VIEW, ENABLE

使用例

(1) パケットフィルター2 の設定状態を簡易表示します。

```
# show packet-filter2 brief
  Group Rule  Status
-------------------------------------------------------------------------------
      1    1 Enabled
      1    2 Disabled
      1    3 Enabled
      2    2 Enabled
      3    1 Enabled
     11    1 Enabled
#
```

(2) パケットフィルター2 の各グループについて、設定状態を簡易表示します。

```
# show packet-filter2 group brief
  group assign        condition-type
-------------------------------------------------------------------------------
      1 port          dst
      2 vlan          ipv4-src-tcp/udp-range
      3 port/vlan     ipv4-dst-tcp/udp-range
     11 port          -
#
```

(3) パケットフィルター2 のグループ：1 について、設定状態を簡易表示します。

```
# show packet-filter2 1 brief
```

```
action:
group rule    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
    1    1  Permit       -       -       -    -    47             -        1-1

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -               -     -
    1    2  Permit       -       -       -    -    48             -        1-1

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -               -     -
    1    3  Permit       -       -       -    -     -             -        1-2

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -               -     -

exceeded-action:
group rule    deny
-------------------------------------------------------------------------------
    1    1       -
    1    2       -
    1    3       -

assign:
group rule assign     port                                     vid vid-m
-------------------------------------------------------------------------------
    1    1 port       1-48                                       -     -
    1    2 port       -                                          -     -
    1    3 port       -                                          -     -

condition:
group rule condition     dst mac address   dst ip address     Type    vid
-------------------------------------------------------------------------------
    1    1 dst         00:00:00:00:00:01                -        -      -
    1    1 dst-m       ff:ff:ff:ff:ff:ff                -        -      -


E = exclusive  Prio = priority  QosProf = QoS profile  Mirr = mirror
Redir = Redirect  Polic = policing  Tos-pre = from ip-tos-precedence
(B) = unit byte  Exc-action = exceeded-action  G = group  R = rule
Prot = protocol  (D) = tos-dscp  (P) = tos-precedence  Flag = tcp flag
S-t/u-pt = source-tcp/udp-port  D-t/u-pt = destination-tcp/udp-port
```

```
T = type  c = condition  m = mask
#
```

(4) パケットフィルター2 のグループ：1 について、設定状態を簡易表示します("block-cpu-control"設定時)。

```
# show packet-filter2 1 brief
action:
group rule    deny     CPU  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
    1    1    None   Block             -          -

exceeded-action:
group rule    deny     CPU
-------------------------------------------------------------------------------
    1    1       -       -

assign:
group rule assign     port                                        vid vid-m
-------------------------------------------------------------------------------
    1    1 -          -                                            -     -



E = exclusive  Prio = priority  QosProf = QoS profile  Mirr = mirror
Redir = Redirect  Polic = policing  Tos-pre = from ip-tos-precedence
(B) = unit byte  Exc-action = exceeded-action  G = group  R = rule
Prot = protocol  (D) = tos-dscp  (P) = tos-precedence  Flag = tcp flag
S-t/u-pt = source-tcp/udp-port  D-t/u-pt = destination-tcp/udp-port
T = type  c = condition  m = mask
#
```

関連コマンド

注意事項

3.28.12 show packet-filter2 counter

パケットフィルター2 のカウンターの状態を表示します。
グループを指定した場合は、そのグループのみ表示します。

コマンドシンタックス

show packet-filter2 counter [<GROUP>]

GROUP　　グループ番号
- Apresia3400/4348/5400/13000 シリーズ：<1-14>
- Apresia4328 シリーズ：<1-7>

コマンドモード

VIEW, ENABLE

使用例

(1) パケットフィルター2 のカウンター状態を表示します。

```
# show packet-filter2 counter
group  c-id       count   unit rule         Wed Jun 21 00:00:00 2006
-------------------------------------------------------------------------------
    1     1     2356695 packet 1-2
    1     2         224 packet 3
    2     2           0 packet 2
#
```

group　　：グループ番号
c-id　　：カウンターの index
count　　：カウンターの値
unit　　：カウンターの動作モード
　packet　　：パケット単位でカウント
　byte　　：バイト単位でカウント
rule　　：このカウンターを使用するルール番号

関連コマンド

注意事項

3.28.13 show packet-filter2 tcp/udp-range

パケットフィルター2 の TCP/UDP ポート範囲指定エントリーの状態を表示します。

コマンドシンタックス

show packet-filter2 tcp/udp-range

コマンドモード

VIEW, ENABLE

使用例

(1) パケットフィルター2 の TCP/UDP ポート範囲指定エントリーの状態を表示します。

```
# show packet-filter2 tcp/udp-range
 range-id  src/dst      port-range
-------------------------------------------------------------------------------
        1      src   1024 to 65535
        2      dst   1024 to 65535
#
```

range-id　　：TCP/UDP ポート範囲指定エントリーのインデックス値 <1-16>
src/dst　　：Source/Destination の状態
　src　　：Source TCP/UDP ポート範囲指定エントリー

dst　　：Destination TCP/UDP ポート範囲指定エントリー
port-range　　：TCP/UDP ポート範囲

関連コマンド

注意事項

3.28.14 show packet-filter2 reserved-group

パケットフィルター2 グループを使用している機能を表示します。

コマンドシンタックス

show packet-filter2 reserved-group

コマンドモード

VIEW, ENABLE

使用例

(1) パケットフィルター2 グループを使用している機能を表示します。

```
# show packet-filter2 reserved-group
 Group   Function
-------------------------------------------------------------------------------
     1   Packet-filter2
     2   Packet-filter2
     3   Packet-filter2 (block-cpu-control with 4)
     4   Packet-filter2 (block-cpu-control with 3)
     5   wide-mode pf2
     6   wide-mode pf2
     7   -
     8   -
     9   -
    10   -
    11   AccessDefender
    12   AccessDefender
    13   AccessDefender
    14   AccessDefender
```

上記使用例ではパケットフィルター2 グループを以下機能で使用

グループ番号 1～2　　：パケットフィルター2 機能
グループ番号 3～4　　：パケットフィルター2 機能(CPU 宛フレーム用)
グループ番号 5～6　　：パケットフィルター2 機能(ワイドモード)
グループ番号 7～10　　：未使用
グループ番号 11～14　：AccessDefender 機能

関連コマンド

注意事項

3.28.15 show tech-support packet-filter2

パケットフィルター2 機能の各種情報を収集し表示します。本コマンドで表示する内容は、表 3-35 に示すコマンドが収集している情報です。system-dump オプションを指定した場合、装置内部のダンプ情報(独自形式で表示)を含めて取得し表示します。

表 3-35 コマンドにより収集可能なパケットフィルター2 情報

show system
show version
show packet-filter2
show packet-filter2 reserved-group
show packet-filter2 counter ※1
show interface counters ※1

※1 1 秒おきに 3 回情報を取得

コマンドシンタックス

show tech-support packet-filter2 [system-dump]

system-dump	装置内部のダンプ情報を出力

コマンドモード

ENABLE

関連コマンド

注意事項

system-dump オプションを指定した場合、装置の性能、及び通信に対して影響を及ぼす可能性があります。使用する場合には、必ず事前にサポート対応窓口へご相談のうえ、指示に従ってください。

3.28.16 clear packet-filter2 counter

カウンターをリセットします。

カウンターID を指定した場合は、特定カウンターの値のみリセットします。

コマンドシンタックス

clear packet-filter2 counter [<GROUP> [<INDEX>]]

GROUP	グループ番号 • Apresia3400/4348/5400/13000 シリーズ：<1-14> • Apresia4328 シリーズ：<1-7>
INDEX	カウンターID <1-64>

コマンドモード

VIEW, ENABLE

使用例

(1) グループ：1のカウンターID：1をリセットします。
(2) グループ：2の全カウンターをリセットします。

```
# clear packet-filter2 counter 1 1
# clear packet-filter2 counter 2
```

関連コマンド

action counter, show packet-filter2 counter

注意事項

3.28.17 ポリシング

ポリシングを使用すると、各ルールのコンディションを満たすフレームが使用する帯域を制限することができます。帯域制限のパラメーターとして「保証帯域」と「バーストサイズ」があり、保証帯域の設定には"action policing cir"コマンド、もしくは"policing cir"コマンドを使用し、バーストサイズの設定には"action policing cbs"コマンド、もしくは"policing cbs"コマンドを使用します。使用可能な帯域は保証帯域の値で制限されますが、バーストサイズに収まる範囲のバーストフレームが一時的に到達した際には、保証帯域内のフレームとして処理されます。

保証帯域内のフレームにはアクション("action"項参照)が適用されます。EXCEEDED アクションを設定した場合、保証帯域を超過したフレームに対して EXCEEDED アクション("exceeded-action"項参照)が適用されます。

"action policing cir/cbs"コマンドではルールに帯域制限条件を設定します。帯域制限条件を使用するルールは、グループごとに 64 個設定することができます。

"policing cbs/cir"コマンドを使用すると帯域制限エントリーに帯域制限条件を設定することができます。帯域制限エントリーを使用する場合、ルールに"action policing group"コマンドを設定し、使用する帯域制限エントリーのインデックスを指定する必要があります。帯域制限エントリーはグループごとに複数個(注)用意されており、複数のルールで個別のエントリーを参照することや、同じエントリーを複数のルール(グループ内)で共有することができます。

(注)：1 グループあたり 64 エントリーです。

注意事項

帯域制限エントリーと"action policing cir/cbs"コマンドを同時に使用することはできません。

帯域制限はフレーム間ギャップ、及びプリアンブル部を除くデータ部分のみを対象としており、使用率(Utilization)とは異なります。

ポリシングはポートブロックごとに独立して ingress 時に適用されます。そのため、ポートブロックが 2 個存在する機種である Apresia3448 シリーズ(port 1～24、49～50 と port 25～48、51～52)、Apresia4348 シリーズ(port 1～24 と port 25～48)、

Apresia13000-48X(port 1～24、50 と port 25～49)では、ポートブロックに跨るポリシングを設定した場合、出力値が設定値の最大 2 倍まで上回ることがあります。

3.28.18 policing cbs

帯域制限エントリーのバーストサイズを設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。バーストサイズは 4-16384 の間で任意の値を入力することができますが、有効な値は以下の 13 種類です(入力値以下で最も大きな値が有効となります)。

4，8，16，32，64，128，256，512，1024，2048，4096，8192，16384

コマンドシンタックス

<GROUP> policing <INDEX> cbs <BURSTSIZE>
no <GROUP> policing <INDEX> cbs

GROUP	グループ番号 • Apresia3400/4348/5400/13000 シリーズ：<1-14> • Apresia4328 シリーズ：<1-7>
INDEX	帯域制限エントリーのインデックス <1-64>
BURSTSIZE	バーストサイズ <4-16384(Kbyte)>

デフォルト

4(Kbyte)

コマンドモード

PACKETFILTER2

使用例

(1) グループ：1 の帯域制限エントリーインデックス：1 のバーストサイズを 2000 Kbyte(実際に有効な値は 1024 Kbyte)に設定します。
(2) エントリーのバーストサイズをデフォルトに戻します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 policing 1 cbs 2000
(config-filter)# no 1 policing 1 cbs
```

関連コマンド

show packet-filter2, show packet-filter2 policing, show running-config

注意事項

3.28.19 policing cir

帯域制限エントリーの保証帯域を設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。保証帯域は 64-33554368 の間で任意の値を入力することができますが、入力値以下で 64 の整数倍となるように切り捨てられた値が有効となります。

コマンドシンタックス

<GROUP> policing <INDEX> cir <RATE>
no <GROUP> policing <INDEX> cir

GROUP	グループ番号 • Apresia3400/4348/5400/13000 シリーズ：<1-14> • Apresia4328 シリーズ：<1-7>
INDEX	帯域制限エントリーのインデックス <1-64>
RATE	保証帯域 <64-33554368(Kbps)>

デフォルト

33554368(Kbps)

コマンドモード

PACKETFILTER2

使用例

(1) グループ：1 の帯域制限エントリーインデックス：1 の保証帯域を 10 Mbps に設定します。
(2) エントリーの保証帯域をデフォルトに戻します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 policing 1 cir 10000
(config-filter)# no 1 policing 1 cir
```

関連コマンド

show packet-filter2, show packet-filter2 policing, show running-config

注意事項

3.28.20 action policing group

ルールで使用する帯域制限エントリーを設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

<GROUP> <RULE> action policing group <INDEX>
no <GROUP> <RULE> action policing group

GROUP	グループ番号 • Apresia3400/4348/5400/13000 シリーズ：<1-14> • Apresia4328 シリーズ：<1-7>
RULE	ルール番号 • Apresia3400/4300/5400 シリーズ/13000-48X：<1-128> • Apresia13000-24GX：<1-256>
INDEX	帯域制限エントリーのインデックス <1-64>

デフォルト
なし(＝設定なし)

コマンドモード
PACKETFILTER2

使用例
(1) グループ:1 のルール:1 で帯域制限エントリーインデックス:1 を使用するように設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 1 action policing group 1
(config-filter)# no 1 1 action policing group
```

関連コマンド
show packet-filter2, show packet-filter2 policing, show running-config

注意事項

3.28.21 action policing cbs

ルールで使用するバーストサイズを設定します。設定を削除する場合は、no コマンドを使用してください。バーストサイズは 4-16384 の間で任意の値を入力することができますが、有効な値は以下の 13 種類です(入力値以下で最も大きな値が有効となります)。

4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384

コマンドシンタックス
<GROUP> <RULE> action policing cbs <BURSTSIZE>
no <GROUP> <RULE> action policing cbs

GROUP	グループ番号 • Apresia3400/4348/5400/13000 シリーズ：<1-14> • Apresia4328 シリーズ：<1-7>
RULE	ルール番号 • Apresia3400/4300/5400 シリーズ/13000-48X：<1-128> • Apresia13000-24GX：<1-256>
BURSTSIZE	バーストサイズ <4-16384(Kbyte)>

デフォルト
なし
"action policing cir"が設定されている場合のデフォルトは 4 Kbyte

コマンドモード
PACKETFILTER2

使用例

(1) グループ：1 のルール：1 のバーストサイズを 2000 Kbyte(実際に有効な値は 1024 Kbyte)に設定します。

(2) 設定を削除します。

```
> enable
# configure terminal
(config)# packet-filter2
(config-filter)# 1 1 action policing cbs 2000
(config-filter)# no 1 1 action policing cbs
```

関連コマンド

show packet-filter2, show running-config

注意事項

3.28.22 action policing cir

ルールで使用する保証帯域を設定します。設定を削除する場合は、no コマンドを使用してください。保証帯域は 64-33554368 の間で任意の値を入力することができますが、入力値以下で 64 の整数倍となるように切り捨てられた値が有効となります。

コマンドシンタックス

<GROUP> <RULE> action policing cir <RATE>

no <GROUP> <RULE> action policing cir

GROUP	グループ番号 • Apresia3400/4348/5400/13000 シリーズ：<1-14> • Apresia4328 シリーズ：<1-7>
RULE	ルール番号 • Apresia3400/4300/5400 シリーズ/13000-48X：<1-128> • Apresia13000-24GX：<1-256>
RATE	保証帯域 <64-33554368(Kbps)>

デフォルト

なし

"action policing cbs"が設定されている場合のデフォルトは 33554368 Kbps

コマンドモード

PACKETFILTER2

使用例

(1) グループ：1 のルール：1 の保証帯域を 10 Mbps に設定します。

(2) 設定を削除します。

```
> enable
# configure terminal
```

```
(config)# packet-filter2
(config-filter)# 1 1 action policing cir 10000
(config-filter)# no 1 1 action policing cir
```

関連コマンド

show packet-filter2, show running-config

注意事項

3.28.23 ポリシーベースルーティング
3.28.24 action routing
3.28.25 pbr arp-interval
3.28.26 pbr icmp

3.28.23～3.28.26 については、TD61-7251 AEOS Ver. 7.44 コマンドリファレンス L3 編のポリシーベースルーティング節をご参照ください。

3.28.27 show packet-filter2 policing

帯域制限エントリーの設定状態を表示します。グループを指定した場合は、そのグループのみ表示します。

コマンドシンタックス

show packet-filter2 policing [<GROUP>]

GROUP　　グループ番号
- Apresia3400/4348/5400/13000 シリーズ：<1-14>
- Apresia4328 シリーズ：<1-7>

コマンドモード

VIEW, ENABLE

使用例

(1) 帯域制限エントリーの設定状態を表示します。

```
# show packet-filter2 policing
   group  m-id       cir    cbs rule
--------------------------------------------------------------------------------
       1     1  33554368      4
 (途中略)
      14    64  33554368      4

  rate unit: Kbps
  size unit: Kbyte

#
```

group　　：グループ番号

m-id	：エントリーの index
cir	：エントリーの保証帯域の設定値
cbs	：エントリーのバーストサイズの設定値
rule	：エントリーを使用するルール番号

関連コマンド

注意事項

本コマンドは、帯域制限エントリー("action policing group")用の表示コマンドです。"action policing cir/cbs"コマンドによる設定時は使用できません。

3.29 ユーザーループ検知

ユーザーループ検知機能は、装置の配下でループ障害が発生したことを検知した場合に、ポートを閉塞("shutdown"コマンド発行)することにより、障害がネットワーク全体に波及しないようにする機能です。ループの検知は、装置から定期的にユーザーループ検知フレームを送信するとともに、ユーザーループ検知フレームが折り返されて受信することがないか監視することにより行っています。ユーザーループ検知フレームはポートごとに送信され、ポートがトランクポート(802.1Q タグ付き VLAN モード)で複数の VLAN に所属する場合は、さらに VLAN ごとに送信されます。

ユーザーループ検知フレームとは、宛先 MAC アドレス"00:40:66:10:cb:92"、送信元 MAC アドレス"自装置の MAC アドレス"、Ether Type "0x8820"を使用したフレームです。フレームフォーマットの詳細については、AEOS Ver. 7 アプリケーションノート(ユーザーループ検知機能)をご覧ください。

ユーザーループ検知機能が有効に設定されており、装置内のいずれかのポートから送信されたユーザーループ検知フレームを受信したポートが閉塞(shutdown)されます。notify-only 設定にはループ検知時にポートの閉塞は行わず警報のみ行います。

"auto-recovery timer"が設定されている場合、設定された時間の経過後に、ポートの閉塞から自動的に回復します。本設定がない場合は、"no shutdown"コマンドによりポートの閉塞を回復させてください。

注意事項

輻輳などの原因により、本装置へ折り返されるユーザーループ検知フレーム自体が下位装置で破棄される場合、ループ障害の発生を検知できません。
下位装置におけるユーザーループ検知フレームの優先度を高く設定しておくことにより、ループ障害発生時に破棄される可能性は低くなり、ループ検知の精度向上を見込めます。

3.28 パケットフィルター2 機能併用時に、ユーザーループ検知機能よりも小さいグループ番号でパケットフィルター2 機能を設定する場合、ethertype 0x8820 のユーザーループ検知フレームがフィルター対象とならないように設定してください。

本機能の設定変更を行うと、すべてのインターフェースのユーザーループ検知フレーム受信回数が消去されます。

3.29.1 no loop-watch

本コマンドでユーザーループ検知機能に関するすべての設定を削除します。

コマンドシンタックス

no loop-watch

デフォルト

なし

コマンドモード

CONFIG
(CONFIG モード以外でも入力可能)

使用例

(1) ユーザーループ検知機能のすべての設定を削除します。

```
> enable
# configure terminal
(config)# no loop-watch
```

関連コマンド

show running-config

注意事項

3.29.2 loop-watch enable

ユーザーループ検知機能を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] loop-watch enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) ユーザーループ検知機能を有効にします。
(2) ユーザーループ検知機能を無効にします。

```
> enable
# configure terminal
(config)# loop-watch enable
(config)# no loop-watch enable
```

関連コマンド

show loop-watch configuration, show running-config

注意事項

本機能は、3.10 ポートミラーリングを設定しているポートでは併用できません。ただし、当該ポートでは、ループ検知フレームを中継します。

3.29.3 loop-watch interval

ユーザーループ検知フレームの送信間隔を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。ユーザーループ検知フレームは、設定された送信間隔ごとに、ユーザーループ検知機能が有効な各ポートの VLAN 数の総和数分を約 20 pps の送信レートで出力されます。

コマンドシンタックス

loop-watch interval <INTERVAL>
no loop-watch interval
　　INTERVAL　　ユーザーループ検知フレームの送信間隔 <2-3600(秒)>

デフォルト

10(秒)

コマンドモード

CONFIG

使用例

(1) ユーザーループ検知フレームの送信間隔を 100 秒にします。
(2) ユーザーループ検知フレームの送信間隔をデフォルト値(10 秒)にします。

```
> enable
# configure terminal
(config)# loop-watch interval 100
(config)# no loop-watch interval
```

関連コマンド

show loop-watch configuration, show running-config

注意事項

ユーザーループ検知機能が有効なインターフェースの数、及びこれが所属する VLAN 数が多い場合、ユーザーループ検知フレームの送信間隔が短いと、すべてのユーザーループ検知フレームを送信間隔内に送信できません。特定のインターフェースや VLAN でユーザーループ検知機能が無効になることを防ぐため、送信間隔は以下の条件で設定してください。

ユーザーループ検知機能有効インターフェースに属する VLAN 数の総和/20(pps)＜送信間隔(秒)

3.29.4 loop-watch threshold

ユーザーループ検知フレームの閾値を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。装置に折り返したユーザーループ検知フレームの受信数が、設定した閾値に達した場合に、当該ポートでループ障害を検知したと判断します。

コマンドシンタックス

loop-watch threshold <THRESHOLD-VALUE>
no loop-watch threshold
　　THRESHOLD-VALUE　　ユーザーループ検知フレームの閾値 <1-1000000(フレーム)>

デフォルト

1

コマンドモード

CONFIG

使用例

(1) ユーザーループ検知フレームの閾値を 100 フレームにします。
(2) ユーザーループ検知フレームの閾値をデフォルト値(1 フレーム)にします。

```
> enable
# configure terminal
(config)# loop-watch threshold 100
(config)# no loop-watch threshold
```

関連コマンド

show loop-watch configuration, show running-config

注意事項

3.29.5 loop-watch auto-recovery timer

ループ検知によるポート閉塞を自動的に回復させるまでの時間を設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

loop-watch auto-recovery timer <TIME>
no loop-watch auto-recovery timer
　　TIME　　自動回復時間 <10-86400(秒)>

デフォルト

なし(＝無効)

コマンドモード

CONFIG

使用例

(1) ループ検知後のポート閉塞の自動回復時間を 100 秒にします。
(2) ループ検知後のポート閉塞の自動回復を無効にします。

```
> enable
# configure terminal
```

```
(config)# loop-watch auto-recovery timer 100
(config)# no loop-watch auto-recovery timer
```

関連コマンド

show loop-watch configuration, show running-config

注意事項

ユーザーループ検知機能が有効("loop-watch enable")な場合、自動回復時間の変更は行えません。自動回復時間を変更する場合は、ユーザーループ検知機能を無効にしてください。

3.29.6 loop-watch group

ユーザーループ検知機能で使用するパケットフィルター2 のグループ番号を設定します。設定を削除する場合は、no コマンドを使用してください。グループは"loop-watch enable"設定時に確保します。他機能で予約済みのグループは確保できません。

本コマンド未設定時は、未使用グループの最大番号を自動的に予約します。

"loop-watch enable"が設定されている状態では、グループ番号を変更できません。グループの予約状況は 3.28.14 "show packet-filter2 reserved-group"コマンドで確認可能です。

コマンドシンタックス

loop-watch group <GROUP>
no loop-watch group

GROUP	グループ番号 • Apresia3400/4348/5400/13000 シリーズ：<1-14> • Apresia4328 シリーズ：<1-7>

デフォルト

自動割り当て(＝未使用グループの最大番号)

コマンドモード

CONFIG

使用例

(1) ユーザーループ検知機能でグループ：1 を使用します。

```
> enable
# configure terminal
(config)# loop-watch group 1
```

関連コマンド

show loop-watch configuration, show running-config

注意事項

表 3-19 の各コマンドは、パケットフィルター2 のグループを使用するため、これら機能設定がある場合、使用するグループが重複しているとコマンドを実行できません。その場合は、指定するグループ番号を変更してください。

ユーザーループ検知機能が有効("loop-watch enable")な場合、グループ番号の変更は行えません。グループ番号を変更する場合は、ユーザーループ検知機能をいったん無効にしてから変更してください。

3.29.7 loop-watch port

ユーザーループ検知機能を有効にするポートを指定します。無効にする場合は、no コマンドを使用してください。

notify-only を指定した場合は、ループを検知してもポートの閉塞(shutdown)は行われません。ログ、及び TRAP の出力のみが行われます。

owner-vlan を指定した場合は、以下のユーザーループ検知フレームを検知してもポートの閉塞(shutdown)は行われません。

(1) 装置に未設定の VLAN ID(3.11.1 "vlan database"コマンドで未定義な VLAN ID)を持つ、タグ付きユーザーループ検知フレーム
(2) トランクポートでのタグなしユーザーループ検知フレーム
(3) 各冗長機能によって論理的にブロッキングになっている VLAN で受信した、ユーザーループ検知フレーム

tx-only を指定した場合は、監視フレームの送信、受信時破棄のみを行い、ループ検出は行われません。tx-only は 3.9 ポートリダンダント機能の ready ポートで使用してください。

no-check-srcmac を指定した場合は、ユーザーループ検知フレームの送信元 MAC アドレスが装置の自局 MAC アドレス以外でもループを検知します。

コマンドシンタックス

```
loop-watch port <PORTRANGE> [ ( notify-only [ owner-vlan ] ) | owner-vlan | tx-only ]
loop-watch port <PORTRANGE> no-check-srcmac [ ( notify-only [ owner-vlan ] ) | owner-vlan ]
no loop-watch port <PORTRANGE>
```

PORTRANGE	ユーザーループ検知機能を有効にするポート(複数指定可能)
notify-only	ループ検知時の警告のみ
owner-vlan	owner-vlan 設定
tx-only	監視フレーム送信、受信時の破棄(ループ検出無)
no-check-srcmac	ユーザーループ検知フレーム送信元 MAC アドレスの未監視

デフォルト

なし(＝設定無し)

コマンドモード

CONFIG

使用例

(1) ポート：1 でユーザーループ検知機能を有効にします。

(2) ポート：1 でユーザーループ検知機能を無効にします。
(3) ポート：2、5～8 でユーザーループ検知機能を有効にします。
(4) ポート：2、5～8 でユーザーループ検知機能を無効にします。
(5) ポート：10 でユーザーループ検知時、警告のみ表示にします。
(6) ポート：11 の特定 VLAN ID でユーザーループ検知時、警告のみ表示する。
(7) ポート：12 の特定 VLAN ID でユーザーループ検知を有効にします。
(8) ポート：13 でユーザーループフレーム送信のみにします。
(9) ポート：14 でユーザーループ検知フレームの送信元 MAC アドレスが装置の自局 MAC アドレス以外でもループ検知するモードにてユーザーループ検知機能を有効にします。

```
> enable
# configure terminal
(config)# loop-watch port 1
(config)# no loop-watch port 1
(config)# loop-watch port 2,5-8
(config)# no loop-watch port 2,5-8
(config)# loop-watch port 10 notify-only
(config)# loop-watch port 11 notify-only owner-vlan
(config)# loop-watch port 12 owner-vlan
(config)# loop-watch port 13 tx-only
(config)# loop-watch port 14 no-check-srcmac
```

関連コマンド

show loop-watch configuration, show running-config

注意事項

ユーザーループ検知機能でループを検知した場合、該当ポート(ユーザーループ検知フレームを受信したポート)には"shutdown"コマンドの設定が入ります。ネットワーク内の配線、接続などを確認し、原因を取り除いた上、"no shutdown"コマンドによりポートの閉塞を回復してください。

本機能を 3.41 MMRP/3.42 MMRP-Plus のマスター/スレーブ/アウェア設定ポートや 3.17 スパニングツリープロトコル(STP/RSTP/MSTP)のブロッキング状態になる可能性のあるポートと併用する場合は、owner-vlan 設定を必ず行ってください。

リンクアグリゲーション、ポートリダンダントを設定しているポートでは notify-only のみ設定可能です。ただし、ポートリダンダント機能の ready ポートに設定する場合は tx-only を設定してください。

3.29.8 loop-watch vlan add

ポートごとにユーザーループ検知フレームを送信する VLAN を指定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

VLAN を指定しない場合は、3.11.6 "switchport trunk"コマンドでポートに設定されているすべての

VLANに対して、ユーザーループ検知フレームを送信します。

コマンドシンタックス

loop-watch vlan add <VLANRANGE>
no loop-watch vlan add [<VLANRANGE>]
　　VLANRANGE　　VLAN ID <1-4094> (複数指定可能)

デフォルト

なし(＝全VLANに送信)

コマンドモード

IF-PORT

使用例

(1) ユーザーループ検知フレームを送信するVLANにVLAN ID：100を設定します。
(2) デフォルトに戻します。

```
> enable
# configure terminal
(config)# interface port 1
(config-if-port)# loop-watch vlan add 100
(config-if-port)# no loop-watch vlan add
```

関連コマンド

show loop-watch configuration, show running-config

注意事項

IF-PORT モードにおいても"no loop-watch"コマンドは入力可能です。"no loop-watch"コマンドを入力するとユーザーループ検知機能に関するすべての設定が消去されますので注意してください。

3.29.9 clear loop-watch information

"show loop-watch status"コマンドで表示される"ユーザーループ検知フレーム受信回数"、及び"ユーザーループ検知によって最後にループを検知した時刻"を消去します。

コマンドシンタックス

clear loop-watch information

コマンドモード

ENABLE

使用例

(1) ユーザーループ検知情報を削除します。

```
> enable
```

```
# clear loop-watch information
```

関連コマンド

show loop-watch status

注意事項

自動復旧時間("loop-watch auto-recovery timer")の動作中にループを検出し、本コマンドを実行した場合、自動復旧機能による"no shutdown"の発行は行われません。

3.29.10 show loop-watch configuration

ユーザーループ検知機能の設定を表示します。

コマンドシンタックス

show loop-watch configuration

コマンドモード

VIEW, ENABLE

使用例

(1) ユーザーループ検知機能の設定を表示します。

```
# show loop-watch configuration
 Status    : Enabled
 Interval  : 10 sec
 Threshold : 1
 Group     : -
 Auto-Recovery Timer : -

--- port information ---
     *=Enable                   S=Enable (owner-vlan)
     n=Enable (notify-only)     N=Enable (notify-only, owner-vlan)
     m=Enable (no-check-srcmac) M=Enable (no-check-srcmac, notify-only)
     o=Enable (no-check-srcmac, owner-vlan)
     O=Enable (no-check-srcmac, notify-only, owner-vlan)
     t=Enable (tx-only)
     1       8 9     16 17    24 25    32 33    40 41    48 49
     +------+ +------+ +------+ +------+ +------+ +------+ +-
     Snnnnnnn nn...... ........ ........ ........ ........ ..

--- vlan information ---
     *=Active(send)
     r=Ready(not send)
     1       8 9     16 17    24 25    32 33    40 41    48 49
 VID +------+ +------+ +------+ +------+ +------+ +------+ +-
```

```
 ALL ******** **...... ........ ........ ........ ........ ..

#
```

Status　　：ユーザーループ検知機能の設定状態
　Disabled　　：ユーザーループ検知機能 OFF
　Enabled　　：ユーザーループ検知機能 ON
Interval　　：ユーザーループ検知フレーム送信間隔
Threshold　　：ユーザーループ検知の閾値
Group　　：使用するグループ番号
Auto-Recovery Timer　　：ループ検知によるポート閉塞の自動復旧までの時間
port information
　*　　：ユーザーループ検知機能が有効
　n　　：notify-only 機能が有効
　S　　：owner-vlan 機能が有効
　N　　：notify-only/owner-vlan 機能が有効
　m　　：no-check-srcmac 機能が有効
　M　　：no-check-srcmac/notify-only 機能が有効
　o　　：no-check-srcmac/owner-vlan 機能が有効
　O　　：no-check-srcmac/notify-only/owner-vlan 機能が有効
　t　　：tx-only 機能が有効
vlan information
　*　　：ユーザーループ検知フレームを送信
　r　　：VLAN 設定は行われているが、ポートのユーザーループ検知機能が無効

関連コマンド

注意事項

3.29.11 show loop-watch status

ユーザーループ検知機能の状態を表示します。

コマンドシンタックス

show loop-watch status

コマンドモード

VIEW, ENABLE

使用例

(1) ユーザーループ検知機能の状態を表示します。

```
> enable
# show loop-watch status
                  Shutdown       Link
 Pt.    Receive (    Notify)     Status          Date
```

```
-----------------------------------------------------------------
  1          1          0       Up
  2          -          1       Disable    2005/12/05 13:22:16
  3          0          3       Up         2005/12/04 20:08:40
  4          1          5       Down       2005/12/06 09:51:31
  5          2          0       Down
```

Pt.　　：ユーザーループ検知機能の有効ポート
Receive　　：ユーザーループ検知フレーム受信回数
Shutdown　　：ユーザーループ検知によってポートがシャットダウンした回数
Link Status　　：ポートの現在のリンク状態
　Disable　　：シャットダウン
　Up　　：リンクアップ
　Down　　：リンクダウン
Date　　：ユーザーループ検知によって最後にループを検知した時刻

関連コマンド

注意事項

3.30 QoS

注意事項

本機能よりもパケットフィルター、パケットフィルター2 の action 機能の qp 指定が優先されます。

Apresia4348 シリーズと Apresia13000-48X において min-band 設定と weight 設定の併用はできません。

QoS 機能の WRR(Weighted Round Robin)/DRR(Deficit Round Robin)と 3.24 Egress シェーピング機能の併用は Apresia3400/5400 シリーズのみ可能です。これ以外の機種では併用できません。

装置発の制御フレームは、QoS の設定によらず、常に qp8 の QoS プロファイルに対応する送信キューから送出されます。

3.30.1 qos enable

QoS を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] qos enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) QoS を有効にします。
(2) QoS を無効にします。

```
> enable
# configure terminal
(config)# qos enable
(config)# no qos enable
```

関連コマンド

show qos, show running-config

注意事項

3.30.2 qos min-bandwidth

qp1～qp8 の 8 種類の QoS プロファイルの最低帯域をポートごとに設定します。最低帯域は Kbps で設定し、各 QoS プロファイルは 64～10000000 Kbps の範囲で設定可能です。最低帯域の設定を無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

qos qosprofile qp1 | qp2 | qp3 | qp4 | qp5 | qp6 | qp7 | qp8 port <PORTRANGE> min-bandwidth <VALUE>

no qos qosprofile qp1 | qp2 | qp3 | qp4 | qp5 | qp6 | qp7 | qp8 port <PORTRANGE> min-bandwidth

qp1～qp8	最低帯域を設定する QoS プロファイル(優先度は qp1 から qp8 の順で高)
PORTRANGE	最低帯域を設定するポート番号(複数指定可能)
VALUE	上で指定したポートから送信される QoS プロファイルのフレームの最低帯域 <64-10000000(Kbps)>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1 に対し、qp1 の QoS プロファイルの最低帯域を 128 Kbps に設定します。

```
> enable
# configure terminal
(config)# qos qosprofile qp1 port 1 min-bandwidth 128
```

関連コマンド

show qos, show running-config

注意事項

帯域は 64～10000000 Kbps の範囲の任意の数値を設定できますが、実際の動作時には 64 の整数倍に切り捨てられます。

実際の最低帯域は、負荷の状態に依存して変動する可能性があります。設定値を厳密に保証するものではありません。

本コマンドは Apresia4328 には対応していません。

Apresia4300/5400/13000 シリーズにおいて、以下に示すポートで qp1～qp7 のいずれかの QoS プロファイルに本コマンドを設定すると、トラフィック状態によっては制御フレームの送信が停止する場合があります。このような設定を行う場合は、制御フレームの送信帯域を確保するため、qp8 に対しても 64 kbps 以上の最低保証帯域を設定

してください。

- **3.41 MMRP、または 3.42 MMRP-Plus のマスター、スレーブ、分散マスター、分散スレーブポート**
- **3.17 スパニングツリープロトコル(STP/RSTP/MSTP)で Blocking 状態になる可能性のあるポート**
- **LLDP による疑似リンクダウン設定のあるポート**

3.30.3 qos max-bandwidth

qp1～qp8 の 8 種類の QoS プロファイルの最大帯域をポートごとに設定します。最大帯域は Kbps で設定し、各 QoS プロファイルは 64～10000000 Kbps の範囲で設定可能です。最大帯域の設定を無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

qos qosprofile qp1 | qp2 | qp3 | qp4 | qp5 | qp6 | qp7 | qp8 port <PORTRANGE> max-bandwidth <VALUE>

no qos qosprofile qp1 | qp2 | qp3 | qp4 | qp5 | qp6 | qp7 | qp8 port <PORTRANGE> max-bandwidth

qp1～qp8	最大帯域を設定する QoS プロファイル(優先度は qp1 から qp8 の順で高)
PORTRANGE	最大帯域を設定するポート番号(複数指定可能)
VALUE	上で指定したポートから送信される QoS プロファイルのフレームの最大帯域 <64-10000000(Kbps)>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1 に対し、qp1 の QoS プロファイルの最大帯域を 64000 Kbps に設定します。

```
> enable
# configure terminal
(config)# qos qosprofile qp1 port 1 max-bandwidth 64000
```

関連コマンド

show qos, show running-config

注意事項

帯域は 64～10000000 Kbps の範囲の任意の数値を設定できますが、実際の動作時には 64 の整数倍に切り捨てられます。

実際の最大帯域は、負荷の状態に依存して変動する可能性があります。設定値を厳密に保証するものではありません。

同一ポート、同一 QoS プロファイルに最大帯域＜最低帯域となる値を設定することはできません。

本コマンドは Apresia4328 には対応していません。

3.30.4 qos weight

qp1～qp8 の 8 種類の QoS プロファイルの重みを設定します。Strict Priority キューに設定する場合はキューの重みを 0 に設定してください。Strict Priority キューに設定したキューが最優先されます。その他の重みを設定した場合については QoS プロファイルの重みと、qp1～qp8 のすべての重みの合計との比から実際の最低帯域が決定されます。最低帯域は weighted-round-robin ではパケット数、deficit-round-robin では出力するバイト数に反映されます。バイト数には MAC フレームの宛先 MAC アドレスから CRC までが含まれます。重みの設定を無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

qos qosprofile qp1 | qp2 | qp3 | qp4 | qp5 | qp6 | qp7 | qp8 port <PORTRANGE> weight <VALUE>
no qos qosprofile qp1 | qp2 | qp3 | qp4 | qp5 | qp6 | qp7 | qp8 port <PORTRANGE> weight

qp1～qp8	重みを設定する QoS プロファイル(優先度は qp1 から qp8 の順で高)
PORTRANGE	重みを設定するポート番号(複数指定可能)
VALUE	各キューの重み <0-15>

表 3-36 deficit-round-robin における qos weight 設定範囲一覧表

シリーズ名称		設定可能範囲	設定範囲制限 (最大設定値－最小設定値≦N) [ただし 0 は除く]
Apresia3400 シリーズ		<0-10>	6 ※1
Apresia 4300 シリーズ	Apresia 4328 シリーズ	<0-10>	6
	Apresia 4348 シリーズ	<0-15>	15
Apresia5400 シリーズ		<0-10>	6
Apresia13000 シリーズ		Apresia13000-24GX-PSR:<0-12> Apresia13000-48X：<0-15>	Apresia13000-24GX-PSR：8 ※2 Apresia13000-48X：15

※1 設定できない例：2 と 10、1 と 8 など。設定できる例：4～10、3～9 など。
※2 設定できない例：2 と 12、1 と 10 など。設定できる例：4～12、2～10 など。

デフォルト

各キューの重み：0

コマンドモード

CONFIG

使用例

(1) 設定不可例(Apresia3424 シリーズ)

```
> enable
# configure terminal
(config)# qos algorithm deficit-round-robin
(config)# qos qosprofile qp1 port 1 weight 10
(config)# qos qosprofile qp2 port 1 weight 1
Difference between minimum and maximum DRR weight must be within 6.
```

(2) 設定可能例(Apresia3424 シリーズ)

```
> enable
# configure terminal
(config)# qos algorithm deficit-round-robin
(config)# qos qosprofile qp1 port 1 weight 7
(config)# qos qosprofile qp2 port 1 weight 1
(config)#
```

関連コマンド

show qos, show running-config

注意事項

deficit-round-robin の時は、設定した<VALUE>の 2 のべき乗の値が実際の重みとなります。

実際の最低帯域は、負荷の状態に依存して変動する可能性があります。設定値を厳密に保証するものではありません。

deficit-round-robin における qos weight の設定範囲は機種ごとに異なります。また、設定可能な範囲は設定状況により変わります。表 3-36 を参考にしてください。

3.30.5 qos algorithm

QoS のスケジュールアルゴリズムを deficit round robin に設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

qos algorithm deficit-round-robin
no qos algorithm

デフォルト

weighted-round-robin

コマンドモード

CONFIG

使用例

(1) スケジュールアルゴリズムを deficit-round-robin に設定します。

(2) スケジュールアルゴリズムを weighted-round-robin に戻します。

```
(config)# qos algorithm deficit-round-robin
(config)# no qos algorithm
```

関連コマンド

show qos, show running-config

注意事項

設定しない場合のスケジュールアルゴリズムは weighted round robin になります。

"qos weight"の設定がある状態で、"[no] qos algorithm"コマンドによりスケジュールアルゴリズムを変更すると、内部動作に変更があるため、通信に影響を及ぼします。通信中の設定変更には注意してください。

3.30.6 qos burst-size

QoS のバーストサイズを設定します。バーストサイズは最低帯域用の min、最大帯域用の max があり、それぞれ個別に任意の数値を設定できます。設定を無効にする場合は、no コマンドを使用してください。

バーストサイズの設定を省略した場合は、デフォルト値が設定されます。

コマンドシンタックス

qos burst-size min | max <BURST_SIZE>

no qos burst-size min | max

min　最低帯域用

max　最大帯域用

BURST_SIZE　トラフィック量を測る際に使用するバーストサイズ <32～131072(Kbit)>

- 任意の数値を設定できるが、動作時には表 3-37 で示す値に切り捨て(2^n Kbps 単位、n=5～17)

表 3-37 設定されるバーストサイズ

バーストサイズ設定値
32
64
128
256
512
1024
2048
4096
8192

バーストサイズ設定値
16384
32768
65536
131072

デフォルト

バーストサイズ：128(Kbit)

コマンドモード

CONFIG

使用例

(1) 最大帯域用のバーストサイズを 1024 Kbit に設定します。
(2) 最大帯域用のバーストサイズをデフォルトに戻します。

```
(config)# qos burst-size max 1024
(config)# no qos burst-size max
```

関連コマンド

show qos, show running-config

注意事項

本コマンドは Apresia4328 には対応していません。

3.30.7 qos mapping

各 QoS プロファイルに対応する IEEE 802.1Q(IEEE 802.1p)プライオリティ値を設定します。0～7 の範囲が設定可能です。

コマンドシンタックス

qos qosprofile qp1 | qp2 | qp3 | qp4 | qp5 | qp6 | qp7 | qp8 mapping <VALUE>
no qos qosprofile qp1 | qp2 | qp3 | qp4 | qp5 | qp6 | qp7 | qp8 mapping

qp1～qp8　IEEE 802.1Q(IEEE 802.1p)プライオリティ値を設定する QoS プロファイル
VALUE　IEEE 802.1Q(IEEE 802.1p)プライオリティ値

デフォルト

qp8：プライオリティ 7
qp7：プライオリティ 6
qp6：プライオリティ 5
qp5：プライオリティ 4
qp4：プライオリティ 3
qp3：プライオリティ 0
qp2：プライオリティ 2
qp1：プライオリティ 1

コマンドモード

CONFIG

使用例

(1) qp1 を IEEE 802.1Q(IEEE 802.1p)プライオリティ値：0 に対応させます。

```
> enable
# configure terminal
(config)# qos qosprofile qp1 mapping 0
```

関連コマンド

show qos, show running-config

注意事項

IEEE 802.1Q(IEEE 802.1p)プライオリティ値のマッピングが無い QoS プロファイルをパケットフィルター2 で設定するとエラーメッセージが表示されます。エラーメッセージが表示された場合の動作は保証されません。再度設定してください。

3.30.8 show qos

QoS の設定状態を表示します。QoS 機能無効時は、QoS 機能の設定状態以外は表示されません。

コマンドシンタックス

show qos [port <PORTRANGE>]

PORTRANGE　　ポート番号(複数指定可能)

コマンドモード

VIEW, ENABLE

使用例

(1) QoS の設定状態を表示します。

```
# show qos
  QoS: Enabled
                          802.1Q priority
  qosprofile              01234567
  ----------------------------------------
      qp8                 -------*
      qp7                 ------*-
      qp6                 -----*--
      qp5                 ----*---
      qp4                 ---*----
      qp3                 *-------
      qp2                 --*-----
      qp1                 -*------
```

```
                 queue weight &  minimum / maximum bandwidth(Kbit/s)
     wgt = queue weight  min = minimum bandwidth  max = maximum bandwidth
  port           qp8     qp7     qp6     qp5     qp4     qp3     qp2     qp1
  ---------------------------------------------------------------------------
   1  wgt          8       7       6       5       4       3       2       1
      min      80000   69952   59968   49984   40000   29952   19968    9984
      max      99968   89984   80000   69952   59968   49984   40000   29952
   2  wgt          8       7       6       5       4       3       2       1
      min      80000   69952   59968   49984   40000   29952   19968    9984
      max      99968   89984   80000   69952   59968   49984   40000   29952
   3  wgt          8       7       6       5       4       3       2       1
      min      80000   69952   59968   49984   40000   29952   19968    9984
      max      99968   89984   80000   69952   59968   49984   40000   29952
                                  ・
                                 中略
                                  ・
  48  wgt          8       7       6       5       4       3       2       1
      min      80000   69952   59968   49984   40000   29952   19968    9984
      max      99968   89984   80000   69952   59968   49984   40000   29952
  49  wgt          8       7       6       5       4       3       2       1
      min      80000   69952   59968   49984   40000   29952   19968    9984
      max      99968   89984   80000   69952   59968   49984   40000   29952
  50  wgt          8       7       6       5       4       3       2       1
      min      80000   69952   59968   49984   40000   29952   19968    9984
      max      99968   89984   80000   69952   59968   49984   40000   29952

 scheduler algorithm: deficit-round-robin
 burst-size  min:     128(Kbit)
             max:     128(Kbit)
```

QoS	：QoS 機能の設定状態
Disabled	：QoS 機能無効
Enabled	：QoS 機能有効
qosprofile	：qos プロファイル名
wgt	：重みの設定状態
min	：最低帯域の設定状態
max	：最大帯域の設定状態
scheduler algorithm	：QoS スケジュールアルゴリズム
weighted-round-robin	：weighted round robin アルゴリズム
deficit-round-robin	：deficit round robin アルゴリズム
burst-size	
min	：最低帯域用 Burst Size
max	：最大帯域用 Burst Size

関連コマンド

注意事項

表示される帯域は、ユーザーが設定した値から 64 の整数倍に切り捨てられた値となります。

3.31 NTP

3.31.1 ntp server

NTP サーバーの指定を行います。NTP サーバーは 1 つだけ設定することができます。

コマンドシンタックス

ntp server <IPADDR>
no ntp server
IPADDR　　NTP サーバーの IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) NTP サーバーとして、192.168.0.1 を指定します。

```
> enable
# configure terminal
(config)# ntp server 192.168.0.1
```

関連コマンド

show ntp, show running-config

注意事項

NTP サーバーの指定がない場合に"no ntp server"コマンドを発行しても、そのコマンドは無視されます。

3.31.2 ntp enable

NTP による時刻合わせを開始します。NTP による時刻合わせは、本装置の起動時、本コマンドの発行時、及び特に指定ない限り約 36 時間ごとに 1 回行われます。

コマンドシンタックス

[no] ntp enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) NTP サーバーとして、192.168.0.1 を指定します。
(2) 指定した NTP サーバーを元に NTP による時刻合わせを開始します。
(3) NTP による時刻合わせを停止します。

```
> enable
# configure terminal
(config)# ntp server 192.168.0.1
(config)# ntp enable
(config)# no ntp enable
```

関連コマンド

show ntp, show running-config

注意事項

本コマンドの発行前に、NTP サーバーを指定することが必要です。

3.31.3 ntp interval

NTP による時刻合わせの間隔を変更します。

コマンドシンタックス

ntp interval <HOUR>
no ntp interval
HOUR　　時刻合わせの間隔 <1-48(時間)>

デフォルト

36(時間)

コマンドモード

CONFIG

使用例

(1) NTP サーバーとして、192.168.0.1 を指定します。
(2) NTP による時刻合わせを 12 時間ごとに行います。
(3) 指定した NTP サーバーを元に NTP による時刻合わせを開始します。

```
> enable
# configure terminal
(config)# ntp server 192.168.0.1
(config)# ntp interval 12
(config)# ntp enable
```

関連コマンド

show ntp, show running-config

注意事項

本コマンドを有効にするには、"ntp enable"を無効に設定する必要があります。"ntp interval"を設定後、有効に再度設定してください。

3.31.4 show ntp

NTP 構成情報を表示します。

コマンドシンタックス

show ntp

コマンドモード

VIEW, ENABLE

使用例

(1) NTP 構成情報を出力します。

```
> enable
# show ntp
NTP Configurations
    NTP Server:   192.168.0.250
Interval  :   36 (hour)
    Status    :   enable
```

NTP Server	：NTP サーバーの IP アドレス
Interval	：サーバーに問い合わせを行う周期
Status	：動作状況
enable	：有効
disable	：無効

関連コマンド

注意事項

3.32 時刻、タイムゾーン

3.32.1 clock set

時刻の設定を行います。

コマンドシンタックス

clock set <HH:MM:SS> [<YYYYMMDD>]

HH:MM:SS	時刻(24 時間表示) • HH：時間 • MM：分 • SS：秒
YYYYMMDD	年月日 • YYYY：年(西暦 4 桁) • MM：月 • DD：日

デフォルト

現在時刻(＝工場出荷時に時刻を設定)

コマンドモード

CONFIG

使用例

(1) 時刻として、午前 7 時 10 分 05 秒を指定します。

(2) 時刻として、午後 3 時 30 分 05 秒を、日付として 2006 年 7 月 1 日を指定します。

```
> enable
# configure terminal
(config)# clock set 07:10:05
(config)# clock set 15:30:05 20060701
```

関連コマンド

show clock

注意事項

UTC(協定世界時：Coordinated Universal Time)の 2038 年 1 月 19 日 3 時 14 分 8 秒以降の日時を正しく設定、及び表示することができません。なお、タイムゾーン("timezone"項参照)のデフォルト値は、日本標準時(UTC+09:00:00)となっていますので、注意してください。

3.32.2 timezone

UTC からのオフセットとしてのタイムゾーンの設定を行います。デフォルトのタイムゾーンに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

timezone <+HH:MM:SS> | <-HH:MM:SS>
no timezone

+HH:MM:SS	UTC からのオフセットが正値の場合(24 時間表示) • HH：時間 • MM：分 • SS：秒
-HH:MM:SS	UTC からのオフセットが負値の場合(24 時間表示) • HH：時間 • MM：分 • SS：秒

デフォルト

UTC+09:00:00

コマンドモード

CONFIG

使用例

(1) タイムゾーンとして、UTC から+7 時間を指定します。
(2) タイムゾーンとして、UTC から-6 時間 30 分を指定します。

```
> enable
# configure terminal
(config)# timezone +07:00:00
(config)# timezone -06:30:00
```

関連コマンド

show running-config, show timezone

注意事項

本コマンドはリブート後反映されます。本コマンドの実行後は、フラッシュメモリーへの書き込み(3.50.2 "copy running-config flash-config, write memory"項参照)を行い、本装置のリブートを行ってください。

3.32.3 show clock

時刻情報を表示します。

コマンドシンタックス

show clock

コマンドモード

VIEW, ENABLE

使用例

(1) 時刻情報を出力します。

```
> enable
# show clock
 Sun Aug 01 17:53:47 2004
```

関連コマンド

注意事項

3.32.4 show timezone

現在動作に反映されているタイムゾーンと、リブート後に使用する設定されているタイムゾーンを表示します。

コマンドシンタックス

show timezone

コマンドモード

VIEW, ENABLE

使用例

(1) タイムゾーンの情報を表示します。

```
> show timezone
timezone(current): UTC+09:00:00
timezone(next)   : UTC+09:00:00
```

関連コマンド

注意事項

3.33 ターミナル設定

3.33.1 line

LINE モードへ移行します。LINE モードは、コンソールラインモード(コンソールポートからのターミナル接続)、及びバーチャルターミナルラインモード(TELNET/SSH による接続)の 2 種類あります。バーチャルターミナルラインは、ライン番号を指定することにより、設定するラインごとに設定が行えます。

コマンドシンタックス

line console | <*VIRTUALTERMINAL*>

VIRTUALTERMINAL = vty <LINENUMBER> [<ENDING_LINENUMBER>]

console	コンソールラインモード
vty	バーチャルターミナルラインモード
LINENUMBER	ライン番号 <0-7>(範囲指定する場合は先端ライン番号)
ENDING_LINENUMBER	範囲指定する場合の終端ライン番号 <0-7>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) コンソールラインの設定を変更します。
(2) バーチャルターミナルライン(ライン番号 0)の設定を行います。
(3) バーチャルターミナルライン(ライン番号 1～7)の設定を行います。

```
(config)# line console
(config-line)# exec-timeout 120
(config-line)# exit
(config)# line vty 0
(config-line)# exec-timeout 120
(config-line)# exit
(config)# line vty 1 7
(config-line)# exec-timeout 10
```

関連コマンド

exec-timeout, show users, show running-config

注意事項

3.33.2 exec-timeout

シリアルコンソール、及び TELNET/SSH での接続時における無通信時のタイムアウト時間を設定します。タイムアウト後はログインプロンプトの状態になります。設定をデフォルト値に戻す場合は、no コマンド使用してください。

本パラメーターの設定は、設定変更後に行われたログインに対して有効になります(設定時にすでに

成立しているログインには、反映されません)。

コマンドシンタックス

exec-timeout <MINUTES> [<SECONDS>]
no exec-timeout

MINUTES	タイムアウト時間(分単位) <0-35791(分)>
SECONDS	タイムアウト時間(秒単位) <0-2147483(秒)> • タイムアウトの機能を有効にするには、30 秒以上の時間を指定 • 0 分 0 秒を指定した場合はタイムアウトしない

デフォルト

300(秒)

コマンドモード

LINE

使用例

(1) TELNET/SSH でログインした時のタイムアウト時間を 1 分に設定します。
(2) 設定したタイムアウト時間を無効にしてデフォルト(300 秒)に戻します。

```
> enable
# configure terminal
(config)# line vty 0 4
(config-line)# exec-timeout 1 0
(config-line)# no exec-timeout
```

関連コマンド

show running-config

注意事項

タイムアウト機能を無効にしたコンソールで、CONFIG モードへ入ったまま放置しておくと、他のコンソールから CONFIG モードへ入ることができなくなります。タイムアウト機能を無効にして使用する場合は、使用後にログアウトするか、VIEW モード、もしくは ENABLE モードにするようにしてください。また、タイムアウト機能の設定に関わらずコンソールのログイン状態を保持したまま放置するのはセキュリティー上お勧めできません。

コンソールケーブルや LAN ケーブルを抜いただけでは、ログアウトしません(モードも遷移しません)。

TELNET/SSH にてログインし、CONFIG モードになっている最中に通信障害などにより通信断が発生し、他のログインから CONFIG モードに移行できなくなった場合、TCP のタイムアウトを待つか、再度 TELNET/SSH にてログイン、もしくはコンソールにて

ログインし、3.34.5 "telnet disconnect"コマンド、及び 3.35.10 "sshd disconnect" コマンドにて回避できます。

3.33.3 terminal length

端末画面出力の一時停止機能を無効にします。no オプションを指定すると、一時停止機能が有効になります。本設定はすべてのセッションに共通で 1 つだけ設定可能です。

本コマンドを指定しない時は、各コマンドの実行時に、コンソールでは 23 行ごと、TELNET/SSH では "terminal が通知する長さ - 1"ごとに画面の表示を停止します。

コマンドシンタックス

terminal length 0
terminal no length

デフォルト

なし(＝一時停止機能有効)

コマンドモード

VIEW, ENABLE, CONFIG

使用例

(1) 端末画面出力の一時停止機能を無効にします。

```
(config)# terminal length 0
```

関連コマンド

show running-config

注意事項

3.33.4 terminal monitor

3.38.4 "logging monitor"コマンドで設定したログメッセージ、及び 3.61.4 "debug"コマンドで指定したデバッグ情報をターミナルに出力します。本設定は設定したログインセッションにのみ有効です。

コマンドシンタックス

terminal [no] monitor

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) ログメッセージ、及びデバッグ情報をターミナルに出力します。

```
# terminal monitor
```

関連コマンド

logging monitor, debug

注意事項

3.34 TELNET

TELNET の設定には、ALLOW モードと DENY モードがあります。ALLOW モードは、デフォルトですべてのクライアントからの TELNET 接続を許可します。DENY モードは、デフォルトですべてのクライアントからの接続を拒否します。

接続管理したいクライアントの IP アドレス、あるいはサブネット情報を TELNET アクセス管理リストに登録することによって、TELNET 接続制限を実現できます。

ALLOW モードの場合：TELNET アクセス管理リストの内容が接続拒否対象となります。

DENY モードの場合　：TELNET アクセス管理リストの内容が接続許可対象となります。

3.34.1 telnet mode deny

本コマンドによって、ALLOW モードと DENY モードを切り替えます。切り替えの前後での TELNET アクセス管理リストの内容は引き継がれます。

コマンドシンタックス

[no] telnet mode deny

デフォルト

no deny(＝ALLOW モード)

コマンドモード

CONFIG

使用例

(1) DENY モードに遷移します。

(2) ALLOW モードに遷移します。

```
> enable
# configure terminal
(config)# telnet mode deny
(config)# no telnet mode deny
```

関連コマンド

show telnet list, show running-config

注意事項

モード切り替えによる接続制限の変更は、変更前に保持されているコネクションに対しては無効です。

3.34.2 telnet server

TELNET サーバー機能を無効にします。無効にした場合でも接続中のセッションは使用可能です。

コマンドシンタックス

[no] telnet server disable

デフォルト
no disable(＝有効)

コマンドモード
CONFIG

使用例
(1) TELNET サーバー機能を無効にします。
(2) TELNET サーバー機能を有効にします。

```
> enable
# configure terminal
(config)# telnet server disable
(config)# no telnet server disable
```

関連コマンド
show telnet server, show running-config

注意事項

3.34.3 telnet ip

指定された IP アドレスを TELNET アクセス管理リストに追加します。

コマンドシンタックス
telnet ip <IP_LISTNO> <IPADDR>
no telnet ip <IP_LISTNO>

IP_LISTNO	追加する IP アドレスに対応した IP リスト番号 <1-255>
IPADDR	追加する IP アドレス

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) IP アドレス：192.168.0.1 を IP リスト番号：1 として TELNET アクセス管理リストに追加します。
(2) IP リスト番号：1 を TELNET アクセス管理リストから削除します。

```
> enable
# configure terminal
(config)# telnet ip 1 192.168.0.1
(config)# no telnet ip 1
```

関連コマンド

show telnet list, show running-config

注意事項

3.34.4 telnet subnet

指定されたサブネットアドレスを TELNET アクセス管理リストに追加します。

コマンドシンタックス

telnet subnet <SUBNET_LISTNO> <NETADDR> <NETMASK>

no telnet subnet <SUBNET_LISTNO>

SUBNET_LISTNO	追加するサブネットに対応したサブネットリスト番号 <1-255>
NETADDR	追加するサブネットのネットワークアドレス
NETMASK	サブネットマスク

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) サブネットアドレス：192.168.0.0、サブネットマスク：255.255.255.0、サブネットリスト番号：2 として TELNET アクセス管理リストに追加します。

(2) サブネットリスト番号：2 を TELNET アクセス管理リストから削除します。

```
> enable
# configure terminal
(config)# telnet subnet 2 192.168.0.0 255.255.255.0
(config)# no telnet subnet 2
```

関連コマンド

show telnet list, show running-config

注意事項

3.34.5 telnet disconnect

すべての TELNET コネクションを強制切断します。

コマンドシンタックス

telnet disconnect

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) すべての TELNET コネクションを切断します。

```
> enable
# telnet disconnect
```

関連コマンド

注意事項

3.34.6 show telnet server

クライアントからの TELNET 接続の可否状態を表示します。

コマンドシンタックス

show telnet server

コマンドモード

VIEW, ENABLE

使用例

(1) TELNET アクセス可否状態を表示します。

```
> enable
# show telnet server
 Telnet server status
 Status     :   ENABLE

 Mode       :   ALLOW
```

Status	：TELNET サーバー機能状態
ENABLE	：有効
DISABLE	：無効
Mode	：TELNET サーバー機能有効時の動作モード
ALLOW	：ALLOW モード
DENY	：DENY モード

関連コマンド

注意事項

3.34.7 show telnet list

TELNET アクセス管理リストを表示します。

コマンドシンタックス

show telnet list

コマンドモード

VIEW, ENABLE

使用例

(1) TELNET アクセス管理リストを表示します。

```
> enable
# show telnet list
Telnet status.
  Server:  ENABLE
  Mode:    DENY
  ---------------------------------
  IP access list
  ---------------------------------
    1   192.168.0.1
    2   192.168.0.3
    3   192.168.0.4
  ---------------------------------
  Subnet access list
  ---------------------------------
    1   192.168.0.0   255.255.255.0
    2   192.168.1.0   255.255.255.0
```

Mode	：TELNET サーバー機能有効時の動作モード
ALLOW	：ALLOW モード
DENY	：DENY モード
IP access list	：TELNET アクセス管理 IP アドレスリスト番号と、TELNET アクセス管理 IP アドレス
Subnet access list	：TELNET アクセス管理ネットワークアドレスリスト番号と、TELNET アクセス管理ネットワークアドレス/サブネットマスク

関連コマンド

注意事項

3.35 SSH

SSH(Secure Shell)は、ネットワークを介してログイン、コマンドの実行の際に、ネットワーク上を流れるデータを暗号化して、通信の漏洩を防ぎ安全性を高めるほか、データを圧縮し、送受信を効率的に行うための機能です。

SSH プロトコルバージョン 1、及び SSH プロトコルバージョン 2 に対応しています。

SSH サーバーの設定変更後、SSH サーバーが起動するまでに時間がかかる場合があります。"show sshd server"コマンドで、SSH サーバーの状態が ENABLE 状態であることを確認してください。

公開鍵認証方式は未サポートです。

3.35.1 sshd keygen rsa

RSAホスト鍵対(SSHプロトコルバージョン2)を生成します。鍵長は<KEYLENGTH>で指定してください。

コマンドシンタックス

sshd keygen rsa [<KEYLENGTH>]

KEYLENGTH　　鍵長 <512-4096(ビット)>

デフォルト

1024(ビット)(＝<KEYLENGTH>の指定省略時)

コマンドモード

ENABLE

使用例

(1) 鍵長を 600 ビットに設定します。

```
# sshd keygen rsa 600
% Generating RSA key pair for version 2 protocol. Wait for a while.
% Done.
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAEwAvwGScYzSuIk9zM+H99JcDTCAF/y6V+kTEhAeZlGCKwrB
2zm/h0+Bk7lxV2kNC3MJKZjMZEycRfbhlqU6tvMfaAYsQ/9CI6U2BEu3 root@
```

関連コマンド

show sshd key rsa

注意事項

本コマンドで RSA ホスト鍵対生成後、3.50.2 "write memory"コマンドを実行してフラッシュメモリーに書き込んでください。"write memory"コマンドを実行せずに装置再起動すると RSA ホスト鍵対は空ファイルとなります。

3.35.2 sshd keygen rsa1

RSAホスト鍵対(SSHプロトコルバージョン1)を生成します。鍵長は<KEYLENGTH>で指定してください。

コマンドシンタックス

sshd keygen rsa1 [<KEYLENGTH>]

KEYLENGTH　　鍵長 <512-4096(ビット)>

デフォルト

1024(ビット)(＝<KEYLENGTH>の指定省略時)

コマンドモード

ENABLE

使用例

(1) 鍵長を600ビットに設定します。

```
# sshd keygen rsa1 600
% Generating RSA key pair for version 1 protocol. Wait for a while.
% Done.
600 35 319883887659555282645202108600162152997740458784392112384147193460403166
0238081447509484718312459886043903469704363051001379927269202998814109807132855
93532326025677061643749648244 3 root@
```

関連コマンド

show sshd key rsa1

注意事項

本コマンドでRSAホスト鍵対生成後、3.50.2 "write memory"コマンドを実行してフラッシュメモリーに書き込んでください。"write memory"コマンドを実行せずに装置再起動するとRSAホスト鍵対は空ファイルとなります。

3.35.3 sshd server

SSHサーバー機能を有効にします。無効にする場合は、noコマンドを使用してください。

コマンドシンタックス

[no] sshd server

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ssh サーバー機能を有効にします。

(2) ssh サーバー機能を無効にします。

```
# configure terminal
(config)# sshd server
(config)# no sshd server
```

関連コマンド

sshd keygen rsa, show sshd key rsa1, show sshd server, show running-config

注意事項

SSH サーバーを有効にするには、RSA ホスト鍵対(SSH プロトコルバージョン 1、及び SSH プロトコルバージョン 2 の両バージョン)を先に生成する必要があります。

SSH サーバー機能のみをサポートしており、クライアント機能をサポートしておりません。

"sshd server-keybits"コマンドの設定値を大きくするほど、SSH サーバーの起動に時間がかかります。鍵長が 2048 ビットの場合、最大で 1～数分かかることがあります。

本コマンドを実行した場合、すべての SSH コネクションは切断されます。

3.35.4 sshd keepalive disable

SSH サーバーのキープアライブ機能を無効にします。本機能を有効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] sshd keepalive disable

デフォルト

no disable(＝有効)

コマンドモード

CONFIG

使用例

(1) キープアライブ機能を無効にします。

(2) キープアライブ機能を有効にします。

```
# configure terminal
(config)# sshd keepalive disable
```

```
(config)# no sshd keepalive disable
```

関連コマンド

show running-config

注意事項

3.35.5 sshd port

SSH サーバーが受け付けるポート番号を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

sshd port <PORT>
no sshd port
PORT　　ポート番号 <1024-65534>

デフォルト

22

コマンドモード

CONFIG

使用例

(1) ポート番号を 2000 に設定します。
(2) 設定したポート番号を削除します。

```
# configure terminal
(config)# sshd port 2000
(config)# no sshd port
```

関連コマンド

show running-config

注意事項

3.35.6 sshd server-keybits

SSH プロトコルバージョン１のセッション鍵交換時に使用される SSH サーバー鍵の長さを設定します。デフォルト値に戻す場合は、no コマンドを使用してください。SSH サーバー鍵は自動生成され、装置に保存されません。

コマンドシンタックス

sshd server-keybits <KEYLENGTH>
no sshd server-keybits
KEYLENGTH　　鍵長 <512-2048(ビット)>

デフォルト
768(ビット)

コマンドモード
CONFIG

使用例
(1) 鍵長を 800 ビットに設定します。
(2) 設定した鍵長を無効にします。

```
# configure terminal
(config)# sshd server-keybits 800
(config)# no sshd server-keybits
```

関連コマンド
show running-config

注意事項

3.35.7 sshd mode deny

SSH サーバーへのアクセス管理設定を ALLOW モード(デフォルト)から DENY モードへ切り替えます。設定をデフォルトモードへ戻す場合は、no コマンドを使用してください。

"sshd mode deny"コマンドは sshd ip/subnet コマンドで指定した IP アドレスやネットワークから SSH サーバーへの接続を許可、または拒否します。ALLOW モードは指定した IP アドレスやネットワークからの接続を拒否し、DENY モードは指定した IP アドレスやネットワークからの接続のみを許可します。

コマンドシンタックス
[no] sshd mode deny

デフォルト
no deny(＝ALLOW モード)

コマンドモード
CONFIG

使用例
(1) SSH サーバーへのアクセス管理設定を DENY モードへ切り替えます。
(2) アクセス管理設定を ALLOW モード(デフォルト)へ戻します。

```
# configure terminal
(config)# sshd mode deny
(config)# no sshd mode deny
```

関連コマンド
show sshd list, show sshd server, show running-config

注意事項

3.35.8 sshd ip

アクセス管理リストに IP アドレスを追加します。設定を削除する場合は、no コマンドを使用してください。

"sshd ip"コマンドは、アクセス管理リストへの IP アドレスの追加・削除を行います。アクセス管理リストは SSH サーバーへの接続を許可・拒否を設定するために用いられます。接続の許可・拒否の設定は"sshd mode deny"コマンドを使用し、デフォルトではアクセス管理リストで指定された IP アドレスからの接続を拒否します。

コマンドシンタックス

sshd ip <ID> <IPADDR>
no sshd ip <ID>

ID	整数値 <1-8>
ADDR	IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) アクセス管理リストに IP アドレスを追加します。
(2) 設定した IP アドレスを削除します。

```
# configure terminal
(config)# sshd ip 1 172.17.20.1
(config)# no sshd ip 1
```

関連コマンド

show sshd list, show running-config

注意事項

3.35.9 sshd subnet

アクセス管理リストにネットワークアドレスを追加します。設定を削除する場合は、no コマンドを使用してください。

"sshd subnet"コマンドは、アクセス管理リストへのネットワークアドレスの追加・削除を行います。アクセス管理リストは SSH サーバーへの接続を許可・拒否を設定するために用いられます。接続の許可・拒否の設定は"sshd mode deny"コマンドを使用し、デフォルトではアクセス管理リストで指定されたネットワークからの接続を拒否します。

コマンドシンタックス

sshd subnet <ID> <NETADDR> <NETMASK>

no sshd subnet <ID>

ID	1-8 の整数値を指定
NETADDR	ネットワークアドレス
NETMASK	サブネットマスク

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) アクセス管理リストにネットワークアドレスを追加します。

(2) 追加したネットワークアドレスを削除します。

```
# configure terminal
(config)# sshd subnet 1 172.17.20.0 255.255.255.0
(config)# no sshd subnet 1
```

関連コマンド

show sshd list, show running-config

注意事項

3.35.10 sshd disconnect

すべての SSH コネクションを強制切断します。

コマンドシンタックス

sshd disconnect

デフォルト

なし

コマンドモード

ENABLE

使用例

(1) すべての SSH コネクションを切断します。

```
# sshd disconnect
```

関連コマンド

注意事項

3.35.11 copy file ssh-key

TFTP サーバー、または SD メモリーカードに保存されている RSA ホスト鍵対をダウンロードします。<FILE>で指定したファイルを秘密鍵、<FILE>で指定したファイルに拡張子".pub"を追加したファイルを公開鍵としてダウンロードします。秘密鍵「ssh-rsa1-key」、公開鍵「ssh-rsa1-key.pub」が保存されている場合、<FILE>に"ssh-rsa1-key"を指定してください。装置のフラッシュメモリーへ RSA ホスト鍵対を保存する場合はダウンロード後、"write memory"コマンドを実行してください。

コマンドシンタックス

copy (tftp <IPADDR>) | memory-card <FILENAME> ssh-rsa-key | ssh-rsa1-key

IPADDR　TFTP サーバーの IP アドレス

FILENAME　RSA ホスト鍵対ファイル名 <1-128(文字)>

- ASCII コードの印字可能な文字の内、["][?]を除いた文字のみ使用可能

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) TFTP サーバーの RSA ホスト鍵対(SSH プロトコルバージョン 2)をダウンロードします。

```
> enable
# copy tftp 172.21.29.110 test-key ssh-rsa-key
```

(2) SD メモリーカードの RSA ホスト鍵対(SSH プロトコルバージョン 2)をダウンロードします。

```
> enable
# copy memory-card test-key ssh-rsa-key
```

関連コマンド

show sshd key rsa, show sshd key rsa1

注意事項

RSA ホスト鍵対ファイルに使用できる改行コードは、LF のみです。CR+LF、または CR は使用できません。

3.35.12 copy ssh-key file

本装置に保存されている RSA ホスト鍵対を TFTP サーバー、または SD メモリーカードへアップロードします。<FILE>で指定したファイルを秘密鍵、<FILE>で指定したファイルに拡張子".pub"を追加したファイルを公開鍵としてアップロードします。秘密鍵「ssh-rsa1-key」、公開鍵「ssh-rsa1-key.pub」が保存されている場合、<FILE>に"ssh-rsa1-key"を指定してください。

コマンドシンタックス

copy ssh-rsa-key | ssh-rsa1-key (tftp <IPADDR>) | memory-card <FILENAME>

IPADDR　TFTP サーバーの IP アドレス

FILENAME　RSA ホスト鍵対ファイル名 <1-128(文字)>

- ASCII コードの印字可能な文字の内、["][?]を除いた文字のみ使用可能

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) TFTP サーバーへ RSA ホスト鍵対(SSH プロトコルバージョン 2)をアップロードします。

```
> enable
# copy ssh-rsa-key tftp 172.21.29.110 test-key
```

(2) SD メモリーカードへ RSA ホスト鍵対(SSH プロトコルバージョン 2)をアップロードします。

```
> enable
# copy ssh-rsa-key memory-card test-key
```

関連コマンド

show sshd key rsa, show sshd key rsa1

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.35.13 show sshd server

SSH サーバーの状態を表示します。

コマンドシンタックス

show sshd server

コマンドモード

VIEW, ENABLE

使用例

(1) SSH サーバーの状態を表示します。

```
# show sshd server
SSH server status
 Status    : STARTING
 Mode      : ALLOW
 SSHv1 Key : VALID
 SSHv2 Key : VALID
```

Status	：SSH サーバーの状態
ENABLE	：有効、かつサーバーが起動処理完了し SSH 接続可能
STARTING	：有効だが、サーバーが起動処理中のため SSH 接続不可
ERROR	：有効だが、サーバーが異常終了し SSH 接続不可
DISABLE	：無効
Mode	：SSH サーバー機能有効時の動作モード
ALLOW	：ALLOW モード
DENY	：DENY モード
SSHv1 Key	：RSA ホスト鍵対(SSH プロトコルバージョン 1)の状態
SSHv2 Key	：RSA ホスト鍵対(SSH プロトコルバージョン 2)の状態
VALID	：有効
INVALID	：無効

関連コマンド

注意事項

RSA ホスト鍵対の状態(SSHv1 Key/SSHv2 Key)が共に INVALID 状態で、SSH の設定変更を実施した場合、SSH サーバーが停止し ERROR 状態となることがあります。正常な RSA ホスト鍵対を作成、またはダウンロードし、"no sshd server"コマンド実行後、再度 "sshd server"コマンドを実行することで復旧します。

3.35.14 show sshd list

SSH サーバーのアクセス管理リストを表示します。

コマンドシンタックス

show sshd list

コマンドモード

VIEW, ENABLE

使用例

(1) SSH サーバーのアクセス管理リストを表示します。

```
# show sshd list
SSH server status
  Status: ENABLE
  Mode  : ALLOW

 --------------------------
 IP access list
 --------------------------
  1      172.17.20.1

 --------------------------
 Subnet access list
 --------------------------
  1      172.17.20.0 255.255.255.0
```

Status	：SSH サーバーの状態
ENABLE	：有効、かつサーバーが起動処理完了し SSH 接続可能
STARTING	：有効だが、サーバーが起動処理中のため SSH 接続不可
ERROR	：有効だが、サーバーが異常終了し SSH 接続不可
DISABLE	：無効
Mode	：SSH サーバー機能有効時の動作モード
ALLOW	：ALLOW モード
DENY	：DENY モード
IP access list	：SSH アクセス管理リストに適用した IP アドレス
Subnet access list	：SSH アクセス管理ネットワークアドレスリストに適用したネットワークアドレス/サブネットマスク

関連コマンド

注意事項

3.35.15 show sshd key rsa

RSA ホスト公開鍵(SSH プロトコルバージョン 2)を表示します。

コマンドシンタックス

show sshd key rsa

コマンドモード

VIEW, ENABLE

使用例

(1) RSA ホスト公開鍵(SSH プロトコルバージョン 2)を表示します。

```
# show sshd key rsa
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAEwAvwGScYzSuIk9zM+H99JcDTCAF/y6V+kTEhAeZlGCKwr
B2zm/h0+Bk7lxV2kNC3MJKZjMZEycRfbhlqU6tvMfaAYsQ/9CI6U2BEu3 root@
```

関連コマンド

注意事項

3.35.16 show sshd key rsa1

RSA ホスト公開鍵(SSH プロトコルバージョン 1)を表示します。

コマンドシンタックス

show sshd key rsa1

コマンドモード

VIEW, ENABLE

使用例

(1) RSA ホスト公開鍵(SSH プロトコルバージョン 1)を表示します。

```
# show sshd key rsa1
600 35 31988388765955528264520210860016215299774045878439211238414719346040316 6
023808144750948471831245988604390346970436305100137992726920299881410980713285 5
93532326025677061643749648244 3 root@
```

関連コマンド

注意事項

3.36 IGMP Snooping

注意事項

同一 VLAN インターフェース内に、サーバー(sender)もクライアント(receiver)も存在する環境では、PIM-SM[IGMP](TD61-7251 AEOS Ver. 7.44 コマンドリファレンス L3 編)と IGMP の併用は避けてください。

3.36.1 ip igmp snooping enable

IGMP Snooping 機能を有効にします。無効にする場合は、no コマンドを使用してください。

本コマンドを有効にした場合、IGMP Membership Report メッセージを検知し、その Report メッセージが属するマルチキャストグループを管理対象として登録します。登録したマルチキャストグループ宛のマルチキャストパケットは、グループメンバーが存在するポートにのみに中継されるようになります。未登録のグループ宛となるマルチキャストパケット(宛先不明マルチキャストパケット)は、フラッディングされます。宛先不明マルチキャストパケットを廃棄する場合は、3.36.13 "ip igmp snooping unregistered-filter"コマンドを使用してください。

コマンドシンタックス

[no] ip igmp snooping enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) IGMP Snooping 機能を有効にします。

```
(config)# ip igmp snooping enable
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

マルチキャストフィルタリングと IGMP Snooping を同時に使用することはできません。

リンクアグリゲーションと IGMP Snooping を同時に使用した場合、以下のような動作となります。
Router Port、Member Port は LAG(リンクアグリゲーショングループ)中最も番号の小さいポートに登録されます。登録されたポートがリンクダウンした場合、表示上の登録ポートは変わりませんが、グループ内でリンクアップしている内の最も番号の小さ

いポートで正常にパケットは中継されます。

IGMP Snooping で登録されたメンバーやルーターポートのエントリーは、登録されたポートがリンクダウンしてもエージング時間が経過するまで削除されません。

3.36.2 ip igmp snooping immediate-leave

マルチキャストグループからの即時脱退機能を有効にします。無効にする場合は、no コマンドを使用してください。IGMP leave メッセージを受信したポートにおいて、そのメッセージに対応するマルチキャストグループからそのポートを即時脱退させます。本機能は、ポートに 1 つのホストしか接続されていない場合にのみ使用してください。

コマンドシンタックス

```
ip igmp snooping immediate-leave port <PORTRANGE>
no ip igmp snooping immediate-leave
```

PORTRANGE	即時脱退機能を有効にするポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1～8 において即時脱退機能を有効にします。

```
(config)# ip igmp snooping immediate-leave port 1-8
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

3.36.3 ip igmp snooping max-member

マルチキャストグループへの参加を許可する最大グループ数を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

```
ip igmp snooping max-member <COUNT> port <PORTRANGE>
no ip igmp snooping max-member [ port <PORTRANGE> ]
```

COUNT	参加を許可する最大グループ数 • Apresia3400/4348/5400/13000 シリーズ：<1-1024> • Apresia4328 シリーズ：<1-255>
PORTRANGE	制限を適用するポート番号(複数指定可能)

デフォルト

Apresia3400/4348/5400/13000 シリーズ：1024(個)
Apresia4328 シリーズ　　：　255(個)

コマンドモード

CONFIG

使用例

(1) ポート：1～8 において、10 グループまでのマルチキャストグループへの参加を許可します。

```
(config)# ip igmp snooping max-member 10 port 1-8
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

