

日立金属スイッチングハブ

ApresiaLightFM シリーズ

Ver. 1.08

CLI マニュアル

制定・改訂履歴表

No.	年 月 日	内 容
-	2014年 1月 30日	<ul style="list-style-type: none"> ・ Ver1.07 CLI マニュアル(TD61-5099A)より新規作成 ・ 表紙の社名変更 ・ 表 1-1 デフォルト設定一覧 MAC Auth Format、MAC Auth Password Type を追加 ・ 3.4.1 download download firmware_fromTFTP と download cfg_fromTFTP の各コマンドを統合 ・ 3.4.2 config firmware_id config firmware から config firmware_id にコマンド名を変更 ・ 3.4.11 show self-test result コマンド追加 ・ 3.4.12 show sfp diag コマンド追加 ・ 3.4.13 show sfp info コマンド追加 ・ 3.9.5 show utilization 使用例(ポート使用統計の単位説明)の追加 ・ 3.17.4 config link_aggregation algorithm 注意事項(LAG の分散動作)の追加 ・ 3.21.1 enable stp 注意事項(認証機能とのポート併用制限)の追加 ・ 3.23.1 config mirror port 注意事項(タグなし送信フレームのミラーリング)の追加 注意事項(送信先ポートの VLAN 削除)の追加 ・ 3.24.1 config port_security ports 注意事項(認証機能とのポート併用制限)の追加 ・ 3.28.3 config vlan 注意事項(複数の VLAN アサイン)の追加 ・ 3.28.6 config vlan vlanid 注意事項(複数の VLAN アサイン)の追加 ・ 3.28.7 enable pvid auto_assign デフォルト値を追加 ・ 3.32.3 config access_profile 注意事項(ACL ルール)の追加 ・ 3.36.6 config mac_based_access_control ports aging_time と hold_time のデフォルト値を追加 ・ 3.36.14 config mac_based_access_control max_users 注意事項 (MAC 認証最大数を越えた場合の表示) の追加 ・ 3.36.18 config mac_based_access_control mac_format コマンド追加 ・ 3.36.19 config mac_based_access_control password_type コマンド追加

No.	年 月 日	内 容
A	2014年2月11日	・ 3.43 Link Error Recovery コマンド追加
B	2016年11月30日	・ 3.22 パケットストーム制御コマンドの説明を修正

はじめに

本書には、スイッチングハブのコマンド説明および操作方法を記述しています。それ以外のハードウェアに関する説明および操作方法については、各適用機種ハードウェアマニュアルを参照ください。

本書適用の機種一覧表

シリーズ名	品名	型式
ApresiaLightFMシリーズ	ApresiaLightFM108GT-SS	APLFM108GTSS
	ApresiaLightFM116GT-SS	APLFM116GTSS
	ApresiaLightFM124GT-SS	APLFM124GTSS
	ApresiaLightFM108GT-POE	APLFM108GTPOE
	ApresiaLightFM116GT-POE	APLFM116GTPOE



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、注目させる為に用います。

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全てのソフトウェア(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。

- (1) 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。
- (2) 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、日立金属(株)の登録商標です。

Ethernet は、米国 Xerox Corp.の登録商標です。

その他ブランド名は、各所有者の商標もしくは登録商標です。

目次

1. パラメーター設定手順	17
1.1 出荷時の設定値一覧	17
1.2 システム最大値一覧	21
1.3 パラメーター設定手順	23
1.4 パラメーター設定端末の準備	25
1.5 パラメーター設定端末の接続	26
2. コマンドラインインターフェースの基本操作	28
2.1 コマンドの表記規則	28
2.2 概要	29
2.2.1 ログイン	29
2.2.2 初期化アカウント ap_recovery	29
2.2.3 コマンド入力	30
3. コマンドの詳細	33
3.1 ツイストケーブル診断コマンド	34
3.1.1 cable_diag ports	34
3.2 基本的な IP コマンド	35
3.2.1 config ipif	35
3.2.2 show ipif	36
3.3 基本的なスイッチコマンド	37
3.3.1 create account	37
3.3.2 config account	37
3.3.3 show account	38
3.3.4 delete account	39
3.3.5 show session	39
3.3.6 show switch	40
3.3.7 show serial_port	41
3.3.8 config serial_port	41
3.3.9 enable clipaging	42
3.3.10 disable clipaging	42
3.3.11 enable telnet	43
3.3.12 disable telnet	43
3.3.13 telnet	44
3.3.14 enable web	44
3.3.15 disable web	45
3.3.16 save	45
3.3.17 reboot	46
3.3.18 reset	47
3.3.19 login	48
3.3.20 logout	48

3.3.21	config terminal_line	49
3.3.22	show terminal_line	49
3.3.23	enable jumbo_frame	49
3.3.24	disable jumbo_frame	50
3.3.25	show jumbo_frame	50
3.3.26	show tech_support	51
3.4	スイッチユーティリティコマンド	53
3.4.1	download	53
3.4.2	config firmware image_id	55
3.4.3	show firmware information	55
3.4.4	show config	57
3.4.5	upload	59
3.4.6	ping	60
3.4.7	ping6	61
3.4.8	traceroute	62
3.4.9	config terminal line	62
3.4.10	show terminal line	63
3.4.11	show self-test result	63
3.4.12	show sfp diag	64
3.4.13	show sfp info	64
3.5	コマンド履歴コマンド	66
3.5.1	?	66
3.5.2	dir	67
3.5.3	config command_history	68
3.5.4	show command_history	68
3.6	LLDP コマンド	69
3.6.1	enable lldp	69
3.6.2	disable lldp	69
3.6.3	config lldp message_tx_interval	70
3.6.4	config lldp message_tx_hold_multiplier	70
3.6.5	config lldp tx_delay	71
3.6.6	config lldp reinit_delay	71
3.6.7	config lldp notification_interval	72
3.6.8	config lldp ports notification	72
3.6.9	config lldp ports admin_status	73
3.6.10	config lldp ports mgt_addr	74
3.6.11	config lldp ports basic_tlvs	74
3.6.12	config lldp ports dot1_tlv_pvid	75
3.6.13	config lldp ports dot1_tlv_protocol_vid	76
3.6.14	config lldp ports dot1_tlv_vlan_name	77

3.6.15	config lldp ports dot1_tlv_protocol_identity	77
3.6.16	config lldp ports dot3_tlvs	78
3.6.17	config lldp forward_message	79
3.6.18	show lldp	80
3.6.19	show lldp mgt_addr	80
3.6.20	show lldp ports	81
3.6.21	show lldp local_ports	82
3.6.22	show lldp remote_ports	85
3.6.23	show lldp statistics	87
3.6.24	show lldp statistics ports	87
3.7	バナーとプロンプトの編集コマンド	89
3.7.1	config command_prompt	89
3.7.2	config greeting_message	89
3.7.3	show greeting_message	90
3.8	ネットワーク管理 (SNMP) コマンド	92
3.8.1	create snmp user	92
3.8.2	delete snmp user	94
3.8.3	show snmp user	94
3.8.4	create snmp view	95
3.8.5	delete snmp view	95
3.8.6	show snmp view	96
3.8.7	create snmp community	97
3.8.8	delete snmp community	98
3.8.9	show snmp community	98
3.8.10	config snmp engineID	99
3.8.11	show snmp engineID	99
3.8.12	create snmp group	100
3.8.13	delete snmp group	101
3.8.14	show snmp groups	101
3.8.15	create snmp host	103
3.8.16	delete snmp host	104
3.8.17	show snmp host	104
3.8.18	create trusted_host	105
3.8.19	delete trusted_host	106
3.8.20	show trusted_host	107
3.8.21	enable snmp	108
3.8.22	disable snmp	109
3.8.23	config snmp linkchange_traps ports	110
3.8.24	show snmp traps	110
3.8.25	config snmp system_contact	112

3.8.26 config snmp system_location	112
3.8.27 config snmp system_name	113
3.8.28 enable rmon	113
3.8.29 disable rmon	114
3.9 ネットワーク監視コマンド	115
3.9.1 show packet ports	115
3.9.2 show error ports	115
3.9.3 config utilization notify	116
3.9.4 clear utilization	117
3.9.5 show utilization	117
3.9.6 show utilization notify	120
3.9.7 clear counters	120
3.9.8 clear log	121
3.9.9 show log	121
3.9.10 enable syslog	122
3.9.11 disable syslog	122
3.9.12 show syslog	123
3.9.13 create syslog host	123
3.9.14 config syslog	125
3.9.15 delete syslog host	126
3.9.16 show syslog host	127
3.9.17 config log_save_timing	128
3.9.18 show log_save_timing	128
3.9.19 delete ipif System	129
3.9.20 enable ipif_ipv6_link_local_auto	129
3.9.21 disable ipif_ipv6_link_local_auto	130
3.9.22 show ipif_ipv6_link_local_auto	130
3.10 SMTP コマンド	131
3.10.1 enable smtp	132
3.10.2 disable smtp	132
3.10.3 config smtp	133
3.10.4 show smtp	134
3.10.5 smtp send_testmsg	134
3.11 スイッチポートコマンド	136
3.11.1 config ports	136
3.11.2 show ports	137
3.12 Time と SNTP コマンド	139
3.12.1 config sntp	139
3.12.2 show sntp	139
3.12.3 enable sntp	140