3.36.4 ip igmp snooping member aging-time

マルチキャストメンバーから IGMP report メッセージを受信しなくなった後、所属するマルチキャストグループから脱退させるための待ち時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。値は 10 から 1000000 まで設定可能です。

コマンドシンタックス

ip igmp snooping member aging-time <VALUE>
no ip igmp snooping member aging-time
　VALUE　　メンバーエージング時間 <10-1000000(秒)>

デフォルト

260(秒)

コマンドモード

CONFIG

使用例

(1) メンバーエージング時間を 10 秒に設定します。

```
(config)# ip igmp snooping member aging-time 10
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

3.36.5 ip igmp snooping member leave-time

マルチキャストグループからの脱退時間を設定します。本機能が有効な場合、IGMP leave メッセージ

を受信したポートはそのメッセージに対応するマルチキャストグループから指定時間後(単位：秒)に脱退します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

```
ip igmp snooping member leave-time <SECONDS>
no ip igmp snooping member leave-time
      SECONDS              マルチキャストグループからの脱退時間 <1-30(秒)>
```

デフォルト

10(秒)

コマンドモード

CONFIG

使用例

(1) 脱退時間を 5 秒にします。

```
(config)# ip igmp snooping member leave-time 5
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

マルチキャストグループからの即時脱退機能("ip igmp snooping immediate-leave")の設定がされているポートについては、即時脱退機能が有効になります。

3.36.6 ip igmp snooping mrouter aging-time

マルチキャストルーターから IGMP query メッセージを受信しなくなった後、マルチキャストルーターが存在しなくなるとみなすまでの待ち時間を指定します。この値に 0 を指定した場合、及び"ip igmp snooping mrouter vlan"コマンドで指定したルーターについては、エージング処理を行いません。値は 0(エージング OFF)、及び 10 から 1000000 まで設定可能です。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

```
ip igmp snooping mrouter aging-time <VALUE>
no ip igmp snooping mrouter aging-time
      VALUE                ルーターエージング時間 <0、10-1000000(秒)>
```

デフォルト

300(秒)

コマンドモード

CONFIG

使用例

(1) ルーターエージング時間を 10 秒に設定します。

```
(config)# ip igmp snooping mrouter aging-time 10
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

3.36.7 ip igmp snooping mrouter vlan

ルーターポートを手動設定します。設定を無効にする場合は、no コマンドを使用してください。本コマンドで指定したルーターについては、エージング処理を行いません。設定可能な登録数は、最大 128 個です。

コマンドシンタックス

ip igmp snooping mrouter vlan <VID> port <PORTRANGE>
no ip igmp snooping mrouter vlan [<VID>]

VID	ルーターポートを設定する VLAN ID
PORTRANGE	ルーターポートを設定するポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：9、10 に VLAN ID：10 のルーターポートを手動設定します。

```
(config)# ip igmp snooping mrouter vlan 10 port 9,10
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

本コマンドの設定に関わらず、本装置は IGMP query メッセージを受信したポートをルーターポートとして認識します。IGMP query メッセージによるルーターポートの自動認識を行わないようにするためには、"ip igmp snooping mrouter filter"コマンドを使用してください。

3.36.8 ip igmp snooping mrouter filter

受信した IGMP query メッセージを無効にするポートを設定します。本コマンドで指定したポートは、

IGMP query メッセージを受信しても、ルーターポートにはなりません。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

ip igmp snooping mrouter filter port <PORTRANGE>
no ip igmp snooping mrouter filter port

PORTRANGE	query フィルターを設定するポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：9、10 で IGMP query メッセージを受信しても、ルーターポートにならないようにします。

```
(config)# ip igmp snooping mrouter filter port 9,10
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

"ip igmp snooping mrouter vlan"コマンドを同一のポートに設定した場合、"ip igmp snooping mrouter vlan"コマンドで指定した VLAN についてはルーターポートとなります。

3.36.9 ip igmp snooping group filter

IGMP report メッセージを受信しても、グループメンバーとして登録しないマルチキャストグループアドレスを設定します(最大 8 エントリー)。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

ip igmp snooping group filter <GROUPADDR/MASK> port <PORTRANGE>
no ip igmp snooping group filter [<GROUPADDR/MASK>]

GROUPADDR	フィルターするマルチキャストグループアドレス
MASK	マルチキャストグループアドレスをネットワークアドレス範囲で指定するためのビットマスク値 • 省略した場合、ビットマスク値 32 が適用
PORTRANGE	フィルターを有効にする受信ポートの番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) ポート：1～8 で、マルチキャストグループ：224.0.0.150 のメンバーを登録しないフィルターを作成します。
(2) ポート：10 で、マルチキャストグループ：230.0.0.0/24 のメンバーを登録しないフィルターを作成します。

```
(config)# ip igmp snooping group filter 224.0.0.150/32 port 1-8
(config)# ip igmp snooping group filter 230.0.0.0/24 port 10
```

関連コマンド
show ip igmp snooping configuration, show running-config

注意事項

3.36.10 ip igmp snooping send report-leave disable

ルーターポートに中継する Report と Leave メッセージをすべて破棄します。設定をデフォルトに戻す場合は、no コマンドを使用してください。
本コマンドの使用により Report や Leave メッセージの中継制限を行い、クエリアの負荷を低減させることが可能になります。

コマンドシンタックス
[no] ip igmp snooping send report-leave disable

デフォルト
no disable(＝中継を行う)

コマンドモード
CONFIG

使用例
(1) Report、及び Leave メッセージのルーターポートへの中継を制限します。

```
(config)# ip igmp snooping send report-leave disable
```

関連コマンド
show ip igmp snooping configuration, show running-config

注意事項

3.36.11 ip igmp snooping report-message-proxy enable

ルーターポートに送る Report メッセージを集約する機能を有効にします。無効にする場合は、no コマンドを使用してください。本機能は、Query メッセージに対する応答(Report メッセージ)をひとつに

集約することによって、クエリアの負荷を低減させ、ルーターに使用します。

コマンドシンタックス

[no] ip igmp snooping report-message-proxy enable

デフォルト

no enable(＝ルーターポートに送る Report メッセージを集約する機能無効)

コマンドモード

CONFIG

使用例

(1) ルーターポートに送る Report メッセージを集約する機能を有効にさせます。

```
(config)# ip igmp snooping report-message-proxy enable
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

本装置が学習済みであるグループに対する Report メッセージを受信した場合に集約されます。また、同一グループに対する Leave メッセージについても集約されます。

本コマンドが有効な場合、"ip igmp snooping mrouter vlan"コマンドを設定したポートや、ルーターポートとして動作するポートに対して、"ip igmp snooping unregistered-filter"コマンド、及び 3.23.1 "egress-filtering umc"コマンドを設定しないでください。

3.36.12 ip igmp snooping leave-message-proxy enable

ルーターポートに送る Leave メッセージを集約する機能を有効にします。無効にする場合は、no コマンドを使用してください。本機能は、本装置が管理しているマルチキャストメンバー情報をもとに、残存しているメンバーがいる場合、不要な Leave メッセージをルーターポート宛に中継させない機能です。

コマンドシンタックス

[no] ip igmp snooping leave-message-proxy enable

デフォルト

no enable(＝ルーターポートに送る Leave メッセージを集約する機能無効)

コマンドモード

CONFIG

使用例

(1) ルーターポートに送る Report メッセージを集約する機能を有効にします。

```
(config)# ip igmp snooping leave-message-proxy enable
```

関連コマンド

show ip igmp snooping configuration, show running-config

注意事項

本機能は、装置とマルチキャストメンバー(端末)がピアツーピアで接続されていることが条件となります。装置とマルチキャストメンバー(端末)の間に IGMP Snooping 機能を持たない装置などが接続される場合は、一時的にマルチキャストソースが配信されない現象が発生します。

本コマンドが有効な場合、"ip igmp snooping mrouter vlan"コマンドを設定したポートや、ルーターポートとして動作するポートに対して、"ip igmp snooping unregistered-filter"コマンド、及び 3.23.1 "egress-filtering umc"コマンドを設定しないでください。

3.36.13 ip igmp snooping unregistered-filter

IGMP Snooping として未登録のマルチキャストパケットを破棄するポートを設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

[no] ip igmp snooping unregistered-filter port <PORTRANGE>

PORTRANGE　　ポート番号(複数指定可)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1 を未登録のマルチキャストパケットを破棄するポートに設定します。

```
(config)# ip igmp snooping unregistered-filter port 1
```

関連コマンド

show running-config

注意事項

本コマンドを設定したポートは、未登録マルチキャストパケットの送信を行わなくなるため、3.36.7 "ip igmp snooping mrouter vlan"を設定したポートや、ルーターポ

ートとして動作するポートへは設定を行わないでください。

本機能による送信制御中に設定を変更すると、一時的に IGMP Snooping として未登録のマルチキャストパケットが、VLAN 内をフラッディングすることがあります。

3.28.8 "block-cpu-control"との併用はできません。

本コマンド設定時は、以下の予約マルチキャストアドレスが透過されます。
- **224.0.0.0/24**

3.36.14 ip igmp snooping unregistered-filter pf2-group

"ip igmp snooping unregistered-filter"で使用するパケットフィルター2 のグループ番号を設定します。設定を削除する場合は、no コマンドを使用してください。グループは"ip igmp snooping unregistered-filter"設定時に確保します。他機能で予約済みのグループは確保できません。

本コマンド未設定時は、未使用の最小グループ番号 1 つを自動的に予約します。

グループを確保できない場合は、"ip igmp snooping unregistered-filter"の設定に関わらず、IGMP Snooping として未登録のマルチキャストパケットが VLAN 内をフラッディングします。

"ip igmp snooping unregistered-filter"が設定されている状態では、グループ番号を変更できません。グループの予約状況は、3.28.14 "show packet-filter2 reserved-group"コマンドで確認可能です。

コマンドシンタックス

ip igmp snooping unregistered-filter pf2-group <GROUP>
no ip igmp snooping unregistered-filter pf2-group

GROUP　　グループ番号
- Apresia3400/4348/5400/13000 シリーズ：<1-14>
- Apresia4328 シリーズ：<1-7>

デフォルト

自動割り当て(＝未使用グループの最小番号)

コマンドモード

CONFIG

使用例

(1) グループ：7 を ip igmp snooping unregistered-filter で使用するように設定します。

```
(config)# ip igmp snooping unregistered-filter pf2-group 7
```

関連コマンド

show running-config, show packet-filter2 reserved-group

注意事項

パケットフィルター2 のグループが確保できない場合、途中でパケットフィルター2

のグループが確保できる状態になっても、"ip igmp snooping unregistered-filter" を再設定しない限り、パケットフィルター2 グループは確保されません。

3.41 MMRP、3.42 MMRP-Plus、3.43 MMRP2 aware と併用する場合に使用するパケットフィルター2 のグループ番号は、本機能で使用する番号より大きくなるようにしてください。

3.36.15 clear ip igmp snooping cpu-counter

CPU で処理した各 IGMP メッセージ数のカウンターをすべてゼロクリアします。

コマンドシンタックス

clear ip igmp snooping cpu-counter

コマンドモード

ENABLE

使用例

(1) ip igmp snooping cpu-counter で管理しているカウンターをすべてゼロクリアします。

```
# clear ip igmp snooping cpu-counter
```

関連コマンド

show ip igmp snooping configuration, show running-config, show ip igmp snooping cpu-counter

注意事項

3.36.16 show ip igmp snooping cpu-counter

CPU で処理した各 IGMP メッセージの数を表示します。各 IGMP メッセージ数はリブート、もしくは電源投入時にゼロクリアされます。

コマンドシンタックス

show ip igmp snooping cpu-counter

コマンドモード

VIEW, ENABLE

使用例

(1) CPU で処理した各 IGMP メッセージの数を表示します。

```
# show ip igmp snooping cpu-counter

active group count : 3
general query relay count : 535
```

```
Group Address query-relay report-recv report-send  leave-recv  leave-send
   224.0.0.10        1234        1234        1234         568         568
   224.0.0.11        1357        1357        1357         128         128
   224.0.0.12         987         987         987          56          56
  Other Group           0           0           0           0           0
```

active group count　：現在登録されたマルチキャストグループ数
general query relay count　：中継した General Query メッセージ数
Group Address　：グループアドレス(ID)
　Other Group　：未登録マルチキャストグループ(メンバーがいないグループや"ip igmp snooping max-member"コマンドで指定した最大登録数を超えたグループなど)
query-relay　：中継した Group-Specific Query メッセージ数
report-recv　：受信した Report メッセージ数
report-send　：送信した Report メッセージ数
leave-recv　：受信した Leave メッセージ数
leave-send　：送信した Leave メッセージ数

関連コマンド

注意事項

このカウンターは、CPU 上で処理した IGMP メッセージのみをカウントしています。そのため、他のハードウェアカウンターと比較して表示値に差が生じる場合があります。

3.36.17 show ip igmp snooping configuration

本装置に設定されている IGMP Snooping の情報を表示します。

コマンドシンタックス

show ip igmp snooping configuration

コマンドモード

VIEW, ENABLE

使用例

(1) IGMP Snooping の情報を表示します。

```
# show ip igmp snooping configuration
    Group Membership Aging Time      = 260(sec)
    Group Membership Leave Time      = 10(sec)
    Router Port Aging Time           = 300(sec)
    Router Port Filter               = 10
    Immediate Leave Port             = None
    Send Report-Leave Message        = Enable
    Report Message Proxy             = Disable
```

```
    Leave Message Proxy              = Disable

    Group Filter
    address             port
    224.1.1.1/32        1

    Static Router Port
    vlan  port
    1     26

    Max Member Count
    port  count
    1     1024
    2     1024
---(省略)---
    50    1024
```

Group Membership Aging Time　：マルチキャストグループメンバーのエージング時間
Group Membership Leave Time　：マルチキャストグループからの脱退時間
Router Port Aging Time　：ルーターポートのエージング時間
Router Port Filter　：ルーターポートのフィルター設定
Immediate Leave Port　：即時脱退処理を行うポート
Send Report-Leave Port　：ルーターポート宛の Report・Leave メッセージの送信設定
Report Message Proxy　：ルーターポート宛の Report メッセージを集約する機能の設定
Leave Message Proxy　：ルーターポート宛の Leave メッセージを集約する機能の設定
Group Filter Address　：マルチキャストグループのフィルター設定
Static Router Port　：手動設定されたルーターポート
Max Member Count　：ポートで参加を許可するグループ数

関連コマンド

注意事項

3.36.18 show ip igmp snooping status

IGMP Snooping のステータス情報を表示します。

コマンドシンタックス

show ip igmp snooping status

コマンドモード

VIEW, ENABLE

使用例

(1) IGMP Snooping のステータス情報を表示します。

```
# show ip igmp snooping status

active group count : 1

m:Member r:Router(dynamic) R:Router(static)
                    Port
                    1    6 7   12 13  18 19  24 25    32 33    40 41    48 49
 Group Address   VID +----+ +----+ +----+ +----+ +------+ +------+ +------+ +-
     224.0.0.10    1 m.r... .....R ...... ...... ........ ........ ........ ..
 (01:00:5e:00:00:0a)
```

active group count　：登録されたマルチキャストグループ数

Group Address　：グループアドレス(ID)、及びマッピングされた MAC アドレス
マルチキャストクライアントから IGMP report メッセージを受信していない場合は表示されない

Port　：物理ポート番号

r　：ルーター接続ポート

R　：手動設定されたルーターポート

m　：マルチキャストクライアント接続ポート

関連コマンド

注意事項

リンクアグリゲーションと IGMP Snooping を同時に使用した場合、Router Port、Member Port は LAG(リンクアグリゲーショングループ)中最も番号の小さいポートに登録されます。登録されたポートがリンクダウンした場合、本コマンドによる表示上は、登録ポートは変わりませんが、グループ内でリンクアップしている内の最も番号の小さいポートで正常にパケットが中継されます。

3.36.19 show tech-support igmp

IGMP 機能の各種情報を収集し表示します。本コマンドで表示する内容は、表 3-38 に示すコマンドが収集している情報です。system-dump オプションを指定した場合、装置内部のダンプ情報(独自形式で表示)を含めて取得し表示します。

表 3-38 コマンドにより収集可能な IGMP 情報

show system
show version
show ip igmp snooping status
show ip igmp snooping cpu-counter
show ip igmp groups
show ip igmp proxy interface

```
show ip igmp proxy groups
```

コマンドシンタックス

show tech-support igmp [system-dump]

system-dump　　装置内部のダンプ情報を出力

コマンドモード

ENABLE

関連コマンド

注意事項

L3 ライセンスを設定していない場合は、"show ip igmp snooping status"、"show ip igmp snooping cpu-counter"コマンドのみ表示されます。

system-dump オプションを指定した場合、装置の性能、及び通信に対して影響を及ぼす可能性があります。使用する場合には、必ず事前にサポート対応窓口へご相談のうえ、指示に従ってください。

3.37 IGMP クエリア

3.37.1 ip igmp querier enable

簡易 IGMP クエリア機能を有効にします。無効にする場合は、no コマンドを使用してください。本機能は、IGMP Snooping 機能と併用して使用することができます。マルチキャストルーターが存在しない VLAN において、IGMP General Query メッセージの送信のみを行います。また、クエリアが複数存在する場合には、最小 IP アドレスの装置が代表クエリアになります。

コマンドシンタックス

[no] ip igmp querier enable

デフォルト

no enable(＝IGMP クエリア無効)

コマンドモード

CONFIG

使用例

(1) IGMP クエリア機能を VLAN ID：1 で有効にします。
(2) IGMP クエリア機能を有効にします。

```
(config)# ip igmp querier vlan add 1
(config)# ip igmp querier enable
```

関連コマンド

show ip igmp querier configuration, show running-config

注意事項

本機能は、PIM-SM、及び IP マルチキャストルーティングが有効時には使用できません。

"ip igmp querier vlan"で指定した VLAN で、かつ IP アドレスが登録されている VLAN に限り動作します。

IGMP report メッセージや IGMP leave メッセージによる動作は行いません。

3.37.2 ip igmp querier vlan

IGMP クエリア機能を有効にさせる VLAN を設定します。有効にできる VLAN の数は 256 個までです。

コマンドシンタックス

ip igmp querier vlan add | remove <VLANRANGE>

add	IGMP クエリア機能を有効にさせる VLAN を追加
remove	IGMP クエリア機能が有効な VLAN を削除

VLANRANGE　　VLAN ID <1-4094> (複数指定可能)

デフォルト
なし(＝設定無し)

コマンドモード
CONFIG

使用例
(1) IGMP クエリア機能を有効にさせる VLAN ID：1 を設定します。

```
# configure terminal
(config)# ip igmp querier vlan add 1
```

関連コマンド
show ip igmp querier configuration, show running-config

注意事項

3.37.3 ip igmp querier query-interval

装置が送信するホストクエリーの送信間隔を指定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス
ip igmp querier query-interval <INTERVAL>
no ip igmp querier query-interval
　INTERVAL　　送信間隔 <1-300(秒)>

デフォルト
125(秒)

コマンドモード
CONFIG

使用例
(1) ホストクエリーの送信間隔を 120 秒に設定します。

```
# configure terminal
(config)# ip igmp querier query-interval 120
```

関連コマンド
show ip igmp querier configuration, show running-config

注意事項

3.37.4 ip igmp querier query-max-response-time

IGMP クエリーの広告に対するレスポンスの最大時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用します。

コマンドシンタックス

ip igmp querier query-max-response-time <RESPONSETIME>
no ip igmp querier query-max-response-time
RESPONSETIME　　IGMP クエリーに対する最大応答時間 <1-25(秒)>

デフォルト

10(秒)

コマンドモード

CONFIG

使用例

(1) IGMP クエリーに対する最大応答時間を 8 秒に設定します。

```
# configure terminal
(config)# ip igmp querier query-max-response-time 8
```

関連コマンド

show ip igmp querier configuration, show running-config

注意事項

3.37.5 ip igmp querier query-timeout

VLAN 内の他装置が代表クエリアとなっている状態で、代表クエリアの障害監視時間を設定します。代表クエリアが障害などでクエリーの送信を停止し、本コマンドにて設定した時間が経過すると本装置がクエリアとなりクエリーの送信を開始します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

ip igmp querier query-timeout <TIMEOUT>
no ip igmp querier query-timeout
TIMEOUT　　代表クエリアを削除するまでの障害監視時間 <2-700(秒)>

デフォルト

自動計算：以下の計算式に基づいて算出された値(すべてデフォルトの場合は 255 秒)
計算式 = (query-interval * robustness) + (query-max-response-time / 2)

コマンドモード

CONFIG

使用例

(1) 代表クエリアを削除するまでの障害監視時間を 8 秒に設定します。

```
# configure terminal
(config)# ip igmp querier query-timeout 8
```

関連コマンド

show ip igmp querier configuration, show running-config

注意事項

3.37.6 ip igmp querier robustness

Robustness Variable で、VLAN 内の代表クエリアの存在有無を判断する時間を調整するパラメーター(予測されるパケットロス数)を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

本値を大きくすると、VLAN 内に代表クエリアが存在しないと判断するまでの時間(query timeout)が長くなります。

コマンドシンタックス

ip igmp querier robustness <COUNT>
no ip igmp querier robustness
COUNT 予測されるパケットロス数 + 1 <2-7>

デフォルト

2

コマンドモード

CONFIG

使用例

(1) パケットロスの頻度を 3 に設定します。

```
# configure terminal
(config)# ip igmp querier robustness 3
```

関連コマンド

show ip igmp querier configuration, show running-config

注意事項

3.37.7 show ip igmp querier configuration

IGMP クエリアに関する構成情報を表示します。

コマンドシンタックス

show ip igmp querier configuration

コマンドモード

VIEW, ENABLE

使用例

(1) IGMP クエリアの構成情報を表示します。

```
# show ip igmp querier configuration
 IGMP querier is enabled
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds

Enable Interface
  vlan      ip address
     1    192.168.26.6
     2    192.168.27.6
     3    192.168.28.6
```

関連コマンド

注意事項

3.38 ロギング

3.38.1 logging buffered

バッファメモリーに出力するログメッセージの優先度を設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。<PRIORITY>に指定した優先度以上のログメッセージがバッファメモリーに保存されます。

コマンドシンタックス

logging buffered <PRIORITY>
no logging buffered
PRIORITY　　ログメッセージの優先度(表 3-39 参照)

表 3-39 ログメッセージ優先度一覧

	優先度	説明
emerg	0	Emergency：システムが使用できない状態になったときに出力
alert	1	Alert：システムを運用するためにただちに処置を施す必要のある問題が発生したときに出力
crit	2	Critical：危険な状態になったときに出力
err	3	Error：エラーイベントが発生したときに出力
warning	4	Warning：警告イベントが発生したときに出力
notice	5	Notice：重要なイベントが発生したときに出力
info	6	Informational：特に問題とはならないイベントが発生したときに出力

デフォルト

info

コマンドモード

CONFIG

使用例

(1) 優先度 notice 以上のログメッセージをバッファメモリーに記憶します。
(2) 設定を元に戻します。

```
(config)# logging buffered notice
(config)# no logging buffered
```

関連コマンド

show running-config

注意事項

ログの内容は、リブートコマンド実行時、及び"logging flash"コマンド実行時にフラッシュメモリーに保存されます。従って、電源再投入やリセットスイッチを押すと、稼動中に蓄積された内容は失われます。ログ内容をフラッシュメモリーに保存したい場合は、リブートコマンドを使用してリブートするか"logging flash"コマンドを実

行してください。

3.38.2 logging sram

SRAM に出力するログメッセージの優先度を設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。<PRIORITY>に指定した優先度以上のログメッセージが SRAM に保存されます。ログメッセージはログ発生時に自動的に SRAM に保存されます。従って、ログメッセージを保存するのにリブートコマンドや"logging flash"コマンドを必要としません。

コマンドシンタックス

logging sram <PRIORITY>
no logging sram
PRIORITY　　ログメッセージの優先度(表 3-39 参照)

デフォルト

info

コマンドモード

CONFIG

使用例

(1) 優先度 notice 以上のログメッセージを SRAM に記憶します。
(2) 設定を元に戻します。

```
(config)# logging sram notice
(config)# no logging sram
```

関連コマンド

show running-config

注意事項

"show logging sram"コマンドは Apresia3400 シリーズ、Apresia5400 シリーズ、Apresia13000 シリーズでのみ対応しております。

3.38.3 logging console

シリアルコンソールに出力するログの優先度を設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

logging console <PRIORITY>
no logging console
PRIORITY　　ログメッセージの優先度(表 3-39 参照)

デフォルト

alert

コマンドモード
CONFIG

使用例
(1) 優先度 err 以上のログメッセージをシリアルコンソールに出力します。
(2) 設定を元に戻します。

```
(config)# logging console err
(config)# no logging console
```

関連コマンド
show running-config

注意事項

シリアルコンソールへのログ出力が過負荷状態(単位時間あたりの出力量が多い)では、ログ出力は抑制されるため、コンソールに表示されない場合があります。

3.38.4 logging monitor

TELNET/SSH のターミナル画面に出力するログの優先度を設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。本コマンドで設定したログを表示させるには、"terminal monitor" コマンドをあわせて設定してください。

コマンドシンタックス
logging monitor <PRIORITY>
no logging monitor
PRIORITY　　ログメッセージの優先度(表 3-39 参照)

デフォルト
なし(＝ターミナル画面にログメッセージを出力しない)

コマンドモード
CONFIG

使用例
(1) 優先度 alert 以上のログメッセージをターミナル画面に出力します。
(2) 設定を元に戻します。

```
(config)# logging monitor alert
(config)# no logging monitor
```

関連コマンド
terminal monitor, show running-config

注意事項

3.38.5 logging ip

ログメッセージを送信する syslog サーバーを設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。<IPADDR>は syslog サーバーの IP アドレス、<FACILITY>は syslog サーバーに送信するファシリティー、<PRIORITY>は syslog サーバーに送信するメッセージの優先度です。<PRIORITY>に指定した優先度以上のログメッセージが syslog サーバーに送信されます。syslog サーバーは 8 個まで設定できます。また、同じ IP アドレスを 2 個設定することはできません。同じ IP アドレスを設定した場合、すでに登録されている syslog サーバーの設定が上書きされます。

コマンドシンタックス

logging ip <IPADDR> <FACILITY> <PRIORITY>
no logging ip <IPADDR>

FACILITY	ファシリティー(表 3-40 参照)
PRIORITY	ログメッセージの優先度(表 3-39 参照)
IPADDR	IP アドレス

表 3-40 ファシリティー一覧

	説明
local0	local use 0
local1	local use 1
local2	local use 2
local3	local use 3
local4	local use 4
local5	local use 5
local6	local use 6
local7	local use 7

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) 優先度 warning 以上のログメッセージをファシリティー：local0 として syslog サーバー：192.168.1.5 に送信します。
(2) 設定を元に戻します。

```
(config)# logging ip 192.168.1.5 local0 warning
(config)# no logging ip 192.168.1.5
```

関連コマンド

show running-config

注意事項

3.38.6 logging source

ログメッセージ送信時の送信元 IP アドレスを指定します。設定を削除する場合は、no コマンドを使用してください。ループバック IP アドレス(127.0.0.0～127.255.255.255)、クラス D(224.0.0.0～239.255.255.255)、クラス E(240.0.0.0～255.255.255.255)は送信元 IP アドレスに指定できません。

コマンドシンタックス

logging source <IPADDR>
no logging source
　　IPADDR　　IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ログメッセージ送信時の送信元 IP アドレスを 192.168.1.5 に設定します。
(2) ログメッセージ送信時の送信元 IP アドレス指定を削除します。

```
(config)# logging source 192.168.1.5
(config)# no logging source
```

関連コマンド

show running-config

注意事項

3.38.7 logging on

ログメッセージの出力・停止を制御します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

[no] logging on

デフォルト

ログを出力

コマンドモード

CONFIG

使用例

(1) ログメッセージの出力を停止します。
(2) ログメッセージを出力します。

```
(config)# no logging on
(config)# logging on
```

関連コマンド

show running-config

注意事項

3.38.8 logging flash

バッファメモリーに記録されているログメッセージをフラッシュメモリーに書き込みます。フラッシュメモリーに保存できるログメッセージは3000件です。

コマンドシンタックス

logging flash

コマンドモード

CONFIG

使用例

(1) ログメッセージをフラッシュメモリーに保存します。

```
(config)# logging flash
```

関連コマンド

注意事項

3.38.9 logging error-frame-received port disable

指定したポートにおいて、各エラーフレーム受信時の syslog 出力を無効にします。設定をデフォルトに戻す場合は、no コマンドを使用してください。

エラーフレーム受信時の syslog は、5 秒間隔でエラーフレーム受信用のカウンターを監視し、カウンターの値が変化した場合に出力します。

コマンドシンタックス

[no] logging error-frame-received port <PORTRANGE> disable

PORTRANGE　　ポート番号(複数指定可能)

デフォルト

no disable(＝syslog を出力する)

コマンドモード

CONFIG

使用例

(1) ポート：1～20 において、エラーフレーム受信時の syslog 出力を無効にします。

```
(config)# logging error-frame-received port 1-20 disable
```

(2) ポート：1～20 において、エラーフレーム受信時の syslog 出力を有効にします。

```
(config)# no logging error-frame-received port 1-20 disable
```

関連コマンド

show running-config

注意事項

3.38.10 show logging

バッファメモリー、もしくは SRAM に保存されたログメッセージを表示します。SRAM パラメーターを指定しない場合はバッファメモリーに保存されたログメッセージを表示します。保存できるログメッセージは 3000 件です。

コマンドシンタックス

show logging [sram] [reverse]

sram	SRAM に保存されたログメッセージを表示
reverse	イベントが発生した順序の逆順で表示

コマンドモード

VIEW, ENABLE

使用例

(1) ログメッセージを表示します。

(2) ログメッセージを逆順に表示します。

```
> show logging
Date            Log messages
Apr 21 21:10:57  <system:warning> Power up. Start logging.
(略)
> show logging reverse
Date            Log messages
Jul 18 13:19:28  <cli:info> show logging reverse
(略)
```

関連コマンド

注意事項

ログの内容は、3.56.1 "reboot"コマンド実行時、及び"logging flash"コマンド実行時にフラッシュメモリーに保存されます。従って、電源再投入やリセットスイッチを

押すと、稼動中に蓄積された内容は失われます。ログ内容をフラッシュメモリーに保存したい場合は、"reboot"コマンドを使用してリブートするか"logging flash"コマンドを実行してください。

3.38.11 clear logging

バッファメモリー、もしくはSRAMに保存されたログメッセージを消去します。sramパラメーターを指定しない場合は、バッファメモリーのログメッセージが消去されます。

コマンドシンタックス

clear logging [sram]

sram　　SRAM

コマンドモード

ENABLE

使用例

(1) バッファメモリーに保存されているログメッセージを消去します。

```
# clear logging
```

関連コマンド

show logging

注意事項

3.39 MLD Snooping

注意事項

MLD 設定時に、3.47 AccessDefender 機能、3.41 MMRP/3.42 MMRP-Plus/3.43 MMRP2 aware(いずれか 1 つ)機能の 3 機能を同時に併用できません。

3.39.1 ipv6 mld snooping enable

MLD Snooping 機能を有効にします。無効にする場合は、no コマンドを使用してください。本コマンドを有効にした場合、管理対象となった(スヌーピングした)マルチキャストグループ内の IPv6 マルチキャストパケットを、グループメンバーが存在するポートにのみに中継します。未登録のグループ宛となるマルチキャストパケット(宛先不明マルチキャストパケット)は、フラッディングされます。宛先不明マルチキャストパケットを廃棄する場合は、3.39.10 "ipv6 mld snooping unregistered-filter"コマンドを使用してください。

コマンドシンタックス

[no] ipv6 mld snooping enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) MLD Snooping 機能を有効にします。

```
(config)# ipv6 mld snooping enable
```

関連コマンド

show ipv6 mld snooping configuration, show running-config

注意事項

3.39.2 ipv6 mld snooping immediate-leave

マルチキャストグループからの即時脱退機能を有効にします。無効にする場合は、no コマンドを使用してください。Multicast Listener Done メッセージを受信したポートにおいて本機能が有効な場合、そのメッセージに対応するマルチキャストグループからそのポートを即時脱退させます。本機能は、ポートに 1 つのホストしか接続されていない場合にのみ使用してください。

コマンドシンタックス

ipv6 mld snooping immediate-leave port <PORTRANGE>
no ipv6 mld snooping immediate-leave

PORTRANGE　　ポート番号(複数指定可能)

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) ポート：1～8 において即時脱退機能を有効にします。

```
(config)# ipv6 mld snooping immediate-leave port 1-8
```

関連コマンド
show ipv6 mld snooping configuration, show running-config

注意事項

3.39.3 ipv6 mld snooping max-member

マルチキャストグループへの参加を許可する最大グループ数を設定します。設定した値を無効にする場合は、no コマンドを使用してください。no コマンドでポート番号を省略した場合は、すべてのポートに設定された、マルチキャストグループへの参加を許可する最大グループ数をデフォルト値にし、ポート番号を指定した場合は、指定したポートに設定されたマルチキャストグループへの参加を許可する最大グループ数をデフォルト値にします。

コマンドシンタックス
ipv6 mld snooping max-member <COUNT> port <PORTRANGE>
no ipv6 mld snooping max-member [port <PORTRANGE>]

COUNT　　参加を許可する最大グループ数 <1-255>
PORTRANGE　　制限を適用するポート番号(複数指定可能)

デフォルト
255(個)

コマンドモード
CONFIG

使用例
(1) ポート：1～8 において、10 グループまでのマルチキャストグループへの参加を許可します。

```
(config)# ipv6 mld snooping max-member 10 port 1-8
```

関連コマンド
show ipv6 mld snooping configuration, show running-config

注意事項

3.39.4 ipv6 mld snooping member aging-time

マルチキャストメンバーからMulticast Listener Reportメッセージを受信しなくなった後、所属するマルチキャストグループから脱退させるため待ち時間を設定します。値は10から1000000まで設定可能です。設定をデフォルト値に戻す場合は、noコマンドを使用してください。

コマンドシンタックス

```
ipv6 mld snooping member aging-time <VALUE>
no ipv6 mld snooping member aging-time
      VALUE              メンバーエージング時間 <10-1000000(秒)>
```

デフォルト

260(秒)

コマンドモード

CONFIG

使用例

(1) メンバーエージング時間を10秒に設定します。

```
(config)# ipv6 mld snooping member aging-time 10
```

関連コマンド

show ipv6 mld snooping configuration, show running-config

注意事項

3.39.5 ipv6 mld snooping member leave-time

ListenerからMulticast Listener Doneメッセージを受信してからのマルチキャストグループからの脱退待ち時間を設定します。本機能が有効な場合、Multicast Listener Doneメッセージを受信したポートはそのメッセージに対応するマルチキャストグループから指定時間後(単位：秒)に脱退します。設定をデフォルト値に戻す場合は、noコマンドを使用してください。

コマンドシンタックス

```
ipv6 mld snooping member leave-time <SECONDS>
no ipv6 mld snooping member leave-time
      SECONDS            マルチキャストグループからの脱退時間 <1-30(秒)>
```

デフォルト

10(秒)

コマンドモード

CONFIG

使用例

(1) 脱退時間を5秒にします。

```
(config)# ipv6 mld snooping member leave-time 5
```

関連コマンド

show ipv6 mld snooping configuration, show running-config

注意事項

3.39.6 ipv6 mld snooping mrouter aging-time

マルチキャストルーターから Multicast Listener Query メッセージを受信しなくなった後、マルチキャストルーターが存在しなくなるとみなすまでの待ち時間を設定します。ただし、"ipv6 mld snooping mrouter vlan"コマンドで指定したルーターについては、エージング処理を行いません。

設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

ipv6 mld snooping mrouter aging-time <VALUE>
no ipv6 mld snooping mrouter aging-time
VALUE　　ルーターエージング時間 <10-1000000(秒)>

デフォルト

300(秒)

コマンドモード

CONFIG

使用例

(1) ルーターエージング時間を10秒に設定します。

```
(config)# ipv6 mld snooping mrouter aging-time 10
```

関連コマンド

show ipv6 mld snooping configuration, show running-config

注意事項

3.39.7 ipv6 mld snooping mrouter vlan

指定した VLAN のポートをルーターポートに手動設定します。無効にする場合は、no コマンドを使用してください。no コマンドにおいて、<VID>を省略した場合、すべての VLAN のルーターポートの手動設定を無効にし、<VID>を指定した場合、指定した VLAN のルーターポートの手動設定を無効にします。本コマンドで指定したルーターについては、エージング処理を行いません。

コマンドシンタックス

ipv6 mld snooping mrouter vlan <VID> port <PORTRANGE>

no ipv6 mld snooping mrouter vlan [<VID>]

VID	ルーターポートを設定する VLAN ID <1-4094>
PORTRANGE	ルーターポートを設定するポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：9、10 に VLAN ID：10 のルーターポートを手動設定します。

```
(config)# ipv6 mld snooping mrouter vlan 10 port 9,10
```

関連コマンド

show ipv6 mld snooping configuration, show running-config

注意事項

3.39.8 ipv6 mld snooping mrouter filter

受信した Multicast Listener Query メッセージを無効にするポートを設定します。本コマンドで指定したポートは、Multicast Listener Query メッセージを受信しても、ルーターポートにはなりません。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

ipv6 mld snooping mrouter filter port <PORTRANGE>

no ipv6 mld snooping mrouter filter port

PORTRANGE	query フィルターを設定するポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：9、10 で Multicast Listener Query メッセージを受信しても、ルーターポートにならないようにします。

```
(config)# ipv6 mld snooping mrouter filter port 9,10
```

関連コマンド

show ipv6 mld snooping configuration, show running-config

注意事項

3.39.9 ipv6 mld snooping group filter

Multicast Listener Report メッセージを受信しても、メンバーとして登録しないマルチキャストグループアドレスを設定します(最大 8 エントリー)。設定を削除する場合は、no コマンドを使用してください。no コマンドにおいて、マルチキャストグループを指定した場合は、指定したマルチキャストグループアドレスの設定を解除し、省略した場合はすべての設定を解除にします。

コマンドシンタックス

ipv6 mld snooping group filter <GROUP/PREFIX> port <PORTRANGE>
no ipv6 mld snooping mrouter filter port

GROUP	フィルターするマルチキャストグループアドレス
PREFIX	マルチキャストグループアドレスをネットワークアドレス範囲で指定するためのプレフィックス
PORTRANGE	フィルターを有効にする受信ポートの番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1～8 で、マルチキャストグループ：ff02::1/128 のメンバーを登録しないフィルターを作成します。
(2) ポート：12 で、マルチキャストグループ：ff12::1111:1111/96 のメンバーを登録しないフィルターを作成します。

```
(config)# ipv6 mld snooping group filter ff02::1/128 port 1-8
(config)# ipv6 mld snooping group filter ff12::1111:1111/96 port 12
```

関連コマンド

show ipv6 mld snooping configuration, show running-config

注意事項

3.39.10 ipv6 mld snooping unregistered-filter

MLD Snooping として未登録のマルチキャストパケットを破棄するポートを設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

[no] ipv6 mld snooping unregistered-filter port <PORTRANGE>

PORTRANGE	ポート番号(複数指定可)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1を未登録のIPv6マルチキャストパケットを破棄するポートに設定します。

```
(config)# ipv6 mld snooping unregistered-filter port 1
```

関連コマンド

show running-config

注意事項

ルーターポートを指定しないでください。

本コマンドが動作中に設定を変更すると、一時的にMLD Snoopingとして未登録のマルチキャストパケットが、VLAN内をフラッディングすることがあります。

3.28.8 "block-cpu-control"との併用はできません。

本コマンド設定時は、以下の予約マルチキャストアドレスが透過されます。

- **FF02::/111**
- **FF02::1:FFXX:XXXX/104**
- **FF05::/111**

3.39.11 ipv6 mld snooping unregistered-filter pf2-group

"ipv6 mld snooping unregistered-filter"で使用するパケットフィルター2のグループ番号を設定します。設定を削除する場合は、no コマンドを使用してください。グループは"ipv6 mld snooping unregistered-filter"設定時に確保します。他機能で予約済みのグループは確保できません。

本コマンド未設定時は、未使用の最小グループ番号1つを自動的に予約します。

グループを確保できない場合は、"ipv6 mld snooping unregistered-filter"の設定に関わらず、MLD Snoopingとして未登録のマルチキャストパケットがVLAN内をフラッディングします。

"ipv6 mld snooping unregistered-filter"が設定されている状態では、グループ番号を変更できません。グループの予約状況は、3.28.14 "show packet-filter2 reserved-group"コマンドで確認可能です。

コマンドシンタックス

ipv6 mld snooping unregistered-filter pf2-group <GROUP>
no ipv6 mld snooping unregistered-filter pf2-group

GROUP　　グループ番号
- Apresia3400/4348/5400/13000シリーズ：<1-14>
- Apresia4328シリーズ：<1-7>

デフォルト
自動割り当て(＝未使用グループの最小番号)

コマンドモード
CONFIG

使用例
(1) グループ：7 を ipv6 mld snooping unregistered-filter で使用するように設定します。

```
(config)# ipv6 mld snooping unregistered-filter pf2-group 7
```

関連コマンド
show running-config, show packet-filter2 reserved-group

注意事項

パケットフィルター2 のグループが確保できない場合、途中でパケットフィルター2 のグループが確保できる状態になっても、"ipv6 mld snooping unregistered-filter" を再設定しない限り、パケットフィルター2 グループは確保されません。

3.41 MMRP、3.42 MMRP-Plus、3.43 MMRP2 aware と併用する場合に使用するパケットフィルター2 のグループ番号は、本機能で使用する番号より大きくなるようにしてください。

3.39.12 show ipv6 mld snooping configuration

本スイッチングハブに設定されている MLD Snooping の情報を表示します。

コマンドシンタックス
show ipv6 mld snooping configuration

コマンドモード
VIEW, ENABLE

使用例
(1) MLD Snooping の構成情報を表示します。

```
# show ipv6 mld snooping configuration
     Group Membership Aging Time = 260(sec)
     Group Membership Leave Time = 10(sec)
     Router Port Aging Time      = 300(sec)
     Router Port Filter          = None
     Immediate Leave Port        = None
     Group Filter                = None
```

```
    Max Member Count
    port count
    1   255
    2   255
  ---(省略)---
    50  255
```

Group Membership Aging Time　：マルチキャストグループメンバーのエージング時間
Group Membership Leave Time　：マルチキャストグループからの脱退時間
Router Port Aging Time　：ルーターポートのエージング時間
Router Port Filter　：ルーターポートのフィルター設定
Immediate Leave Port　：即時脱退処理を行うポート
Group Filter　：マルチキャストグループのフィルター設定
Static Router Port　：手動設定されたルーターポート
Max Member Count　：ポートでマルチキャストグループへの参加を許可するグループ数

関連コマンド

注意事項

3.39.13 show ipv6 mld snooping status

MLD Snooping のステータス情報を表示します。

コマンドシンタックス

show ipv6 mld snooping status

コマンドモード

VIEW, ENABLE

使用例

(1) MLD Snooping のステータス情報を表示します。

```
# show ipv6 mld snooping status

active group count : 0

m:Member r:Router(dynamic) R:Router(static)

 Group Address -----
  Port       1       8 9      16 17     24 25     32 33     40 41     48 49
             +------+ +------+ +------+ +------+ +------+ +------+ +-
   VID   10 R....... ........ ........ ........ ........ ........ ..

#
```

active group count　：登録されたマルチキャストグループ数

Group Address	：登録されたマルチキャストグループアドレス、及びマッピングされた MAC アドレス
Port	：物理ポート番号
r	：ルーター接続ポート
R	：手動設定されたルーターポート
m	：マルチキャストクライアント接続ポート

関連コマンド

注意事項

3.40 DHCP サーバー

DHCP サーバーは、DHCP クライアントに対して IP アドレスなどの構成情報を割り当てる機能です。
なお、DHCP クライアントに割り当てできる IP アドレスは最大で 2048 個です。

3.40.1 dhcp policy

DHCP サーバーの設定は、ネットワークアドレスごとに行います。その設定単位をポリシーと呼びます。設定を削除する場合は、no コマンドを使用してください。また、DHCP リレー装置を経由して DHCP クライアントに IP アドレスを割り当てる場合、DHCP パケットを受信するインターフェースに対してもポリシーの設定が必要です。

本コマンドによって、コマンドモードが DHCP モードに移行します。DHCP モードに移行すると、そのポリシーに関する設定の追加、変更が行えるようになります。

コマンドシンタックス

[no] dhcp policy <POLICY_NAME>

POLICY_NAME　16 文字以内の任意文字列
- ポリシーの数は 128 個まで
- ダブルクォーテーションで囲めば、空白文字を使用可能

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポリシー名：POLICY1 の設定を開始します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)#
```

(2) ポリシー名：POLICY1 に関するすべての設定を削除します。

```
> enable
# configure terminal
(config)# no dhcp policy POLICY1
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

設定したポリシーを有効にするには、"dhcp policy enable"コマンドを使用してください。

DHCP サーバー機能が有効の状態でポリシーの設定を変更することはできません。

複数のポリシーに同一のネットワークアドレスを設定する場合、"range"コマンドの設定は最後に設定したポリシーでのみ動作します。

3.40.2 dhcp policy enable

設定済みのポリシーを有効にします。設定を無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] dhcp policy enable <POLICY_NAME>

POLICY_NAME　　設定済みの DHCP ポリシー名

デフォルト

no enable(＝ポリシー作成時該当ポリシーは無効)

コマンドモード

CONFIG

使用例

(1) ポリシー名：POLICY1 の設定を有効にします。
(2) ポリシー名：POLICY1 の設定を無効にします。

```
> enable
# configure terminal
(config)# dhcp policy enable POLICY1
(config)# no dhcp policy enable POLICY1
```

関連コマンド

show dhcp policy, show running-config

注意事項

ポリシーを有効にするには、"network"コマンドを用いてのサブネットアドレスとサブネットマスクの設定が必須です。

3.40.3 dhcp server enable

DHCP サーバーを有効にします。設定を無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] dhcp server enable

デフォルト

no enable(＝無効)

コマンドモード
CONFIG

使用例
(1) DHCP サーバーを有効にします。
(2) DHCP サーバーを無効にします。

```
> enable
# configure terminal
(config)# dhcp server enable
(config)# no dhcp server enable
```

関連コマンド
show running-config

注意事項

DHCP サーバーを有効にするには、ポリシーを 1 つ以上有効にする必要があります。

DHCP リレー機能との併用はできません。

本機能と 3.47.42 "dhcp-snooping mode mac-authentication"は併用できません。

3.40.4 dhcp server restart

DHCP サーバー起動後に行った設定を反映させるため、DHCP サーバーを再起動します。この時、DHCP サーバーは、再起動後もリースしている IP アドレスの情報(リース先のポート情報を除く)を保持します。

コマンドシンタックス
dhcp server restart

デフォルト
なし

コマンドモード
CONFIG

使用例
(1) DHCP サーバーを再起動します。

```
> enable
# configure terminal
(config)# dhcp server restart
```

関連コマンド
show logging

注意事項

3.40.5 dhcp server address-check arp

DHCP サーバーが DHCP の Discover フレームを受信したときに、IP アドレスを貸し出す前にその IP アドレスの固定端末が存在するかどうかの確認処理を ARP で行うように設定します。設定がない場合は ICMP で行います。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス
[no] dhcp server address-check arp

デフォルト
なし(＝ICMP)

コマンドモード
CONFIG

使用例
(1) IP アドレス重複確認処理を ARP で行うように設定します。

```
> enable
# configure terminal
(config)# dhcp server address-check arp
```

関連コマンド
show running-config

注意事項

3.40.6 dhcp port max-lease-num

ポートごとのリース数制限を行います。設定を削除する場合は、no コマンドを使用してください。リース制限数は 1 から 256 まで行えます。

コマンドシンタックス
dhcp port max-lease-num <PORTNO> <MAX-LEASE>
no dhcp port max-lease-num <PORTNO>

PORTNO	ポート番号
MAX-LEASE	リース制限数 <1-256>

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) ポート番号：1 のリース数を 30 に制限します。

```
> enable
# configure terminal
(config)# dhcp port max-lease-num 1 30
```

関連コマンド
show running-config

注意事項

3.40.7 clear dhcp leases
リース履歴をすべて解放した状態で DHCP サーバーを再起動します。

コマンドシンタックス
clear dhcp leases

コマンドモード
ENABLE

使用例
(1) リース履歴をすべて解放した状態で DHCP サーバーを再起動します。

```
> enable
# clear dhcp leases
```

関連コマンド
show dhcp current

注意事項

3.40.8 network
DHCP サーバーが配布する IP アドレスのネットワークアドレス、サブネットマスクを指定します。設定を削除する場合は、no コマンドを使用してください。DHCP リレー装置を経由して DHCP クライアントに IP アドレスを割り当てる場合、DHCP パケットを受信するインターフェースを指定します。

コマンドシンタックス
[no] network <NETADDR> <NETMASK>
[no] network <NETADDR/MASK>

NETADDR	サブネットアドレス
NETMASK	サブネットマスク

MASK　　サブネットマスク(ビット数)

デフォルト

なし(＝設定なし)

コマンドモード

DHCP

使用例

(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) サブネットアドレスを 192.168.0.0、サブネットマスクを 255.255.255.0 で設定します。
(3) サブネットアドレスとサブネットマスクの設定を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# network 192.168.0.0 255.255.255.0
(config-dhcp)# no network 192.168.0.0 255.255.255.0
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

本コマンドでサブネットアドレスとサブネットマスクの設定が行われていない場合、"dhcp policy enable"コマンドを使用してもそのポリシーは有効にはなりません。

DHCP リレー装置を経由して DHCP クライアントに IP アドレスを割り当てる場合、以下に示す 2 つのポリシーが必要です。

- **DHCP サーバーが配布する IP アドレスのネットワークアドレス、サブネットマスク設定を行うポリシー**
- **DHCP パケットを受信するインターフェースを指定したポリシー**

3.40.9 range

DHCP サーバーが割り当てるアドレスの範囲を設定します。同時に 3 つまで指定できます。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

range <RANGE_ID> <LOW_ADDR> <HIGH_ADDR>
no range <RANGE_ID>

RANGE_ID　　割り当て範囲に対応したレンジ ID <1-3>

LOW_ADDR　　アドレス範囲のうち、下位アドレスを指定
HIGH_ADDR　　アドレス範囲のうち、上位アドレスを指定

デフォルト
なし(＝設定なし)

コマンドモード
DHCP

使用例
(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) 割り当てアドレス範囲：192.168.0.1～192.168.0.9 をレンジ ID が 1 として設定します。
(3) 割り当てアドレス範囲：192.168.1.1～192.168.1.9 をレンジ ID が 2 として設定します。
(4) レンジ ID：1 の設定を削除します。
(5) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# range 1 192.168.0.1 192.168.0.9
(config-dhcp)# range 2 192.168.1.1 192.168.1.9
(config-dhcp)# no range 1
(config-dhcp)# exit
(config)#
```

関連コマンド
show dhcp policy, show running-config

注意事項

"static entry"コマンドで指定するアドレスと重複しないように設定します。

セカンダリーIP アドレスとして設定したアドレス範囲は指定できません。

複数のポリシーに同一のネットワークアドレスを設定する場合、"range"コマンドの設定は最後に設定したポリシーでのみ動作します。

3.40.10 domain-name

クライアントに通知するドメイン名を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス
domain-name <DOMAIN_NAME>
no domain-name

DOMAIN_NAME　　クライアントに通知するドメイン名 <1-255(文字)>
- ASCII 文字
- ダブルクォーテーション、空白文字は使用できません

デフォルト
なし(＝設定なし)

コマンドモード
DHCP

使用例
(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) ドメイン名：apresia.jp を設定します。
(3) ドメイン名の設定を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# domain-name apresia.jp
(config-dhcp)# no domain-name
(config-dhcp)# exit
(config)#
```

関連コマンド
show dhcp policy, show running-config

注意事項

3.40.11 dns-server

クライアントに通知する DNS サーバーを設定します。同時に 3 つまで指定できます。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス
[no] dns-server <IPADDR1> [<IPADDR2> [<IPADDR3>]]

IPADDR1　　1 つ目の DNS サーバーのアドレス
IPADDR2　　2 つ目の DNS サーバーのアドレス
IPADDR3　　3 つ目の DNS サーバーのアドレス

デフォルト
なし(＝設定なし)

コマンドモード
DHCP

使用例

(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) DNS サーバーとして 192.168.0.1、192.168.0.2 を設定します。
(3) DNS サーバー：192.168.0.1 を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# dns-server 192.168.0.1 192.168.0.2
(config-dhcp)# no dns-server 192.168.0.1
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.12 wins-server

クライアントに通知する WINS サーバーを設定します。同時に 3 つまで指定できます。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

[no] wins-server <IPADDR1> [<IPADDR2> [<IPADDR3>]]

IPADDR1	1 つ目の WINS サーバーのアドレス
IPADDR2	2 つ目の WINS サーバーのアドレス
IPADDR3	3 つ目の WINS サーバーのアドレス

デフォルト

なし(＝設定なし)

コマンドモード

DHCP

使用例

(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) WINS サーバーとして 192.168.0.1、192.168.0.2 を設定します。
(3) WINS サーバー：192.168.0.1 を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# wins-server 192.168.0.1 192.168.0.2
(config-dhcp)# no wins-server 192.168.0.1
```

```
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.13 router

クライアントに通知するルーターのアドレスを設定します。同時に 3 つまで指定できます。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

[no] router <IPADDR1> [<IPADDR2> [<IPADDR3>]]

IPADDR1	1 つ目のルーターのアドレス
IPADDR2	2 つ目のルーターのアドレス
IPADDR3	3 つ目のルーターのアドレス

デフォルト

なし(＝設定なし)

コマンドモード

DHCP

使用例

(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) ルーターとして 192.168.0.1、192.168.0.2 を設定します。
(3) ルーター：192.168.0.1 を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# router 192.168.0.1 192.168.0.2
(config-dhcp)# no router 192.168.0.1
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.14 lease

最大リース時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

lease <LEASE_TIME>
no lease
　　LEASE_TIME　　最大リース時間を秒単位で設定 <1-604800(秒)>

デフォルト

604800(秒)

コマンドモード

DHCP

使用例

(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) 最大リース時間として 604800 秒を設定します。
(3) 最大リース時間の設定を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# lease 604800
(config-dhcp)# no lease
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.15 renewing

クライアントがアドレスを取得してから renewing(リースの再延長要求)するまでの時間(秒)を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

renewing <RENEW_TIME>
no renewing
　　RENEW_TIME　　リースの再延長要求するまでの時間を秒単位で設定 <1-604800(秒)>

デフォルト

なし(＝設定なし)

コマンドモード
DHCP

使用例
(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) 再延長時間として 604800 秒を設定します。
(3) 再延長時間の設定を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# renewing 604800
(config-dhcp)# no renewing
(config-dhcp)# exit
(config)#
```

関連コマンド
show dhcp policy, show running-config

注意事項

3.40.16 rebinding

クライアントがアドレスを取得してから rebinding(IP アドレスの再取得)するまでの時間(秒)を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス
rebinding <REBIN_TIME>
no rebinding
REBIN_TIME　IP アドレスの再取得するまでの時間を秒単位で設定 <1-604800(秒)>

デフォルト
なし(＝設定なし)

コマンドモード
DHCP

使用例
(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) 最大リース時間として 604800 秒を設定します。
(3) 最大リース時間の設定を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# rebinding 604800
(config-dhcp)# no rebinding
```

```
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.17 logs

ログサーバーを設定します。同時に3つまで指定できます。設定を削除する場合は、noコマンドを使用してください。

コマンドシンタックス

[no] logs <IPADDR1> [<IPADDR2> [<IPADDR3>]]

IPADDR1	1つ目のログサーバーのアドレス
IPADDR2	2つ目のログサーバーのアドレス
IPADDR3	3つ目のログサーバーのアドレス

デフォルト

なし(＝設定なし)

コマンドモード

DHCP

使用例

(1) DHCPポリシー名：POLICY1の設定を行います。
(2) ログサーバーとして192.168.0.1、192.168.0.2を設定します。
(3) ログサーバー：192.168.0.1を削除します。
(4) DHCPポリシー名：POLICY1の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# logs 192.168.0.1 192.168.0.2
(config-dhcp)# no logs 192.168.0.1
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.18 merit

クライアントに障害が発生したときに、クライアントのコアメモリーイメージをダンプするファイルのパス名を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

merit <PATH_NAME>
no merit
PATH_NAME　　パス名の設定(NVT ASCII 文字) <1-255(文字)>

デフォルト

なし(＝設定なし)

コマンドモード

DHCP

使用例

(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) merit 指定として/tmp を設定します。
(3) merit 指定を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# merit /tmp
(config-dhcp)# no merit
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.19 next-server

初期ブートファイルをロードするサーバーのホストアドレスを設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

next-server <IPADDR>
no next-server
IPADDR　　サーバーの IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

DHCP

使用例

(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) next-server 指定として 192.168.0.1 を設定します。
(3) next-server 指定を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# next-server 192.168.0.1
(config-dhcp)# no next-server
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.20 root-path

クライアントのルートディスクが含まれるパス名を指定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

root-path <PATH_NAME>
no root-path

PATH_NAME	パス名(NVT ASCII 文字) <1-255(文字)> • ダブルクォーテーション、空白文字は使用できません

デフォルト

なし(＝設定なし)

コマンドモード

DHCP

使用例

(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) root-path 指定として/tmp を設定します。
(3) root-path 指定を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
```

```
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# root-path /tmp
(config-dhcp)# no root-path
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.21 ntp-server

クライアントが使用するNTPサーバーのIPアドレスを設定します。NTPサーバーのアドレスは最大3エントリーまで設定可能です。"ntp-server"コマンドは、指定したNTPサーバーのアドレスを現在の設定に追加します。追加の結果登録済みのサーバーのアドレスの数が3を超える場合は、超えた分のサーバーのアドレスは設定されません。NTPサーバーのアドレスを削除する場合は、noコマンドを使用してください。

コマンドシンタックス

[no] ntp-server <NTP_SERVER1> [<NTP_SERVER2> [<NTP_SERVER3>]]

NTP_SERVER1	1つ目のNTPサーバーのアドレス
NTP_SERVER2	2つ目のNTPサーバーのアドレス
NTP_SERVER3	3つ目のNTPサーバーのアドレス

デフォルト

なし(＝設定なし)

コマンドモード

DHCP

使用例

(1) DHCPポリシー名：POLICY1の設定を行います。
(2) NTPサーバーとして、133.141.5.5と10.74.8.1を登録します。
(3) 10.74.8.1のサーバーを削除します。
(4) DHCPポリシー名：POLICY1の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# ntp-server 133.141.5.5 10.74.8.1
(config-dhcp)# no ntp-server 10.74.8.1
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

3.40.22 static-entry

IP アドレスの静的割り当てを行うクライアントの MAC アドレスと IP アドレスを登録します。最大登録数は 2048 個です。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

static-entry <IPADDR> <MACADDR>
no static-entry <IPADDR>

IPADDR	IP アドレス
MACADDR	MAC アドレス

デフォルト

なし(＝設定なし)

コマンドモード

DHCP

使用例

(1) DHCP ポリシー名：POLICY1 の設定を行います。
(2) static-entry 指定として MAC アドレス：00:40:66:00:00:01、IP アドレス：192.168.0.1 を設定します。
(3) static-entry 指定を削除します。
(4) DHCP ポリシー名：POLICY1 の設定を終了します。

```
> enable
# configure terminal
(config)# dhcp policy POLICY1
(config-dhcp)# static-entry 192.168.0.1 00:40:66:00:00:01
(config-dhcp)# no static-entry 192.168.0.1
(config-dhcp)# exit
(config)#
```

関連コマンド

show dhcp policy, show running-config

注意事項

"range"コマンドで指定するアドレス範囲と重複しないように設定する必要があります。

複数のポリシーで同じ MAC アドレスを登録することはできません。

3.40.23 show dhcp current

DHCP サーバーが管理する IP アドレスの割り当て情報を、2048 エントリーまで表示します。all、またはポリシー名を省略した場合は、active エントリーのみ表示されます。

コマンドシンタックス

show dhcp current [all | <POLICY_NAME>]

all	すべてのポリシーの割り当て情報
POLICY_NAME	設定済みの DHCP ポリシー名 <1-16(文字)> • ASCII 文字 • ダブルクォーテーションで囲めば、空白文字を使用可能

コマンドモード

VIEW, ENABLE

使用例

(1) DHCP サーバーが管理する全ポリシーの IP アドレスの割り当て情報を表示します。

```
> enable
# show dhcp current all
Pool: 2       Active: 0
IP Address      MAC Address       State   Type     Lease Expiration        Port
-------------------------------------------------------------------------------
192.168.20.242                     free    dynamic                          -
192.168.20.243                     free    dynamic                          -
```

pool	：最大リース数
Active	：現在リース数
IP Address	：リースした IP アドレス
MAC Address	：リース要求のあった MAC アドレス
State	：アドレスの状態
active	：貸出中
free	：空き
abandon	：すでに使われているなどの理由で貸出不可
Type	：リースアドレスの割り当て種別
dynamic	：動的割り当て
static	：静的割り当て
Lease Expiration	：リース満了時間
Port	：リース先のポート番号

関連コマンド

注意事項

同一装置で 3.46 NA 機能と DHCP サーバーを併用した場合、NA 機能の user-base・user/mac-base 認証設定ポートで、未認証端末が DHCP サーバーより IP アドレスを取

得した場合、"show dhcp current"の Port 表示はされません。「-」となります。

"static-entry"コマンドで割り当てられた IP アドレスが、DHCP クライアントにおいてリリースされた場合は、free エントリーとして表示されます。

3.40.24 show dhcp policy

DHCP ポリシーの構成情報を出力します。

コマンドシンタックス

show dhcp policy <POLICY_NAME> | all

POLICY_NAME　設定済みの DHCP ポリシー名 <1-16(文字)>

- ASCII 文字
- ダブルクォーテーションで囲めば、空白文字を使用可能

コマンドモード

VIEW, ENABLE

使用例

(1) DHCP ポリシー名：test の構成情報を表示します。

```
> enable
# show dhcp policy test
 Policy Name     : test
   Status        : disable
   Subnet        : 192.168.0.0
   Netmask       : 255.255.255.0
   Range         : 192.168.0.1  192.168.0.9
   Domain Name   : apresia.jp
   DNS Server    : 192.168.0.1  192.168.0.2
   Router        : 192.168.0.5  192.168.0.6
   Lease time    : 604800
   WINS server   : 192.168.0.3  192.168.0.4
   Merit         : /tmp
   Root path     : /boot
   Static entry  : 192.168.0.100   00:40:66:00:00:01
```

関連コマンド

注意事項

3.41 MMRP

MMRP(Multi Master Ring Protocol)機能は、Apresia シリーズによるリング型ネットワークをサポートします。

注意事項

MMRP、3.42 MMRP-Plus、3.43 MMRP2 aware を同一リングで混在して使用することはできません。

MMRP、MMRP-Plus を装置で同時に使用することはできません。

MMRP が動作している LAG(リンクアグリゲーショングループ)への、ポートの追加、削除は行えません。

MMRP 設定時に、3.47 AccessDefender 機能、3.39 MLD 機能の 3 機能を同時に併用できません。

MMRP と STP との同一装置内での併用は可能ですが、RSTP、MSTP を使用した場合の動作は保証されません。

マスタースイッチとして設定できるのは、Apresia13000-48X のみです。これ以外の機種はアウェアスイッチとしてのみ設定できます。

3.28 パケットフィルター2 機能併用時に、MMRP 機能よりも小さいグループ番号でパケットフィルター2 機能を設定する場合、ethertype 0x8820 の MMRP 制御フレームがフィルター対象とならないように設定してください。

Apresia13000-48X では、ポートブロック(port 1～24、50 と port 25～49)を跨いだリンクアグリゲーションを MMRP で使用するポートとして設定しないでください。

3.41.1 mmrp switch hello-interval

マスターポート、及びスレーブポートから送信する MMRP ハローフレームの送信間隔を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp switch hello-interval <INTERVAL>
no mmrp switch hello-interval

INTERVAL　MMRP ハローフレーム送信間隔 <1(100 ミリ秒)-10(1000 ミリ秒)>
- 設定は 1 から 10 までの整数で指定
- 1 は 100 ミリ秒に相当

デフォルト
1(＝100 ミリ秒)

コマンドモード
CONFIG

使用例
(1) MMRP ハローフレーム送信間隔を 500 ミリ秒に変更します。

```
> enable
# configure terminal
(config)# mmrp switch hello-interval 5
```

関連コマンド
show mmrp configuration, show running-config

注意事項

MMRP ハローフレームの送信間隔を大きくすると、ネットワークの構成により MMRP の動作が不安定になることがあります。

3.41.2 mmrp group

MMRP で使用するグループを設定します。設定を削除する場合は、no コマンドを使用してください。
MMRP では、本コマンドで設定した番号のパケットフィルター2 のグループを使用して動作します。MMRP の動作中は、使用しているグループを他の機能で指定することはできません。また、他の機能で使用しているグループを MMRP で指定することもできません。

コマンドシンタックス
mmrp group <GROUP> [<NUMBER>]
no mmrp group

GROUP	MMRP で使用するグループの先頭番号 • Apresia4328：<1-7> • Apresia3400/4348/5400/13000 シリーズ：<1-14>
NUMBER	グループ数の指定 • Apresia5412 シリーズ/13000-24GX：<1> • Apresia3424/4300 シリーズ/5428GT/13000-48X：<1-2> • Apresia3448：<1-3>

デフォルト
1(グループ 1 を使用)　　：Apresia3400/4328/5400 シリーズ/13000-24GX
2(グループ 1、2 を使用)：Apresia4348 シリーズ/13000-48X

コマンドモード
CONFIG

使用例

(1) MMRP がグループ：10、11 を使用するように設定します。

(2) MMRP グループを削除します。

```
> enable
# configure terminal
(config)# mmrp group 10 2
(config)# no mmrp group
```

関連コマンド

show mmrp configuration, show running-config, assign

注意事項

表 3-19 の各コマンドは、パケットフィルター2 のグループを使用するため、これら機能設定がある場合、使用するグループが重複し、MMRP を有効("mmrp enable")にできない場合があります。その場合は、指定するグループ番号を変更し再度有効にしてください。

MMRP 機能は 3.43 MMRP2 aware 機能と同一のグループを使用します。両機能を併用させる場合、必ず同一のグループ番号を指定してください。

本機能の使用ポート数に応じてパケットフィルター2 のグループを使用します。使用可能ポート数と使用グループ数は以下のとおり決まります。

Apresia3400/4300/5400/13000-48X 使用可能ポート数	Apresia13000-24GX 使用可能ポート数	パケットフィルター2 使用グループ数
1～25	28	1
26～50	-	2
51～52	-	3

本機能として使用できるポート数については以下を参照ください。なお論理ポート(リンクアグリゲーション機能)も 1 つのポートとして認識します。

- **シングルマスター構成(マスタースイッチ)：1 リングに対し 2 ポート必要**
- **分散マスター構成(マスタースイッチ)：1 リングに対し 1 ポート必要**
- **MMRP アウェアスイッチ：1 リングに対し 1 ポート必要**

本装置再起動後は構成情報の記載順にパケットフィルター2 のグループが確保されます。他機能で確保済みのグループを本コマンドで指定した場合、MMRP 機能は有効になりません。

3.41.3 mmrp enable

MMRP を有効にします。無効にする場合は、no コマンドを使用してください。

MMRP は、パケットフィルター2 のグループを使用します。"mmrp group"で指定したグループを確保で

きない場合は、本設定はエラーを返します。本設定が有効な間は、"mmrp group"コマンドで指定したグループ設定を変更することはできません。また、本設定が有効な間は、MMRP-Plus を有効にすることはできません。

以下のコマンドで設定した MMRP のリング動作を開始するには本設定が必須です。

(1) 3.41.5 mmrp ring master master-port slave-port
(2) 3.41.8 mmrp ring aware port
(3) 3.41.9 mmrp ring divided-master master-port
(4) 3.41.15 mmrp ring divided-shadow slave-port

コマンドシンタックス

[no] mmrp enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) MMRP を有効にします。
(2) MMRP を無効にします。

```
> enable
# configure terminal
(config)# mmrp enable
(config)# no mmrp enable
```

関連コマンド

show mmrp status, show running-config, assign

注意事項

プライマリーIP アドレスを 86 個以上設定した場合は、MMRP 機能で使用するデフォルトグループと重複するため、MMRP 機能を有効にすることはできません。
デフォルトグループと重複するプライマリーIP アドレス設定数
- **Apresia3400/4348/5400/13000 シリーズ：86 個以上**
- **Apresia4328 シリーズ：43 個以上**

表 3-19、表 3-20 を参考に"mmrp group"コマンドで重複しないグループ番号に設定を変更してください。

3.41.4 no mmrp ring

MMRP の設定をリング名ごとに無効します。本コマンドは、指定したリング名を使用しているすべての設定を無効にします。

コマンドシンタックス

no mmrp ring <NAME>

NAME	MMRP リング名 <1-32(文字)>

デフォルト

なし

コマンドモード

CONFIG

使用例

(1) ring01 を削除します。

```
> enable
# configure terminal
(config)# no mmrp ring ring01
```

関連コマンド

show mmrp configuration, show running-config

注意事項

3.41.5 mmrp ring master master-port slave-port

マスタースイッチのマスターポートとスレーブポートを設定します。設定を削除する場合は、no コマンドを使用してください。

ポートの代わりに LAG(リンクアグリゲーショングループ)を指定することもできます。その場合、3.8 リンクアグリゲーションにより事前に LAG の設定を行う必要があります。

コマンドシンタックス

mmrp ring <NAME> master master-port <PORT1> slave-port <PORT2>

mmrp ring <NAME> master master-lag <LAG1> slave-lag <LAG2>

no mmrp ring <NAME>

NAME	MMRP リング名 <1-32(文字)>
PORT1	マスターポート
PORT2	スレーブポート
LAG1	マスターLAG ID
LAG2	スレーブ LAG ID

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 のポート：25 をマスターポート、ポート：26 をスレーブポートに設定します。
(2) リング名：ring01 のポート：25 をマスターポート、LAG ID：1 をスレーブ LAG ID に設定します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 master master-port 25 slave-port 26
(config)# no mmrp ring ring01
(config)# mmrp ring ring01 master master-port 25 slave-lag 1
```

関連コマンド

show mmrp configuration, show mmrp configuration ring, show running-config

注意事項

MMRP アウェア機能を搭載しないスイッチングハブをリングのノードとしたネットワークを構築する場合、そのスイッチングハブでのリンク障害が復旧するとき、リング型ネットワークが一時的にループになり、ブロードキャストストームが発生することがあります。フラッディング制限機能を併用することにより、ブロードキャストストームを最小限に抑えることができます。

本コマンドにより LAG を指定する場合は、先にリンクアグリゲーションにより LAG を設定しておく必要があります。

本コマンドにより指定した LAG に対して、リンクアグリゲーションによりポートの追加、削除はできません。LAG の設定を変更する場合は、いったん"no mmrp ring"コマンドでリングの設定を削除する必要があります。

Apresia13000-48X では、LAG に含まれる XENPAK ポート(ポート番号 49、50)を、マスターポート、及びスレーブポートに設定した場合、動作は保証されません。

3.41.6 mmrp ring master master-vid

マスタースイッチのマスターポートから送信する MMRP ハローフレームの VLAN ID を変更します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> master master-vid <VID>
no mmrp ring <NAME> master master-vid

NAME	MMRP リング名 <1-32(文字)>
VID	マスターポートから送信する MMRP ハローフレームの VLAN ID <1-4094>

デフォルト

なし(＝untag)

コマンドモード
CONFIG

使用例
(1) リング名：ring01 のマスタースイッチのマスターポートから送信する MMRP ハローフレームの VLAN ID を 100 に変更します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 master master-vid 100
```

関連コマンド
show mmrp configuration, show mmrp configuration ring, show running-config

注意事項

3.41.7 mmrp ring master slave-vid

マスタースイッチのスレーブポートから送信する MMRP フレームの VLAN ID を変更します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス
mmrp ring <NAME> master slave-vid <VID>
no mmrp ring <NAME> master slave-vid

NAME	MMRP リング名 <1-32(文字)>
VID	スレーブポートから送信する MMRP ハローフレームの VLAN ID <1-4094>

デフォルト
なし(＝untag)

コマンドモード
CONFIG

使用例
(1) リング名：ring01 のマスタースイッチのスレーブポートから送信する MMRP ハローフレームの VLAN ID を 100 に変更します。

```
# configure terminal
(config)# mmrp ring ring01 master slave-vid 100
```

関連コマンド
show mmrp configuration, show mmrp configuration ring, show running-config

注意事項

3.41.8 mmrp ring aware port

アウェアスイッチのポートを設定します。ポートの代わりに3.8 リンクアグリゲーションにより設定した LAG(リンクアグリゲーショングループ)を指定することもできます。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

```
mmrp ring <NAME> aware port <PORT> port <PORT>
mmrp ring <NAME> aware lag <LAG> lag <LAG>
mmrp ring <NAME> aware lag <LAG> port <PORT>
no mmrp ring <NAME>
```

NAME	MMRP リング名 <1-32(文字)>
PORT	MMRP リングを構成するポート
LAG	MMRP リングを構成する LAG ID

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：41 とポート：48 をリング名：ring01 のアウェアポートとして設定します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 aware port 41 port 48
```

関連コマンド

show mmrp configuration, show mmrp configuration ring, show running-config, switchport mode, switchport trunk

注意事項

本コマンドにより指定した LAG に対して、リンクアグリゲーションコマンドによりポートの追加、削除はできません。LAG の設定を変更する場合は、いったん"no mmrp ring"コマンドでリングの設定を削除する必要があります。

設定したアウェアポートがトランクポートモードに設定されている場合、必ずポートにネイティブ VLAN の設定をしてください。設定しない場合は、リングの切り替え動作が遅くなる場合があります(ネイティブ VLAN は、"switchport trunk native <VID>" (3.11.6 "switchport trunk")コマンドで設定した VLAN です)。

同一 MMRP リングを構成しているポートの untag/native VLAN には同じ VLAN ID を設定してください。

Apresia13000-48X では、LAG に含まれる XENPAK ポート(ポート番号 49、50)を、アウェアポートに設定した場合、動作は保証されません。

3.41.9 mmrp ring divided-master master-port

分散マスタースイッチのマスターポートを設定します。ポートの代わりにリンクアグリゲーションコマンドにより LAG(リンクアグリゲーショングループ)を指定することもできます。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

```
mmrp ring <NAME> divided-master master-port <PORT>
mmrp ring <NAME> divided-master master-lag <LAG>
no mmrp ring <NAME>
```

NAME	MMRP リング名 <1-32(文字)>
PORT	マスターポート
LAG	マスターLAG ID

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：25 をリング名：ring01 のマスターポートとして分散マスタースイッチを設定します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-master master-port 25
```

関連コマンド

show mmrp configuration, show mmrp configuration ring, show running-config

注意事項

Apresia13000-48X では、LAG に含まれる XENPAK ポート(ポート番号 49、50)を、マスターポートに設定した場合、動作は保証されません。

3.41.10 mmrp ring divided-master master-vid

分散マスタースイッチのマスターポートから送信する MMRP ハローフレームの VLAN ID を変更します。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

```
mmrp ring <NAME> divided-master master-vid <VID>
```

no mmrp ring <NAME> divided-master master-vid

NAME	MMRP リング名 <1-32(文字)>
VID	マスターポートから送信する MMRP ハローフレームの VLAN ID <1-4094>

デフォルト

なし(untag)

コマンドモード

CONFIG

使用例

(1) リング名:ring01 の分散マスタースイッチのマスターポートから送信する MMRP ハローフレームの VLAN ID を 100 に変更します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-master master-vid 100
```

関連コマンド

show mmrp configuration, show mmrp configuration ring, show running-config

注意事項

3.41.11 mmrp ring divided-master uplink-forcedown-method

分散マスタースイッチが管理するリング上において、障害の発生と復旧により MMRP が動作したとき、アップリンクポートを瞬断します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> divided-master uplink-forcedown-method an-restart | phy-stop
no mmrp ring <NAME> divided-master uplink-forcedown-method

NAME	MMRP リング名 <1-32(文字)>
an-restart	自動認識機能(3.7.4 "auto-negotiation")のリスタートによりアップリンクポートを瞬断
phy-stop	一定時間送信を停止することによりアップリンクポートを瞬断

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 のアップリンクを phy-stop により瞬断します。

```
> enable
# configure terminal
```

```
(config)# mmrp ring ring01 divided-master uplink-forcedown-method phy-stop
```

関連コマンド

show mmrp configuration, show running-config

注意事項

本機能は、リング上で MMRP が動作し経路が変更されたときに、アップリンクポートに接続されるスイッチングハブの MAC アドレステーブルをクリアするためのものです。ネットワークの構成によっては、本機能を有効にする必要はありません。

対向装置に、アップリンク瞬断機能によるリンク断の通知ができない場合は、本機能は使用できません。

本機能により、アップリンクポート経由の通信が一時的に停止します。

自動認識機能("auto-negotiation")のリスタートによる瞬断では、MAC アドレステーブルがクリアされないスイッチングハブがあります。

XENPAK ポートは、自動認識機能("auto-negotiation")のリスタートでは瞬断しません。

3.41.12 mmrp ring divided-master uplink-forcedown-time

分散マスタースイッチのアップリンク瞬断機能において、ポートの送信を停止する時間を変更します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> divided-master uplink-forcedown-time <TIME>
no mmrp ring <NAME> divided-master uplink-forcedown-time

NAME	MMRP リング名 <1-32(文字)>
TIME	アップリンクポートを瞬断させる時間 <1(100 ミリ秒)-30(3000 ミリ秒)> • 設定は 1 から 30 までの整数で指定 • 1 は 100 ミリ秒に相当

デフォルト

5(500 ミリ秒)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 の瞬断時間を 1000 ミリ秒に変更します。

```
> enable
```

```
# configure terminal
(config)# mmrp ring ring01 divided-master uplink-forcedown-time 10
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

アップリンクポートに接続するスイッチングハブによって、MAC アドレステーブルをクリアするために必要な瞬断時間は異なります。

3.41.13 mmrp ring divided-master uplink-port

分散マスタースイッチのアップリンクポートを指定します。指定したアップリンクポートにリンク障害が発生したとき、MMRP が動作しスレーブポートが Forwarding になります。設定をデフォルトに戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> divided-master uplink-port <PORTRANGE>
no mmrp ring <NAME> divided-master uplink-port

NAME	MMRP リング名 <1-32(文字)>
PORTRANGE	分散マスター機能のアップリンクポート(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 のアップリンクポートをポート：1～5 に設定します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-master uplink-port 1-5
```

関連コマンド

show mmrp configuration, show running-config

注意事項

以下の機能とアップリンクポートは同一ポートで併用できません。

- **LACP 機能(3.8 リンクアグリゲーション参照)**
- **3.17 スパニングツリープロトコル(STP/RSTP/MSTP)**

3.41.14 mmrp ring divided-master uplink-up-wait

分散マスタースイッチのアップリンクポート瞬断後のリンクアップ待ち時間を変更します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> divided-master uplink-up-wait <TIME>
no mmrp ring <NAME> divided-master uplink-up-wait

NAME	MMRP リング名 <1-32(文字)>
TIME	リンクアップ待ち時間 <1(100 ミリ秒)-50(5000 ミリ秒)> • 設定は 1 から 50 までの整数で指定 • 1 は 100 ミリ秒に相当

デフォルト

30(3000 ミリ秒)

コマンドモード

CONFIG

使用例

(1) アップリンクポートの瞬断後のリンクアップ待ち時間を 1000 ミリ秒に変更します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-master uplink-up-wait 10
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

リンクアップ待ち時間を小さくしすぎると、リンクアップ待ち時間以内にリンクアップしないときに MMRP の不要な切り替り/切り戻りが生じることがあります。

3.41.15 mmrp ring divided-shadow slave-port

分散シャドウスイッチのスレーブポートを設定します。ポートの代わりに 3.8 リンクアグリゲーションにより設定した LAG(リンクアグリゲーショングループ)を指定することもできます。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> divided-shadow slave-port <PORT>
mmrp ring <NAME> divided-shadow slave-lag <LAG>
no mmrp ring <NAME>