3.12.4	disable sntp	140
3.12.5	config time	141
3.12.6	config time_zone	141
3.12.7	config dst	142
3.12.8	show time	143
3.13	Asymmetric VLAN コマンド	145
3.13.1	enable asymmetric_vlan	145
3.13.2	disable asymmetric_vlan	145
3.13.3	show asymmetric_vlan	145
3.14	BPDU ガードコマンド	146
3.14.1	enable bpdu_guard	146
3.14.2	disable bpdu_guard	146
3.14.3	config bpdu_guard ports	147
3.14.4	config bpdu_guard recovery_time	148
3.14.5	config bpdu_guard log	148
3.14.6	show bpdu_guard	149
3.15	フォワーディングデータベースコマンド	151
3.15.1	create fdb	151
3.15.2	create multicast_fdb	151
3.15.3	config multicast_fdb	152
3.15.4	config fdb aging_time	152
3.15.5	delete fdb	153
3.15.6	clear fdb	154
3.15.7	show multicast_fdb	154
3.15.8	show fdb	155
3.15.9	config multicast port_filtering_mode	156
3.15.10	show multicast port_filtering_mode	156
3.16	IGMP スヌープコマンド	157
3.16.1	config igmp_snooping	157
3.16.2	config igmp_snooping querier	158
3.16.3	config router_ports	159
3.16.4	config router_ports_forbidden	160
3.16.5	enable igmp_snooping	160
3.16.6	disable igmp_snooping	161
3.16.7	show igmp_snooping	161
3.16.8	show router_ports	162
3.16.9	show igmp_snooping group	163
3.16.10	show igmp_snooping host	164
3.17	リンクアグリゲーションコマンド	165
3.17.1	create link_aggregation	165

3.17.2 delete link_aggregation group_id	166
3.17.3 config link_aggregation group_id	166
3.17.4 config link_aggregation algorithm	167
3.17.5 show link_aggregation	168
3.17.6 config lacp_ports	169
3.17.7 show lacp_ports	170
3.18 ループ防止コマンド	171
3.18.1 config loopdetect	171
3.18.2 config loopdetect ports	172
3.18.3 enable loopdetect	173
3.18.4 disable loopdetect	173
3.18.5 show loopdetect	174
3.18.6 show loopdetect ports	175
3.19 MAC ベース VLAN コマンド	176
3.19.1 create mac_based_vlan	176
3.19.2 delete mac_based_vlan	176
3.19.3 show mac_based_vlan	177
3.20 MLD スヌープコマンド	178
3.20.1 config mld_snooping	178
3.20.2 config mld_snooping querier	178
3.20.3 config mld_snooping mrouter_ports	179
3.20.4 config mld_snooping mrouter_ports_forbidden	180
3.20.5 enable mld_snooping	180
3.20.6 disable mld_snooping	181
3.20.7 show mld_snooping	181
3.20.8 show mld_snooping group	182
3.20.9 show mld_snooping mrouter_ports	183
3.21 マルチプルスパニングツリープロトコル (MSTP) コマンド	185
3.21.1 enable stp	185
3.21.2 disable stp	186
3.21.3 config stp version	186
3.21.4 config stp	187
3.21.5 config stp ports	188
3.21.6 create stp instance_id	190
3.21.7 config stp instance_id	190
3.21.8 delete stp instance_id	191
3.21.9 config stp priority	192
3.21.10 config stp mst_config_id	193
3.21.11 config stp mst_ports	194
3.21.12 show stp	195

3.21.13	show stp ports	197
3.21.14	show stp instance	197
3.21.15	show stp mst_config_id	198
3.22	パケットストーム制御コマンド	200
3.22.1	config traffic control	200
3.22.2	show traffic control	202
3.23	ポートミラーリングコマンド	203
3.23.1	config mirror port	203
3.23.2	enable mirror	204
3.23.3	disable mirror	204
3.23.4	show mirror	205
3.24	ポートセキュリティコマンド	206
3.24.1	config port_security ports	206
3.24.2	delete port_security_entry vlan_name	207
3.24.3	clear port_security_entry port	207
3.24.4	show port_security	208
3.25	プロトコル VLAN コマンド	209
3.25.1	create dot1v_protocol_group	209
3.25.2	config dot1v_protocol_group	210
3.25.3	delete dot1v_protocol_group	210
3.25.4	show dot1v_protocol_group	211
3.25.5	config port dot1v ports	212
3.25.6	show port dot1v	212
3.26	Q-in-Q コマンド	214
3.26.1	enable qinq	214
3.26.2	disable qinq	214
3.26.3	show qinq	215
3.26.4	show qinq ports	215
3.26.5	config qinq ports	216
3.26.6	create vlan_translation	216
3.26.7	delete vlan_translation cvid	217
3.26.8	show vlan_translation cvid	217
3.27	トラフィックセグメンテーションコマンド	219
3.27.1	config traffic_segmentation	219
3.27.2	show traffic_segmentation	219
3.28	VLAN コマンド	221
3.28.1	create vlan	221
3.28.2	delete vlan	221
3.28.3	config vlan	222
3.28.4	create vlan vlanid	223

3.28.5 delete vlan vlanid	223
3.28.6 config vlan vlanid	224
3.28.7 enable pvid auto_assign	225
3.28.8 disable pvid auto_assign	225
3.28.9 show pvid auto_assign	225
3.28.10 config gvrp	226
3.28.11 enable gvrp	227
3.28.12 disable gvrp	227
3.28.13 show vlan	228
3.28.14 show gvrp	229
3.29 ARP コマンド	230
3.29.1 create arprentary	230
3.29.2 config arprentary	230
3.29.3 delete arprentary	231
3.29.4 config arp_aging time	231
3.29.5 show arprentary	232
3.29.6 clear arptable	232
3.30 ルーティングテーブルコマンド	233
3.30.1 create iproute	233
3.30.2 delete iproute	233
3.30.3 show iproute	234
3.30.4 create ipv6 neighbor_cache ipif	234
3.30.5 delete ipv6 neighbor_cache ipif	235
3.30.6 show ipv6 neighbor_cache ipif	235
3.30.7 create ipv6route	236
3.30.8 delete ipv6route	237
3.30.9 show ipv6 nd	237
3.30.10 show ipv6route	238
3.30.11 config ipv6 nd ns ipif	238
3.31 QoS コマンド	239
3.31.1 config bandwidth_control	239
3.31.2 show bandwidth_control	240
3.31.3 config scheduling	241
3.31.4 show scheduling	241
3.31.5 config scheduling_mechanism	242
3.31.6 show scheduling_mechanism	243
3.31.7 config 802.1p user_priority	244
3.31.8 show 802.1p user_priority	245
3.31.9 config 802.1p default_priority	245
3.31.10 show 802.1p default_priority	246

3.31.11 config cos mapping	247
3.31.12 show cos mapping	247
3.31.13 config cos tos value	248
3.31.14 show cos tos	249
3.31.15 config dscp_mapping	249
3.31.16 show dscp_mapping	250
3.32 アクセス制御リスト (ACL)コマンド	251
3.32.1 create access_profile	252
3.32.2 delete access_profile	255
3.32.3 config access_profile	256
3.32.4 show access_profile	261
3.33 フローメーターコマンド	262
3.33.1 config flow_meter profile_id	262
3.33.2 show flow_meter	263
3.34 802.1X コマンド	264
3.34.1 enable 802.1x	264
3.34.2 disable 802.1x	264
3.34.3 show 802.1x	265
3.34.4 config 802.1x capability ports	268
3.34.5 config 802.1x auth_parameter ports	269
3.34.6 config 802.1x auth_protocol	270
3.34.7 config 802.1x init	270
3.34.8 config 802.1x reauth	271
3.34.9 config radius add	272
3.34.10 config radius delete	272
3.34.11 config radius	273
3.34.12 config radius parameter	274
3.34.13 show radius	274
3.34.14 show acct_client	275
3.34.15 show auth_client	275
3.34.16 show auth_diagnostics	276
3.34.17 show auth_session_statistics	277
3.34.18 show auth_statistics	278
3.34.19 create 802.1x user	279
3.34.20 show 802.1x user	280
3.34.21 delete 802.1x user	280
3.35 アクセス認証制御コマンド	281
3.35.1 enable authen_policy	282
3.35.2 disable authen_policy	283
3.35.3 show authen_policy	283

3.35.4	create authen_login method_list_name	284
3.35.5	config authen_login	284
3.35.6	delete authen_login method_list_name	286
3.35.7	show authen_login	287
3.35.8	create authen_enable method_list_name	288
3.35.9	config authen_enable	289
3.35.10	delete authen_enable method_list_name	291
3.35.11	show authen_enable	292
3.35.12	config authen application	294
3.35.13	show authen application	295
3.35.14	create authen server_host	296
3.35.15	config authen server_host	297
3.35.16	delete authen server_host	298
3.35.17	show authen server_host	298
3.35.18	create authen server_group	299
3.35.19	config authen server_group	300
3.35.20	delete authen server_group	301
3.35.21	show authen server_group	301
3.35.22	config authen parameter response_timeout	302
3.35.23	config authen parameter attempt	303
3.35.24	show authen parameter	303
3.35.25	enable admin	304
3.35.26	config admin local_enable	305
3.36	MAC ベースアクセス制御コマンド	306
3.36.1	enable mac_based_access_control	306
3.36.2	disable mac_based_access_control	306
3.36.3	config mac_based_access_control password	306
3.36.4	config mac_based_access_control method	307
3.36.5	config mac_based_access_control auth_failover	307
3.36.6	config mac_based_access_control ports	308
3.36.7	clear mac_based_access_control auth_mac	309
3.36.8	create mac_based_access_control_local mac	309
3.36.9	config mac_based_access_control_local mac	310
3.36.10	delete mac_based_access_control_local	310
3.36.11	show mac_based_access_control	311
3.36.12	show mac_based_access_control_local	312
3.36.13	show mac_based_access_control auth_mac	313
3.36.14	config mac_based_access_control max_users	313
3.36.15	enable authorization network	314
3.36.16	disable authorization network	315

3.36.17	show authorization	315
3.36.18	config mac_based_access_control mac_format	315
3.36.19	config mac_based_access_control password_type	316
3.37	マルチプル認証コマンド	317
3.37.1	config authentication auth_mode	317
3.37.2	show authentication ports	317
3.38	SSH コマンド	318
3.38.1	enable ssh	318
3.38.2	disable ssh	318
3.38.3	config ssh authmode	319
3.38.4	show ssh authmode	319
3.38.5	config ssh server	320
3.38.6	show ssh server	321
3.38.7	config ssh user	321
3.38.8	show ssh user authmode	322
3.38.9	config ssh algorithm	323
3.38.10	show ssh algorithm	324
3.39	SSL コマンド	325
3.39.1	enable ssl	326
3.39.2	disable ssl	327
3.39.3	config ssl cachetimeout timeout	328
3.39.4	show ssl cachetimeout	328
3.39.5	show ssl	329
3.39.6	show ssl certificate	329
3.39.7	download ssl certificate	330
3.40	WEB 認証コマンド	331
3.40.1	enable web_authentication	331
3.40.2	disable web_authentication	331
3.40.3	create web_authentication user	332
3.40.4	config web_authentication user	332
3.40.5	config web_authentication auth_failover	333
3.40.6	config web_authentication authorization network	333
3.40.7	config web_authentication clear_redir_url	334
3.40.8	config web_authentication method	334
3.40.9	config web_authentication ports	335
3.40.10	config web_authentication redir_url	336
3.40.11	config web_authentication switch_http_port	336
3.40.12	config web_authentication auth_page	338
3.40.13	config web_authentication virtual_ip	339
3.40.14	clear web_authentication auth_state	340

3.40.15 delete web_authentication	341
3.40.16 show web_authentication	341
3.40.17 show web_authentication auth_state ports	342
3.40.18 show web_authentication ports	343
3.40.19 show web_authentication user	343
3.40.20 show web_authentication auth_page	344
3.41 POE コマンド	345
3.41.1 config poe ports	345
3.41.2 show poe ports	346
3.41.3 config poe system	347
3.41.4 show poe system	348
3.42 COMMAND LOGGING コマンド	349
3.42.1 enable command logging	349
3.42.2 disable command logging	349
3.42.3 show command logging	350
3.43 Link Error Recovery コマンド	351
3.43.1 config auto_recovery_mode	351
3.43.2 show auto_recovery_mode	351
4. 使用上の注意事項	352
5. トラブルシューティング	353
5.1 表示 LED に関連する現象と対策	353
5.2 コンソール端末に関連する現象と対策	353
5.3 Telnet に関連する現象と対策	354
5.4 スイッチングハブ機能に関連する現象と対策	354
5.5 VLAN に関連する現象と対策	354
5.6 SFP に関連する現象と対策	354
5.7 PoE に関連する現象と対策	355
5.8 内蔵冷却ファンに関連する現象と対策	355
6. 準拠規格	356

1. パラメーター設定手順

パラメーターの設定は下記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1.4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あるいはTelnet(最大8セッション)による)は3章で詳述します。WEBベース GUI方式は別紙(SWマニュアル)を参照してください。

1.1 出荷時の設定値一覧

全般的な機能に関する出荷時のデフォルト設定値を表 1-1に示します。

設定変更した場合には、「save」コマンドの実行により設定が保存されます。

出荷時の設定に戻す場合には、「reset system」コマンドの実行により設定が初期化されます。

表 1-1 デフォルト設定一覧

設定項目	内容	出荷時の設定値
Account Admin	管理者アカウント(パスワード)	“ adpro ” (なし)
Account User	ユーザーアカウント(パスワード)	なし(なし)
Command Prompt	コマンドプロンプト	管理者アカウント “ # ” 一般アカウント “ > ”
Auto Logout	自動ログアウトの時間	10(分)
CLI Paging	画面スクロールの一時停止	Enabled(動作)
Terminal Line	画面表示の行数	24(行)
TELNET	TELNET による装置接続	Enabled(TCP 23)
WEB	WEB ベース GUI による装置接続	Enabled(TCP 80)
IPif DHCP Mode	DHCP による管理 IP アドレス割り当て	Disabled(非動作)
IPif IPaddress	管理 IPv4 アドレス	設定なし(0.0.0.0)
IProute Default	IPv4 デフォルトゲートウェイ	設定なし
IPv6 Address	管理 IPv6 アドレス	設定なし
IPv6 Neighbor	IPv6 スタティックネイバー	設定なし
ARP Aging Time	ARP テーブル学習機能によるエージング時間	20(分)
FDB Aging Time	MAC テーブル学習機能によるエージング時間	300(秒)
VLAN State	VLAN の動作状態	Enabled(動作)
VLAN Name	VLAN 名	default(vid=1)
Port State	ポートの状態(活性/非活性)	活性(Enabled)
Medium Type	コンポポートのメディアタイプ(Fiber/Copper)	Copper(UTP)
Port Speed Duplex	通信速度/通信方式の自動認識	Auto-Nego(自動認識)
Port MDIX	MDI/MDI-X の自動認識	Auto-MDIX(自動認識)
Port Flow Control	フロー制御の動作状態	Disabled(非動作)
Jumbo Frame	Jumbo Frame 機能	Enabled(動作)
Link Aggregation Status	リンクアグリゲーション機能の動作状態	Disabled(非動作)

設定項目	内 容	出荷時の設定値
Link Aggregation Type	リンクアグリゲーションのタイプ(Static/Lacp)	Static
Link Aggregation Algorithm	リンクアグリゲーションのアルゴリズム	MAC source
Mirror	ポートミラーリング機能の動作状態	Disabled(非動作)
Syslog	ログ転送機能の動作状態	Disabled(非動作)
Syslog Host	ログ転送先 IP アドレス	設定なし
SNMP Status ¹	SNMP の動作状態	Enabled(動作)
SNMP Community	コミュニティ名	public(Read_Only) private(Read_Write)
SNMP Traps	トラップ送信機能の動作状態	Enabled(動作)
SNMP Host	トラップ送信先 IP アドレス	設定なし
SNMP System Contact	システムコンタクト	設定なし
SNMP System Location	システムロケーション	設定なし
SNMP System Name	システムネーム	設定なし
RMON	リモートモニタリング機能の動作状態	Disabled(非動作)
SSH	SSH 機能	Disabled(非動作)
SSL	SSL 機能の動作状態	Disabled(非動作)
LLDP	LLDP 機能の動作状態	Disabled(非動作)
GVRP	GVRP 機能の動作状態	Disabled(非動作)
IGMP Snooping	IGMP Snooping 機能	Disabled(非動作)
MLD Snooping	MLD Snooping 機能	Disabled(非動作)
Traffic Control Status	パケットストーム制御機能の動作状態	Disabled(非動作)
Traffic Control Action	ストーム検知の動作モード(Drop/Shutdown)	Drop(パケット破棄)
Traffic Control Threshold	ストーム制御の閾値	64(kbps) Shutdown モード(pps)
Traffic Control Interval	ストーム監視の間隔時間	5(秒)
Traffic Control Countdown	ストーム制御時のポート閉塞までの時間	0(秒)
Traffic Control Recover	ストーム制御時のポート開放までの時間	300(秒)
LoopDetect Status	ループ防止機能の動作状態	Disabled(非動作)
LoopDetect Method	ループ検知時の動作モード(Drop/Shutdown)	Shutdown(ポート閉塞)
LoopDetect Interval	ループ監視の間隔時間	10(秒)
LoopDetect Recover Timer	ループ制御時にポート開放するまでの時間	60(秒)
BPDU Guard Status	BPDU ガード機能の動作状態	Disabled(非動作)
BPDU Guard Recovery Time	BPDU ガード制御時にポート開放までの時間	60(秒)
STP Status	スパニングツリープロトコル機能の動作状態	Disabled(非動作)
STP Version	動作バージョン(MSTP/RSTP/STP)	RSTP
STP Max Age	BPDU の最大経過時間	20(秒)
STP Hello Time	ハロー間隔時間	2(秒)

設定項目	内 容	出荷時の設定値
STP Forward Delay	フォワードディレイ時間	15(秒)
STP Max Hop	最大ホップカウント	20
SMTP Status	SMTP クライアント機能の動作状態	Disabled(非動作)
SMTP Server	SMTP サーバー IP アドレス	設定なし(0.0.0.0)
SNTP Status	SNTP クライアント機能の動作状態	Disabled
SNTP Server	SNTP サーバー IP アドレス	設定なし(0.0.0.0)
SNTP Poll Interval	SNTP サーバーへの問い合わせ間隔時間	720(秒)
MAC Auth State	MAC 認証機能	Disabled(非動作)
MAC Auth Method	MAC 認証方法(Local/Radius)	Local
MAC Auth Failover	RADIUS 未応答時の Local 認証切り替え	Disabled(非動作)
MAC Auth Format	MAC 認証時のアドレスフォーマット	Case:uppercase Delimiter:none
MAC Auth Password Type	MAC 認証時のパスワードタイプ	Manual_string
WEB Auth State	WEB 認証機能	Disabled(非動作)
WEB Auth Method	WEB 認証方法(Local/Radius)	Local
WEB Auth Virtual IP	WEB 認証用の仮想 IP アドレス	設定なし(0.0.0.0)
WEB Auth Failover	RADIUS 未応答時の Local 認証切り替え	Disabled(非動作)
802.1X Auth State	802.1x 認証機能	Disabled(非動作)
802.1X Auth Protocol	802.1x 認証方法(Local/Radius_EAP)	Radius_EAP
RADIUS Server	RADIUS サーバー IP アドレス	設定なし
RADIUS Timeout	RADIUS サーバー応答のタイムアウト時間	5(秒)
RADIUS Retransmit	RADIUS サーバー未応答の再送回数	2(回)
QinQ Status	拡張タグ VLAN 機能の動作状態	Disabled(非動作)
QinQ Role	ポートタイプの分類(NNI/UNI)	NNI
QinQ VLAN Translation	VLAN 変換機能の動作状態	Disabled(非動作)
Bandwidth Control	帯域幅制御	制御なし(no_limit)
COS Mapping	COS マッピング(Eth_Priority/IP_Priority)	Eth_Priority(802.1p)
802.1p User Priority	Tag User Priority 値のハードウェアキュー	802.1p 0 (Class 1) 802.1p 1 (Class 0) 802.1p 2 (Class 0) 802.1p 3 (Class 1) 802.1p 4 (Class 2) 802.1p 5 (Class 2) 802.1p 6 (Class 3) 802.1p 7 (Class 3)
802.1p Default Priority	Tag なし 802.1p 優先値	802.1p 0 Priority
IP Priority TOS Value	TOS 値に関連付けのハードウェアキュー	TOS 0-7 (Class 0)
IP Priority DSCP Value	DSCP 値に関連付けのハードウェアキュー	DSCP 0-63 (Class 0)
ACL	アクセス制御リストの設定	設定なし