NAME	MMRP リング名 <1-32(文字)>
PORT	スレーブポート

LAG　　スレーブ LAG ID

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) ポート：26 をリング名：ring01 のスレーブポートとして分散シャドウスイッチを設定します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-shadow slave-port 26
```

関連コマンド
show mmrp configuration, show mmrp configuration ring, show running-config

注意事項

本コマンドにより LAG を指定する場合は、先にリンクアグリゲーションより、LAG を設定しておく必要があります。

本コマンドにより指定した LAG に対して、リンクアグリゲーションによりポートの追加、削除はできません。LAG の設定を変更する場合は、いったん"no mmrp ring"コマンドでリングの設定を削除する必要があります。

Apresia13000-48X では、LAG に含まれる XENPAK ポート(ポート番号 49、50)を、スレーブポートに設定した場合、動作は保証されません。

3.41.16 mmrp ring divided-shadow slave-vid

分散シャドウスイッチのスレーブポートから送信する MMRP ハローフレームの VLAN ID を変更します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス
mmrp ring <NAME> divided-shadow slave-vid <VID>
no mmrp ring <NAME> divided-shadow slave-vid

NAME　　MMRP リング名 <1-32(文字)>
VID　　MMRP ハローフレームの VLAN ID <1-4094>

デフォルト
なし(＝untag)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 のスレーブポートから送信する MMRP ハローフレームの VLAN ID を 100 に変更します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-shadow slave-vid 100
```

関連コマンド

show mmrp configuration, show mmrp configuration ring, show running-config

注意事項

3.41.17 mmrp ring divided-shadow uplink-forcedown-method

分散シャドウスイッチが管理するリング上において、障害の発生と復旧により MMRP が動作したとき、アップリンクポートを瞬断します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> divided-shadow uplink-forcedown-method an-restart | phy-stop
no mmrp ring <NAME> divided-shadow uplink-forcedown-method

NAME	MMRP リング名 <1-32(文字)>
an-restart	自動認識機能(3.7.4 "auto-negotiation")のリスタートによりアップリンクポートを瞬断
phy-stop	一定時間送信を停止することによりアップリンクポートを瞬断

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 のアップリンクを自動認識機能("auto-negotiation")のリスタートにより瞬断する設定にします。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-shadow uplink-forcedown-method an-restart
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

本機能は、リング上で MMRP が動作し経路が変更されたときに、アップリンクポートに接続されるスイッチングハブの MAC アドレステーブルをクリアするためのものです。ネットワークの構成によっては、本機能を有効にする必要はありません。

対向装置に、アップリンク瞬断機能によるリンク断の通知ができない場合は、本機能は使用できません。

本機能により、アップリンクポート経由の通信が一時的に停止します。

自動認識機能("auto-negotiation")のリスタートによる瞬断では、MAC アドレステーブルがクリアされないスイッチングハブがあります。

XENPAK ポートは、自動認識機能("auto-negotiation")のリスタートでは瞬断しません。

3.41.18 mmrp ring divided-shadow uplink-forcedown-time

分散シャドウスイッチのアップリンク瞬断機能において、ポートの送信を停止する時間を変更します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> divided-master uplink-forcedown-time <TIME>
no mmrp ring <NAME> divided-master uplink-forcedown-time

NAME　MMRP リング名 <1-32(文字)>
TIME　アップリンクポートを瞬断させる時間 <1(100 ミリ秒)-30(3000 ミリ秒)>
- 設定は 1 から 30 までの整数で指定
- 1 は 100 ミリ秒に相当

デフォルト

5(500 ミリ秒)

コマンドモード

CONFIG

使用例

(1) リング名:ring01 の分散シャドウスイッチのアップリンクポート瞬断時間を 1000 ミリ秒に変更します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-shadow uplink-forcedown-time 10
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

アップリンクポートに接続するスイッチングハブによって、MAC アドレステーブルを消去するために必要な瞬断時間は異なります。

3.41.19 mmrp ring divided-shadow uplink-port

分散シャドウスイッチのアップリンクポートを変更します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

```
mmrp ring <NAME> divided-shadow uplink-port <PORTRANGE>
no mmrp ring <NAME> divided-shadow uplink-port
```

NAME	MMRP リング名 <1-32(文字)>
PORTRANGE	分散シャドウスイッチのアップリンクポート(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング名:ring01の分散シャドウスイッチのアップリンクポートをポート:1～5に設定します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-shadow uplink-port 1-5
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

以下の機能とアップリンクポートは同一ポートで併用できません。

- **LACP 機能(3.8 リンクアグリゲーション参照)**
- **3.17 スパニングツリープロトコル(STP/RSTP/MSTP)**

3.41.20 mmrp ring divided-shadow uplink-up-wait

分散シャドウスイッチのアップリンクポート瞬断後のリンクアップ待ち時間を変更します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

```
mmrp ring <NAME> divided-shadow uplink-up-wait <TIME>
```

no mmrp ring <NAME> divided-shadow uplink-up-wait

NAME　　MMRP リング名 <1-32(文字)>

TIME　　リンクアップ待ち時間 <1(100 ミリ秒)-50(5000 ミリ秒)>

- 設定は 1 から 50 までの整数で指定
- 1 は 100 ミリ秒に相当

デフォルト

30(3000 ミリ秒)

コマンドモード

CONFIG

使用例

(1) 分散シャドウスイッチのアップリンクポートの瞬断後のリンクアップ待ち時間を1000ミリ秒に変更します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 divided-shadow uplink-up-wait 10
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

リンクアップ待ち時間を小さくしすぎると、リンクアップ待ち時間以内にリンクアップしないときに MMRP の不要な切り替り/切り戻りが生じることがあります。

3.41.21 mmrp ring fdb-flush-timer

MMRP による MAC アドレステーブルのクリア後の MAC アドレス学習停止時間を変更します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> fdb-flush-timer <TIME>

no mmrp ring <NAME> fdb-flush-timer

NAME　　MMRP リング名 <1-32(文字)>

TIME　　MAC アドレスクリア後、学習を停止してフレームを中継する時間 <0-10(秒)>

- 0 を指定した場合学習を停止しない。

デフォルト

5(秒)

コマンドモード

CONFIG

使用例

(1) FDB 消去後の無学習時間を 1 秒に変更します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 fdb-flush-timer 1
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

L3 機能と MMRP 機能を併用する場合、"mmrp ring fdb-flush-timer"の値を 0 にしてください(本タイマーが満了するまで ARP の学習を開始しません)。

3.41.22 mmrp ring listening-timer

MMRPが設定されているポートがリンクアップした直後に遷移するListening状態のタイムアウト時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> listening-timer <TIME>
no mmrp ring <NAME> listening-timer

NAME	MMRP リング名 <1-32(文字)>
TIME	タイムアウト時間 <1-1000000(秒)>

デフォルト

3(秒)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 の MMRP を構成するポートのリスニングタイムアウト時間を 30 秒に変更します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 listening-timer 30
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

3.41.23 mmrp ring bidirectional-check disable

片断線監視機能の動作を無効にします。有効に戻す場合は、no コマンドを使用してください。

片断線監視機能は、マスターポートからスレーブポートへ向かう片方向通信断を検出し、その逆方向のループ(片方向ループ)を防止するためにマスターポートを閉塞状態にする機能です。本機能を無効にする場合、MMRP リングの片方向通信断時に、マスターポート、及びスレーブポート両方がフォワード状態になり、片方向ループ状態となる可能性があります。

コマンドシンタックス

mmrp ring <NAME> bidirectional-check disable
no mmrp ring <NAME> bidirectional-check disable
NAME　　MMRP リング名 <1-32(文字)>

デフォルト

no disable(＝有効)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 の片断線監視機能を無効にします。

```
> enable
# configure terminal
(config)# mmrp ring ring01 bidirectional-check disable
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

3.41.24 mmrp ring bidirectional-check error-disabled-timer

片断線監視機能において、マスターポートが片方向通信断を検出してから、マスターポートを閉塞状態にするまでのタイムアウト時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp ring <NAME> bidirectional-check error-disabled-timer <TIME>
no mmrp ring <NAME> bidirectional-check error-disabled-timer
NAME　　MMRP リング名 <1-32(文字)>
TIME　　タイムアウト時間 <3-1000000(秒)>

デフォルト

10(秒)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 のタイムアウト時間を 5 秒に変更します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 bidirectional-check error-disabled-timer 5
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

3.41.25 mmrp ring bidirectional-check revertive-timer

マスターポートが片方向ループでないことを検出し、閉塞したポートを Forwarding 状態に遷移させるまでの遅延時間です。設定をデフォルトに戻す場合は、no コマンドを使用してください。

マスターポートは、スレーブポートからハローフレームが到着しないか、スレーブポートから Blocking 状態を示すハローフレームを受信したときに、片方向ループでないと判定します。

コマンドシンタックス

mmrp ring <NAME> bidirectional-check revertive-timer <TIME>
no mmrp ring <NAME> bidirectional-check revertive-timer

NAME	MMRP リング名 <1-32(文字)>
TIME	遅延時間 <3-1000000(秒)>

デフォルト

なし(自動復旧しない)

コマンドモード

CONFIG

使用例

(1) リング名：ring01 の遅延時間を 5 秒に設定します。

```
> enable
# configure terminal
(config)# mmrp ring ring01 bidirectional-check revertive-timer 5
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

3.41.26 show mmrp status

MMRP の動作状態を表示します。

コマンドシンタックス

show mmrp status

コマンドモード

VIEW, ENABLE

使用例

(1) MMRP の動作状態を表示します。

```
> show mmrp status
 R.M.: Ring Master, R.A.: Ring Aware, D.M.: Divided Master, S.M.: Shadow Master
-------------------------------------------------------------------------------
 Pt.  Link     MMRP          MMRP         Connection   Ring name
 /Lag Status   Port Mode     Port Status  Status
-------------------------------------------------------------------------------
  1   100M/F   D.M. Master   Forwarding   Normal       ring01
  2   100M/F   R.M. Master   Forwarding   Normal       ring02
  3   100M/F   S.M. Slave    Blocking     Normal       ring03
  4   100M/F   R.M. Slave    Blocking     Normal       ring16
  5   100M/F   D.M. Master   Forwarding   Normal       ring05
 L 1  100M/F   R.M. Master   Forwarding   Normal       ring04
 L 2  100M/F   R.M. Slave    Blocking     Normal       ring04
                             --- 以下省略 ---
```

Pt./Lag　：ポート番号、または LAG(リンクアグリゲーショングループ) ID
Link Status　：リンク状態
MMRP Port Mode　：ポートに設定されている MMRP 動作モードと MMRP ポートタイプ
　R.M.　：マスタースイッチ
　R.A.　：アウェアスイッチ
　D.M.　：分散マスタースイッチ
　S.M.　：分散シャドウスイッチ
　Master　：マスターポート
　Slave　：スレーブポート
　Default　：アウェアにハローフレームを受信せずマスターポート、スレーブポートが決定していない状態
MMRP Port Status　：MMRP が設定されているポートの MMRP 動作状態
　Down　：リンクダウン状態
　Listening　：ポートがリンクアップした直後のネットワークのループを防ぐ Listening 状態
　MMRP 制御フレームだけを中継し、他のユーザーフレームは中継しない
　Forwarding　：ユーザーフレームを中継する Forwarding 状態
　Blocking　：すべてのフレームを廃棄する Blocking 状態
　ネットワークが物理的にループになるのを防ぐ

R.M.スレーブ、または S.M.スレーブに設定されているポートだけが遷移

Disabled(U)　：リングトラヒックのマスターからスレーブに向かう片方向の
Disabled(D)　　通信断を装置が検出し、ポートを閉塞している状態
括弧内は、そのポートがリンクアップしている場合は"U"、
リンクダウンしている場合は"D"と表示

Connection Status　：リングの接続状態
Normal　：リング型ネットワーク上に障害がないことを表す
Broken　：リング型ネットワーク上に障害が発生し、MMRP ハローフレームが到達していないことを表す
Abnormal　：MMRP ハローフレームが逆流していることを表す
マスターポート同士、スレーブポート同士を接続すると表示される
Loop Detect　：リングトラヒックのスレーブからマスターに向かう片方向のループが発生したことを検出した場合に表示

Ring name　：MMRP が管理するリング型ネットワークの呼称
11 文字以上の呼称を設定している場合は、10 文字に短縮して表示

関連コマンド

注意事項

3.41.27 show mmrp status port

ポートごとの詳細な MMRP の状態を表示します。ポートの代わりに 3.8 リンクアグリゲーションにより設定した LAG(リンクアグリゲーショングループ)、またはリング名を指定することもできます。

コマンドシンタックス

show mmrp status port <PORTRANGE>
show mmrp status lag <LAG>

PORTRANGE　表示するポート番号(複数指定可能)
LAG　表示する LAG ID

コマンドモード

VIEW, ENABLE

使用例

(1) ポート：1 の MMRP の詳細な状態を表示します。

```
> show mmrp status port 1
==============================================================================
Port  1
  Ring Name : ring01
  Type      : Ring Master Master Port
  Status    : Forwarding
  Connection: Normal
-------------------------------------------------------------
```

```
  Frame Type       Receive Frame Count     Transmit Frame Count
-------------------------------------------------------------
  HelloA                             0                     3473
  HelloB                          3470                        0
  HelloF                            19                        -
  FDB Flush                          0                        0
  Link Down                          0                        0
  Link Up                            1                        0
  Blocking                           1                        0
```

Port　：ポート番号
Lag　：LAG ID
Ring Name　：MMRP が管理するリング型ネットワークの呼称
Type　：ポートに設定されている MMRP 動作モードと MMRP ポートタイプ
Status　：MMRP が設定されているポートの MMRP 動作状態
Connection　：リングの接続状態を表示
Frame Type　：MMRP 制御フレームの種別
  HelloA　：マスターポートから送信される MMRP ハローフレーム
  HelloB　：スレーブポートから送信される MMRP ハローフレーム
  HelloF　：スレーブポートから送信される片断線監視機能用の MMRP ハローフレーム
  FDB Flush　：MAC アドレステーブルのクリアを表すフレーム
  Link Down　：リンクダウン障害が発生したことを表す制御フレーム
  Link Up　：リンクダウン障害が復旧し、リンクアップしたことを表すフレーム
  Blocking　：スレーブポートがスレーブ状態に遷移したことを表すフレーム
Receive Frame Count　：受信したフレーム数
Transmit Frame Count　：送信したフレーム数

関連コマンド

注意事項

3.41.28 show mmrp configuration

MMRP の構成情報を表示します。

コマンドシンタックス

show mmrp configuration

コマンドモード

VIEW, ENABLE

使用例

(1) MMRP の構成情報を表示します。

```
> show mmrp configuration
```

```
MMRP Switch Configuration:
        Status          : Enable
        Group           : 12
        Hello time      : 100ms

MMRP Ring Configuration:
 R.M.: Ring Master, R.A.: Ring Aware, D.M.: Divided Master, S.M.: Shadow Master
-------------------------------------------------------------------------------
 Ring name  Mode  Pt. VLAN Type    Pt. VLAN Type
-------------------------------------------------------------------------------
 node240    R.M.  25  1    Master  26  1    Slave
 ring01     R.M.  L1  ---- Master  L24 ---- Slave
```

Hello time　：MMRP ハローフレームを送信する間隔
Ring name　：MMRP が管理するリング型ネットワークの呼称
　　11 文字以上の呼称を設定している場合は、10 文字に短縮して表示
Mode　：MMRP 動作モード
Pt.　：ポート番号、または LAG(リンクアグリゲーショングループ) ID
VLAN　：MMRP ハローフレームの VLAN ID
Type　：MMRP ポートタイプ

関連コマンド

注意事項

3.41.29 show mmrp configuration ring

MMRP リングの詳細な構成情報を表示します。

コマンドシンタックス

show mmrp configuration ring <NAME>
　NAME　　MMRP リング名 <1-32(文字)>

コマンドモード

VIEW, ENABLE

使用例

(1) リング名：ring01 の MMRP リングの詳細な構成情報を表示します。
(2) リング名：ring02 の MMRP リングの詳細な構成情報を表示します。

```
> show mmrp configuration ring ring01
Ring name: ring01
  Type          : Ring Master
  Master port   : 1
    VLAN ID     : untag
  Slave port    : 13
    VLAN ID     : untag
```

```
  Listening Time: 3s
  FDB Flush Time: 5s
  Bidirectional Check : Enable
      Failure Time    : 5s
      Revertive Time  : 5s
> show mmrp configuration ring ring02
Ring name: ring02
  Type          : Ring Aware
  Aware Port 1  : 25
  Aware Port 2  : 26
  Listening Time: 3s
  FDB Flush Time: 5s
```

Ring name	：MMRP が管理するリング型ネットワークの呼称
Type	：MMRP 動作モード
Master port	：マスターポートのポート番号
Master lag	：マスターLAG(リンクアグリゲーショングループ) ID
VLAN ID	：MMRP ハローフレームの VLAN ID
Slave port	：スレーブポートのポート番号
Slave lag	：スレーブ LAG ID
Aware Port	：アウェアポートのポート番号
Aware Lag	：アウェア LAG ID
Listening Time	：Listening 状態のタイムアウト時間
FDB Flush Time	：MAC アドレステーブルクリア後のアドレス無学習時間
Bidirectional Check	：双方向監視機能の動作状態
Failure Time	：双方向監視機能において、マスターポートがスレーブポートの Forwarding 状態を検出してからポートを閉塞するまでの遅延時間
Revertive Time	：双方向監視機能において、マスターポートがスレーブポートのスレーブ状態を検出してからポートを Forwarding 状態にするまでの遅延時間

関連コマンド

注意事項

3.41.30 show tech-support mmrp

MMRP 機能の各種情報を収集し表示します。本コマンドで表示する内容は、表 3-41 に示すコマンドが収集している情報です。system-dump オプションを指定した場合、装置内部のダンプ情報(独自形式で表示)を含めて取得し表示します。

表 3-41 コマンドにより収集可能な MMRP 情報

show system
show version
show mmrp configuration

```
show mmrp status port ※1
show interface counters ※1
```

※1 1秒おきに3回情報を取得

コマンドシンタックス

show tech-support mmrp [system-dump]

system-dump　　装置内部のダンプ情報を出力

コマンドモード

ENABLE

関連コマンド

注意事項

system-dump オプションを指定した場合、装置の性能、及び通信に対して影響を及ぼす可能性があります。使用する場合には、必ず事前にサポート対応窓口へご相談のうえ、指示に従ってください。

3.41.31 clear mmrp error-disabled

片方向ループを検出しているマスターポートの閉塞状態を強制解除します。閉塞状態が解除されると、マスターポートは Listening 状態に遷移します。Listening 状態遷移後にリング状態の監視を行い、片方向ループの解除を検出した場合は Forwarding 状態に遷移し、再度片方向ループを検出した場合は閉塞状態に遷移します。

コマンドシンタックス

clear mmrp error-disabled ring <NAME>

NAME　　MMRP リング名 <1-32(文字)>

コマンドモード

ENABLE

使用例

(1) リング名：ring01 の閉塞状態を解除します。

```
> enable
# clear mmrp error-disabled ring ring01
```

関連コマンド

show mmrp configuration ring, show running-config

注意事項

3.42 MMRP-Plus

MMRP-Plus機能は、MMRP機能と同様のリング型ネットワークを構成し、VLAN分散を実現する機能です。VLAN分散は、VLANごとにForwarding状態、Blocking状態となるポートを指定し、経路を分散することにより、リング内の帯域を有効に利用できる機能です。MMRP機能と同様にアウェア機能、分散マスター機能、分散シャドウ機能が使用できます。

注意事項

- **3.41 MMRP、MMRP-Plus、3.43 MMRP2 aware を同一リングで混在して使用することはできません。**
- **MMRP-Plus と MMRP を装置で同時に使用することはできません。**
- **MMRP-Plus と 3.46 NA 機能、動的リンクアグリゲーション(LACP)、3.17 スパニングツリープロトコル(STP/RSTP/MSTP)を装置で同時に使用することはできません。**
- **MMRP-Plus で使用するポートはトランクポートに設定することを推奨します。**
- **分散マスター、及び分散スレーブスイッチにおいて、複数のリングで制御フレーム用 VLAN を同一 VLAN ID に設定した場合、ハローフレームを複数のポートで受信するため、FDB 書き換えが常時発生します。このため、リングを複数設定する場合、制御フレーム用 VLAN はリングごとに異なる VLAN ID を設定("mmrp-plus ring vid")することを推奨します。**
- **MMRP-Plus を搭載しないスイッチングハブをリングのノードとしたネットワークを構築する場合、そのスイッチングハブでのリンク障害が復旧するとき、リング型ネットワークが一時的にループになります。**
- **メディアコンバーターなどによりリンク断検出不可のリンクがあるネットワークを構築する場合、そのリンク障害が復旧するとき、リング型ネットワークが一時的にループになります。**
- **MMRP-Plus は片断線通知機能双方向監視機能に対応していないため、片方向通信断の場合、ネットワークがループになります。**
- **上記の場合、ブロードキャストストームが発生することがあります。フラッディング制限機能を併用することにより、ブロードキャストストームを最小限に抑えることができます。**
- **MMRP-Plus が動作している LAG(リンクアグリゲーショングループ)への、ポートの追加、削除は行えません。**

Apresia13000-48X では、LAG に含まれる XENPAK ポート(ポート番号 49、50)を、MMRP-Plus のマスター/スレーブ/アウェアポートに設定した場合、動作は保証されません。

MMRP-Plus 設定時に、3.47 AccessDefender 機能、3.39 MLD 機能の 3 機能を同時に併用できません。

Apresia13000-48X、及び Apresia4348 シリーズにおいて、MMRP-Plus の動作ポートで 3.12 LLDP 機能を使用する場合はネイティブ VLAN の設定(3.11.6 "switchport trunk native <VID>")をしないでください。

3.28 パケットフィルター2 機能併用時に、MMRP-Plus 機能よりも小さいグループ番号でパケットフィルター2 機能を設定する場合、ethertype 0x8820 の MMRP-Plus 制御フレームがフィルター対象とならないように設定してください。

Apresia13000-48X では、ポートブロック(port 1～24、50 と port 25～49)を跨いだリンクアグリゲーションを MMRP-Plus で使用するポートとして設定しないでください。

以下のコマンドで設定するタイマー値は、同一リング内の全装置で揃えてください。

- **"mmrp-plus switch hello-cycle"**
- **"mmrp-plus switch hello-interval"**
- **"mmrp-plus switch polling-rate"**
- **"mmrp-plus ring divided-master uplink-up-wait"**
- **"mmrp-plus ring divided-shadow uplink-up-wait"**
- **"mmrp-plus ring fdb-flush-timer"**
- **"mmrp-plus ring listening-timer"**
- **"mmrp-plus ring hello-timeout"**
- **"mmrp-plus ring port-restart linkup-wait"**

3.42.1 mmrp-plus switch hello-cycle

MMRP-Plus の動作基準時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

本機能は、MMRP-Plus 機能をサポートしていないスイッチ(以下、非 MMRP-Plus 対応スイッチ)が MMRP-Plus リングに参加している場合に、非 MMRP-Plus 対応スイッチでのリンク断障害を、MMRP-Plus 対応スイッチが高速に検出し経路を切り替えることを可能にします。

以下の 3 つのコマンドにより hello-cycle、polling-rate、hello-interval の 3 つのパラメーターを変更し、マスタースイッチが MMRP-Plus ハローフレームを受信しないことによりリンク断と判定する速度を変更することが可能です。

- MMRP-Plus ハローフレーム送信間隔
  hello-cycle × hello-interval(ミリ秒)

- MMRP-Plus ハローフレームの状態監視時間
  hello-cycle × polling-rate(ミリ秒)

コマンドシンタックス

mmrp-plus switch hello-cycle <TIME>
no mmrp-plus switch hello-cycle

TIME	MMRP-Plus 基準タイマー <1-1000(1 ミリ秒)>

デフォルト

100(ミリ秒)

コマンドモード

CONFIG

使用例

(1) hello-cycle を 50 ミリ秒に変更します。

```
> enable
# configure terminal
(config)# mmrp-plus switch hello-cycle 50
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

パラメーターの変更により、放置可能な軽微な障害での切り替わりや、切り替わり遅延を引き起こすなど MMRP-Plus の動作が不安定になる場合があります。パラメーターの設定においては、運用ネットワークと同一構成で充分な事前検証を行うことをお勧めします。

MMRP-Plus リング内の全 MMRP-Plus 対応スイッチでパラメーターを統一してください。マスタースイッチのパラメーターのみを変更するなどした場合、MMRP-Plus が正常に動作せずループが発生するか、または FDB(Forwarding Data Base)のクリアが頻発することがあります。

1～1000 の範囲の任意の数値を設定できますが、実際の数値は約 10.0 ミリ秒(Apresia4300 シリーズの場合は約 15.6 秒)単位に切り詰められます。ただし、設定値が 10 以下の場合は約 10.0 ミリ秒となります(Apresia4300 シリーズの場合は、設定値が 15 以下の場合は約 15.6 ミリ秒となります)。

hello-cycleを小さくするとCPU負荷の増加により他機能の動作に影響を及ぼす場合があります。

3.42.2 mmrp-plus switch hello-interval

MMRP-Plus ハローフレームの送信間隔のパラメーターを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

実際の MMRP-Plus ハローフレームの送信間隔は、hello-interval × hello-cycle(ミリ秒)となります。

コマンドシンタックス

mmrp-plus switch hello-interval <TIME>
no mmrp-plus switch hello-interval
TIME　　MMRP-Plus ハローフレームの送信間隔 <1-10>

デフォルト

1(hello-cycle がデフォルト値の場合：100 ミリ秒)

コマンドモード

CONFIG

使用例

(1) MMRP-Plus ハローフレームの送信間隔を hello-cycle の 5 倍に変更します。

```
> enable
# configure terminal
(config)# mmrp-plus switch hello-interval 5
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

MMRP-Plus ハローフレームの送信間隔を大きくすると、ネットワークの構成により MMRP-Plus の動作が不安定になることがあります。

MMRP-Plus ハローフレームの送信間隔を変更する場合は、アウェア装置を含むすべての MMRP-Plus 装置で統一してください。

3.42.3 mmrp-plus switch polling-rate

MMRP-Plus ハローフレームの状態監視間隔のパラメーターを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。MMRP-Plus ハローフレームの受信停止を検出するためのタイムアウト値に関与する値となります。

実際に MMRP-Plus ハローフレーム途絶から受信断と判断される時間は、最大(2 × polling-rate ×

hello-cycle)(ミリ秒)になります。値を大きくするほど、障害発生から障害検出までの時間を要することになります。

コマンドシンタックス

mmrp-plus switch polling-rate <RATE>
no mmrp-plus switch polling-rate
RATE　　MMRP-Plus 状態監視間隔(hello-cycle の倍数で定義) <2-100>

デフォルト

10(hello-cycle がデフォルト値の場合：1 秒)

コマンドモード

CONFIG

使用例

(1) polling-rate を 5 に変更します。

```
> enable
# configure terminal
(config)# mmrp-plus switch polling-rate 5
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

メディアに 1000BASE-T を使用し、LAG(リンクアグリゲーショングループ)を MMRP-Plus リングのノードに適用する場合、polling-rate をデフォルト値より大きく設定してください(推奨値：15 以上)。

polling-rate を小さくすると、MMRP-Plus ハローフレームの伝送遅延やランダムな喪失により、ハローフレームの受信タイムアウトを誤検出する場合があります。

polling-rate の変更に応じて、MMRP-Plus ハローフレームの受信タイムアウト時間も変更されます。このため、polling-rate を変更する場合は、アウェア装置を含むすべての MMRP-Plus 装置で統一してください。

3.42.4 mmrp-plus group

MMRP-Plus で使用するパケットフィルター2 の先頭グループ番号とグループ数を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。使用するグループ数を省略した場合、グループ数には 1 が設定されます。グループは"mmrp-plus enable"設定時に確保します。他機能で予約済みのグループは確保できません。

本コマンド設定時は、指定した先頭グループ番号から昇順に、連番のグループを予約します。本コマンド未設定時は、未使用の最小グループ番号 1 つを自動的に予約します。

"mmrp-plus enable"が設定されている状態では、グループ番号を変更できません。グループの予約状況は 3.28.14 "show packet-filter2 reserved-group"コマンドで確認可能です。

コマンドシンタックス

mmrp-plus group <GROUP> [<NUMBER>]
no mmrp-plus group

GROUP　先頭グループ番号
- Apresia4328：<1-7>
- Apresia3400/4348/5400/13000 シリーズ：<1-14>

NUMBER　グループ数
- Apresia5412 シリーズ/13000-24GX：<1>
- Apresia3424/4300/5428GT シリーズ/13000-48X：<1-2>
- Apresia3448：<1-3>

デフォルト

GROUP 1、NUMBER 1(グループ 1 を使用)　：Apresia3400/5400 シリーズ/4328/13000-24GX
GROUP 1、NUMBER 2(グループ 1、2 を使用)：Apresia4348/13000-48X

コマンドモード

CONFIG

使用例

(1) グループ：10、11 を MMRP-Plus で使用するように設定します。
(2) MMRP-Plus グループをデフォルト値に戻します。

```
> enable
# configure terminal
(config)# mmrp-plus group 10 2
(config)# no mmrp-plus group
```

関連コマンド

show mmrp-plus configuration, show running-config, show packet-filter2 reserved-group

注意事項

MMRP-Plus 機能は 3.43 MMRP2 aware と同一のグループを使用します。両機能を併用させる場合、必ず同一のグループ番号を指定してください。

本機能の使用ポート数に応じてパケットフィルター2 のグループを使用します。使用可能ポート数と使用グループ数は以下の通り決まります。

パケットフィルター2 使用グループ数	Apresia3400/4300/5400/13000-48X 使用可能ポート数	Apresia13000-24GX 使用可能ポート数
1	1～25	28
2	26～50	-

パケットフィルター2 使用グループ数	Apresia3400/4300/5400/13000-48X 使用可能ポート数	Apresia13000-24GX 使用可能ポート数
3	51～52	-

本機能として使用できるポート数については以下を参照ください。なお論理ポート(リンクアグリゲーション)も 1 つのポートとして認識します。
- **シングルマスター構成(マスタースイッチ)：1 リングに対し 2 ポート必要**
- **分散マスター構成(マスタースイッチ)：1 リングに対し 1 ポート必要**
- **MMRP アウェアスイッチ：1 リングに対し 1 ポート必要**

本装置再起動後は構成情報の記載順にパケットフィルター2 のグループが確保されます。他機能で確保済みのグループを本コマンドで指定した場合、MMRP-Plus 機能は有効になりません。

3.42.5 mmrp-plus enable

MMRP-Plus を有効にします。無効にする場合は、no コマンドを使用してください。

MMRP-Plus リングの動作を開始します。リング動作を開始するには本設定が必要です。MMRP-Plus は、パケットフィルター2 のグループを使用します。"mmrp-plus group"コマンドで指定したグループを確保できない場合は、本設定はエラーを返します。本設定が有効な間は、"mmrp-plus group"コマンドで指定したグループ設定を変更することはできません。また、本設定が有効な間は、MMRP を有効にすることはできません。

コマンドシンタックス

[no] mmrp-plus enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) MMRP-Plus を有効にします。
(2) MMRP-Plus を無効にします。

```
> enable
# configure terminal
(config)# mmrp-plus enable
(config)# no mmrp-plus enable
```

関連コマンド

show mmrp-plus configuration, show mmrp-plus status, show running-config

注意事項

装置に以下に示すプライマリーIP アドレスを設定する場合、MMRP-Plus 機能で使用するパケットフィルター2 のデフォルトグループと重複するため、MMRP-Plus 機能を有効にすることはできません。
- デフォルトグループと重複するプライマリーIP アドレス設定数 -
Apresia3400/4348/5400/13000 シリーズ：86 個以上
Apresia4328 シリーズ：43 個以上
表 3-19、表 3-20 を参考に"mmrp-plus group"コマンドで重複しないグループ番号に設定を変更してください。

リング単位で、MMRP-Plus 機能の有効、無効の制御は行えません。

3.42.6 no mmrp-plus ring

指定したリング ID のリングに関する設定を解除します(すべてデフォルト値に戻ります)。

コマンドシンタックス

no mmrp-plus ring <RINGID>
RINGID　　MMRP-Plus リング ID <1-1000>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の設定を解除します。

```
> enable
# configure terminal
(config)# no mmrp-plus ring 1
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

3.42.7 mmrp-plus ring name

MMRP-Plus のリングに名前を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp-plus ring <RINGID> name <NAME>
no mmrp-plus ring <RINGID> name

RINGID　　MMRP-Plus リング ID <1-1000>
NAME　　MMRP-Plus リング名 <1-32(文字)>
- ASCII 文字
- ダブルクォーテーションで囲めば、空白文字を使用可能

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) リング ID：1 の MMRP-Plus リング名を Ring1 に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 name Ring1
```

関連コマンド
show mmrp-plus configuration, show mmrp-plus status, show running-config

注意事項

3.42.8 mmrp-plus ring vid

MMRP-Plus で使用する MMRP-Plus 制御フレームの VLAN ID を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス
mmrp-plus ring <RINGID> vid <VID>
no mmrp-plus ring <RINGID> vid
RINGID　　MMRP-Plus リング ID <1-1000>
VID　　MMRP-Plus 制御フレームの VLAN ID <1-4094>

デフォルト
全リング ID に対し 1

コマンドモード
CONFIG

使用例
(1) リング ID：1 の MMRP-Plus 制御フレームの VLAN ID を 100 に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 vid 100
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

VLAN ID には vlan database に登録していない VLAN ID も指定可能です。

同一リングに属する全装置において、MMRP-Plus 制御フレーム用の VLAN ごとに、同一の VLAN ID を指定してください。

MMRP-Plus の制御フレームは、ポートの VLAN 設定に関わらず、本コマンドで設定された VLAN ID で、タグ付きフレームとして送信されます。

3.11.8 "tag-type"で TPID(Tag Protocol Identifier)を変更した場合も MMRP-Plus 制御フレームの TPID は常に 0x8100 です。tag-type 設定により装置が認識する TPID をデフォルトの 0x8100 から変更した場合、該当する装置で MMRP-Plus 機能は使用できません。

3.42.9 mmrp-plus vlangroup slave-vid

MMRP-Plus で使用する VLAN グループのスレーブ VLAN を設定します。本コマンドで指定した VLAN ID がスレーブ VLAN、その他の VLAN ID がマスターVLAN となります。リングにスレーブ VLAN の VLAN ID を割り当てるには"mmrp-plus ring vlangroup"コマンドを使用する必要があります。

VLAN グループをリングに割り当てると、マスターVLAN はマスターポートが Forwarding、スレーブポートが Blocking となり、スレーブ VLAN はマスターポートが Blocking、スレーブポートが Forwarding となります。指定した VLAN ID をマスターVLAN に戻すには、no コマンドを使用してください。VLAN ID の指定を省略した場合、すべての VLAN がデフォルト設定に戻ります。

slave-vid を設定した VLAN グループは 3.49.1 "show running-config"において slave-vid の指定が表示されます。

コマンドシンタックス

mmrp-plus vlangroup <GROUP> slave-vid <VLANRANGE>
no mmrp-plus vlangroup <GROUP> [slave-vid <VLANRANGE>]

GROUP	VLAN グループ番号 • Apresia4348/13000 シリーズ：<1-8> • Apresia3400/4328/5400 シリーズ：<1-6>
VLANRANGE	VLAN グループでのスレーブ VLAN となる VLAN ID <1-4094> (複数指定可能)

デフォルト

なし(マスターVLAN ID：1-4094)

コマンドモード

CONFIG

使用例

(1) VLAN グループ：1 のスレーブ VLAN ID を 1～100 に設定します。
(2) VLAN グループ：1 のスレーブ VLAN ID を 101～200 に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus vlangroup 1 slave-vid 1-100
(config)# mmrp-plus vlangroup 1 slave-vid 101-200
```

関連コマンド

show mmrp-plus configuration ring, show mmrp-plus vlangroup, show running-config

注意事項

"mmrp-plus vlangroup master-vid"設定済の VLAN グループは本コマンドを設定できません。

"vlan database"未登録の VLAN ID も指定可能です。

VLAN ID は複数指定、レンジ指定が可能です。slave-vid 設定済の状態で本コマンドを設定した場合、指定した VLAN ID がスレーブ VLAN へ追加されます。

Apresia4348 シリーズ/13000-48X では、全 VLAN グループ(1～8)でスレーブ VLAN となる VLAN は設定できません。

マスターVLAN の設定/変更はリング内の任意の経路がリンクダウンしている状態(master-port(lag)、slave-port(lag)の status が Forwarding、または Down)で実施してください。リング内の全経路がリンクアップしている状態で実施するとループが発生する場合があります。

分散マスター環境で使用する場合、分散マスター側と分散シャドウ側で設定を合わせてください。異なる設定の場合、MMRP-Plus が正常に動作しない場合があります。

3.42.10 mmrp-plus vlangroup master-vid

MMRP-Plus で使用する VLAN グループのマスターVLAN を設定します。本コマンドで指定した VLAN ID がマスターVLAN、その他の VLAN ID がスレーブ VLAN となります。リングにマスターVLAN の VLAN ID を割り当てるには"mmrp-plus ring vlangroup"コマンドを使用する必要があります。

VLAN グループをリングに割り当てると、マスターVLAN はマスターポートが Forwarding、スレーブポートが Blocking となり、スレーブ VLAN はマスターポートが Blocking、スレーブポートが Forwarding となります。指定した VLAN ID をスレーブ VLAN に戻すには、no コマンドを使用してください。VLAN ID の指定を省略した場合、すべての VLAN がデフォルト設定に戻ります。

master-vid を設定した VLAN グループは 3.49.1 "show running-config"において master-vid の指定

が表示されます。

コマンドシンタックス

mmrp-plus vlangroup <GROUP> master-vid <VLANRANGE>
no mmrp-plus vlangroup <GROUP> [master-vid <VLANRANGE>]

GROUP	VLAN グループ番号 • Apresia4348/13000 シリーズ：<1-8> • Apresia3400/4328/5400 シリーズ：<1-6>
VLANRANGE	VLAN グループでのマスターVLAN となる VLAN ID <1-4094> (複数指定可能)

デフォルト

なし(マスターVLAN ID：1-4094)

コマンドモード

CONFIG

使用例

(1) VLAN グループ：1 のマスターVLAN ID を 1～100 に設定します。
(2) VLAN グループ：1 のマスターVLAN ID を 101～200 に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus vlangroup 1 master-vid 1-100
(config)# mmrp-plus vlangroup 1 master-vid 101-200
```

関連コマンド

show mmrp-plus configuration ring, show mmrp-plus vlangroup, show running-config

注意事項

本コマンドは Apresia3400 シリーズのみサポートします。

"mmrp-plus vlangroup slave-vid"設定済の VLAN グループは本コマンドを設定できません。

"vlan database"未登録の VLAN ID も指定可能です。

VLAN ID は複数指定、レンジ指定が可能です。master-vid 設定済の状態で本コマンドを設定した場合、指定した VLAN ID がマスターVLAN へ追加されます。

Apresia4348 シリーズ/13000-48X では、全 VLAN グループ(1～8)でスレーブ VLAN となる VLAN は設定できません。

マスターVLAN の設定/変更はリング内の任意の経路がリンクダウンしている状態

(master-port(lag)、slave-port(lag)の status が Forwarding、または Down)で実施してください。リング内の全経路がリンクアップしている状態で実施するとループが発生する場合があります。

分散マスター環境で使用する場合、分散マスター側と分散シャドウ側で設定を合わせてください。異なる設定の場合、MMRP-Plus が正常に動作しない場合があります。

3.42.11 mmrp-plus ring vlangroup

"mmrp-plus vlangroup slave-vid"、または"mmrp-plus vlangroup master-vid"で設定した MMRP-Plus の VLAN グループとリング ID を関連付けます。設定をデフォルトに戻す場合は、no コマンドを使用してください。デフォルト状態では全 VLAN がマスターVLAN として動作します。

コマンドシンタックス

mmrp-plus ring <RINGID> vlangroup <GROUP>
no mmrp-plus ring <RINGID> vlangroup

RINGID	MMRP-Plus リング ID <1-1000>
GROUP	VLAN グループ番号 • Apresia4348/13000 シリーズ：<1-8> • Apresia3400/4328/5400 シリーズ：<1-6>

デフォルト

なし(＝VLAN 分散をしない)

コマンドモード

CONFIG

使用例

(1) リング ID：1 に VLAN グループ：8 を設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 vlangroup 8
```

関連コマンド

show mmrp-plus configuration, show mmrp-plus status, show running-config

注意事項

運用中に本設定を変更した場合、実際に反映されるのは Blocking 状態への遷移が発生後です。

3.42.12 mmrp-plus ring master master-port slave-port

MMRP-Plus リングマスター機能のマスターポートとスレーブポートを設定します。設定を削除する場

合は、no コマンドを使用してください。ポートの代わりに 3.8.1 "link-aggregation"コマンドにより設定したLAG(リンクアグリゲーショングループ)を指定することもできます。

コマンドシンタックス

```
mmrp-plus ring <RINGID> master master-port <PORT1> slave-port <PORT2>
mmrp-plus ring <RINGID> master master-lag <LAG1> slave-port <PORT2>
mmrp-plus ring <RINGID> master master-port <PORT1> slave-lag <LAG2>
mmrp-plus ring <RINGID> master master-lag <LAG1> slave-lag <LAG2>
no mmrp-plus ring <RINGID> master
```

RINGID	MMRP-Plus リング ID <1-1000>
PORT1	マスターポート番号
PORT2	スレーブポート番号
LAG1	マスターLAG ID
LAG2	スレーブ LAG ID

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 において、マスターポートにポート：45 を、スレーブポートにポート：46 を設定します。

(2) リング ID：2 において、マスターポートにポート：47 を、スレーブポートにポートに LAG ID：1 を設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 master master-port 45 slave-port 46
(config)# mmrp-plus ring 2 master master-port 47 slave-lag 1
```

関連コマンド

show mmrp-plus configuration, show mmrp-plus status, show running-config

注意事項

本コマンドにより LAG を指定する場合は、先に"link-aggregation"コマンドにより、LAG を設定しておく必要があります。

本コマンドにより指定した LAG に対して、"link-aggregation"コマンドによりポートの追加、削除はできません。LAG の設定を変更する場合は、いったん"no mmrp-plus ring"コマンドでリングの設定を削除する必要があります。

3.42.13 mmrp-plus ring aware port

アウェアスイッチのMMRP-Plusリングポート(アウェアポート)を設定します。設定を削除する場合は、no コマンドを使用してください。ポートの代わりに 3.8.1 "link-aggregation"コマンドにより設定したLAG(リンクアグリゲーショングループ)を指定することもできます。

コマンドシンタックス

```
mmrp-plus ring <RINGID> aware port <PORT> port <PORT>
mmrp-plus ring <RINGID> aware lag <LAG> port <PORT>
mmrp-plus ring <RINGID> aware lag <LAG> lag <LAG>
no mmrp-plus ring <RINGID> aware
```

RINGID	MMRP-Plus リング ID <1-1000>
PORT	アウェアポート番号
LAG	アウェア LAG ID

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 において、アウェアポートにポート：45 とポート：46 を設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 aware port 45 port 46
```

関連コマンド

show mmrp-plus configuration, show mmrp-plus status, show running-config

注意事項

リングアウェア機能を設定した場合、QoS 機能を有効にしてください。QoS 機能を併用することにより MMRP-Plus 制御フレームを qp8 にて優先中継します。MMRP 制御フレームで利用するキュー(qp8)はユーザー通信では利用しないでください。

本コマンドにより LAG を指定する場合は、先に"link-aggregation"コマンドにより、LAG を設定しておく必要があります。

本コマンドにより指定した LAG に対して、"link-aggregation"コマンドによりポートの追加、削除はできません。LAG の設定を変更する場合は、いったん"no mmrp-plus ring"コマンドでリングの設定を削除する必要があります。

設定対象リング ID に"port-restart enable"設定がある場合、本コマンドの投入はできません。

3.42.14 mmrp-plus ring revertive

リンクダウン障害復旧後のFailure状態からの切り戻り方法を選択します。切り戻り方法は、自動切り戻り、手動切り戻りの2種類あります。設定をデフォルトに戻す場合は、noコマンドを使用してください。

自動切り戻り(<REVERT_TIMER>指定)に指定した場合は、障害復旧後のFailure状態から、<REVERT_TIMER>設定値の経過後にListening状態へ遷移し、リング復旧処理を開始します。

手動切り戻り(disable指定)に指定した場合は、障害復旧後はFailure状態となり、"clear mmrp-plus failure ring"コマンドが投入されるまでリング復旧処理は実施されません。

コマンドシンタックス

```
mmrp-plus ring <RINGID> revertive <REVERT_TIMER> | disable
no mmrp-plus ring <RINGID> revertive
```

RINGID	MMRP-Plus リングID <1-1000>
REVERT_TIMER	自動切り戻りタイマー値 <0-86400(秒)> • 0設定時は、Failure状態を経由しない(デフォルト)
disable	手動切り戻り

デフォルト

障害復旧後瞬時にリング復旧処理が開始(Failure状態を経由しない)

コマンドモード

CONFIG

使用例

(1) リングID：1において、自動切り戻りタイマーを10秒に設定します。
(2) リングID：1において、手動切り戻りに設定します。
(3) リングID：1において、自動切り戻りタイマーをデフォルトに戻します。

```
(config)# mmrp-plus ring 1 revertive 10
(config)# mmrp-plus ring 1 revertive disable
(config)# no mmrp-plus ring 1 revertive
```

関連コマンド

clear mmrp-plus failure, show mmrp-plus configuration ring, show running-config

注意事項

ユーザーループ検知機能(3.29.7 "loop-watch port notify-only/owner-vlan")とMMRP-Plus機能を併用し、自動切り戻り("mmrp-plus ring revertive")を設定する場合は、自動切り戻りタイマー値をマスタースイッチとアウェアスイッチで同じ値に設定してください。
また、マスタースイッチに自動切り戻りを設定しない場合は、マスタースイッチの"mmrp-plus ring listening-timer"を対向のアウェアスイッチの自動切り戻りタイマ

一値より長くして設定してください。

MMRP-Plus 機能と L3("ip forwarding")機能を併用する場合は、本コマンドは使用できません。

リンクダウンを伴わない、ハローフレームの受信タイムアウトによる障害復旧後は Failure 状態を経由しません。

3.42.15 mmrp-plus ring divided-master master-port

分散マスタースイッチのマスターポートを設定します。設定を削除する場合は、no コマンドを使用してください。ポートの代わりに 3.8.1 "link-aggregation"コマンドにより設定した LAG(リンクアグリゲーショングループ)を指定することもできます。

コマンドシンタックス

```
mmrp-plus ring <RINGID> divided-master master-port <PORT>
mmrp-plus ring <RINGID> divided-master master-lag <LAG>
no mmrp-plus ring <RINGID> divided-master master
```

RINGID	MMRP-Plus リング ID <1-1000>
PORT	マスターポート番号
LAG	マスターLAG ID

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 において、マスターポートにポート：45 を設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-master master-port 45
```

関連コマンド

show mmrp-plus configuration, show mmrp-plus status, show running-config

注意事項

3.42.16 mmrp-plus ring divided-master uplink-forcedown-method

分散マスタースイッチのアップリンクポートの瞬断方法を設定します。設定を削除する場合は、no コマンドを使用してください。分散マスター機能が管理するリング上において、障害の発生と復旧により MMRP-Plus が動作したとき、アップリンクポートを瞬断します。

コマンドシンタックス

mmrp-plus ring <RINGID> divided-master uplink-forcedown-method an-restart | phy-stop
no mmrp-plus ring <RINGID> divided-master uplink-forcedown-method

RINGID	MMRP-Plus リング ID <1-1000>
an-restart	自動認識機能(3.7.4 "auto-negotiation")のリスタートによりアップリンクポートを瞬断
phy-stop	一定時間 PHY の TX を停止することによりアップリンクポートを瞬断

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 のアップリンクポートに phy-stop を設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-master uplink-forcedown-method phy-stop
```

関連コマンド

show mmrp-plus configuration ring, show running-config

注意事項

アップリンクポートに MMRP-Plus の他リングのポート設定がある場合、本設定によらず瞬断動作は行われません。

対向装置に、アップリンク瞬断機能によるリンク断の通知ができない場合は、本機能は使用できません。

本機能は、リング上で MMRP が動作し経路が変更されたときに、アップリンクポートに接続されるスイッチングハブの MAC アドレステーブルをクリアするためのものです。ネットワークの構成によっては、本機能を有効にする必要はありません。

本機能により、アップリンクポート経由の通信が一時的に停止します。

自動認識機能("auto-negotiation")のリスタートによる瞬断では、MAC アドレステーブルがクリアされないスイッチングハブがあります。

UTP ポートをアップリンクポートとして使用する場合、uplink-up-wait × hello-cycle を 5000 以上に設定してください。

アップリンクポートが MMRP2 リングのポートの場合には、本機能を設定しないでください。

3.42.17 mmrp-plus ring divided-master uplink-forcedown-time

瞬断方法が phy-stop の時に、分散マスタースイッチのアップリンクポートの瞬断時間のパラメーターを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

実際のアップリンクポートの復旧待ち時間は uplink-forcedown-time × hello-cycle(ミリ秒)となります。

コマンドシンタックス

mmrp-plus ring <RINGID> divided-master uplink-forcedown-time <TIME>
no mmrp-plus ring <RINGID> divided-master uplink-forcedown-time

RINGID	MMRP-Plus リング ID <1-1000>
TIME	アップリンクポートを瞬断させる時間 <1-30>

デフォルト

5(hello-cycle がデフォルト値の場合：500 ミリ秒)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の瞬断時間を 1000 ミリ秒に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-master uplink-forcedown-time 10
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

アップリンクポートに接続するスイッチングハブによって、MAC アドレステーブルをクリアするために必要な瞬断時間は異なります。

3.42.18 mmrp-plus ring divided-master uplink-port

分散マスタースイッチのアップリンクポートを設定します。設定を削除する場合は、no コマンドを使用してください。指定したアップリンクポートのすべてにリンク障害が発生したとき、MMRP-Plus が動作しスレーブポートが Forwarding になります。

コマンドシンタックス

mmrp-plus ring <RINGID> divided-master uplink-port <PORTRANGE>
no mmrp-plus ring <RINGID> divided-master uplink-port

RINGID	MMRP-Plus リング ID <1-1000>
PORTRANGE	アップリンクポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 のアップリンクポートをポート：1～5 に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-master uplink-port 1-5
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

ポートは、複数指定、レンジ指定可能です。複数回設定した場合は最後の設定が有効になります。

以下の機能とアップリンクポートは同一ポートで併用できません。
- **LACP 機能(3.8 リンクアグリゲーション参照)**
- **3.17 スパニングツリープロトコル(STP/RSTP/MSTP)**

アップリンクポートに別リングの MMRP-Plus ポートを指定する場合、そのポートが所属するリングに"mmrp-plus ring revertive"を設定しないでください。

3.42.19 mmrp-plus ring divided-master uplink-up-wait

分散マスタースイッチのアップリンクポートの瞬断後復旧待ち時間のパラメーターを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。実際のアップリンクポートの復旧待ち時間は uplink-up-wait × hello-cycle(ミリ秒)となります。

コマンドシンタックス

mmrp-plus ring <RINGID> divided-master uplink-up-wait <TIME>
no mmrp-plus ring <RINGID> divided-master uplink-up-wait

RINGID	MMRP-Plus リング ID <1-1000>
TIME	アップリンクポートを瞬断後、リンクアップするまでの最大待ち時間 <1-864000>

デフォルト
30(hello-cycle がデフォルト値の場合：3000 ミリ秒)

コマンドモード
CONFIG

使用例
(1) リング ID：1 のアップリンクポートの瞬断後のリンクアップ待ち時間を 1000 ミリ秒に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-master uplink-up-wait 10
```

関連コマンド
show mmrp-plus configuration ring, show running-config

注意事項

リンクアップ待ち時間を小さくしすぎると、リンクアップ待ち時間以内にリンクアップしないときに MMRP の不要な切り替り/切り戻りが生じることがあります。また、アップリンクポートに UTP ポートを使用する場合、SFP ポートと UTP ポートではリンクアップの検知時間が異なるため、設定値をデフォルト値より大きく設定してください。

3.42.20 mmrp-plus ring divided-master uplink-fdbflush-transmit

分散マスタースイッチのアップリンクポートが MMRP-Plus の他リングのポートであっても経路変更時にアップリンクポートへの FDB フラッシュフレームを送出する機能を有効にします。無効にする場合は、no コマンドを使用してください。障害発生時に複数の Ring の経路変更が連動して動作する必要があるネットワーク構成の場合は設定を有効に、必要がないネットワーク構成の場合は設定を無効にしてください。

コマンドシンタックス
[no] mmrp-plus ring <RINGID> divided-master uplink-fdbflush-transmit enable
RINGID MMRP-Plus リング ID <1-1000>

デフォルト
no enable(＝無効)

コマンドモード
CONFIG

使用例
(1) 分散マスタースイッチのアップリンクポートが MMRP-Plus の他リングのポートであっても FDB

フラッシュフレームを送信するように設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-master uplink-fdbflush-transmit enable
```

関連コマンド

show mmrp-plus, show running-config

注意事項

アップリンクポートが MMRP2 リングのポートの場合には、本機能を設定しないでください。

3.42.21 mmrp-plus ring divided-shadow slave-port

分散シャドウスイッチのスレーブポートを設定します。設定を削除する場合は、no コマンドを使用してください。ポートの代わりに 3.8.1 "link-aggregation"コマンドにより設定した LAG(リンクアグリゲーショングループ)を指定することもできます。

コマンドシンタックス

```
mmrp-plus ring <RINGID> divided-shadow slave-port <PORT>
mmrp-plus ring <RINGID> divided-shadow slave-lag <LAG>
no mmrp-plus ring <RINGID> divided-shadow slave
```

RINGID	MMRP-Plus リング ID <1-1000>
PORT	スレーブポート番号
LAG	スレーブ LAG ID

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 のスレーブポートにポート：46 を設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-shadow slave-port 46
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

本コマンドにより LAG を指定する場合は、先に"link-aggregation"コマンドにより、

LAG を設定しておく必要があります。

本コマンドにより指定した LAG に対して、"link-aggregation"コマンドによりポートの追加、削除はできません。LAG の設定を変更する場合は、いったん"no mmrp-plus ring"コマンドでリングの設定を削除する必要があります。

3.42.22 mmrp-plus ring divided-shadow uplink-forcedown-method

分散シャドウスイッチのアップリンクポートの瞬断方法を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

```
mmrp-plus ring <RINGID> divided-shadow uplink-forcedown-method an-restart | phy-stop
no mmrp-plus ring <RINGID> divided-shadow uplink-forcedown-method
```

RINGID	MMRP-Plus リング ID <1-1000>
an-restart	自動認識機能(3.7.4 "auto-negotiation")のリスタートによりアップリンクポートを瞬断
phy-stop	一定時間 PHY の TX を停止することによりアップリンクポートを瞬断

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の分散シャドウスイッチのアップリンクを自動認識機能("auto-negotiation")のリスタートにより瞬断する設定にします。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-shadow uplink-forcedown-method an-restart
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

アップリンクポートに MMRP-Plus の他リングのポート設定がある場合、本設定によらず瞬断動作は行われません。

対向装置に、アップリンク瞬断機能によるリンク断の通知ができない場合は、本機能は使用できません。

本機能は、リング上で MMRP が動作し経路が変更されたときに、アップリンクポート

に接続されるスイッチングハブの MAC アドレステーブルをクリアするためのものです。ネットワークの構成によっては、本機能を有効にする必要はありません。

本機能により、アップリンクポート経由の通信が一時的に停止します。

自動認識機能("auto-negotiation")のリスタートによる瞬断では、MAC アドレステーブルがクリアされないスイッチングハブがあります。

UTP ポートをアップリンクポートとして使用する場合、uplink-up-wait × hello-cycle を 5000 以上に設定してください。

アップリンクポートが MMRP2 リングのポートの場合には、本機能を設定しないでください。

3.42.23 mmrp-plus ring divided-shadow uplink-forcedown-time

瞬断方法が phy-stop の時に、分散シャドウスイッチのアップリンクポートの瞬断時間のパラメーターを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

実際のアップリンクポートの復旧待ち時間は uplink-forcedown-time × hello-cycle(ミリ秒)となります。

コマンドシンタックス

```
mmrp-plus ring <RINGID> divided-shadow uplink-forcedown-time <TIME>
no mmrp-plus ring <RINGID> divided-shadow uplink-forcedown-time
```

RINGID	MMRP-Plus リング ID <1-1000>
TIME	アップリンクポートを瞬断させる時間 <1-30>

デフォルト

5(hello-cycle がデフォルト値の場合：500 ミリ秒)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の分散シャドウスイッチのアップリンクポート瞬断時間を 1000 ミリ秒に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-shadow uplink-forcedown-time 10
```

関連コマンド

show mmrp-plus configuration ring, show running-config

注意事項

アップリンクポートに接続するスイッチングハブによって、MAC アドレステーブルをクリアするために必要な瞬断時間は異なります。

3.42.24 mmrp-plus ring divided-shadow uplink-port

分散シャドウスイッチのアップリンクポートを設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

```
mmrp-plus ring <RINGID> divided-shadow uplink-port <PORTRANGE>
no mmrp-plus ring <RINGID> divided-shadow uplink-port
      RINGID              MMRP-Plus リング ID <1-1000>
      PORTRANGE           アップリンクポート番号(複数指定可能)
```

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の分散シャドウスイッチのアップリンクポートをポート：1～5 に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-shadow uplink-port 1-5
```

関連コマンド

show mmrp-plus configuration ring, show running-config

注意事項

ポートは、複数指定、レンジ指定可能です。複数回設定した場合は最後の設定が有効になります。

以下の機能とアップリンクポートは同一ポートで併用できません。

- **LACP 機能(3.8 リンクアグリゲーション参照)**
- **3.17 スパニングツリープロトコル(STP/RSTP/MSTP)**

アップリンクポートに別リングの MMRP-Plus ポートを指定する場合、そのポートが所属するリングに"mmrp-plus ring revertive"を設定しないでください。

3.42.25 mmrp-plus ring divided-shadow uplink-up-wait

分散シャドウスイッチのアップリンクポートの瞬断後復旧待ち時間のパラメーターを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

実際のアップリンクポートの復旧待ち時間は uplink-up-wait × hello-cycle(ミリ秒)となります。

コマンドシンタックス

```
mmrp-plus ring <RINGID> divided-shadow uplink-up-wait <TIME>
no mmrp-plus ring <RINGID> divided-shadow uplink-up-wait
      RINGID        MMRP-Plus リング ID <1-1000>
      TIME          アップリンクポートを瞬断後、リンクアップするまでの最大待ち時間
                    <1-864000>
```

デフォルト

30(hello-cycle がデフォルト値の場合：3000 ミリ秒)

コマンドモード

CONFIG

使用例

(1) 分散シャドウスイッチのアップリンクポートの瞬断後のリンクアップ待ち時間を1000ミリ秒に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-shadow uplink-up-wait 10
```

関連コマンド

show mmrp-plus configuration ring, show running-config

注意事項

リンクアップ待ち時間を小さくしすぎると、リンクアップ待ち時間以内にリンクアップしないときに MMRP の不要な切り替り/切り戻りが生じることがあります。また、アップリンクポートに UTP ポートを使用する場合、SFP ポートと UTP ポートではリンクアップの検知時間が異なるため、設定値をデフォルト値より大きく設定してください。

3.42.26 mmrp-plus ring divided-shadow uplink-fdbflush-transmit

アップリンクポートが MMRP-Plus の他リングのポートであっても経路変更時にアップリンクポートへの FDB フラッシュフレームを送出する機能を有効にします。無効にする場合は、no コマンドを使用してください。障害発生時に複数のリングの経路変更が連動して動作する必要があるネットワーク構成の場合は設定を有効に、必要がないネットワーク構成の場合は設定を無効にしてください。

コマンドシンタックス

```
[ no ] mmrp-plus ring <RINGID> divided-shadow uplink-fdbflush-transmit enable
```

RINGID　　MMRP-Plus リング ID <1-1000>

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) 分散マスター機能のアップリンクポートが MMRP-Plus の他リングのポートであっても FDB フラッシュフレームを送信するように設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 divided-shadow uplink-fdbflush-transmit enable
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

アップリンクポートが MMRP2 リングのポートの場合には、本機能を設定しないでください。

3.42.27 mmrp-plus ring fdb-flush-timer

FDB フラッシュタイマーのパラメーターを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。MMRP-Plus による MAC アドレステーブルクリア後の MAC アドレス学習停止時間を変更します。

実際の学習停止時間は、fdb-flush-timer × hello-cycle × polling-rate(ミリ秒)となります。

コマンドシンタックス

mmrp-plus ring <RINGID> fdb-flush-timer <TIME>

no mmrp-plus ring <RINGID> fdb-flush-timer

RINGID　　MMRP-Plus リング ID <1-1000>

TIME　　タイマー値 <0-10>

- 0 を指定した場合は、学習停止を行わない

デフォルト

5(hello-cycle、及び polling-rate がデフォルト値の場合：5000 ミリ秒)

コマンドモード

CONFIG

使用例

(1) MAC アドレステーブルクリア後の無学習時間を 1 秒に変更します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 fdb-flush-timer 1
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

3.42.28 mmrp-plus ring listening-timer

リスニングタイマーのパラメーターを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。MMRP-Plus が設定されているポートがリンクアップした直後に遷移する Listening 状態のタイムアウト時間を設定します。

実際のタイムアウト時間は、listening-timer × hello-cycle × polling-rate(ミリ秒)となります。

コマンドシンタックス

mmrp-plus ring <RINGID> listening-timer <TIME>
no mmrp-plus ring <RINGID> listening-timer

RINGID	MMRP-Plus リング ID <1-1000>
TIME	タイマー値 <1-1000000>

デフォルト

3(hello-cycle、及び polling-rate がデフォルト値の場合：3000 ミリ秒)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の MMRP-Plus を構成するポートのリスニングタイムアウト時間を 30000 ミリ秒に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 listening-timer 30
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

hello-cycle、polling-rate を変更した場合、リスニングタイマーの動作に遅延が生じます。遅延させたくない場合、listening-timer 値を直接変更してください。

3.42.29 mmrp-plus ring hello-timeout

MMRP-Plus ハローフレームの受信タイムアウト時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。MMRP-Plus ハローフレームの受信停止を検出してから、経路切り替えの動作をするまでのタイマー(保護時間)となります。タイムアウト時間経過後、経路切り替えが動作します。

コマンドシンタックス

mmrp-plus ring <RINGID> hello-timeout <TIME>
no mmrp-plus ring <RINGID> hello-timeout

RINGID	MMRP-Plus リング ID <1-1000>
TIME	タイマー値 <1-86400(秒)>

デフォルト

1(秒)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の MMRP-Plus ハローフレームの受信タイムアウト時間を 10 秒に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1 hello-timeout 10
```

関連コマンド

show mmrp-plus configuration, show running-config

注意事項

本コマンドの設定値をデフォルトから変更する場合、かつ"mmrp-plus switch polling-rate"、または"mmrp-plus switch hello-cycle"をデフォルト値より大きく設定している場合は、これらのコマンドの設定値をデフォルト値以下へ変更してください。

LLDP 疑似リンクダウン機能と併用する場合、本設定を LLDP 隣接機の情報保持時間(lldp msg-tx-interval × lldp msg-tx-hold)以上に設定してください。
各種タイマー値は以下推奨値を参考に設定してください("lldp msg-tx-interval"を最低値(1)とした場合)。
推奨値

- **tx-hold：3 回(TTL：3 秒)**
- **hello-timeout：5 秒以上**

3.42.30 mmrp-plus ring port-restart enable

指定リング ID でポートリスタート機能を有効にします。無効にする場合は、no コマンドを使用してください。本機能を有効にした場合、リング復旧時にマスター(スレーブ)ポートのリンクを瞬断し、対向スイッチの FDB をクリアします。

マルチリングでポートリスタート機能を有効にする場合、制御フレーム用 VLAN はそれぞれ別 VLAN を使用することを推奨しています。

コマンドシンタックス

[no] mmrp-plus ring <RINGID> port-restart enable

RINGID　　MMRP-Plus リング ID <1-1000> (範囲指定可)

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) リング ID：1～10 に対し、ポートリスタート機能を有効にします。

```
> enable
# configure terminal
(config)# mmrp-plus ring 1-10 port-restart enable
```

関連コマンド

show mmrp-plus configuration ring, show running-config

注意事項

指定されたリング ID にアウェアポート設定がある場合は("mmrp-plus ring aware")本コマンドの投入はできません。

MMRP-Plus Aware 装置との接続はできません。

LLDP 疑似リンクダウン機能との併用はできません。

本コマンドで設定可能なリング数は最大 64 個です。

アップリンクポートとの併用はできません。

同一リングに属する装置のマスター/スレーブポートは、ポートリスタート機能の設定値を同一にしてください。

制御フレーム用 VLAN とユーザーフレーム用 VLAN に同一 VLAN ID を設定しないでください。

3.42.31 mmrp-plus ring port-restart forcedown-time

ポートリスタート機能によるリンク瞬断時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。実際のリンク断時間は forcedown-time × hello-cycle(ミリ秒)となります。

コマンドシンタックス

mmrp-plus ring <RINGID> port-restart forcedown-time <TIME>
no mmrp-plus ring <RINGID> port-restart forcedown-time

RINGID	MMRP-Plus リング ID <1-1000> (範囲指定可)
TIME	タイマー値 <1-30(ミリ秒)>

デフォルト

5

コマンドモード

CONFIG

使用例

(1) リング ID：2 に対し、ポートリスタート機能によるリンク瞬断時間のタイマー値を 10 に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 2 port-restart forcedown-time 10
```

関連コマンド

show mmrp-plus configuration ring, show running-config

注意事項

forcedown-time が短い場合、アウェアスイッチの FDB がクリアされない場合があります。

本コマンドで設定可能なリング数は最大 64 個です。

3.42.32 mmrp-plus ring port-restart linkup-wait

ポートリスタート機能のリンク保護時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。リンク保護時間とは、対向装置のリンク復旧時間までの間に MMRP-Plus の不要な切り替え/切り戻りを防止するためのものです。対向装置によってリンク保護時間の設定を行ってください。

実際の保護時間は linkup-wait × hello-cycle(ミリ秒)となります。

リンク復旧時(＝ポートリスタート動作開始)よりリンク保護時間満了までの間、マスター/スレーブポートのリンク検知、及び MMRP-Plus ハローフレーム受信タイムアウト検知は停止されます。

コマンドシンタックス

mmrp-plus ring <RINGID> port-restart linkup-wait <TIME>
no mmrp-plus ring <RINGID> port-restart linkup-wait

RINGID	MMRP-Plus リング ID <1-1000> (範囲指定可)
TIME	タイマー値 <40-100(ミリ秒)>

デフォルト

50

コマンドモード

CONFIG

使用例

(1) リング ID：5 に対し、ポートリスタート機能による瞬断保護時間のタイマー値を 100 に設定します。

```
> enable
# configure terminal
(config)# mmrp-plus ring 5 port-restart linkup-wait 100
```

関連コマンド

show mmrp-plus configuration ring, show running-config

注意事項

本コマンドで設定可能なリング数は最大 64 個です。

リンク保護時間が短い場合、対向装置のリンクが確立せず、MMRP-Plus の不要な切り替り/切り戻りが生じることがあります。

3.42.33 show mmrp-plus configuration

MMRP-Plus の構成情報を表示します。

コマンドシンタックス

show mmrp-plus configuration

コマンドモード

VIEW, ENABLE

使用例

(1) MMRP-Plus の構成情報を表示します。

```
# show mmrp-plus configuration
MMRP-Plus Switch Configuration:
        Status          : Enable
```

```
        Group          : 7
        Hello cycle    : 100ms
        Hello interval : 1 (100ms)
        Polling rate   : 10 (1000ms)

MMRP-Plus Ring Configuration:
 R.M.: Ring Master, R.A.: Ring Aware, D.M.: Divided Master, D.S.: Divided Shadow
 Vid : Hello VID
 Fdb : FDB Flush Timer
 Pr  : Port Restart (0: enable -: disable)
 Vg  : VLAN Group
 Re  : Revertive setting
 Ht  : Hello Timeout Timer
 Lis : Listening Timer

ID   Name    Type Pt1   Pt2   | Vid  Fdb Pr Vg Re      Ht    Lis
-----------------------------+-----------------------------------------------
1    abcdefg D.M. 25          | 4094 10  0  8  86400   86400 1000000
2    1234567 R.M. 27(M) 28(S) | 1    5   -  -  disable 1     3
3    -       R.A. 13    14    | 4094 0   -  -  disable 1     3
```

Status　　：MMRP-Plus の動作状態
Group　　：MMRP-Plus が使用するグループ番号
Hello cycle　　：MMRP-Plus の動作基準時間
Hello interval　　：MMRP-Plus ハローフレームの送信間隔
Polling rate　　：MMRP-Plus 状態受信間隔
ID　　：MMRP-Plus リング ID
Name　　：MMRP-Plus リング名
　8 文字以上で設定している場合は、7 文字目までを表示
Pt1/Pt2　　：ポート番号、または LAG(リンクアグリゲーショングループ) ID
　LAG ID は ID の前に「L」を表示
　リングマスター構成で、マスターには(M)、スレーブには(S)を表示
Vid　　：MMRP-Plus ハローフレームの VLAN ID
Fdb　　：FDB フラッシュタイマーの設定値
Pr　　：ポートリスタート機能の設定の有無を表示
Vg　　：MMRP-Plus リングに対応づけられた VLAN グループ番号
Re　　：自動切り戻り時間
　設定がない場合(0 秒)は"0"
　手動切り戻り設定の際は"disable"と表示
Ht　　：ハローフレームの受信タイムアウト時間
Lis　　：リスニング状態のタイムアウト時間

関連コマンド

注意事項

3.42.34 show mmrp-plus configuration ring

MMRP-Plus のリング単位での構成情報を表示します。

コマンドシンタックス

show mmrp-plus configuration ring <RINGID>

RINGID　　MMRP-Plus リング ID <1-1000>

コマンドモード

VIEW, ENABLE

使用例

(1) リング ID：1 の MMRP-Plus リングの詳細な構成情報を表示します。

```
# show mmrp-plus configuration ring 1
Ring name      :
Type           : Ring Master
Master port    : 4
Slave port     : 5
VLAN ID        : 1
VLAN Group     : (none)
Listening Time: 1 (0.002s)
FDB Flush Time: 1 (0.002s)
Hello-timeout : 1s
Revertive      : 1 (0.002s)

# show mmrp-plus configuration ring 2
Ring name      :
Type           : Divided Master
Master lag     : 1 (Port 10-12)
VLAN ID        : 300
VLAN Group     : 1
  Master VID     : 1-199,201-4094
  Slave VID      : 200
Listening Time: 3 (3.0s)
FDB Flush Time: 5 (5.0s)
Hello-timeout : 1s
Revertive      : 0s
Port-Restart   : Enable
  Forcedown Time     :   5 (500 ms)
  Link Up Wait       :  50 (5000 ms)
Uplink option
  Port               : -
  Forcedown Method   : -
  Forcedown Time     :        5 (500 ms)
  Link Up Wait       :       30 (3000 ms)
```

```
  Transmit FDBFlush : Disable

# show mmrp-plus configuration ring 999
Ring name     :
Type          : Shadow Master
Slave port    : 12
VLAN ID       : 1
VLAN Group    : (none)
Listening Time: 1 (0.002s)
FDB Flush Time: 1 (0.002s)
Hello-timeout : 1s
Revertive     : 1 (0.002s)
Port-Restart  : Enable
  Forcedown Time    :   5 (500 ms)
  Link Up Wait      :  50 (5000 ms)
Uplink option
  Port              :
  Forcedown Method  :
  Forcedown Time    :        1 (1 ms)
  Link Up Wait      :        1 (1 ms)
  Transmit FDBFlush : Disable

# show mmrp-plus configuration ring 1000
Ring name     :
Type          : Ring Aware
Aware Port 1  : 25
Aware Port 2  : 26
VLAN ID       : 1
Listening Time: 1 (0.002s)
FDB Flush Time: 1 (0.002s)
Hello-timeout : 1s
Revertive     : 1 (0.002s)
```

Ring ID　　：MMRP-Plus リング ID
Ring name　　：MMRP-Plus リング名
Type　　：MMRP-Plus リングの動作モード
Master Port　　：マスターポート番号
Master LAG　　：マスターLAG(リンクアグリゲーショングループ) ID
Slave Port　　：スレーブポート番号
Slave Lag　　：スレーブ LAG ID
Aware Port　　：アウェアポート番号
Aware LAG　　：アウェア LAG ID
VLAN ID　　：MMRP-Plus ハローフレームの VLAN ID
VLAN Group　　：MMRP-Plus リングに対応づけられた VLAN グループ番号
  Master VID　　：マスターVLAN として動作する VLAN ID
  Slave VID　　：スレーブ VLAN として動作する VLAN ID

Listening Time　　：リスニングタイムアウト時間
FDB Flush Time　　：FDB フラッシュタイマーの設定値
Hello-timeout　　：ハローフレームの受信タイムアウト時間
Revertive　　：自動切り戻り時間
　　設定がない場合(0 秒)は"0s"
　　手動切り戻り設定の際は"disable"と表示
Port-Restart　　：ポートリスタートの設定
　Forcedown Time　　：ポートリスタートのリンク瞬断時間
　Link Up Wait　　：ポートリスタートのリンクアップ保護時間
Uplink Option　　：アップリンクポートの設定
　Port　　：アップリンクポート番号
　Forcedown Method　　：アップリンクポートの瞬断方法
　Forcedown Time　　：アップリンクポートの停止時間
　Link Up Wait　　：アップリンクポート瞬断後のリンクアップ待ち時間
　Transmit FDBFlush　　：アップリンクポートが MMRP-Plus の他リングポートの場合
　　の FDB フラッシュフレーム送信有無

関連コマンド

注意事項

3.42.35 show mmrp-plus vlangroup

各 VLAN グループのマスターVLAN、及びスレーブ VLAN を表示します。<GROUP>を省略することにより、すべての VLAN グループのマスターVLAN、及びスレーブ VLAN を表示します。

コマンドシンタックス

show mmrp-plus vlangroup [group <GROUP>]
　GROUP　　VLAN グループ番号 <1-8>

コマンドモード

VIEW, ENABLE

使用例

(1) VLAN グループ：1 のマスターVLAN を表示します。

```
# show mmrp-plus vlangroup group 1
Vlan Group Configuration: Group 1
  Master VID   : 1-4094
  Slave VID    :
```

関連コマンド

注意事項

3.42.36 show mmrp-plus status

MMRP-Plus の動作状態を表示します。

コマンドシンタックス

show mmrp-plus status

コマンドモード

VIEW, ENABLE

使用例

(1) MMRP-Plus の動作状態を表示します。

```
> show mmrp-plus status
R.M.: Ring Master, R.A.: Ring Aware, D.M.: Divided Master, S.M.: Shadow Master
-------------------------------------------------------------------------------
 Pt.  Ring  Link     MMRP-Plus     MMRP-Plus      Connection   Ring Name
 /Lag ID    Status   Port Mode     Port Status    Status
-------------------------------------------------------------------------------
 17   1     100M/F   R.M. Master   Forwarding     Broken       ring0001
 18   1     Down     R.M. Slave    Down           -            ring0001
```

Pt./Lag　：ポート番号、または LAG(リンクアグリゲーショングループ) ID
Ring ID　：MMRP-Plus リング ID
Link Status　：ポート、または LAG のリンク状態
MMRP-Plus Port Mode　：ポートに設定されている MMRP-Plus 動作モードと MMRP-Plus ポートタイプ
　R.M.　：マスタースイッチ
　R.A.　：アウェアスイッチ
　D.M.　：分散マスタースイッチ
　S.M.　：分散シャドウスイッチ
　Master　：マスターポート
　Slave　：スレーブポート
　Default　：アウェアにてハローフレームを受信せずマスターポート、スレーブポートが決定していない状態
MMRP-Plus Port Status　：MMRP-Plus が設定されているポートの MMRP-Plus 動作状態
　Down　：リンクダウン状態
　Listening　：ポートがリンクアップした直後のネットワークのループを防ぐ Listening 状態
　MMRP-Plus 制御フレームだけを中継し、他のユーザーフレームは中継しない
　Forwarding　：全 VLAN のユーザーフレームを中継する Forwarding 状態
　リング内に障害が発生した場合、通信を継続するためにマスターポート、及びスレーブポートに設定されているポートが遷移
　Blocking　：マスターVLAN(マスターポート)、またはスレーブ VLAN(スレーブポート)のどちらか一方のフレームのみを中継する Blocking 状態
　ネットワークが物理的にループになるのを防ぐ
　リング正常状態ではマスターポート、スレーブポートどちらも

Blocking 状態に遷移
Connection Status　：リングの接続状態
Normal　：リング型ネットワーク上に障害がないことを表す
Broken　：リング型ネットワーク上に障害が発生し、MMRP-Plus ハローフレームが到達していないことを表す
Abnormal　：MMRP-Plus ハローフレームが逆流していることを表す
マスターポート同士、スレーブポート同士を接続すると表示される
Ring name　：MMRP-Plus リングに付与されたリング名
11 文字以上の呼称を設定している場合は、10 文字に短縮して表示

関連コマンド

注意事項

3.42.37 show mmrp-plus status port

MMRP-Plus のポート単位での詳細状態を表示します。ポートの代わりに 3.8.1 "link-aggregation"コマンドにより設定した LAG(リンクアグリゲーショングループ)、またはリング ID を指定することもできます。

コマンドシンタックス

```
show mmrp-plus status port <PORTRANGE>
show mmrp-plus status lag <LAG>
show mmrp-plus status ring <RINGID>
```

PORTRANGE　表示するポート番号(複数指定可能)
LAG　表示する LAG ID
RINGID　MMRP-Plus リング ID <1-1000>

コマンドモード

VIEW, ENABLE

使用例

(1) LAG1 の MMRP-Plus リングの詳細な動作状態を表示します。

```
# show mmrp-plus status lag 1
================================================================================
Lag  1 (Port 3)
  Ring ID   : 1
  Ring Name :
  Type      : Ring Master Master Lag
  Status    : Blocking
  Connection: Normal
-----------------------------------------------------------------
  Frame Type       Receive Frame Count     Transmit Frame Count
-----------------------------------------------------------------
  HelloB1                         118                        -
```

HelloB2	0	126
HelloF1	0	-
HelloF2	0	0
FDB Flush	0	0
Link Down	0	0
Link Up	0	0
Blocking	2	2

Port　：ポート番号
Lag　：LAG ID
Ring ID　：MMRP-Plus リング ID
Ring Name　：MMRP-Plus リング名
Type　：ポートに設定されている MMRP-Plus 動作モードと MMRP-Plus ポートタイプ
Status　：MMRP-Plus が設定されているポートの MMRP-Plus 動作状態
Connection　：リングの接続状態
Frame Type　：MMRP-Plus 制御フレームの種別
　HelloB1　：スレーブポートが Blocking 状態時にマスターポートへ送信される MMRP-Plus ハローフレーム
　HelloB2　：マスターポートが Blocking 状態時にスレーブポートへ送信される MMRP-Plus ハローフレーム
　HelloF1　：スレーブポートが Forwarding 状態時にマスターポートへ送信される MMRP-Plus ハローフレーム
　HelloF2　：マスターポートが Forwarding 状態時にスレーブポートへ送信される MMRP-Plus ハローフレーム
　FDB Flush　：MAC アドレステーブル情報をクリアする要求を表すフレーム
　Link Down　：リンクダウン障害が発生したことを表す制御フレーム
　Link Up　：リンクダウン障害が復旧し、リンクアップしたことを表すフレーム
　Blocking　：マスターポート、及びスレーブポートが Blocking 状態に遷移したことを表すフレーム
Receive Frame Count　：受信したフレーム数
Transmit Frame Count　：送信したフレーム数

関連コマンド

注意事項

3.42.38 show tech-support mmrp-plus

MMRP-Plus 機能の各種情報を収集し表示します。本コマンドで表示する内容は、表 3-42 に示すコマンドが収集している情報です。system-dump オプションを指定した場合、装置内部のダンプ情報(独自形式で表示)を含めて取得し表示します。

表 3-42 コマンドにより収集可能な MMRP-Plus 情報

show system
show version

```
show mmrp-plus configuration
show mmrp-plus status port ※1
show interface counters ※1
```

※1 1秒おきに3回情報を取得

コマンドシンタックス

show tech-support mmrp-plus [system-dump]

system-dump　　装置内部のダンプ情報を出力

コマンドモード

ENABLE

関連コマンド

注意事項

system-dump オプションを指定した場合、装置の性能、及び通信に対して影響を及ぼす可能性があります。使用する場合には、必ず事前にサポート対応窓口へご相談のうえ、指示に従ってください。

3.42.39 clear mmrp-plus failure ring

Failure 状態を解除し、リング復旧処理を開始します(Listening 状態へ遷移します)。

自動切り戻り("mmrp-plus ring revertive"コマンド)設定時でも、本コマンド投入により、タイマー満了を待たずに Failure 状態を解除します。

コマンドシンタックス

clear mmrp-plus failure ring <RINGID>

RINGID　　MMRP-Plus リング ID <1-1000>

コマンドモード

ENABLE

使用例

(1) リング ID：1 の Failure 状態を解除し、リング復旧処理を開始します。

```
# clear mmrp-plus failure ring 1
```

関連コマンド

mmrp-plus ring revertive, show mmrp-plus status

注意事項

3.43 MMRP2 aware

MMRP2 aware 機能は、Apresia6000/8000/18000 シリーズをマスター・スレーブとしたリング型ネットワークに Apresia13000 シリーズをアウェアスイッチとして接続することを可能にします。

MMRP2 aware 機能により、障害発生・復旧時において MAC アドレステーブルのクリアを行い、アウェアスイッチに収容された端末の通信を高速に回復させることが可能になります。

注意事項

MMRP2 aware は、Apresia13000 シリーズでのみ有効です。

Apresia6000/8000/18000 シリーズと Apresia13000 シリーズの MMRP 機能は相互接続性がありません。MMRP2 aware 機能を有効にした場合のみ、Apresia6000/8000/18000 シリーズをマスター・スレーブとした MMRP リングに Apresia13000 シリーズをアウェアスイッチとして接続することが可能になります。本書では便宜上、Apresia6000/8000/18000 シリーズの MMRP 機能を MMRP2 と呼びます。

3.41 MMRP、3.42 MMRP-Plus、MMRP2 aware を同一リングで混在して使用することはできません。

MMRP2 aware 機能と STP、RSTP、MSTP を同一ポートで混在して使用することはできません。

MMRP2 機能で使用するポートはトランクに設定することを推奨します。

MMRP2 機能ではリングの識別にリング ID を使用します。リング ID は制御フレームの識別に使用しているため、1 個のリング内では同一番号を指定する必要があります。同一番号が設定されていない場合には、MMRP2 のリングが正常に構成されずループが発生することがあります。

MMRP2 aware 設定時に、3.47 AccessDefender 機能、3.39 MLD 機能の 3 機能を同時に併用できません。

Apresia13000-48X では、ポートブロック(port 1～24、50 と port 25～49)を跨いだリンクアグリゲーションを MMRP2 aware で使用するポートとして設定しないでください。

3.43.1 mmrp2 group

MMRP2 aware で使用するグループを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

MMRP2 aware 動作中は、使用しているグループを他の機能で指定することはできません。また、他の機能で使用しているグループを MMRP2 aware で指定することもできません。

コマンドシンタックス

mmrp2 group <GROUP> [<NUMBER>]
no mmrp2 group

GROUP	MMRP2 aware で使用するグループの先頭番号 <1-14>
NUMBER	グループ数の指定 • Apresia13000-24GX：<1> • Apresia13000-48X：<1-2>

デフォルト

1(グループ 1 を使用)　：Apresia13000-24GX
2(グループ 1、2 を使用)：Apresia13000-48X

コマンドモード

CONFIG

使用例

(1) MMRP がグループ：10、11 を使用するように設定します。
(2) MMRP グループを削除します。

```
> enable
# configure terminal
(config)# mmrp2 group 10 2
(config)# no mmrp2 group
```

関連コマンド

show mmrp configuration, show running-config, assign

注意事項

表 3-19 の各コマンドは、パケットフィルター2 のグループを使用するため、これら機能設定がある場合、使用するグループが重複し、MMRP2 aware を有効(3.43.2 "mmrp2 enable")にできない場合があります。その場合は、指定するグループ番号を変更し再度有効にしてください。

MMRP2 aware 機能は 3.41 MMRP 機能と同一のグループを使用します。両機能を併用させる場合、必ず同一のグループ番号を指定してください。

MMRP2 aware 機能は 3.42 MMRP-Plus と同一のグループを使用します。両機能を併用させる場合、必ず同一のグループ番号を指定してください。

本機能の使用ポート数に応じてパケットフィルター2 のグループを使用します。使用可能ポート数と使用グループ数は以下のとおり決まります。

Apresia13000-48X 使用可能ポート数	Apresia13000-24GX 使用可能ポート数	パケットフィルター2 使用グループ数
1～25	28	1
26～50	-	2
51～52	-	3

本機能として使用できるポート数については以下を参照ください。なお論理ポート(リンクアグリゲーション機能)も 1 つのポートとして認識します。
- **シングルマスター構成(マスタースイッチ)：1 リングに対し 2 ポート必要**
- **分散マスター構成(マスタースイッチ)：1 リングに対し 1 ポート必要**
- **MMRP アウェアスイッチ：1 リングに対し 1 ポート必要**

本装置再起動後は構成情報の記載順にパケットフィルター2 のグループが確保されます。他機能で確保済みのグループを本コマンドで指定した場合、MMRP2 aware 機能は有効になりません。

3.43.2 mmrp2 enable

MMRP2 aware 機能を有効にします。無効にする場合は、no コマンドを使用してください。

MMRP2 aware は、パケットフィルター2 のグループを使用します。"mmrp2 group"で指定したグループを確保できない場合は、本設定はエラーを返します。本設定が有効な間は、"mmrp2 group"コマンドで指定したグループ設定を変更することはできません。

コマンドシンタックス

[no] mmrp2 enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) MMRP2 aware を有効にします。
(2) MMRP2 aware を無効にします。

```
> enable
# configure terminal
(config)# mmrp2 enable
(config)# no mmrp2 enable
```

関連コマンド

show mmrp status, show running-config, assign

注意事項

3.43.3 mmrp2 aware port

MMRP2 aware 機能を使用するポートを設定します。設定を削除する場合は、no コマンドを使用してください。ポートの代わりに 3.8.1 "link-aggregation"コマンドにより設定した LAG(リンクアグリゲーショングループ)を指定することも可能です。

コマンドシンタックス

```
mmrp2 <ID> aware port <PORT> port <PORT>
mmrp2 <ID> aware lag <LAG> lag <LAG>
mmrp2 <ID> aware lag <LAG> port <PORT>
no mmrp2 <ID> aware
```

ID	リング ID <1-1000>
PORT	MMRP リングを構成するポート
LAG	MMRP リングを構成する LAG ID

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：25 とポート：26 でリング ID：1 の MMRP2 aware 機能を使用します。

```
> enable
# configure terminal
(config)# mmrp2 1 aware port 25 port 26
```

関連コマンド

show mmrp2, show mmrp2 detail, show running-config

注意事項

QoS 機能と併用することにより、MMRP2 aware 機能を設定した Apresia シリーズは MMRP2 制御フレームをユーザートラフィックより優先して中継し、ユーザートラフィック増の影響による不要なリングの再構成を抑止することが可能になります。このため QoS 機能を有効にしてください。

本コマンドにより LAG を指定する場合は、先に"link-aggregation"コマンドにより LAG を設定しておく必要があります。

本コマンドにより指定した LAG に対して、"link-aggregation"コマンドによりポートの追加、削除はできません。LAG の設定を変更する場合は、いったん no コマンドでリングの設定を削除する必要があります。

3.43.4 no mmrp2

MMRP2 aware の設定を無効にします。本コマンドは対応するリングの全設定を無効にします。

コマンドシンタックス

no mmrp2 <ID>

ID	リング ID <1-1000>

デフォルト

なし

コマンドモード

CONFIG

使用例

(1) リング ID：1 を削除します。

```
> enable
# configure terminal
(config)# no mmrp2 1
```

関連コマンド

show mmrp2, show mmrp2 detail, show running-config

注意事項

3.43.5 mmrp2 vid

送受信する MMRP2 ハローフレーム/制御フレームの VLAN ID を変更します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp2 <ID> vid <VID>

no mmrp2 <ID> vid

ID	リング ID <1-1000>
VID	送受信する MMRP2 フレームの VLAN ID <1-4094>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の MMRP2 ハローフレームの VLAN ID を 100 に変更します。

```
> enable
# configure terminal
(config)# mmrp2 1 vid 100
```

関連コマンド

show mmrp2, show mmrp2 detail, show running-config

注意事項

1 個のリング内では同一 VLAN ID を指定する必要があります。

3.43.6 mmrp2 name

MMRP2 のリング名を変更します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp2 <ID> name <NAME>
no mmrp2 <ID> name

ID	リング ID <1-1000>
NAME	MMRP2 リング名(最大 32 文字)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の MMRP2 の名称を ring1 に変更します。

```
> enable
# configure terminal
(config)# mmrp2 1 name ring1
```

関連コマンド

show mmrp2, show mmrp2 detail, show running-config

注意事項

3.43.7 mmrp2 listening-timeout

MMRP2 aware の設定されているポートが failure から回復した直後に遷移するリスニング状態のタイムアウト時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp2 <ID> listening-timeout <LISTENINGTIME>

no mmrp2 <ID> listening-timeout

ID	リング ID <1-1000>
LISTENINGTIME	タイムアウト時間 <0-86400(秒)>

デフォルト

3(秒)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の MMRP2 リスニング状態のタイムアウトを 60 秒に変更します。

```
> enable
# configure terminal
(config)# mmrp2 1 listening-timeout 60
```

関連コマンド

show mmrp2, show mmrp2 detail, show running-config

注意事項

リスニングタイムアウト時間を 0 に設定すると、リング復旧時に短時間のループが発生する可能性があります。

リスニングタイムアウト時間を小さくしすぎると、復旧時に短時間のループが発生する可能性があります。

3.43.8 mmrp2 revertive

MMRP2 aware が設定されているポートが failure から自動で回復してリスニング状態に遷移する時間を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

mmrp2 <ID> revertive <TIME>

no mmrp2 <ID> revertive

ID	リング ID <1-1000>
TIME	時間 <0-86400(秒)>

デフォルト

なし(＝自動で遷移しない)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の MMRP2 遷移時間を 0 に変更します。

```
> enable
# configure terminal
(config)# mmrp2 1 revertive 0
```

関連コマンド

show mmrp2, show mmrp2 detail, show running-config, clear mmrp2 failure

注意事項

本設定を行わない場合 failure からリスニング状態への復旧は"clear mmrp2 failure"コマンドを使用する必要があります。

3.43.9 mmrp2 enable

MMRP2 aware の動作を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] mmrp2 <ID> enable

ID　　リング ID <1-1000>

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) リング ID：1 の MMRP2 を有効にします。

```
> enable
# configure terminal
(config)# mmrp2 1 enable
```

関連コマンド

show mmrp2, show mmrp2 detail, show running-config

注意事項

"mmrp2 enable"コマンドを実行するためには、最低限"mmrp2 aware port"コマンド、"mmrp2 vid"コマンドでの設定が必要です。

MMRP2 が enable 中は"mmrp2 aware port"コマンド、"mmrp2 vid"コマンドは使用できません。

3.43.10 show mmrp2

MMRP2 aware の動作状態を表示します。

コマンドシンタックス

show mmrp2

コマンドモード

VIEW, ENABLE

使用例

(1) MMRP2 aware の動作状態を表示します。

```
# show mmrp2
MMRP2 Switch Configuration:
    Status  : Enable
    Group   : 1
-------------------------------------------------------------------------------
 ID   Name         Port1 Mode   Status[Connect]  Port2 Mode   Status[Connect]
-------------------------------------------------------------------------------
    1 ring1           1 Aware  Forwarding  [N]      2 Aware  Forwarding  [U]
```

ID　　：リング ID
Name　　：リング名
Port1 (Port2)　　：ポート番号、または LAG(リンクアグリゲーショングループ) ID
Mode　　：ポートに設定されている MMRP2 動作モードと MMRP2 ポートタイプ
Status　　：MMRP2 が設定されているポートの MMRP2 動作状態
　Down　　：リンクダウン状態
　Listening　　：Listening 状態
　　MMRP2 制御フレームだけを中継し、他のユーザーフレームは中継しない
　Forwarding　　：ユーザーフレームを中継する Forwarding 状態
　failure　　：リンクアップ後の状態
　　MMRP2 制御フレームも中継しないが、受信はするため、接続状態の確認は可能
Connect　　：接続状態
　N　　：ネットワーク上に障害がないことを表す
　U　　：リング型ネットワーク上に障害が発生し、MMRP2 ハローフレームが到達していないことを表す

関連コマンド

注意事項

3.43.11 show mmrp2 detail

MMRP2 aware の動作状態を詳細表示します。

コマンドシンタックス

show mmrp2 <ID> detail

ID　　リング ID <1-1000>

コマンドモード

VIEW, ENABLE

使用例

(1) リング ID：1 の MMRP2 aware の状態を表示します。

```
# show mmrp2 10 detail
Ring ID 10
  Name       :
  Status     : Enabled
  Lock       : Disabled
  Listening  : 10 sec
  Revertive  : 0 sec
  FDB Flush  : All
  Hello  VID : 3000
  Master VID : -
  Slave  VID : -
  Aware  VID : -
  Port 1: Lag 1
  Mode       : Aware
  Status     : Forwarding
  Connection : Normal
----------------------------------------------------------------
  Frame Type       Receive Frame Count     Transmit Frame Count
----------------------------------------------------------------
  HelloB1                            0                        -
  HelloB2                          122                        -
  HelloF1                            0                        -
  HelloF2                           20                        -
  Link Down                          0                        0
  Blocking                           1                        0
  Forwarding                         1                        0
  Information                        0                        -
  Port 2: Lag 2
  Mode       : Aware
  Status     : Forwarding
  Connection : Normal
----------------------------------------------------------------
  Frame Type       Receive Frame Count     Transmit Frame Count
----------------------------------------------------------------
  HelloB1                          122                        -
```

HelloB2	0	-
HelloF1	20	-
HelloF2	0	-
Link Down	0	0
Blocking	1	0
Forwarding	1	0
Information	0	-

ID　　：リング ID
Name　　：リング名
Status　　：MMRP2 動作状態
Lock　　：状態遷移禁止機能設定状態(未サポート)
Listening　　：Listening 状態タイムアウト時間
Revertive　　：Failure 状態からの回復待ち時間
　non-revertive の場合、自動では回復しない
FDB Flush　　：all(FDB 全体を消去)のみ
Hello　VID　　：ハローフレーム・制御フレームで使用する VLAN ID
Master VID　　：マスターポート経由で送受信する VLAN ID(aware には無関係)
Slave　VID　　：スレーブポート経由で送受信する VLAN ID(aware には無関係)
Aware　VID　　：(未サポート)
Port 1 (Port 2)　　：MMRP2 が設定されているポート番号、
　または LAG(リンクアグリゲーショングループ) ID
Mode　　：Aware のみ
Status　　：MMRP2 が設定されているポートの MMRP2 動作状態
　Down　　：リンクダウン状態
　Listening　　：Listening 状態
　　MMRP2 制御フレームだけを中継し、他のユーザーフレームは
　　中継しない
　Forwarding　　：ユーザーフレームを中継する状態(Forwarding)
　Failure　　：リンクアップ後の状態
　　MMRP2 制御フレームも中継しないが、受信はするため、
　　接続状態の確認は可能
Connection　　：接続状態
　Normal　　：ネットワーク上に障害がないことを表す
　Unreach　　：リング型ネットワーク上に障害が発生し、
　　MMRP2 ハローフレームが到達していないことを表す
HelloB1～　　：各パケットの送受信数
　Information

関連コマンド

注意事項

3.43.12 clear mmrp2 failure

MMRP2 リングの failure 状態を解除しリスニングにします。

コマンドシンタックス

clear mmrp2 failure <ID>

ID　　リング ID <1-1000>

コマンドモード

ENABLE

使用例

(1) リング ID：1 の MMRP2 リングを failure からリスニングに変更します。

```
> enable
# clear mmrp2 failure 1
```

関連コマンド

show mmrp2, show mmrp2 detail, mmrp2 revertive

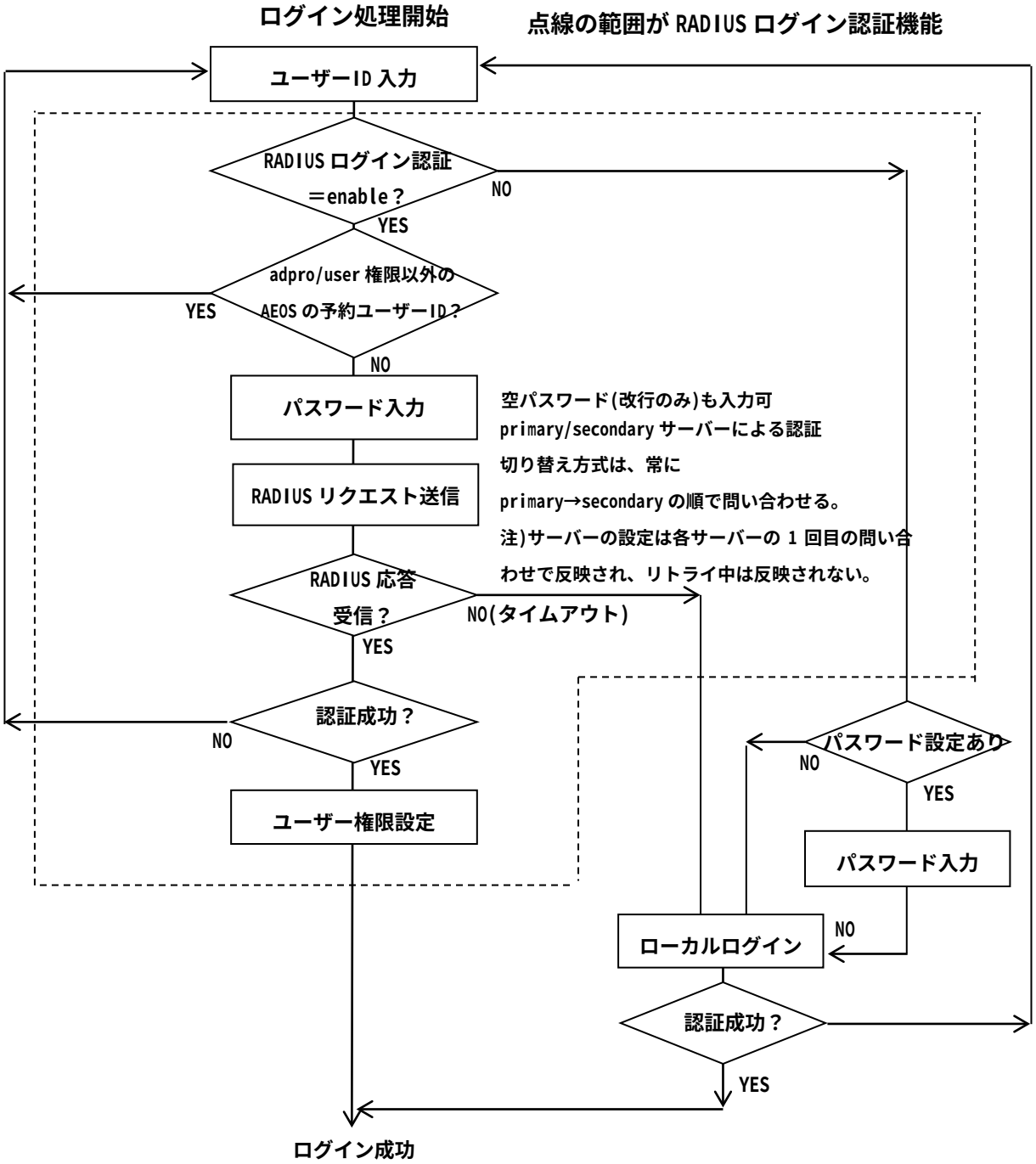
注意事項

隣接するスイッチが MMRP2 対応のスイッチの場合、両方の failure 状態を解除しないと通信を再開しません。

3.44 RADIUS ログイン認証機能

RADIUS ログイン認証機能は、スイッチにログインする際に、RADIUS サーバーでユーザー認証を行う機能です。本機能を設定しない場合通常のローカルログイン(3.1 LOGIN)が行われます。以下に、RADIUS ログイン認証機能の概略フローを示します。

ログイン処理フロー



■RADIUS 認証ユーザーID の仕様
1. 登録されているユーザーID の権限が RADIUS 認証成功の応答と異なる場合、RADIUS の応答の権限が優先される。
2. show running-config、show username では表示されない。
3. username コマンドで登録できるユーザーID の制限値(8 つ)には影響しない。
4. 以下に示す AEOS で設定できるユーザーID の形式ではない場合、ログインを拒否する。
　英数字、「.」「_」「-」、先頭が「-」でない、最大 31 文字

3.44.1 radius login enable

RADIUS ログイン認証を有効にします。無効にする場合は、no コマンドを使用してください。RADIUS ログイン認証を行うには本装置に少なくとも次の設定が必要です。

"radius login ip"
"radius login secret-key"

コマンドシンタックス

[no] radius login enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) RADIUS ログイン認証機能を有効にします。
(2) RADIUS ログイン認証機能を無効にします。

```
> enable
# configure terminal
(config)# radius login enable
(config)# no radius login enable
```

関連コマンド

show radius login configuration, show running-config

注意事項

3.44.2 radius login local-authentication disable

RADIUS サーバーからの応答がタイムアウトになった場合に、ローカルログイン(3.1 LOGIN)を行う機能を無効にします。再度有効にする場合は、no コマンドを使用してください。

通常 RADIUS サーバーからの応答がタイムアウトになった場合、RADIUS ログイン認証を行わずローカルログインを行います。本コマンドでローカルログインを行う機能を無効にすると、RADIUS サーバーからの応答がタイムアウトになった場合のローカルログインは行われません。そのためセキュリティーは確保されますが、本装置にログインできなくなる可能性があります。このため本コマンドの使用に際しては、RADIUS サーバー設定、接続などを確認のうえ慎重に行うようにしてください。

コマンドシンタックス

[no] radius login local-authentication disable

デフォルト

no disable(＝ローカルログイン有効)

コマンドモード
CONFIG

使用例
(1) ローカルログインを行う機能を無効にします。
(2) ローカルログインを行う機能を有効にします。

```
> enable
# configure terminal
(config)# radius login local-authentication disable
(config)# no radius login local-authentication disable
```

関連コマンド
show radius login configuration, show running-config

注意事項

本コマンドでローカルログインを行う機能を無効(disable)にし、RADIUS サーバーと通信できない場合、本装置にログインできません。

3.44.3 radius login ip

RADIUS ログイン認証を行う RADIUS サーバーの IP アドレス、UDP ポート番号を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

プライマリー/セカンダリー、2 つの RADIUS サーバーを設定することができます。プライマリーのみ、またはセカンダリーのみの設定も可能です。プライマリー/セカンダリーと 2 種類のサーバーを設定し、プライマリーサーバーと通信不可の場合、セカンダリーサーバーと接続を試行します。各 RADIUS サーバーと通信できない場合に、通信不可と判断するタイムアウト時間は「最大送信回数 × 再送間隔」で決まり、デフォルトで 9 秒になります。

コマンドシンタックス

```
radius login primary | secondary ip <IPADDR> [ port <PORT> ]
no radius login primary | secondary ip
```

IPADDR	RADIUS サーバーの IP アドレス
PORT	RADIUS サーバーの UDP ポート番号

デフォルト
RADIUS サーバーの IP アドレス　：なし
RADIUS サーバーの UDP ポート番号：1812

コマンドモード
CONFIG

使用例
(1) プライマリーRADIUS サーバーの IP アドレスを「192.168.10.1」、UDP ポート番号を 1645 に設定します。

(2) 設定をデフォルト値に戻します。

```
> enable
# configure terminal
(config)# radius login primary ip 192.168.10.1 port 1645
(config)# no radius login primary ip
```

関連コマンド

show radius login configuration, show running-config

注意事項

3.44.4 radius login secret-key

RADIUS サーバーと共通の secret key を設定します。設定を削除する場合は、no コマンドを使用してください。

設定する secret key は RADIUS サーバーと同一の Key を設定する必要があります。secret key は最大 127 文字長まで設定できます。

コマンドシンタックス

radius login primary | secondary secret-key <SECRET-KEY>
no radius login primary | secondary secret-key
SECRET-KEY　　RADIUS サーバーの secret key <最大 127 文字>

デフォルト

なし(＝secret key 未設定)

コマンドモード

CONFIG

使用例

(1) プライマリーRADIUS サーバーの secret key を loginsecret に設定します。
(2) プライマリーRADIUS サーバーの secret key をデフォルトに戻します。

```
# configure terminal
(config)# radius login primary secret-key loginsecret
(config)# no radius login primary secret-key
```

関連コマンド

show radius login configuration, show running-config

注意事項

secret key に使用できる文字は、ASCII コードの印字可能な文字です。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。
これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

設定した secret key は、"show radius login configuration"コマンドにおいては暗号化されて表示されます。

3.44.5 radius login max-request

RADIUS サーバーへ問い合わせるリクエストの最大送信回数を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

最大送信回数は RADIUS サーバーから応答がない状態で、RADIUS サーバーとの通信を試行する回数を示します。各 RADIUS サーバーと通信できない場合に、通信不可と判断するタイムアウト時間は「最大送信回数 × 再送間隔」となります。

コマンドシンタックス

radius login max-request <COUNT>
no radius login max-request
COUNT　　リクエスト最大送信回数 <1-5(回)>

デフォルト

3(回)

コマンドモード

CONFIG

使用例

(1) リクエストの最大送信回数を 4 回に設定します。
(2) 設定したリクエストの最大送信回数をデフォルト(3 回)に戻します。

```
# configure terminal
(config)# radius login max-request 4
(config)# no radius login max-request
```

関連コマンド

show radius login configuration, show running-config

注意事項

3.44.6 radius login request-interval

RADIUS サーバーへ問い合わせるリクエストの再送間隔を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

再送間隔は RADIUS サーバーにリクエストを送信し応答がない場合に再試行を試みる間隔です。各 RADIUS サーバーと通信できない場合に、通信不可と判断するタイムアウト時間は「最大送信回数 × 再送間隔」となります。

コマンドシンタックス

radius login request-interval <SEC>
no radius login request-interval

SEC　　リクエストを再送する間隔 <1-20(秒)>

デフォルト
3(秒)

コマンドモード
CONFIG

使用例
(1) リクエストの再送間隔を 10 秒に設定します。
(2) 設定したリクエストの再送間隔をデフォルト(3 秒)に戻します。

```
# configure terminal
(config)# radius login request-interval 10
(config)# no radius login request-interval
```

関連コマンド
show radius login configuration, show running-config

注意事項

3.44.7 show radius login configuration

RADIUS ログイン認証に関する構成情報を表示します。

コマンドシンタックス
show radius login configuration

コマンドモード
VIEW, ENABLE

使用例
(1) RADIUS ログイン認証の詳細な状態を表示します。

```
> show radius login configuration
Radius Login Authentication Configuration:
     Authentication Status       : enable
     Local Authentication Status : enable
     Server Request Interval     : 3
     Server Max Request          : 3

Primary Radius Server Configuration:
     IP Address                  : 192.168.33.213
     Port Number                 : 1812
     Secret Key (Encrypted)      : +X28xL9YI/l+QigidzZmwD$$

Secondary Radius Server Configuration:
```

```
IP Address                  : 0.0.0.0
Port Number                 : 1812
Secret Key (Encrypted)      : nmld7xDA+F1+QigidzZmwD$$
```

関連コマンド

show radius login configuration, show running-config

注意事項

3.44.8 RADIUS 属性

本項目は、RADIUS ログイン認証機能における、RADIUS サーバーとの認証要求・応答の属性項目を参考情報として示しています。装置で設定や表示を行うものではありません。

3.44.8.1 認証要求属性

属性	実装
User-Name	認証されるユーザー名
User-Password	パスワード
NAS-IP-Address	認証要求している Authenticator の IP アドレス
NAS-PORT	0：コンソール n：TELNET 接続数
NAS-PORT-Type	0(Async　：非同期(コンソール)) 5(Virtual：仮想的接続(TELNET))
Calling-Station-Id	ログイン端末の IP アドレス

3.44.8.2 認証応答属性

認証結果	属性名	実装
認証成功	Service-Type	6：adpro 権限指定 (Administrative：管理インターフェース)
	上記以外	上記以外：user 権限指定
認証失敗	なし	

3.45 SSL 機能

本機能は、NA 機能のユーザーベース認証、及び AccessDefender 機能の Web 認証で HTTPS 通信を利用する際に使用します。

装置にインストールされているデフォルトのサーバー証明書は、HTTPS 通信の動作確認のためにプライベート認証局で発行したものです。

実際の運用では、正規の認証局から発行された証明書を使用することを推奨します。

3.45.1 ssl gencsr rsakey

証明書要求と秘密鍵を作成します。秘密鍵作成の公開鍵暗号方式は RSA を使用します。使用する署名アルゴリズムはパラメーターにより指定します。

本コマンドで作成した秘密鍵は暗号化されていない状態で保存されます。既に証明書要求と秘密鍵がある場合で本コマンドを使用すると、それぞれ上書きされます。

コマンドシンタックス

ssl gencsr [sha224 | sha256 | sha384 | sha512] rsakey [<KEYLENGTH>]

sha224	署名アルゴリズムに SHA-2 のハッシュ関数 SHA-224 を使用
sha256	署名アルゴリズムに SHA-2 のハッシュ関数 SHA-256 を使用
sha384	署名アルゴリズムに SHA-2 のハッシュ関数 SHA-384 を使用
sha512	署名アルゴリズムに SHA-2 のハッシュ関数 SHA-512 を使用
省略時	署名アルゴリズムに MD5 を使用
KEYLENGTH	鍵長 <512-2048> • 署名アルゴリズムに sha512 を指定した場合 <752-2048> • 署名アルゴリズムに sha384 を指定した場合 <624-2048> • 署名アルゴリズムに上記以外を指定した場合、または省略した場合(MD5) <512-2048> • <KEYLENGTH>の指定を省略した場合 1024

デフォルト

鍵長：1024

コマンドモード

CONFIG

使用例

(1) 鍵長 1000 を指定し、証明書要求と秘密鍵を作成します。

```
> enable
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# ssl gencsr rsakey 1000
Country Name (2 letter code):JP
State or Province Name (full name):Tokyo
Locality Name (eg, city):chiyoda-ku
Organization Name (eg, company):apresia
Organizational Unit Name (eg, section):network
```

```
Common Name (YOUR domain name):www.apresia.jp
Email Address:xxx@apresia.jp
Generating a 1000 bit RSA private key
.....++++++
.......................++++++
Writing new private key
Writing to flash memory...
done.
```

表 3-43 証明書要求の項目

項目	内容	例	文字数制限
Country	国別記号	JP	2
State or Province	都道府県	Tokyo	1-128
Locality	市区町村名	shibuya-ku	1-128
Organization	組織名	example.corp	1-64
Organizational Unit	部門名	section 1	1-64
Common Name	ドメイン名(必須)	http://www.wyx.co.jp/	1-64
Email Address	電子メールアドレス	ttt@example.com	1-128

Common Name 以外は省略可能

関連コマンド

show na configuration, show running-config, show ssl csr

注意事項

文字"?"は入力できません。また、Country についてはローマ字アルファベットの大文字("A"～"Z")のみ入力可能です。

署名アルゴリズム SHA-2 の SHA-512/224、及び SHA-512/256 は未サポートです。

署名アルゴリズムは、特別な理由がない限り、最も安全性の高い SHA-512 を使用することを推奨します。

3.47.10 "web-authentication https-port"が設定されている場合、証明書要求、秘密鍵の作成ができません。作成するには、いったん"web-authentication https-port"の設定を削除してください。

3.45.2 copy csr tftp

作成した証明書要求を TFTP サーバー上のファイルにコピーします。

コマンドシンタックス

copy csr tftp <IPADDR> <FILE>

IPADDR　　TFTP サーバーの IP アドレス

FILE　　証明書要求のファイル名 <1-128(文字)>

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) 証明書要求をファイル名：SSL として IP アドレス：172.17.41.10 の TFTP サーバーにアップロードします。

```
# copy csr tftp 172.17.41.10 SSL
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

3.45.3 copy file https-file

証明書、秘密鍵を TFTP サーバー、または SD メモリーカードからダウンロードします。本装置にダウンロードした証明書、秘密鍵は即時に反映されます。

コマンドシンタックス

copy (tftp <IPADDR>) | memory-card <FILE> https-certificate | https-private-key

IPADDR　　TFTP サーバーの IP アドレス

FILE　　証明書、秘密鍵のファイル名 <1-128(文字)>

- ASCII コードの印字可能な文字の内、["][?]を除いた文字のみ使用可能

コマンドモード

ENABLE

使用例

(1) TFTP サーバーの秘密鍵をダウンロードします。

```
# copy tftp 172.17.33.21 key.pem https-private-key
getting from 172.17.33.21: key.pem
Received 1394 bytes in 0.0 seconds
Enter PEM pass phrase:
Writing to flash memory...
done.
```

(2) SD メモリーカードの秘密鍵をダウンロードします。

```
# copy memory-card key.pem https://private-key
Writing to flash memory...
done.
```

関連コマンド

注意事項

秘密鍵のファイルが暗号化されている場合、パスフレーズを入力する旨メッセージが表示されますので、秘密鍵を暗号化するのに使用したパスフレーズを入力してください。なお、暗号化の方式については DES、3DES にのみ対応します。

正しくない秘密鍵をダウンロードした場合、パスフレーズの入力を求められますが、復号に失敗します。このため有効な秘密鍵となりません。

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

中間証明書には、証明書チェーン(第三の証明書、第二の証明書を連結したもの)をお使いください。

3.47.10 "web-authentication https-port"が設定されている場合、証明書、秘密鍵はダウンロードできません。ダウンロードする場合は、いったん"web-authentication https-port"の設定を削除してください。

証明書、秘密鍵のファイルに使用できる改行コードは LF、または CR+LF です。CR は使用できません。

3.45.4 copy https-file file

本装置に保存された証明書、秘密鍵を TFTP サーバー、または SD メモリーカードへアップロードします。

コマンドシンタックス

copy https-certificate | https-private-key (tftp <IPADDR>) | memory-card <FILE>

IPADDR	TFTP サーバーの IP アドレス
FILE	証明書、秘密鍵のファイル名 <1-128(文字)> • ASCII コードの印字可能な文字の内、["][?]を除いた文字のみ使用可能

コマンドモード
ENABLE

使用例
(1) TFTP サーバーへ証明書をアップロードします。

```
# copy https-certificate tftp 172.17.33.21 key
```

(2) SD メモリーカードへ証明書をアップロードします。

```
# copy https-certificate memory-card key
```

関連コマンド

注意事項

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.45.5 erase ssl-files

証明書要求、証明書、秘密鍵を初期化します。

コマンドシンタックス
erase ssl-files

デフォルト
なし(＝設定なし)

コマンドモード
ENABLE

使用例
(1) 証明書要求、証明書、秘密鍵を初期化します。

```
# erase ssl-files
```

関連コマンド

注意事項

3.45.6 show ssl csr

証明書要求情報を表示します。

コマンドシンタックス

show ssl csr

コマンドモード

VIEW, ENABLE

使用例

(1) 証明書要求情報を表示します。

```
# show ssl csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=JP, ST=Tokyo, L=Chiyoda-ku, O=Example Domain., OU=Example Gr
oup., CN=Apresia/emailAddress=example@example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c8:60:de:59:af:79:56:e3:28:d7:ca:7e:7a:3d:
                    d7:14:07:1e:82:4c:25:d6:c4:d2:0c:a9:c6:81:84:
                    fc:2e:d8:3f:3a:85:c0:e9:6a:04:f4:c3:7c:17:b5:
                    5f:a4:81:21:e7:85:09:02:5a:a5:3e:9b:9d:78:0e:
                    ab:0b:6a:57:41:1d:ac:a4:f4:7e:54:2e:55:b8:57:
                    fa:c7:21:77:d7:5a:31:62:51:8a:ef:28:4f:39:72:
                    99:0f:f9:48:15:0a:4b:1d:34:a3:92:f2:88:49:56:
                    3d:69:f8:da:cf:72:3e:ea:02:70:09:a8:83:13:88:
                    d9:af:c8:49:5e:bf:3f:eb:19
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         a4:2f:bf:8d:06:6c:61:86:1b:93:b6:54:6d:94:0b:39:48:a8:
         e0:12:a2:33:0a:9b:c7:dd:f9:9c:1a:64:1f:ec:6c:11:b1:07:
         0d:e8:77:b3:ee:6b:e3:4c:66:41:84:6b:b0:2c:27:34:74:1d:
         bd:f4:9c:44:37:8d:3a:9e:e2:5e:67:6a:a8:9c:60:46:c3:94:
         2e:8b:b2:77:c2:4f:d7:1d:2a:77:6d:6a:32:90:12:aa:02:6f:
         59:20:39:ac:6a:1f:ca:71:30:81:fe:ca:ca:dd:8a:f6:5a:e6:
         59:86:34:81:2c:2e:a7:31:83:42:61:d4:5a:f8:b4:54:4d:61:
         de:fd
#
```

(2) 証明書要求が存在しない場合

```
# show ssl csr
% Cannot show Certificate Signing Request.
```

関連コマンド

注意事項

3.45.7 show ssl https-certificate

証明書の情報を表示します。

コマンドシンタックス

show ssl https-certificate

コマンドモード

VIEW, ENABLE

使用例

(1) 証明書の情報を表示します。

```
# show ssl https-certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bb:a5:02:2c:1d:09:56:14
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=JP, ST=Tokyo, L=Chiyoda-ku, O=Example Domain., OU=Example Gro
up., CN=Apresia/emailAddress=example@example.com
        Validity
            Not Before: Jun 24 00:23:56 2020 GMT
            Not After : Jun 19 00:23:57 2040 GMT
        Subject: C=JP, ST=Tokyo, L=Chiyoda-ku, O=Example Domain., OU=Example Gr
oup., CN=Apresia/emailAddress=example@example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c8:60:de:59:af:79:56:e3:28:d7:ca:7e:7a:3d:
                    d7:14:07:1e:82:4c:25:d6:c4:d2:0c:a9:c6:81:84:
                    fc:2e:d8:3f:3a:85:c0:e9:6a:04:f4:c3:7c:17:b5:
                    5f:a4:81:21:e7:85:09:02:5a:a5:3e:9b:9d:78:0e:
                    ab:0b:6a:57:41:1d:ac:a4:f4:7e:54:2e:55:b8:57:
                    fa:c7:21:77:d7:5a:31:62:51:8a:ef:28:4f:39:72:
                    99:0f:f9:48:15:0a:4b:1d:34:a3:92:f2:88:49:56:
```

```
                    3d:69:f8:da:cf:72:3e:ea:02:70:09:a8:83:13:88:
                    d9:af:c8:49:5e:bf:3f:eb:19
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                8A:0F:13:AA:B5:B6:B2:58:28:BB:CA:52:6F:AF:CE:CB:72:07:43:79
            X509v3 Authority Key Identifier:

keyid:88:80:80:A0:3A:0F:4A:87:5D:3F:29:A2:F1:39:66:B6:F1:FE:94:
63

    Signature Algorithm: sha256WithRSAEncryption
         ad:92:6e:30:dc:d8:02:08:4a:7c:df:a9:5f:82:8b:ea:61:27:
         5a:60:6d:04:fd:65:6d:55:bd:41:b8:37:10:eb:ef:a4:43:79:
         94:54:c6:e0:b5:89:50:2f:a3:3f:51:fb:51:97:51:c7:17:15:
         34:a1:52:f9:d2:c5:31:19:9b:c8:43:89:07:be:c1:b1:36:3f:
         e4:47:a2:b2:ed:a6:01:d2:42:ec:23:60:1a:91:c9:cb:32:d2:
         a3:5b:ad:f1:d4:4d:30:a8:83:69:76:74:b5:f9:b7:f1:0d:0f:
         e8:57:13:a3:fc:f0:83:6c:68:e4:d9:0f:cb:4c:7f:27:a7:05:
         e1:17
#
```

関連コマンド

注意事項

3.45.8 show ssl https-private-key

秘密鍵の情報を表示します。

コマンドシンタックス

show ssl https-private-key

コマンドモード

VIEW, ENABLE

使用例

(1) ファームウェアにあらかじめ埋め込まれていた場合、以下の表示になります。

```
# show ssl https-private-key
```

```
Private key is embedded in firmware.
```

(2) TFTP 経由でユーザーが本装置にインストールした場合、もしくはユーザーが"ssl gencsr rsakey"コマンドを使用して秘密鍵を生成した場合は以下の表示になります。

```
# show ssl https-private-key
Private key is installed by user.
```

関連コマンド

注意事項

3.46 NA 機能

NA(Network Authentication)機能は、ユーザー名、パスワード、MAC アドレスなどによってネットワークに接続できるユーザーを制限します。ただし、本機能を利用するにはライセンスキーの入力が必要となります。

NA では、SSLv2、SSLv3、TLS1.0、TLS1.1、TLS1.2 に対応しています。

注意事項

NA(Network Authentication)機能は、Apresia13000-48X でのみ有効です。

NA と 3.42 MMRP-Plus を装置で同時に使用できません。

NA 機能の認証ポートで OSPF、RIP、3.17 スパニングツリープロトコル(STP/RSTP/MSTP)は併用できません。

3.46.1 ライセンスキー追加

ライセンスが必要な機能を有効にします。ライセンスを別途購入する必要があります。ライセンスの購入方法については、弊社営業、または代理店にお問い合せください。

3.46.1.1 license na key

NA 機能を有効にします。

コマンドシンタックス

license na key <LICENSE_KEY>

LICENSE_KEY　　NA 機能を有効にするライセンスキー(英数字)

デフォルト

なし

コマンドモード

CONFIG

使用例

(1) NA ライセンスを有効にします。

```
(config)# license na key 913b24d4fad50337e1c8
```

関連コマンド

show license

注意事項

本ライセンスを有効にするには装置の再起動が必要となります。

3.46.1.2 show license

ライセンス情報を表示します。

コマンドシンタックス

show license

デフォルト

なし

コマンドモード

VIEW, ENABLE

使用例

(1) ライセンス情報を表示します。

```
# show license

    network authentication   enabled
    MMRP                     enabled
    Layer3 functions         enabled
```

関連コマンド

注意事項

3.46.2 na enable

NA 機能を有効にします。無効にするには、no コマンドを使用してください。

コマンドシンタックス

[no] na enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) NA 機能を有効にします。

(2) NA 機能を無効にします。

```
> enable
# configure terminal
```

```
(config)# na enable
(config)# no na enable
```

関連コマンド

show na configuration, show running-config

注意事項

本装置の時刻を戻す変更を行った場合、NA 機能が動作しない場合があります。本コマンドで再設定を行ってください。

3.46.3 na radius ip

プライマリー/セカンダリーRADIUS サーバーの IP アドレスを設定します。NA 機能を使用する際は、必ず設定してください。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

na radius primary | secondary ip <IPADDR>
no na radius primary | secondary ip
IPADDR　　RADIUS サーバーの IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) プライマリーRADIUS サーバーの IP アドレスを「192.168.33.253」に設定します。
(2) プライマリーRADIUS サーバーの IP アドレスを削除します。

```
> enable
# configure terminal
(config)# na radius primary ip 192.168.33.253
(config)# no na radius primary ip
```

関連コマンド

show na configuration, show running-config

注意事項

3.46.4 na radius port

RADIUS サーバーの UDP ポート番号を設定します。NA 機能を使用する際は、必ず設定してください。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

na radius primary | secondary port <UDP-PORT>
no na radius primary | secondary port
UDP-PORT　　RADIUS サーバーの UDP ポート番号

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) プライマリーRADIUS サーバーの UDP ポート番号を 1812 に設定します。
(2) プライマリーRADIUS サーバーのポート番号を削除します。

```
> enable
# configure terminal
(config)# na radius primary port 1812
(config)# no na radius primary port
```

関連コマンド

show na configuration, show running-config

注意事項

3.46.5 na radius secret

RADIUS サーバーの secret key を設定します。NA 機能を使用する際は、必ず設定してください。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

na radius primary | secondary secret <SECRET-KEY>
no na radius primary | secondary secret
SECRET-KEY　　RADIUS サーバーの secret key(最大 127 文字)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) プライマリーRADIUS サーバーの secret key を nasecret に設定します。
(2) プライマリーRADIUS サーバーの secret key を削除します。

```
# configure terminal
(config)# na radius primary secret nasecret
```

```
(config)# no na radius primary secret
```

関連コマンド

show na configuration, show running-config

注意事項

secret key に使用できる文字は、ASCII コードの印字可能な文字です。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。
これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

設定した secret key は、"show running-config"コマンド、"show na configuration" コマンドにおいては暗号化されて表示されます。

3.46.6 na radius max-req

RADIUS 認証時のリクエスト最大送信回数を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

na radius max-req <COUNT>
no na radius max-req
COUNT　　リクエスト最大送信回数 <1-5(回)>

デフォルト

3(回)

コマンドモード

CONFIG

使用例

(1) リクエスト最大送信回数を 4 回に設定します。
(2) 設定したリクエスト最大送信回数をデフォルト値(3 回)に戻します。

```
(config)# na radius max-req 4
(config)# no na radius max-req
```

関連コマンド

show running-config

注意事項

3.46.7 na radius request-interval

RADIUS 認証時のリクエスト再送間隔を設定します。設定をデフォルト値に戻す場合は、no コマンド

を使用してください。

コマンドシンタックス

na radius request-interval <SEC>
no na radius request-interval
SEC　　リクエストを再送する間隔 <1-60(秒)>

デフォルト

3(秒)

コマンドモード

CONFIG

使用例

(1) リクエスト再送間隔を 10 秒に設定します。
(2) 設定したリクエスト再送間隔をデフォルト(3 秒)に戻します。

```
(config)# na radius request-interval 10
(config)# no na radius request-interval
```

関連コマンド

show running-config

注意事項

リクエスト再送間隔を 1 で設定すると、初回リクエスト送信時に、リクエストの再送が同時に行われる場合があります。その場合、リクエストの再送に対する RADIUS サーバーの応答が認証結果となるため、リクエスト最大送信回数を 1 に設定していた場合は、RADIUS サーバーの状態にかかわらず認証失敗する場合があります。リクエスト再送間隔 1 での運用は避けてください。

3.46.8 na httpd name radius

認証 Web サーバー名とそれに対応する RADIUS サーバーの secret key、IP アドレス、UDP ポート番号を設定します。本コマンドで設定した認証 Web サーバー名で認証 Web ページを開くことにより、認証で使用する RADIUS サーバーを振り分けることができます。設定できる認証 Web サーバー名は最大 8 個です。

コマンドシンタックス

na httpd name <SERVER-NAME> primary-radius | secondary-radius secret-key <SECRET-KEY> ip <IPADDR> [port <UDP-PORT>]
no na httpd name <SERVER-NAME> [primary-radius | secondary-radius]
SERVER-NAME　認証 Web サーバー名(FQDN)

- 最大 63 文字
- 使用可能な文字は、ASCII コードの印字可能な文字のうち、「!」「#」

「$」「%」「&」「'」「(」「)」「*」「+」「,」「/」「:」「;」「=」「?」「@」
「[」「¥」「]」を除いた文字
- 英字の大文字小文字は同一文字とみなす

SECRET-KEY　RADIUS サーバーの secret key
- 最大 127 文字
- 使用可能な文字は、ASCII コードの印字可能な文字
- [¥]["]は制御文字として扱われる

UDP-PORT　RADIUS サーバーの UDP ポート番号 <1-65535>

デフォルト

認証 Web サーバー名：なし
RADIUS サーバーの secret key：なし
RADIUS サーバーの IP アドレス：なし
RADIUS サーバーの UDP ポート番号：1812

コマンドモード

CONFIG

使用例

(1) 認証 Web サーバー名を www.auth1.ne.jp、プライマリーRADIUS サーバーの secret key を nasecret1、IP アドレスを 172.21.41.10、UDP ポート番号を 1645 に設定します。
(2) 認証 Web サーバー名を www.auth1.ne.jp、セカンダリーRADIUS サーバーの secret key を nasecret2、IP アドレスを 172.21.41.11 に設定します。
(3) 認証 Web サーバーwww.auth1.ne.jp のセカンダリーRADIUS サーバーをデフォルトに戻します。
(4) 認証 Web サーバーwww.auth1.ne.jp の設定を削除します。

```
> enable
# configure terminal
(config)# na httpd name www.auth1.ne.jp primary-radius secret-key nasecret1 ip
172.21.41.10 port 1645
(config)# na httpd name www.auth1.ne.jp secondary-radius secret-key nasecret2
ip 172.21.41.11
(config)# no na httpd name www.auth1.ne.jp secondary-radius
(config)# no na httpd name www.auth1.ne.jp
```

関連コマンド

show na configuration, show running-config

注意事項

認証端末のブラウザーの URL で Web サーバー名により認証画面が開けるように、DNS、または認証端末のホストテーブル(hosts)により、Web サーバーの IP アドレスと Web サーバー名をマッピングしておく必要があります。

Web サーバー名は、英字の大文字小文字は同一文字とみなされます。本コマンドで設

定したWebサーバー名が、すでに設定してあるWebサーバー名と英字の大文字小文字による違いのみの場合、後から設定した文字列で上書きされます。

Webサーバー名が1つでも設定されている場合、本機能は有効となり、Webサーバー名により以下の処理を行います。
(a) 設定されたWebサーバー名の場合
(1) Webサーバー名に対するRADIUSサーバーに問い合わせる。
(2) ローカル認証/強制認証の設定がある場合、ローカル認証/強制認証を行う。
(b) 設定されたWebサーバー名以外の場合
(1) RADIUSサーバーには問い合わせない。
(2) ローカル認証/強制認証の設定があっても、ローカル認証/強制認証は行わない。

本機能が有効の場合でも、MAC認証では"na radius"コマンドで設定したRADIUSサーバーを使用しますが、usr/mac-base認証のMAC認証は本機能で設定したRADIUSサーバーを使用します。

secret keyに使用できる文字は、ASCIIコードの印字可能な文字です。ただし、「¥」「"」はRADIUSサーバーでは制御文字として扱われます。
これら文字を使用する場合には、RADIUSサーバーの仕様に従い、定義してください。

設定したsecret keyは、"show running-config"コマンド、"show na configuration"コマンドにおいては暗号化されて表示されます。

認証処理中に設定を変更して、構成情報のエントリー(プライマリー/セカンダリーのセット)にずれが生じた場合、本来問合せるRADIUSサーバーと異なるRADIUSサーバーに認証要求を送ってしまう場合があります。

3.46.9 na httpd ip

認証Webサーバーの IPアドレスを設定します。設定を削除する場合は、noコマンドを使用してください。端末と認証Webサーバーの通信は端末-Apresia間のみで行われ、通信時のパケットが他のポートに中継されることはありません。

コマンドシンタックス

```
na httpd ip <IPADDR>
no na httpd ip
```

IPADDR　　認証Webサーバーの IPアドレス

デフォルト

なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) 認証 Web サーバーの IP アドレスを 192.0.2.1 に設定します。
(2) 認証 Web サーバーの IP アドレスを削除します。

```
> enable
# configure terminal
(config)# na httpd ip 192.0.2.1
(config)# no na httpd ip
```

関連コマンド
show na configuration, show running-config

注意事項

認証用 Web サーバーの IP アドレスに、管理用 IP アドレスと同一の IP アドレス、管理用 IP アドレスと同一のネットワークアドレスを持つ IP アドレスは設定できません。

3.46.10 na httpd port

認証 Web サーバーの TCP ポート番号を設定します。NA 使用時には、必ず TCP ポート番号を設定してください。認証 Web サーバーの TCP ポートは、ネットワーク上の Web サーバーと同じポート番号には設定できません。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス
na httpd port <TCP-PORT>
no na httpd port
TCP-PORT 認証 Web サーバーの TCP ポート番号

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) 認証 Web サーバーのポート番号を 8080 に設定します。
(2) 認証 Web サーバーのポート番号を削除します。

```
> enable
# configure terminal
(config)# na httpd port 8080
(config)# no na httpd port
```

関連コマンド

show na configuration, show running-config

注意事項

3.46.11 na httpd url

認証 Web ページに表示する外部の URL と表示位置を設定します。設定を削除する場合は、no コマンドを使用してください。1 を指定した場合は認証 Web ページの上部に、2 を指定した場合は認証 Web ページの下部に、設定した URL がフレームで分割表示されます。未認証端末が外部の URL を参照するためには、HTTP パケットが外部に中継されるアクセスリストの設定が必要になります。

コマンドシンタックス

na httpd url 1 | 2 <URL>
no na httpd url 1 | 2

1	認証 Web ページの上部に表示
2	認証 Web ページの下部に表示
URL	認証 Web ページの上部、または下部に表示する URL

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) 認証 Web ページの上部に表示する URL を http://192.168.1.100 に設定します。
(2) 認証 Web ページの上部に表示する URL を削除します。

```
> enable
# configure terminal
(config)# na httpd url 1 http://192.168.1.100/
(config)# no na httpd url 1
```

関連コマンド

show na configuration, show running-config

注意事項

本コマンドと"na auth-page redirect"コマンド、もしくは"na auth-page redirect proxy-port"コマンドとの併用はできません。

3.46.12 na httpd ssl enable

認証 Web ページの SSL(Secure Socket Layer)機能を有効にします。無効にする場合は、no コマンドを使用してください。SSL 機能を有効にすることにより、SSL で認証を行うことができ、クライアント～サーバー間の安全な通信経路を確保します。ファームウェアにはあらかじめテスト用の証明書と秘密

鍵が埋め込まれており、証明書をインストールしなくても本機能をご利用頂けます。なお、お客さまの方で証明書を用意する場合は以下のいずれかの手順で、証明書/秘密鍵をインストールしてください。

(a) 証明書要求(CSR)を本装置で発行する場合

(1) CSR、及び秘密鍵の生成

3.45.1 "ssl gencsr rsakey"コマンドにより、CSR、及び秘密鍵を生成します。

(2) CSR のアップロード

3.45.2 "copy csr tftp"コマンドにより、本装置から CSR を TFTP サーバー上にアップロードします。

(3) 証明書の発行

CSR を認証局(CA)に送付し、証明書を発行してもらいます。

(4) 証明書のダウンロード

TFTP サーバー上に証明書をおき、3.45.3 "copy file https-file"コマンドにより、TFTP サーバーから本装置に証明書をダウンロードします。

(b) 証明書要求(CSR)を本装置で発行しない場合

(1) CSR、及び秘密鍵の生成

フリーソフトウェアの OpenSSL などを使用し、CSR、及び秘密鍵を生成します。

(2) 証明書の発行

CSR を認証局(CA)に送付し、証明書を発行してもらいます。

(3) 証明書、及び秘密鍵のダウンロード

TFTP サーバー上に証明書、及び秘密鍵をおき、"copy file https-file"コマンドにより、証明書、及び秘密鍵を本装置にダウンロードします。

コマンドシンタックス

[no] na httpd ssl enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) 認証 Web ページの SSL 機能を有効にします。

(2) 認証 Web ページの SSL 機能を無効にします。

```
> enable
# configure terminal
(config)# na httpd ssl enable
(config)# no na httpd ssl enable
```

関連コマンド

show na configuration, show running-config, copy file https-file

注意事項

3.46.13 na httpd sslv2 enable

認証用 Web サーバーで使用する SSL プロトコルのバージョン 2(SSLv2)を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] na httpd sslv2 enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) 認証用 Web サーバーが使用する SSL プロトコルのバージョン 2 を有効にします。
(2) 認証用 Web サーバーで使用する SSL プロトコルのバージョン 2 を無効にします。

```
> enable
# configure terminal
(config)# na httpd sslv2 enable
(config)# no na httpd sslv2 enable
```

関連コマンド

show running-config

注意事項

SSLv2 は脆弱性が確認されているため、本コマンドの設定は推奨しません。

SSLv2 は中間証明書が利用できません。中間証明書を利用する場合は、TLS(Transport Layer Security)を利用することを推奨します。

SSLv2 を使用する場合、SHA-1、または SHA-2 で作成した証明書は使用できません。

3.46.14 na httpd sslv3 enable

認証用 Web サーバーで使用する SSL プロトコルのバージョン 3(SSLv3)を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] na httpd sslv3 enable

デフォルト

no enable(＝無効)

コマンドモード
CONFIG

使用例
(1) 認証用 Web サーバーが使用する SSL プロトコルのバージョン 3 を有効にします。
(2) 認証用 Web サーバーで使用する SSL プロトコルのバージョン 3 を無効にします。

```
> enable
# configure terminal
(config)# na httpd sslv3 enable
(config)# no na httpd sslv3 enable
```

関連コマンド
show running-config

注意事項

SSLv3 は脆弱性が確認されているため、本コマンドの設定は推奨しません。

3.46.15 na httpd english-language enable

認証 Web ページの画面を英語で表示します。日本語に戻す場合は、no コマンドを使用してください。

コマンドシンタックス
[no] na httpd english-language enable

デフォルト
no enable(＝無効)

コマンドモード
CONFIG

使用例
(1) 認証 Web ページの英語表示を有効にします。
(2) 認証 Web ページの英語表示を無効にします。

```
> enable
# configure terminal
(config)# na httpd english-language enable
(config)# no na httpd english-language enable
```

関連コマンド
show na configuration, show running-config

注意事項

3.46.16 na port shared mode

shared ポートモードを適用するポートと、そのポートでの認証方法(MAC ベース、ユーザーベース、ユーザー/MAC ベース、またはデュアルベース)を指定します。設定を削除する場合は、no コマンドを使用してください。shared ポートモードは、主に 1 ポートあたり複数端末の認証を行う場合に使用し、同一 VLAN 内の異なるポート間でのローミングが可能です("na roaming enable"項参照)。

MAC ベース認証は、ポートに接続した端末の MAC アドレスによる認証を行います。

ユーザーベース認証では、Web ブラウザーへ入力されたユーザー名とパスワードによる認証を行います。

ユーザー/MAC ベース認証では、ユーザーベース認証に加え、MAC アドレスによる認証を行います。

デュアルベース認証では、MAC ベース認証かユーザーベース認証のいずれでも認証できます。

MAC ベース認証では MAC アドレスと MAC パスワード("na mac-base passwd"項参照)を、ユーザーベース認証ではユーザー名とパスワードを、認証方法によって、RADIUS サーバー、またはローカルデータベースに登録しておく必要があります。また、ユーザー/MAC ベース認証ではそれらの両方を、デュアルベース認証では、いずれかを登録しておく必要があります。

コマンドシンタックス

na port <PORTRANGE> shared mode dual-mac-user-base | mac-base | user-base | user/mac-base
no na port <PORTRANGE>

PORTRANGE	ポート番号(複数指定可能)
dual-mac-user-base	デュアルベースモード
mac-base	MAC ベースモード
user-base	ユーザーベースモード
user/mac-base	ユーザー/MAC ベースモード

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1～3 を shared mode、user-base 認証に設定します。
(2) ポート：1～3 の設定を削除します。

```
> enable
# configure terminal
(config)# na port 1-3 shared mode user-base
(config)# no na port 1-3
```

関連コマンド

show na configuration, show running-config

注意事項

ユーザーベース認証、ユーザー/MAC ベース認証、及びデュアルベース認証で用いる

ユーザーID は 63 文字まで、パスワードは 63 文字まで入力可能ですが、使用する RADIUS サーバーの仕様に従い、定義する必要があります。

ユーザーベース認証、ユーザー/MAC ベース認証、及びデュアルベース認証で用いるユーザーID とパスワードに使用できる文字は、ASCII コードの印字可能な文字です。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。
これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

認証のために装置に接続可能な端末数は装置 1 台あたり最大 300 になります(端末の認証が同時に行われた場合の性能を保証するものではありません)。

NA と 3.27 ポートセキュリティー、3.11.7 "vlan add protocol"機能を同一のポートで使用しないでください。同一のポートで使用した場合の動作は保証されません。

認証装置の 3.40 DHCP サーバー機能により認証端末が IP アドレスを取得する構成では、RADIUS サーバーが未接続の場合、MAC ベース、及びデュアルベース認証の認証端末は、DHCP サーバーより IP アドレスを取得することができません。RADIUS サーバー接続後に認証端末が正常認証、もしくは discard 登録後、IP アドレスを取得することができます。

認証端末の MAC アドレスが FDB への登録に失敗した場合、FDB が消去されます。その場合、認証処理は失敗となるため再度認証処理を行ってください。

認証端末が DHCP サーバー機能より IP アドレスを取得する構成では、必ず、"na dhcp-relay-port"コマンドの設定を行ってください(認証装置の DHCP サーバー機能より IP アドレスを取得する構成の場合は、認証ポート以外の任意のポートを指定する)。

3.46.17 na port designated mode

designated ポートモードを適用するポートと、そのポートでの認証方法(MAC ベース、ユーザーベース、またはユーザー/MAC ベース)を指定します。設定を削除する場合は、no コマンドを使用してください。デュアルベースは選択できません。designated ポートモードは、1 ポートあたり 1 端末の認証を行う場合に使用し、認証端末接続ポートに対する動的な VLAN の割り当てが可能です。designated ポートモードはアクセスポートのみで指定でき、トランクポートでは指定できません。また、designated ポートモードで認証された認証端末に対しては、ポーリングによるログアウト、ローミングによる接続ポートの移動を行うことはできません。

コマンドシンタックス

```
na port <PORTRANGE> designated mode mac-base | user-base | user/mac-base
no na port <PORTRANGE>
```

PORTRANGE　　ポート番号(複数指定可能)

mac-base	MAC ベースモード
user-base	ユーザーベースモード
user/mac-base	ユーザー/MAC ベースモード

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1～3 を designated mode、user-base 認証に設定します。

(2) ポート：1～3 の設定を削除します。

```
> enable
# configure terminal
(config)# na port 1-3 designated mode user-base
(config)# no na port 1-3
```

関連コマンド

show na configuration, show running-config

注意事項

ユーザーベース認証、及びユーザー/MAC ベース認証で用いるユーザーID は 63 文字まで、パスワードは 63 文字まで入力可能ですが、使用する RADIUS サーバーの仕様に従い、定義する必要があります。

ユーザーベース認証、及びユーザー/MAC ベース認証で用いるユーザーID とパスワードに使用できる文字は、ASCII コードの印字可能な文字です。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

NA と 3.27 ポートセキュリティー、3.11.7 "vlan add protocol"機能を同一のポートで使用しないでください。同一のポートで使用した場合の動作は保証されません。

認証装置の 3.40 DHCP サーバー機能により認証端末が IP アドレスを取得する構成では、RADIUS サーバーが未接続の場合、MAC ベース認証の認証端末は、DHCP サーバーより IP アドレスを取得することができません。RADIUS サーバー接続後に認証端末が正常認証、もしくは discard 登録後、IP アドレスを取得することができます。

認証端末の MAC アドレスが FDB への登録に失敗した場合、FDB が消去されます。その場合、認証処理は失敗となるため再度認証処理を行ってください。

認証端末が DHCP サーバー機能より IP アドレスを取得する構成では、必ず、"na dhcp-relay-port"コマンドの設定を行ってください(認証装置の DHCP サーバー機能より IP アドレスを取得する構成の場合は、認証ポート以外の任意のポートを指定する)。

3.46.18 na port shared-dynamic-vlan mode

shared-dynamic-vlan ポートモードを適用するポートと、そのポートでの認証方法(MAC ベース、ユーザーベース、ユーザー/MAC ベース、デュアルベース)を指定します。設定を削除する場合は、no コマンドを使用してください。

shared-dynamic-vlan ポートモードは、認証時に認証端末ごとに動的に VLAN を割り当てる認証モードです。本モードは、designated モードとは異なり、1 ポートで複数端末の認証が可能であり、認証端末ごとに VLAN の割り当てが可能です。

また、shared-dynamic-vlan ポートモードで認証された認証端末に対しては、ポーリングによるログアウト、ローミングによる接続ポートの移動を行うことはできません。

コマンドシンタックス

na port <PORTRANGE> shared-dynamic-vlan mode mac-base | user-base | user/mac-base | dual-mac-user-base

no na port <PORTRANGE>

PORTRANGE	ポート番号(複数指定可能)
mac-base	MAC ベースモード
user-base	ユーザーベースモード
user/mac-base	ユーザー/MAC ベースモード
dual-mac-user-base	デュアルベースモード

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1～3 を shared-dynamic-vlan mode、user-base 認証に設定します。

(2) ポート：1～3 の設定を削除します。

```
> enable
# configure terminal
(config)# na port 1-3 shared-dynamic-vlan mode user-base
(config)# no na port 1-3
```

関連コマンド

show na configuration, show running-config

注意事項

ユーザーベース認証、ユーザー/MAC ベース認証、及びデュアルベース認証で用いるユーザーID は 63 文字まで、パスワードは 63 文字まで入力可能ですが、使用する RADIUS サーバーの仕様に従い、定義する必要があります。

ユーザーベース認証、ユーザー/MAC ベース認証、及びデュアルベース認証で用いるユーザーID とパスワードに使用できる文字は、ASCII コードの印字可能な文字です。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。
これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

NA と 3.27 ポートセキュリティー、3.11.7 "vlan add protocol"を同一のポートで使用しないでください。同一のポートで使用した場合の動作は保証されません。

認証のために装置に接続可能な端末数は装置 1 台あたり最大 300 になります(端末の認証が同時に行われた場合の性能を保証するものではありません)。

認証端末の MAC アドレスが FDB への登録に失敗した場合、FDB が消去されます。その場合、認証処理は失敗となるため再度認証処理を行ってください。

本装置の 3.40 DHCP サーバー機能を併用して、端末へ動的に VLAN を割り当てる場合、認証前 VLAN 用の DHCP サーバーと、認証後 VLAN 用の DHCP サーバーは同一装置内に設定しないでください。認証後 VLAN の IP アドレスに切り替わらないことがあります。

デュアルベース認証使用時、認証 Web ページにアクセスした未認証端末は、ユーザーベース認証待ち状態となるため、最終アクセス以後の 60 秒間は新規に MAC 認証を行いません。

認証端末が DHCP サーバー機能より IP アドレスを取得する構成では、必ず、"na dhcp-relay-port"コマンドの設定を行ってください(認証装置の DHCP サーバー機能より IP アドレスを取得する構成の場合は、認証ポート以外の任意のポートを指定する)。

3.46.19 na filter permit-ttl

ユーザーベース認証、及びユーザー/MAC ベースの認証ポートでフィルタリング認証を行う TTL、ポートを設定します。設定を削除する場合は、no コマンドを使用してください。設定できる TTL、ポートの組み合わせは最大 8 個です。

コマンドシンタックス

```
na filter permit-ttl <TTL> port <PORTRANGE>
no na filter permit-ttl [ <TTL> [ port <PORTRANGE> ] ]
```

TTL　　IP ヘッダーの TTL(Time To Live)値 <1-255>

PORTRANGE　　フィルタリング認証対象ポート(複数指定可能)

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) 認証を行う TTL の値を 128、フィルタリング認証対象ポートを 1～3、10、12～15 ポートに設定します。
(2) 認証を行う TTL の値 128 のフィルタリング認証対象ポートのうち、1～3、10 ポートを削除します。
(3) 認証を行う TTL の値 128 を削除します。
(4) 認証を行う TTL の値を工場出荷時の値に設定します。

```
> enable
# configure terminal
(config)# na filter permit-ttl 128 port 1-3,10,12-15
(config)# no na filter permit-ttl 128 port 1-3,10
(config)# no na filter permit-ttl 128
(config)# no na filter permit-ttl
```

関連コマンド
show na configuration, show running-config

注意事項

3.46.20 na force-authorized port

強制認証機能を有効にします。無効にする場合は、no コマンドを使用してください。強制認証を有効にしたポートでは RADIUS サーバーが無い場合、RADIUS サーバーからの応答がタイムアウトした場合、ならびに secret key が異なる場合、未認証のままネットワークに接続することができます。

コマンドシンタックス
[no] na force-authorized port <PORTRANGE>
PORTRANGE　　ポート番号(複数指定可能)

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) ポート：1～3 で強制認証を有効にします。

(2) ポート：1～3 の強制認証を無効します。

```
> enable
# configure terminal
(config)# na force-authorized port 1-3
(config)# no na force-authorized port 1-3
```

関連コマンド

show na configuration, show running-config

注意事項

強制認証機能はセキュリティー上の問題となる可能性がありますので、十分検討の上使用してください。

designated モードを適用したポートでは強制認証機能を有効にすることは可能ですが、未認証端末がネットワークに接続された場合に動的な VLAN の割り当ては行われません。

3.46.21 na local-authorized port

ローカル認証を有効にするポートを設定します。設定を無効にする場合は、no コマンドを使用してください。

ローカル認証を有効にしたポートは、RADIUS サーバーの設定がない場合、または RADIUS サーバーからの応答がタイムアウトした場合に本装置内に設定された認証用のローカルデータベースをチェックし、該当する端末に対してローカル認証を行います。

ローカルデータベースのフォーマットについては、"copy tftp local-db"の項を参照してください。

コマンドシンタックス

[no] na local-authorized port <PORTRANGE>

PORTRANGE　　ポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ポート：1～3 でローカル認証を有効にします。

(2) ポート：1～3 のローカル認証を無効します。

```
(config)# na local-authorized port 1-3
(config)# no na local-authorized port 1-3
```

関連コマンド

show running-config

注意事項

3.46.22 na logout aging

エージングログアウト機能の設定を行います。設定を削除する場合は、no コマンドを使用してください。

エージングログアウト機能は、認証済み端末が設定したエージング間隔の期間無通信状態の場合に、認証済み端末を自動的にログアウトさせる機能です。エージング間隔は 0、10-86400(秒)、0-59(分)、0-23(時間)、0-31(日数)の間で指定し、0 を指定した場合にはエージングログアウトは行われません。

パラメーター指定の際は、秒、分、時間、日数の順で行い、分、時間、日数については省略することができます。

パラメーターは、すべての時間の合計を秒に換算します。パラメーターを"100 1 0 0"に設定した場合には 160 秒後にログアウトします。

また、"show na configuration"コマンドで確認する際の設定時間は秒単位表示となります。

AEOS Ver. 7.09.01 より分、時間、日数の設定が可能になっていますが、これら設定ができない従来版からのコマンドの引継ぎは可能です。

無通信時間のカウントは、本装置と認証済み端末間の通信が終了してから、最大 2 × 装置のポート数(秒)で開始されます。必ずしも通信終了後に、即座にカウントが開始するわけではないことに注意してください。

また、無通信時間のカウント状況は"show na aging"コマンドで確認してください。

コマンドシンタックス

na logout aging <SECONDS> [<MINUTES> [<HOURS> [<DAYS>]]]
no na logout aging

SECONDS	エージング間隔 <10-86400(秒)>
MINUTES	エージング間隔 <0-59(分)>
HOURS	エージング間隔 <0-23(時間)>
DAYS	エージング間隔 <0-31(日数)>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) エージング間隔を 300 秒に設定します。
(2) エージング間隔の設定を削除します。

```
> enable
# configure terminal
(config)# na logout aging 300
(config)# no na logout aging
```

関連コマンド
show na configuration, show running-config, show na aging

注意事項

無通信時間のカウントを開始するまでの時間は、以下のようになります。
最小：0 秒～最大：(2 × 装置のポート数)秒
従って、エージングログアウトされるタイミングは設定時間に加え、最大(2 × 装置のポート数)秒の誤差が出ます。

(計算例)
Apresia13000-48X(50 ポート) エージング間隔：10(秒)の場合
最大エージングログアウト時間 = 2 * 50 + 10 = 110(秒)

3.46.23 na logout ping ttl

logout ping の TTL を設定します。設定を削除する場合は、no コマンドを使用してください。認証済み端末から本コマンドで指定した TTL の ping を受信すると、送信元の端末は自動的にログアウトされ、未認証状態になります。

コマンドシンタックス
na logout ping ttl <TTL>
no na logout ping ttl
TTL IP パケットの TTL(Time To Live)値

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) logout ping の TTL を 1 に設定します。
(2) logout ping の TTL の設定を削除します。

```
> enable
# configure terminal
(config)# na logout ping ttl 1
(config)# no na logout ping ttl
```

関連コマンド
show na configuration, show running-config

注意事項

3.46.24 na logout ping dest-ip

logout ping の宛先 IP アドレスを設定します。設定を削除する場合は、no コマンドを使用してください。認証済み端末から本コマンドで指定した宛先 IP アドレスの ping を受信すると送信元の端末は自動的にログアウトされ、未認証状態になります。

コマンドシンタックス

na logout ping dest-ip <IPADDR>
no na logout ping dest-ip
IPADDR　　logout ping の宛先 IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) logout ping の宛先 IP アドレスを 1.2.3.4 に設定します。
(2) logout ping の宛先 IP アドレスの設定を削除します。

```
> enable
# configure terminal
(config)# na logout ping dest-ip 1.2.3.4
(config)# no na logout ping dest-ip
```

関連コマンド

show na configuration, show running-config

注意事項

"ip forwarding"機能が有効な場合、かつ認証端末のゲートウェイ(ネクストホップ)アドレスを認証装置の IP アドレスに設定した場合は、logout ping の宛先 IP アドレスを、認証端末と同じ VLAN 内で通信可能な装置の IP アドレスに設定してください。それ以外に設定した場合、NA Logout Ping 機能によるログアウトが有効にならない場合があります。

3.46.25 na logout timeout

認証済み端末のタイムアウト時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。認証済み端末は、本コマンドで指定した時間が経過すると自動的にログアウトされ、未認証状態になります。タイムアウト時間は 0、10-86400(秒)、0-59(分)、0-23(時間)、0-31(日数)の間で指定し、0 を指定した場合、自動ログアウトを行いません。パラメーター指定の際は、(秒)、(分)、(時間)、(日数)の順で行い、(分)、(時間)、(日数)については省略することができます。

パラメーターは、すべての時間の合計を秒に換算します。パラメーターを"100 1 0 0"に設定した場

合には160秒後にログアウトします。
また"show na configuration"コマンドで確認する際の設定時間は秒単位表示となります。
AEOS Ver. 7.09.01 より分、時間、日数の設定が可能になっていますが、これら設定ができない従来版からのコマンドの引継ぎは可能です。

コマンドシンタックス

na logout timeout <SECONDS> [<MINUTES> [<HOURS> [<DAYS>]]]
no na logout timeout

SECONDS	認証済み端末の自動ログアウトタイムアウト時間 <0-86400(秒)>
MINUTES	認証済み端末の自動ログアウトタイムアウト時間 <0-59(分)>
HOURS	認証済み端末の自動ログアウトタイムアウト時間 <0-23(時間)>
DAYS	認証済み端末の自動ログアウトタイムアウト時間 <0-31(日数)>

デフォルト

0(秒)

コマンドモード

CONFIG

使用例

(1) タイムアウトを3600秒に設定します。
(2) タイムアウトの設定を削除します。

```
> enable
# configure terminal
(config)# na logout timeout 3600
(config)# no na logout timeout
```

関連コマンド

show na configuration, show running-config

注意事項

3.46.26 na logout polling interval

本装置から認証済み端末へのポーリング間隔を設定します。設定をデフォルト値に戻す場合は、noコマンドを使用してください。ポーリングの対象は、sharedポートモードのユーザーベース、ユーザー/MACベース、デュアルベースでログインした端末のみです(sharedポートモードのMACベースでログインした端末は対象外)。またデュアルベースモードでログインした場合、ユーザーベース認証でログインした端末のみにポーリングは有効です。本装置は、本コマンドで指定した時間ごとにpingを認証済み端末に送信します。0を指定した場合、ポーリングを行いません。また、"na logout polling count"コマンドで、ポーリング回数に0を指定した場合も、ポーリングは行いません。

コマンドシンタックス

na logout polling interval <SEC>
no na logout polling interval

SEC　　本装置から認証済み端末へのポーリング間隔 <0-86400(秒)>

デフォルト
0(秒)

コマンドモード
CONFIG

使用例
(1) ポーリング間隔を 300 秒に設定します。
(2) ポーリング間隔の設定を削除します。

```
> enable
# configure terminal
(config)# na logout polling interval 300
(config)# no na logout polling interval
```

関連コマンド
show na configuration, show running-config

注意事項

3.46.27 na logout polling count

本装置から認証済み端末あてポーリングの最大失敗回数を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。"na logout polling interval"コマンドで設定したポーリングに、本コマンドで指定した回数分連続して失敗すると、認証済み端末は自動的にログアウトされ、未認証状態になります。0 を指定した場合、ポーリング送信は行いません。

コマンドシンタックス
na logout polling count <NUMBER>
no na logout polling count
NUMBER　　自動的にログアウトするポーリングの失敗回数 <0-255(回)>

デフォルト
0(回)

コマンドモード
CONFIG

使用例
(1) ポーリングの失敗回数を 5 回に設定します。
(2) ポーリングの失敗回数の設定を削除します。

```
> enable
# configure terminal
(config)# na logout polling count 5
```

```
(config)# no na logout polling count
```

関連コマンド

show na configuration, show running-config

注意事項

3.46.28 na logout clock

認証済み端末のログアウト時刻を設定します。設定を削除する場合は、no コマンドを使用してください。時刻は 8 個まで設定できます。認証済み端末は、本コマンドで指定した時刻になると自動的にログアウトされ、未認証状態になります。

コマンドシンタックス

na logout clock <HH:MM>
no na logout clock [<HH:MM>]

HH:MM　　時刻を 24 時間表記で次のように指定
- HH 時間
- MM 分

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ログアウト時刻を 17 時 15 分に設定します。
(2) (1)の設定を削除します。
(3) ログアウト時刻の設定を削除します。

```
> enable
# configure terminal
(config)# na logout clock 17:15
(config)# no na logout clock 17:15
(config)# no na logout clock
```

関連コマンド

show na configuration, show running-config

注意事項

本装置の時刻を戻す変更を行った場合、設定時刻にログアウトが行われない場合があります。ログアウト時刻の再設定を行ってください。

3.46.29 na mac-base passwd

MACベース認証のパスワードを設定します。設定を削除する場合は、noコマンドを使用してください。MACベース認証を使う場合、認証方法によって、RADIUSサーバー、またはローカルデータベースにMAC認証のパスワードとして本コマンドで設定したパスワードを登録しておく必要があります。

コマンドシンタックス

na mac-base passwd <PASSWORD>
no na mac-base passwd
PASSWORD　　MACベース認証を行うためのパスワード

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) MACベース認証のパスワードを"napasswd"に設定します。
(2) MACベース認証のパスワードの設定を削除します。

```
> enable
# configure terminal
(config)# na mac-base passwd napasswd
(config)# no na mac-base passwd
```

関連コマンド

show na configuration, show running-config

注意事項

3.46.30 na arp-relay-port

NA適用ポートに接続された端末からのARPをリレーするポートを設定します。設定を削除する場合は、noコマンドを使用してください。本機能は、未認証端末のARPを解決するために使用します。

コマンドシンタックス

[no] na arp-relay-port <PORTRANGE>
PORTRANGE　　NA適用ポートに接続された端末からのARPをリレーするポート(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ARP をリレーするポートをポート：1～3 に設定します。

(2) ARP をリレーするポートの設定を削除します。

```
> enable
# configure terminal
(config)# na arp-relay-port 1-3
(config)# no na arp-relay-port 1-3
```

関連コマンド

show na configuration, show running-config

注意事項

本コマンドを有効にするとパケットフィルター2 のグループを 1 個使用します。

本機能は NA MAC ベースモードでは動作しません。

3.8 リンクアグリゲーション、3.9 ポートリダンダントのメンバーポートをリレー先ポートに設定する場合、すべてのメンバーポートをリレー先に設定してください。

3.46.31 na arp-relay-port vid

NA 適用ポートに接続された端末からの ARP のうち、リレー対象となる送信元 VLAN ID を設定します。設定を削除する場合は、no コマンドを使用してください。リレー先ポートは"na arp-relay-port"で設定します。最大 8 個まで設定できます。