設定項目	内 容	出荷時の設定値
PoE State ²	電力供給機能の動作状態	Enabled(動作)
PoE System Power_Limit	スイッチ全体の供給制限値	125(W)
PoE Ports Power_Limit	ポート単位の供給制限値	15,400(mW)
Command Logging State ³	コマンドログ機能の動作状態	Enabled(動作)

1 SNMP機能はデフォルト設定状態において、SNMPコミュニティ名が一致する全てのSNMPマネージャ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、delete snmp community 設定でコミュニティ名を削除する必要があります。

2 PoE機能はデフォルト設定状態において、Enabled(動作)とするようにソフトウェアバージョン(FM1.05.00以降)で変更しました。FMシリーズの2機種(APLFM108GTPOE/APLFM116GTPOE)で対応します。

3 コマンドログ機能は、ソフトウェアバージョン(FM1.07.00/GM1.03.00以降)で追加しました。

1.2 システム最大値一覧

全般的な機能に関するシステム最大値を表 1-2に示します。

表 1-2 システム最大値一覧

項目	内容	最大値
FDB(MAC Address Table)	MAC アドレステーブル登録数	8191 (スタティック含む)
	unicast スタティックエントリー数	256
	multicast スタティックエントリー数	128
ARP	ARP テーブル登録数	1024 (スタティック含む)
	スタティックエントリー数	255
VLAN	VLAN 数	4094
Q-in-Q	VLAN トランスレーションルール数	16 (Replace)
802.1v	プロトコル VLAN グループ数	16
802.3ad Link Aggregation	リンクアグリゲーショングループ数	製品別 APLFM124 : 14 グループ APLFM116 : 9 グループ APLFM108 : 5 グループ APLGM124 : 8 グループ APLGM118 : 8 グループ APLGM110 : 5 グループ
	1 グループに対するメンバーポート数	8
QOS	ハードウェアキュー数	4 (Class 0-3)
ACL	アクセスリストのプロファイル数	製品別 FM シリーズ : 512 GM シリーズ : 256
	1 プロファイルに対するルール数	製品別 FM シリーズ : 512 GM シリーズ : 256
Port security	ポートで制限する MAC アドレス学習数	64
Telnet Session	Telnet の同時セッション数	8
User Account	装置ログインのアカウント数	8
Trusted Host	Trusted ホストの IP エントリー数	10
Syslog Host	Syslog 送信先の IP エントリー数	4
IGMP Snooping	IGMP マルチキャストグループ数	製品別 FM シリーズ : 1024 GM シリーズ : 128
	IP ホスト数	1024
MLD Snooping	MLD マルチキャストグループ数	製品別 FM シリーズ : 1024 GM シリーズ : 128

項目	内容	最大値
MAC Based Access Control	MAC 認証で RADIUS 認証による収容端末数	128 (装置全体)
	MAC 認証で Local 認証によるエントリー数	128
Web Authentication	WEB 認証で RADIUS 認証による収容端末数	512 (装置全体)
	WEB 認証で Local 認証によるエントリー数	16
802.1x Authentication	802.1x 認証で RADIUS 認証による収容端末数	16 (ポート単位)
	802.1x 認証で Local 認証によるエントリー数	128
Radius Server	RADIUS サーバーの IP エントリー数	3
MSTP	MSTP インスタンス数	4
LLDP	LLDP 通知 VLAN 数	32
Bandwidth	トラフィック制限値	製品別 1024000(Kbps) FM シリーズ : 62.5 倍数 GM シリーズ : 64 倍数
Jumbo	ジャンボフレームサイズ (Un-Tag)	製品別 FM シリーズ : 2044(Byte) GM シリーズ : 9212(Byte)
	ジャンボフレームサイズ (Tag)	製品別 FM シリーズ : 2048(Byte) GM シリーズ : 9216(Byte)
SMTP	SMTP サーバーの IP エントリー数	1
SNTP	SNTP サーバーの IP エントリー数	2
AAA	AAA 認証サーバーの IP エントリー数	16
	AAA 認証サーバーグループ数	4
	AAA 認証サーバー1グループの IP エントリー数	8
SSH	SSH の同時セッション数	8
SNMP	SNMP MIB ビューのエントリー数	30
	SNMP MIB グループのエントリー数	30
	SNMP Community 名のエントリー数	10
	SNMP v3 ユーザー名のエントリー数	10
	SNMP トラップ送信先の IP エントリー数	10
LOG	ログの保存件数	6000(Line)
Mirror	ミラーリングの転送先ポート数	1
SSL Certificate	証明書のインポート数	1
PoE	装置全体の供給電力制限値	125(W)
	ポート単位の供給電力制限値	15,400(mW)

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

PWR 表示 LED が点灯していることを確認してください。

表示されたら、何かキーを押して下さい。
表示されない場合、Ctrl+r を押し、コンソール画面を更新してください。
<表示例>
Press any key to login...

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。
表示されない場合、Ctrl+r を押し、コンソール画面を更新してください。
<表示例>
ApresiaLightFM108GT-SS Fast Ethernet Switch
Command Line Interface

Firmware: 1.08.00
Copyright(C) 2014 Hitachi Metals, Ltd. All rights reserved.
UserName:

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)

本装置からログアウト

```
#logout
```

Press any key to login...

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 10.0.0.1

プロンプト(UserName:)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

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 1-3、表 1-4 に示します。

表 1-3 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 1-4 通信条件

項番	項目	仕様
1	キャラクター	8bit/キャラクター
2	ストップビット	1bit
3	パリティ	なし
4	フロー制御	なし
5	ボー・レート	9600bps
6	端末接続ケーブル	RS-232C ケーブル(ストレート)、 ただし、本装置側は DB-9 オ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標準添付されている専用コンソールケーブル(ストレート)を用いて接続します。

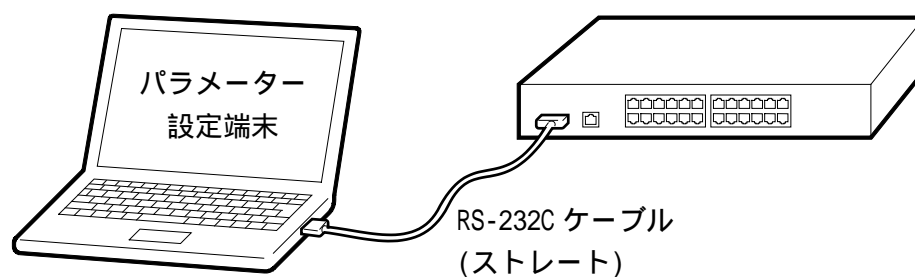


図 1-1 RS-232C ケーブルの接続

下記に本装置のコンソールポートのピン仕様を記載します。コンソールポートは、RS-232C(DTE仕様,メス)になっています。

表 1-5 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	-	-	-
2	SD	送信データ	出力
3	RD	受信データ	入力
4	-	-	-
5	SG	回路アース	-
6	-	-	-
7	-	-	-
8	-	-	-
9	-	-	-

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 ケーブルのピン配置を下記に記載します。

表 1-6 RS-232C ケーブル接続結線例 (D-SUB9 ピン-9 ピンの場合)

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

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章および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
<i>ITALIC</i> 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ませんので、そのままリターンを押してログインしてください。

```
ApresiaLightFM108GT-SS Fast Ethernet Switch
Command Line Interface

Firmware: 1.08.00
Copyright(C) 2014 Hitachi Metals, Ltd. All rights reserved.
UserName:adpro
PassWord:

#
```

2.2.2 初期化アカウント ap_recovery

Ver. 1.05.00 から実装された「ap_recovery」は装置のパスワード、設定を全て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、フラッシュメモリーに保存された設定、ログの全てを消去して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。このアカウントはコンソールポートのみで有効です。

```
ApresiaLightFM124GT-SS Fast Ethernet Switch
Command Line Interface

Firmware: 1.08.00
Copyright(C) 2014 Hitachi Metals, Ltd. All rights reserved.
UserName:ap_recovery
System will be reset, save and reboot!
Load Factory Default Configuration... Done.
Saving all configurations to NV-RAM... Done.
Please wait, the switch is rebooting...
```

2.2.3 コマンド入力

2.2.3.1 コマンド入力文字

本コマンドライン方式は大文字/小文字を区別します。

2.2.3.2 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、全ての文字列の入力は必要ありません。

(例) “save config”コマンドを省略して入力

```
# save config
```

```
# sa c
```

- (2) 使用可能なコマンドを知りたい場合には、[?]キーを押してください。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、選択可能な全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]キーを押すと、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しますので、全ての文字列を入力する必要がありません。例えば “sa” という文字列から選択可能なコマンドは “save” であることを知ることができます。

(例)

```
# sa[TAB]キー
```

```
# save
```

2.2.3.3 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、“save config”コマンドを使ってください。
(例)

```
#save config
Command: save config

Saving all configurations to NV-RAM..... Done.
Success.

#
```

2.2.3.4 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、画面下に表示制御キーが表示されま
す。この状態で、必要に応じた表示制御キーを入力して下さい。

注意事項

! コマンドの文字列が長い場合、行のズレが起きます。その場合はお使いのターミナル
ソフトの1行辺りの文字列数を80文字に設定ください。

2.2.3.5 キーの使い方

コマンド編集キーと表示制御キーの使い方を以下に記載します。

表 2-2 コマンド編集キーの使い方


Delete キー	カーソルを当てた文字を削除して、次に、その行に残った文字を左にシフトします。
Backspace キー	文字をカーソルの左方向に削除して、次に、その行に残っている文字を左にシフトします。
Insert キーまたは Ctrl+R	オンとオフを切り替えます。 オンの場合、文字を挿入し、前の文字を右にシフトします。
左向き矢印キー	左にカーソルを移動します。
右向き矢印キー	右にカーソルを移動します。
上向き矢印キー	前に入力したコマンドを繰り返します。 上向き矢印キーを押すたびに表示されているものよりも前のコマンドが表示されます。このように、現在のセッションのコマンド履歴を見直すことができます。コマンド履歴を順番に沿って前に進めるためには、下向き矢印キーを使用します。
下向き矢印キー	下向き矢印キーは現在のセッションに入力されたコマンド履歴において次のコマンドを表示します。各コマンドは、入力した順番に表示されます。上向き矢印キーを使用して、前のコマンドを見直します。
Tab キー	左にある次のフィールドにカーソルをシフトします。

表 2-3 表示制御キーの使い方

スペースバー	次のページを表示します。
CTRL+c	複数のページが表示される場合、残りのページの表示を止めます。
ESC キー	複数のページが表示される場合、残りのページの表示を止めます。
n	次のページを表示します。
p	前のページを表示します。
q	複数のページが表示される場合、残りのページの表示を止めます。
r	現在表示されているページを更新します。
a	ページ表示を中断せずに、残りのページを表示します。
Enter キー	次の行またはテーブルエントリを表示します。

3. コマンドの詳細

注意事項

-  本ファームウェア(Ver.1.08.00)では、本章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 ツイストケーブル診断コマンド

3.1.1 cable_diag ports

目的	ツイストケーブルの接続をテストします。ツイストケーブルにエラーが発生した場合、エラーのタイプと発生箇所を診断します。
構文	cable_diag ports < <portlist> all >
説明	10/100M ポートの場合、2組のツイストケーブルを診断します。ツイストケーブルのエラータイプは、「open」または「short」です。「open」とは、エラーになっている対のツイストケーブルが特定された箇所で接続していないことを示します。「short」とは、エラーになっている対のツイストケーブルが特定された箇所でショートしていることを示します。ステータスがリンクアップの場合、「short」や「open」エラーの問題はありませんが、リンクダウンでは調査の必要があります。テストで正常なツイストケーブルが接続されておりリモートパートナーの電源が落ちている場合には、リモートパートナーの電源が入っているとしてツイストケーブルの健全性を診断することができます。ツイストケーブル接続されていない場合には、No Cable と表示されます。テストでは、ツイストケーブルの長さも検出しますが参考値としてください。ケーブル種類やインターフェースの状態により実際の長さとは異なる場合があります。本テストの実行時に診断パケットを送出します。また、ポートのリンクアップおよびリンクダウンが発生しますのでご注意ください。なお、光ファイバケーブルを接続しているポートでは、本テストの対象にはなりません。
パラメーター	<portlist> - テストするポート範囲を指定します。 all - すべてのポート
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ポート 25 ~ 28 のツイストケーブル診断を行うには

```
#cable_diag ports 25-28
Command: cable_diag ports 25-28

Perform Cable Diagnostics ...

Port   Type   Link Status   Test Result   Cable Length (M)
-----
25     GE     Link Up       OK             3
26     GE     Link Down     No Cable      -
27     GE     Link Down     No Cable      -
28     GE     Link Down     No Cable      -

#
```

3.2 基本的な IP コマンド

3.2.1 config ipif

目的	IP インターフェースを設定します。
構文	<pre>config ipif System < ipaddress bootp dhcp ipv6 ipv6address <ipv6networkaddr> > /paddress =ipaddress <network_address> < vlan <vlan_name 32> state < enable disable > ></pre>
説明	本コマンドは、IP インターフェースをスイッチに設定します。
パラメーター	<p>ipaddress <network_address> - 作成する IP インターフェースの IP アドレスとネットマスクを入力します。従来の形式でアドレスとマスクの情報を指定できます (例: 10.1.2.3/255.0.0.0 または 10.1.2.3/8 の CIDR 形式など)。</p> <p><vlan_name 32> - IP インターフェースに対応する VLAN 名。</p> <p>state <enable disable> - IP インターフェースを「enable」(有効)または「disable」(無効)にします。</p> <p>bootp - スwitchの IP インターフェースに IP アドレスを割り当てるために、BOOTP プロトコルを選択します。</p> <p>dhcp - スwitchの IP インターフェースに IP アドレスを割り当てるために、DHCP プロトコルを選択します。</p> <p>ipv6 ipv6address <ipv6networkaddr> - IPV6 ネットワークアドレス。このアドレスはホストアドレスとネットワークプレフィックスの長さを定義します。一つのインターフェースに複数の IPv6 アドレスを設定することができます。新しいアドレスが定義されると、この ipif に追加されます。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: IP インターフェースを設定するには

```
#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

#
```

使用例: IP インターフェースを初期化するには

```
#config ipif System ipaddress 0.0.0.0/0
Command: config ipif System ipaddress 0.0.0.0/0

Success.

#
```

3.2.2 show ipif

目的	スイッチの IP インターフェース設定を表示します。
構文	show ipif
説明	本コマンドは、スイッチの IP インターフェース設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: IP インターフェース設定を表示するには

```
#show ipif
Command: show ipif

IP Interface Settings

Interface Name   : System
IP Address      : 10.90.90.90    (MANUAL)
Subnet Mask     : 255.0.0.0
VLAN Name       : default
Admin. State    : Enabled
Link Status     : Link UP
Member Ports    : 1-28

Total Entries : 1

#
```

3.3 基本的なスイッチコマンド

3.3.1 create account

目的	アカウントを作成します。
構文	create account < admin user > <username 15>
説明	本コマンドは、1～15文字までのユーザー名と0～15文字までのパスワードでユーザーアカウントを作成できます。アカウントは8個まで作成できません。
パラメーター	admin <username> - 管理者アカウントの名前。 user <username> - ユーザーアカウントの名前。
制限事項	管理者アカウントのみ本コマンドを実行できます。 ユーザー名は1～15文字になります。 パスワードは0～15文字になります
対応バージョン	1.00.00以降

使用例: 「HCL」というユーザー名を使用して管理者アカウントを作成するには

```
#create account admin HCL
Command: create account admin HCL

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

#
```

3.3.2 config account

目的	アカウントにパスワードを設定します。
構文	config account <username>
説明	本コマンドは、「create account」コマンドで作成したアカウントにパスワードを設定します。コマンド入力後に、古いパスワード、新しいパスワード、新しいパスワードの再入力を促す表示がされます。
パラメーター	<username> - アカウント名。アカウントは既に定義されている必要があります。
制限事項	管理者アカウントのみ本コマンドを実行できます。 ユーザー名は1～15文字になります。 パスワードは0～15文字になります。
対応バージョン	1.00.00以降

使用例: 「HCL」というアカウントのパスワードを設定するには

```
#config account HCL
Command: config account HCL

Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

#
```

3.3.3 show account

目的	アカウントを表示します。
構文	show account
説明	本コマンドは、スイッチに作成済みのすべてのアカウントを表示します。アカウントは1度に8個まで作成できます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 作成したアカウントを表示するには

```
#show account
Command: show account

Current Accounts:
Username          Access Level
-----          -
HCL               Admin

Total Entries: 1

#
```

3.3.4 delete account

目的	既存のアカウントを削除します。
構文	delete account <username>
説明	本コマンドは、「create account」コマンドで作成したアカウントを削除します。
パラメーター	<username> - 削除するアカウント名。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 「HCL」というアカウントを削除するには

```
#delete account HCL
Command: delete account HCL

Success.

#
```

3.3.5 show session

目的	現在ログイン中のユーザーのリストを表示します。
構文	show session
説明	本コマンドは、コマンドが出されたときにログインしている全ユーザーのリストを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ユーザーがログインした方法を表示するには

```
#show session
Command: show session

ID Live Time           From                Level   Name
--
8  0:0:53.410  Serial Port        4      adpro
Total Entries: 1

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```


3.3.6 show switch

目的	スイッチに関する一般的な情報を表示します。
構文	show switch
説明	本コマンドは、スイッチに関する情報を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチの情報を表示するには

#show switch	
Command: show switch	
Device Type	: APLFM108GTSS Fast Ethernet Switch
MAC Address	: 00-40-66-00-00-01
IP Address	: 10.73.60.100 (Manual)
VLAN Name	: default
Subnet Mask	: 255.0.0.0
Default Gateway	: 0.0.0.0
Boot PROM Version	: 1.00.00
Firmware Version	: 1.08.00
System Name	:
System Location	:
System Contact	:
Spanning Tree	: Disabled
GVRP	: Disabled
IGMP Snooping	: Disabled
802.1X	: Disabled
Telnet	: Enabled (TCP 23)
Web	: Enabled (TCP 80)
RMON	: Disabled
SSH	: Disabled
SSL	: Disabled
CLI Paging	: Enabled
Syslog Global State	: Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All	

3.3.7 show serial_port

目的	現在のシリアルポート設定を表示します。
構文	show serial_port
説明	本コマンドは、現在のシリアルポート設定を表示します。
パラメーター	なし。
制限事項	なし
対応バージョン	1.00.00 以降

使用例:シリアルポート設定を表示するには

```
#show serial_port
Command: show serial_port

Baud Rate      : 9600
Data Bits      : 8
Parity Bits     : None
Stop Bits      : 1
Auto-Logout    : 10 mins

#
```

3.3.8 config serial_port

目的	シリアルポートの設定をします。
構文	config serial_port < baud_rate auto_logout > baud_rate =baud_rate < 9600 19200 38400 115200 > auto_logout =auto_logout < never 2_minutes 5_minutes 10_minutes 15_minutes >
説明	本コマンドは、シリアルポートボーレートと自動ログアウト時間を設定します。
パラメーター	baud_rate <9600 19200 38400 115200> - 管理ホストとの通信に使用されるシリアルボーレート。 次の4つのオプションがあります: 9600、19200、38400、および115200。 never - ユーザーからの入力がない場合でもコンソールはログアウトせずに開いた状態を維持します。 2_minutes - ユーザーからの入力がない場合から2分経過後に、コンソールは自動的にログアウトします。 5_minutes- ユーザーからの入力がない場合から5分経過後に、コンソールは自動的にログアウトします。 10_minutes - ユーザーからの入力がない場合から10分経過後に、コンソールは自動的にログアウトします。 15_minutes - ユーザーからの入力がない場合から15分経過後に、コンソールは自動的にログアウトします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: シリアルボーレートを設定するには

```
#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Success.