コマンドシンタックス

[no] na arp-relay-port vid <VID>

VID　　送信元 VLAN ID <1-4094>

デフォルト

なし

コマンドモード

CONFIG

使用例

(1) NA 適用ポートに接続された端末から受信する ARP パケットのうち、送信元 VLAN ID が 41 のパケットをリレー対象パケットとして設定します。

(2) 送信元 VLAN ID が 41 の ARP リレー対象パケットの設定を削除します。

```
> enable
# configure terminal
(config)# na arp-relay-port vid 41
(config)# no na arp-relay-port vid 41
```

関連コマンド

na arp-relay-port, show na configuration, show running-config

注意事項

本コマンドで VLAN ID を設定しない場合は、NA 適用ポートに接続された端末からの ARP をすべてリレー先ポートにリレーします。リレー対象パケットの中継処理は CPU 処理となるため、CPU 負荷増を極力抑える必要があり、VLAN ID 設定によるリレー対象パケットを限定することを推奨致します。

本コマンドで設定する VLAN ID は、designated モードで使用する暫定 VLAN の VLAN ID を設定し、それ以外の VLAN ID は設定しないようにしてください。

3.46.32 na dhcp-relay-port

NA 適用ポートに接続された端末からの DHCP をリレーするポートを設定します。設定を削除する場合は、no コマンドを使用してください。dhcp-relay-port の設定がある場合、認証状態に関わらず設定に従って DHCP パケットのリレーを行います。

コマンドシンタックス

[no] na dhcp-relay-port <PORTRANGE>

PORTRANGE	NA 適用ポートに接続された端末からの DHCP をリレーするポート (複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) DHCP をリレーするポートをポート：1～3 に設定します。

(2) DHCP をリレーするポートの設定を削除します。

```
> enable
# configure terminal
(config)# na dhcp-relay-port 1-3
(config)# no na dhcp-relay-port 1-3
```

関連コマンド

show na configuration, show running-config

注意事項

本コマンドを有効にするとパケットフィルター2 のグループを 1 個使用します。

本機能は NA MAC ベースモードでは動作しません。

3.8 リンクアグリゲーション、3.9 ポートリダンダントのメンバーポートをリレー先ポートに設定する場合、すべてのメンバーポートをリレー先に設定してください。

3.46.33 na roaming enable

NA のローミング機能を有効にします。無効にする場合は、no コマンドを使用してください。認証済み端末がログアウトせずに接続ポートを移動した場合、端末からのパケットをトリガとして、認証したポートを自動的に切り替えることができます。ローミング機能は、同じ装置内で、かつ同じ VLAN 内の shared ポートモードに設定されたポート間のみで可能です。

コマンドシンタックス

[no] na roaming enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) ローミング機能を有効にします。
(2) ローミング機能の設定を削除します。

```
> enable
# configure terminal
(config)# na roaming enable
(config)# no na roaming enable
```

関連コマンド

show na configuration, show running-config

注意事項

3.46.34 na disc-mac-delete interval

MAC ベース認証で認証に失敗した MAC アドレスを FDB に discard で登録する時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。MAC ベース認証では、受信した任意のパケットをもとに認証を行いますが、認証に失敗した MAC アドレスを FDB に discard で登録することにより、当該 MAC アドレスからのパケットを廃棄して装置の CPU の負荷を軽減させています。本コマンドで指定した時間が経過すると FDB に discard で登録された MAC アドレスを自動的に削除し、未認証状態にします。

0を指定した場合、discardで登録したままの状態で、削除は行いません。

コマンドシンタックス

na disc-mac-delete interval <SECOND>
no na disc-mac-delete interval
SECOND　認証失敗によりFDBにdiscardで登録されるMACアドレスの登録時間 <0-86400(秒)>

デフォルト

300(秒)

コマンドモード

CONFIG

使用例

(1) discard登録時間を3600秒に設定します。
(2) discard登録時間を工場出荷時の値に設定します。

```
> enable
# configure terminal
(config)# na disc-mac-delete interval 3600
(config)# no na disc-mac-delete interval
```

関連コマンド

show na configuration, show running-config

注意事項

FDBにdiscardで登録できるMACアドレスは100個までです。

intervalに0を指定した状態で100個以上認証失敗した場合、101個目以降のMACアドレスはdiscardで登録することができないため、CPUに負荷がかかり、装置の動作が遅くなる場合があります。

3.46.35 na clear

mac <MACADDR>を指定すると、認証に成功、または失敗したMACアドレスを未認証状態にします。disc-macを指定すると、認証に失敗したすべてのMACアドレスを未認証状態にします。

コマンドシンタックス

na clear mac <MACADDR>
na clear disc-mac
MACADDR　認証に成功、または失敗したMACアドレス

コマンドモード

CONFIG

使用例

(1) 認証に成功(または失敗)した MAC アドレスを未認証状態にします。
(2) 認証に失敗したすべての MAC アドレスを未認証状態にします。

```
> enable
# configure terminal
(config)# na clear mac 00:0b:db:d7:53:18
(config)# na clear disc-mac
```

関連コマンド

show na client, show mac-address-table

注意事項

3.46.36 na custom-relay-port port

NA 適用ポートに接続された端末から受信するパケットのリレー先ポートを設定します。設定を削除する場合は、no コマンドを使用してください。リレー対象パケットは、"na custom-relay-port ip"、"na custom-relay-port tcp"、"na custom-relay-port udp"で指定します。

コマンドシンタックス

[no] na custom-relay-port port <PORTRANGE>

PORTRANGE	NA 適用ポートに接続された端末から受信するパケットのリレー先ポート(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) NA 適用ポートに接続された端末から受信するパケットのリレー先ポートを 1～3、10、12～15 ポートに設定します。
(2) custom-relay の設定を削除します。

```
> enable
# configure terminal
(config)# na custom-relay-port port 1-3,10,12-15
(config)# no na custom-relay-port port 1-3,10,12-15
```

関連コマンド

show na configuration, show running-config

注意事項

指定されたリレー対象パケットは、ソフトウェア中継されます。対象パケットのトラフィック量が多い場合に、CPU に過剰な負荷をかけることになります。このため定常的に(頻繁に)通信が発生するファイルサーバーなどを極力宛先に指定しないようにするか、宛先、パケット種別などを限定して指定してください。

本機能は NA MAC ベースモードでは動作しません。

本機能をはじめとするリレー機能(custom-relay、dhcp-relay、arp-relay)は、装置がレイヤー2 として動作している場合("ip forwarding"機能が disable の状態)でのみ使用可能です。装置がレイヤー3 として動作している場合("ip forwarding"機能が enable の状態)、同一装置の同一ポートにて L3 中継とリレー機能を併用することはできません。詳細は別冊の、「アプリケーションノート(Network Authentication 編)」の「未認証端末のパケット強制転送」の項目を参照ください。

3.8 リンクアグリゲーション、3.9 ポートリダンダントのメンバーポートにリレー先ポートを設定する場合、すべてのメンバーポートにリレー先を設定してください。

3.46.37 na custom-relay-port ip

NA 適用ポートに接続された端末から受信するリレー対象パケットの宛先 IP アドレス、宛先 TCP/UDP ポート番号、VLAN ID を指定します。設定を削除する場合は、no コマンドを使用してください。一つのコマンドで対象条件を複数指定した場合は、条件をすべて満たしたパケットがリレーされます。リレー先ポートは"na custom-relay-port port"で設定します。リレー先ポートが設定されていない場合、本コマンドで指定した対象パケットを受信してもパケットのリレーは行われません。

コマンドシンタックス

```
[ no ] na custom-relay-port ip <IPADDR> [ vid <VID> ]
[ no ] na custom-relay-port ip <IPADDR> tcp <TCP PORT> [ vid <VID> ]
[ no ] na custom-relay-port ip <IPADDR> udp <UDP PORT> [ vid <VID> ]
```

IPADDR	リレーする宛先 IP アドレス
TCP PORT	リレーする宛先 TCP ポート番号 <1-65535>
UDP PORT	リレーする宛先 UDP ポート番号 <1-65535>
VID	リレー対象パケットの VLAN ID <1-4094>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) NA 適用ポートに接続された端末から受信するパケットのうち、宛先 IP アドレスが 172.17.41.5、

宛先 TCP ポート番号が 60001 のパケットをリレー対象パケットとして設定します。

(2) (1)の設定を削除します。

(3) NA 適用ポートに接続された端末から受信するパケットのうち、宛先 IP アドレスが 172.17.41.10、宛先 TCP ポート番号が 60100、VLAN ID が 100 のパケットをリレー対象パケットとして設定します。

(4) (3)の設定を削除します。

```
> enable
# configure terminal
(config)# na custom-relay-port ip 172.17.41.5 tcp 60001
(config)# no na custom-relay-port ip 172.17.41.5 tcp 60001
(config)# na custom-relay-port ip 172.17.41.10 tcp 60100 vid 100
(config)# no na custom-relay-port ip 172.17.41.10 tcp 60100 vid 100
```

関連コマンド

show na configuration, show running-config

注意事項

設定可能な数は、custom-relay-port ip、custom-relay-port tcp、custom-relay-port udp 合わせて 8 個までです。

リレー対象パケットの中継処理は CPU 処理となるため、CPU 負荷増を極力抑える必要があり、VLAN ID 設定によるリレー対象パケットを限定することを推奨致します。

3.46.38 na custom-relay-port tcp

NA 適用ポートに接続された端末から受信するリレー対象パケットの宛先 TCP ポート番号、VLAN ID を指定します。設定を削除する場合は、no コマンドを使用してください。一つのコマンドで対象条件を複数指定した場合は、条件をすべて満たしたパケットがリレーされます。リレー先ポートは"na custom-relay-port port"で設定します。リレー先ポートが設定されていない場合、本コマンドで指定した対象パケットを受信してもパケットのリレーは行われません。

コマンドシンタックス

```
[ no ] na custom-relay-port tcp <TCP PORT> [ vid <VID> ]
      TCP PORT            リレーする宛先 TCP ポート番号 <1-65535>
      VID                 リレー対象パケットの VLAN ID <1-4094>
```

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) NA 適用ポートに接続された端末から受信するパケットのうち、宛先 TCP ポート番号が 60001 の TCP パケットをリレー対象パケットとして設定します。
(2) (1)の設定を削除します。
(3) NA 適用ポートに接続された端末から受信するパケットのうち、宛先 TCP ポート番号が 60100、VLAN ID が 100 のパケットをリレー対象パケットとして設定します。
(4) (3)の設定を削除します。

```
> enable
# configure terminal
(config)# na custom-relay-port tcp 60001
(config)# no na custom-relay-port tcp 60001
(config)# na custom-relay-port tcp 60100 vid 100
(config)# no na custom-relay-port tcp 60100 vid 100
```

関連コマンド

show na configuration, show running-config

注意事項

設定可能な数は、custom-relay-port ip、custom-relay-port tcp、custom-relay-port udp 合わせて 8 個までです。

リレー対象パケットの中継処理は CPU 処理となるため、CPU 負荷増を極力抑える必要があり、VLAN ID 設定によるリレー対象パケットを限定することを推奨致します。

3.46.39 na custom-relay-port udp

NA 適用ポートに接続された端末から受信するリレー対象パケットの宛先 UDP ポート番号、VLAN ID を指定します。設定を削除する場合は、no コマンドを使用してください。一つのコマンドで対象条件を複数指定した場合は、条件をすべて満たしたパケットがリレーされます。リレー先ポートは"na custom-relay-port port"で設定します。リレー先ポートが設定されていない場合、本コマンドで指定した対象パケットを受信してもパケットのリレーは行われません。

コマンドシンタックス

```
[ no ] na custom-relay-port udp <UDP PORT> [ vid <VID> ]
      UDP PORT            リレーする宛先 UDP ポート番号 <1-65535>
      VID                 リレー対象パケットの VLAN ID <1-4094>
```

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) NA 適用ポートに接続された端末から受信するパケットのうち、宛先 UDP ポート番号が 60001 の TCP パケットをリレー対象パケットとして設定します。
(2) (1)の設定を削除します。
(3) NA 適用ポートに接続された端末から受信するパケットのうち、宛先 UDP ポート番号が 60100、VLAN ID が 100 のパケットをリレー対象パケットとして設定します。
(4) (3)の設定を削除します。

```
> enable
# configure terminal
(config)# na custom-relay-port udp 60001
(config)# no na custom-relay-port udp 60001
(config)# na custom-relay-port udp 60100 vid 100
(config)# no na custom-relay-port udp 60100 vid 100
```

関連コマンド

show na configuration, show running-config

注意事項

設定可能な数は、custom-relay-port ip、custom-relay-port tcp、custom-relay-port udp 合わせて 8 個までです。

リレー対象パケットの中継処理は CPU 処理となるため、CPU 負荷増を極力抑える必要があり、VLAN ID 設定によるリレー対象パケットを限定することを推奨致します。

3.46.40 na auth-page redirect

認証ページリダイレクト機能を有効にします。無効にする場合は、no コマンドを使用してください。

本機能は、未認証端末から送信される HTTP リクエスト(宛先 IP アドレスは任意)を認識し、強制的に認証 Web ページを表示する機能です。

本機能は HTTP/HTTPS プロトコルを選択でき、HTTP プロトコルを使用する場合は、宛先ポート番号が 80、HTTPS プロトコルを使用する場合は、宛先ポート番号が 443 の HTTP リクエストがリダイレクトの対象となります。

本機能の対象となるポートモード、及び認証方法は以下となります。

- shared mode user-base
- shared mode user/mac-base
- shared-dynamic-vlan mode user-base
- shared-dynamic-vlan mode user/mac-base
- shared-dynamic-vlan mode dual-mac-user-base

コマンドシンタックス

[no] na auth-page redirect http | https

http	HTTP プロトコル
https	HTTPS プロトコル

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) HTTP プロトコルを選択します。
(2) 設定を無効にします。

```
> enable
# configure terminal
(config)# na auth-page redirect http
(config)# no na auth-page redirect http
```

関連コマンド
show na configuration, show running-config

注意事項

本機能を有効にする場合、"na httpd ip"コマンドで、任意の IP アドレスをあらかじめ設定しておく必要があります。

本機能を使用して認証を行った場合、表示される認証結果画面からのログアウトはできません。認証画面からログアウトする場合は、再度"na httpd ip"コマンドで設定した認証ページを表示させ、ログアウトしてください。

"na auth-page redirect https"の設定をする場合、"na httpd ssl enable"コマンドの設定は必要ありません。

"na httpd ssl enable"コマンド設定時でも、"na auth-page redirect http"によってリダイレクトされた場合は、SSL で認証を行いません。

"na httpd ssl enable"コマンド未設定時でも、"na auth-page redirect https"によってリダイレクトされた場合は、SSL で認証を行います。

認証端末のゲートウェイ(ネクストホップ)アドレスを認証装置の IP アドレスに設定した状態では使用できません。

本機能の対象となるポートモード、及び認証方法は以下となります。以下を除いて、使用しないでください。
- **shared mode user-base**
- **shared mode user/mac-base**
- **shared-dynamic-vlan mode user-base**

- **shared-dynamic-vlan mode user/mac-base**
- **shared-dynamic-vlan mode dual-mac-user-base**

shared-dynamic-vlan mode dual-mac-user-base の場合は、"na auth-page redirect vid"コマンドの設定が必要です。

本コマンドと"na httpd url"コマンドとの併用はできません。

本コマンドが有効な場合は、shared mode dual-mac-user-base の設定はできません。

本コマンドと"na httpd name radius"コマンド(RADIUS サーバー選択機能)との併用はできません。

3.46.41 na auth-page redirect proxy-port

認証ページリダイレクトプロキシー機能を有効にします。無効にする場合は、no コマンドを使用してください。

本機能は、認証端末が指定したポートのプロキシーを経由して任意の Web ページを参照したとき、強制的に認証 Web ページを表示させる機能です。

本機能の対象となるポートモード、及び認証方法は以下となります。

- shared mode user-base
- shared mode user/mac-base
- shared-dynamic-vlan mode user-base
- shared-dynamic-vlan mode user/mac-base
- shared-dynamic-vlan mode dual-mac-user-base

コマンドシンタックス

```
na auth-page redirect proxy-port <PORT>
no na auth-page redirect proxy-port
      PORT                ポート番号 <1-65535>
```

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) 本機能を有効にします。

(2) 本機能の設定を無効にします。

```
> enable
# configure terminal
(config)# na auth-page redirect proxy-port 1080
(config)# no na auth-page redirect proxy-port
```

関連コマンド

show na configuration, show running-config

注意事項

認証端末が HTTPS プロトコルを使用した場合、リダイレクトはされません。

本機能を有効にする場合、"na httpd ip"コマンドで、任意の IP アドレスをあらかじめ設定しておく必要があります。

本機能を使用して認証を行った場合、表示される認証結果画面からのログアウトはできません。認証画面からログアウトする場合は、再度"na httpd ip"コマンドで設定した認証ページを表示させ、ログアウトしてください。

認証端末のゲートウェイ(ネクストホップ)アドレスを認証装置の IP アドレスに設定した状態では使用できません。

本機能の対象となるポートモード、及び認証方法は以下となります。以下を除いて、使用しないでください。

- **shared mode user-base**
- **shared mode user/mac-base**
- **shared-dynamic-vlan mode user-base**
- **shared-dynamic-vlan mode user/mac-base**
- **shared-dynamic-vlan mode dual-mac-user-base**

shared-dynamic-vlan mode dual-mac-user-base の場合は、"na auth-page redirect vid"コマンドの設定が必要です。

本コマンドと"na httpd url"コマンドとの併用はできません。

本コマンドが有効な場合は、shared mode dual-mac-user-base の設定はできません。

本コマンドと"na httpd name radius"コマンド(RADIUS サーバー選択機能)との併用はできません。

3.46.42 na auth-page redirect vid

認証ページリダイレクト VLAN 指定機能を有効にします。設定を無効にする場合は、no コマンドを使用してください。

本機能は、認証ページリダイレクトを行う対象として、所属ポートの VLAN ID を指定し、強制的に認証 Web ページを表示する機能です。

未認証端末が本コマンドで指定したVLAN IDのshared-dynamic-vlan mode dual-mac-user-baseのポートで、"na auth-page redirect"コマンド、または"na auth-page redirect proxy-port"コマンドで指定したプロトコルで任意のURLを参照したとき、強制的に認証Webページを表示します。

コマンドシンタックス

```
na auth-page redirect vid <VID>
no na auth-page redirect vid
     VID                VLAN ID <1-4094>
```

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) 認証ページリダイレクトを行うVLAN IDを指定します。
(2) 設定を無効にします。

```
> enable
# configure terminal
(config)# na auth-page redirect vid 100
(config)# no na auth-page redirect vid
```

関連コマンド

show na configuration, show running-config

注意事項

本機能はshared-dynamic-vlan mode dual-mac-user-baseでのみ有効です。また、事前に"na auth-page redirect"コマンド、もしくは"na auth-page redirect proxy-port"コマンドでリダイレクトを行う対象プロトコルを設定する必要があります。

本機能を有効にする場合、"na httpd ip"コマンドで、任意のIPアドレスをあらかじめ設定しておく必要があります。

本コマンドが有効な場合は、shared mode dual-mac-user-baseの設定はできません。

本コマンドと"na httpd name radius"コマンド(RADIUS サーバー選択機能)との併用はできません。

3.46.43 na auth-page redirect url

認証Webページのリダイレクト先外部URLを指定します。設定を削除する場合は、noコマンドを使用

してください。
　本機能は、"na auth-page redirect"コマンドで指定したプロトコルで任意の URL を参照したとき、強制的に指定した外部の認証 Web ページを表示する機能です。

コマンドシンタックス

na auth-page redirect url <URL>
no na auth-page redirect url
　　URL　　リダイレクト先の URL <1-255(文字)>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リダイレクト先 URL を設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# na auth-page redirect url http://192.168.1.1:8080/
(config)# no na auth-page redirect url
```

関連コマンド

show na configuration, show running-config

注意事項

本機能を有効にする場合、"na httpd ip"コマンドで、任意の IP アドレスをあらかじめ設定しておく必要があります。

本機能を有効にする場合、事前に"na auth-page redirect"コマンドでリダイレクトを行う対象プロトコルを設定する必要があります。

"na auth-page redirect http"コマンドの設定がある場合、指定 URL のポート番号を 80 に設定すると、未認証端末-Web サーバー間で大量の TCP パケットが流れる場合があります。その場合、URL のポート番号を 80 以外に変更してください。

本機能と"na auth-page redirect proxy-port"コマンドは同時に設定できません。

本機能を有効にするには、3.28 パケットフィルター2 を利用して、未認証端末から設定した URL 宛の HTTP パケットをリダイレクトさせる必要があります。
<設定例>

```
packet-filter2
```

```
1 1 assign port 13-24
1 1 condition ipv4 dst ip 192.168.1.1/32
1 1 condition ipv4 dst tcp/udp 8080
1 1 action permit
1 1 action redirect 11
```

設定	内容
condition dst ip	リダイレクト先 IP アドレスを指定
condition dst tcp/udp	リダイレクト先ポート番号を指定

本コマンドが有効な場合は、shared mode dual-mac-user-base の設定はできません。

本コマンドと"na httpd name radius"コマンド(RADIUS サーバー選択機能)との併用はできません。

3.46.44 na success-url

認証成功後に表示する Web ページのリダイレクト先外部 URL を指定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

na success-url <URL>
no na success-url
URL　　リダイレクト先の URL <最大 255 文字>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) リダイレクト先外部 URL を指定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# na success-url http://192.168.1.1/
(config)# no na success-url
```

関連コマンド

show na configuration, show running-config

注意事項

3.46.45 na success-url timeout

認証成功の Web ページが表示されてから、"na success-url"コマンドで設定した URL に移動するまでの時間を設定します。設定を削除する場合は、no コマンドを使用しください。

コマンドシンタックス

na success-url timeout <SECONDS>
no na success-url timeout
SECONDS 移動時間 <0-60(秒)>

デフォルト

0(秒)

コマンドモード

CONFIG

使用例

(1) 移動時間を 10 秒に設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# na success-url timeout 10
(config)# no na success-url timeout
```

関連コマンド

show na configuration, show running-config

注意事項

3.46.46 copy tftp local-db

TFTP サーバー上の NA ユーザー、パスワードのデータをローカルデータベースに保存します。
ローカルデータベースのフォーマットを表 3-44、その登録例を表 3-45 に示します。

コマンドシンタックス

copy tftp <IPADDR> <FILE> local-db
IPADDR TFTP サーバーの IP アドレス
FILE データベースファイル名

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) IP アドレス：172.17.20.1 の TFTP サーバー上から NA ユーザー、パスワードのデータをローカルデータベースに保存します。

```
# copy tftp 172.17.20.1 local1 local-db
```

関連コマンド

注意事項

ローカルデータベースのファイルにおいて、改行のみの行がある場合、ダウンロードできません。ローカルデータベースのファイル中に改行のみの行を含めないでください。

表 3-44 ローカルデータベースフォーマット

項目	内容
形式	userid,password[,vid]の CSV 形式(userid、password は最大 63 文字)
最大登録行数	300 行

表 3-45 ローカルデータベースの登録例

```
temp01,temp01,10
temp02,temp02
temp03,temp03,30
00096b82c51e,1q2w3d,100
```

MAC ベース認証の場合、MAC アドレス(16 進文字列、区切り文字無しの 16 文字)を、userid として登録してください。なお、アルファベットは小文字(a-f)で記述する必要があります。

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

ローカルデータベースに使用できる改行コードは LF、または CR+LF です。CR は使用できません。

3.46.47 copy local-db tftp

ローカルデータベースに保存されていた NA ユーザー、パスワードのデータを TFTP サーバー上のファイルに保存します。

コマンドシンタックス

copy local-db tftp <IPADDR> <FILE>

IPADDR	TFTP サーバーの IP アドレス
FILE	データベースファイル名

デフォルト
なし(＝設定なし)

コマンドモード
ENABLE

使用例
(1) ローカルデータベースに保存されている NA ユーザー、パスワードを IP アドレス：172.17.20.1 の TFTP サーバー上に userdate.txt として保存します。

```
# copy local-db tftp 172.17.20.1 userdate.txt
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

3.46.48 erase local-db

ローカルデータベースに保存されていた NA ユーザー、パスワードのデータを削除します。

コマンドシンタックス
erase local-db

デフォルト
なし(＝設定なし)

コマンドモード
ENABLE

使用例
(1) ローカルデータベースに保存されている NA ユーザー、パスワードを削除します。

```
# erase local-db
```

関連コマンド

注意事項

3.46.49 show na aging

認証済み端末の無通信時間を表示します。無通信時間は、本装置と認証済み端末間で通信がない場合にカウントされます。

無通信時間のカウントは、本装置と認証済み端末間の通信が終了してから、最大 2 × ポート総数(秒)で開始されます。必ずしも通信終了後に、即座にカウントが開始するわけではないことに注意してください。

カウント開始後、無通信時間が"na logout aging"コマンドで設定したエージング時間経つと、認証端末は自動的にログアウトされます。

コマンドシンタックス

show na aging

コマンドモード

ENABLE

使用例

(1) 認証済み端末の無通信時間を表示します。

```
# show na aging
 MAC address        port  VID      Time    Aging user
 00:16:d3:3e:35:63    1   100   0:01:31  0:00:13 webuser01
```

MAC address　：MAC アドレス
port　：ポート番号
VID　：VID
Time　：ログインしてからの時間
Aging　：無通信時間
user　：認証を行ったユーザー名

関連コマンド

na logout aging, show running-config

注意事項

無通信時間のカウントが始まる前に"show na aging"を行った場合、Aging(無通信時間)は 00:00:00 と表示されます。

3.46.50 show na configuration

NA に関する構成情報を表示します。

コマンドシンタックス

show na configuration

コマンドモード

VIEW, ENABLE

使用例

(1) NA の詳細な状態を表示します。

```
> show na configuration
Network Authentication Configuration:
     NA Status                : enable
     NA Roaming               : enable
     NA WEB Server IP         : 192.0.2.1
     NA WEB Server Port       : 8080
     NA WEB Server Page 1     : http://192.168.1.100
     NA WEB Server Page 2     :
     NA WEB English           : enable
     NA WEB Server SSL        : disable
     NA Success URL           : http://success-url/
     NA Success URL Timeout   : 60
     NA disc-mac-del interval : 300

RADIUS Server Configuration:
     [WEB Authentication(WEB Server Name: www.auth1.ne.jp)]
     Primary Radius Server
         IP Address           : 172.21.41.10
         Port Number          : 1812
         Encrypted Secret Key : nmld7xDA+F1+Qigidz
     Secondary Radius Server
         IP Address           : 172.21.41.11
         Port Number          : 1812
         Encrypted Secret Key : osHgs+soiIkmg+zZmwD

     [WEB Authentication(WEB Server Name: www.auth2.ne.jp)]
     Primary Radius Server
         IP Address           : 172.21.51.10
         Port Number          : 1645
         Encrypted Secret Key : nmld7xDA+F1+Qigidz
     Secondary Radius Server
         IP Address           : 0.0.0.0
         Port Number          : 1812
         Encrypted Secret Key :

(中略)
     [MAC Address Authentication(mac-base, dual-mac-user-base)]
     Primary
         IP Address           : 172.21.41.10
         Port Number          : 1812
         Encrypted Secret Key : nmld7xDA+F1+Qigidz
     Secondary
```

```
        IP Address           : 172.21.41.11
        Port Number          : 1812
        Encrypted Secret Key : osHgs+soiIkmg+zZmwD

Logout Configuration:
     logout ping dest IP      : 0.0.0.0
     logout ping TTL          : 0
     logout polling interval  : 0
     logout polling count     : 0
     logout timeout           : 0
     logout aging             : 0
     logout clock             : 12:00
                                17:15
                                20:20

HTTP Redirect Configuration:
     HTTP Port                : 80
     HTTPS Port               :
     Proxy Port               :
     URL                      :
     VID                      :

(中略)

Arp Relay Configuration:
     [VID] 41
     [VID] 51

Custom Relay Configuration:
     [TCP] 60001
     [IP] 172.17.41.5 [UDP] 60001 [VID] 41
     [IP] 172.17.41.5 [TCP] 60002 [VID] 51
     [IP] 172.17.41.10
     [IP] 172.17.41.10 [UDP] 60002

Filter Configuration:
     filter1 permit-ttl       : 1
     filter2 permit-ttl       : 128
     filter3 permit-ttl       : 255

Port Configuration:
  d=designated mode,       s=shared mode        S=shared-dynamic-vlan mode
  f=force-authorized,  l=local-authorized
r=relay port
 Port   :
```

```
        : 1    6 7   12 13  18 19  24 25
        : +----+ +----+ +----+ +----+ +-
 mode   : dddddd ...... ...... ...... ..
 usr    : ...... ...... ...... ...... ..
 mac    : oooooo ...... ...... ...... ..
 dual   : ...... ...... ...... ...... ..
 auth   : ll.... f..... ...... ...... ..
 arp    : ...... ...... ...... ...... ..
 dhcp   : ...... ...... ...... ...... ..
 custom : ...... ...... ...... ...... ..
 filter1: ..oo.. ...... ...... ...... ..
 filter2: o..... ...... ...... ...... ..
 filter3: .o.... ...... ...... ...... ..
```

NA Status　：NA の動作状態
NA Roaming　：認証端末のローミングの状態
NA WEB Server IP　：認証 Web サーバーの IP アドレス
NA WEB Server Port　：認証 Web サーバーの TCP ポート番号
NA WEB Page 1　：認証 Web ページに表示する外部の URL
NA WEB Page 2　：認証 Web ページに表示する外部の URL
NA WEB English　：認証 Web ページの英語表示
NA WEB Server SSL　：認証 Web ページの SSL(Secure Socket Layer)機能
NA Success URL
NA Success URL Timeout
NA disc-mac-del interval　：FDB の discard MAC アドレスの登録時間

WEB Server Name　：認証 Web サーバー名
IP Address　：RADIUS サーバーの IP アドレス
Port Number　：RADIUS サーバーの UDP ポート番号
Encrypted Secret Key　：RADIUS サーバーの secret key

logout ping dest IP　：logout ping の宛先 IP アドレス
logout ping TTL　：logout ping の TTL
logout polling interval　：ポーリング間隔
logout polling count　：未認証状態になるまでのポーリングの失敗回数
logout timeout　：ログアウトするまでのタイムアウト時間
logout interval　：未認証状態になるまでのタイムアウト時間
logout aging　：エージング間隔
logout clock　：未認証状態になるログアウト時刻

filter N　：指定された値のパケットのみ認証を行うポート
(N はエントリー数：最大 8 個)

HTTP Port
HTTPS Port
Proxy Port

URL
VID

mode　　：ポートのモード(shared/designate)
usr　　：ユーザーベース認証が有効になっているポート
mac　　：MAC ベース認証が有効になっているポート
dual　　：デュアルベース認証が有効になっているポート
auth　　：強制認証、ローカル認証が有効になっているポート
arp　　：ARP リレー先のポート
dhcp　　：DHCP リレー先のポート
custom　　：CUSTOM リレー先のポート

関連コマンド

注意事項

3.46.51 show na local-db

ローカルデータベースに保存されている内容を表示します。

コマンドシンタックス

show na local-db

コマンドモード

ENABLE

使用例

(1) ローカルデータベースに保存されている内容を表示します。

```
# show na local-db
-----------------------------------------
No. Username                        VID
-----------------------------------------
1   user1                           0
2   user2                           0
-----------------------------------------
```

関連コマンド

注意事項

3.46.52 show na client

認証済みの端末の状態を表示します。

コマンドシンタックス

show na client

コマンドモード

VIEW, ENABLE

使用例

(1) 認証済みの端末の状態を表示します。

```
> show na client
  MAC address         port  VID       Time  count             user
  00:40:26:4f:00:f1      6   33   00:00:04      0            admin
```

MAC address　：MAC アドレス
port　：ポート番号
VID　：VLAN ID
Time　：ログインしてからの時間
count　：ポーリングの失敗回数
user　：認証を行ったユーザー名

関連コマンド

注意事項

3.46.53 show tech-support na

NA 機能の各種情報を収集し表示します。本コマンドで表示する内容は、表 3-46 に示すコマンドが収集している情報です。system-dump オプションを指定した場合、装置内部のダンプ情報(独自形式で表示)を含めて取得し表示します。

表 3-46 コマンドにより収集可能な NA 情報

show system
show version
show na configuration
show na client
show na aging
show na local-db

コマンドシンタックス

show tech-support na [system-dump]
　system-dump　　装置内部のダンプ情報を出力

コマンドモード

ENABLE

関連コマンド

注意事項

system-dump オプションを指定した場合、装置の性能、及び通信に対して影響を及ぼす可能性があります。使用する場合には、必ず事前にサポート対応窓口へご相談のうえ、指示に従ってください。

3.46.54 RADIUS サーバー設定例

Cistron RADIUS server version 1.6.6 (http://www.radius.cistron.nl)を使用する場合の設定ファイルの例を示します。

dictionary ファイル
dictionary ファイルに以下の設定を追加してください。
Vlan-Id を Vendor-Specific でカプセル化する場合：

```
VENDOR          Hitachi-Cable-Ltd       278
ATTRIBUTE       NA-Vlan-Id              192     integer Hitachi-Cable-Ltd
```

Vlan-Id を Vendor-Specific でカプセル化しない場合：

```
ATTRIBUTE       Vlan-Id                 192     integer
```

user ファイル
ユーザー名：v33、パスワード：v33pass、VLAN ID：33 のユーザーを追加する場合、user ファイルに以下の設定を追加してください。

```
v33     Auth-Type = Local, Password = "v33pass"
        NA-Vlan-Id = 33
```

MAC ベース認証(MAC 認証パスワード："macpass")を使用し、MAC アドレスが 00:01:02:03:0a:0b である端末を認証する場合、user ファイルに以下の設定を追加してください。

```
000102030a0b    Auth-Type = Local, Password = "macpass"
```

3.47 AccessDefender

AccessDefender は、ライセンス不要のユーザー認証機能です。ユーザー名、パスワード、MAC アドレスなどによってネットワークに接続可能なユーザーを制限します。パケットフィルター2 と連動して動作することにより、より高速で柔軟性の高いネットワークを構成できます。

AccessDefender では、SSLv2、SSLv3、TLS1.0、TLS1.1、TLS1.2 に対応しています。

注意事項

AccessDefender 認証ポートで OSPF、RIP、3.17 スパニングツリープロトコル(STP/RSTP/MSTP)は併用できません。

AccessDefender 認証ポートで 3.27 ポートセキュリティー、3.41 MMRP、3.43 MMRP2 aware、3.42 MMRP-Plus は併用できません。

MAC 認証ポートで VRRP を併用する場合、VRRP パケットの仮想 MAC アドレスを認証させてください。

認証端末の所属する VLAN に IP アドレスを設定して使用する場合、認証状態を問わず、端末から本装置への通信(TELNET/SSH や SNMP)が可能です。通信を制限したい場合は、TELNET/SSH、及び SNMP のアクセス制限機能により、アクセス可能な端末を制限してください。

DHCP リレーが設定されている場合、端末の認証有無の状態にかかわらず、DHCP リレーが動作し、IP の取得が可能です。

AccessDefender 機能による認証ポートにリンクアグリゲーション、ポートリダンダントを設定する場合は、対象ポートの認証方法をすべて同一にし、あわせてリンクダウンログアウト無効("logout linkdown port disable")とローミング("roaming port enable")を設定してください。

認証成功後にその認証ポートを他の認証モードに変更した場合、変更前の認証モードが有効のままとなります。認証モードを変更する場合は、認証端末がログアウト後に再認証するか、認証中の端末に対し再認証をしてください。

3.12 LLDP 機能による論理リンクダウン検知時は、認証端末はログアウトしますが、LACP 機能による論理リンクダウン検知時は、認証端末はログアウトしません。

OSPF/RIP/IGMP/スパニングツリープロトコル(STP/RSTP/MSTP)等のプロトコル制御用マルチキャストフレームは MAC 認証の対象となります(これらフレームを送出する機器の MAC アドレスは、Discard 登録対象となります)。

IEEE802.1X 認証は、Supplicant から受信する EAPOL フレームの宛先 MAC アドレスが以下いずれか条件の場合のみ、STP との併用が可能です。
(1) IEEE802.1X 認証用で使用される固有 MAC アドレス(00:40:66:33:1D:A9)
(2) 装置の自局 MAC アドレスの場合

複数認証モード(MAC 認証、Web 認証、802.1X)を組み合わせて認証する際、ログイン済み端末と MAC アドレスが重複した場合は新たな認証要求は失敗します。

ログアウトせずに認証済み端末の接続ポートを変更する場合、ローミング機能("roaming port enable")を使用してください。

認証ポートにスイッチングハブを接続し Web 認証(動的 VLAN 割り当て)を利用する場合、認証ポートのローミング機能("roaming port enable")を有効にしてください。

認証済み端末数が最大認証数に達した状態でも、端末の Web 画面上に認証成功と表示される場合があります。
-具体例-
最大認証数 1024 に対して、1021 端末が認証済みの状態で 5 端末が同時認証

トランクポートへ、タグ VLAN として設定された VLAN ID に動的 VLAN 割り当てによる認証端末が存在する場合、その VLAN ID はアクセスポートとして動作します(タグ中継されません)。

同一ポートにおいて複数端末/複数 VLAN を動的に割り当てる場合、認証済み端末の IP アドレスを認証済み別セグメントに設定すると不要な ARP フレームが転送されることがあります。
パケットフィルター2 機能(表 3-24)の arp-sender-ip を設定することにより、不要なフレームの転送を防止することができます。

動的な VLAN 割り当てによる収容端末数は以下の通りです。
なお、実装上の仕様により、以下に満たない場合でも登録できないことがあります。
- Apresia4328：128
- Apresia3400/4348/5400/13000 シリーズ：256

AccessDefender 設定時に、MLD 機能、MMRP/MMRP-Plus/MMRP2 aware(いずれか 1 つ)機能の 3 機能を同時に併用できません。

MAC 認証と動的な VLAN 割り当て使用時に暫定 VLAN 上に 3.40 DHCP サーバーがある場合、"mac-authentication ignore-dhcp"の設定が必要です。

Web/MAC 認証(AND)で行われる MAC 認証に対する動的な VLAN 変更の指定は無効となり

ます。

認証成功後にその認証ポートの認証モードを変更しても、変更前の認証成功端末の通信設定は変わりません。
変更した認証モードを認証端末へ反映させる場合には、認証成功端末がログアウトした後に再認証するか、認証成功端末に対し再認証をしてください。

3.36 IGMP Snooping、3.39 MLD Snooping が設定されている場合、query/report メッセージを送信する機器の認証有無の状態にかかわらず、query メッセージを受信したポートはルーターポートに設定され、report メッセージを送信した機器はメンバーに登録されます。ただし、未認証端末からのマルチキャストは中継されません。

3.28 パケットフィルター2 機能併用時に、AccessDefender よりも小さいグループ番号でパケットフィルター2 機能を設定する場合、未認証端末からのパケットが action permit によって意図せず中継されないように、action none を設定してください。

DHCP Snooping 有効時に、パケットフィルター2 機能を AccessDefender よりも小さいグループ番号で設定する場合、DHCP パケットが action permit の対象とならないように、action none を設定してください。

"mac-authentication port"コマンドを設定しているポートで VRRP を併用する場合、VRRP パケットの仮想 MAC アドレスを認証させてください。

AccessDefender 認証ポートを VRRP の VLAN インターフェースとして設定している状態で、仮想 MAC アドレスを、動的 VLAN を利用して MAC 認証する場合は、VRRP の VLAN インターフェース以外を指定してください。

3.47.1 access-defender

ACCESSDEFENDER モードへ移行します。ACCESSDEFENDER モードから CONFIG モードへ移行する場合は exit コマンド、ENABLE モードへ移行する場合は end コマンドを使用してください。

コマンドシンタックス
access-defender

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) ACCESSDEFENDER モードに移行します。

```
> enable
# configure terminal
(config)# access-defender
```

関連コマンド

show running-config

注意事項

3.47.2 aaa authentication

RADIUS サーバー、ローカル/強制認証の設定を行います。設定を削除する場合は、no コマンドを使用してください。

Web 認証では、<ID>ごとに認証方法を指定することにより、ユーザーがブラウザー上で認証方法(<ID>)を選択することが可能です。"no aaa authentication web"コマンドでは、"aaa authentication web <ID>"設定を削除できません。"aaa authentication web <ID>"設定を削除する場合は、"no aaa authentication web <ID>"コマンドを使用してください。

コマンドシンタックス

aaa authentication (web [<ID>]) | mac radius <INDEX1> [<INDEX2>] [local | (force [vlan <VID>])]

aaa authentication (web [<ID>]) | mac local [radius <INDEX1> [<INDEX2>] [force [vlan <VID>]]

aaa authentication (web [<ID>]) | mac | dot1x force [vlan <VID>]

aaa authentication dot1x radius <INDEX1> [<INDEX2>] [force [vlan <VID>]]

no aaa authentication (web [<ID>]) | mac | dot1x

ID	認証 ID <1-4>
INDEX1	プライマリーRADIUS サーバーのインデックス <1-8>
INDEX2	セカンダリーRADIUS サーバーのインデックス <1-8>

- no aaa authentication web | mac | dot1x コマンドを実行すると、Web 認証/MAC 認証/IEEE802.1X 認証を解除します。

デフォルト

なし

コマンドモード

CONFIG

使用例

(1) Web 認証 ID：1 の RADIUS サーバーにインデックス：1 を指定します。
(2) MAC 認証の RADIUS サーバーにインデックス：2 を指定します。
(3) Web 認証 ID：1 の RADIUS サーバー指定を削除します。
(4) MAC 認証の RADIUS サーバー指定を削除します。

```
> enable
```

```
# configure terminal
(config)# aaa authentication web 1 radius 1
(config)# aaa authentication mac radius 2
(config)# no aaa authentication web 1
(config)# no aaa authentication mac
```

関連コマンド

show running-config

注意事項

強制認証はセキュリティー上の問題となる可能性がありますので、十分検討の上使用してください。設定されていない INDEX を指定した場合は、ERROR 通知を行い設定はされません。

IEEE802.1X 認証の RADIUS サーバー冗長構成では、"aaa radius deadtime"を設定してください。

3.47.3 aaa authentication control

認証順序・移行条件変更機能を有効にします。無効にする場合は、no コマンドを使用してください。本機能を有効にすると複数の認証(プライマリー/セカンダリーRADIUS サーバー、ローカル、強制)が設定されている場合、いずれか 1 つの認証に成功すれば認証成功になります。

コマンドシンタックス

```
[ no ] aaa authentication ( web [ <ID> ] ) | mac control sufficient
      ID                    認証 ID <1-4>
```

デフォルト

なし

コマンドモード

CONFIG

使用例

(1) Web 認証の認証順序・移行条件変更機能を有効にします。
(2) Web 認証の認証順序・移行条件変更機能を無効にします。

```
> enable
# configure terminal
(config)# aaa authentication web control sufficient
(config)# no aaa authentication web control sufficient
```

関連コマンド

show running-config

注意事項

認証方法として RADIUS サーバーと強制認証を選択している場合、RADIUS サーバーでのユーザー名、またはパスワード誤りによる認証失敗時は強制認証へ移行しません。RADIUS サーバーがタイムアウトした際は強制認証へ移行します。

3.47.4 aaa radius host

認証に使用する RADIUS サーバーに関する設定を行います。設定を削除する場合は、no コマンドを使用してください。

RADIUS サーバーに関する設定は、インデックス番号ごとに行い、最大 8 個設定できます。設定項目は、RADIUS サーバーの IP アドレス、認証 UDP ポート番号、タイムアウト時間、リトライ回数、secret key の 5 項目です。AccessDefender で RADIUS 認証を有効にするには、最低限、RADIUS サーバーの IP アドレス、secret key を設定する必要があります。

タイムアウト時間は RADIUS サーバーにリクエストを送信し応答がない場合に再試行を試みる間隔、リトライ回数は RADIUS サーバーとの通信を試行する回数を示します。RADIUS サーバーと通信不可の場合に、通信不可と判断するまでのタイムアウト時間は「リトライ回数 × タイムアウト時間」となります。

コマンドシンタックス

aaa radius <INDEX> host <IPADDR> [auth-port <PORT>] [timeout <SEC>] [retransmit <RETRIES>] [key <KEY>]

no aaa radius <INDEX>

INDEX	インデックス番号 <1-8>
IPADDR	RADIUS サーバーの IP アドレス
PORT	認証 UDP ポート番号 <1-65535>
SEC	タイムアウト時間 <1-30(秒)>
RETRIES	リトライ回数 <1-5(回)>
KEY	secret key <1-127(文字)>

デフォルト

INDEX ：なし
IPADDR ：なし
PORT ：1812
SEC ：3(秒)
RETRIES：3(回)
KEY ：なし

コマンドモード

CONFIG

使用例

(1) インデックス番号：1 に、RADIUS サーバーの IP アドレスを 172.21.29.40、認証 UDP ポート番号を 10、タイムアウト時間：10 秒、リトライ回数：4 回、secret key を ac-df に設定します。

(2) インデックス：1 の RADIUS サーバーの設定を削除します。

```
> enable
# configure terminal
(config)# aaa radius 1 host 172.21.29.40 auth-port 10 timeout 10 retransmit 4 key
ac-df
(config)# no aaa radius 1
```

関連コマンド

show running-config

注意事項

secret key に使用できる文字は、ASCII コードの印字可能な文字です。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

設定した secret key は、"show running-config"コマンド、"show flash-config"コマンドにおいては暗号化されて表示されます。

3.47.5 aaa radius client-ip

RADIUS サーバーへ送信するパケットの送信元 IP アドレス/IPv6 アドレス、及び RADIUS 属性の NAS-IP-Address を設定します。設定を削除する場合は、no コマンドを使用してください。

本コマンド設定と装置への IP アドレス設定の有無に応じて、実際に使用するアドレスについて、表 3-47、表 3-48 に示します。

表 3-47 "aaa radius client-ip"コマンド設定に対して使用する送信元 IP アドレス

設定条件		送信元 IP アドレス
"aaa radius client-ip" コマンド	装置において当該 IP 設定の有無	
設定なし	-	出力インターフェースの IP アドレス
設定あり	設定なし	出力インターフェースの IP アドレス
設定あり	設定あり	client-ip で設定した IP アドレス ※1、※2

※1 当該 IPv4 アドレスを設定したポートがダウンした場合、RADIUS サーバーからの応答パケットを受信できません。

※2 当該 IPv6 アドレスを設定したポートがダウンした場合、出力インターフェースの IPv6 アドレスに変わります。

表 3-48 "aaa radius client-ip"コマンド設定に対して使用する NAS-IP-ADDRESS

設定条件		NAS-IP-ADDRESS
"aaa radius client-ip" コマンド	装置において当該 IP 設定の有無	
設定なし	-	出力インターフェースの IP アドレス

設定あり	設定なし	client-ip で設定した IP アドレス
設定あり	設定あり	client-ip で設定した IP アドレス ※1

※1 IPv6 アドレスを設定したポートがダウンした場合、出力インターフェースの IPv6 アドレスになります。IPv4 アドレスの場合は変わらず、本コマンドで設定した IP アドレスのままです。

コマンドシンタックス

aaa radius client-ip <IPADDR>
no aaa radius client-ip
IPADDR 送信元 IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) RADIUS サーバーへ送信するパケットの送信元 IP アドレスを 192.168.10.1 に設定します。

```
> enable
# configure terminal
(config)# aaa radius client-ip 192.168.10.1
```

関連コマンド

show running-config

注意事項

3.47.6 aaa radius deadtime

RADIUS サーバーの DeadTime を設定します。設定を削除する場合は、no コマンドを使用してください。
RADIUS サーバーへの問い合わせがタイムアウトすると、以降 Deadtime 間 RADIUS サーバーへの問い合わせを行いません。

コマンドシンタックス

aaa radius deadtime <MIN>
no aaa radius deadtime
MIN DeadTime <1-1440(分)>

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) DeadTime を 100 分に設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# aaa radius deadtime 100
(config)# no aaa radius deadtime
```

関連コマンド

show running-config

注意事項

3.47.7 web-authentication enable

Web 認証を有効にします。無効にする場合は、no コマンドを使用してください。

Web 認証は、認証時にユーザー名/パスワードにより認証を行う機能です。RADIUS サーバー(ローカル認証使用時はローカルデータベース)にユーザーごとに VLAN 情報を追加した場合、認証時にユーザーの属性に従って動的に VLAN を割り当てることが可能です。また、1 ポートで複数端末の認証が可能であり、認証端末ごとに VLAN を割り当てることも可能です。

また、パケットフィルター2 認証バイパス機能(authentication-bypass コマンド)を利用することにより、特定の端末のみ Web 認証を行わないで、通信を許可させることが可能です(詳細はパケットフィルター2 の 3.28.5 "action"の authentication-bypass の項を参照ください)。

Web 認証の特徴

(1) ユーザー名/パスワードによる認証
(2) 認証端末への動的な VLAN 割り当て
(3) 認証用 Web サーバー搭載(SSL 対応)
(4) 同一ポートでの MAC 認証/IEEE 802.1X/DHCP Snooping との併用
(5) プライマリー/セカンダリーの RADIUS サーバーの登録
(6) RADIUS サーバー無応答時のローカル認証、強制認証
(7) RADIUS サーバーを使用しないローカル認証、強制認証
(8) MAC アドレス/ユーザー名/パスワードによる認証(Web/MAC 認証(AND)："web-authentication port <PORT> mac-authentication"、及び"web-authentication mac-authentication-password"設定時)

コマンドシンタックス

[no] web-authentication enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) Web 認証を有効にします。

(2) Web 認証を無効にします。

```
> enable
# configure terminal
(config)# web-authentication enable
(config)# no web-authentication enable
```

関連コマンド

show running-config

注意事項

Web 認証で用いるユーザーID、パスワードは 63 文字まで入力可能ですが、使用する RADIUS サーバーの仕様に従い、定義する必要があります。

同一ポートで他の認証(MAC 認証/IEEE 802.1X)を併用して設定した場合は、他の認証ですでにログインが完了している時は、Web 認証は行われません。

ユーザーID とパスワードに使用できる文字は、ASCII コードの印字可能な文字です(日本語は使用できません)。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

本装置の DHCP サーバー機能を併用して、端末へ動的に VLAN を割り当てる場合、認証前 VLAN 用の DHCP サーバーと、認証後 VLAN 用の DHCP サーバーは同一装置内に設定しないでください。認証後 VLAN の IP アドレスに切り替わらないことがあります。

Web 認証ポートに認証バイパスが設定されている場合、認証バイパス対象パケットの中継に対して認証 Web ページを表示できません。

3.28 パケットフィルター2 の認証バイパスを AccessDefender よりも大きいグループ番号で設定すると AccessDefender の Web 認証、及び MAC 認証の discard 登録の設定が優先となり、認証バイパスは有効に動作しません。パケットフィルター2 の認証バイパス設定は、必ず AccessDefender のグループ番号より、小さい番号を設定してください。

Web 認証ポートでは、未認証端末からの ARP フレームは、遮断されません。DHCP Snooping ポートと併用している場合は、DHCP Snooping に登録されることで ARP フレームの中継が行われます。

Web 認証、ゲートウェイ認証において同一の IP アドレスでログインした場合、最後にログインした認証方法が有効になります。

認証端末が DHCP サーバーより、IP アドレスを取得して Web 認証を行う場合は、パケットフィルター2 を利用して、未認証端末から送信する DHCP フレームの通信を許可させる必要があります。

<設定例>

```
packet-filter2
 1 1 assign port 1-44
 1 1 condition ipv4 dst tcp/udp 67
 1 1 action permit
```

設定	内容
condition ipv4 dst tcp/udp 67	DHCP フレームを指定

3.47.8 web-authentication port

Web 認証を有効にするポートを指定します。無効にする場合は、no コマンドを使用してください。MAC 認証/IEEE 802.1X/DHCP Snooping を同一ポートで併用して指定することが可能です。MAC 認証/IEEE 802.1X で認証端末が認証成功した場合は、Web 認証は行うことはできません。

オプション mac-authentication を指定したポートは Web/MAC 認証(AND)の対象ポートとなります。Web/MAC 認証(AND)の対象ポートは Web 認証に先立ち、認証端末の MAC 認証を行います。"show access-defender port-configuration"では Web/MAC 認証(AND)ポートも Web 認証ポートとして表示されます。

オプション dot1x を指定したポートは Web/IEEE802.1X 認証(AND)の対象ポートとなります。無効にする場合は、no コマンドにオプション dot1x を指定してください。Web/IEEE802.1X 認証(AND)の対象ポートでは、Web 認証、及び IEEE802.1X 認証に成功した端末が通信可能となります。"show access-defender port-configuration"では Web/IEEE802.1X 認証(AND)ポートとして表示されます。また、同一ポートにオプション mac-authentication を指定することで、Web 認証の代わりに Web/MAC 認証(AND)となります。MAC 認証、Web 認証、及び IEEE802.1X 認証のすべてに成功した端末が通信可能となります。この場合、"show access-defender port-configuration"では、Web/IEEE802.1X 認証(AND)ポートとして表示されます。Web/IEEE802.1X 認証(AND)時、認証属性(VLAN など)は最後に認証された方の認証情報が設定されます(Web --> IEEE 802.1X の順番に認証が行われた場合は IEEE 802.1X の認証情報にて通信が可能となります)。

コマンドシンタックス

web-authentication port <PORTRANGE> [mac-authentication | gateway | dot1x]
no web-authentication port <PORTRANGE> [dot1x]

PORTRANGE	ポート番号(複数指定可能)
mac-authentication	Web/MAC 認証(AND)を指定
gateway	ゲートウェイ認証を指定
dot1x	Web/IEEE802.1X 認証(AND)を指定

デフォルト

なし(＝設定なし)

コマンドモード

使用例

(1) ポート：1～10 を Web 認証ポートに指定します。
(2) ポート：11～20 を Web/MAC 認証(AND)ポートに指定します。
(3) ポート：1～10 を Web 認証ポートから除外します。
(4) ポート：1～5 を Web/IEEE802.1X 認証(AND)ポートに設定します。
(5) ポート：6～10 を Web/MAC 認証(AND)、及び IEEE802.1X 認証の併用ポートに設定します(設定順不同)。
(6) ポート：1～10 を Web/IEEE802.1X 認証(AND)ポートから除外します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication port 1-10
(config-a-def)# web-authentication port 11-20 mac-authentication
(config-a-def)# no web-authentication port 1-10
(config-a-def)# web-authentication port 1-5 dot1x
(config-a-def)# web-authentication port 6-10 dot1x
(config-a-def)# web-authentication port 6-10 mac-authentication
(config-a-def)# no web-authentication port 1-10 dot1x
```

関連コマンド

show access-defender port-configuration, show running-config

注意事項

Web 認証ログイン中に、ログアウトせずに接続ポートを移動した場合は、Web 認証でのみ再ログインが可能です。

装置の認証 Web サーバーと認証端末間の通信は、装置のルーティングテーブルに従って行われます(装置を L2 として使用している場合には、デフォルトゲートウェイの設定に従う)。このため認証 Web サーバーと認証端末間の通信は、上位ルーターを経由して行われる場合があります。
(例)
装置を L2 として使用し、自局 IP アドレスと認証端末 IP アドレスが異なるサブネットとなる場合など、上位ルーターを経由することになります。

ゲートウェイ認証でログインした端末が、ログイン後に端末の IP アドレスを変更すると通信不可となります。

ゲートウェイ認証において、動的な VLAN 変更を指定しても無効となります(動的な VLAN 変更は行われません)。

ゲートウェイ認証と、Web 認証(gateway オプションなし)、Web/MAC 認証(AND)、MAC 認証、IEEE802.1X 認証、IEEE802.1X/MAC 認証(AND)、DHCP Snooping、ポートセキュリティーは同一ポートに設定できません。

ゲートウェイ認証は Apresia13000 シリーズでのみ有効です。

Web/IEEE802.1X 認証(AND)に設定されたポートが Web 認証ポート、IEEE802.1X 認証ポートに設定済みの場合、ログイン済みの Web 認証端末、IEEE802.1X 認証端末はログアウトされます。

Web/IEEE802.1X 認証(AND)を使用する場合、Web 認証の有効設定("web-authentication enable")と IEEE802.1X 認証の有効設定("dot1x enable")をする必要があります。

no コマンドにオプション dot1x を指定した場合、Web/IEEE802.1X 認証(AND)ポートの削除と Web/IEEE802.1X 認証(AND)ポートと同一ポートに設定された Web/MAC 認証(AND)ポートの削除が行われます(Web/IEEE802.1X 認証(AND)ポート以外の Web 認証ポート、Web/MAC 認証(AND)ポートを指定しても無視されます)。

Web/IEEE802.1X 認証(AND)ポートに設定されているポートに対して Web 認証ポートの設定("web-authentication port <PORT>")をしても無視されます。

Web/IEEE802.1X 認証(AND)ポートで IEEE 802.1X、または Web のみ認証済みの端末は無通信端末の扱いとなり、エージングログアウトの設定が有効の場合、設定時間が満了した時点でログアウトされます。

Web/IEEE802.1X 認証(AND)ポートで IEEE 802.1X、または Web のみ認証済みの端末は "vlan mode dynamic port-base"コマンドの制限対象外となります(上記端末のログイン状態でも別 VLAN 端末のログインが可能です)。

Web/IEEE802.1X 認証(AND)ポートを設定した状態で、装置を 7.29 以前にバージョンダウンすると、"web-authentication port dot1x"以下の Config が消えます。

<例>

```
# show running-config
 :
access-defender
 web-authentication port 2
 web-authentication port 1,4 mac-authentication
 web-authentication port 3 gateway
 web-authentication port 1 dot1x
 web-authentication ttl 255 port 1
```

```
 web-authentication redirect url aaa
 web-authentication redirect http
 web-authentication redirect https
 web-authentication snooping proxy-port 1
 web-authentication ip 192.0.2.1
 web-authentication http-port 81
 web-authentication mac-authentication-encrypted-password RMNZRS5k2Up+QigidzZmwA$$
 mac-authentication ignore-dhcp
 mac-authentication port 2
 mac-authentication encrypted-password qvk242hRVid+QigidzZmwA$$
 dot1x port 2
 dot1x port 1 reauthentication
 dot1x port 1 ignore-eapol-start
 dot1x port 1 timeout re-authperiod 2147483647
 dot1x port 1 timeout supp-timeout 65535
 dot1x port 1 timeout tx-period 65535
 dot1x port 1 timeout quiet-period 65535
 dot1x mac-authentication-encrypted-password 80N39xvwzL5+QigidzZmwA$$
!
 :

※ Version down 後
# show running-config
 :
access-defender
 web-authentication port 2
 web-authentication port 1,4 mac-authentication
 web-authentication port 3 gateway
!
```

3.47.9 web-authentication http-port

認証 Web サーバーとして使用する HTTP プロトコルの TCP ポート番号を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

web-authentication http-port <HTTP-PORT>
no web-authentication http-port

HTTP-PORT	認証 Web サーバーの TCP ポート番号

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) TCP ポート番号を 8080 に設定します。

(2) TCP ポート番号を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication http-port 8080
(config-a-def)# no web-authentication http-port
```

関連コマンド

show running-config

注意事項

認証 Web サーバーの TCP ポート番号に 23(TELNET プロトコル)、及び "web-authentication https-port"コマンド、または"web-authentication redirect proxy-port"コマンドで指定した番号は指定できません。

"web-authentication redirect http"設定時は TCP ポート番号に 80 を設定できません。

3.47.10 web-authentication https-port

認証 Web サーバーとして使用する HTTPS プロトコルの TCP ポート番号を設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

web-authentication https-port <HTTPS-PORT>

no web-authentication https-port

HTTPS-PORT　　認証 Web サーバーの TCP ポート番号

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) TCP ポート番号を 443 に設定します。

(2) TCP ポート番号を削除します。

```
> enable
# configure terminal
(config)# access-defender
```

```
(config-a-def)# web-authentication https-port 443
(config-a-def)# no web-authentication https-port
```

関連コマンド

show running-config

注意事項

認証 Web サーバーの TCP ポート番号に 23(TELNET プロトコル)、及び "web-authentication http-port"コマンド、または"web-authentication redirect proxy-port"コマンドで指定した番号は指定できません。

不正な秘密鍵と証明書が装置にダウンロードされている状態で、本コマンドを設定した場合、Web 認証動作は保証されません。

"web-authentication redirect https"設定時は TCP ポート番号に 443 を設定できません。

本コマンドが設定されている場合、3.61.7 "restore"や 3.45.3 "copy file https-file"による証明書、秘密鍵のダウンロードはできません。
また 3.45.1 "ssl gencsr rsakey"による証明書要求と秘密鍵の作成もできません。

3.47.11 web-authentication http-session-timeout

Web 認証で使用する HTTP/HTTPS セッションタイムアウト時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

web-authentication http-session-timeout <SECONDS>
no web-authentication http-session-timeout
SECONDS　　HTTP/HTTPS セッションタイムアウト時間 <1-60(秒)>

デフォルト

60(秒)

コマンドモード

ACCESSDEFENDER

使用例

(1) HTTP/HTTPS セッションタイムアウト時間を 10 秒に設定します。
(2) HTTP/HTTPS セッションタイムアウト時間をデフォルト値に戻します。

```
(config)# access-defender
(config-a-def)# web-authentication http-session-timeout 10
(config-a-def)# no web-authentication http-session-timeout
```

関連コマンド

show running-config

注意事項

HTTP/HTTPS セッションタイムアウト時間を短く設定すると、Web 認証の同時認証性能が低下する場合があります。本コマンド未設定時と同等の性能を維持するためには、HTTP/HTTPS セッションタイムアウト時間を 10 秒以上に設定してください。

3.47.12 web-authentication ip

Web 認証時に認証端末が参照する認証 Web サーバーの IP アドレスを設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

web-authentication ip <IPADDR>
no web-authentication ip
IPADDR 認証 Web サーバーの IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) 認証 Web サーバーの IP アドレスを 192.0.2.3 に設定します。
(2) 設定した IP アドレスを削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication ip 192.0.2.3
(config-a-def)# no web-authentication ip
```

関連コマンド

show running-config

注意事項

同一ネットワークの存在しない IP アドレスを指定しないでください。

3.47.13 web-authentication redirect url

認証 Web ページのリダイレクト先 URL を指定します。設定を削除する場合は、no コマンドを使用してください。

本機能は、"web-authentication redirect http"、"web-authentication redirect https"、"web-authentication redirect proxy-port"で指定したプロトコルで任意の URL、プロキシーを参照したとき、強制的に指定した認証 Web ページへリダイレクトさせる機能です。

コマンドシンタックス

web-authentication redirect url <URL>
no web-authentication redirect url

URL　　Web 認証ページの URL <1-255(文字)>
- ASCII コードの印字可能な文字の内、[?]を除いた文字のみ使用可能

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) リダイレクト先 URL を http://192.0.2.3:8080 に設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect url http://192.0.2.3:8080
(config-a-def)# no web-authentication redirect url
```

関連コマンド

show running-config

注意事項

本機能を有効にする場合、事前に"web-authentication redirect http"、"web-authentication redirect https"、"web-authentication redirect proxy-port"コマンドでリダイレクトを行う対象プロトコルを設定する必要があります。

外部の認証 Web ページを参照せず、リダイレクト先に、本装置の認証 Web ページを表示させる場合、本装置の URL(認証 Web サーバーの IP アドレスと TCP ポート番号)を指定する必要があります。

3.47.14 web-authentication redirect http

HTTP リダイレクトを設定します。設定を削除する場合は、no コマンドを使用してください。

本機能は、未認証端末から送信される HTTP リクエスト(宛先 IP アドレスは任意)を認識し、強制的に認証 Web ページを表示する機能です。ポート番号が 80 の HTTP リクエストがリダイレクト対象になります。

コマンドシンタックス

[no] web-authentication redirect http

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) HTTP リダイレクトを設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect http
(config-a-def)# no web-authentication redirect http
```

関連コマンド

show running-config

注意事項

リダイレクト先 URL のポート番号を 80 以外に設定してください。

本機能を有効にする場合、"web-authentication ip"コマンドで、任意の IP アドレスをあらかじめ設定しておく必要があります。

リダイレクト先として、本装置に設定した認証 Web ページを使用する場合、"web-authentication redirect url"コマンドで本装置の URL(認証 Web サーバーの IP アドレスと TCP ポート番号)を指定する必要があります。

Web 認証端末のゲートウェイ(ネクストホップ)アドレスを認証装置の IP アドレスに設定した状態では使用できません。

認証 Web サーバーの TCP ポート("web-authentication http-port"、"web-authentication https-port")は、ネットワーク上の Web サーバーと必ず異なるポート番号を設定してください。

3.47.15 web-authentication redirect https

HTTPS リダイレクトを設定します。設定を削除するには、no コマンドを使用してください。

本機能は、未認証端末から送信される HTTPS リクエスト(宛先 IP アドレスは任意)を認識し、強制的に認証 Web ページを表示する機能です。ポート番号が 443 の HTTPS リクエストがリダイレクト対象になります。

コマンドシンタックス

[no] web-authentication redirect https

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) HTTPS リダイレクトを設定します。

(2) 設定を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect https
(config-a-def)# no web-authentication redirect https
```

関連コマンド

show running-config

注意事項

リダイレクト先 URL のポート番号を 443 以外に設定してください。

リダイレクト先として、本装置に設定した認証 Web ページを使用する場合、"web-authentication redirect url"コマンドで本装置の URL(認証 Web サーバーの IP アドレスと TCP ポート番号)を指定する必要があります。

Web 認証端末のゲートウェイ(ネクストホップ)アドレスを認証装置の IP アドレスに設定した状態では使用できません。

本機能を有効にする場合、"web-authentication ip"コマンドで、任意の IP アドレスをあらかじめ設定しておく必要があります。

認証 Web サーバーの TCP ポート("web-authentication http-port"、"web-authentication https-port")は、ネットワーク上の Web サーバーと必ず異なるポート番号を設定してください。

本機能で HTTPS がリダイレクトされた場合、ブラウザーに「証明書エラー」、「セキュリティーの警告」、「信頼できない接続」などセキュリティーに関わる警告が表示されます。これは HTTPS の仕様によるもので装置の異常ではありません。装置に正式な証明書をダウンロード、またはブラウザーに CA 証明書を追加した場合でも、警告は表示されます。

3.47.16 web-authentication redirect proxy-port

プロキシーリダイレクトを有効にします。無効にする場合は、no コマンドを使用してください。

本機能は、認証端末が指定したプロキシーポート番号を経由して任意の Web ページを参照したとき、強制的に認証 Web ページを表示させる機能です。

コマンドシンタックス

web-authentication redirect proxy-port <PROXY-PORT>
no web-authentication redirect proxy-port
PROXY-PORT　　プロキシーポート番号 <1-65535>

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) プロキシーポート番号を 10080 に設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication redirect proxy-port 10080
(config-a-def)# no web-authentication redirect proxy-port
```

関連コマンド

show running-config

注意事項

リダイレクト先として、本装置に設定した認証 Web ページを使用する場合、"web-authentication redirect url"コマンドで本装置の URL(認証 Web サーバーの IP アドレスと TCP ポート番号)を指定する必要があります。

Web 認証端末のゲートウェイ(ネクストホップ)アドレスを認証装置の IP アドレスに設定した状態では使用できません。

本機能を有効にする場合、"web-authentication ip"コマンドで、任意の IP アドレスをあらかじめ設定しておく必要があります。

認証端末が HTTPS プロトコルを使用した場合、リダイレクトはされません。

プロキシーポート番号に 23(TELNET プロトコル)、及び"web-authentication http-port"コマンド、または"web-authentication https-port"コマンドで指定した番号は指定できません。

本機能と"web-authentication snooping proxy-port"コマンドは同時に設定できません。

3.47.17 web-authentication snooping proxy-port

スヌーピングプロキシー機能を有効にします。無効にする場合は、no コマンドを使用してください。

本機能は、認証端末が指定したプロキシーポート番号を経由して任意の Web ページを参照したとき、強制的に認証 Web ページを表示させる機能です。リダイレクトは行わず装置の認証 Web ページを返します。プロキシーリダイレクト機能のように、Web ブラウザーのプロキシー設定で、内部認証 Web ページの URL を例外指定する必要はありません。

コマンドシンタックス

web-authentication snooping proxy-port <PROXY-PORT>
no web-authentication snooping proxy-port
PROXY-PORT　　プロキシーポート番号 <1-65535>

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) プロキシーポート番号を 10080 に設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication snooping proxy-port 10080
(config-a-def)# no web-authentication snooping proxy-port
```

関連コマンド

show running-config

注意事項

外部認証 Web ページを表示させることはできません。

リダイレクト先 URL の設定は不要です。

本機能と"web-authentication redirect proxy-port"コマンドは同時に設定できません。

認証成功後は認証 Web ページを表示させることはできません。ログアウトなどで Web 認証画面を表示させる場合は、認証 Web サーバーの IP アドレスをブラウザーのプロキシー例外に設定し、認証 Web サーバーとして使用する HTTP、または HTTPS プロトコルの TCP ポート番号から、認証 Web サーバーの IP アドレスにアクセスしてください。

3.47.18 web-authentication mac-authentication-password

Web/MAC 認証(AND)における MAC 認証用パスワードを設定します。設定を無効にする場合は、no コマンドを使用してください。

Web/MAC 認証(AND)を有効にするポートは"web-authentication port"コマンドにてオプション mac-authentication を指定してください。また、認証方法によって、RADIUS サーバー、またはローカルデータベースに本コマンドで設定したパスワードを MAC 認証のパスワードとしてあらかじめ登録しておく必要があります。

コマンドシンタックス

web-authentication mac-authentication-password <PASSWORD>
no web-authentication mac-authentication-password

PASSWORD	Web/MAC 認証(AND)における MAC 認証用パスワード <1-63(文字)> • 表示可能な ASCII コード("?"を除く)

デフォルト

なし

コマンドモード

ACCESSDEFENDER

使用例

(1) Web/MAC 認証(AND)における MAC 認証用パスワードとして、aaaaa を指定します。
(2) Web/MAC 認証(AND)における MAC 認証用パスワードを削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication mac-authentication-password aaaaa
(config-a-def)# no web-authentication mac-authentication-password
```

関連コマンド

show running-config

注意事項

パスワードに使用できる文字は、ASCII コードの印字可能な文字です。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

設定したパスワードは、"show running-config"コマンド、"show flash-config"コマンドにおいては暗号化されて表示されます。

Ver. 7.19 以前から 7.20 以降へバージョンアップした場合、Web/MAC 認証(AND)ポートには Web/MAC 認証(AND)を有効にするポート指定("web-authentication port mac-authentication"コマンド)が必要です。

3.47.19 web-authentication ttl

TTL フィルター機能を設定します。Web 認証において、指定した TTL 値の IP パケットのみ認証可能とします。設定を無効にする場合は、no コマンドを使用してください。指定可能な TTL 値は最大 8 個です。

コマンドシンタックス

web-authentication ttl <TTL> port <PORTRANGE>
no web-authentication ttl [<TTL> [port <PORTRANGE>]]

TTL	IP ヘッダーの TTL(Time To Live)値 <1-255>
PORTRANGE	ポート番号(複数指定可能)

デフォルト

なし(＝無効)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1 に TTL 値：255 の TTL フィルター機能を設定します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication ttl 255 port 1
```

関連コマンド

show running-config, show access-defender port-configuration

注意事項

3.47.20 web-authentication sslv2 enable

認証用 Web サーバーで使用する SSL プロトコルのバージョン 2(SSLv2)を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] web-authentication sslv2 enable

デフォルト

no enable(＝無効)

コマンドモード

ACCESSDEFENDER

使用例

(1) 認証用 Web サーバーが使用する SSL プロトコルのバージョン 2 を有効にします。
(2) 認証用 Web サーバーで使用する SSL プロトコルのバージョン 2 を無効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication sslv2 enable
(config-a-def)# no web-authentication sslv2 enable
```

関連コマンド

show running-config

注意事項

SSLv2 は脆弱性が確認されているため、本コマンドの設定は推奨しません。

SSLv2 は中間証明書が利用できません。中間証明書を利用する場合は、TLS(Transport Layer Security)を利用することを推奨します。

SSLv2 を使用する場合、SHA-1、または SHA-2 で作成した証明書は使用できません。

3.47.21 web-authentication sslv3 enable

認証用 Web サーバーで使用する SSL プロトコルのバージョン 3(SSLv3)を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] web-authentication sslv3 enable

デフォルト

no enable(＝無効)

コマンドモード

ACCESSDEFENDER

使用例

(1) 認証用 Web サーバーが使用する SSL プロトコルのバージョン 3 を有効にします。

(2) 認証用 Web サーバーで使用する SSL プロトコルのバージョン 3 を無効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# web-authentication sslv3 enable
(config-a-def)# no web-authentication sslv3 enable
```

関連コマンド

show running-config

注意事項

SSLv3 は脆弱性が確認されているため、本コマンドの設定は推奨しません。

3.47.22 mac-authentication enable

MAC 認証を有効にします。無効にする場合は、no コマンドを使用してください。

MAC 認証は、認証端末の MAC アドレスにより自動的に認証を行う機能です。認証時にユーザーの属性に従って動的に VLAN を割り当てることも可能です。また、1 ポートで複数端末の認証が可能であり、認証端末ごとに VLAN を割り当てることもできます。

MAC 認証で認証拒否(ローカル認証も含む)された認証端末は、MAC アドレスが discard 登録されます。discard 登録中は、discard 登録された認証端末よりフレームを受信しても、MAC 認証は行われません。discard 登録は、300 秒経過後に自動的に解除されます。また、"access-defender-logout mac"コマンドで認証端末の MAC アドレスを指定するか、"access-defender-logout user"コマンドで認証端末のユーザーID を指定することにより、discard 登録を解除することも可能です。認証端末、及び discard 登録の確認は、"show access-defender client"コマンドで確認してください。

また、パケットフィルター2 の"authentication-bypass"コマンドを利用することにより、特定の端末のみ MAC 認証の結果を問わず、通信を許可させることが可能です(詳細はパケットフィルター2 の 3.28.5 "action"の authentication-bypass の項を参照ください)。

MAC 認証の特徴

(1) MAC アドレスによる認証

(2) 認証端末への動的な VLAN 割り当て

(3) 同一ポートでの Web 認証/IEEE 802.1X/DHCP Snooping との併用

(4) プライマリー/セカンダリーの RADIUS サーバーの登録

(5) RADIUS サーバー無応答時のローカル認証、強制認証

(6) RADIUS サーバーを使用しないローカル認証、強制認証

コマンドシンタックス

[no] mac-authentication enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) MAC 認証を有効にします。

(2) MAC 認証を無効にします。

```
> enable
# configure terminal
(config)# mac-authentication enable
(config)# no mac-authentication enable
```

関連コマンド

show running-config

注意事項

discard 登録できる MAC アドレスは最大 100 個です。

本装置の DHCP サーバー機能を併用して、端末へ動的に VLAN を割り当てる場合、認証前 VLAN 用の DHCP サーバーと、認証後 VLAN 用の DHCP サーバーは同一装置内に設定しないでください。認証後 VLAN の IP アドレスに切り替わらないことがあります。

DHCP での IP アドレス取得中に認証が成功し、VLAN が IP アドレス取得よりも先に動的に割り当たった場合、DHCP のシーケンスが途中で止まり IP アドレスが取得できなくなります。その際は、"mac-authentication ignore-dhcp"コマンドを使用してください。

認証フレームとして VLAN タグつきフレームを受信した場合、認証端末の VLAN ID は VLAN タグの VLAN ID になります。

MAC 認証有効ポートに認証バイパスを設定したとき、認証バイパスの対象となるフレームが自局 IP アドレス宛などの CPU 宛てである場合やソフト中継される場合、認証が動作します。

MAC 認証に失敗し、discard 登録された端末の通信が認証バイパスの対象となる場合

でも、認証バイパスにより通信は可能です。

本コマンドを有効にするには、"packet-filter2 max-rule"を設定する必要があります。

3.47.23 mac-authentication port

MAC 認証を有効にするポートを指定します。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] mac-authentication port <PORTRANGE>

PORTRANGE　　ポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1～20 を MAC 認証ポートに指定します。

(2) ポート：1～10 を MAC 認証ポートから解除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# mac-authentication port 1-20
(config-a-def)# no mac-authentication port 1-10
```

関連コマンド

show access-defender port-configuration, show running-config

注意事項

MAC 認証ログイン中に、ログアウトせずに接続ポートを移動した場合は、MAC 認証でのみ再ログインが可能です。

3.47.24 mac-authentication password

MAC 認証のパスワードを設定します。設定を削除する場合は、no コマンドを使用してください。

MAC 認証を使用する場合、認証方法によって、RADIUS サーバー、またはローカルデータベースに本コマンドで設定したパスワードを登録しておく必要があります。

コマンドシンタックス

mac-authentication password <PASSWORD>

no mac-authentication password

PASSWORD　　パスワード <1-63(文字)>

- 表示可能な ASCII コード("?"を除く)

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) MAC 認証のパスワードとして、xxxxx を設定します。

(2) 設定を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# mac-authentication password xxxxx
(config-a-def)# no mac-authentication password
```

関連コマンド

show running-config

注意事項

パスワードに使用できる文字は、ASCII コードの印字可能な文字です。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

設定したパスワードは、"show running-config"コマンド、"show flash-config"コマンドにおいては暗号化されて表示されます。

3.47.25 mac-authentication password-mac-address

MAC 認証のパスワードとして認証端末の MAC アドレスを使用します。設定を削除する場合は、no コマンドを使用してください。MAC 認証を使用する場合、認証方法によって、RADIUS サーバー、またはローカルデータベースにMAC認証のパスワードとしてユーザーIDと同じ文字列を登録しておく必要があります。

MAC 認証のユーザーID は、16 進文字列(英小文字)、区切り文字無し 12 文字の認証端末 MAC アドレスを使用します。本コマンドを使用することで、各認証端末ごとにパスワードを設定します。

コマンドシンタックス

[no] mac-authentication password-mac-address

デフォルト

なし(＝設定なし)

コマンドモード
ACCESSDEFENDER

使用例
(1) MAC 認証のパスワードを認証端末の MAC アドレスに設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# mac-authentication password-mac-address
(config-a-def)# no mac-authentication password-mac-address
```

関連コマンド
mac-authentication password, show running-config

注意事項

本コマンドは、MAC 認証単体のみ有効となります(Web/MAC 認証(AND)、IEEE802.1X/MAC 認証には影響しません)。本コマンド設定時に、Web/MAC 認証(AND)、または IEEE802.1X/MAC 認証と併用する場合、"aaa authentication web"コマンド、及び"aaa authentication dot1x"コマンドで指定する RADIUS サーバー、もしくはローカルデータベースは、"aaa authentication mac"コマンドで指定する RADIUS サーバー、もしくはローカルデータベースと同じものを指定しないでください。

3.47.26 mac-authentication ignore-dhcp

MAC 認証において、認証端末から送信される UDP ポート 67(DHCP サーバー)宛のパケットを MAC 認証の対象外とします。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス
[no] mac-authentication ignore-dhcp

デフォルト
なし(＝設定なし)

コマンドモード
ACCESSDEFENDER

使用例
(3) 認証端末から送信される UDP ポート：67(DHCP サーバー)宛のパケットを MAC 認証の対象外とします。
(4) 設定を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# mac-authentication ignore-dhcp
(config-a-def)# no mac-authentication ignore-dhcp
```

関連コマンド

show running-config

注意事項

3.47.27 dot1x enable

IEEE 802.1X を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] dot1x enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) IEEE 802.1X を有効にします。

```
> enable
# configure terminal
(config)# dot1x enable
```

関連コマンド

show running-config

注意事項

STP と併用する場合、supplicant から受信する EAPOL フレームの宛先 MAC アドレスが特定のユニキャストアドレス(00:40:66:33:1D:A9)、または装置の自局 MAC アドレスの場合のみ、動作が保証されます。

3.47.28 dot1x port

IEEE 802.1X を有効にするポートを設定します。設定を無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] dot1x port <PORTRANGE>
PORTRANGE　　ポート番号(複数指定可能)

デフォルト
なし(＝設定なし)

コマンドモード
ACCESSDEFENDER

使用例
(1) ポート：1～5 で IEEE 802.1X を有効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dot1x port 1-5
```

関連コマンド
show access-defender port-configuration, show running-config

注意事項

Web/IEEE802.1X 認証(AND)ポートに設定されているポートに対して IEEE802.1X 認証ポートの設定("dot1x port <PORT>")をしても無視されます。

IEEE Std 802.1X-2001 に準拠しているため、タグ付きの IEEE802.1X 認証フレームに対しては、認証できません。ただし、VLAN ID：0 のタグ付きフレーム(プライオリティタグフレーム)は認証できます。