#
```

3.3.9 enable clipaging

目的	コマンドが1ページ以上を表示する場合、コンソール画面のスクローリングを一時停止します。
構文	enable clipaging
説明	本コマンドは、コンソール画面で複数ページに表示される場合、ページごとに一時停止します。デフォルト値は「enable」（有効）です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例: 「show」コマンドの出力がページの最後に達したとき、画面の表示を一時停止させるには

```
#enable clipaging
Command: enable clipaging

Success.

#
```

3.3.10 disable clipaging

目的	コマンドが1画面以上の情報を表示する場合、各画面の最後でコンソール画面のスクローリングを一時停止する機能を無効にします。
構文	disable clipaging
説明	本コマンドは、1画面以上の情報を表示する場合、各画面の最後でコンソール画面のスクローリングを一時停止する機能を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例: 「show」コマンドの出力がページの最後に達したとき、画面表示の一時停止を無効にするには

```
#disable clipaging
Command: disable clipaging

Success.

#
```

3.3.11 enable telnet

目的	Telnet プロトコルを使用したスイッチとの通信を有効にします。
構文	enable telnet [<tcp_port_number 1-65535>]
説明	本コマンドは、スイッチの Telnet プロトコルを有効にします。スイッチの Telnet リクエストポート番号を指定できます。
パラメーター	<tcp_port_number 1-65535> - TCP ポート番号。TCP ポート番号は、1～65535 です。デフォルト値は、23 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Telnet を有効にし、ポート番号「23」を設定するには

```
#enable telnet 23
Command: enable telnet 23

Success.

#
```

3.3.12 disable telnet

目的	スイッチの Telnet プロトコルを無効にします。
構文	disable telnet
説明	本コマンドは、スイッチの Telnet プロトコルを無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの Telnet プロトコルを無効にするには

```
#disable telnet
Command: disable telnet

Success.

#
```

3.3.13 telnet

目的	telnet プロトコルを介して他の機器に接続します。
構文	telnet <ipaddr> [tcp_port <value 0-65535>]
説明	本コマンドは、Telnet プロトコルを介して他の機器に接続します。
パラメーター	<ipaddr> - Telnet を使用して接続する機器の IP アドレスを入力します。 tcp_port <value 0-65535> - 接続に使用する TCP ポート番号を入力します。 デフォルト値は、23 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。 本装置からの IPv6 Telnet クライアント機能には対応しておりません。 本装置への IPv6 Telnet アクセスは可能です。
対応バージョン	1.00.00 以降

使用例:TCP ポート番号「23」の Telnet プロトコルを介して IP アドレス (10.53.13.99) の機器に接続するには

```
#telnet 10.53.13.99 tcp_port 23
Command: telnet 10.53.13.99 tcp_port 23
```

3.3.14 enable web

目的	スイッチの web ベース GUI を有効にします。
構文	enable web [<tcp_port_number 1-65535>]
説明	本コマンドは、スイッチの web ベース GUI を有効にします。 スイッチの HTTP ポート番号を指定できます。
パラメーター	<tcp_port_number 1-65535>- TCP ポート番号。 TCP ポート番号は、1 ~ 65535 です。 デフォルト値は、80 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:HTTP を有効にし、ポート番号「80」を設定するには

```
#enable web 80
Command: enable web 80

Note: SSL will be disabled if web is enabled.
Success.

#
```

3.3.15 disable web

目的	スイッチの web ベース GUI を無効にします。
構文	disable web
説明	スイッチの web ベース GUI を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:web ベース GUI を無効にするには

```
#disable web
Command: disable web

Success.

#
```

3.3.16 save

目的	NV-RAM にスイッチコンフィギュレーションの変更を保存します。
構文	save [< config log all >]
説明	本コマンドは、NV-RAM に現在のスイッチコンフィギュレーションを保存します。保存されたスイッチコンフィギュレーションは、スイッチを再起動するたびにスイッチのメモリーにロードされます。
パラメーター	config - 現在のスイッチコンフィギュレーションを NV-RAM に保存します。 log - 現在のログを NV-RAM に保存します。保存されたログは削除できません。 all - 現在アクチベートされたコンフィギュレーションの変更とログを保存します。現在のスイッチコンフィギュレーションと現在のログの両方を NV-RAM に保存します。キーワードを指定しない場合は、config を指定した場合と同じになります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:NV-RAM にスイッチの現在のコンフィギュレーションを保存するには

```
#save config
Command: save config

Saving all configurations to NV-RAM..... Done.
Success.

#
```

使用例:NV-RAM にスイッチの現在のログを保存するには

```
#save log
Command: save log

Saving all log information to NV-RAM..... Done.
Success.

#
```

使用例:NV-RAM にスイッチの現在のコンフィギュレーションとログを保存するには

```
#save all
Command: save all

Saving all configurations and log information to NV-RAM..... Done.
Success.

#
```

3.3.17 reboot

目的	スイッチを再起動します。
構文	reboot [force_agree]
説明	本コマンドは、スイッチを再起動します。
パラメーター	force_agree - force_agree を指定すると、再起動の確認を行わずに、すぐに再起動が始まります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチを再起動するには

```
#reboot
Command: reboot
Are you sure you want to proceed with the system reboot?(Y|N)
Please wait, the switch is rebooting...
```

使用例:スイッチを強制再起動するには

```
#reboot force_agree
Command: reboot force_agree

Please wait, the switch is rebooting...
```

3.3.18 reset

目的	スイッチをデフォルト設定に戻します。
構文	reset [config system] [force_agree]
説明	本コマンドは、スイッチのコンフィギュレーションをデフォルト設定に戻します。
パラメーター	<p>config - config のキーワードを指定すると、IP アドレス、アカウント、スイッチ履歴ログなどを含むすべての設定がデフォルト設定に戻ります。スイッチは再起動せずに、即時反映されます。</p> <p>system - system のキーワードを指定すると、スイッチの設定がデフォルト値に変更された後、保存および再起動が行われます。再起動するとフォワーディングデータベース内のすべてのエントリがクリアされます。</p> <p>force_agree - force_agree を指定すると、確認を行わずに、Reset コマンドがすぐに実行されます。</p> <p>パラメーターを指定しないと、スイッチの現在の IP アドレス、アカウント、およびスイッチの履歴ログは変更されません。他のすべてのパラメーターはデフォルト設定にリストアされます。スイッチは保存または再起動しません。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: IP アドレス、ユーザーアカウント、およびスイッチログ履歴以外のデフォルト値にスイッチパラメーターをリストアするには

```
#reset
Command: reset

Are you sure you want to proceed with system reset
except IP address, log and user account?(y/n)
Success.

#
```

使用例: スイッチパラメーターをデフォルト値にリストアするには

```
#reset config
Command: reset config

Are you sure you want to proceed with system reset?(y/n)

Success.

#
```


使用例:すべてのスイッチパラメータをデフォルト値にリストアし、保存して、スイッチを再起動するには

```
#reset system
Command: reset system

Are you sure you want to proceed with system reset, save and reboot?(y/n)
Load Factory Default Configuration... Done.
Saving all configurations to NV-RAM.. Done.
Please wait, the switch is rebooting...
```

3.3.19 login

目的	スイッチのコンソールにログインします。
構文	login
説明	本コマンドは、ログインを開始します。 ユーザー名とパスワードプロンプトが表示されます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ログインを開始するには

```
#login
Command: login

UserName:
```

3.3.20 logout

目的	スイッチのコンソールからログアウトします。
構文	logout
説明	本コマンドは、スイッチのコンソールからログアウトします。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ログアウトするには

```
#logout
```

3.3.21 config terminal_line

目的	画面に表示できるコマンドの行数を設定します。
構文	config terminal_line < default <value 20-80> >
説明	本コマンドは、画面に表示できるコマンドの行数を設定します。デフォルト値は24です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:画面に表示されるコマンドの行数を30行に設定するには

```
#config terminal_line 30
Command: config terminal_line 30

Success.

#
```

3.3.22 show terminal_line

目的	画面に表示できる行数を表示します。
構文	show terminal_line
説明	本コマンドは、画面に表示できるコマンドの行数を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:表示できる現在の行数を表示するには

```
#show terminal_line
Command: show terminal_line

Terminal Line : 24 (Default)

#
```

3.3.23 enable jumbo_frame

目的	ジャンボフレーム機能を有効にします。
構文	enable jumbo_frame
説明	本コマンドは、ジャンボフレームを有効に設定します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ジャンボフレーム機能を有効にするには

```
#enable jumbo_frame
Command: enable jumbo_frame

Success.

#
```

3.3.24 disable jumbo_frame

目的	ジャンボフレーム機能を無効にします。
構文	disable jumbo_frame
説明	本コマンドは、ジャンボフレームを無効に設定します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ジャンボフレーム機能を無効にするには

```
#disable jumbo_frame
Command: disable jumbo_frame

Success.

#
```

3.3.25 show jumbo_frame

目的	ジャンボフレーム機能の現在設定を表示します。
構文	show jumbo_frame
説明	本コマンドは、ジャンボフレーム機能設定の現在設定を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ジャンボフレームの設定を表示するには

```
#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State      : Enabled
Maximum Jumbo Frame Size : 2048 Bytes

#
```

3.3.26 show tech_support

目的	テクニカルサポート情報を表示します。
構文	show tech_support
説明	本コマンドは、テクニカルサポートに必要なスウィッチの動作情報を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: テクニカルサポート情報を表示するには

```
# show tech_support
Command: show tech_support

=====
                        APLFM108GTPOE Fast Ethernet Switch
                        Technical Information Report
=====

[CPU Utilization 94091190ms]
CPU Utilization :
-----
Five Seconds - 25 %           One Minute - 12 %           Five Minutes - 11 %

[Device Information 94091390ms]
Device Type       : APLFM108GTPOE Fast Ethernet Switch
MAC Address       : 00-40-66-00-01-08
IP Address        : 10.9.68.93 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.00
Firmware Version  : Build 1.08.00
Hardware Version  : A
Serial number     :
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
802.1x            : Disabled
TELNET            : Enabled (TCP 23)
WEB               : Enabled (TCP 80)
RMON              : Disabled
SSH               : Disabled
```

SSL : Disabled
Syslog Global State: Disabled
Dual Image : Supported

[Connection Session Status 94091590ms]

ID	Login Time	Live Time	From	Level	Name
8	0/00/00 00:54:05	1:14:5.820	Serial Port	4	adpro

(続 く)

3.4 スイッチユーティリティコマンド

3.4.1 download

目的	TFTP サーバーから新しいファームウェアまたはスイッチのコンフィギュレーションファイルをダウンロードしてインストールします。
構文	download <firmware_fromTFTP <<ipaddr> <ipv6addr> > <path_filename 64> image_id <value 1-2> cfg_fromTFTP <<ipaddr> <ipv6addr> > <path_filename 64> [increment] >
説明	本コマンドは、TFTP サーバーから新しいファームウェアまたはスイッチのコンフィギュレーションファイルをダウンロードします。
パラメーター	<ipaddr> - TFTP サーバーの IP アドレス。 <ipv6addr> - TFTP サーバーの IPv6 アドレス。 <path_filename 64> - TFTP サーバーにあるファームウェアのパスとファームウェア名。例：apIfmR10500.img または、TFTP サーバーにあるコンフィギュレーションファイルのパスとコンフィギュレーションファイル名。例：setting.txt image_id <value 1-2> - 動作しているセクション ID を指定します。セクション ID を指定することによって、スイッチに選択した 2 個のファームウェアバージョンを格納できます。 increment - 部分的なスイッチコンフィギュレーションファイルのダウンロードが可能です。コンフィギュレーションファイルに明示されているスイッチパラメーターのみを変更するようにファイルをダウンロードすることができます。他のすべてのスイッチパラメーターは変更されずにそのまま残ります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

注意事項



ダウンロードしたコンフィギュレーションファイルを現在の設定に置き換えるため、リンクアップしているポートは一時切断されます。

使用例: コンフィギュレーションファイルをダウンロードするには

```
#download cfg_fromTFTP 10.48.74.121 c:¥cfg¥setteing.txt
Command: download cfg_fromTFTP 10.48.74.121 c:¥cfg¥setteing.txt

Connecting to server..... Done.
Download configuration..... Done.
Success.

#
##-----
##                               APLFM108GTSS Configuration
##
##                               Firmware: 1.08.00
##                               Copyright(C) 2014 Hitachi Metals, Ltd. All rights reserved.
##-----
#
#
## BASIC
#
#config serial_port baud_rate 9600 auto_logout 10_minutes
Command: config serial_port baud_rate 9600 auto_logout 10_minutes
```

ダウンロード設定コマンドによって、コンフィギュレーションファイルの各設定順に様々な設定のダウンロードが開始されます。ダウンロードが完了すると、「End of configuration file for APLFM108GTSS」のメッセージが表示され、コマンドプロンプトが続きます。

```
#disable authen_policy
Command: disable authen_policy

Success.

#
```

3.4.2 config firmware image_id

目的	ファームウェアセクションイメージを起動セクションとして指定、またはファームウェアセクションイメージを削除します。
構文	config firmware image_id <value 1-2> < delete boot_up >
説明	本コマンドは、ファームウェアセクションイメージを設定します。ファームウェアセクションを起動セクションとして使用するか削除するか、選択できません。
パラメーター	<value 1-2> - 動作しているセクションイメージを指定します。スイッチは2つのファームウェアバージョンを保持し、イメージ ID を指定することで選択できます。 delete - このパラメーターを入力し、指定したファームウェアセクションイメージを削除します。 boot_up - このパラメーターを入力し、起動セクションイメージとしてファームウェアイメージ ID を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ファームウェアセクションイメージ 1 を起動セクションとして指定するには

<pre># config firmware image_id 1 boot_up Command: config firmware image_id 1 boot_up Success. #</pre>
--

3.4.3 show firmware information

目的	ファームウェアセクション情報を表示します。
構文	show firmware information
説明	本コマンドは、ファームウェアセクション情報を表示します。
パラメーター	なし。
制限事項	なし
対応バージョン	1.00.00 以降

使用例:スイッチの現在のファームウェア情報を表示するには

```
#show firmware information  
Command: show firmware information
```

```
Image ID   : 1(Boot up firmware)  
Version    : 1.05.00  
Size       : 3362728 Bytes  
Update Time: 0000/00/00 00:00:00  
From       : 10.0.0.10  
User       : adpro(CONSOLE)
```



```
Image ID   : 2  
Version    : 1.03.00  
Size       : 3346184 Bytes  
Update Time: 0000/00/00 00:00:00  
From       : 10.0.0.10  
User       : adpro(CONSOLE)
```

```
#
```

3.4.4 show config

目的	スイッチの現在または保存されているコンフィギュレーション設定を表示します。	
構文	show config < current_config config_in_nvram > [modified]	
説明	<p>本コマンドは、NV RAM に保存されているすべてのコンフィギュレーション設定または現在設定されているコンフィギュレーション設定を表示します。キーボードを使用して、「Enter」で1行ずつ、「Space」で1ページずつ、「a」ですべての設定をリストします。</p> <p>コンフィギュレーション設定は、以下の順でカテゴリ別にリストされます。</p>	
	<p>Basic (serial port, Telnet and web management status)</p> <p>storm control</p> <p>IP group management</p> <p>Syslog</p> <p>QoS</p> <p>port mirroring</p> <p>traffic segmentation</p> <p>port</p> <p>port lock</p> <p>8021x</p> <p>SNMPv3</p> <p>management (SNMP traps RMON)</p> <p>VLAN</p> <p>FDB (forwarding data base)</p> <p>STP</p> <p>SSH</p> <p>SSL</p>	<p>ACL</p> <p>SNTP</p> <p>IP route</p> <p>LACP</p> <p>ARP</p> <p>IP</p> <p>IGMP snooping</p> <p>access authentication control (TACACS etc.)</p> <p>Bandwidth</p> <p>GM</p> <p>Banner_promp</p> <p>SMTP</p> <p>AAA</p> <p>LLDP</p> <p>LOOP_DETECT</p> <p>MBA</p>
パラメーター	<p>current_config - NV-RAM に保存せずに入力した設定を表示します。</p> <p>config_in_NVRAM - NV-RAM に保存した設定を表示します。</p> <p>modified - デフォルト状態から変更された設定のみを表示します。</p>	
制限事項	管理者アカウントのみ本コマンドを実行できます。	
対応バージョン	1.05.00 以降	

注意事項

-  パラメーター current_config により表示される設定情報には、account 情報は含まれません。
-  802.1x 認証でローカルユーザーにより登録したパスワード情報は、暗号化されずに表示されます。

使用例:現在のコンフィギュレーション設定を参照するには

```
#show config current_config
Command: show config current_config

#-----
#                               APLFM108GTSS Configuration
#
#                               Firmware: 1.08.00
#                               Copyright(C) 2014 Hitachi Metals, Ltd. All rights reserved.
#-----

# BASIC

config serial_port baud_rate 9600 auto_logout 10_minutes
config default_language japanese
config terminal_line default
enable clipaging

# STORM

config traffic control 1 broadcast disable multicast disable unicast disable action drop
threshold 64 countdown 0 time_interval 5
config traffic control 2 broadcast disable multicast disable unicast disable action drop
threshold 64 countdown 0 time_interval 5

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.4.5 upload

目的	現在のスイッチ設定またはスイッチの履歴ログを TFTP にアップロードします。
構文	upload < cfg_toTFTP log_toTFTP > < <ipaddr> <ipv6addr> > <path_filename 64>
説明	本コマンドは、現在のスイッチ設定またはスイッチの履歴ログのいずれかを TFTP にアップロードします。
パラメーター	cfg_toTFTP - スwitchの現在の設定を TFTP サーバーにアップロードする場合に指定します。 log_toTFTP - スwitch履歴ログを TFTP サーバーにアップロードする場合に指定します。 <ipaddr> - TFTP サーバーの IP アドレス。 <ipv6addr> - TFTP サーバーの IPv6 アドレス。 <path_filename 64> - スwitchコンフィギュレーションファイルの場所を TFTP サーバーに指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

注意事項



パラメーター `cfg_toTFTP` によりアップロードした設定情報には、`account` 情報は含まれません。

使用例: コンフィギュレーションファイルをアップロードするには

```
#upload cfg_toTFTP 10.48.74.121 coufig_up.txt
Command: upload cfg_toTFTP 10.48.74.121 coufig_up.txt
Success.
Connecting to server..... Done.
Upload configuration.....Done.

#
```

3.4.6 ping

目的	ネットワーク機器間の接続性をテストします。
構文	ping <ipaddr> [times <value 0-255>] [size <value 1-60000>] [timeout <sec 1-99>]
説明	本コマンドは、リモート IP アドレスに Internet Control Message Protocol (ICMP) エコーメッセージを送信します。その後、リモート IP アドレスは、メッセージを返します。これは、スイッチとリモートデバイス間の接続性を確認するために使用されます。
パラメーター	<p><ipaddr> - ホストの IP アドレスを指定します。</p> <p>times <value 0-255> - 送信する各 ICMP エコーメッセージ数。「0」の値に設定した場合、ICMP エコーメッセージを無限に送信します。最大値は「255」です。デフォルト値は「0」です。</p> <p>size <value 1-60000> - テスト用パケットのサイズ。値の範囲は、1～60000 です。</p> <p>timeout <sec 1-99> - リモートデバイスからの応答を待つタイムアウトまでの時間を定義します。1～99 秒の範囲で指定できます。デフォルト値は 1 秒です。</p>
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: IP アドレス「10.48.74.121」に 4 回 ping するには

<pre>#ping 10.48.74.121 times 4 Command: ping 10.48.74.121 Reply from 10.48.74.121, time<10ms Reply from 10.48.74.121, time<10ms Reply from 10.48.74.121, time<10ms Reply from 10.48.74.121, time<10ms Ping statistics for 10.48.74.121 Packets: Sent =4, Received =4, Lost =0 #</pre>