3.47.29 dot1x mac-authentication-password

IEEE802.1X/MAC 認証(AND)を有効にし、MAC 認証用パスワードを設定します。設定を無効にする場合は、no コマンドを使用してください。

IEEE802.1X/MAC 認証(AND)を有効にした場合、IEEE 802.1X によるユーザー認証に先立ち、認証端末 MAC アドレスによる認証を実施します。認証端末の MAC 認証と IEEE 802.1X の両モード認証成功時のみ通信可となります。

IEEE802.1X/MAC 認証(AND)を使用する場合、認証方法によって、RADIUS サーバー、またはローカルデータベースに本コマンドで設定したパスワードを MAC 認証のパスワードとして登録しておく必要があります。

コマンドシンタックス
dot1x mac-authentication-password <PASSWORD>
no dot1x mac-authentication-password
PASSWORD　IEEE802.1X/MAC 認証(AND)における MAC 認証用パスワード <1-63(文字)>
- 表示可能な ASCII コード("?"を除く)

デフォルト
なし(＝無効)

コマンドモード
ACCESSDEFENDER

使用例
(1) IEEE802.1X/MAC 認証(AND)を有効にし、MAC 認証用パスワードとして aaaaa を指定します。
(2) IEEE802.1X/MAC 認証(AND)を無効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dot1x mac-authentication-password aaaaa
(config-a-def)# no dot1x mac-authentication-password
```

関連コマンド
show running-config

注意事項

パスワードに使用できる文字は、ASCII コードの印字可能な文字です。ただし、「¥」「"」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。

設定したパスワードは、"show running-config"コマンド、"show flash-config"コマンドにおいては暗号化されて表示されます。

IEEE802.1X/MAC 認証(AND)を有効にした場合、"dot1x port"で指定した全ポートで IEEE802.1X/MAC 認証(AND)が有効になります。

3.47.30 dot1x port ignore-eapol-start

EAPOL-Start 受信時の動作を設定します。本設定を有効にしたポートでは、supplicant からの EAPOL-Start 受信時に EAP 要求フレームを送信しません。設定を無効にする場合は、no コマンドを使用してください。

コマンドシンタックス
[no] dot1x port <PORTRANGE> ignore-eapol-start
PORTRANGE　　ポート番号(複数指定可能)

デフォルト
なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1～5 で ignore-eapol-start を有効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dot1x port 1-5 ignore-eapol-start
```

関連コマンド

show running-config

注意事項

3.47.31 dot1x port initialize

IEEE 802.1X の初期化を行い、登録された認証済み端末を消去します。

コマンドシンタックス

dot1x port <PORTRANGE> initialize

PORTRANGE	ポート番号(複数指定可能)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1～5 の IEEE 802.1X を初期化します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dot1x port 1-5 initialize
```

関連コマンド

注意事項

3.47.32 dot1x port max-req

RADIUS サーバーから受信した EAP 要求フレームを supplicant に送信する最大送信回数を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

dot1x port <PORTRANGE> max-req <ATTEMPTS>

no dot1x port <PORTRANGE> max-req

PORTRANGE　　ポート番号(複数指定可能)
ATTEMPTS　　再送する最大回数 <1-10(回)>

デフォルト
2(回)

コマンドモード
ACCESSDEFENDER

使用例
(1) ポート：1における再送する最大回数を1回に設定します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dot1x port 1 max-req 1
```

関連コマンド
show running-config

注意事項

3.47.33 dot1x port reauthentication

再認証を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス
[no] dot1x port <PORTRANGE> reauthentication
PORTRANGE　　ポート番号(複数指定可能)

デフォルト
なし(＝設定なし)

コマンドモード
ACCESSDEFENDER

使用例
(1) ポート：1の再認証を有効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dot1x port 1 reauthentication
```

関連コマンド
show running-config

注意事項

3.47.34 dot1x port re-authenticate

再認証を行います。

コマンドシンタックス

dot1x port <PORTRANGE> re-authenticate

PORTRANGE　　ポート番号(複数指定可能)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1の再認証を行います。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dot1x port 1 re-authenticate
```

関連コマンド

注意事項

3.47.35 dot1x port timeout quiet-period

認証失敗時のステータス保持時間を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

dot1x port <PORTRANGE> timeout quiet-period <SECS>

no dot1x port <PORTRANGE> timeout quiet-period

PORTRANGE　　ポート番号(複数指定可能)

SECS　　ステータス保持時間 <0-65535(秒)>

デフォルト

60(秒)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1における認証失敗時のステータス保持時間を 10 秒に設定します。

```
> enable
# configure terminal
```

```
(config)# access-defender
(config-a-def)# dot1x port 1 timeout quiet-period 10
```

関連コマンド

show running-config

注意事項

3.47.36 dot1x port timeout re-authperiod

再認証の間隔を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

dot1x port <PORTRANGE> timeout re-authperiod <SECS>
no dot1x port <PORTRANGE> timeout re-authperiod

PORTRANGE	ポート番号(複数指定可能)
SECS	再認証間隔 <5-2147483647(秒)>

デフォルト

3600(秒)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1 における再認証間隔を 300 秒に設定します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dot1x port 1 timeout re-authperiod 300
```

関連コマンド

show running-config

注意事項

3.47.37 dot1x port timeout supp-timeout

RADIUS サーバーから受信した EAP 要求フレームを supplicant に送信した後、supplicant からの EAP 応答フレームを受信できずにタイムアウトとみなし、EAP 要求フレームを再送する間隔を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

dot1x port <PORTRANGE> timeout supp-timeout <SECS>
no dot1x port <PORTRANGE> timeout supp-timeout

PORTRANGE　　ポート番号(複数指定可能)
SECS　　タイムアウト時間 <5-65535(秒)>

デフォルト
30(秒)

コマンドモード
ACCESSDEFENDER

使用例
(1) ポート：1～2 におけるタイムアウト時間を 10000 秒に設定します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dot1x port 1-2 timeout supp-timeout 10000
```

関連コマンド
show running-config

注意事項

3.47.38 dot1x port timeout tx-period

認証開始時に supplicant に対して送信する EAP 要求/認識フレームを送信した後、supplicant からの EAP 応答フレームを受信できずにタイムアウトとみなし、EAP 要求/認識フレームを再送する間隔を設定します。0 を指定すると EAP 要求/認識フレームは再送されません。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス
dot1x port <PORTRANGE> timeout tx-period <SECS>
no dot1x port <PORTRANGE> timeout tx-period
PORTRANGE　　ポート番号(複数指定可能)
SECS　　送信間隔 <0、5-65535(秒)>

デフォルト
30(秒)

コマンドモード
ACCESSDEFENDER

使用例
(1) ポート：1、2～5 における EAP 要求/認識フレームの再送間隔を 40 秒に設定します。

```
> enable
# configure terminal
(config)# access-defender
```

```
(config-a-def)# dot1x port 1,2-5 timeout tx-period 40
```

関連コマンド

show running-config

注意事項

3.47.39 dhcp-snooping enable

DHCP Snoopingを有効にします。無効にする場合は、noコマンドを使用してください。

コマンドシンタックス

[no] dhcp-snooping enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) DHCP Snoopingを有効にします。
(2) DHCP Snoopingを無効にします。

```
> enable
# configure terminal
(config)# dhcp-snooping enable
(config)# no dhcp-snooping enable
```

関連コマンド

show access-defender dhcp-snooping configuration, show running-config

注意事項

DHCP Snooping を有効にするには、"packet-filter2 max-rule"を設定する必要があります。

DHCPリレー機能を同時に有効にすることはできません。

PERMIT モード時に他の認証を併用している時は、他の認証状態に関係なく通信が可能です。

DHCP Snoopingでは、リンクダウンによるログアウトを行いません。リンクダウン後でもリース期間満了になるまで登録が継続されます。

装置を認証端末のゲートウェイとして使用する場合、DHCP Snooping と他認証(Web/MAC/ゲートウェイ/dot1x)は同一インターフェースで併用できません。

同一 VLAN インターフェースにて DHCP サーバーと DHCP Snooping を併用する場合、"dhcp-snooping internal-dhcp-vlan"を設定する必要があります。

DHCP Snooping 有効時は、DHCP パケットを 3.28 パケットフィルター2 の authentication-bypass 対象に設定しないでください。

端末が PXE ブートを行う場合、PXE サーバーによっては DHCP Snooping で認証できない場合があります。PXE ブートを行う端末は"dhcp-snooping port"の設定がないポートに接続してください。

3.47.40 dhcp-snooping port

DHCP Snooping を実施するポート番号を指定します。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] dhcp-snooping port <PORTRANGE>

PORTRANGE　　DHCP Snooping を実施するポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1～12 で DHCP Snooping を実施します。
(2) ポート：1～12 を DHCP Snooping を実施するポートから除外します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping port 1-12
(config-a-def)# no dhcp-snooping port 1-12
```

関連コマンド

show access-defender dhcp-snooping configuration, show access-defender port-configuration, show running-config

注意事項

DHCP Snooping 有効時、本設定のないポートにおいて受信した DHCP パケットは中継

されます。

3.47.41 dhcp-snooping mode deny

DHCP Snooping の動作モードを、DENY モードに設定します。PERMIT モードにする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] dhcp-snooping mode deny

デフォルト

no deny(＝PERMIT モード)

コマンドモード

ACCESSDEFENDER

使用例

(1) DHCP Snooping の動作モードを DENY モードに設定します。
(2) DHCP Snooping の動作モードを PERMIT モードに設定します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping mode deny
(config-a-def)# no dhcp-snooping mode deny
```

関連コマンド

show access-defender dhcp-snooping configuration,
show access-defender dhcp-snooping mode-status, show running-config

注意事項

3.47.42 dhcp-snooping mode mac-authentication

DHCP Snooping の動作モードを、mac-authentication モードに設定します。無効にする場合は、no コマンドを使用してください。本モード設定時、MAC 認証と DHCP Snooping の併用ポートにおいて、認証成功端末のみ、DHCP パケットを中継し、DHCP Snooping 対象端末として登録します。他認証モードを同時に使用している場合も、DHCP Snooping 併用時の MAC 認証に対して有効になります。

本モード設定時でも、MAC 認証を併用していない DHCP Snooping の処理には影響ありません。

コマンドシンタックス

[no] dhcp-snooping mode mac-authentication

デフォルト

なし(＝mac-authentication モード無効)

コマンドモード
ACCESSDEFENDER

使用例
(1) DHCP Snooping の動作モードを mac-authentication モードに設定します。
(2) DHCP Snooping の mac-authentication モードを無効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping mode mac-authentication
(config-a-def)# no dhcp-snooping mode mac-authentication
```

関連コマンド
show access-defender dhcp-snooping configuration,
show access-defender dhcp-snooping mode-status, show running-config

注意事項

本動作モードと 3.40 DHCP サーバー機能は併用できません。

3.47.43 dhcp-snooping mode timer

DHCP Snooping は、PERMIT モードで起動した場合、一定時間が経過した後、自動で DENY モードに切り替わります。設定をデフォルト値に戻す場合は、no コマンドを使用してください。
本コマンドで、自動的に DENY モードに切り替わるまでの時間を設定します。

コマンドシンタックス
dhcp-snooping mode timer <TIME>
no dhcp-snooping mode timer

TIME　DENY モードに切り替わるまでの時間を秒単位で設定 <0、30-604800(秒)>
- 0 は PERMIT モードを保持(DENY モードへの切り替えなし)

デフォルト
1800(秒)

コマンドモード
ACCESSDEFENDER

使用例
(1) DENY モードに切り替わるまでの時間を 3600 秒に設定します。
(2) DENY モードに切り替わるまでの時間をデフォルトに戻します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping mode timer 3600
```

```
(config-a-def)# no dhcp-snooping mode timer
```

関連コマンド

show access-defender dhcp-snooping configuration,
show access-defender dhcp-snooping mode-status, show running-config

注意事項

PERMIT モード中に切り替わり時間を変更した場合、設定済みの値で上書き設定した場合は、それまでの経過時間がリセットされます。

3.47.44 dhcp-snooping static-entry port

DHCP Snooping は動的にフィルターを自動作成しますが、本コマンドにて、コマンドラインから静的にフィルターを作成することも可能です。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

dhcp-snooping static-entry port <PORT> <IPADDR>
no dhcp-snooping static-entry [port <PORT> [<IPADDR>]]

PORT	ポート
IPADDR	IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) 対象ポートがポート：1、対象 IP アドレスが 192.168.1.10 の静的フィルターを追加します。
(2) 対象ポートがポート：2、対象 IP アドレスが 192.168.1.100 の静的フィルターを削除します。
(3) ポート：5 の静的フィルターをすべて削除します。
(4) すべての静的フィルターを削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping static-entry port 1 192.168.1.10
(config-a-def)# no dhcp-snooping static-entry port 2 192.168.1.100
(config-a-def)# no dhcp-snooping static-entry port 5
(config-a-def)# no dhcp-snooping static-entry
```

関連コマンド

show access-defender dhcp-snooping configuration, show running-config,
show access-defender client, show access-defender dhcp-snooping status

注意事項

本コマンドで登録された静的フィルターは、自動では削除されません。フィルターを削除する場合、手動で削除する必要があります。

各ポートで登録可能な静的フィルターの上限数は(クライアント制限数－動的に登録されているフィルター数)となります。

すでに登録されている動的フィルターと同じポート、同じ IP アドレスの静的フィルターを登録した場合、その動的フィルターに対して静的フィルターが上書きされます。

DHCP Snooping の Static エントリーを設定している場合、他の認証を有効にした後に DHCP Snooping を有効("dhcp-snooping enable")にしてください。

3.47.45 dhcp-snooping internal-dhcp-vlan

DHCP Snooping と DHCP サーバー機能を併用する VLAN インターフェースを設定します。設定を削除する場合は、no コマンドを使用してください。最大 12 個設定可能です。

コマンドシンタックス

```
dhcp-snooping internal-dhcp-vlan add <VID>
no dhcp-snooping internal-dhcp-vlan add [ <VID> ]
      VID                VLAN ID
```

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) VLAN インターフェース：100 を DHCP Snooping と DHCP サーバー機能の併用 VLAN インターフェースに設定します。

(2) VLAN インターフェース：100 を DHCP Snooping と DHCP サーバー機能の併用 VLAN インターフェースから削除します。

(3) 全 VLAN インターフェースを DHCP Snooping と DHCP サーバー機能の併用 VLAN インターフェースから削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# dhcp-snooping internal-dhcp-vlan add 100
(config-a-def)# no dhcp-snooping internal-dhcp-vlan add 100
(config-a-def)# no dhcp-snooping internal-dhcp-vlan add
```

関連コマンド

show access-defender dhcp-snooping configuration, show running-config,
show access-defender client, show access-defender dhcp-snooping status

注意事項

3.47.46 logout aging-time

エージングログアウトの設定を行います。設定を無効にする場合は、no コマンドを使用してください。Web 認証、ゲートウェイ認証、MAC 認証、IEEE 802.1X の各認証方式に設定することが可能です。

エージングログアウトは、認証済み端末と設定したエージング間隔無通信の場合に、認証済み端末を自動的にログアウトさせる機能です。エージング間隔は、0、10-86400(秒)、0-59(分)、0-23(時間)、0-31(日数)の間で指定し、0 を指定した場合にはエージングログアウトは行われません。

パラメーター指定の際は、(秒)、(分)、(時間)、(日数)の順で行い、(分)、(時間)、(日数)については省略することができます。

パラメーターはすべての時間の合計を秒に換算します。パラメーターを"100 1 0 0"に設定した場合には 160 秒後にログアウトします。

AEOS Ver. 7.09.01 より分、時間、日数の設定が可能になっていますが、これら設定ができない従来版からのコマンドの引継ぎは可能です。

無通信時間のカウントは、本装置と認証済み端末間の通信が終了してから即座に行われます。
無通信時間のカウント状況は"show access-defender client"コマンドで確認してください。

コマンドシンタックス

logout aging-time <SECONDS> [<MINUTES> [<HOURS> [<DAYS>]]] [web | gateway | mac | dot1x]
no logout aging-time [web | gateway | mac | dot1x]

SECONDS	エージング間隔 <0、10-86400(秒)>
MINUTES	エージング間隔 <0-59(分)>
HOURS	エージング間隔 <0-23(時間)>
DAYS	エージング間隔 <0-31(日数)>

デフォルト

0(秒)(＝エージングログアウト無効)

コマンドモード

ACCESSDEFENDER

使用例

(1) エージング間隔を 1000 秒に設定します。
(2) エージングログアウトを無効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# logout aging-time 1000
(config-a-def)# no logout aging-time
```

関連コマンド

show running-config, show access-defender client

注意事項

3.47.47 logout timeout

タイムアウト時間設定します。設定を削除する場合は、no コマンドを使用してください。Web 認証、ゲートウェイ認証、MAC 認証、IEEE 802.1X の各認証方式に設定することが可能です。

認証端末は、本コマンドで指定した時間が経過すると自動的にログアウトされ、未認証状態になります。0、10-86400(秒)、0-59(分)、0-23(時間)、0-31(日数)の間で指定し、0 を指定した場合には自動ログアウトは行われません。

パラメーター指定の際は、(秒)、(分)、(時間)、(日数)の順で行い、(分)、(時間)、(日数)については省略することができます。

パラメーターはすべての時間の合計を秒に換算します。パラメーターを"100 1 0 0"に設定した場合には 160 秒後にログアウトします。

AEOS Ver. 7.09.01 より分、時間、日数の設定が可能になっていますが、これら設定ができない従来版からのコマンドの引継ぎは可能です。

コマンドシンタックス

logout timeout <SECONDS> [<MINUTES> [<HOURS> [<DAYS>]]] [web | gateway | mac | dot1x]
no logout timeout [web | gateway | mac | dot1x]

SECONDS	タイムアウト時間 <0、10-86400(秒)>
MINUTES	タイムアウト時間 <0-59(分)>
HOURS	タイムアウト時間 <0-23(時間)>
DAYS	タイムアウト時間 <0-31(日数)>

デフォルト

0(秒)(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) タイムアウト時間を 1000 秒に設定します。
(2) タイムアウト時間を無効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# logout timeout 1000
(config-a-def)# no logout timeout
```

関連コマンド

show running-config, show access-defender client

注意事項

3.47.48 logout linkdown port disable

リンクダウンログアウトを無効にします。有効に戻す場合は、no コマンドを使用してください。本設定とローミング機能("roaming port enable"コマンド)の設定を併用することにより、リンクアグリゲーション、ポートリダンダントのポートにおいて、認証済み端末の通信ポートがリンクダウンにより切り替わっても、ログアウトすることなく通信が継続されます。

また、IEEE802.1X 認証で STP を併用する場合、本設定が必要となります。

コマンドシンタックス

[no] logout linkdown port <PORTRANGE> disable

PORTRANGE　　ポート番号(複数指定可能)

デフォルト

enable(＝有効)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1 のリンクダウンログアウトを無効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# logout linkdown port 1 disable
```

関連コマンド

show access-defender port-configuration, show running-config

注意事項

3.47.49 logout linkdown time port enable

リンクダウン監視時間("logout linkdown time"コマンドで設定)を有効とするポートを指定します。設定を無効にする場合は、no コマンドを使用してください。

有効ポートではリンクダウンがリンクダウン監視時間継続しない場合は認証済み端末がログアウトされません。無効の場合、リンクダウン後即時に認証済み端末がログアウトされます。

コマンドシンタックス

[no] logout linkdown time port <PORTRANGE> enable

PORTRANGE　　ポート番号(複数指定可能)

デフォルト

no enable(＝無効)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1のリンクダウン監視時間を有効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# logout linkdown time port 1 enable
```

関連コマンド

show access-defender port-configuration, show running-config

注意事項

3.47.50 logout linkdown time

リンクダウン監視時間を設定します。設定を削除する場合は、no コマンドを使用してください。

"logout linkdown time port enable"コマンドの指定ポートは、リンクダウンがリンクダウン監視時間継続しない場合は認証済み端末がログアウトされません。

コマンドシンタックス

logout linkdown time <TIME>

no logout linkdown time

TIME　　リンクダウン監視時間 <1-300(秒)>

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) リンクダウン監視時間を 10 秒に設定します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# logout linkdown time 10
```

関連コマンド

show running-config

注意事項

3.47.51 logout ping dst-ip

宛先 IP アドレス指定の PING ログアウト機能を設定します。指定した IP アドレス宛の ICMP Request パケットを認証済み端末から受信すると、当該認証済み端末は自動的にログアウトして未認証状態になります。設定を無効にする場合は、no コマンドを使用してください。指定可能な宛先 IP アドレスは 1 個です。

コマンドシンタックス

logout ping dst-ip <IPADDR>
no logout ping dst-ip
　　IPADDR　　宛先 IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) 192.168.1.254 宛の PING ログアウト機能を設定します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# logout ping dst-ip 192.168.1.254
```

関連コマンド

show running-config

注意事項

本コマンドは Web 認証、ゲートウェイ認証でのみ有効です。

本コマンドと"logout ping ttl"コマンド併用時は、2 つの条件を満たした場合に認証済み端末がログアウトされます。

3.47.52 logout ping ttl

TTL 指定の PING ログアウト機能を設定します。指定した TTL 値の ICMP Request パケットを認証済み端末から受信すると、当該認証済み端末は自動的にログアウトして未認証状態になります。設定を無効にする場合は、no コマンドを使用してください。指定可能な TTL 値は 1 個です。

コマンドシンタックス

logout ping ttl <TTL>
no logout ping ttl

TTL　　IP ヘッダーの TTL(Time To Live)値 <1-255>

デフォルト
なし(＝設定なし)

コマンドモード
ACCESSDEFENDER

使用例
(1) TTL 値：1 の PING ログアウト機能を設定します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# logout ping ttl 1
```

関連コマンド
show running-config

注意事項

本コマンドは Web 認証、ゲートウェイ認証でのみ有効です。

本コマンドと"logout ping dst-ip"コマンド併用時は、2 つの条件を満たした場合に認証済み端末がログアウトされます。

3.47.53 logout clock

時刻指定ログアウトを設定します。認証済み端末は設定した時刻に自動的にログアウトして未認証状態になります。認証モード指定を省略した場合は全認証モード共通のログアウト時刻を設定します。設定を無効にする場合は、no コマンドを使用してください。指定可能なログアウト時刻は認証モードごとに 8 個です。認証モードごとのログアウト時刻と全認証モード共通のログアウト時刻を設定した場合、認証モードごとのログアウト時刻が優先されます。gateway は Apresia13000 シリーズのみ指定可能です。

コマンドシンタックス
logout clock <HH:MM> [web | gateway | mac | dot1x]
no logout clock [<HH:MM> [web | gateway | mac | dot1x]] | [web | gateway | mac | dot1x]

デフォルト
なし(＝設定なし)

コマンドモード
ACCESSDEFENDER

使用例
(1) MAC 認証の時刻指定ログアウトを 17:00 に設定します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# logout clock 17:00 mac
```

関連コマンド

show running-config

注意事項

3.47.54 access-defender-deny

認証を拒否する対象の端末と時間を設定します。本コマンドで指定した MAC アドレス、及び IP アドレスの端末は指定した時間、認証が拒否されます。本機能を使用する場合、事前に"packet-filter2 max-rule"コマンドで deny-rule を設定する必要があります。

コマンドシンタックス

access-defender-deny (ip <IPADDR>) | (mac <MACADDR>) timer <MINUTES>

IPADDR	認証拒否する端末の IP アドレス
MACADDR	認証拒否する端末の MAC アドレス
MINUTES	認証拒否時間 <1-60(分)>

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) IP アドレス：10.0.0.1 の端末を 10 分間認証拒否します。

```
# access-defender-deny ip 10.0.0.1 timer 10
```

関連コマンド

show access-defender deny, show access-defender packet-filter2 rule-statistics

注意事項

"access-defender-deny ip"指定端末からの ARP によって MAC 認証が行われる場合があります。MAC 認証が成功しても認証拒否時間内は通信できません。

3.47.55 access-defender-logout ip

認証種別に関わらずログインした端末(本項内では以下認証端末)の強制ログアウトを行います。

認証端末の IP アドレスを指定した場合、AccessDefender ログイン中の該当 IP アドレス端末のログアウトが行われ認証端末は未認証状態になります。

認証端末の確認は、"show access-defender client"コマンドで確認してください。

コマンドシンタックス

access-defender-logout ip <IPADDR>

IPADDR　　ログアウトさせる認証端末の IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) 認証端末(10.0.0.1)をログアウトさせます。

```
> enable
# access-defender-logout ip 10.0.0.1
```

関連コマンド

show access-defender client

注意事項

3.47.56 access-defender-logout mac

認証種別に関わらずログインした端末(本項内では以下認証端末)の強制ログアウト、または discard 登録の解除を行います。

認証端末の MAC アドレスを指定した場合、AccessDefender ログイン中の当該 MAC アドレス端末のログアウトが行われ認証端末は未認証状態になります。

また、discard 登録されている端末の MAC アドレスを指定した場合は、discard 登録の解除が行われます。

認証端末、及び discard 登録の確認は、"show access-defender client"コマンドで確認してください。

コマンドシンタックス

access-defender-logout mac <MACADDR>

MACADDR　　ログアウト、もしくは discard を解除させる認証端末の MAC アドレス

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) 認証端末(00:00:00:10:00:77)をログアウトさせます。

```
> enable
# access-defender-logout mac 00:00:00:10:00:77
```

関連コマンド

show access-defender client

注意事項

3.47.57 access-defender-logout user

認証種別に関わらずログインした認証端末の強制ログアウトを行います。

認証端末のユーザーID を指定した場合、AccessDefender ログイン中の当該ユーザーID 端末のログアウトが行われ認証端末は未認証状態になります。

また、discard 登録されている端末のユーザーID を指定した場合は、discard 登録の解除が行われます。

認証端末、及び discard 登録の確認は、"show access-defender client"コマンドで確認してください。

コマンドシンタックス

access-defender-logout user <USERID>

USERID　　ログアウトさせる認証端末のユーザーID <1-63(文字)>

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) 認証端末(ABCD)をログアウトさせます。

```
> enable
# access-defender-logout user ABCD
```

関連コマンド

show access-defender client

注意事項

3.47.58 port max-client

ポートごとに認証可能な接続端末数を設定します。設定を削除する場合は、no コマンドを使用してください。

ポートごとに認証可能な接続端末数を１から装置あたり最大数(機種ごとに異なる)まで設定できます。本コマンドで、接続端末数を制限しない場合は、１ポートにつき装置あたり最大数まで認証可能です。

コマンドシンタックス

port <PORTRANGE> max-client <NUMBER>
no port <PORTRANGE>

PORTRANGE	ポート番号(複数指定可能)
NUMBER	接続端末数 • Apresia4328 シリーズ：<1-512> • Apresia3400/4348/5400/13000-48X シリーズ：<1-1408> • Apresia13000-24GX シリーズ：<1-2816>

デフォルト

装置あたり最大数

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1 の接続端末数を 500 に制限します。
(2) ポート：1 の接続端末数を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# port 1 max-client 500
(config-a-def)# no port 1
```

関連コマンド

show running-config

注意事項

3.47.59 packet-filter2 max-rule

AccessDefender で使用するパケットフィルター2 の最大ルール数を設定します。AccessDefender を有効にするには最大ルール数を必ず設定する必要があります。設定を削除する場合は、no コマンドを使用してください。

AccessDefender では 1 端末につき 1 ルール使用します。本コマンドで、最大ルール数を設定することにより、認証可能な最大数を設定できます。

Apresia4328 シリーズでは使用グループ数は、最大ルール数が 1～128 ルールまで 4 個使用し、以降 128 ルール増加するたびに、使用グループが 1 つ増加します。よって、最大設定数 512 ルール設定時は 7 個のグループを使用します。

Apresia3400/4348/5400 シリーズ、Apresia13000-48X では使用グループ数は、最大ルール数が 1～128 ルール(端末)まで 4 個使用し、以降 128 ルール増加するたびに、使用グループが 1 つ増加します。よって、最大設定数 1408 ルール設定時は 14 個のグループを使用します。

Apresia13000-24GX では使用グループ数は、最大ルール数が 1～256 ルールまで 4 個使用し、以降 256 ルール増加するたびに、使用グループが 1 つ増加します。よって、最大設定数 2816 ルール設定時は 14 個のグループを使用します。詳しいルール数とグループ数については、表 3-22 AccessDefender で使用

するルール数とグループ数をご確認ください。
グループは、自動的に連番で予約されます。グループが連番で予約できない場合は、最大ルール数の設定は行えません。その場合は、グループを使用している他機能を変更するか、"packet-filter2 group"コマンドで先頭のグループ番号を変更してください。また、グループの予約状況は"show packet-filter2 reserved-group"コマンドで確認できます。
認証拒否機能("access-defender-deny")を使用する場合、deny-rule を設定する必要があります。

コマンドシンタックス

packet-filter2 max-rule <RULE1> [deny-rule <RULE2>]
no packet-filter2 max-rule

RULE1	パケットフィルター2 の最大ルール数 • Apresia4328 シリーズ：<1-512> • Apresia3400/4348/5400/13000-48X シリーズ：<1-1408> • Apresia13000-24GX シリーズ：<1-2816>
RULE2	deny-rule の最大ルール数 <1-128>

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) 認証可能な設定数を 100 ルールに設定します。
(2) 設定を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# packet-filter2 max-rule 100
(config-a-def)# no packet-filter2 max-rule
```

関連コマンド

show packet-filter2 reserved-group, show access-defender packet-filter2 rule-statistics, show running-config

注意事項

Web 認証、MAC 認証、IEEE 802.1X、DHCP Snooping のうちいずれか 1 つが有効である(enable に設定)場合、本コマンドを使用できません。

指定したルール数を確保するのに必要なグループが、連番で予約できない場合は、本コマンドは設定できません。

装置 1 台あたりの最大認証端末数はパケットフィルター2 の最大ルール数となります

(DHCP Snooping を除く)。ただし、端末の認証が同時に行われた場合の性能を保証するものではありません。

DHCP Snooping では、201 端末目以降(Apresia13000-24GX は 401 端末目以降)は 1 端末につき 2 ルール使用します。

例：最大ルール数が 1024 ルールの場合、DHCP Snooping では 612 端末が認証可能です。
ルール数の計算式(Apresia13000-48X の場合)
200 + (612 - 200) * 2 = 1024(ルール)

端末が使用するルールに空きがない場合、端末のログインは失敗し、装置の最大認証数によるログイン不可のログを出力します。

本装置再起動後は構成情報の記載順にパケットフィルター2 のグループが確保されます。他機能とグループ番号が重複しないよう、表 3-19 をご確認ください。
※"packet-filter2 group"への誘導は既に説明欄で行っているので変更不要。

3.47.60 packet-filter2 group

AccessDefender で使用するパケットフィルター2 の先頭グループ番号を設定します。設定を削除する場合は、no コマンドを使用してください。グループは"packet-filter2 max-rule"設定時に確保します。他機能で予約済みのグループは確保できません。

本設定がある場合は、指定した先頭グループ番号から昇順に、連番のグループを予約します。本設定がない場合は、未使用の最大グループ番号から降順に、連番のグループを予約します。

"web-authentication enable"、"mac-authentication enable"、"dhcp-snooping enable"、"dot1x enable"のいずれかが設定されている状態では、グループ番号を変更できません。グループの予約状況は 3.28.14 "show packet-filter2 reserved-group"コマンドで確認可能です。

コマンドシンタックス

packet-filter2 group <GROUP>
no packet-filter2 group

GROUP	先頭グループ番号 • Apresia4328 シリーズ：<1-4> • Apresia3400/4348/5400/13000 シリーズ：<1-11>

デフォルト

自動割り当て

コマンドモード

ACCESSDEFENDER

使用例

(1) パケットフィルター2の先頭グループ番号を4に指定します。
(2) 設定したグループ番号を削除します。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# packet-filter2 group 4
(config-a-def)# no packet-filter2 group
```

関連コマンド

show packet-filter2 reserved-group, show running-config

注意事項

Web認証、MAC認証、IEEE 802.1X、DHCP Snoopingのうちいずれか1つが有効である(enableに設定)場合、本コマンドを使用できません。

本装置再起動後は構成情報の記載順にパケットフィルター2 のグループが確保されます。他機能で確保済みのグループを本コマンドで指定した場合、AccessDefender機能は有効になりません。他機能とグループ番号が重複しないよう、表3-19をご確認ください。

3.47.61 roaming port enable

ローミング機能を有効にするポートを指定します。無効にする場合は、noコマンドを使用してください。本設定とリンクダウンログアウトを無効にする("logout linkdown port disable"コマンド)設定を併用することにより、リンクアグリゲーション、ポートリダンダントなどの冗長化ポートにおいて、認証済み端末の通信ポートがリンクダウンにより切り替わっても、ログアウトすることなく通信が継続されます。

本コマンドによりローミング機能のポートの設定を変更しても、すでにログイン中の端末のパケットフィルター2の設定は変わりません。

また、IEEE802.1X認証でSTPを併用する場合、本設定が必要となります。

コマンドシンタックス

[no] roaming port <PORTRANGE> enable

PORTRANGE	ポート番号(複数指定可能)

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) ポート：1のローミング機能を有効にします。

```
> enable
# configure terminal
(config)# access-defender
(config-a-def)# roaming port 1 enable
```

関連コマンド

show access-defender port-configuration, show running-config

注意事項

ローミングは、同一装置内の"roaming port enable"、同一の認証方式が設定されているポート間でのみ有効です。

AccessDefender のローミング機能は、3.46 NA 機能のローミング機能と以下の点で異なるためご注意ください。

(1) ローミング前のポートのリンクダウンによるログアウトが発生します。このログアウトを発生させたくない場合には、ローミング前のポートに"logout linkdown port disable"コマンドを設定してください。

(2) ローミングを行い接続ポートの変更をしても、"show access-defender client"で表示されるポート番号は、ログイン時のポート番号が表示されます(ローミング機能が有効なポートにはポート番号の先頭に*が付きます)。

設定変更により、ローミングポートの設定が変わっても変更以前にログインした端末はログアウトせず、設定変更以前のローミングポートの設定状態でログインしたままとなります。設定の変更が反映されるのは、変更後にログインした端末のみとなります。

ローミング機能が有効なポートで端末の認証が成功し、その後 VLAN が変更された場合、ローミング機能が有効なすべてのポートにおいて、変更後の VLAN のトラフィックが中継されます。

認証端末が存在しないローミングポートの認証を無効にした場合、他のローミングポートで認証を行った端末がログアウトするまで、動的な VLAN、及びクラス ID の変更は解除されません。動的な VLAN、及びクラス ID の変更を解除するためには、再起動、またはいったん認証を無効にしてください。

3.47.62 vlan mode dynamic port-base

本機能は、1 ポート 1VLAN で端末のログインを制限する機能です。設定を無効にする場合は、no コマンドを使用してください。

デフォルトでは、1 ポート複数 VLAN でログイン可能です。

本機能の特徴は以下です。

(1) 動的 VLAN は、ポートベース VLAN で設定されます。
(2) 最初にログインしている端末が同一インターフェースに存在している場合、後から認証を行う端末のログイン可否は、各端末の VLAN の状態によって決まります。詳細は表 3-49 に示します。
(3) MAC 認証の場合のみ、ログイン失敗と同時に DISCARD 登録されます。

表 3-49 各端末の VLAN の状態と後から認証を行う端末のログイン可否

ログイン中の端末	後から認証を行う端末	ログイン可否
装置に設定済みの VLAN	VLAN 指定なし	可
	VLAN 指定あり (ログイン中の端末と同じ VLAN)	可
	VLAN 指定あり (ログイン中の端末と異なる VLAN)	不可
装置に設定済みの VLAN と異なる VLAN	VLAN 指定なし	不可
	VLAN 指定あり (ログイン中の端末と同じ VLAN)	可
	VLAN 指定あり (ログイン中の端末と異なる VLAN)	不可

コマンドシンタックス

vlan mode dynamic port-base
no vlan mode

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) vlan mode を dynamic port-base に設定します。
(2) 設定を無効にします。

```
> enable
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# access-defender
(config-a-def)# vlan mode dynamic port-base
(config-a-def)# no vlan mode
```

関連コマンド

show access-defender client

注意事項

以下のいずれかが設定されている場合、本機能は設定できません。

- **web-authentication enable**
- **mac-authentication enable**
- **dot1x enable**
- **dhcp-snooping enable**

本機能設定時に MAC 認証と他の認証が同時に行われた場合、タイミングにより MAC 認証の VLAN 変更制限でログイン失敗となっても Discard 登録されない場合があります。ただし、その後の MAC 認証でログイン失敗となった際は、Discard 登録されます。

3.47.63 vlan mode static

認証に成功した端末がログインする VLAN のモードを設定します。static モードでは認証成功端末は装置に設定されたポート VLAN にログインします。設定を無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

vlan mode static
no vlan mode

デフォルト

なし(＝設定なし)

コマンドモード

ACCESSDEFENDER

使用例

(1) vlan mode を static に設定します。
(2) 設定を無効にします。

```
> enable
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# access-defender
(config-a-def)# vlan mode static
(config-a-def)# no vlan mode
```

関連コマンド

show access-defender client

注意事項

以下のいずれかが設定されている場合、本機能は設定できません。

- **web-authentication enable**
- **mac-authentication enable**
- **dot1x enable**

- **dhcp-snooping enable**

3.47.64 logging access-defender web-access on

認証 Web サーバーへのアクセスと HTTP/HTTPS/プロキシーリダイレクト機能を使用した場合のアクセスログを有効にします。設定を無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] logging access-defender web-access on

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) 認証 Web サーバーのアクセスログを有効にします。
(2) 認証 Web サーバーのアクセスログを無効にします。

```
> enable
# configure terminal
(config)# logging access-defender web-access on
(config)# no logging access-defender web-access on
```

関連コマンド

show running-config

注意事項

本コマンドを有効にした場合、認証 Web サーバーへのアクセスや HTTP/HTTPS/プロキシーリダイレクトが行われるたびにログが出力されます。

出力されるログメッセージの文字列の長さは最大 512 文字で、それ以降は切り捨てられます。

本コマンドはトラブルシューティング用のコマンドとなります。通常運用時には本機能を無効にしてください。また、使用する場合には、必ず事前にサポート対応窓口にご相談のうえ、指示に従ってください。

3.47.65 copy file WEB-PAGE

Web 認証に使用する各 Web ページを TFTP サーバー、または SD メモリーカードからダウンロードします。ダウンロードできるファイルサイズは 1 ファイルあたり最大 5 kbytes(5120 bytes)です。保存した Web ページを削除するには、erase コマンドを使用してください。

AccessDefenderでは、ログイン認証ページ、認証成功ページ、認証失敗ページ、ログアウト成功ページ、ログアウト失敗ページ、リダイレクト失敗ページの各ページをカスタマイズすることができます。カスタマイズの詳細は認証ページを参照してください。本コマンドでは、カスタマイズしたページを本装置に保存します。eraseコマンドを使用して保存したWebページを削除した場合は、デフォルトページ(工場出荷時の状態)が使用されます。

ログイン認証ページ	ユーザーID、パスワード
認証成功ページ	認証成功時に表示されるページ
認証失敗ページ	認証失敗時に表示されるページ
ログアウト成功ページ	ログアウト成功時に表示されるページ
ログアウト失敗ページ	ログアウト失敗時に表示されるページ
リダイレクト失敗ページ	リダイレクト失敗時に表示されるページ

コマンドシンタックス

copy (tftp <IPADDR>) | memory-card <FILENAME> login-page | login-success-page | login-failure-page | logout-success-page | logout-failure-page | redirect-error-page

erase login-page | login-success-page | login-failure-page | logout-success-page | logout-failure-page | redirect-error-page

IPADDR	TFTPサーバーのIPアドレス
FILENAME	ファイル名
login-page	ログイン認証ページ
login-success-page	認証成功ページ
login-failure-page	認証失敗ページ
logout-success-page	ログアウト成功ページ
logout-failure-page	ログアウト失敗ページ
redirect-error-page	リダイレクト失敗ページ

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) TFTPサーバー上のファイルを、ログイン認証ページに保存します。

(2) ログイン認証ページをデフォルトに戻します。

```
> enable
# copy tftp 172.21.29.110 login-success-page.html login-success-page
# erase login-success-page
```

(3) SDメモリーカードのファイルを、ログイン認証ページに保存します。

```
> enable
# copy memory-card login-success-page.html login-success-page
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

各種 Web ページのファイルに使用できる改行コードは LF、または CR+LF です。CR は使用できません。

3.47.66 copy WEB-PAGE file

本装置に保存されている各 Web ページを TFTP サーバー、または SD メモリーカードに保存します。

コマンドシンタックス

copy login-page | login-success-page | login-failure-page | logout-success-page | logout-failure-page | redirect-error-page (tftp <IPADDR>) | memory-card <FILENAME>

IPADDR	TFTP サーバーの IP アドレス
FILENAME	ファイル名
login-page	ログイン認証ページ
login-success-page	認証成功ページ
login-failure-page	認証失敗ページ
logout-success-page	ログアウト成功ページ
logout-failure-page	ログアウト失敗ページ
redirect-error-page	リダイレクト失敗ページ

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) ログイン認証ページを TFTP サーバーに保存します。

```
> enable
# copy login-success-page tftp 172.21.29.110 login-success-page.html
```

(2) ログイン認証ページを SD メモリーカードに保存します。

```
> enable
# copy login-success-page memory-card login-success-page.html
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.47.67 copy file aaa-local-db

TFTP サーバー、または SD メモリーカードに保存されている AccessDefender ローカルデータベース(ユーザーID、パスワード、VLAN ID)を本装置に保存します。保存したローカルデータベースを削除するには、erase コマンドを使用してください。

ローカルデータベースのフォーマットを表 3-50 AccessDefender ローカルデータベースフォーマット、その登録例を表 3-51 AccessDefender ローカルデータベースの登録例に示します。

コマンドシンタックス

```
copy ( tftp <IPADDR> ) | memory-card <FILENAME> aaa-local-db
erase aaa-local-db
```

IPADDR	TFTP サーバーの IP アドレス
FILENAME	ローカルデータベースファイル名

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) TFTP サーバー上のローカルデータベースを本装置に保存します。

(2) ローカルデータベースを削除します。

```
> enable
# copy tftp 172.21.29.110 local-db.txt aaa-local-db
# erase aaa-local-db
```

(3) SD メモリーカード上のローカルデータベースを本装置に保存します。

```
> enable
# copy memory-card local-db.txt aaa-local-db
```

関連コマンド

show access-defender aaa-local-db

注意事項

ローカルデータベースのファイルにおいて、改行のみの行がある場合、ダウンロードできません。ローカルデータベースのファイル中に改行のみの行を含めないでください。

表 3-50 AccessDefender ローカルデータベースフォーマット

項目	内容
形式	userid,password[,vid]の CSV 形式(userid、password は最大 63 文字)
最大登録行数	3000 行
最大ファイルサイズ	改行コード LF の場合：258032 バイト 改行コード CR+LF の場合：(ファイルサイズ － 登録行数) ≦ 258032 を満たすサイズ

表 3-51 AccessDefender ローカルデータベースの登録例

```
temp01,temp01,10
temp02,temp02
temp03,temp03,30
00096b82c51e,1q2w3d,100
```

MAC ベース認証の場合、MAC アドレス(16 進文字列、区切り文字無しの 16 文字)を、ユーザーID として登録してください。なお、アルファベットは小文字(a-f)で記述する必要があります。

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

ローカルデータベースの最終行に改行を入れてください。使用できる改行コードは LF、または CR+LF です。CR は使用できません。

重複したユーザーID のエントリーが含まれるローカルデータベースは本装置に保存できません。

Apresia4300 シリーズにおいて、7.11.04 以前のファームウェアでダウンロードした local-db は、ファームウェアの更新後に使用できなくなります。
ファームウェアの更新後に、TFTP サーバーから local-db を再度ダウンロードしてください。更新手順については以下をご参考ください。

(1) ローカル DB を"copy aaa-local-db file"コマンドで TFTP サーバーにアップロード
(2) ファームウェアをバージョンアップ
(3) バージョンアップ後、装置をリブートする
(4) (1)のローカル DB を"copy file aaa-local-db"コマンドで機器へダウンロード

3.47.68 copy aaa-local-db file

本装置に保存されている AccessDefender ローカルデータベース(ユーザーID、パスワード、VLAN ID)を TFTP サーバー、または SD メモリーカードに保存します。

コマンドシンタックス

copy aaa-local-db (tftp <IPADDR>) | memory-card <FILENAME>

IPADDR	TFTP サーバーの IP アドレス
FILENAME	ローカルデータベースファイル名

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) 本装置に保存されているローカルデータベースを TFTP サーバーへ保存します。

```
> enable
# copy aaa-local-db tftp 172.21.29.110 local-db.txt
```

(2) 本装置に保存されているローカルデータベースを SD メモリーカードへ保存します。

```
> enable
# copy aaa-local-db memory-card local-db.txt
```

関連コマンド

show access-defender aaa-local-db

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

Apresia4300 シリーズにおいて、7.11.04 以前のファームウェアでダウンロードした local-db は、ファームウェアの更新後に使用できなくなります。
ファームウェアの更新後に、TFTP サーバーから local-db を再度ダウンロードしてください。更新手順については以下をご参考ください。

(1) ローカル DB を"copy aaa-local-db file"コマンドで TFTP サーバーにアップロード
(2) ファームウェアをバージョンアップ
(3) バージョンアップ後、装置をリブートする
(4) (1)のローカル DB を"copy file aaa-local-db"コマンドで機器へダウンロード

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.47.69 aaa-local-db add user

本装置に保存されている AccessDefender ローカルデータベースにエントリー(ユーザーID、パスワード、VLAN ID)を追加します。<PASSWORD>省略時はパスワード無しとして、<VID>省略時は VLAN ID：0 として登録されます。

コマンドシンタックス

aaa-local-db add user <USERID> [password <PASSWORD>] [vlan <VID>]

USERID	ユーザーID <1-63(文字)> • ASCII コードの印字可能な文字の内、 ,、|、?、空白文字を除いた文字のみ使用可能 • ダブルクォーテーションで囲めば、|、空白文字を使用可能
PASSWORD	パスワード <1-63(文字)> • ASCII コードの印字可能な文字の内、 ,、|、?、空白文字を除いた文字のみ使用可能 • ダブルクォーテーションで囲めば、|、空白文字を使用可能
VID	VLAN ID <1-4094>

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) ローカルデータベースにユーザーID：apresia、パスワード：apresia のエントリーを追加します。

```
> enable
# aaa-local-db add user apresia password apresia
Writing to flash memory...
done.
```

関連コマンド

show access-defender aaa-local-db

注意事項

3.47.70 aaa-local-db del user

本装置に保存されている AccessDefender ローカルデータベースのエントリーを削除します。

コマンドシンタックス

aaa-local-db del user <USERID>

USERID	ユーザーID <1-63(文字)> • ASCII コードの印字可能な文字の内、 ,、|、?、空白文字を除いた文字のみ使用可能 • ダブルクォーテーションで囲めば、|、空白文字を使用可能

デフォルト

なし(＝設定なし)

コマンドモード

ENABLE

使用例

(1) ローカルデータベースのユーザーID：apresia のエントリーを削除します。

```
> enable
# aaa-local-db del user apresia
Writing to flash memory...
done.
```

関連コマンド

show access-defender aaa-local-db

注意事項

3.47.71 show access-defender aaa-local-db

AccessDefender 機能のローカルデータベースに保存されている内容を表示します。

コマンドシンタックス

show access-defender aaa-local-db

コマンドモード

VIEW, ENABLE

使用例

(1) AccessDefender ローカルデータベース情報を表示します。

```
> enable
# show access-defender aaa-local-db
----------------------------------------------------------------------
No. Username                                                      VID
----------------------------------------------------------------------
1   user1                                                          10
2   user2                                                          20
3   user3                                                          30
4   user4                                                          40
5   user5                                                          50
6   user6                                                          60
----------------------------------------------------------------------
```

Username　　：ローカルデータベースに保存されたユーザー名
VID　　：ローカルデータベースに保存された VLAN ID

関連コマンド

注意事項

3.47.72 show access-defender client

認証済み端末、discard 状態の端末を表示します。

コマンドシンタックス

show access-defender client [port <PORTRANGE>] [type <TYPE>]

PORTRANGE　　ポート番号(複数指定可能)
TYPE　　認証タイプ
dhcp-snooping：DHCP Snooping 端末の指定
disc　　：認証失敗端末の指定
dot1x　　：IEEE802.1X 認証成功端末の指定
gateway　　：ゲートウェイ認証成功端末の指定
(Apresia13000 シリーズのみ)

mac　　：MAC 認証成功端末の指定
web　　：Web 認証成功端末の指定

コマンドモード

VIEW, ENABLE

使用例

(1) 認証済み端末、discard 状態の端末を表示します。

```
> enable
# show access-defender client
Total number of Clients          :    6
Total number of Discarded Clients :    0

   Codes: W = web-authentication, G = web-authentication gateway,
          M = mac-authentication, - = mac-authentication (discard),
          X = IEEE802.1X, D = DHCP snooping,
          WD = web-authentication & DHCP snooping,
          MD = mac-authentication & DHCP snooping,
          XD = IEEE802.1X & DHCP snooping

   MAC address       IP              Port  VID       Time    Aging User
-----------------------------------------------------------------------
W  00:1d:09:a3:80:18 172.17.100.150    48   51    0:21:16  0:00:00 webuser01
W  00:1d:09:d1:17:07 172.17.100.149    47   51    0:21:19  0:00:00 webuser01
W  00:17:a4:d6:b3:a5 172.170.100.200    2   10    0:20:45  0:00:00 webuser02
X  00:17:a4:d6:b3:a5 0.0.0.0            2 4094    0:20:50  0:00:00 dlxuser02
W  00:17:a4:d6:b3:a6 172.170.100.201    3   10    0:22:00  0:00:00 webuser03
XD 00:17:a4:d6:b3:a6 172.170.100.201    3 4094    0:21:00  0:00:00 dlxuser03
```

MAC address　　：認証端末の MAC アドレス
IP　　：ログイン時の認証端末の IP アドレス
Port　　：認証端末のポート番号(ローミングが有効な場合は左に"*"が付きます)
VID　　：認証端末の VLAN ID
Time　　：認証成功からの経過時間
Aging　　：本装置との無通信時間
User　　：認証端末のユーザー名

※ 併用認証端末と DHCP Snooping 共通の端末が存在する場合、通信可能な端末が"WD"、"XD"の表示になります。

関連コマンド

注意事項

動的に VLAN が割り当てられた認証端末から、動的な VLAN が割り当てられていないユーザー名で再ログインした場合、再ログイン前の VLAN ID が表示されます。

ユーザー名は 63 文字まで表示されますが、一行に収まらない場合は折り返して表示されます。

Aging 時間は、5 秒ごとに更新されます。

3.47.73 show access-defender deny

認証拒否端末の情報を表示します。

コマンドシンタックス

show access-defender deny

コマンドモード

VIEW, ENABLE

使用例

(1) 認証拒否端末の情報を表示します。

```
> enable
# show access-defender deny
Total number of Denied Clients    :    4

   MAC address       IP                  Timer
  ---------------------------------------------
   00:00:00:00:00:10 0.0.0.0            0:02:50
   00:00:00:00:00:20 0.0.0.0            0:02:54
   00:00:00:00:00:00 192.168.10.1       0:04:52
   00:00:00:00:00:00 192.168.20.1       0:04:57
```

MAC address　　：認証拒否端末の MAC アドレス
IP　　：認証拒否端末の IP アドレス
Timer　　：認証拒否設定の残り時間

関連コマンド

注意事項

3.47.74 show access-defender dot1x

IEEE 802.1X の情報を表示します。

本コマンドでポート指定した場合、ログイン認証端末の情報のみ表示し、ポート指定が無い場合は、ログイン済/未済に関わらず接続した端末の情報が表示されます。

コマンドシンタックス

show access-defender dot1x [port <PORTRANGE>]

PORTRANGE　　ポート番号(複数指定可能)

コマンドモード

VIEW, ENABLE

使用例

(1) IEEE 802.1X の情報を表示します。

```
> enable
# show access-defender dot1x
802.1X Port-Based Authentication Enabled
802.1X info for interface port1
  Supplicant name: user1
  Supplicant address: 00ac.1164.6600
  portEnabled: true - portControl: Auto
  portStatus: authorized - currentId: 9
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:T
  PAE: state: Authenticated - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 1
  PAE: quietPeriod: 60 - reauthMax: 3 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 8
  BE: suppTimeout: 30 - serverTimeout: 310 - maxReq: 2
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

802.1X Port-Based Authentication　：dot1x system-auth-ctrl の設定状態
　Enabled　：有効
　Disabled　：無効
802.1X info for interface <port name>　：802.1X 情報を表示するポート番号
　<port name>は"port"の後にポート番号を付けた文字列
Supplicant name　：Supplicant のユーザーID(ユーザーID 取得後に表示)
Supplicant address　：Supplicant の MAC アドレス(MAC アドレス取得後に表示)
portEnabled　：Link 状態
　true　：Linkup 検出済("true"固定)
portControl　：dot1x port-control の認証モード
　Auto　：自動モード
　Force Authorized　：強制認証モード
portStatus　：Supplicant の認証状態
　unauthorized　：未認証状態
　authorized　：認証済状態
currentId　：Supplicant に最後に送信した現時点のリクエスト ID
reAuthenticate　：dot1x reauthentication の設定状態
　enabled　：有効
　disabled　：無効
reAuthPeriod　：再認証間隔(デフォルト：3600 秒)

abort　　：abort 処理状態
　T　　：abort 処理中
　F　　：abort 処理中でない
fail　　：EAP-Fail の送信の有無
　T　　：あり
　F　　：なし
start　　：認証処理(開始)状態
　T　　：認証処理中
　F　　：認証処理中でない
timeout　　：タイムアウト発生の有無
　T　　：発生中
　F　　：未発生
success　　：認証(成功)状態
　T　　：認証成功
　F　　：認証成功でない(認証失敗に限らず、認証前、認証中も含む)
PAE: state　　：Port Access Entity(Supplicant の状態管理)の現在の状態
　Down　　：ダウン状態
　Init　　：初期化中
　Disconnected　　：コネクション非接続
　Connecting　　：コネクション接続中
　Authenticating　　：認証中
　Authenticated　　：認証済
　Aborting　　：abort 中
　Held　　：EAPoL-Fail 送信
PAE: portMode　　：ポートモード
　Auto　　：auto 設定
　Force Authorized　　：強制認証モード
PAE: reAuthCount　　：Supplicant へのリクエスト ID 送信リトライ回数(初回送信を含む)
PAE: rxRespId　　：Supplicant からのレスポンス受信の状態
　1　　：受信済
　0　　：受信未済
PAE: quietPeriod　　：Supplicant からのレスポンス受信の状態(認証処理中の異常により EAPoL-Fail を送信してから再度リクエスト ID を送信するまでの時間：60 秒固定)
PAE: reauthMax　　：Supplicant へのリクエスト ID 最大送信回数
PAE: txPeriod　　：Supplicant へのリクエスト ID 送信間隔
BE: state　　：Backend 認証状態(Apresia の Supplicant ごとの状態)
　Invalid　　：無効
　Request　　：リクエスト送信済
　Response　　：レスポンス受信済
　Success　　：認証成功
　Fail　　：認証失敗
　Timeout　　：応答タイムアウト
　Idle　　：アイドル

Initializing	：初期化中
BE: reqCount	：suppTimeout の時間内の Supplicant へのリクエスト ID 送信回数
BE: idFromServer	：RADIUS サーバーから受信したパケットの現時点のリクエスト ID
BE: suppTimeout	：Supplicant の応答待ち時間(デフォルト：30 秒)
BE: serverTimeout	：RADIUS サーバーの応答待ち時間(固定値：310 秒)
BE: maxReq	：suppTimeout の時間内の Supplicant へのリクエスト ID 最大送信回数(デフォルト：2 回)
CD: adminControlledDirections	：未認証時のパケットを廃棄する方向
in	：Supplicant からの受信パケットのみ廃棄
both	：Supplicant からの受信パケット、及び Supplicant への送信パケット両方を廃棄("both"は未サポートのため"in"固定)
CD: operControlledDirections	：未サポート("in"固定)
CD: bridgeDetected	：未サポート("false"固定)
KR: rxKey	：未サポート("false"固定)
KT: keyAvailable	：未サポート("false"固定)
KT: keyTxEnabled	：未サポート("false"固定)

関連コマンド

注意事項

3.47.75 show access-defender dot1x statistics port

IEEE 802.1X のポートごとの統計情報を表示します。

コマンドシンタックス

show access-defender dot1x statistics port <PORTRANGE>

PORTRANGE　　ポート番号(複数指定可能)

コマンドモード

VIEW, ENABLE

使用例

(1) ポートごとの IEEE 802.1X 統計情報を表示します。

```
> enable
# show access-defender dot1x statistics port 1
802.1X statistics for interface port1
  EAPOL Frames Rx: 24 - EAPOL Frames Tx: 0
  EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
  EAP Rsp/Id Frames Rx: 12 - EAP Response Frames Rx: 12
  EAP Req/Id Frames Tx: 2 - EAP Request Frames Tx: 12
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
```

関連コマンド

注意事項

3.47.76 show access-defender dhcp-snooping configuration

DHCP Snooping の設定状態を表示します。

コマンドシンタックス

show access-defender dhcp-snooping configuration

コマンドモード

VIEW, ENABLE

使用例

(1) DHCP Snooping 機能の設定状態を表示します。

```
# show access-defender dhcp-snooping configuration
 Port Config (*:snooping ON)
  No: 1      8 9     16 17    24 25    32 33    40 41    48 49
      +------+ +------+ +------+ +------+ +------+ +------+ +-
      ******** ****
 Snooping: DISABLE
 Mode : PERMIT Mode
 Timer : 1800

 Internal DHCP VLAN : none

 Lease-limit:
 Port       1    2    3    4    5    6    7    8
       ----------------------------------------
 limit   1608 1608 1608 1608 1608 1608 1608 1608

 Port       9   10   11   12   13   14   15   16
       ----------------------------------------
 limit   1608 1608 1608 1608    -    -    -    -

 Port      17   18   19   20   21   22   23   24
       ----------------------------------------
 limit      -    -    -    -    -    -    -    -

 Port      25   26   27   28   29   30   31   32
       ----------------------------------------
 limit      -    -    -    -    -    -    -    -

 Port      33   34   35   36   37   38   39   40
```

```
        ---------------------------------------
limit      -    -    -    -    -    -    -    -

Port      41   42   43   44   45   46   47   48
        ---------------------------------------
limit      -    -    -    -    -    -    -    -

Port      49   50
        ----------
limit      -    -

Lease-total-limit: 0

Static-Entry:
Port  IP Address
---------------------
  1   192.168.1.10
  2   192.168.1.20
```

Port Config　　：DHCP Snooping を行うポート
Snooping　　：DHCP Snooping の有効/無効
Mode　　：DHCP Snooping の設定モード
Timer　　：PERMIT モードから DENY モードに切り替わるまでの時間
Internal DHCP VLAN　　：DHCP サーバー機能併用 VLAN インターフェース
Lease-limit　　：各ポートのクライアントの制限数
Lease-total-limit　　：装置全体でのクライアントの制限数
Static-Entry　　：登録されている静的フィルター一覧

関連コマンド

注意事項

3.47.77 show access-defender dhcp-snooping mode-status

DHCP Snooping の現在の動作モード状態を表示します。

コマンドシンタックス

show access-defender dhcp-snooping mode-status

コマンドモード

VIEW, ENABLE

使用例

(1) DHCP Snooping の動作モード状態を表示します。

```
> enable
# show access-defender dhcp-snooping mode-status
```

```
Mode      Timer         Remaining time
 -------------------------------------
 PERMIT    0:00:30:00    0:00:00:20
 MAC AUTH  -:--:--:--    -:--:--:--
```

Mode　　：現在の DHCP Snooping の動作モード
Timer　　：DENY モードに切り替わるまでの設定時間
Remaining time　：DENY モードに切り替わるまでの残り時間

関連コマンド

注意事項

Remaining time は 10 秒ごとに更新されます。

3.47.78 show access-defender dhcp-snooping status

DHCP Snooping の現在の状態を表示します。

コマンドシンタックス

show access-defender dhcp-snooping status

コマンドモード

VIEW, ENABLE

使用例

(1) DHCP Snooping のステータスを表示します。

```
> enable
# show access-defender dhcp-snooping status
 Snooping: ENABLE
 Mode : PERMIT Mode
 Mode : MAC Authentication Mode

Total : 1 (static 0, dynamic 1)
Port  IP Address      MAC Address        Lease Expiration
-------------------------------------------------------------
  2   172.17.100.250  00:1D:09:D1:14:55  2009/06/08 17:33:35
```

Snooping　　：DHCP Snooping の有効/無効
Mode　　：DHCP Snooping の動作モード
Total　　：現在のクライアントの総数
Static　　：現在の静的なクライアントの総数
dynamic　　：現在の動的なクライアントの総数
Port　　：クライアントの接続先ポート
IP Address　　：クライアントにリースしている IP アドレス
MAC Address　　：クライアントの MAC アドレス

Lease Expiration　　：リース満了時間
(static：静的フィルター。リース満了時間は無期限)

関連コマンド

注意事項

3.47.79 show access-defender packet-filter2 rule-statistics

AccessDefender 機能で使用する、パケットフィルター2 のルール使用状況を表示します。

コマンドシンタックス

show access-defender packet-filter2 rule-statistics

コマンドモード

VIEW, ENABLE

使用例

(1) パケットフィルター2 のルール使用状況を表示します。

```
> enable
# show access-defender packet-filter2 rule-statistics
Total Rules       : 1408
Unused Rules      : 0
Used Rules        : 1408
                                          Rule  Client
              ----------------------------------------
               web-authentication            0       0
               web-authentication gateway    0       0
               mac-authentication         1408    1408
               IEEE802.1X                    0       0
               DHCP snooping                 0       0
              ----------------------------------------
```

Total Rules　　：パケットフィルター2 の最大ルール数
Unused Rules　　：パケットフィルター2 の未使用ルール数
Used Rules　　：パケットフィルター2 の使用ルール数
Rule　　：認証方式ごとの使用ルール数
Client　　：認証方式ごとの認証済端末数

関連コマンド

注意事項

web-authentication gateway は、Apresia13000 シリーズでのみ表示されます。

Web/IEEE802.1X 認証(AND)端末の Client 数はそれぞれの認証方式に計上され、Rule

数は最後に認証された方の認証方式に計上されます。

例(IEEE802.1X 認証→Web 認証の順番で認証された場合)

1. 認証前の状態

```
# show access-defender packet-filter2 rule-statistics
Total Rules  : 1024
Unused Rules : 1024
Used Rules   : 0
                                          Rule  Client
              ----------------------------------------
               web-authentication            0       0
               web-authentication gateway    0       0
               mac-authentication            0       0
               IEEE802.1X                    0       0
               DHCP snooping                 0       0
              ----------------------------------------
```

2. IEEE802.1X 認証完了時 IEEE802.1X 認証の Client に 1 加算

```
# show access-defender packet-filter2 rule-statistics
Total Rules  : 1024
Unused Rules : 1024
Used Rules   : 0
                                          Rule  Client
              ----------------------------------------
               web-authentication            0       0
               web-authentication gateway    0       0
               mac-authentication            0       0
               IEEE802.1X                    0       1
               DHCP snooping                 0       0
              ----------------------------------------
```

3. Web 認証完了時 Web 認証の Client に 1 加算、Web 認証の使用 Rule 数に 1 加算

```
# show access-defender packet-filter2 rule-statistics
Total Rules  : 1024
Unused Rules : 1023
Used Rules   : 1
                                          Rule  Client
              ----------------------------------------
               web-authentication            1       1
               web-authentication gateway    0       0
               mac-authentication            0       0
               IEEE802.1X                    0       1
               DHCP snooping                 0       0
              ----------------------------------------
```

3.47.80 show access-defender port-configuration

AccessDefender 機能で使用するポートの設定状態を表示します。

コマンドシンタックス

show access-defender port-configuration

コマンドモード

VIEW, ENABLE

使用例

(1) ポートの AccessDefender 機能設定状態を表示します。

```
> enable
# show access-defender port-configuration
AccessDefender Port Configuration:
  web = web-authentication, gateway = web-authentication gateway
  mac = mac-authentication, 802.1X = IEEE802.1X, DHCPSNP = DHCP snooping,
  web/.1X = web/IEEE802.1X authentication,
  LD LO = Linkdown Logout, TTL = web-authentication ttl filter,
  ld time = logout linkdown time,
  o = enable, x = disable
 Port   :
        : 1      8 9      16 17     24 25     32 33     40 41     48 49
        : +------+ +------+ +------+ +------+ +------+ +------+ +-
 web    : oooooooo oooooooo ........ ........ ........ ........ ..
 gateway: ........ ........ oooooooo oooooooo ........ ........ ..
 mac    : ........ oooooooo ........ ........ oooooooo ........ ..
 802.1X : ........ oooooooo ........ ........ oooooooo ........ ..
 DHCPSNP: ........ oooooooo ........ ........ ........ ........ ..
 roaming: oooooooo oooooooo ........ oooooooo oooooooo oooooooo ..
 LD LO  : xxxxxxxx xxxxxxxx ........ xxxxxxxx ........ xxxxxxxx ..
 ld time: oooooooo oooooooo ........ ........ ........ ........ ..
 web/.1X: ........ ........ ........ ........ ........ oo...... ..
 TTL 255: ........ oooooooo ........ ........ ........ ........ ..
```

関連コマンド

注意事項

gateway は、Apresia13000 シリーズでのみ表示されます。

Web/IEEE802.1X 認証(AND)に設定されているポートは Web/MAC 認証(AND)、IEEE 802.1X/MAC 認証(AND)との併用状態の場合もすべて web/.1X として表示されます。

3.47.81 show tech-support access-defender

AccessDefender 機能の各種情報を収集し表示します。本コマンドで表示する内容は、表 3-52 に示すコマンドが収集している情報、及び装置内部のダンプ情報(独自形式で表示)です。system-dump オプションを指定した場合、装置内部のダンプ情報を詳細に取得します。

表 3-52 コマンドにより収集可能な AccessDefender 情報

show system
show version
show access-defender aaa-local-db
show access-defender deny
show access-defender dhcp-snooping configuration
show access-defender dhcp-snooping mode-status
show access-defender dhcp-snooping status
show access-defender packet-filter2 rule-statistics
show access-defender port-configuration
show access-defender dot1x
show access-defender dot1x statistics port
show access-defender client ※1
show interface counters ※1

※1 10 秒おきに 2 回情報を取得

コマンドシンタックス

show tech-support access-defender [system-dump]

system-dump　　詳細な装置内部のダンプ情報を出力

コマンドモード

ENABLE

関連コマンド

注意事項

system-dump オプションを指定した場合、装置の性能、及び通信に対して影響を及ぼす可能性があります。使用する場合には、必ず事前にサポート対応窓口へご相談のうえ、指示に従ってください。

3.47.82 認証ページ

認証ページをカスタマイズするポイント、外部の Web サーバー上の任意のページでユーザー認証ページを表示・実行するポイントを示します。

3.47.82.1 認証ページのカスタマイズ

ポイントは以下です。

(1) ユーザー名、パスワードの変数名をそれぞれ name、pass にする。
(2) form の method を POST に指定する。
(3) 未認証端末から外部の Web サーバーに対する通信を許可しておく。
(4) 認証 URL が FQDN(Fully Qualified Domain Name)の場合には DNS サーバーへの通信も許可しておく。

ログイン用の form 例

```
<form method="POST" action="/cgi-bin/adeflogin.cgi">
<table summary="login form" width="230" style="text-align:center;">
<tr>
<td style="text-align:center">
<span style="font: bold medium Verdana, Arial, Helvetica, sans-serif; color:#FFFFFF; ">
User ID</span>
</td>
<td style="text-align:center">
<input name="name" type="text" value="" size="30" maxlength="63">
</td></tr>
<tr>
<td style="text-align:center">
<span style="font: bold medium Verdana, Arial, Helvetica, sans-serif; color:#FFFFFF; ">
Password</span>
</td>
<td style="text-align:center">
<input name="pass" type="password" size="30" maxlength="63">
</td></tr>
<tr>
<td colspan="2">
<input type="submit" name="action" value="login">
<input type="reset" value="reset">
</td></tr>
</table>
</form>
```

ログアウト用の form 例

```
<form method="POST" action="/cgi-bin/adeflogout.cgi">
<input type="submit" name="action" value="logout">
</form>
```

3.47.82.2 外部サーバー

Web 認証用 CGI は本装置内部のファームウェアに実装されているため、CGI そのものを別サーバーで実行することはできません。ユーザー認証ページの form の action を「/cgi-bin/adeflogin.cgi」から「http://AccessDefender 認証用 IP アドレス:port/cgi-bin/adeflogin.cgi」に変更することで外部の Web サーバー上の任意のページでユーザー認証ページを表示・実行することが可能となります(SSL 有効時には「https://AccessDefender 認証用 IP アドレス:port/cgi-bin/adeflogin.cgi」)。

ポイントは以下です。

(1) form の action を本装置の認証 CGI に指定する。
(2) ユーザー名、パスワードの変数名をそれぞれ name、pass にする。
(3) form の method を POST に指定する。
(4) 未認証端末から外部の Web サーバーに対する通信を許可しておく。
(5) 認証 URL が FQDN(Fully Qualified Domain Name)の場合には DNS サーバーへの通信も許可しておく。

認証 URL の設定が「http://192.0.2.1:8080」の場合に外部のページに埋め込むフォームの例を示します。

ログイン用の form 例

```
<form method="POST" action="http://192.0.2.1:8080/cgi-bin/adeflogin.cgi">
<table summary="login form" width="230" style="text-align:center;">
<tr>
<td style="text-align:center">
<span style="font: bold medium Verdana, Arial, Helvetica, sans-serif; color:#FFFFFF; ">
User ID</span>
</td>
<td style="text-align:center">
<input name="name" type="text" value="" size="30" maxlength="63">
</td></tr>
<tr>
<td style="text-align:center">
<span style="font: bold medium Verdana, Arial, Helvetica, sans-serif; color:#FFFFFF; ">
Password</span>
</td>
<td style="text-align:center">
<input name="pass" type="password" size="30" maxlength="63">
</td></tr>
<tr>
<td colspan="2">
<input type="submit" name="action" value="login">
<input type="reset" value="reset">
</td>
</tr></table>
</form>
```

ログアウト用の form 例

```
<form method="POST" action="http://192.0.2.1:8080/cgi-bin/adeflogout.cgi">
<input type="submit" name="action" value="logout">
</form>
```

3.47.83 RADIUS 属性

本項目は、3.46 NA 機能、AccessDefender 機能における、RADIUS サーバーとの認証要求・応答の属性項目を参考情報として示しています。装置で設定や表示を行うものではありません。

3.47.83.1 認証要求属性

表 3-53 NA 機能、AccessDefender 機能(Web 認証、MAC 認証)で使用する RADIUS 属性

属性	実装
User-Name	認証されるユーザー名
User-Password	パスワード
NAS-Port	認証端末が接続されているインターフェース番号
Calling-Station-Id	認証端末の MAC アドレス
NAS-Identifier	認証された端末が属している VLAN ID
NAS-IP-Address	認証要求している RADIUS クライアントの IP アドレス

表 3-54 AccessDefender 機能(IEEE 802.1X)で使用する RADIUS 属性

属性	実装
User-Name	認証されるユーザー名
Service-Type	提供するサービスタイプ(Framed-User(2)固定)
Framed-MTU	サプリカントと Authenticator 間の最大フレームサイズ(1452 固定)
NAS-IP-Address	認証要求している Authenticator の IP アドレス
NAS-Port	サプリカントが接続されている Authenticator のインターフェース番号
NAS-Port-Type	ユーザー認証に使用しているインターフェースのタイプ(Ethernet(15)固定)
Calling-Station-Id	サプリカントの MAC アドレス
EAP-Message	EAP メッセージの送受信に使用
Message-Authenticator	RADIUS パケットの内容を保証するために使用
State	Authenticator と RADIUS サーバー間の State 情報の保持

3.47.83.2 認証応答属性

表 3-55 動的な VLAN 変更で使用する RADIUS 属性(Web 認証、MAC 認証)

属性番号	値	属性の型
192 ※	割り当てる VID	整数(INTEGER)

※ 属性番号 192 を NA-VLAN-ID として使用

表 3-56 動的な VLAN 変更で使用するベンダー独自属性(Web 認証、MAC 認証)

属性	独自属性の値	実装
Vendor-Specific	ベンダーID	278
	ベンダー属性番号	192
	値	割り当てる VLAN ID
	属性の型	整数(INTEGER)

表 3-57 動的な VLAN 変更で使用する RADIUS 属性(IEEE 802.1X)

属性名	実装
Tunnel-Type	動的 VLAN 割り当て用応答属性(VLAN(13)に設定)
Tunnel-Medium-Type	動的 VLAN 割り当て用応答属性(IEEE 802(6)に設定)
Tunnel-Private-Group-ID	動的 VLAN 割り当て用応答属性(割り当てる VLAN ID、または VLAN 名) • 1-4094 の数値を指定した場合、VLAN ID として扱う (例)"1"、"01"、"4094" • それ以外の場合、VLAN 名として扱う (例)"0"、"00"、"1"、"VLAN10"

3.48 SNMP

注意事項

SNMP レスポンスパケットの送信元 IP アドレスは、SNMP リクエストパケットの宛先 IP アドレスにかかわらず、SNMP レスポンスパケットを送信するインターフェースの IP アドレスとなります。

3.48.1 snmp-server disable

SNMP を無効にします。有効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] snmp-server disable

デフォルト

no disable(＝有効)

コマンドモード

CONFIG

使用例

(1) SNMP を無効にします。
(2) SNMP を有効にします。

```
> enable
# configure terminal
(config)# snmp-server disable
(config)# no snmp-server disable
```

関連コマンド

show snmp-server, show running-config

注意事項

端末より装置にログインし、CONFIG モードに入っている場合は SNMP による MIB の設定が失敗することがあります。

3.48.2 snmp-server community

MIB へのアクセスを許可する SNMP マネージャーに関する設定を行います。設定を削除する場合は、no コマンドを使用してください。コミュニティー名が一致し、Read Only、Read/Write 管理マネージャーの IP アドレスに設定された管理マネージャーのみ MIB へアクセス可能です。これらの項目が設定されていない場合、コミュニティー名が一致するすべての SNMP マネージャーからのアクセスが許可されま

す。

コミュニティー名は、指定したコミュニティー以外を設定したSNMPマネージャーからのMIB取得/設定を拒否するためのパラメーターであり、MIBに対するアクセス権によってRead OnlyとRead/Writeの2種類を指定可能です。Read OnlyとRead/Writeに同一のコミュニティー名を設定した場合は、Read Onlyと同一の動作になります。

コミュニティー名は、ASCII 文字を使用し 127 文字以内で設定してください。SNMP マネージャーは、Read Only、Read/Write それぞれ 20 個ずつ設定できます。

コマンドシンタックス

```
snmp-server community ro | rw <NAME> <IPADDR> | <IPADDR/MASK> | ( <IPADDR> <NETMASK> )
no snmp-server community ro | rw [ <NAME> ] [ <IPADDR> ]
```

ro	Read Only
rw	Read/Write
NAME	コミュニティー名 <1-127(文字)>
IPADDR	IPアドレス
MASK	ネットマスク長
NETMASK	ネットマスク

デフォルト

Read Only マネージャーのコミュニティー名 ：public
Read/Write マネージャーのコミュニティー名：private

コマンドモード

CONFIG

使用例

(1) Read Only マネージャーのコミュニティー名を Manager1 に、IP アドレスを 192.168.1.100 に設定します。
(2) Read/Write マネージャーのコミュニティー名を Manager2 に、IP アドレスを 192.168.2.200/24 に設定します。
(3) コミュニティー名が Manager1、IP アドレスが 192.168.1.100 の Read Only マネージャーを削除します。
(4) コミュニティー名が Manager1 である Read Only マネージャーをすべて削除します。
(5) Read Only マネージャーをすべて削除し、デフォルトに戻します。

```
> enable
# configure terminal
(config)# snmp-server community ro Manager1 192.168.1.100
(config)# snmp-server community rw Manager2 192.168.2.200/24
(config)# no snmp-server community ro Manager1 192.168.1.100
(config)# no snmp-server community ro Manager1
(config)# no snmp-server community ro
```

関連コマンド

show snmp-server, show running-config

注意事項

3.48.3 snmp-server access-disable

MIB へのアクセス禁止を設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。read-write オプションを指定した場合、Read Only、及び Read/Write マネージャーからのアクセスが禁止され、MIB の取得/設定ができなくなります。write オプションを指定した場合、Read/Write マネージャーからのアクセスが禁止され、MIB の取得/設定ができなくなります。

コマンドシンタックス

snmp-server access-disable read-write | write
no snmp-server access-disable

read-write	Read Only、及び Read/Write マネージャー
write	Read/Write マネージャー

デフォルト

no disable(＝Read Only、及び Read/Write マネージャーからのアクセスを許可)

コマンドモード

CONFIG

使用例

(1) Read Only、及び Read/Write マネージャーをアクセス禁止に設定します。
(2) Read/Write マネージャーをアクセス禁止に設定します。
(3) Read Only、及び Read/Write マネージャーのアクセス禁止を解除します。

```
> enable
# configure terminal
(config)# snmp-server access-disable read-write
(config)# snmp-server access-disable write
(config)# no snmp-server access-disable
```

関連コマンド

show snmp-server, show running-config

注意事項

3.48.4 snmp-server host

トラップ送信先マネージャーの設定を行います。設定を削除する場合は、no コマンドを使用してください。コミュニティー名は、ASCII 文字を使用し 127 文字以内で設定してください。トラップ送信先マネージャーは 10 個まで設定できます。

コマンドシンタックス

snmp-server host <NAME> <IPADDR> [version 1 | 2]
no snmp-server host [<NAME> [<IPADDR>]]

NAME	コミュニティー名 <1-127(文字)>
IPADDR	IP アドレス
1	バージョン 1 トラップを送信します。
2	バージョン 2 トラップを送信します。

デフォルト

なし(＝トラップ送信時のバージョンは 1)

コマンドモード

CONFIG

使用例

(1) トラップ送信先マネージャーのコミュニティー名を Manager1、IP アドレスを 192.168.2.200 に設定します。
(2) トラップ送信先マネージャーのコミュニティー名を Manager1、IP アドレスを 192.168.2.200、トラップのバージョンを 2 に設定します。
(3) コミュニティー名が Manager1、IP アドレスが 192.168.2.200 であるトラップ送信先マネージャーを削除します。
(4) コミュニティー名が Manager1 であるトラップ送信先マネージャーをすべて削除します。
(5) トラップ送信先マネージャーをすべて削除し、デフォルトに戻します。

```
> enable
# configure terminal
(config)# snmp-server host Manager1 192.168.2.200
(config)# snmp-server host Manager1 192.168.2.200 version 2
(config)# no snmp-server host Manager1 192.168.2.200
(config)# no snmp-server host Manager1
(config)# no snmp-server host
```

関連コマンド

show snmp-server, show running-config

注意事項

トラップ送信先をマネージャーを複数設定し、かつ"snmp-server traps transmit-gap disable"コマンドを設定時に、以下の動作となります。

- **複数のトラップ送信先マネージャーが、同じ Gateway を通過し、該当 Gateway の ARP(アドレス)が未解決の場合、設定しているすべてのマネージャーへトラップが送信されない場合があります。**

複数のトラップ送信先マネージャーを設定している状態で、OSPF のトラップを送信時に OSPF のネイバーが切断したり、ネイバー確立ができなくなることがあります。その場合、"snmp-server traps transmit-gap disable"コマンドを設定してください。設定後も改善しない場合は、"snmp-server traps ospf disable"コマンドにて、OSPF のトラップ送信機能を無効にするか、トラップ送信先マネージャーを 1 個にしてくだ

さい。

3.48.5 snmp-server trap source

トラップパケットにおける IP ヘッダー内の送信元 IP アドレスを設定します。設定を削除する場合は、no コマンドを使用してください。ループバック IP アドレス(127.0.0.0～127.255.255.255)、クラス D(224.0.0.0～239.255.255.255)、クラス E(240.0.0.0～255.255.255.255)は送信元 IP アドレスに指定できません。

本コマンド未設定の場合と、<IPADDR>へ装置に存在しない IP アドレスを指定した場合は、本装置が選択した送信元 IP アドレスが使用されます。

SNMPv1 の場合、エージェントアドレスフィールドの値も本コマンドで設定した IP アドレスになります。表 3-58 に送信元 IP アドレスと SNMPv1 エージェントアドレスフィールドの値を示します。

表 3-58 送信元 IP アドレスと SNMPv1 エージェントアドレスフィールドの値

	送信元 IP アドレス	SNMPv1 エージェントアドレスフィールド
設定なし (デフォルト)	装置が選択した IP アドレス (トラップ送信インターフェースの IP アドレス)	• 管理ポート有:管理ポートの IP アドレス ※1 • 管理ポート無：デフォルト VLAN(VLAN：1)の IP アドレス ※1
設定あり	指定した IP アドレス ※2	本コマンドで指定した IP アドレス ※3

※1 未設定の場合は 0.0.0.0
※2 装置に存在しない IP アドレスを指定した場合はトラップ送信インターフェースの IP アドレス
※3 装置に存在しない IP アドレスの場合は 0.0.0.0

コマンドシンタックス

```
snmp-server trap source <IPADDR>
no snmp-server trap source
```

IPADDR　　IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) トラップパケットにおける IP ヘッダー内の送信元 IP アドレスを 192.168.2.200 に設定します。
(2) トラップパケットにおける IP ヘッダー内の送信元 IP アドレス指定を削除します。

```
> enable
# configure terminal
(config)# snmp-server trap source 192.168.2.200
(config)# no snmp-server trap source
```

関連コマンド

show snmp-server, show running-config

注意事項

"snmp-server trap-source"コマンドを設定している場合、本コマンドは設定できません。

3.48.6 snmp-server traps

トラップの種類ごとにトラップ送信機能の有効/無効を設定します。本コマンドで有効/無効に設定されるトラップの詳細は、ログ・トラップ対応一覧を参照してください。

コマンドシンタックス

```
[ no ] snmp-server traps access-defender mac-authentication | web-authentication enable
[ no ] snmp-server traps authentication disable
[ no ] snmp-server traps auto-shutdown disable
[ no ] snmp-server traps cold disable
[ no ] snmp-server traps cpu-utilization disable
[ no ] snmp-server traps error-frame-threshold port <PORTRANGE> disable
[ no ] snmp-server traps error-frame-received port <PORTRANGE> disable
[ no ] snmp-server traps fan disable
[ no ] snmp-server traps flooding control disable
[ no ] snmp-server traps lacp enable
[ no ] snmp-server traps link manage disable
[ no ] snmp-server traps link port <PORTRANGE> disable
[ no ] snmp-server traps login-incorrect disable
[ no ] snmp-server traps loop-watch disable
[ no ] snmp-server traps memory-error auto-recovery disable
[ no ] snmp-server traps memory-error temporary-error disable
[ no ] snmp-server traps memory-used-notify disable
[ no ] snmp-server traps mmrp enable
[ no ] snmp-server traps na enable
[ no ] snmp-server traps ospf disable
[ no ] snmp-server traps pbr disable
[ no ] snmp-server traps poe enable [ block 1 | 2 ]
[ no ] snmp-server traps poe-system disable
[ no ] snmp-server traps port-security <PORTRANGE> disable
[ no ] snmp-server traps system-status disable
[ no ] snmp-server traps temperature disable
[ no ] snmp-server traps topology disable
```

access-defender mac-authentication	AccessDefender MAC 認証における端末状態変化時
access-defender web-authentication	AccessDefender Web 認証、ゲートウェイ認証における端末状態変化時
authentication	SNMP の認証失敗時
auto-shutdown	自動 shutdown 機能による shutdown 時
cold	電源投入、またはリブート時

cpu-utilization	CPU 使用率
error-frame-threshold port <PORTRANGE>	各エラー種別のフレームカウンター閾値超過
error-frame-received port <PORTRANGE>	エラーフレーム受信時
fan	ファン停止時
flooding control	フラッディング制御の変化時
lacp	LACP 状態変化時、及び対向装置設定・接続異常時
link manage	Management ポートのリンク状態変化時 (Management ポート付きモデルのみ)
link port <PORTRANGE>	リンク状態変化時(複数指定可能)
login-incorrect	ログイン失敗時
loop-watch	ユーザーループ検知機能の変化時
memory-error auto-recovery	メモリーエラー自動復旧時
memory-error temporary-error	バッファメモリーにおける一時的なメモリーエラー検出時
memory-used-notify	メモリー使用容量増加時
mmrp	MMRP 状態変化時
na	NA 状態変化時
ospf	ospf 状態変化時(L3 ライセンスのみ対応)
pbr	ポリシーベースルーティング状態変化時 (L3 ライセンスのみ対応)
poe	PoE 状態変化時 (Apresia3424GT-PoE/3424GT-HiPoE/5412GT-PoE のみ対応) block 指定は 3424GT-PoE のみ指定可能
poe-system	PoE 用電源の障害発生時 (Apresia3424GT-PoE/3424GT-HiPoE/5412GT-PoE のみ対応)
port-security <PORTRANGE>	ポートセキュリティー状態変化時(複数指定可能)
system-status	システム状態変化時
temperature	外気温度状態が基準値より変化時 (温度センサー付きモデルのみ)
topology	トポロジー変化時

デフォルト

access-defender, lacp, mmrp, na, poe：no enable(＝トラップを送信しない)
上記以外：no disable(＝トラップを送信する)

コマンドモード

CONFIG

使用例

(1) SNMP の認証に失敗した時にトラップ送信を行う機能を無効にします。
(2) ポート：5 のリンク状態が変化した時にトラップ送信を行う機能を無効にします。

(3) SNMP の認証に失敗したときにトラップ送信を行う機能を有効にします。
(4) ポート：5 のリンク状態が変化した時にトラップ送信を行う機能を有効にします。

```
> enable
# configure terminal
(config)# snmp-server traps authentication disable
(config)# snmp-server traps link port 5 disable
(config)# no snmp-server traps authentication disable
(config)# no snmp-server traps link port 5 disable
```

関連コマンド

show snmp-server, show running-config

注意事項

FAN レス対応機種(Apresia3424GT-SS/3424GT-SS2)において、"[no] snmp-server traps fan disable"コマンドは未サポートです。また、"show snmp-server"コマンドの SNMP trap management の fan 項目は表示しません。

L3 ライセンス有り(機種)のみ"[no] snmp-server traps ospf disable"、"[no] snmp-server traps pbr disable"コマンドをサポートしています。また、"show snmp-server"コマンドの SNMP trap management の ospf、pbr 項目を表示します。

3.48.7 snmp-server contact

システムグループ MIB のシステムコンタクトを設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

snmp-server contact <STRING>
no snmp-server contact

STRING	システムコンタクトを指定する文字列 ASCII 文字 <1-255(文字)> • contact の後、空白文字を含む行末までを文字列として解釈

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) システムコンタクトを administrator に設定します。

```
> enable
# configure terminal
(config)# snmp-server contact administrator
```

関連コマンド

show snmp-server, show running-config

注意事項

3.48.8 snmp-server location

システムグループ MIB のシステムロケーションを設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

snmp-server location <STRING>
no snmp-server location

STRING　　システムロケーションを指定する文字列 ASCII 文字 <1-255(文字)>
- location の後、空白文字を含む行末までを文字列として解釈

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) システムロケーションを Office of Works に設定します。
(2) システムロケーションの設定を削除します。

```
> enable
# configure terminal
(config)# snmp-server location Office of Works
(config)# no snmp-server location
```

関連コマンド

show snmp-server, show running-config

注意事項

3.48.9 snmp-server name

システムグループ MIB のシステムネームを設定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

snmp-server name <STRING>
no snmp-server name

STRING　　システムネームを指定する文字列 ASCII 文字 <1-255(文字)>

- name の後、空白文字を含む行末までを文字列として解釈

デフォルト
なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) システムネームを Switch No.1 に設定します。

```
> enable
# configure terminal
(config)# snmp-server name Switch No.1
```

関連コマンド
show snmp-server, show running-config

注意事項

3.48.10 snmp-server trap-source

送信するトラップのエージェントアドレスフィールドの値を、本コマンドで設定したインターフェースに割り当られた IP アドレスに設定します。設定を削除する場合は、no コマンドを使用してください。

エージェントアドレスフィールドの設定はトラップバージョン 1 のみ反映されます。送信するトラップをバージョン 2 に設定した場合、本コマンドは反映されません。

本コマンドの設定は、トラップパケットの送信元 IP アドレスには影響しません。本コマンド設定時も、トラップパケットの送信元 IP アドレスは、トラップ送信インターフェースの IP アドレスとなります。表 3-59 に本コマンド設定状態によるエージェントアドレスフィールドの値を示します。

表 3-59 エージェントアドレスフィールドの設定値

	エージェントアドレスフィールド
設定なし (デフォルト)	• 管理ポート有：管理ポートの IP アドレス ※1 • 管理ポート無：デフォルト VLAN(VLAN：1)の IP アドレス ※1
設定あり	指定したインターフェース(VLAN)の IP アドレス ※1

※1 未設定の場合は 0.0.0.0

コマンドシンタックス
snmp-server trap-source interface vlan <VID>
no snmp-server trap-source

VID	トラップ送信元となるインターフェースの VLAN ID

デフォルト
なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) エージェントアドレスフィールドの値をインターフェース VLAN ID：10 の IP アドレスに設定します。

(2) エージェントアドレスフィールドの値を管理ポートの IP アドレスに設定します。

```
> enable
# configure terminal
(config)# snmp-server trap-source interface vlan 10
(config)# no snmp-server trap-source
```

関連コマンド

show snmp-server, show running-config

注意事項

"snmp-server trap source"コマンドを設定している場合、本コマンドは設定できません。

3.48.11 snmp-server traps boot-time-delay

装置起動時に、SNMP トラップを出力開始するまでのディレイ時間を秒単位で設定します。設定をデフォルトに戻す場合は、no コマンドを使用してください。SNMP トラップ送出時に、トラップ送出ポートのネットワークのルート確立や ARP 未解決などが原因でトラップ送出が失敗する場合、適切な値を設定してください。

コマンドシンタックス

snmp-server traps boot-time-delay <SECONDS>
no snmp-server traps boot-time-delay
SECONDS　　ディレイ時間 <1-600(秒)>

デフォルト

なし(＝設定なし、ディレイ時間は 0 秒)

コマンドモード

CONFIG

使用例

(1) SNMP トラップを出力開始するまでのディレイ時間を 30 秒に設定します。

```
> enable
# configure terminal
(config)# snmp-server traps boot-time-delay 30
```

関連コマンド

show snmp-server, show running-config, snmp-server disable

注意事項

以下に示すコマンドを用いて SNMP を再度有効にしたとき、その直後に SNMP トラップ送出が発生する場合も本コマンドの設定が機能します。その場合は、SNMP を再度有効にしてから SNMP トラップを出力するまでのディレイ時間となります。
- **"snmp-server disable"後の"no snmp-server disable"コマンド**

ディレイ時間に設定する目安値を示します。以下は、あくまでも目安値となります。実際の構成情報、運用にあわせて調整のうえご使用ください。
- **最大 4094 個の VLAN を設定している場合、ディレイ時間を 30 秒に設定**

3.48.12 snmp-server traps transmit-delay

リンクダウントラップの送信ディレイ時間の設定値を変更することができます。設定をデフォルト値に戻す場合は、no コマンドを使用してください。リンクダウン時にリンクダウントラップを送信するように設定した場合、本機能により、リンクダウントラップを送信する際の送信ディレイ時間の設定値を変更可能としています。値は 0(遅延なし)から 5 秒まで設定可能です。

コマンドシンタックス

```
snmp-server traps transmit-delay <SECONDS>
no snmp-server traps transmit-delay
     SECONDS            送信ディレイ時間 <0-5(秒)>
```

デフォルト

1(秒)

コマンドモード

CONFIG

使用例

(1) リンクダウントラップの送信ディレイ時間を 4 秒にします。

```
> enable
# configure terminal
(config)# snmp-server traps transmit-delay 4
```

関連コマンド

show snmp-server, show running-config

注意事項

ルーティングプロトコルなどを使用し、リンクダウントラップを送信する経路が動的に切り替わる環境において、経路の切り替わりが最大遅延時間設定値(5 秒)を超える場合、送信ディレイ時間を最大値に設定してもリンクダウントラップが管理装置に正

常に到達しない場合もあります。

装置起動時にリンクダウントラップが発生した場合、本コマンドによる設定よりも、トラップ送出遅延設定である"snmp-server traps boot-time-delay"コマンドが優先となります。

3.48.13 snmp-server traps transmit-gap disable

トラップ送信先を、複数設定した場合の送信動作の切り替えを行います。設定をデフォルトに戻す場合は、no コマンドを使用してください。

トラップを複数のマネージャーに送信する場合、デフォルト状態では各マネージャーに所定の間隔を置いてからトラップを送信します。本コマンドを設定することで、送信間隔を置かずにトラップを送信します。

"snmp-server traps transmit-delay"コマンドと併用可能です。

コマンドシンタックス

[no] snmp-server traps transmit-gap disable

デフォルト

no disable(＝設定なし)

コマンドモード

CONFIG

使用例

(1) 各マネージャーへ送信間隔を置かずにトラップを送信します。

(2) 各マネージャーへ所定の間隔を置いてトラップを送信します。

```
> enable
# configure terminal
(config)# snmp-server traps transmit-gap disable
(config)# no snmp-server traps transmit-gap disable
```

関連コマンド

show snmp-server, show running-config

注意事項

3.48.14 snmp-server rmon-history

装置の再起動時、または"no snmp-server disable"コマンド設定時に、リモートネットワークモニタリング機能(RMON)の historyControlGroup のデフォルトエントリーを設定します。enable に設定した場合は、その後の装置の再起動時、または"no snmp-server disable"コマンド設定時に、デフォルトのエントリーが追加されます。no コマンドを使用した場合、エントリーは追加されません。リモートネットワークモニタリング機能(RMON)の詳細については、「MIB 項目の実装仕様」をご確認ください。

コマンドシンタックス

[no] snmp-server rmon-history default-entry enable

デフォルト

no enable(＝デフォルトエントリーを追加しない)

コマンドモード

CONFIG

使用例

(1) RMON の historyControlGroup のデフォルトエントリー追加設定を enable にします。
(2) RMON の historyControlGroup のデフォルトエントリー追加設定を disable にします。

```
> enable
# configure terminal
(config)# snmp-server rmon-history default-entry enable
(config)# no snmp-server rmon-history default-entry enable
```

関連コマンド

show snmp-server, show running-config

注意事項

3.48.15 snmp-server counter ifinerrors-exclude-oversize

interface MIB の ifInErrors カウンターにおいて、oversize 値の加算対象の有無を設定します。加算対象とする場合には、no コマンドを使用してください。

コマンドシンタックス

[no] snmp-server counter ifinerrors-exclude-oversize

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) ifInErrors カウンターにおいて、oversize 値を加算の対象としません。
(2) ifInErrors カウンターにおいて、oversize 値を加算の対象とします。

```
> enable
# configure terminal
(config)# snmp-server counter ifinerrors-exclude-oversize
(config)# no snmp-server counter ifinerrors-exclude-oversize
```

関連コマンド

show running-config

注意事項

3.48.16 show snmp-server

SNMP マネージャーに関する構成情報を表示します。

コマンドシンタックス

show snmp-server

コマンドモード

VIEW, ENABLE

使用例

(1) SNMP マネージャーに関する構成情報を表示します(Apresia13000-48X の場合)。

```
# show snmp-server

SNMP management: Enabled

SNMP mib management:
    Read-Only manager:  Enabled
        IP address              Community Name
                                public

    Read-Write manager: Enabled
        IP address              Community Name
                                private

SNMP trap management:
        authentication failure: Enabled
        auto-recovery         : Enabled
        temporary-error       : Enabled
        cold start            : Enabled
        cpu utilization       : Enabled
        memory utilization    : Enabled
        system status         : Enabled
        topology change       : Enabled
        fan error             : Enabled
        login incorrect       : Enabled
        flooding control      : Enabled
        loop-watch            : Enabled
        na                    : Disabled
        na logout clock       : Enabled
```

```
        mmrp                  : Disabled
        lacp                  : Disabled
        link change mng port  : Enabled
        temperature condition : Enabled
        pbr                   : Enabled
        ospf                  : Enabled
        mac-authentication    : Disabled
        web-authentication    : Disabled
        gateway               : Disabled
        auto-shutdown         : Enabled
        link change     port 1: Enabled        port 2: Enabled
                              (省略)
                        port49: Enabled        port50: Enabled
        port-security   port 1: Enabled        port 2: Enabled
                              (省略)
                        port49: Enabled        port50: Enabled
        Error Frame Counter threshold
                        port 1: Enabled        port 2: Enabled
                              (省略)
                        port49: Enabled        port50: Enabled
        Error Frame Counter received
                        port 1: Enabled        port 2: Enabled
                              (省略)
                        port49: Enabled        port50: Enabled

        IP address             Community Name         Trap Version

SysContact :
SysLocation:
SysName    :

Trap Source: manage
Trap delay time: 1 seconds
Trap boot time delay: 0 seconds
Trap transmit-gap: Enabled

RMON history default entry: Disabled
```

関連コマンド

注意事項

FAN レス対応機種(Apresia3424GT-SS/3424GT-SS2)において、"[no] snmp-server traps fan disable"コマンドは未サポートです。また、SNMP trap management の fan 項目は表示しません。

PoE 対応機種のみ SNMP trap management の poe、poe-system 項目を表示します。

L3 ライセンス有り(機種)のみ"[no] snmp-server traps ospf disable"、"[no] snmp-server traps pbr disable"コマンドをサポートしています。また、SNMP trap management の ospf、pbr 項目を表示します。

3.49 構成情報の表示

3.49.1 show running-config

RAM に設定されている構成情報のデフォルト値からの差分を表示します。"write terminal"コマンドでも同内容が表示されます。

コマンドシンタックス

show running-config

コマンドモード

VIEW モード以外の全モードで使用可能

使用例

(1) 動作中の構成情報を表示します。

```
# show running-config
!
username adpro adpro
username user user
!
no ip multicast-routing
!
interface loopback
!
interface manage
 ip address 172.21.29.25/24
!
interface port 1
 utp auto-negotiation disable
 utp link-speed-duplex 100m/full
!
interface port 2

     (省略)

interface port 50
!
interface vlan 1
!
!
!
end

#
```

関連コマンド

注意事項

3.49.2 show flash-config

フラッシュメモリーに保存されている構成情報のデフォルト値からの差分を表示します。

コマンドシンタックス

show flash-config

コマンドモード

ENABLE

使用例

(1) 装置に保存されている構成情報を表示します。

```
# show flash-config
!
username adpro adpro
username user user
!
no ip multicast-routing
!
interface loopback
!
interface manage
 ip address 172.21.29.25/24
!
interface port 1
 utp auto-negotiation disable
 utp link-speed-duplex 100m/full
!
interface port 2

     (省略)

interface port 50
!
interface vlan 1
!
!
!
end

#
```

関連コマンド

注意事項

3.50 構成情報のチェックと保存

3.50.1 check config

現在動作中の設定("show running-config"コマンドの表示内容)とフラッシュメモリーに保存されている設定("show flash-config"コマンドの表示内容)を比較して、差異がある場合はプロンプトに"*"を付加してユーザーに警告を出します。差分があった場合の警告のプロンプトは、パラメーターの保存(3.50.2 項参照)、または装置の再起動が行われるまで保持されます。

コマンドシンタックス

check config

コマンドモード

VIEW, ENABLE

使用例

(1) 動作設定とフラッシュメモリーの設定に差異がないかを確認します。

(2) "write memory"コマンドで設定を保存し、差異をなくします。

```
# check config
*# write memory
Current running-config is saved to flash-config.
Writing to flash memory...
[OK]
Writing to SD memory...
upload completed.(hc-flash-config)

#
```

関連コマンド

注意事項

3.50.2 copy running-config flash-config, write memory

"copy running-config flash-config"コマンドで、現在動作中の設定されている構成情報をフラッシュメモリーに保存します、及び SD メモリーカードに保存します。"write memory"コマンドでも同様の処理が行われます。

SD メモリーカード非対応機種では、フラッシュメモリーにのみ構成情報を保存します。SD メモリーカード対応機種は、3.54 メモリーカードを参照してください。

コマンドシンタックス

copy running-config flash-config
write memory

コマンドモード

ENABLE

使用例

(1) 動作中の構成情報を装置に保存します。

```
# copy running-config flash-config
Current running-config is saved to flash-config.
Writing to flash memory...
[OK]
Writing to SD memory...
upload completed.(hc-flash-config)

# write memory
Current running-config is saved to flash-config.
Writing to flash memory...
[OK]
Writing to SD memory...
upload completed.(hc-flash-config)
```

関連コマンド

注意事項

3.55 ブートスクリプトコマンドにより、SD メモリーカード内の構成情報が選択されている場合、フラッシュメモリーだけに保存された設定は再起動後に反映されません。

SD メモリーカードから起動する場合は、別途 3.55.4 "copy flash-config memory-card"コマンドにより、SD メモリーカードに構成情報を保存してください。

本コマンド実行中は装置のリセットボタンの使用、電源断などのリブート動作を行わないでください。

本コマンドにより、SD メモリーカードにも構成情報(hc-flash-config)を保存します。

SD メモリーカードが装置に挿入されていない場合、または SD メモリーカードにプロテクトをかけて挿入されている場合は、以下のエラーメッセージが出力されますが、装置のフラッシュメモリーに対しては、以前と同様に書き込まれるため、従来どおりご利用いただけます。

- **SD メモリーカード未挿入で実施した場合のエラーメッセージ**
  "ERROR: SD Memory card mount error"
- **SD メモリーカードプロテクト時に実施した場合のエラーメッセージ**
  "ERROR: SD Memory card copy error"

3.35.1 "sshd keygen rsa"、3.35.2 "sshd keygen rsa1"、及び 3.35.3 "sshd server"

で RSA ホスト鍵対生成後、本コマンドを実行してフラッシュメモリーに書き込んでください。本コマンドを実行せずに装置再起動すると、RSA ホスト鍵対は空ファイルとなります。

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.50.3 copy tftp server file flash-config

TFTP サーバー上の構成情報を、フラッシュメモリーに保存します。フラッシュメモリーに保存された構成情報は、リブート後に反映されます。リブートコマンド実行時、以下の使用例のように"save running config?"と表示されますが、取得した設定を反映する場合は"n"を入力します。

コマンドシンタックス

copy tftp <SERVER> <FILE> flash-config

SERVER	TFTP サーバーのアドレス
FILE	構成情報のファイル名 • 最大 128 文字 • 使用可能な文字は、ASCII コードの印字可能な文字のうち、["][?] を除いた文字

コマンドモード

ENABLE

使用例

(1) IP アドレス：172.17.33.21 の TFTP サーバー上の構成情報を装置に保存します。

```
# copy tftp 172.17.33.21 Apresia.conf flash-config
override? (y/n): y
getting from 172.17.33.21: Apresia.conf
Received 784 bytes in 0.0 seconds
Writing to flash memory...
done.
This setting is validated after rebooting.
# reboot
check config? (y/n): y
save running config? (y/n): n
reboot system? (y/n): y
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

構成情報(テキストファイル)に使用できる改行コードは LF、または CR+LF です。CR は使用できません。

3.50.4 copy flash-config tftp server file

フラッシュメモリーに保存されている起動時の構成情報を、TFTP サーバー上のファイルにコピーします。

コマンドシンタックス

copy flash-config tftp <SERVER> <FILE>

SERVER	TFTP サーバーのアドレス
FILE	構成情報のファイル名 • 最大 128 文字 • 使用可能な文字は、ASCII コードの印字可能な文字のうち、["][?]を除いた文字

コマンドモード

ENABLE

使用例

(1) 装置の構成情報を IP アドレス：172.17.33.21 の TFTP サーバー上に backup2.aaa として保存します。

```
# copy flash-config tftp 172.17.33.21 backup2.aaa
Sent 784 bytes in 0.1 seconds
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

3.50.5 copy running-config file

3.49.1 "show running-config"コマンドで表示される現在の構成情報を TFTP サーバー、または SD メ

モリーカードへアップロードします。

コマンドシンタックス

copy running-config (tftp <IPADDR>) | memory-card <FILE>

IPADDR	TFTP サーバーの IP アドレス
FILE	構成情報のファイル名 • 最大 128 文字 • 使用可能な文字は、ASCII コードの印字可能な文字のうち、["][?] を除いた文字

コマンドモード

ENABLE

使用例

(1) "show running-config"コマンドで表示される現在の構成情報を TFTP サーバーに保存します。

```
# copy running-config tftp 172.21.29.161 config_up.txt
Sent 1325 bytes in 0.1 seconds
```

(2) "show running-config"コマンドで表示される現在の構成情報を SD メモリーカードに保存します。

```
# copy running-config memory-card config_up.txt
upload completed.(config_up.txt)
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

3.51 構成情報の初期化

3.51.1 erase flash-config

フラッシュメモリーに設定されている構成情報のうち、時刻以外のシステムパラメーターをデフォルト値に設定します。

コマンドシンタックス

erase flash-config

コマンドモード

ENABLE

使用例

(1) フラッシュメモリーに設定されている情報を初期化します。

```
# erase flash-config
*#
```

関連コマンド

注意事項

本コマンドを実行すると SSH 機能の RSA ホスト鍵対も削除され、空の鍵対を生成します。本コマンド実行後に SSH の設定変更を行う場合は、以下のコマンドを使用して RSA ホスト鍵対を作成、またはダウンロードしてください。

- **3.35.1 "sshd keygen rsa"**
- **3.35.2 "sshd keygen rsa1"**
- **3.35.11 "copy file ssh-key"**

3.52 Default disable

本機能を有効にすることにより、3.51.1 "erase flash-config"コマンドの実行による起動時のデフォルトの flash-config に対して、全物理ポートの 3.7.1 "shutdown"(非活性状態)を設定することができます。これにより"erase flash-config"コマンド投入後に、単純な L2 スイッチで起動することにより発生する L2 ループの問題など、不用意なポートの活性化によるネットワークへの悪影響を防止することができます。

3.52.1 default disable

Default disable 機能を有効にします。無効に戻す場合は、no コマンドを使用してください。本設定を追加しても、"erase flash-config"コマンドを入力時の動作以外に装置の動作に影響は与えません。

コマンドシンタックス

[no] default disable

デフォルト

なし(＝Default disable 機能無効)

コマンドモード

CONFIG

使用例

(1) default disable を有効にします。

```
# configure terminal
(config)# default disable
```

関連コマンド

erase flash-config, show running-config

注意事項

3.53 構成情報自動ダウンロード

3.53.1 auto-download

構成情報自動ダウンロード機能を有効にします。無効にする場合は、no コマンドを使用してください。

本コマンドを有効にした場合、起動時に設定された TFTP サーバーから構成情報を自動でダウンロードして設定を行います。

コマンドシンタックス

auto-download <IPADDR> <FILE-NAME>
no auto-download

IPADDR	TFTP サーバーの IP アドレス
FILE-NAME	構成情報ファイル名

コマンドモード

CONFIG

使用例

(1) 192.168.1.1 の TFTP サーバーから"config.txt"という構成情報ファイルをダウンロードするように設定します。

```
> enable
# configure terminal
(config)# auto-download 192.168.1.1 config.txt
```

関連コマンド

show auto-download, show running-config

注意事項

本機能は、装置の保持している構成情報ファイル(flash-config)と、ダウンロードしてきた構成情報ファイルが完全に一致するまで、リブート、及びダウンロードを繰り返しますので、ダウンロードする構成情報ファイルの整合性に十分ご注意ください。

例として、ダウンロードする構成情報ファイルを保存している TFTP サーバーが 2 台存在し、各サーバーに保存された構成情報ファイルが以下のようになっていた場合、上記繰り返し動作になります。

(1) サーバー1 に保存されている構成情報ファイル内の構成情報自動ダウンロード設定にて、サーバー2 の IP アドレスが指定されている。

(2) サーバー2 に保存されている構成情報ファイル内の構成情報自動ダウンロード設定にて、サーバー1 の IP アドレスが指定されている。

また、1 台の TFTP サーバーに 2 つの構成情報ファイルが存在し、各ファイルに保存された構成情報ファイルが以下のようになっている場合にも、上記繰り返し動作になります。

(1) ファイル 1 に保存されている構成情報ファイル内の構成情報自動ダウンロード設

定にて、ファイル 2 が指定されている。

(2) ファイル 2 に保存されている構成情報ファイル内の構成情報自動ダウンロード設定にて、ファイル 1 が指定されている。

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

3.53.2 show auto-download

構成情報自動ダウンロードの設定状態を表示します。

コマンドシンタックス

show auto-download

コマンドモード

VIEW, ENABLE

使用例

(1) 構成情報自動ダウンロードの設定状態を表示します。

```
> enable
# show auto-download
Server IP : 192.168.1.1
File Name : config.txt
```

関連コマンド

注意事項

3.54 メモリーカード

本機能は、SD メモリーカードからシステムソフトウェア(ファームウェア)、及び構成情報(flash-config)をダウンロード、またはメモリーカードに構成情報、及びログを保存する機能です。本機能を用いることにより、SD メモリーカードによる保守が可能になります。

SD メモリーカードに保存された構成情報(テキストファイル)を使用して装置を起動する場合、改行コードは LF、CR+LF、CR のいずれも使用できます。

注意事項

SD メモリーカードは、Apresia3400/5400/13000 シリーズでのみ使用できます。

SD メモリーカードはあらかじめフォーマットしておく必要があります。

SD メモリーカードを再初期化する際は、FAT16 でフォーマットしてください。フォーマット方法は SD メーカー各社より提供されている SD メモリーカードフォーマットソフトウェアをご使用ください。

3.54.1 copy memory-card software

SD メモリーカードからファームウェアをダウンロードします。ダウンロードしたファームウェアはリブート後に反映されます。

Apresia3400/5400 シリーズではプライマリー領域にファームウェアをダウンロードします。Apresia13000 シリーズではプライマリー/セカンダリー領域両方にファームウェアをダウンロードします。

コマンドシンタックス

copy memory-card <FILE> software

FILE　　ファームウェアのファイル名

コマンドモード

ENABLE

使用例

(1) SD メモリーカードからファイル名：apresia.img のファームウェアに更新します。

```
# copy memory-card apresia.img software
```

関連コマンド

注意事項

HSW5Ware、AEOS Ver. 6.x などの AEOS Ver. 7.x 以外のファームウェアをダウンロードしないでください。ダウンロードした場合、装置が起動しません。

3.54.2 copy memory-card flash-config

SD メモリーカードから構成情報(flash-config)をダウンロードします。ダウンロードした構成情報はリブート後に反映されます。

コマンドシンタックス

copy memory-card <FILE> flash-config

FILE	構成情報のファイル名

コマンドモード

ENABLE

使用例

(1) SD メモリーカードからファイル名：ap13k.txt の構成情報に更新します。

```
# copy memory-card ap13k.txt flash-config
```

関連コマンド

注意事項

構成情報(テキストファイル)に使用できる改行コードは LF、または CR+LF です。CR は使用できません。

3.54.3 copy tftp memory-card

TFTP サーバーからシステムソフトウェア(ファームウェア)を SD メモリーカードにダウンロードします。

コマンドシンタックス

copy tftp <IPADDR> <FILE1> memory-card <FILE2>

IPADDR	TFTP サーバーの IP アドレス
FILE1	ファームウェアのファイル名
FILE2	SD メモリーカードに保存するファームウェアのファイル名

コマンドモード

ENABLE

使用例

(1) TFTP サーバーからファイル名：aeosR7XXXX.img のファームウェアを、SD メモリーカードにファイル名：apresia.img で保存します。

```
# copy tftp 10.249.23.245 aeosR7XXXX.img memory-card apresia.img
getting from 10.249.23.245:aeosR7XXXX.img
Received 6394067 bytes in 16.1 seconds
Writing to SD-memory...
upload completed.(apresia.img)
```

```
CRC Checking.
Ok.
done.
#
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.54.4 copy flash-config memory-card

SD メモリーカードに構成情報(flash-config)を保存します。

コマンドシンタックス

copy flash-config memory-card <FILE>

FILE	構成情報のファイル名

コマンドモード

ENABLE

使用例

(1) SD メモリーカードに構成情報を、ファイル名：ap13k.txt として保存します。

```
# copy flash-config memory-card ap13k.txt
```

関連コマンド

注意事項

"$&'()^~¥|`{}[]*;<>?はファイル名として使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.54.5 copy log memory-card

SD メモリーカードに log を保存します。

コマンドシンタックス

copy log memory-card <FILE>

FILE　　log のファイル名

コマンドモード

ENABLE

使用例

(1) SD メモリーカードに log を、ファイル名：ap13k.log として保存します。

```
# copy log memory-card ap13k.log
```

関連コマンド

注意事項

"$&'()^~¥|`{}[]*;<>?はファイル名として使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.54.6 cat memory-card

SD メモリーカード内のファイル内容を表示します。

コマンドシンタックス

cat memory-card <FILE>

FILE　　SD メモリーカード内のファイル名

コマンドモード

ENABLE

使用例

(1) SD メモリーカードに保存された sample.conf の内容を表示します。

```
# cat memory-card sample.conf
!
username adpro adpro
username user user
!
interface loopback
!
interface manage
   (省略)
```

関連コマンド

注意事項

"$&'()^~¥|`{}[]*;<>?はファイル名として使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

3.54.7 erase memory-card

SD メモリーカード内のファイルを削除します。

コマンドシンタックス

erase memory-card <FILE>

FILE	SD メモリーカード内のファイル名

コマンドモード

ENABLE

使用例

(1) SD メモリーカード内の apresia.img を削除します。

```
# erase memory-card apresia.img
```

関連コマンド

注意事項

"$&'()^~¥|`{}[]*;<>?はファイル名として使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

3.54.8 rename memory-card

SD メモリーカード内ファイルのファイル名を変更します。

コマンドシンタックス

rename memory-card <FILE1> <FILE2>

FILE1	変更前のファイル名
FILE2	変更後のファイル名

コマンドモード

ENABLE

使用例

(1) SD メモリーカード内の sample.conf を test.conf に変更します。

```
# rename memory-card sample.conf test.conf
```

関連コマンド

注意事項

- **"$&'()^~¥|`{}[]*;<>?はファイル名として使用できません。**
- **ファイル名として、..を含む文字列は使用できません。**
- **/はディレクトリ指定として扱われます。**
- **すでに存在するファイルを変更後のファイル名に指定した場合、存在するファイルへ上書きします。また、存在するディレクトリを変更後のファイル名に指定した場合、ディレクトリへファイルを移動します。**

3.54.9 show memory-card files

SD メモリーカードに保存されているファイル名を表示します。

コマンドシンタックス

show memory-card files

コマンドモード

VIEW, ENABLE

使用例

(1) SD メモリーカードに保存されているファイル名を表示します。

```
# show memory-card files
total 9600
----------  1 root  wheel     6635 Feb 19  2007 HONSHAL3_AP1
----------  1 root  wheel  4843238 Oct  5 01:57 apresia.img
----------  1 root  wheel     2598 Oct  3 15:52 config(Ap4328).config
```

関連コマンド

注意事項

3.55 ブートスクリプト

ブートスクリプトは起動時に使用するファームウェアと構成情報の選択情報を記録しており、装置内部、及びSDメモリーカード内に保存できます。

製品出荷時は、装置内部にデフォルトのブートスクリプトが保存されています。デフォルトのブートスクリプトは、装置内部(フラッシュメモリー内)のプライマリー領域のファームウェア、及びプライマリー領域の構成情報を選択して起動するように記録されています。

SDメモリーカード内に装置の運用情報(ブートスクリプト、ファームウェア、構成情報)を保存しておくことにより、SDメモリーカードを交換して装置を起動するだけで、装置の運用、保守が可能となります。

SDメモリーカード上のブートスクリプトの読み込み処理の順番は、以下となります。

(1) SD メモリーカードにブートスクリプトファイルがある場合、SD メモリーカードのブートスクリプトファイルを読み込みます。
(2) SDメモリーカードのブートスクリプトで指定したファームウェアの起動において、プライマリー、セカンダリー共に失敗した場合、フラッシュメモリーに保存されたブートスクリプトを読み込みます。
(3) フラッシュメモリーのブートスクリプトで指定したファームウェアの起動において、プライマリー、セカンダリー共に失敗した場合、装置は正しく起動できません。

注意事項

ブートスクリプトは、Apresia3400/5400/13000 シリーズでのみ有効です。

ブートスクリプトを工場出荷後初めて編集する際、"warning: HCLoader version string is not found."というメッセージが表示される場合がありますが、動作には問題ありません。

"$&'()^~¥|`{}[]*;<>?はファイル名として使用できません。

/はディレクトリ指定として扱われます。

ファイル名として、..を含む文字列は使用できません。

起動設定でプライマリーファームウェアは、フラッシュメモリー内のプライマリー領域を指定しているにも関わらず、意図せずセカンダリーファームウェアで起動した場合、フラッシュメモリーのプライマリー領域が故障している可能性があります。その場合は、サポート対応窓口にお問い合わせください。

ブートスクリプトで指定するファイルの内容が、ファームウェア、または構成情報のファイルであることの整合性は確認していないため、指定するファイルが適切であることを確認してください。

3.55.1 boot-script system primary

装置起動時に優先的に使用するプライマリーファームウェアの選択情報をブートスクリプトに記録します。プライマリーファームウェアは、フラッシュメモリー内のプライマリー領域、もしくはセカンダリー領域、または SD メモリーカード内のファイルを指定できます。

コマンドシンタックス

boot-script system primary primary | secondary | (memory-card <FILE>)

primary	フラッシュメモリー内のプライマリー領域
secondary	フラッシュメモリー内のセカンダリー領域
memory-card	SD メモリーカード
FILE	SD メモリーカード内のファイル名

コマンドモード

ENABLE

使用例

(1) フラッシュメモリー内のプライマリー領域をプライマリーファームウェアに指定します。

```
# boot-script system primary primary
Writing configured-script...
done.
```

関連コマンド

注意事項

装置起動時にプライマリー/セカンダリーファームウェア両方に異常がある場合、装置は正しく起動しません。ただし、SD メモリーカード内のブートスクリプトにて指定したプライマリー/セカンダリーファームウェア両方が SD メモリーカード内のファイルである場合、フラッシュメモリー内のファームウェアにより起動します。

3.55.2 boot-script system secondary

装置起動時にプライマリーファームウェアが使用できない場合に使用するセカンダリーファームウェアの選択情報をブートスクリプトに記録します。セカンダリーファームウェアは、フラッシュメモリー内のプライマリー領域、もしくはセカンダリー領域、または SD メモリーカード内のファイルを指定できます。

コマンドシンタックス

boot-script system secondary primary | secondary | (memory-card <FILE>)

primary	フラッシュメモリー内のプライマリー領域
secondary	フラッシュメモリー内のセカンダリー領域
memory-card	SD メモリーカード
FILE	SD メモリーカード内のファイル名

コマンドモード

ENABLE

使用例

(1) フラッシュメモリー内のプライマリー領域をセカンダリーファームウェアに指定します。

```
# boot-script system secondary primary
Writing configured-script...
done.
```

関連コマンド

注意事項

装置起動時にプライマリー/セカンダリーファームウェア両方に異常がある場合、装置は正しく起動しません。ただし、SD メモリーカード内のブートスクリプトにて指定したプライマリー/セカンダリーファームウェア両方が SD メモリーカード内のファイルである場合、フラッシュメモリー内のファームウェアにより起動します。

3.55.3 boot-script configuration primary

装置起動時に、優先的に使用するプライマリー構成情報の選択情報をブートスクリプトに記録します。プライマリー構成情報は、フラッシュメモリー内のプライマリー領域、もしくはセカンダリー領域、または SD メモリーカード内のファイルを指定できます。

コマンドシンタックス

boot-script configuration primary primary | secondary | (memory-card <FILE>)

primary	フラッシュメモリー内のプライマリー領域
secondary	フラッシュメモリー内のセカンダリー領域
memory-card	SD メモリーカード
FILE	SD メモリーカード内のファイル名

コマンドモード

ENABLE

使用例

(1) フラッシュメモリー内のプライマリー領域をプライマリー構成情報に指定します。

```
# boot-script configuration primary primary
Writing configured-script...
done.
```

関連コマンド

注意事項

装置起動時にプライマリー/セカンダリー構成情報両方に異常がある場合、装置は正しく起動しません。

3.55.4 boot-script configuration secondary

装置起動時にプライマリー構成情報が使用できない場合に使用するセカンダリー構成情報の選択情報をブートスクリプトに記録します。セカンダリー構成情報は、フラッシュメモリー内のプライマリー領域、もしくはセカンダリー領域、または SD メモリーカード内のファイルを指定できます。

コマンドシンタックス

boot-script configuration secondary primary | secondary | (memory-card <FILE>)

primary	フラッシュメモリー内のプライマリー領域
secondary	フラッシュメモリー内のセカンダリー領域
memory-card	SD メモリーカード
FILE	SD メモリーカード内のファイル名

コマンドモード

ENABLE

使用例

(1) フラッシュメモリー内のプライマリー領域をセカンダリー構成情報に指定します。

```
# boot-script configuration secondary primary
Writing configured-script...
done.
```

関連コマンド

注意事項

装置起動時にプライマリー/セカンダリー構成情報両方に異常がある場合、装置は正しく起動しません。

3.55.5 copy configured-script

設定したブートスクリプトをフラッシュメモリー、もしくは SD メモリーカードに保存します。ブートスクリプトをデフォルトに戻す場合は、"copy default-script configured-script"コマンドを使用してください。

コマンドシンタックス

copy configured-script memory-card | flash-script

memory-card	SD メモリーカード
flash-script	フラッシュメモリー

コマンドモード

ENABLE

使用例

(1) ブートスクリプトをフラッシュメモリーに保存します。

```
# copy configured-script flash-script
Writing flash-script...
done.
```

関連コマンド

注意事項

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.55.6 copy default-script configured-script

設定したブートスクリプトをデフォルトに戻します。

コマンドシンタックス

copy default-script configured-script

コマンドモード

ENABLE

使用例

(1) 設定したブートスクリプトをデフォルト設定に戻します。

```
# copy default-script configured-script
Writing configured-script...
done.
```

関連コマンド

注意事項

3.55.7 erase boot-script

SD メモリーカードに保存された、ブートスクリプトを消去します。

コマンドシンタックス

erase boot-script

コマンドモード

ENABLE

使用例

(1) ブートスクリプトを消去します。

```
# erase boot-script
```

関連コマンド

注意事項

3.55.8 show boot-script configured

設定用の一時的なブートスクリプトを表示します。

コマンドシンタックス

show boot-script configured

コマンドモード

VIEW, ENABLE

使用例

(1) 設定用の一時的なブートスクリプトを表示します。

```
# show boot-script configured
! User configuration for: HCLoader
configure boot primary system built-in primary
configure boot primary configuration built-in primary
configure boot secondary system built-in secondary
configure boot secondary configuration built-in secondary
boot
!
! End
```

User configuration for ：ブートスクリプトを作成したローダーソフトウェアのバージョン
primary system ：通常起動時に使用するファームウェア
primary configuration ：通常起動時に使用する構成情報
secondary system ：primary system による起動不可時に使用するファームウェア
secondary configuration ：primary configuration による起動不可時に使用する構成情報
built-in primary ：フラッシュメモリー内のプライマリー領域
built-in secondary ：フラッシュメモリー内のセカンダリー領域
memory-card <FILE> ：SD メモリーカード内のファイル

関連コマンド

注意事項

3.55.9 show boot-script flash

フラッシュメモリー内に保存されたブートスクリプトを表示します。

コマンドシンタックス

show boot-script flash

コマンドモード

VIEW, ENABLE

使用例

(1) ブートスクリプトを表示します。

```
# show boot-script flash
! User configuration for: HCLoader
configure boot primary system built-in primary
configure boot primary configuration built-in primary
configure boot secondary system built-in secondary
configure boot secondary configuration built-in secondary
boot
!
! End
```

User configuration for ：ブートスクリプトを作成したローダーソフトウェアのバージョン
primary system ：通常起動時に使用するファームウェア
primary configuration ：通常起動時に使用する構成情報
secondary system ：primary system による起動不可時に使用するファームウェア
secondary configuration ：primary configuration による起動不可時に使用する構成情報
built-in primary ：フラッシュメモリー内のプライマリー領域
built-in secondary ：フラッシュメモリー内のセカンダリー領域
memory-card <FILE> ：SD メモリーカード内のファイル

関連コマンド

注意事項

3.55.10 show boot-script memory-card

SD メモリーカードに保存されているブートスクリプトを表示します。

コマンドシンタックス

show boot-script memory-card

コマンドモード

VIEW, ENABLE

使用例

(1) SD メモリーカード内のブートスクリプトを表示します。

```
# show boot-script memory-card
! User configuration for: HCLoader
configure boot primary system built-in primary
configure boot primary configuration built-in primary
configure boot secondary system built-in secondary
configure boot secondary configuration built-in secondary
boot
!
! End
```

User configuration for ：ブートスクリプトを作成したローダーソフトウェアのバージョン
primary system ：通常起動時に使用するファームウェア
primary configuration ：通常起動時に使用する構成情報
secondary system ：primary system による起動不可時に使用するファームウェア
secondary configuration ：primary configuration による起動不可時に使用する構成情報
built-in primary ：フラッシュメモリー内のプライマリー領域
built-in secondary ：フラッシュメモリー内のセカンダリー領域
memory-card <FILE> ：SD メモリーカード内のファイル

関連コマンド

注意事項

3.56 再起動

3.56.1 reboot

本装置をリブートします。

リブート直前に、現在動作中の設定とフラッシュメモリーへ保存済みの設定を比較して相違がある場合には、動作中の設定をフラッシュメモリーへ保存するかを問い合わせます。

コマンドシンタックス

reboot

コマンドモード

ENABLE

使用例

(1) 設定を比較し、動作中の設定を保存してから、装置を再起動します。

```
# reboot
check config? (y/n): y
save running config? (y/n): y
Current running-config is saved to flash-config.
Writing to flash memory...
[OK]
Writing to SD memory...
upload completed.(hc-flash-config)

reboot system? (y/n): y
Oct  6 12:46:43  <system:emerg> Rebooting.
```

関連コマンド

注意事項

設定変更後、フラッシュメモリー、または SD メモリーカードへの書込みを行わずにリブートした場合、変更内容は失われます。

3.55 ブートスクリプトコマンドにより、SD メモリーカード内の構成情報が選択されている場合、フラッシュメモリーだけに保存された設定は再起動後に反映されません。

PoE 機能対応機種(Apresia3424GT-PoE/3424GT-HiPoE/5412GT-PoE)では、装置を再起動すると PoE による電源供給は一時的に停止します。

3.56.2 reboot timer

時間指定リブートを設定します。指定時間後、本装置が自動的にリブートします。設定を解除する場合は、no コマンドを使用してください。本設定は 3.49.1 "show running-config"、3.49.2 "show

flash-config"に反映されません。指定時間後の自動リブート後に再度、自動リブートを実施したい場合、改めて本コマンドを設定してください。指定時間内に"reboot"コマンド、本装置の電源 OFF、電源 ON による再起動が発生すると、本設定は削除されます。

コマンドシンタックス

reboot timer <HOURS> <MINUTES>
no reboot timer

HOURS	時間 <0-10000>
MINUTES	分 <0-59>

コマンドモード

ENABLE

使用例

(1) 24 時間後の自動リブートを設定します。

```
# reboot timer 24 0
```

関連コマンド

注意事項

3.56.3 show reboot timer

時間指定リブートによりリブートされるまでの残り時間を表示します。

コマンドシンタックス

show reboot timer

コマンドモード

ENABLE

使用例

(1) 時間指定リブートによりリブートされるまでの残り時間を表示します。

```
# show reboot timer
REBOOT TIME : 00023:58:19
```

REBOOT TIME　　：リブートまでの残り時間

関連コマンド

注意事項

3.57 ファームウェアの管理

3.57.1 archive download-sw

TFTP サーバー、または SD メモリーカードからファームウェアをダウンロードします。ダウンロードしたファームウェアはリブート後に反映されます。

Apresia3400/4300/5400 シリーズと Apresia13000 シリーズでは、使用できるファームウェアが異なります。

Apresia3400/4300/5400 シリーズでは、公式リリースされているファームウェア名の末尾に"-x300"が表記されているファームウェアを使用してください。なお、実際の運用では、ファームウェア名を変更して使用できます。

<ファームウェア名>

Apresia3400/4300/5400 シリーズ	aeosR7XXXX-x300.img
Apresia13000 シリーズ	aeosR7XXXX.img

Apresia3400/4300/5400 シリーズではファイル名の後に secondary を指定することにより、セカンダリー領域にファームウェアをダウンロードが行えます。ダウンロードしたファームウェアはリブート後に反映されます。また、未指定の際はプライマリー領域にファームウェアのダウンロードを行います。

Apresia3400/4300/5400 シリーズと Apresia13000 シリーズのファームウェア、ローダーソフトウェアのバージョンの組み合わせは、ローダ__ファームウェアバージョン対応表を参照してください。

コマンドシンタックス

archive download-sw (tftp <IPADDR>) | memory-card <FILE> [secondary]

IPADDR	TFTP サーバーの IP アドレス
FILE	ファームウェアのファイル名
secondary	セカンダリー領域指定

コマンドモード

ENABLE

使用例

(1) IP アドレス：172.17.33.21 の TFTP サーバーからファイル名：apresia.img のファームウェアをダウンロードします。

```
# archive download-sw tftp 172.17.33.21 apresia.img
override? (y/n): y
getting from 172.17.33.21:apresia.img
Received 4026708 bytes in 20.0 seconds
Filesize is 4026708 bytes
Writing ... done.
```

(2) SD メモリーカードからファイル名：apresia.img のファームウェアをダウンロードします。

```
# archive download-sw memory-card apresia.img
override? (y/n): y
Filesize is 5765844 bytes
Writing ... done.
```

関連コマンド

注意事項

- HSW5Ware、AEOS Ver. 6.x などの AEOS Ver. 7.x 以外のファームウェアをダウンロードしないでください。ダウンロードした場合、装置が起動しません。

- 3.55 ブートスクリプトコマンドにより、SD メモリーカード内のファームウェアが選択されている場合、フラッシュメモリーに保存されたファームウェアでは通常起動しません。

- ファームウェア以外をダウンロードしないでください。ダウンロードした場合、装置が起動しません。

- ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

- ファイル名として、..を含む文字列は使用できません。

- /はディレクトリ指定として扱われます。

- ファームウェアのバージョンを下げる場合は、リリースノートなどにより、当該ファームウェアが対象装置をサポートしていることを確認してください(ファームウェアの Ver.により、サポート対象機種が異なります)。
  未サポートのファームウェアをダウンロードした場合、装置が起動しなくなる場合がありますのでご注意ください。

- Apresia13000 シリーズにおいて、Ver. 7.09.01 以前から、Ver. 7.12.01 以降へバージョンアップする場合、一度、Ver. 7.10.01～7.11.04 へバージョンアップ後に Ver. 7.12.01 以降へバージョンアップしてください。

- Apresia4300/13000 シリーズにおいて、Ver. 7.11.04 以前から Ver. 7.12.01 以降へバージョンアップする際、装置の AccessDefender ローカルデータベース(以下、ローカル DB)は引き継がれません。

- Ver. 7.16.02 より、3.46 NA 機能、3.47 AccessDefender の SSL 機能で使用可能なテスト用の証明書が更新されています。テスト用証明書を更新するには、ファームウェアの更新後に一度 3.45.5 "erase ssl-files"を実行してください。テスト用証明書を使用していない場合、本操作は不要です。

- Apresia4300 シリーズにおいて、Ver. 7.12.01 以降へバージョンアップする場合、HCLoader は Ver. 1.05.04 以降を使用してください。

Apresia3424GT-HiPoE は Ver. 7.19.01 より前のバージョン、または HCLoader が Ver. 1.09.00 より前のバージョンの場合、装置が起動しません。必ずローダ＿ファームウェアバージョン対応表に示した組み合わせの HCLoader バージョンをご使用ください。

Apresia4300 シリーズにおいて、Ver. 7.09.01 以前から、Ver. 7.24.01 以降へバージョンアップする場合、一度、Ver. 7.10.01～7.23.02 へバージョンアップ後に Ver. 7.24.01 以降へバージョンアップしてください。

3.57.2 archive download-loader

TFTP サーバー、または SD メモリーカードからローダーソフトウェアをダウンロードします。ダウンロードしたソフトウェアはリブート後に反映されます。

Apresia3400/4300/5400 シリーズと Apresia13000 シリーズでは、使用できるローダーソフトウェアが異なります。

Apresia3400/4300/5400 シリーズでは、公式リリースされているローダーソフトウェアの Version 番号の 2 桁目が、"02"以降で表記されるローダーソフトウェアを使用してください。なお、実際の運用では、ローダーソフトウェア名を変更して使用できます。

対応ローダーソフトウェア

Apresia3400/4300/5400 シリーズ	Ver. 1.02.XX (aeosR7XXXX-loader-x300.img)
Apresia13000 シリーズ	Ver. 1.01.XX (aeosR7XXXX-loader.img)

コマンドシンタックス

archive download-loader (tftp <IPADDR>) | memory-card <FILE>

IPADDR	TFTP サーバーの IP アドレス
FILE	ローダーソフトウェアのファイル名

コマンドモード

ENABLE

使用例

(1) IP アドレス：172.21.29.202 の TFTP サーバーからファイル名：aeosR70401-loader.img のローダーソフトウェアをダウンロードします。

```
# archive download-loader tftp 172.21.29.202 aeosR70401-loader.img
override? (y/n): y
getting from 172.21.29.202: aeosR70401-loader.img
Received 189992 bytes in 0.5 seconds
Filesize is 189992 bytes
Writing ... done.
```

(2) SD メモリーカードからファイル名：aeosR70401-loader.img のローダーソフトウェアをダウンロードします。

```
# archive download-loader memory-card aeosR70401-loader.img
override? (y/n): y
Filesize is 191016 bytes
Writing ... done.
```

関連コマンド

注意事項

未サポートのローダーソフトウェア、もしくはローダーソフトウェア以外をダウンロードしないでください。ダウンロードした場合、装置が起動しません。

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

3.57.3 archive upload-sw

装置内のファームウェアを TFTP サーバー、または SD メモリーカードへアップロードします。

Apresia3400/4300/5400 シリーズではファイル名の後に secondary を指定することにより、セカンダリー領域のファームウェアをアップロードします。secondary 未指定の場合はプライマリー領域のファームウェアをアップロードします。

コマンドシンタックス

archive upload-sw (tftp <IPADDR>) | memory-card <FILE> [secondary]

IPADDR	TFTP サーバーの IP アドレス
FILE	アップロード先のファイル名
secondary	セカンダリー領域指定

コマンドモード

ENABLE

使用例

(1) 装置内のファームウェアをファイル名：apresia.img として IP アドレス：172.17.33.21 の TFTP サーバーへアップロードします。

```
# archive upload-sw tftp 172.17.33.21 apresia.img
Sent 5582035 bytes in 26.4 seconds
```

(2) 装置内のファームウェアをファイル名：apresia.img として SD メモリーカードへアップロードします。

```
# archive upload-sw memory-card apresia.img
upload completed.(apresia.img)
CRC Checking.
Ok.
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

ファイル名として、..を含む文字列は使用できません。

/はディレクトリ指定として扱われます。

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.57.4 archive upload-loader

装置内のローダーソフトウェアを TFTP サーバー、または SD メモリーカードへアップロードします。

コマンドシンタックス

archive upload-loader (tftp <IPADDR>) | memory-card <FILE>

IPADDR	TFTP サーバーの IP アドレス
FILE	ローダーソフトウェアのファイル名

コマンドモード

ENABLE

使用例

(1) 装置内のローダーソフトウェアをファイル名：aeosR71901-loader.img として IP アドレス：172.17.33.21 の TFTP サーバーへアップロードします。

```
# archive upload-loader tftp 172.17.33.21 aeosR71901-loader.img
Sent 103200 bytes in 2.2 seconds
```

(2) 装置内のローダーソフトウェアをファイル名：aeosR71901-loader.img として SD メモリーカードへアップロードします。

```
# archive upload-loader memory-card aeosR71901-loader.img
upload completed.(aeosR71901-loader.img)
```

関連コマンド

注意事項

- ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。
- ファイル名として、..を含む文字列は使用できません。
- /はディレクトリ指定として扱われます。
- SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。
- ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.58 AEOS6 へのダウングレード(Apresia4348 シリーズ)

Apresia4348 シリーズは、AEOS Ver. 7 から AEOS Ver. 6 にダウングレードすることが可能です。

ダウングレードは、コマンド実行により TFTP サーバーから更新用ファイルをダウンロード(自動的に)再起動することにより行います。

3.58.1 archive downgrade-aeos6

AEOS7 から AEOS6 にファームウェアをダウングレードします。ダウングレード中(情報保存中)はコマンドを中断できません。PFILE/SFILE が AEOS6 用のファームウェアでない場合、処理は中止されます。

コマンドシンタックス

archive downgrade-aeos6 tftp <IPADDR> <PFILE> <SFILE> [<CFILE6>]

IPADDR	TFTP サーバーの IP アドレス
PFILE	AEOS6 のダウングレード用プライマリーファームウェア (AEOS62401_primary.rom のみ利用可能)
SFILE	AEOS6 のダウングレード用セカンダリーファームウェア (AEOS62402_secondary.img のみ利用可能)
CFILE6	AEOS6 形式の構成情報(指定がない場合は再起動後に構成情報が初期化)

コマンドモード

ENABLE

使用例

(1) IP アドレス:172.21.31.15 の TFTP サーバーからファイル名:apresia.img のファームウェアに更新します。

```
# archive downgrade-aeos6 tftp 172.21.31.15 AEOS62401_primary.rom
AEOS62402_secondary.img u_d.conf
override? (y/n): y
getting from 172.21.31.15:AEOS62401_primary.rom
Received 5051426 bytes in 20.2 seconds
Testing image ... OK.
getting from 172.21.31.15:AEOS62402_secondary.img
Received 2574223 bytes in 10.3 seconds
Testing image ... OK.
getting from 172.21.31.15:u_d.conf
Received 1766 bytes in 0.0 seconds
Writing ... done.
```

関連コマンド

注意事項

本機能は、AEOS Ver. 7.09.01 以降でのみ有効です。

本機能は、Apresia4348 シリーズでのみ有効です。

AEOS Ver. 6 へのダウングレード後でも以下の設定は保存されます。
ライセンス情報
SSH RSA 鍵(3.35.1 "sshd keygen rsa"/3.35.2 "sshd keygen rsa1"で作成)
SSL 証明書、秘密鍵、CSR(3.45.1 "ssl gencsr rsakey"で作成)

"reboot"コマンド実行時に現行 AEOS Ver. 6 はフラッシュメモリーにログの内容の保存を行いますが、本コマンド実行による再起動については、フラッシュメモリーへログの書き込みを行いません。

フラッシュメモリーへのファームウェアの書き込み開始以降、本コマンドを中断することはできません。

3.47 AccessDefender のローカルデータベース(3.46.46 "copy tftp local-db")と Web 認証ページ(3.47.65 "copy file WEB-PAGE")は、ダウングレード後に初期化されます。

AEOS6 からアップグレードする際は、AEOS6 コマンドリファレンス(AEOS Ver. 6.24.02 以降)のアップグレードコマンド("archive upgrade-aeos7")を参照ください。

3.59 CPU 使用率通知

3.59.1 cpu-utilization-notify threshold polling

CPU 使用率(過去 1 分平均)が一定以上になった場合にトラップ、syslog による通知を行う機能を有効にします。無効にする場合は、no コマンドを使用してください。

本機能を有効にするには、通知を行う CPU 使用率(%)の閾値(<THRESHOLD-VALUE>)とポーリング間隔(<INTERVAL>)を設定します。閾値は、5 %単位で設定します。5 %未満の入力値に対しては、これを超えない最も小さな 5 %単位の値が保持されます。例えば 79 %が入力された場合、75 %として設定/保持され、3.61.16 "show system"、3.49.1 "show running-config"コマンドにおいても 75 %と表示されます。ポーリング間隔は 1 秒単位で設定できます。

コマンドシンタックス

cpu-utilization-notify threshold <THRESHOLD-VALUE> polling <INTERVAL>
no cpu-utilization-notify

THRESHOLD-VALUE	CPU 使用率の閾値 <50-100(%)>
INTERVAL	ポーリング間隔 <10-300(秒)>

デフォルト

なし(＝無効：CPU 使用率が一定以上かの確認なし/トラップ、syslog による通知なし)

コマンドモード

CONFIG

使用例

(1) 閾値を 70 %、ポーリング間隔を 60 秒として設定します。
(2) 設定を無効にします。

```
> enable
# configure terminal
(config)# cpu-utilization-notify threshold 70 polling 60
(config)# no cpu-utilization-notify
```

関連コマンド

show running-config, show system

注意事項

ポーリング間隔が短いと CPU 使用率が若干増加します。

3.59.2 clear cpu-utilization history

3.61.16 "show system"コマンドによる表示、及び MIB による取得が可能な CPU 使用率をゼロクリアします。

コマンドシンタックス

clear cpu-utilization history

コマンドモード

ENABLE

使用例

(1) CPU 使用率をゼロクリアします。

```
# clear cpu-utilization history
# show system
Hardware Model   : Apresia13000-48X
MAC Address      : 00:40:66:13:09:73
Serial Number    : 02060244
UpTime           : 6 days, 21:55:23.343
CPU Rate(2sec, %): 0
CPU Rate(1min, %): 0
CPU Rate(5min, %): 0
CPU Rate(max, %) : 0
CPU Rate(min, %) : 0
-------------------------------
Notification threshold:
  cpu-utilization(%)  : disable
Health Status         : Normal(0x0)
```

関連コマンド

注意事項

現在の CPU 使用率、CPU 使用率の最大値は、表示のためのコマンド入力により即座に増加するため、通常 0 になることはありませんが異常ではありません(例：CPU 使用率をゼロクリア後、表示のため"show system"コマンド入力した場合、本コマンド入力自体に要した CPU 使用率が表示されるため、CPU 使用率が 0 と表示されない)。

本コマンド実行時、CPU 使用率の最小値はしばらく 0 のままになりますが異常ではありません。

3.60 メモリー使用容量通知

3.60.1 memory-used-notify threshold polling

メモリー使用容量(使用中のメモリー容量)が一定以上になった場合にトラップ、syslog による通知を行う機能を有効にします。無効にする場合は、no コマンドを使用してください。

本機能を有効にするには、通知を行うメモリー使用容量の閾値<THRESHOLD_VALUE>とポーリング間隔<INTERVAL>を設定します。

閾値を使用中のメモリー使用容量以下の値として設定した場合、次回のメモリー使用容量確認時から、トラップ、syslog による通知が行われます。ポーリング間隔は 1 秒単位で設定できます。

コマンドシンタックス

memory-used-notify threshold <THRESHOLD_VALUE> polling <INTERVAL>
no memory-used-notify

THRESHOLD_VALUE	メモリー使用容量の閾値 <10000-10000000(ページ)>
INTERVAL	ポーリング間隔 <10-300(秒)>

デフォルト

なし(＝無効：メモリー使用容量が一定以上かの確認なし/トラップ、syslog による通知なし)

コマンドモード

CONFIG

使用例

(1) 閾値を 10000(アクティブな仮想ページ数)、ポーリング間隔を 60 秒に設定します。
(2) 設定を無効にします。

```
> enable
# configure terminal
(config)# memory-used-notify threshold 10000 polling 60
(config)# no memory-used-notify
```

関連コマンド

show vmstat, show running-config

注意事項

ポーリング間隔が短いと CPU 使用率が若干増加します。

3.61 保守/運用コマンド

3.61.1 ping

指定した装置に対して PING を実行します。終了するときは[Ctrl+C]を入力してください。本装置に設定されていない IP アドレスや管理ポートに設定されている IP アドレスを送信元 IP アドレスに指定できません。

コマンドシンタックス

ping <IPADDR1> [<*OPTIONS*>]

OPTIONS には、以下のオプションを複数指定可能

OPTIONS = (count <COUNT>) | (interval <INTERVAL>) | (size <SIZE>) | (timeout <TIMEOUT>) | (source <IPADDR2>)

IPADDR1	PING の宛先 IP アドレス
IPADDR2	送信元 IP アドレス
COUNT	PING の試行回数 <0-10000(回)> • 0 を指定した場合、[Ctrl+C]キーが入力されるまで、繰り返し実行
INTERVAL	PING 送信間隔 <1-3600(秒)>
SIZE	ICMP パケットのデータサイズ <8-65467(バイト)>
TIMEOUT	応答待ち時間 <1-20(秒)>

デフォルト

COUNT：4(回)
INTERVAL：1(秒)
SIZE：56(バイト)
TIMEOUT：1(秒)

コマンドモード

VIEW, ENABLE

使用例

(1) IP アドレス：172.17.51.1 に対して、PING による疎通確認を行います。

```
# ping 172.17.51.1
PING 172.17.51.1 (172.17.51.1): 56 data bytes
64 bytes from 172.17.51.1: icmp_seq=0 ttl=255 time=0.625 ms
64 bytes from 172.17.51.1: icmp_seq=1 ttl=255 time=0.728 ms
64 bytes from 172.17.51.1: icmp_seq=2 ttl=255 time=0.700 ms
64 bytes from 172.17.51.1: icmp_seq=3 ttl=255 time=0.773 ms

----172.17.51.1 PING Statistics----
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.625/0.707/0.773/0.062 ms
#
```

関連コマンド

注意事項

AEOS Ver. 7.31 以前のファームウェアでは、応答待ち時間が 4 秒固定となります。その他は、デフォルト値と同じ値です。

本コマンドは疎通確認を行うためのものであり、場合によっては応答時間に差があります。応答時間については、あくまでも目安としてお考えください。

3.61.2 traceroute

本装置から送信されたフレームが、指定した宛先までに通る経路を表示します。中断するときは[Ctrl+C]を入力してください。送信元 IP アドレスには本装置に設定されていない IP アドレスや管理ポートに設定されている IP アドレスを指定できません。

コマンドシンタックス

traceroute <IPADDR1> [source <IPADDR2>]

IPADDR1	宛先 IP アドレス
IPADDR2	送信元 IP アドレス

コマンドモード

VIEW, ENABLE

使用例

(1) IP アドレス：172.17.8.1 までの通信経路を表示します。

```
# traceroute 172.17.8.1
traceroute to 172.17.8.1 (172.17.8.1), 30 hops max, 40 byte packets
 1  172.17.51.1 (172.17.51.1)  0.002 ms  0.603 ms  0.004 ms
 2  172.17.33.1 (172.17.33.1)  0.004 ms  1.026 ms  0.004 ms
 3  172.17.8.1 (172.17.8.1)  0.004 ms  0.012 ms  15.316 ms
#
```

関連コマンド

注意事項

3.61.3 telnet

指定したアドレスに対して TELNET を行います。

コマンドシンタックス

telnet <IPADDR> [<PORT>]

IPADDR	TELNET の宛先 IP アドレス
PORT	TELNET サーバーの TCP ポート番号

コマンドモード

VIEW, ENABLE

使用例

(1) IP アドレス：172.17.51.177 の装置に TELNET を行います。

```
# telnet 172.17.51.177
Trying 172.17.51.177...
Connected to 172.17.51.177.
Escape character is '^]'.

Ethernet Switch Apresia13000-48X

login:
```

関連コマンド

注意事項

設定保存"write memory"実行中には、装置のリセットボタンの使用、電源断などのリブート動作を行わないでください。

3.61.4 debug

デバッグ用ログ出力機能を有効にします。無効にする場合は、no コマンドを使用してください。本コマンドで有効にしたデバッグログを表示させるには、3.33.4 "terminal monitor"コマンドをあわせて設定する必要があります。no debug all で全デバッグオプションを解除できます。

コマンドシンタックス

[no] debug nsm [all | events | kernel | (packet [recv | send] [detail])]
[no] debug dot1x [all | event | nsm | packet | timer]
[no] debug lacp all | event | packet | sync | timer
no debug all
※ ただし、カッコ内の引数が複数指定可能

nsm	管理機能に関するログ出力を有効
dot1x	IEEE 802.1X に関するログ出力を有効
lacp	lacp に関するログ出力を有効
all	管理機能の全デバッグ情報
events	イベント情報
kernel	基本ソフトに関する情報
packet	管理情報部がやりとりするパケットに関する情報
recv	受信パケット
send	送信パケット

コマンドモード

CONFIG

使用例

(1) 管理機能のデバッグ出力を有効にします。

```
(config)# debug nsm all
# Jun 22 16:54:37  NSM[132]: NSM: If-arbiter timer expire
Jun 22 16:54:37  NSM[132]: NSM: interface fib0 index 1
Jun 22 16:54:37  NSM[132]: NSM: interface fib1 index 2
Jun 22 16:54:37  NSM[132]: NSM: interface manage index 3
Jun 22 16:54:37  NSM[132]: NSM: interface loopback index 4
Jun 22 16:54:37  NSM[132]: NSM: [raw0]: 1000 MB link speed
Jun 22 16:54:37  NSM[132]: NSM: interface raw0 index 5
Jun 22 16:54:37  NSM[132]: NSM: interface port1 index 6
```

関連コマンド

terminal monitor

注意事項

debug 機能を有効にした場合、本装置の性能に若干影響を及ぼす可能性がありますので、通常運用時には debug 機能を無効にしてください。また、使用する場合には、必ず事前にサポート対応窓口にご相談のうえ、指示に従ってください。

3.61.5 backup tftp, backup memory-card

本装置に保存されている各種ファイルを TFTP サーバー、または SD メモリーカードへ一括アップロードします。アップロード対象ファイルを表 3-60 に示します。

オプション no-access-defender を指定した場合、3.47 AccessDefender 関連ファイル(aaa-local-db、login-page、login-success-page、login-failure-page、logout-success-page、logout-failure-page、redirect-error-page、https-certificate、https-private-key)はアップロードされません。

オプション no-software を指定した場合、software、loader はアップロードされません。

アップロードにより作成されるファイル名は<BASENAME>-xxx となります。

例)<BASENAME>に AEOS を指定した場合のファイル名

AEOS-flash-config、AEOS-software 等

表 3-60 アップロード対象ファイル

対象ファイル	説明
flash-config	flash-config
running-config	running-config
software	ファームウェア
loader	ローダーソフトウェア
aaa-local-db	ローカルデータベース
login-page	ログイン認証ページ
login-success-page	認証成功ページ
login-failure-page	認証失敗ページ

対象ファイル	説明
logout-success-page	ログアウト成功ページ
logout-failure-page	ログアウト失敗ページ
redirect-error-page	リダイレクト失敗ページ
https-certificate	証明書
https-private-key	秘密鍵
ssh-rsa-key	RSA ホスト鍵対(SSH プロトコルバージョン 2)
ssh-rsa1-key	RSA ホスト鍵対(SSH プロトコルバージョン 1)

コマンドシンタックス

backup (tftp <IPADDR>) | memory-card <BASENAME> [no-access-defender] [no-software]

IPADDR　　TFTP サーバーの IP アドレス

BASENAME　　ファイル名 <1-64(文字)>

コマンドモード

ENABLE

使用例

(1) 装置内の各種ファイルをファイル名：AEOS として、IP アドレス：172.17.33.21 の TFTP サーバーへ一括アップロードします。

```
# backup tftp 172.17.33.21 AEOS
Upload flash-config ...
Sent 1455 bytes in 0.1 seconds

Upload running-config ...
Sent 1455 bytes in 0.0 seconds

Upload software ...
Sent 5582035 bytes in 25.2 seconds

Upload loader ...
Sent 103200 bytes in 2.6 seconds
        (中略)
Upload ssh-rsa-key ...
Upload ssh-rsa1-key ...
```

(2) 装置内の各種ファイルをファイル名：AEOS として、SD メモリーカードへ一括アップロードします。

```
# backup memory-card AEOS
Upload flash-config ...
upload completed.(AEOS-flash-config)

Upload running-config ...
upload completed.(AEOS-running-config)

Upload software ...
```

```
upload completed.(AEOS-software)
CRC Checking.
Ok.

Upload loader ...
upload completed.(AEOS-loader)
       (中略)
Upload ssh-rsa1-key ...
upload completed.(AEOS-ssh-rsa1-key)
```

関連コマンド

注意事項

ファイル名として、&;`'¥"|*?~<>^()[]{}$の各文字は使用できません。

SD メモリーカードに作成可能な最大ファイル数は、FAT16 ファイルシステムの仕様に依存します。そのため、SD メモリーカードに空き容量があったとしても、ファイル数の制限により保存できない場合があります。SD メモリーカードに大量のファイルを保存する場合は、あらかじめ SD メモリーカードにサブディレクトリを作成して保存することを推奨します。

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.61.6 backup clone

本装置に保存されている運用情報(ブートスクリプト、ファームウェア、構成情報)を SD メモリーカードへ一括アップロードします。ブートスクリプト(flash を除く)には、本コマンドによりアップロードした運用情報で起動するように保存されます。アップロード対象ファイルを表 3-61 に示します。

表 3-61 アップロード対象ファイル

対象ファイル	説明
flash-config	flash-config
hc-software	装置に保存されているファームウェア
hc-system-name.txt	装置に保存されているファームウェアのシステムバージョン
hcloader.conf	SD メモリーカード起動ブートスクリプト

コマンドシンタックス

backup clone

コマンドモード

ENABLE

使用例

(1) 本装置に保存されている運用情報を SD メモリーカードへ一括アップロードします。

```
# backup clone
Upload flash-config ...
upload completed.(hc-flash-config)

Upload hc-system-name.txt ...
upload completed.(hc-system-name.txt)

Upload software ...
upload completed.(hc-software)
CRC Checking.
Ok.

Upload boot-script ...
upload completed.(hcloader.conf)

#
```

関連コマンド

注意事項

ファイルのアップロード時に"Verify Error: CRC Mismatch."が表示された場合、SD メモリーカードに正しくファイルが作成されていない可能性があります。SD メモリーカードを挿し直して、コマンドを再実行してください。その後も本ログが出力する場合は、SD メモリーカードを交換してください。

3.61.7 restore

TFTP サーバー、または SD メモリーカードから各種ファイルを一括ダウンロードします。ダウンロード対象ファイルを表 3-62 に示します。

オプション no-access-defender を指定した場合、AccessDefender 関連ファイル(aaa-local-db、login-page、login-success-page、login-failure-page、logout-success-page、logout-failure-page、redirect-error-page、https-certificate、https-private-key)はダウンロードされません。

オプション no-software を指定した場合、software、loader はダウンロードされません。

オプション reboot を指定した場合、ダウンロード終了後、全ファイルを装置のフラッシュメモリーに保存した状態で本装置が再起動します。ただし、全ファイルのダウンロードに失敗した場合は再起動しません。

オプション reboot を指定しなかった場合、ダウンロード終了後に本装置は再起動しませんが、ダウンロードのみでは RSA ホスト鍵対(ssh-rsa-key、ssh-rsa1-key)は装置のフラッシュメモリーに保存されません。装置のフラッシュメモリーへ RSA ホスト鍵対を保存する場合はダウンロード後、"write

memory"コマンドの実行が必要になります。ただし、本コマンド実行後に"write memory"コマンドを実行すると、起動中の構成情報でダウンロードした flash-config を更新することになるため、オプション reboot を指定して実行することを推奨します。

表 3-62 ダウンロード対象ファイル

対象ファイル	説明
flash-config	flash-config
software	ファームウェア
loader	ローダーソフトウェア
aaa-local-db	ローカルデータベース
login-page	ログイン認証ページ
login-success-page	認証成功ページ
login-failure-page	認証失敗ページ
logout-success-page	ログアウト成功ページ
logout-failure-page	ログアウト失敗ページ
redirect-error-page	リダイレクト失敗ページ
https-certificate	証明書
https-private-key	秘密鍵
ssh-rsa-key	RSA ホスト鍵対(SSH プロトコルバージョン 2)
ssh-rsa1-key	RSA ホスト鍵対(SSH プロトコルバージョン 1)

コマンドシンタックス

restore (tftp <IPADDR>) | memory-card <BASENAME> [no-access-defender] [no-software] [reboot]

IPADDR　　TFTP サーバーの IP アドレス

BASENAME　　ファイル名 <1-64(文字)>

コマンドモード

ENABLE

使用例

(1) IP アドレス：172.17.33.21 の TFTP サーバーから各種ファイルを一括ダウンロードします。

```
# restore tftp 172.17.33.21 AEOS
override? (y/n): y
getting from 172.20.32.247:AEOS-flash-config
Received 1455 bytes in 0.3 seconds
Writing to flash memory...
done.
This setting is validated after rebooting
        (中略)
getting from 172.20.32.247:AEOS-ssh-rsa-key
getting from 172.20.32.247:AEOS-ssh-rsa-key.pub
getting from 172.20.32.247:AEOS-ssh-rsa1-key
getting from 172.20.32.247:AEOS-ssh-rsa1-key.pub
```

(2) SD メモリーカードから各種ファイルを一括ダウンロードします。

```
# restore memory-card AEOS
override? (y/n): y
Download flash-config ...
Writing to flash memory...
done.
This setting is validated after rebooting.
       (中略)
Download ssh-rsa-key ...
done.
Download ssh-rsa1-key ...
done.
Writing to flash memory...
done.
```

関連コマンド

注意事項

3.47.10 "web-authentication https-port"が設定されている場合、証明書、秘密鍵はダウンロードできません。ダウンロードする場合は、いったん"web-authentication https-port"の設定を削除してください。

3.61.8 tftp source

TFTP サーバーへ送信するパケットの送信元 IP アドレスを設定します。設定を削除する場合は、no コマンドを使用してください。送信元 IP アドレス未設定の場合、本装置が選択した送信元 IP アドレスが使用されます。

ループバック IP アドレス(127.0.0.0～127.255.255.255)、クラス D(224.0.0.0～239.255.255.255)、クラス E(240.0.0.0～255.255.255.255)は送信元 IP アドレスに指定できません。対象コマンドを表 3-63 に示します。

表 3-63 送信元 IP アドレス指定対象コマンド

3.35.11 copy file ssh-key
3.35.12 copy ssh-key file
3.45.2 copy csr tftp
3.45.3 copy file https-file
3.45.4 copy https-file file
3.46.46 copy tftp local-db
3.46.47 copy local-db tftp
3.47.65 copy file WEB-PAGE
3.47.66 copy WEB-PAGE file
3.47.67 copy file aaa-local-db
3.47.68 copy aaa-local-db file
3.50.3 copy tftp server file flash-config

```
3.50.4 copy flash-config tftp server file
3.50.5 copy running-config file
3.53.1 auto-download
3.54.3 copy tftp memory-card
3.57.1 archive download-sw
3.57.2 archive download-loader
3.57.3 archive upload-sw
3.57.4 archive upload-loader
3.58.1 archive downgrade-aeos6
3.61.5 backup tftp, backup memory-card
3.61.7 restore
```

コマンドシンタックス

tftp source <IPADDR>
no tftp source

IPADDR	送信元 IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) TFTP サーバーへ送信するパケットの送信元 IP アドレスを 192.168.100.1 に設定します。

```
> enable
# configure terminal
(config)# tftp source 192.168.100.1
(config)# no tftp source
```

関連コマンド

注意事項

3.61.9 memory-error auto-recovery-mode enable

メモリーエラー自動復旧機能を有効に設定します。無効にする場合は、no コマンドを使用してください。無効にすると、構成情報より本コマンドが削除され、"memory-error auto-recovery-mode disable" が書き込まれます。

メモリーエラー自動復旧機能が有効の状態でスイッチ LSI のメモリーエラーを検知した場合、自動で復旧動作を行います。また、同じメモリーでメモリーエラーの多発を検知した場合、そのメモリーを監視対象外として、スイッチ LSI のメモリー状態が異常になります。監視対象外となったメモリーに対しては、自動復旧は行いません。

メモリーエラー自動復旧機能の設定を変更した場合、"clear memory-error"コマンド実行時と同様に、スイッチ LSI のメモリー状態を正常に戻し、メモリーエラー検出により監視対象外となったメモリーを

メモリーエラーの監視対象に戻すとともに、メモリーエラー自動復旧の回数、及び復旧不可能なメモリーエラーの発生回数のカウントをクリアします。

コマンドシンタックス

[no] memory-error auto-recovery-mode enable

デフォルト

AEOS Ver 7.36.XX 以前：no enable(＝無効)
AEOS Ver 7.37.01 以降：enable(＝有効)

コマンドモード

CONFIG

使用例

(1) メモリーエラー自動復旧を有効に設定します。
(2) メモリーエラー自動復旧を無効に設定します。

```
(config)# memory-error auto-recovery-mode enable
(config)# no memory-error auto-recovery-mode enable
```

関連コマンド

show system, show hardware, clear memory-error, show running-config

注意事項

AEOS Ver. 7.37 以降より、フラッシュメモリーに保存されている構成情報に本コマンドが書き込まれていない状態で装置を起動した場合、自動的にメモリーエラー自動復旧機能が有効化され、現在起動中の構成情報に本コマンドが書き込まれます。そのため、フラッシュメモリーに保存されている構成情報とは差異が発生します。この場合、3.50.2 "write memory"コマンドを実行してフラッシュメモリーに書き込んでください。

3.61.10 memory-error auto-recovery-mode notify disable

メモリーエラー自動復旧時のトラップ、syslog による通知を無効に設定します。有効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] memory-error auto-recovery-mode notify disable

デフォルト

no disable(＝有効)

コマンドモード

CONFIG

使用例

(1) メモリーエラー自動復旧時のトラップ、syslogによる通知を無効にします。
(2) メモリーエラー自動復旧時のトラップ、syslogによる通知を有効にします。

```
(config)# memory-error auto-recovery-mode notify disable
(config)# no memory-error auto-recovery-mode notify disable
```

関連コマンド

show hardware, memory-error auto-recovery-mode enable, snmp-server traps, show running-config

注意事項

3.61.11 error-frame threshold polling-rate

各ポートにおいて、指定したエラー種別のフレームカウンターを監視し、一定以上になった場合にsyslog、トラップによる通知を行う機能を有効にします。無効にする場合は、noコマンドを使用してください。各機能のメンバーポートについて監視を行う場合は、それぞれに所属している全メンバーポートに設定してください。エラー種別のフレームカウンターを複数監視する場合、エラー種別ごとにそれぞれ設定してください。

本機能を有効にするには、監視を行うエラー種別のフレームカウンター閾値<THRESHOLD_VALUE>とポーリング間隔<RATE>を設定します。各エラー種別のフレームカウンターは、3.7.16 "show interface counters"コマンドで表示されるカウンターとは異なるカウンターを使用し、設定したポーリング間隔が経過する度に値をクリアします。ポーリング間隔は、polling-rate × 5秒(最小ポーリング間隔)となります。設定するカウンター閾値は、設定したポーリング間隔での閾値となります。

shutdownオプションを指定した場合は、閾値を超えたときに当該ポートを閉塞("shutdown")します。shutdownオプションにより閉塞が発生すると、当該物理ポートに3.7.1 "shutdown"コマンドが自動的に設定されます。閉塞を解除する場合は、当該物理ポートに対して"no shutdown"コマンドを実行してください。

設定を変更する場合、本コマンドを再度実行すれば上書き設定され、ポーリング途中でも即時反映されます。

コマンドシンタックス

error-frame <*ERRORTYPE*> threshold <THRESHOLD_VALUE> polling-rate <RATE> [shutdown]
no error-frame <*ERRORTYPE*>
ERRORTYPE = fcs | alignment | fragments | jabbers | carrier-sense

THRESHOLD_VALUE	フレームカウンター閾値 <100-4294967295>
RATE	ポーリング間隔 <1-100> • ただしポーリング間隔とは、<RATE> (polling-rate) × 5秒(最小ポーリング間隔)のこと

デフォルト

なし(＝設定なし)

コマンドモード

IF-PORT

使用例

(1) ポート：1～5、8 において、FCS エラーフレームのフレームカウンター閾値を 100、polling-rate を 100 に設定します。

```
(config)# interface port 1-5,8
(config-if-port)# error-frame fcs threshold 100 polling-rate 100
```

(2) ポート：1～5、8 において、FCS エラーフレームのフレームカウンター閾値を 500、polling-rate を 1 に設定し、閾値を超えた場合に該当のポートを閉塞します。

```
(config)# interface port 1-5,8
(config-if-port)# error-frame fcs threshold 500 polling-rate 1 shutdown
```

(3) ポート：1～5、8 において、FCS エラーフレームのフレームカウンター閾値の設定を解除します。

```
(config)# interface port 1-5,8
(config-if-port)# no error-frame fcs
```

関連コマンド

snmp-server traps error-frame-threshold, show running-config

注意事項

受信フレームのカウンターを監視しているため、本コマンドによって syslog・トラップの出力(並びにポートの"shutdown")が発生したとしても、原因が当該ポートの故障とは限りません。エラーフレーム発生原因については対向装置(トランシーバー含む)、伝送路、本装置(トランシーバー含む)について切り分けが必要です。

ポートのリンクダウン/アップ時にエラーフレームとしてカウントする場合があります。

3.61.12 power-down-notify enable

電源断が発生した場合に syslog による通知を行う機能を有効にします。無効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] power-down-notify enable

デフォルト

なし(＝無効：電源断の確認なし/syslog による通知なし)

コマンドモード

CONFIG

使用例

(1) 電源断通知機能を有効にします。

(2) 電源断通知機能を無効にします。

```
> enable
# configure terminal
(config)# power-down-notify enable
(config)# no power-down-notify enable
```

関連コマンド

show running-config, show logging

注意事項

本コマンドは Apresia5412GT-PoE でのみ有効です。

電源断を検知した直後に電源が回復した場合、タイミングによって電源断通知の syslog を出力しますが、電源断は発生していない場合があります。

装置の設置環境によっては、syslog を出力するために必要な時間内に電圧が低下してしまい、syslog が出力されないことがあります。

3.61.13 show debugging

デバッグ用ログ出力機能の構成情報を表示します。

コマンドシンタックス

show debugging [dot1x | igmp | lacp | nsm | ospf | pim | rip | vrrp]

dot1x	IEEE 802.1X に関するログ出力の構成情報
igmp	IGMP に関するログ出力の構成情報
lacp	LACP に関するログ出力の構成情報
nsm	管理機能に関するログ出力の構成情報
ospf	OSPF に関するログ出力の構成情報
pim	PIM に関するログ出力の構成情報
rip	RIP に関するログ出力の構成情報
vrrp	VRRP に関するログ出力の構成情報

コマンドモード

ENABLE

使用例

(1) デバッグログ出力の設定を表示します。

```
# show debugging nsm
NSM debugging status:
  NSM event debugging is on
  NSM packet detail debugging is on
  NSM kernel debugging is on
```

関連コマンド

注意事項

3.61.14 show version

ファームウェア、ローダーソフトウェアのバージョン情報を表示します。

コマンドシンタックス

show version

コマンドモード

VIEW, ENABLE

使用例

(1) バージョン情報を表示します。

```
# show version
System Revision          : 7.32.01
System Date              : Wed Dec  4 13:31:47 2013
System Booted from       : memory-card (hc-software)
Configuration Booted with: memory-card (hc-flash-config)
HCLoader Revision        : 1.11.02
HCLoader Date            : Fri Jul 26 17:12:32 2013
Compiled by              : compiler
Hardware Revision        : 0
```

System Revision　：動作中ファームウェアのバージョン
System Date　：動作中ファームウェアの作成日
System Booted from　：動作中ファームウェアの起動元
　primary　：フラッシュメモリーのプライマリーファームウェア
　secondary　：フラッシュメモリーのセカンダリーファームウェア
　memory-card (<FILENAME>)　：SD メモリーカードのファームウェア(ファイル名)
Configuration Booted with　：動作中構成情報の起動元
　Primary　：フラッシュメモリーのプライマリー構成情報
　Secondary　：フラッシュメモリーのセカンダリー構成情報
　memory-card (<FILENAME>)　：SD メモリーカードの構成情報(ファイル名)
　default　：デフォルト(工場出荷時)の構成情報
HCLoader Revision　：ローダーソフトウェアのバージョン
HCLoader Date　：ローダーソフトウェアの作成日
Compiled by　：コンパイル元(正式リリースの証明)
Hardware Revision　：ハードウェアリビジョンの識別子
　(Rev. A、B、C...などに依存せず"0"固定)

関連コマンド

注意事項

ローダーソフトウェアのバージョンが 1.00 以前の場合、HCLoader Revision、及び HCLoader Date は UNKNOWN と表示されます。

起動設定でプライマリーファームウェアは、フラッシュメモリー内のプライマリー領域を指定しているにも関わらず、意図せずセカンダリーファームウェアで起動した場合、フラッシュメモリーのプライマリー領域が故障している可能性があります。その場合は、サポート対応窓口にお問い合わせください。

3.61.15 show version flash

装置内部メモリーに保存されているプライマリー/セカンダリーファームウェア、ローダーソフトウェアのバージョンを表示します。バージョンが、AEOS Ver. 7.15.01 より前のファームウェア、及びローダーソフトウェア(ローダーソフトウェアバージョン 1.06.00 より前)の場合は、Unknown と表示されます。

detail オプションを指定することにより、装置内部のファームウェアの状態を表示します。

コマンドシンタックス

show version flash [detail]

コマンドモード

VIEW, ENABLE

使用例

(1) 装置のプライマリー/セカンダリーファームウェア、ローダーソフトウェアのバージョン情報を表示します。

```
# show version flash
Primary System   : 7.15.01
Secondary System : 7.15.01
HCLoader         : 1.06.00
#
# show version flash detail
Primary System   : 7.15.01(Normal)
Secondary System : 7.15.01(Normal)
HCLoader         : 1.06.00(Normal)
#
```

Primary System　：プライマリーファームウェアのバージョン(状態)
Secondary System　：セカンダリーファームウェアのバージョン(状態)
HCLoader　：ローダーソフトウェアのバージョン(状態)
(状態)Normal：正常、Broken：異常、Unknown：判別不明
Unknown　：以下のバージョンを使用している場合
- プライマリー/セカンダリーファームウェア Ver. 7.15.01 より前

- ローダーソフトウェア Ver. 1.06.00 より前

関連コマンド

注意事項

Broken が表示された場合は、サポート対応窓口に連絡してください。

SD メモリーカード内のファームウェアのバージョンは表示されません。

3.61.16 show system

ファームウェアのシステム情報、装置の MAC アドレス、CPU 使用率の設定を表示します。

コマンドシンタックス

show system

コマンドモード

VIEW, ENABLE

使用例

(1) システム情報、MAC アドレス、CPU 使用率を表示します(Apresia13000-48X)。

```
# show system
Hardware Model    : Apresia13000-48X
MAC Address       : 00:40:66:12:a3:f7
Serial Number     : 02060004
UpTime            : 1 year, 2 days, 00:00:04.228
CPU Rate(2sec, %): 2
CPU Rate(1min, %): 2
CPU Rate(5min, %): 2
CPU Rate(max, %) : 69
CPU Rate(min, %) : 0
-------------------------------
Notification threshold:
  cpu-utilization(%)  : disable
Health Status         : Normal(0x0)

#
```

(2) システム情報、MAC アドレス、CPU 使用率を表示します(Apresia5428GT)。

```
# show system
Hardware Model    : Apresia5428GT
MAC Address       : 00:40:66:54:5b:3d
UpTime            : 1 year, 2 days, 00:00:02.618
CPU Rate(2sec, %): 19
CPU Rate(1min, %): 7
```

```
CPU Rate(5min, %): 6
CPU Rate(max, %) : 31
CPU Rate(min, %) : 0
------------------------------
Notification threshold:
  cpu-utilization(%)  : disable
Health Status         : Normal(0x0)

#
```

Hardware Model　：ハードウェアタイプ
MAC Address　：MAC アドレス
Serial Number　：シリアルナンバー
UpTime　：システム稼動時間(最大で約 136 年まで表示可能)
- 年：YYY year(s)形式(YYY：1～136)
  - 1 年は 365 日固定で換算
  - 1 年未満の場合は省略
- 日：DDD day(s)形式(DDD：0～364)
  - 1 日未満の場合は省略
    ただし、1 年以上稼動している場合は"1 year, 0 day,"と表示
- 時間：HH:MM:SS.SSS 形式

CPU Rate　(2sec)　：現在の CPU 使用率(コマンド実行前から現在までの 2 秒間平均)
(1min)　：1 分前から現在までの CPU 使用率
(5min)　：5 分前から現在までの CPU 使用率
(max)　：5 分前から現在までの CPU 使用率の最大値
(min)　：5 分前から現在までの CPU 使用率の最小値
cpu-utilization(%)　：CPU 使用率通知の設定
Health Status　：システム状態(括弧内は障害コード)
Normal　：正常時
Abnormal　：異常時
障害コード
- bit14、16(0x4000、0x10000)スイッチ LSI のメモリーエラー
  (例：0x4000 はスイッチ LSI のメモリーエラーを示す)

関連コマンド

注意事項

Serial Number が表示されるのは、Apresia13000 シリーズのみです。Apresia3400/4300/5400 シリーズでは、Serial Number は表示されません。

スイッチ LSI のメモリーエラーが発生した場合、「4.10 装置の表示、エラーログに関連する現象と対策」を参照ください。

本ドキュメントに記載されていない障害コードが記録された場合、ハードウェア障害の可能性があるため、サポート対応窓口にお問い合せください。

3.61.17 show hardware

ハードウェアに関する情報を表示します。

"POWER" は、電源二重化モデルのみ表示されます。"TEMPERATURE" は、Apresia3448G-PSR(RevB)/3448G-PSR2/4348 シリーズ/5412GT-HRSS/5412GT-HRSS2/5412GT-HRSS-DC48V/5412GT-HRSS-DC110V/13000 シリーズのみ表示されます。

コマンドシンタックス

show hardware

コマンドモード

VIEW, ENABLE

使用例

(1) ハードウェアに関する情報を表示します。

```
# show hardware
  FAN
   FAN 1:   Normal
   FAN 2:   Normal
   FAN 3:   Normal
   FAN 4:   Normal
   FAN 5:   Normal

  TEMPERATURE
   Normal condition.

  SW-LSI MEMORY Status
   Normal
     Auto Recovery Mode        : Disabled
       Recovery Count          : 0
     Auto Recovery Notify      : Enabled
#
```

(2) ハードウェアに関する情報を表示します(電源二重化モデル)。

```
# show hardware
  POWER
   Power 1: Status:   Normal, FAN 1:   Normal, FAN 2:   Normal,
 Type: AC
   Power 2: Status: Abnormal, FAN 1: Abnormal, FAN 2: Abnormal,
Type: REMOVED

  TEMPERATURE
   Normal condition.
```

```
  SW-LSI MEMORY Status
   Normal
     Auto Recovery Mode        : Enabled
       Recovery Count          : 1
     Auto Recovery Notify      : Enabled
#
```

Power　：二重化電源状態
　Normal　：正常
　Abnormal　：異常
FAN　：電源内蔵 FAN 状態
　Normal　：正常
　Abnormal　：異常
　unknown　：不明
　NotRunning　：未動作(Apresia3424GT-HiPoE/3448GT/4328GT/5428GT のみ)
　internal　：装置内部の FAN(外から確認不可)
Type　：供給電源状態
　AC　：AC 電源供給
　DC　：DC 電源供給
　REMOVED　：電源未装着状態
TEMPERATURE　：外気温度状態
　Normal condition.　：外気温度正常状態
　[Alert] high threshold：外気温度異常状態
　(Apresia3448G-PSR(RevB)/3448G-PSR2/4348 シリーズは 50 ℃超、Apresia5412GT-HRSS/5412GT-HRSS2/5412GT-HRSS-DC48V/5412GT-HRSS-DC110V は 60 ℃超、Apresia13000 シリーズは 40 ℃超)
SW-LSI MEMORY Status　：スイッチ LSI のメモリー状態
　Normal　：正常
　Abnormal　：メモリーエラー発生状態
　メモリーエラー自動復旧機能無効：メモリーエラーの発生を検知
　メモリーエラー自動復旧機能有効：メモリーエラーの多発を検知
Auto Recovery Mode　：メモリーエラー自動復旧設定状態
　Enabled　：有効
　Disabled　：無効
Recovery Count　：メモリーエラーの自動復旧を行った回数
Auto Recovery Notify　：メモリーエラー自動復旧時の通知設定状態
　Enabled　：有効
　Disabled　：無効

(3) ハードウェアに関する情報を表示します(PoE モデル)。

```
# show hardware
  FAN
   FAN 1:   Normal
   FAN 2:   Normal
```

```
    FAN 3:   Normal

   PoE System
    Block 1: Normal
    Block 2: Abnormal

   SW-LSI MEMORY Status
    Abnormal
      Auto Recovery Mode        : Enabled
        Recovery Count          : 10
      Auto Recovery Notify      : Enabled
#
```

FAN　　：電源内蔵 FAN 状態
　Normal　　：正常
　Abnormal　　：異常
PoE　　：PoE システム状態
　Normal　　：正常
　Abnormal　　：異常
SW-LSI MEMORY Status　　：スイッチ LSI のメモリー状態
　Normal　　：正常
　Abnormal　　：メモリーエラー発生状態
　　メモリーエラー自動復旧機能無効：
　　メモリーエラーの発生を検知
　　メモリーエラー自動復旧機能有効：
　　メモリーエラーの多発を検知
Auto Recovery Mode　　：メモリーエラー自動復旧設定状態
　Enabled　　：有効
　Disabled　　：無効
Recovery Count　　：メモリーエラーの自動復旧を行った回数
Auto Recovery Notify　　：メモリーエラー自動復旧時の通知設定状態
　Enabled　　：有効
　Disabled　　：無効

(4) ハードウェアに関する情報を表示します(Apresia3424GT-SS)。

```
# show hardware
  SW-LSI MEMORY Status
   Normal
     Auto Recovery Mode        : Enabled
       Recovery Count          : 0
     Auto Recovery Notify      : Enabled
#
```

SW-LSI MEMORY Status　　：スイッチ LSI のメモリー状態
　Normal　　：正常
　Abnormal　　：メモリーエラー発生状態
　　メモリーエラー自動復旧機能無効：
　　メモリーエラーの発生を検知

メモリーエラー自動復旧機能有効：
メモリーエラーの多発を検知

Auto Recovery Mode　：メモリーエラー自動復旧設定状態
　Enabled　：有効
　Disabled　：無効
Recovery Count　：メモリーエラーの自動復旧を行った回数
Auto Recovery Notify　：メモリーエラー自動復旧時の通知設定状態
　Enabled　：有効
　Disabled　：無効

関連コマンド

注意事項

FAN の異常検出は FAN 停止によってのみ検出します。

電源二重化モデルでは、電源が供給されていない状態は、Abnormal と表示されます。

Recovery Count の値は、メモリーエラー自動復旧機能が有効時のみカウントされます。

Recovery Count の値は、メモリーエラー自動復旧機能の設定変更時、及び"clear memory-error"コマンドの実行によりクリアされます。

3.61.18 show history

入力されたコマンドの履歴を表示します。履歴は最大 15 コマンドまで保持されます。

コマンドシンタックス

show history

コマンドモード

VIEW, ENABLE

使用例

(1) 入力されたコマンドの履歴を表示します。

```
# show history
   enable
   conf t
   end
   show history
```

関連コマンド

注意事項

3.61.19 show tech-support

装置の各種情報を収集し表示します。表示される内容は、表 3-64 に示すコマンドにより収集可能な装置情報、及び装置内部のダンプ情報(独自形式にて表示)です。

表 3-64 コマンドにより収集可能な装置情報

show system
show version
show clock
show ip address
show ip interface brief
show running-config
show flash-config
show boot-script configured
show boot-script flash
show boot-script memory-card
show vlan
show logging
show logging sram
show interface status
show interface status detail
show interface counters [ポート番号]
show mac-address-table
show arp
show hardware
show poe status ※2
show poe power status ※2
show license
show ip route
show ip route cache ※1
show pbr status ※1
show memory-card files

※1 3.6.4 "show ip route cache"、及び"show pbr status"コマンドは、L3 ライセンスが有効のときのみ表示される。

※2 3.62.7 "show poe status"コマンド、及び 3.62.8 "show poe power status"コマンドは、PoE 対応機種(Apresia3424GT-PoE/3424GT-HiPoE/5412GT-PoE)のみ表示される。

コマンドシンタックス

show tech-support

コマンドモード

ENABLE

使用例

(1) 装置の各種情報を一括で取得します。

```
# show tech-support

*** show system ***
Hardware Model   : Apresia3448GT
MAC Address      : 00:40:66:34:48:33
UpTime           : 00:01:34.674
CPU Rate(2sec, %): 6
CPU Rate(1min, %): 19
CPU Rate(5min, %): 14
CPU Rate(max, %) : 100
CPU Rate(min, %) : 0
-------------------------------
Notification threshold:
  cpu-utilization(%)  : disable
Health Status         : Normal(0x0)



*** show version ***
System Revision          : 7.38.01
System Date              : Wed Mar  2 09:18:58 2016
System Booted from       : primary
Configuration Booted with: primary
HCLoader Revision        : 1.11.03
HCLoader Date            : Fri May 22 11:53:21 2015
Compiled by              : compiler
Hardware Revision        : 0


*** show clock ***
Wed Mar 02 10:20:59 2016


---(以下略) ---
```

関連コマンド

注意事項

Apresia3424GT-SS/3424GT-SS2 では、"show hardware"("show tech-support"内の表示も含む)は表示されません。

3.61.20 show netstat

装置のバッファメモリー情報を表示します。

コマンドシンタックス

show netstat -m

コマンドモード

VIEW, ENABLE

使用例

(1) バッファメモリー情報を表示します。

```
# show netstat -m
25 mbufs in use:
        17 mbufs allocated to data
        8 mbufs allocated to packet headers
20/28 mapped pages in use
80 Kbytes allocated to network (73% in use)
0 requests for memory denied
0 requests for memory delayed
0 calls to protocol drain routines
```

関連コマンド

注意事項

サポート対応窓口が必要とするソフトウェア情報を表示するコマンドです。サポート対応窓口から取得をお願いする場合があります。

3.61.21 show ps

動作中のプロセス情報を表示します。

コマンドシンタックス

show ps

コマンドモード

VIEW, ENABLE

使用例

(1) プロセス情報を表示します。

```
# show ps
USER  PID %CPU %MEM    VSZ   RSS TTY STAT STARTED    TIME COMMAND
root    0  0.0  0.9      0  4224 ?   DKs  10:01AM 0:00.01 swapper
root    1  0.0  0.4  79936  1584 ?   Is   10:01AM 0:00.02 init
root    2  0.0  0.9      0  4224 ?   DK   10:01AM 0:00.04 hcwdt
```

```
root    3  0.0  0.9      0  4224 ?   DK   10:01AM 0:00.01 sal:bcmDPC
root    4  0.0  0.9      0  4224 ?   DK   10:01AM 0:00.36 sal:PortMon.0
root    5  0.1  0.9      0  4224 ?   DK   10:01AM 3:42.63 sal:bcmCNTR.0
root    6  0.0  0.9      0  4224 ?   DK   10:01AM 0:00.01 sal:bcmTX
root    7  0.0  0.9      0  4224 ?   DK   10:01AM 0:00.01 sal:bcmXGS3Asyn
---(以下略)---
```

USER　　：ユーザー名
PID　　：プロセス番号
%CPU　　：CPU 使用率
%MEM　　：メモリー使用率
VSZ　　：仮想メモリー量
RSS　　：使用中の物理メモリー量
TTY　　：端末名
STAT　　：ステータス
STARTED　　：プロセス開始時間
TIME　　：経過時間
COMMAND　　：プロセスのコマンド名

関連コマンド

注意事項

サポート対応窓口が必要とするソフトウェア情報を表示するコマンドです。サポート対応窓口から取得をお願いする場合があります。

3.61.22 show vmstat

仮想メモリーの使用状況を表示します。

コマンドシンタックス

show vmstat

コマンドモード

VIEW, ENABLE

使用例

(1) 仮想メモリーの使用状況を表示します。

```
# show vmstat
 procs    memory      page                        disks      faults      cpu
 r b w    avm    fre  flt  re  pi   po   fr   sr s0 s1 m0   in   sy  cs us sy id
 0 0 0  64448 359056  115   0   0    0    0    0  0  0  0  827    0 710  2 10 88
```

procs　　：プロセス数
r　　：run キューにあるプロセス数
b　　：ブロックしているプロセス数
w　　：スワップしているプロセス数

memory　　：メモリー情報
　avm　　：アクティブな仮想ページ
　fre　　：フリーリストのサイズ
page　　：ページングの情報(5秒間平均を秒単位表示)
　flt　　：ページフォルト数
　re　　：要求されたページ数
　pi　　：ページインされたページ数
　po　　：ページアウトされたページ数
　fr　　：フリーされたページ数
　sr　　：スキャンされたページ数
disks　　：ディスクごとの1秒間のread/write回数
　s0　　：ディスクs0
　s1　　：ディスクs1
　m0　　：ディスクm0
faults　　：5秒間の平均トラップ・割り込みレート
　in　　：デバイス割り込み
　sy　　：システムコールの回数
　cs　　：CPUのコンテキストスイッチ回数
cpu　　：CPU利用時間
　us　　：ユーザー時間
　sy　　：システム時間
　id　　：CPUアイドル時間

関連コマンド

注意事項

サポート対応窓口が必要とするソフトウェア情報を表示するコマンドです。サポート対応窓口から取得をお願いする場合があります。

3.61.23 clear memory-error

スイッチLSIのメモリー状態を正常に戻し、メモリーエラー検出により監視対象外となったメモリーをメモリーエラーの監視対象に戻します。

メモリーエラー自動復旧機能が有効である場合は、同時にメモリーエラー自動復旧の回数、及び復旧不可能なメモリーエラーの発生回数のカウントをクリアします。

コマンドシンタックス

clear memory-error

コマンドモード

ENABLE

使用例

(1) スイッチLSIのメモリー状態を正常に戻し、メモリーをメモリーエラーの監視対象に戻します。

```
# clear memory-error
```

関連コマンド

show hardware

注意事項

3.62 PoE

PoE(Power over Ethernet)は、LAN ケーブルでデータ伝送に加えて電力供給する機能です。

IEEE 802.3af では、供給側(給電機器)の電力が 15.4 W、供給を受ける側(受電機器)の電力は 12.95 W として、電力の上限値が規定されており、本規格に準拠した受電機器に対してのみ給電対応します。

装置の電力供給量は 4 段階から用意されており、装置は受電機器に応じて、必要な電力を判断して効率的に供給することが可能です。

注意事項

PoE は Apresia3424GT-PoE、3424GT-HiPoE、5412GT-PoE でのみ有効です。

Apresia3424GT-PoE、3424GT-HiPoE は Class4 の受電機器には対応しておりません。Class4 の受電機器が接続された場合、給電動作、及び"show poe status"/"show poe power status"コマンドによる状態表示を行うことがありますが、これらの動作は保証されません。

Apresia3424GT-PoE は 12 ポート/ブロックの 2 ブロック(Block1 が 1～12 ポート、Block2 が 13～24 ポート)で構成され、ブロックごとに最大供給電力が 125 W に制限されています。

最大電力供給量を超える受電機器が接続された場合、最大ポート番号(Apresia3424GT-PoE は同一ブロック内の最大ポート番号)から給電が停止します(新たに接続した受電機器が最大電力供給量を超過した場合でも、必ずしも新たに接続した受電機器の電力供給が停止するわけではありません)。

3.62.1 poe threshold power(最大値設定)

最大電力供給量を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。ブロックを指定しない場合は、両ブロックの最大電力供給量を設定します(Apresia3424GT-PoE のみ)。

コマンドシンタックス

```
[ no ] poe threshold power <POWER> [ block <NUMBER> ]
    POWER          最大電力供給量設定
                   <10-125(W)>(Apresia3424GT-PoE/5412GT-PoE)
                   <10-370(W)>(Apresia3424GT-HiPoE)
    NUMBER         ブロック番号 <1-2>
```

デフォルト

125(W)：Apresia3424GT-PoE/5412GT-PoE
370(W)：Apresia3424GT-HiPoE

コマンドモード

CONFIG

(CONFIG モード以外でも入力可能)

使用例

(1) ブロック：2 の最大電力供給量を 100 W に設定します。
(2) デフォルト値に戻します(全ブロックをデフォルト値に戻します)。

```
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# poe threshold power 100 block 2
(config)# no poe threshold power
```

関連コマンド

show running-config, show poe status

注意事項

Apresia3424GT-HiPoE/5412GT-PoE は、ブロック指定できません。

3.62.2 poe threshold power(ポート設定)

各ポートの電力供給量を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

poe threshold power <POWER>
no poe threshold power

POWER	最大電力供給量設定 <3000-16200(mW)>(Apresia3424GT-PoE/3424GT-HiPoE) <3000-31600(mW)>(Apresia5412GT-PoE) • 任意の数値を設定できるが、動作時は 200 mW 単位で切り捨て

デフォルト

なし(dynamic)

コマンドモード

IF-PORT

使用例

(1) ポート：1 の最大電力供給量を 3000 mW に設定します。
(2) デフォルト値に戻します。

```
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# interface port 1
(config-if-port)# poe threshold power 3000
(config-if-port)# no poe threshold power
```

関連コマンド

show running-config, show poe status, show poe power status

注意事項

Apresia3424GT-PoE は、12 ポート/ブロックの 2 ブロック(Block1 が 1～12 ポート、Block2 が 13～24 ポート)で構成され、ブロックごとに最大供給電力が 125 W に制限されています。

ポートを shutdown しても電力供給可能です。

3.62.3 poe disable

各ポートにおいて PoE による給電を無効にします。有効にする場合は、no コマンドを使用してください。

コマンドシンタックス

[no] poe disable

デフォルト

no disable(＝有効)

コマンドモード

IF-PORT

使用例

(1) ポート：1 において PoE を無効にします。
(2) ポート：1 において PoE を有効にします。

```
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# interface port 1
(config-if-port)# poe disable
(config-if-port)# no poe disable
```

関連コマンド

show running-config, show poe status, show poe power status

注意事項

3.62.4 poe priority

各ポートの電力供給プライオリティを設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

電力供給プライオリティが同じ場合、若番ポートの方が優先的に電力供給されます。

供給電力の不足時には、プライオリティの低いポートから先に電力供給が停止されます。

コマンドシンタックス

poe priority critical | high | low
no poe priority

critical	最重要ポートとして常時電力供給する必要があるポートのみ設定 一番プライオリティが高い
high	二番目にプライオリティが高い
low	一番プライオリティが低い

デフォルト

low

コマンドモード

IF-PORT

使用例

(1) ポート：1において電力供給プライオリティをhighに設定します。
(2) ポート：1において電力供給プライオリティをデフォルト値に戻します。

```
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# interface port 1
(config-if-port)# poe priority high
(config-if-port)# no poe priority
```

関連コマンド

show running-config, show poe status

注意事項

最大電力供給中でも、プライオリティの高いポートに受電機器が接続された場合、電力供給中ポート内でプライオリティが一番低いポートの電力供給が停止し、プライオリティの高いポートに電力供給が開始されます。

同じプライオリティの設定が装置内(Apresia3424GT-HiPoE は同一ブロック内)に複数ポートあり、それ未満のプライオリティが設定されていない場合に最大給電量を超えると、同じプライオリティの最大ポート番号から給電停止します。

Apresia3424GT-HiPoE の電力供給プライオリティ設定はブロックごとに独立して機能します。

電力供給プライオリティが critical であっても、常時電力供給を保証するものではありません。

電力供給プライオリティ critical の最大設定数は装置あたり(Apresia3424GT-PoE は 1 ブロックあたり)8 ポートです。

3.62.5 poe power management class-based

給電総量の算出方法を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

block オプションを指定しない場合は、両ブロックに対して設定します。

Dynamic(デフォルト)　：受電機器側への供給量をリアルタイムで算出し、最大給電量を超える場合には優先順位に基づく給電許可・停止を行います。

Class Based　：各ポートの消費電力 Class に基づく最大給電量、もしくは "poe threshold power(ポート設定)"コマンドの設定値によって算出した最大給電量を超える場合には、優先順位に基づく給電許可・停止を行います。

1 ポートあたりの Class 別給電量は以下の通りです。

表 3-65 1 ポートあたりの Class 別給電量

Class	給電量
Class1	4.2 W
Class2	7.4 W
Class3	16.2 W
Class4	31.6 W(Apresia5412GT-PoE のみ)

コマンドシンタックス

poe power management class-based [block <NUMBER>]
no poe power management [block <NUMBER>]
　NUMBER　　ブロック番号 <1-2>

デフォルト

なし(dynamic)

コマンドモード

CONFIG

使用例

(1) ブロック：2 の給電モードを Class Based 設定にします。
(2) ブロック：2 の給電モードをデフォルト値に戻します。

```
(config)# poe power management class-based block 2
(config)# no poe power management block 2
```

関連コマンド

show running-config, show poe status

注意事項

Apresia3424GT-HiPoE/5412GT-PoE は、ブロック指定できません。

Class Based 設定の場合、Class3 の受電機器に対し、Apresia3424GT-PoE(1 ブロックあたり)/5412GT-PoE は最大 7 ポートまで、Apresia3424GT-HiPoE は最大 22 ポートまで同時給電可能となります。
受電機器を多数接続する場合には、"poe threshold power(ポート設定)"コマンドでポートあたりの最大給電量を調整してください。

3.62.6 poe other-fault retry-interval

PoE の出力電力超過状態、及び給電容量超過状態からの復旧リトライ間隔を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

```
poe other-fault retry-interval <RETRYTIME> [ block <NUMBER> ]
no poe other-fault retry-interval [ block <NUMBER> ]
    RETRYTIME          復旧リトライ間隔 <3-300(秒)>
    NUMBER             ブロック番号 <1-2>
```

デフォルト

9(秒)

コマンドモード

CONFIG

使用例

(1) ブロック：2 の復旧リトライ間隔を 100 秒に設定します。
(2) 復旧リトライ間隔をデフォルト値に戻します(ブロック：2 のみデフォルト値に戻します)。

```
(config)# poe other-fault retry-interval 100 block 2
(config)# no poe other-fault retry-interval block 2
```

関連コマンド

show running-config

注意事項

Apresia3424GT-HiPoE/5412GT-PoE は、ブロック指定できません。

3.62.7 show poe status

PoE による電力供給の設定状態を表示します。

コマンドシンタックス

show poe status

コマンドモード

VIEW, ENABLE

使用例

(1) PoE による電力供給の設定状態を表示します(Apresia3424GT-PoE)。

```
# show poe status
PoE System status:
                            Block1       Block2
   Threshold Power(W) :       125.0        125.0
   Available Power(W) :        61.6         30.8
   Power Management   :     dynamic      dynamic

PoE Port status:
Port  Blk  Priority  Threshold Type  Available  Detection Status
  1    1   critical  dynamic          16200mW  Delivering Power, Class 0.
  2    1   high      static           14800mW  Delivering Power, Class 1.
  3    1   low       static            3600mW  Delivering Power, Class 2.
  4    1   low       dynamic           7400mW  Delivering Power, Class 3.
  5    1   low       dynamic              0mW  Disabled.
  6    1   low       dynamic              0mW  Searching.
  7    1   low       dynamic              0mW  Other Fault, Over Load.
～中略～
 24    2   low       dynamic              0mW  Searching.
```

(2) PoE による電力供給の設定状態を表示します(Apresia5412GT-PoE)。

```
# show poe status
PoE System status:
     Threshold Power(W) :        125.0
     Available Power(W) :         32.0
     Power Management   :      dynamic

PoE Port status:
Port  Priority  Threshold Type  Available  Detection Status
  1   low       dynamic           4200mW  Delivering Power, Class 1.
  2   low       dynamic           7400mW  Delivering Power, Class 2.
  3   low       dynamic          16200mW  Delivering Power, Class 3.
  4   low       dynamic          31600mW  Delivering Power, Class 4.
  5   low       dynamic              0mW  Searching.
  6   low       dynamic              0mW  Searching.
  7   low       dynamic              0mW  Searching.
  8   low       dynamic          16200mW  Delivering Power, Class 0.
```

(3) PoE による電力供給の設定状態を表示します(Apresia3424GT-HiPoE)。

```
# show poe status
```

```
PoE System status:
     Threshold Power(W) :        370.0
     Available Power(W) :        368.1
     Power Management   :      dynamic

PoE Port status:
Port  Priority  Threshold Type  Available  Detection Status
  1   low       dynamic           16200mW  Delivering Power, Class 3.
  2   low       dynamic           16200mW  Delivering Power, Class 3.
  3   low       dynamic           16200mW  Delivering Power, Class 3.
  4   low       dynamic           16200mW  Delivering Power, Class 3.
  5   low       dynamic           16200mW  Delivering Power, Class 3.
～中略～
 24   low       dynamic           16200mW  Delivering Power, Class 0.
```

Threshold Power(W)　：最大電力供給量(W)
Available Power(W)　：実効電力供給総量(W)
Power Management　：給電モード
　dynamic　：Dynamic 設定
　class based　：Class Based 設定
Power Management　：給電総量設定
Block1　：電力供給 Block1(Apresia3424GT-PoE のみ表示)
Block2　：電力供給 Block2(Apresia3424GT-PoE のみ表示)
Port　：ポート番号
Blk　：ブロック番号(Apresia3424GT-PoE のみ表示)
Priority　：電力供給プライオリティ
Threshold Type　：最大電力供給量
Available　：電力供給割り当て量(mW)
Detection Status　：ポート検出状態、及び給電クラス
　Delivering Power, Class <0-4>　：給電クラス
　Searching　：受電機器検索中状態
　Disabled　：給電無効状態
　Other Fault, Over Load　：出力電力超過状態(ポートの出力電力が上限値を上回ったため給電停止)
　Requesting Power, Class <0-4>　：給電容量超過状態(装置全体の給電総量が最大給電量を超えたため、優先順位に基づいて給電停止)

関連コマンド

poe threshold power(最大値設定), poe disable, poe priority,
poe threshold power(ポート設定), poe power management class-based

注意事項

3.62.8 show poe power status

PoE の実効電力供給量を表示します。

コマンドシンタックス

show poe power status

コマンドモード

VIEW, ENABLE

使用例

(1) PoE の実効電力供給量を表示します(Apresia3424GT-PoE)。

```
# show poe power status
PoE Port Power status:
Port  Blk  Practical  Available  Detection Status
  1    1      6700mW     7000mW  Delivering Power, Class 2.
  2    1         0mW        0mW  Searching.
  3    1         0mW        0mW  Searching.
  4    1      3600mW     7000mW  Delivering Power, Class 2.
～中略～
 24    2         0mW        0mW  Searching.
```

(2) PoE の実効電力供給量を表示します(Apresia5412GT-PoE)。

```
# show poe power status
PoE Port Power status:
Port  Practical  Available  Detection Status
  1      1700mW     4200mW  Delivering Power, Class 1.
  2      4700mW     7400mW  Delivering Power, Class 2.
  3      9900mW    16200mW  Delivering Power, Class 3.
  4     14900mW    31600mW  Delivering Power, Class 4.
  5         0mW        0mW  Searching.
  6         0mW        0mW  Searching.
  7         0mW        0mW  Searching.
  8       800mW    16200mW  Delivering Power, Class 0.
```

(3) PoE の実効電力供給量を表示します(Apresia3424GT-HiPoE)。

```
# show poe power status
PoE Port Power status:
Port  Practical  Available  Detection Status
  1     15400mW    16200mW  Delivering Power, Class 3.
  2     15200mW    16200mW  Delivering Power, Class 3.
  3     15000mW    16200mW  Delivering Power, Class 3.
  4     15200mW    16200mW  Delivering Power, Class 3.
～中略～
 24     15100mW    16200mW  Delivering Power, Class 0.
```

Port　　：ポート番号
Blk　　：ブロック番号
Practical　　：実効電力供給量(mW)
Available　　：電力供給割り当て量(mW)
Detection Status　　：ポート検出状態、及び給電クラス

Delivering Power, Class <0-4>	：給電クラス
Searching	：受電機器検索中状態
Disabled	：給電無効状態
Other Fault, Over Load	：出力電力超過状態(ポートの出力電力が上限値を上回ったため給電停止)
Requesting Power, Class <0-4>	：給電容量超過状態(装置全体の給電総量が最大給電量を超えたため、優先順位に基づいて給電停止)

関連コマンド

poe disable, poe threshold power(ポート設定)

注意事項

3.63 sFlow

sFlow は、LAN スイッチやルーターなどを流れるトラフィックをパケットサンプリングに基づくトラフィック管理技術(RFC 3176)にてモニターする機能です。トラフィックに関する情報を送信する sFlow エージェント(本装置)と、トラフィック情報を受信して解析する sFlow コレクタで構成されます。

3.63.1 sflow enable

sFlow 統計機能を有効にします。無効にする場合は、no コマンドを使用してください。sFlow 統計機能の有効、無効を設定します。

コマンドシンタックス

[no] sflow enable

デフォルト

no enable(＝無効)

コマンドモード

CONFIG

使用例

(1) sFlow 統計情報を有効にします。

```
# configure terminal
(config)# sflow enable
```

関連コマンド

show sflow, show running-config

注意事項

sFlow を動作させるには、"sflow destination"、"sflow forwarding"、"sflow source" の設定が必須です。設定がない場合は動作しません。

3.63.2 sflow destination

sFlow コレクタの IP アドレスとポート番号を指定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

sflow destination <NUMBER> <IPADDR> [<PORT-NO>]
no sflow destination <NUMBER>

NUMBER	sFlow コレクタの番号 <1-4>
IPADDR	sFlow コレクタの IP アドレス
PORT-NO	sFlow コレクタのポート番号

デフォルト
ポート番号(6343)以外は、なし(＝設定なし)

コマンドモード
CONFIG

使用例
(1) sFlow コレクタの IP アドレスとポート番号を指定します。

```
# configure terminal
(config)# sflow destination 1 172.20.11.11
```

関連コマンド
show sflow, show running-config

注意事項

コレクタを 4 個まで指定可能ですが、1 個(最大 2 個まで)の使用を推奨します。

ポート番号を指定する場合、sFlow コレクタ側で設定したポート番号を指定してください。SNMP トラップ、TFTP などの UDP ポート番号を指定すると、それぞれのサーバーで誤動作することがあります。

3.63.3 sflow forwarding

sFlow による監視対象のポートを指定します。各ポートに指定してください。設定を削除する場合は、no コマンドを使用してください。同一ポートへ egress、ingress 両方を指定することが可能です。

コマンドシンタックス
[no] sflow forwarding egress | ingress

egress	監視対象パケットを egress に指定
ingress	監視対象パケットを ingress に指定

デフォルト
なし(＝設定なし)

コマンドモード
IF-PORT

使用例
(1) ポート：25 において、ingress パケットを監視対象に指定します。

```
# configure terminal
(config)# interface port 25
(config-if-port)# sflow forwarding ingress
```

関連コマンド

show sflow, show running-config

注意事項

ポートブロックが 2 つ以上存在する機種 Apresia3448 シリーズ(ポート 1～24、49～50 とポート 25～48､51～52)､Apresia4348 シリーズ(ポート 1～24 とポート 25～48)、Apresia13000-48X(ポート 1～24、50 とポート 25～49)では、ポートブロックを跨いで転送されたパケットは設定の有無にかかわらず、egress でのサンプリング対象とはなりません。

3.63.4 sflow mode

フローサンプルのモードを設定します。モード変更により、フローサンプルのパケットにおける Source ID の ifIndex 値、Input Interface/Output Interface の ifIndex 値が実際のものから変更されます。設定をデフォルトに戻す場合は、no コマンドを使用してください。

変更先である最若番ポートの番号は"sflow forwarding ingress"/"sflow forwarding egress"設定したポートの中で、一番小さな数字を持つポートの番号です。フローサンプルにおいて、不明なポートとなっている場合でも、モード変更により最若番ポートに置き換えることが可能です。

モードを変更しても、カウンターサンプルでのポート番号情報に影響はありません。

モードを変更した場合、CPU 使用率に影響を及ぼす可能性があります。

表 3-66 フローサンプル内の ifIndex

監視対象パケット	フローサンプル内 ifIndex	モード		
		0	1	2
Ingress	Source ID	入力ポート	入力ポート	Ingress 指定ポートの最若番ポート
	Input Interface	入力ポート	入力ポート	Ingress 指定ポートの最若番ポート
	Output Interface	常に 0	常に 0	常に 0
Egress	Source ID	常に 0	Egress 指定ポートの最若番ポート	Egress 指定ポートの最若番ポート
	Input Interface	入力ポート	入力ポート	入力ポート
	Output Interface	常に 0	Egress 指定ポートの最若番ポート ※1	Egress 指定ポートの最若番ポート ※1

※1 Egress 指定ポートの最若番ポートで受信したパケットの場合は 0

コマンドシンタックス

sflow mode 1 | 2

no sflow mode

デフォルト

0

コマンドモード
CONFIG

使用例
(1) フローサンプルのモードを 1 に設定します。

```
# configure terminal
(config)# sflow mode 1
```

関連コマンド
show sflow, show running-config

注意事項

3.63.5 sflow polling-interval

カウンターサンプルの報告間隔を指定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。カウンターサンプルの報告間隔設定後、初回カウンターサンプルが出力されるまでの時間は、0 秒～設定値までの乱数になります。

コマンドシンタックス
sflow polling-interval <SECS>
no sflow polling-interval

SECS	カウンターサンプル報告間隔 <0-2147483647(秒)> • 0 は報告なし

デフォルト
20(秒)

コマンドモード
CONFIG

使用例
(1) カウンターサンプルの報告間隔を 60 秒に指定します。

```
# configure terminal
(config)# sflow polling-interval 60
```

関連コマンド
show sflow, show running-config

注意事項

カウンターサンプル種別として GENERIC(一般的な統計、RFC 2233 参照)のみサポートとなります。

3.63.6 sflow sample

sFlow によるフローサンプル報告のためのパケットサンプリング間隔を設定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

sflow sample <PACKETS>
no sflow sample

PACKETS　　パケットサンプリング間隔 <256-16777216(パケット)>

- 指定された値は、2^8～2^{24} ごとに繰り上げ
  (例)
  257 を指定した場合、$257>2^8$ となるため、繰り上げられ $2^9=512$

デフォルト

512(パケット)

コマンドモード

CONFIG

使用例

(1) パケットサンプリング間隔を 2048 パケットに指定します。

```
# configure terminal
(config)# sflow sample 2048
```

関連コマンド

show sflow, show running-config

注意事項

フローサンプルでの基本データ形式は、Raw Packet Header 形式となります。なお拡張データ形式には対応していません。

sFlow 機能のみを動作させた状態(他機能はデフォルト設定)で CPU 使用率(3.61.16 "show system"コマンドの CPU Rate(1min、%))が 40 %以下となるよう、表 3-67 の推奨値を参考に各パラメーターを適正な値に設定してください。

表 3-67 sFlow 機能における推奨値

	設定項目	設定コマンド	推奨値
1	コレクタ数	sflow destination	1(最大 2)
2	監視対象ポート数 (同一ポート内で Ingress/Egress 併用可)	sflow forwarding	Apresia13000 シリーズ：14 ポート Apresia3400/4300/5400 シリーズ：4 ポート
3	カウンターサンプルの 報告間隔	sflow polling-interval	監視対象ポート数 × 1 秒より大きい値

表 3-68 稼動環境でのパケットサンプリング間隔の目安(Apresia13000 シリーズ)

パケット数合計(注)	トラフィック量の目安	パケットサンプリング間隔の目安
60k pps	100M bps の 40 %相当	256
120k pps	100M bps の 80 %相当	512
750k pps	1G bps の 50 %相当	4096
1.5M pps	1G bps の 100 %相当	8192
7.5M pps	10G bps の 50 %相当	65536
15M pps	10G bps の 100 %相当	131072

表 3-69 稼動環境でのパケットサンプリング間隔の目安(Apresia3400/4300/5400 シリーズ)

パケット数合計(注)	トラフィック量の目安	パケットサンプリング間隔の目安
48k pps	100M bps の 32 %相当	256
96k pps	100M bps の 64 %相当	512
750k pps	1G bps の 50 %相当	8192
1.5M pps	1G bps の 100 %相当	16384
7.5M pps	10G bps の 50 %相当	131072
15M pps	10G bps の 100 %相当	262144

(注)パケット数合計とは、3.7.15 "show interface counters"コマンドにおける、sFlow 監視対象とする全ポートの稼動状態の受信、または送信 pps の合計値です。
稼動環境でのパケットサンプリング間隔は以下条件下での目安値です。
実際のネットワークの構成、運用に合わせて調整のうえご使用ください。
-測定条件-
- polling-interval 20(秒)
- パケットサイズ 64(bytes)
- sFlow のみ動作(他機能はデフォルト設定)

3.63.7 sflow source

sFlow データグラムの送信元 IP アドレスを指定します。設定を削除する場合は、no コマンドを使用してください。

コマンドシンタックス

sflow source <IPADDR>
no sflow source

IPADDR　　sFlow データグラム上の送信元 IP アドレス

デフォルト

なし(＝設定なし)

コマンドモード

CONFIG

使用例

(1) sFlow データグラムの送信元 IP アドレスを 172.20.0.11 に指定します。

```
# configure terminal
(config)# sflow source 172.20.0.11
```

関連コマンド

show sflow, show running-config

注意事項

sFlow データグラムの送信元 IP アドレス設定がない場合、sFlow は動作しません。送信元 IP アドレスは必ず設定してください。

3.63.8 sflow max-header-size

sFlow サンプルとしてコピーされるヘッダーサイズの最大値を指定します。設定をデフォルト値に戻す場合は、no コマンドを使用してください。

コマンドシンタックス

sflow max-header-size <NUM>
no sflow max-header-size
NUM 最大ヘッダーサイズ <0-256(バイト)>

デフォルト

128(バイト)

コマンドモード

CONFIG

使用例

(1) sFlow サンプルとしてコピーされるヘッダーサイズの最大値を 64 バイトに指定します。

```
# configure terminal
(config)# sflow max-header-size 64
```

関連コマンド

show sflow, show running-config

注意事項

3.63.9 show sflow

sFlow 統計機能の設定状態を表示します。

コマンドシンタックス

show sflow

コマンドモード

VIEW, ENABLE

使用例

(1) sFlow 統計機能の設定状態を表示します。

```
# show sflow
 Status           : Enabled
 destination      : 1 172.20.11.11     6343
 source           : 172.20.11.254
 sampling         : 512
 polling interval : 20 sec
 max header size  : 128 bytes
 mode             : 0 (Default)

 --- port information ---
        * = sFlow Forwarding
        1      8 9     16 17    24 25    32 33    40 41    48 49
        +------+ +------+ +------+ +------+ +------+ +------+ +---
 Egress  ........ ....**.. ........ **...... ........ ........ ****
 Ingress ........ ........ ........ ........ ........ ........ ....
```

関連コマンド

注意事項

4. トラブルシューティング

詳細は、別冊の保守マニュアル、ハードウェアマニュアル、標準仕様書を参照してください。

4.1 表示 LED に関連する現象と対策

現象	対策
「POWER」LED が点灯しない	電源コードが本装置の AC インレットと電源コンセントに正常に接続されていることを確認してください。 電源モジュールが正常に接続されていることを確認してください。
	ボルトメータを使用し、電圧が規定値内であることを確認してください。
「FAULT」LED(または「ERR」LED)が点灯する	電源コードを抜き、周囲温度が本装置の仕様温度範囲内であることを確認したうえで、再度本装置を立ち上げてください。立ち上げなおしても FAULT LED(または ERR LED)が点灯したままの場合は、起動時のセルフテストにおいて何らかの異常を検出したと考えられますので、サポート対応窓口にお問い合わせください。
ケーブルを接続しても「LINK」、「ACT」LED が点灯しない	ケーブルに異常がないかどうか確認してください。
	接続相手の端末が正常に動作しているかどうか確認してください。
	モジュラープラグ(RJ-45)の接続に異常がないかどうか確認してください。
	接続相手が NIC、またはハブのカスケードポートである場合、ツイストペアケーブルがストレートケーブルであることを確認してください。 また、接続相手がハブの MDI-X ポートの場合、ツイストペアケーブルがクロスケーブルであることを確認してください。
	ツイストペアケーブルがエンハンストカテゴリ 5 であることを確認してください(ただし相手側端末が 10M bit/s 仕様の場合を除く)。
	SFP モジュールが正しく挿入されていることを確認してください。
	光ケーブルのコネクタ端面を再度清掃して接続してください。
	光ケーブルの接続に異常がないかどうか確認してください。
	3.7.15 "show interface status"コマンドで、ポートの設定が Disable になっていないか確認してください。

4.2 コンソール端末に関連する現象と対策

現象	対策
電源投入しても Login プロンプトが出力されない	コンソール端末の通信条件の設定が正しいことを確認してください。 設定値は通信速度 9600 bps、1 キャラクター8 ビット、ストップビット 1 ビット、パリティーなし、フロー制御なし、RS、ER は常時「ON」です。
	「CONSOLE」とコンソール端末との RS-232C 接続ケーブルが正しいことを確認してください。
	「CONSOLE」への接続が正常かどうか確認してください。
	「POWER」LED が点灯していること、及び「FAULT」LED(または「ERR」LED)が消灯していることを確認してください。
設定値が正常に入力されていない	正常な文字数であれば、内部のメモリーに異常が発生していると考え

	られます。サポート対応窓口にお問い合わせください。

4.3 SNMP マネージャーに関連する現象と対策

現象	対策
SNMP マネージャーからアクセスできない	IP アドレス、ネットマスク、デフォルトルーターの設定が正常であることを確認してください。また設定後にリセット、もしくは電源再投入がされていることも確認してください。
	SNMPマネージャーに正常なIPアドレスが登録されていることを確認してください。
	SNMPマネージャーと本装置のSNMPコミュニティー名称が同一であることを確認してください。
SNMP マネージャーがトラップを受信しない	トラップ送信先の IP アドレスが正常に設定されていることを確認してください。

4.4 TELNET に関連する現象と対策

現象	対策
端末からTELNETによりログインすることができない	本装置の IP アドレス、ネットマスク、デフォルトルーターの設定が正常であることを確認してください。また設定後にリセット、もしくは電源再投入がされていることも確認してください。
	接続しているポートの通信設定が ENABLE 状態になっていることを確認してください。ENABLE 状態ならば、ケーブルの接続を確認してください。
	TELNET しようとするアドレスが本装置のアドレスであることを確認してください。
	本装置が正常に起動し、動作していることを確認してください。
	装置に対して 1 分間に 40 回以上 TELNET 接続を試みた場合、約 10 分間ログイン出来なくなります。その場合、10 分以上待ってから再接続を行ってください。

4.5 スイッチングハブ機能に関連する現象と対策

現象	対策
端末から別の端末にデータの中継ができない	各端末が別々のポート VLAN グループに所属していないかどうか確認してください。
	各端末と本装置間のケーブルの接続が正常であることを確認してください。
	各端末の接続されているポートが ENABLE 状態であるかどうか確認してください。

4.6 VLAN に関連する現象と対策

現象	対策
VLAN ID を指定するとエラーメッセージが表示される	指定した VLAN ID が、すでに他の VLAN グループで使用されているとき、エラーメッセージが表示されます。VLAN ID の設定を修正してください。
リンクアグリゲーションポートを指定するとエラーメッセージが表	複数の VLAN グループにまたがるリンクアグリゲーションのメンバーポートがあります。メンバーポートの設定を修正してください。

示される	

4.7 リンクアグリゲーションに関連する現象と対策

現象	対策
リンクアグリゲーショングループを設定するとエラーメッセージ(リンクアグリゲーションとスピードのコンフリクト)が表示される	メンバーポートに指定したポートのすべての設定が同じになっているか確認してください。
	メンバーポートに指定したポートの通信モードが全二重モードになっているか確認してください。
	メンバーポートに指定したポートの advertise 設定が一種類の通信モード(全二重)のみになっているか確認してください。

4.8 内蔵冷却ファンに関連する現象と対策

現象	対策
電源投入しても冷却ファンが回転しない	FAULT LED(または ERR LED)が点灯していれば、ファンに関係する配線の異常、またはファンそのものの異常が考えられます。カバーをあけることなく、サポート対応窓口にお問い合わせください。

4.9 XENPAK に関連する現象と対策

現象	対策
XENPAK を認識している状態で通信しない	XENPAK を認識している状態で通信しない場合は、XENPAK が不完全装着になっている可能性があります。XENPAK を再度装着し直してください。現象が再発する場合は、XENPAK、または装置の異常が考えられますので、サポート対応窓口にお問い合わせください。

4.10 装置の表示、エラーログに関連する現象と対策

現象	対策
3.61.16 "show system"コマンドで Health Status の表示が「Abnormal」となっており、かつ 3.61.17 "show hardware"コマンドで SW-LSI MEMORY Status の表示が「Abnormal」となっている場合 ※ この状態になる場合、以下ログが出力します <bist:warning> System Status Code is changed(0xXXXX-0xYYYY).	スイッチ LSI のメモリーにおいてパリティエラーが発生している可能性があります。 [対象] • AEOS7.28.01～7.29.xx の OS • AEOS7.30.01 以降の OS で 3.61.9 "memory-error auto-recovery-mode enable"コマンドが無効の場合 [対策] 速やかに 3.61.23 "clear memory-error"コマンドを実行し、事象が復旧するかどうかご確認ください。 "clear memory-error"コマンドで事象が復旧した場合は、そのまま継続してご使用ください。 複数回"clear memory-error"コマンド入力後も事象が再発する場合には、装置再起動をお願いします。 再起動後も事象が再発する場合は、ハードウェア故障の疑いがあるため、装置交換のご検討をお願いします。
	スイッチ LSI のメモリーにおいてハードエラーが発生している可能性があります。 [対象]

	• AEOS7.30.01 以降の OS で 3.61.9 "memory-error auto-recovery-mode enable"コマンドが有効の場合 [対策] ハードウェア故障の疑いがあるため、装置交換のご検討をお願いします。

5. 準拠規格

No.	項目	準拠規格
1	LAN インターフェース	IEEE 802.3：10BASE-T IEEE 802.3u：100BASE-TX IEEE 802.3u：Auto-Negotiation IEEE 802.3z：1000BASE-X IEEE 802.3ab：1000BASE-T IEEE 802.3ae：10GBASE-R
2	コンソール インターフェース	ITU-T 勧告 V.24/V.28
3	ネットワーク管理 プロトコル	RFC 1157：SNMP(Simple Network Management Protocol) RFC 3416：Version 2 of the Protocol Operations for SNMP
4	ネットワーク管理対象	RFC 1213：Internet 標準 MIB RFC 1493：Bridge MIB RFC 3636：MAU MIB RFC 1724：RIP v2 MIB RFC 1850：OSPF v2 MIB RFC 2096：IP フォワーディングテーブル MIB RFC 1757：RMON MIB 4 グループ RFC 2021：RMON2 MIB のうち Probe config の一部 IEEE Std 802.3ad：IEEE8023-LAG-MIB RFC 3176：sFlow RFC 3621：powerEthernet MIB RFC 2787：VRRP MIB RFC 1907：MIB-II RFC 2233：interface MIB RFC 1700：ASSIGNED NUMBERS IEEE 802.3 Mgt IEEE 802.3 Std ベンダー独自 MIB
5	通信プロトコル	RFC 793：TCP RFC 768：UDP RFC 1350：THE TFTP PROTOCOL(REVISION 2)(client operation) RFC 791：IP RFC 792：ICMP RFC 826：ARP RFC 854：TELNET RFC 5905：NTP(client operation) RFC 2616：HTTP RFC 3164：SYSLOG
6	セキュリティ プロトコル	RFC 2865：RADIUS(client operation) IEEE 802.1X：認証 - SSH(サーバー) -

No.	項目	準拠規格
		RFC 4250：The Secure Shell (SSH) Protocol Assigned Numbers RFC 4251：The Secure Shell (SSH) Protocol Architecture RFC 4252：The Secure Shell (SSH) Authentication Protocol RFC 4253：The Secure Shell (SSH) Transport Layer Protocol RFC 4254：The Secure Shell (SSH) Connection Protocol RFC 4256：Generic Message Exchange Authentication for the Secure Shell Protocol (SSH) RFC 4716：The Secure Shell (SSH) Public Key File Format
7	その他	VCCI Class A 準拠 IEEE 802.1ad：Q-in-Q(stacked VLAN) IEEE 802.3ad：リンクアグリゲーション IEEE 802.1Q：tag group VLAN, QoS(IEEE802.1Q priority mapping/queuing) IEEE 802.1D：STP IEEE 802.1w：RSTP IEEE 802.1s：MSTP IEEE 802.1AB：LLDP IEEE 802.3x：フロー制御 IEEE 802.3af：PoE IEEE 802.3at draft3.3：PoE Plus RFC 1591：DNS(client operation) RFC 3768：VRRP(Virtual Router Redundancy Protocol) RFC 2131：DHCP(Dynamic Host Configuration Protocol) RFC 3176：sFlow - RIP - RFC 1058：RIP v1 RFC 2453：RIP v2 RFC 2082：RIP-2 MD5 Authentication - OSPF - RFC 2328：OSPF v2 RFC 3101：OSPF NSSA Option RFC 1765：OSPF Database Overflow RFC 2370：OSPF Opaque LSA Option RFC 3509：Alternative Implementation of OSPF Area Border Routers RFC 2154：OSPF with Digital Signatures(password MD-5) - BGP - RFC 1771：Border Gateway Protocol version 4 (BGP-4) RFC 1997：BGP Communities Attribute RFC 2796：BGP Route Reflection -An Alternative to Full Mesh IBGP RFC 2842：Capabilities Advertisement with BGP-4 RFC 2918：Route Refresh Capability for BGP-4 - Multicast - RFC 4601：Protocol Independent Multicast - Sparse Mode (PIM-SM)：Protocol Specification(Revised)

No.	項目	準拠規格
		RFC 1112：IGMP v1 RFC 2236：IGMP v2

6. 設定・表示コマンド/設定メニュー索引

aaa authentication 487
aaa authentication control 488
aaa radius client-ip 490
aaa radius deadtime 491
aaa radius host 489
aaa-local-db add user 549
aaa-local-db del user 550
access-defender 486
access-defender-deny 533
access-defender-logout ip 534
access-defender-logout mac 534
access-defender-logout user 535
action 202
action policing cbs 228
action policing cir 229
action policing group 227
action routing 230
advertise delete 44
archive downgrade-aeos6 620
archive download-loader 616
archive download-sw 614
archive upload-loader 618
archive upload-sw 617
arp static 116
assign 191
auto-download 595
auto-mdi-x 45
auto-negotiation 42
auto-shutdown port 41
auto-shutdown timer 41
backup clone 630
backup tftp, backup memory-card 628
block-cpu-control 212
boot-script configuration primary 606
boot-script configuration secondary ... 607
boot-script system primary 605
boot-script system secondary 605
bpdu-forward 153
cat memory-card 601
check config 588
clear arp 117
clear cpu-utilization history 622
clear dhcp leases 322
clear interface counters 59
clear ip igmp snooping cpu-counter 290
clear lacp counters 73
clear logging 307
clear loop-watch information 239
clear mac-address-table 112
clear memory-error 651
clear mmrp error-disabled 363
clear mmrp2 failure 414
clear mmrp-plus failure ring 403
clear packet-filter2 counter 224
clear spanning-tree detected protocols 152
clock set 256
condition 196
copy aaa-local-db file 548
copy configured-script 607
copy csr tftp 424
copy default-script configured-script . 608
copy file aaa-local-db 546
copy file https-file 425
copy file ssh-key 275
copy file WEB-PAGE 543
copy flash-config memory-card 599
copy flash-config tftp server file 591
copy https-file file 426
copy local-db tftp 475
copy log memory-card 600
copy memory-card flash-config 598
copy memory-card software 597
copy running-config file 591
copy running-config flash-config 588
copy ssh-key file 275
copy tftp local-db 474

copy tftp memory-card 598
copy tftp server file flash-config 590
copy WEB-PAGE file 545
counter-mode txdiscard only-buffer-overflow 50
cpu-utilization-notify threshold polling 622
debug 627
default disable 594
description 49
dhcp policy 318
dhcp policy enable 319
dhcp port max-lease-num 321
dhcp server address-check arp 321
dhcp server enable 319
dhcp server restart 320
dhcp-snooping enable 521
dhcp-snooping internal-dhcp-vlan 526
dhcp-snooping mode deny 523
dhcp-snooping mode mac-authentication . 523
dhcp-snooping mode timer 524
dhcp-snooping port 522
dhcp-snooping static-entry port 525
dns-server 325
domain-name 324
dot1x enable 513
dot1x mac-authentication-password 514
dot1x port 513
dot1x port ignore-eapol-start 515
dot1x port initialize 516
dot1x port max-req 516
dot1x port re-authenticate 518
dot1x port reauthentication 517
dot1x port timeout quiet-period 518
dot1x port timeout re-authperiod 519
dot1x port timeout supp-timeout 519
dot1x port timeout tx-period 520
egress shape 175
egress-filtering 172
egress-shape count-mode include-ifg-pa 176
erase boot-script 608
erase flash-config 593
erase local-db 476
erase memory-card 602
erase ssl-files 427
error-frame threshold polling-rate 636
exceeded-action 209
exec-timeout 259
factory-default 25
flooding control action 162
flooding control enable 163
flooding control interval 166
flooding control pps-hi 163
flooding control pps-low 164
flooding control shutdown pps-hi 165
flooding enable 158
flooding limit 159
flush-fdb rp-e port 113
flush-fdb rp-g port 113
forwarding 178
forwarding enable 178
hostname 28
ignore-tag 90
ingress-filter disable 170
instance priority 132
instance vlan 133
ip address 31
ip igmp querier enable 295
ip igmp querier query-interval 296
ip igmp querier query-max-response-time 297
ip igmp querier query-timeout 297
ip igmp querier robustness 298
ip igmp querier vlan 295
ip igmp snooping enable 280
ip igmp snooping group filter 285
ip igmp snooping immediate-leave 281
ip igmp snooping leave-message-proxy enable 287
ip igmp snooping max-member 281
ip igmp snooping member aging-time 282

ip igmp snooping member leave-time 282
ip igmp snooping mrouter aging-time ... 283
ip igmp snooping mrouter filter 284
ip igmp snooping mrouter vlan 284
ip igmp snooping report-message-proxy enable 286
ip igmp snooping send report-leave disable 286
ip igmp snooping unregistered-filter .. 288
ip igmp snooping unregistered-filter pf2-group 289
ip route 34
ipv6 mld snooping enable 308
ipv6 mld snooping group filter 313
ipv6 mld snooping immediate-leave 308
ipv6 mld snooping max-member 309
ipv6 mld snooping member aging-time ... 310
ipv6 mld snooping member leave-time ... 310
ipv6 mld snooping mrouter aging-time .. 311
ipv6 mld snooping mrouter filter 312
ipv6 mld snooping mrouter vlan 311
ipv6 mld snooping unregistered-filter . 313
ipv6 mld snooping unregistered-filter pf2-group 314
lacp port-priority 65
lacp system-priority 65
lacp timeout short 66
lease 328
license na key 432
line 259
link-aggregation 61
link-aggregation algorithm 62
link-aggregation lacp 64
link-speed-duplex 43
lldp enable 95
lldp err-disable-mode 100
lldp management-address 100
lldp mode 96
lldp msg-tx-hold 97
lldp msg-tx-interval 97
lldp reinit-delay 98
lldp tx-delay 99
logging access-defender web-access on . 543
logging buffered 300
logging console 301
logging error-frame-received port disable 305
logging flash 305
logging ip 303
logging monitor 302
logging on 304
logging source 304
logging sram 301
login-message 29
logout aging-time 527
logout clock 532
logout linkdown port disable 529
logout linkdown time 530
logout linkdown time port enable 529
logout ping dst-ip 531
logout ping ttl 531
logout timeout 528
logs 330
loop-watch auto-recovery timer 235
loop-watch enable 233
loop-watch group 236
loop-watch interval 234
loop-watch port 237
loop-watch threshold 234
loop-watch vlan add 238
mac-address-table aging-time 109
mac-address-table static 109
mac-authentication enable 509
mac-authentication ignore-dhcp 512
mac-authentication password 511
mac-authentication password-mac-address485, 510, 512
mac-authentication port 511
mdi 47
mdi-x 46

media 48
memory-error auto-recovery-mode enable 634
memory-error auto-recovery-mode notify
disable 635
memory-used-notify threshold polling .. 624
merit 331
mirroring 80
mmrp enable 339
mmrp group 338
mmrp ring aware port 344
mmrp ring bidirectional-check disable . 356
mmrp ring bidirectional-check
error-disabled-timer 356
mmrp ring bidirectional-check
revertive-timer 357
mmrp ring divided-master master-port .. 345
mmrp ring divided-master master-vid ... 345
mmrp ring divided-master
uplink-forcedown-method 346
mmrp ring divided-master
uplink-forcedown-time 347
mmrp ring divided-master uplink-port .. 348
mmrp ring divided-master uplink-up-wait 349
mmrp ring divided-shadow slave-port ... 349
mmrp ring divided-shadow slave-vid 350
mmrp ring divided-shadow
uplink-forcedown-method 351
mmrp ring divided-shadow
uplink-forcedown-time 352
mmrp ring divided-shadow uplink-port .. 353
mmrp ring divided-shadow uplink-up-wait 353
mmrp ring fdb-flush-timer 354
mmrp ring listening-timer 355
mmrp ring master master-port slave-port 341
mmrp ring master master-vid 342
mmrp ring master slave-vid 343
mmrp switch hello-interval 337
mmrp2 aware port 407
mmrp2 enable 406
mmrp2 enable (リング対象) 411
mmrp2 group 404
mmrp2 listening-timeout 409
mmrp2 name 409
mmrp2 revertive 410
mmrp2 vid 408
mmrp-plus enable 370
mmrp-plus group 368
mmrp-plus ring aware port 377
mmrp-plus ring divided-master master-port
..... 380
mmrp-plus ring divided-master
uplink-fdbflush-transmit 384
mmrp-plus ring divided-master
uplink-forcedown-method 380
mmrp-plus ring divided-master
uplink-forcedown-time 382
mmrp-plus ring divided-master uplink-port
..... 382
mmrp-plus ring divided-master
uplink-up-wait 383
mmrp-plus ring divided-shadow slave-port
..... 385
mmrp-plus ring divided-shadow
uplink-fdbflush-transmit 389
mmrp-plus ring divided-shadow
uplink-forcedown-method 386
mmrp-plus ring divided-shadow
uplink-forcedown-time 387
mmrp-plus ring divided-shadow uplink-port
..... 388
mmrp-plus ring divided-shadow
uplink-up-wait 388
mmrp-plus ring fdb-flush-timer 390
mmrp-plus ring hello-timeout 391
mmrp-plus ring listening-timer 391
mmrp-plus ring master master-port slave-port
..... 376
mmrp-plus ring name 371
mmrp-plus ring port-restart enable 392
mmrp-plus ring port-restart forcedown-time

..... 393
mmrp-plus ring port-restart linkup-wait 394
mmrp-plus ring revertive 379
mmrp-plus ring vid 372
mmrp-plus ring vlangroup 376
mmrp-plus switch hello-cycle 365
mmrp-plus switch hello-interval 367
mmrp-plus switch polling-rate 367
mmrp-plus vlangroup master-vid 374
mmrp-plus vlangroup slave-vid 373
mtu 107
multi 209
multicast-filtering 155
na arp-relay-port 458
na arp-relay-port vid 459
na auth-page redirect 467
na auth-page redirect proxy-port 469
na auth-page redirect url 471
na auth-page redirect vid 470
na clear 462
na custom-relay-port ip 464
na custom-relay-port port 463
na custom-relay-port tcp 465
na custom-relay-port udp 466
na dhcp-relay-port 460
na disc-mac-delete interval 461
na enable 433
na filter permit-ttl 449
na force-authorized port 450
na httpd english-language enable 444
na httpd ip 439
na httpd name radius 437
na httpd port 440
na httpd ssl enable 441
na httpd sslv2 enable 443
na httpd sslv3 enable 443
na httpd url 441
na local-authorized port 451
na logout aging 452
na logout clock 457
na logout ping dest-ip 454
na logout ping ttl 453
na logout polling count 456
na logout polling interval 455
na logout timeout 454
na mac-base passwd 458
na port designated mode 446
na port shared mode 445
na port shared-dynamic-vlan mode 448
na radius ip 434
na radius max-req 436
na radius port 434
na radius request-interval 436
na radius secret 435
na roaming enable 461
na success-url 473
na success-url timeout 474
name 133
network (DHCPサーバー) 322
next-server 331
no flooding 158
no flooding control 161
no loop-watch 232
no mmrp ring 340
no mmrp2 408
no mmrp-plus ring 371
ntp enable 253
ntp interval 254
ntp server 253
ntp-server 333
packet-filter2 190
packet-filter2 group 538
packet-filter2 max-rule 536
password 22
pause 47
pbr arp-interval 230
pbr icmp 230
ping 625
poe disable 655
poe other-fault retry-interval 658

poe power management class-based 657
poe priority 655
poe threshold power(ポート設定) 654
poe threshold power(最大値設定) 653
policing cbs 226
policing cir 226
port max-client 535
port-bridge enable 181
port-security delete mac 186
port-security delete port 186
port-security enable 183
power-down-notify enable 637
qos algorithm 247
qos burst-size 248
qos enable 243
qos mapping 249
qos max-bandwidth 245
qos min-bandwidth 244
qos weight 246
radius login enable 417
radius login ip 418
radius login local-authentication disable
..... 417
radius login max-request 420
radius login request-interval 420
radius login secret-key 419
RADIUS サーバー設定例 483
range 323
rebinding 329
reboot 612
reboot timer 612
redundant group-number 75
redundant mac-address-table update 77
redundant port-priority 76
rename memory-card 602
renewing 328
restore 631
revision 134
roaming port enable 539
root-path 332
router 327
sflow destination 663
sflow enable 663
sflow forwarding 664
sflow max-header-size 669
sflow mode 665
sflow polling-interval 666
sflow sample 667
sflow source 668
show access-defender aaa-local-db 550
show access-defender client 551
show access-defender deny 553
show access-defender dhcp-snooping
configuration 557
show access-defender dhcp-snooping
mode-status 558
show access-defender dhcp-snooping status
..... 559
show access-defender dot1x 553
show access-defender dot1x statistics port
..... 556
show access-defender packet-filter2
rule-statistics 560
show access-defender port-configuration 562
show arp 117
show auto-download 596
show auto-shutdown 51
show boot-script configured 609
show boot-script flash 610
show boot-script memory-card 610
show bpdu-forward 153
show clock 257
show debugging 638
show dhcp current 335
show dhcp policy 336
show egress-filtering 173
show egress-shape 177
show flash-config 586
show flooding 160
show flooding control 166

show flooding control port 168
show flush-fdb rp-e 114
show flush-fdb rp-g 115
show forwarding 179
show hardware 643
show history 646
show ignore-tag 93
show ingress-filter 170
show interface counters 56
show interface status 51
show ip address 32
show ip igmp querier configuration 298
show ip igmp snooping configuration ... 291
show ip igmp snooping cpu-counter 290
show ip igmp snooping status 292
show ip route 35
show ip route cache 37
show ip route database 36
show ip route summary 38
show ipv6 mld snooping configuration .. 315
show ipv6 mld snooping status 316
show lacp 67
show lacp port 71
show lacp sys-id 70
show lacp-counter 70
show license 433
show link-aggregation 67
show lldp configuration 104
show lldp port 101
show lldp port detail 103
show lldp statistics 105
show logging 306
show login-message 30
show loop-watch configuration 240
show loop-watch status 241
show mac-address-table 110
show mac-address-table aging-time 111
show memory-card files 603
show mirroring 82
show mmrp configuration 360
show mmrp configuration ring 361
show mmrp status 358
show mmrp status port 359
show mmrp2 412
show mmrp2 detail 412
show mmrp-plus configuration 395
show mmrp-plus configuration ring 396
show mmrp-plus status 399
show mmrp-plus status port 401
show mmrp-plus vlangroup 399
show mtu 107
show multicast-filtering 156
show na aging 477
show na client 481
show na configuration 477
show na local-db 481
show netstat 648
show ntp 255
show packet-filter2 215
show packet-filter2 brief 219
show packet-filter2 counter 221
show packet-filter2 policing 230
show packet-filter2 reserved-group 223
show packet-filter2 tcp/udp-range 222
show poe power status 660
show poe status 658
show port-bridge 181
show port-security 187
show ps 649
show qos 250
show radius login configuration 421
show reboot timer 613
show redundant 78
show redundant portbase 78
show running-config 585
show sflow 669
show snmp-server 582
show spanning-tree configuration 138
show spanning-tree mst 143
show spanning-tree mst config 144

show spanning-tree mst detail 145
show spanning-tree mst instance 149
show spanning-tree mst port 150
show spanning-tree port 138
show spanning-tree rst 141
show spanning-tree statistics 140
show spanning-tree switch 139
show sshd key rsa 278
show sshd key rsa1 279
show sshd list 277
show sshd server 276
show ssl csr 428
show ssl https-certificate 429
show ssl https-private-key 430
show system 641
show tag-type 93
show tech-support 647
show tech-support access-defender 563
show tech-support igmp 293
show tech-support link-aggregation 73
show tech-support mmrp 362
show tech-support mmrp-plus 402
show tech-support na 482
show tech-support packet-filter2 224
show tech-support spanning-tree 151
show telnet list 267
show telnet server 266
show timezone 258
show username 23
show users 24
show version 639
show version flash 640
show vlan 92
show vmstat 650
shutdown 40
snap-nonzero-oui 91
snmp-server access-disable 570
snmp-server community 568
snmp-server contact 575
snmp-server counter
ifinerrors-exclude-oversize 581
snmp-server disable 568
snmp-server host 570
snmp-server location 576
snmp-server name 576
snmp-server rmon-history 580
snmp-server trap source 572
snmp-server traps 573
snmp-server traps boot-time-delay 578
snmp-server traps transmit-delay 579
snmp-server traps transmit-gap disable 580
snmp-server trap-source 577
spanning-tree cost 129
spanning-tree disable 122
spanning-tree enable 121
spanning-tree force-version 130
spanning-tree forward-time 123
spanning-tree hello-time 124
spanning-tree interconnection-mode 137
spanning-tree link-type 124
spanning-tree max-age 125
spanning-tree mode 119
spanning-tree mst configuration 130
spanning-tree mst instance 135
spanning-tree mst instance cost 136
spanning-tree mst instance port-priority
..... 135
spanning-tree mst max-hops 131
spanning-tree portfast 127
spanning-tree port-priority 128
spanning-tree priority 126
sshd disconnect 274
sshd ip 273
sshd keepalive disable 270
sshd keygen rsa 268
sshd keygen rsa1 269
sshd mode deny 272
sshd port 271
sshd server 269
sshd server-keybits 271

sshd subnet 273
ssl gencsr rsakey 423
state 190
static-entry 334
switchport access 85
switchport mode 85
switchport port-security aging-time ... 184
switchport port-security enable 183
switchport port-security maximum 185
switchport trunk 87
tag-type 89
telnet 626
telnet disconnect 265
telnet ip 264
telnet mode deny 263
telnet server 263
telnet subnet 265
terminal length 261
terminal monitor 261
tftp source 633
timezone 256
traceroute 626
username 21
vlan add protocol 88
vlan database 83
vlan mode dynamic port-base 540
vlan mode static 542
vlan name 83
vlan state 84
web-authentication enable 492
web-authentication http-port 497
web-authentication http-session-timeout 499
web-authentication https-port 498
web-authentication ip 500
web-authentication
mac-authentication-password 506
web-authentication port 494
web-authentication redirect http 501
web-authentication redirect https 502
web-authentication redirect proxy-port 504
web-authentication redirect url 500
web-authentication snooping proxy-port 505
web-authentication sslv2 enable 508
web-authentication sslv3 enable 508
web-authentication ttl 507
wide-mode 213
wins-server 326
write memory 588
ポリシーベースルーティング 230
ポリシング 225
外部サーバー 564
認証ページ 563
認証ページのカスタマイズ 563
認証応答属性 (AccessDefender) 566
認証応答属性 (RADIUS ログイン認証) 422
認証要求属性 (AccessDefender) 566
認証要求属性 (RADIUS ログイン認証) 422

AEOS Ver. 7.44 コマンドリファレンス L2編

Copyright(c) 2020 APRESIA Systems, Ltd.
2020年9月 初版

APRESIA Systems株式会社
東京都中央区築地二丁目3番4号
築地第一長岡ビル
https://www.apresiasystems.co.jp/