3.4.7 ping6

目的	IPv6 ネットワークの診断を行います。
構文	ping6 <ipv6addr> [times <value 1-255> size <value 1-6000> timeout <value 1-10>]
説明	本コマンドは、IPv6 ネットワークの診断に使用します。
パラメーター	<p><ipv6addr> - ホストの IPv6 アドレスを指定します。</p> <p>times <value 1-255> - 送信する各 ICMP エコーメッセージ数。最大値は「255」です。指定しない場合は、ICMP エコーメッセージを送信し続けます。</p> <p>size <value 1-6000> - テスト用パケットのサイズ。値の範囲は、1～6000 です。</p> <p>timeout <value 1-10> - リモートデバイスからの応答を待つタイムアウトまでの時間を定義します。1～10 秒の範囲で指定できます。デフォルト値は 1 秒です。</p>
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: IPv6 アドレス「FE80::254:85FF:FE32:1804」に 6 回 ping を行うには

```
#ping6 FE80::254:85FF:FE32:1804%System times 6
Command: ping6 FE80::254:85FF:FE32:1804%System times 6

Reply from FE80::254:85FF:FE32:1804, bytes=100 time=10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Ping Statistics for FE80::254:85FF:FE32:1804
Packets: Sent =6, Received =6, Lost =0
Success.

#
```

3.4.8 traceroute

目的	スイッチと送信先間の経路を追跡します。
構文	traceroute <ipaddr> [ttl <value 1-60>] [port <value 30000-64900>] [timeout <sec 1-65535>] [probe <value 1-9>]
説明	本コマンドは、スイッチと送信先間の経路を追跡します。
パラメーター	<ipaddr> - 送信先の IP アドレス。 ttl<lvalue 1-60> - 追跡ルートリクエストの TTL 値。ルーターの最大数です。本コマンドは、2つのデバイス間のネットワーク経路を検索する間、交差しません。 port <value 30000-64900> - ポート番号。1024 を超える必要があります。値の範囲は、30000 ~ 64900 です。 probe <value 1-9> - プローブの回数です。範囲は、1 ~ 9 になります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチと 10.48.74.121 間の経路を追跡するには

<pre>#traceroute 10.48.74.121 probe 3 Command: traceroute 10.48.74.121 probe 3 1 <10 ms. 10.48.74.121 1 <10 ms. 10.48.74.121 1 <10 ms. 10.48.74.121 #</pre>

3.4.9 config terminal line

目的	画面に表示できるコマンドの行数を設定します。
構文	config terminal_line < default <value 20-80> >
説明	本コマンドは、画面に表示できるコマンドの行数を設定します。デフォルト値は 24 です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 画面に表示されるコマンドの行数を「30」に設定するには

<pre># config terminal_line 30 Command: config terminal_line 30 Success. #</pre>
--

3.4.10 show terminal line

目的	画面に表示できるコマンドの行数を表示します。
構文	show terminal_line
説明	本コマンドは、画面に表示できるコマンドの行数を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: 画面に表示されるコマンドの行数を表示するには

```
# show terminal_line
Command: show terminal_line

Current terminal line number : 30

#
```

3.4.11 show self-test result

目的	スイッチの起動時に実施された self test 結果を表示します。
構文	show self-test result
説明	本コマンドは、スイッチの起動時に実施された DRAM、FLASH メモリ、SW-LSI、PHY、POE コントローラーの self test 結果を表示します。
パラメーター	なし。
制限事項	POE Test の結果は、APLFM108GT-POE および APLFM116GT-POE の 2 機種のみ表示されます。
対応バージョン	1.08.00 以降

使用例: セルフテストの結果を表示するには

```
#show self-test result
Command: show self-test result

Self-test Result
-----
DRAM Test : No error
FLASH Test : No error
SWLSI Test : No error
PHY Test : No error
POE Test : N/A

#
```


3.4.12 show sfp diag

目的	トランシーバーの光入出力レベルを表示します。
構文	show sfp diag [<portlist>]
説明	本コマンドは、SFPポートに実装されたトランシーバーの光入出力レベルをdBmで表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。 ポートリストを指定しない場合、すべてのポートの情報が表示されます。
制限事項	SFF-8472 準拠品が対象です。型式(H-FX-SFP/R)には対応していません。
対応バージョン	1.08.00 以降

使用例: トランシーバーの光入出力レベルを表示するには

```
#show sfp diag
Command: show sfp diag

  Port          TX Power      RX Power
              (dBm)         (dBm)
-----
  17            -4.77         -5.35
  18            -4.98         -5.30

#
```

3.4.13 show sfp info

目的	トランシーバーのメーカー名、型式などの情報を表示します。
構文	show sfp info [<portlist>]
説明	本コマンドは、SFPポートに実装されたトランシーバーのメーカー名、型式、シリアル番号を表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。 ポートリストを指定しない場合、すべてのポートの情報が表示されます。
制限事項	なし。
対応バージョン	1.08.00 以降

使用例: トランシーバーの情報を表示するには

```
#show sfp info
Command: show sfp info

SFP Port      : 17
Vendor Name   : FINISAR CORP.
Vendor Part Number : FTLF8519P2BNL
Serial Number : PC80ZMP

SFP Port      : 18
```

Vendor Name : FINISAR CORP.
Vendor Part Number : FTLF8519P2BNL
Serial Number : PC80ZMK

#

3.5 コマンド履歴コマンド

3.5.1 ?

目的	コマンドラインインターフェース(CLI)におけるすべてのコマンドを表示します。
構文	? [<command>]
説明	本コマンドは、コマンドラインインターフェース(CLI)で利用可能なすべてのコマンドを表示します。
パラメーター	[<command>] - 適切なコマンドと共に「?」を入力すると、指定したコマンドに対するすべてのパラメーターの一覧がコマンド機能の簡単な説明とコマンド内に同じ用語を持つ類似のコマンドと共に表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:CLI に含まれるすべてのコマンドを表示するには

```
#?  
Command: ?  
  
..  
?  
cable_diag ports  
clear  
clear arptable  
clear counters  
clear fdb  
clear log  
clear mac_based_access_control auth_mac  
clear port_security_entry port  
clear web_authentication auth_state  
config 802.1p default_priority  
config 802.1p user_priority  
config 802.1x auth_parameter ports  
config 802.1x auth_protocol  
config 802.1x capability ports  
config 802.1x init  
config 802.1x reauth  
config access_profile profile_id  
config account  
config admin local_enable  
config arp_aging time  
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

使用例: 特定のコマンドに対するパラメータを表示するには

```
#? config account
Command: ? config account

Command: config account
Usage: <username>
Description: config user account

#
```

3.5.2 dir

目的	コマンドラインインターフェース(CLI)におけるすべてのコマンドを表示します。
構文	dir
説明	本コマンドは、コマンドラインインターフェース(CLI)で利用可能なすべてのコマンドを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: すべてのコマンドを表示するには

```
#dir
Command: dir

..
?
cable_diag ports
clear
clear arptable
clear counters
clear fdb
clear log
clear mac_based_access_control auth_mac
clear port_security_entry port
clear web_authentication auth_state
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
```

```

config admin local_enable
config arp_aging time
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

```

3.5.3 config command_history

目的	コマンド履歴を設定します。
構文	config command_history <value 1-40>
説明	本コマンドは、コマンド履歴を設定します。
パラメーター	<value 1-40> - バッファで維持される、前に実行したコマンド数。40 までの最後に実行したコマンドが表示できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: コマンド履歴を「20」に設定するには

```

#config command_history 20
Command: config command_history 20

Success.

#

```

3.5.4 show command_history

目的	コマンド履歴を表示します。
構文	show command_history
説明	本コマンドは、コマンド履歴を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: コマンド履歴を表示するには

```

#show command_history
Command: show command_history

?
? show
show vlan
show command history

#

```

3.6 LLDP コマンド

3.6.1 enable lldp

目的	スイッチの LLDP 操作を有効にします。
構文	enable lldp
説明	本コマンドは、LLDP 機能のグローバル制御に使用します。 本機能を有効にすると、スイッチは、LLDP パケットの送受信を開始し、LLDP パケットの処理を行います。 各ポートの具体的な機能は、ポートごとの LLDP 設定に依存します。LLDP パケットの通知のために、スイッチはポートを介して情報をネイバーに知らせます。 LLDP パケットを受信するためには、スイッチはネイバーデバイステーブル内のネイバーデバイスから通知された LLDP パケットより情報を学習します。 デフォルト値では LLDP の状態は無効です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:LLDP を有効にするには

```
# enable lldp
Command: enable lldp

Success.

#
```

3.6.2 disable lldp

目的	スイッチの LLDP 操作を無効にします。
構文	disable lldp
説明	本コマンドは、LLDP 通知パケットの送受信を中止します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:LLDP を無効にするには

```
# disable lldp
Command: disable lldp

Success.

#
```

3.6.3 config lldp message_tx_interval

目的	パケット送信間隔を変更します。
構文	config lldp message_tx_interval <sec 5-32768>
説明	本コマンドは、アクティブなポートがネイバーに通知を再送する頻度を制御します。
パラメーター	message_tx_interval - 任意のポートにおける LLDP 通知の連続する送信間の間隔を変更します。範囲は 5 ~ 32768 秒です。デフォルト値は 30 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:パケット送信間隔を「30」に設定するには

```
# config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

#
```

3.6.4 config lldp message_tx_hold_multiplier

目的	本コマンドは、メッセージホールドマルチプライヤを設定します。
構文	config lldp message_tx_hold_multiplier <int 2-10>
説明	本コマンドは、LLDPDU での txTTL における TTL 値を計算するのに使用される msgTxInterval の乗数です。TTL は LLDPDU パケットによって送信されます。その保持期間は 65535 と (message_tx_interval * message_tx_hold_multiplier) の小さい方になります。パートナースイッチでは、指定された通知の保持期間 (TTL) の期限が来ると、通知データはネイバースイッチの MIB から削除されます。
パラメーター	message_tx_hold_multiplier - 範囲は、2 ~ 10 です。デフォルト値は 4 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:マルチプライヤの値を「3」に変更するには

```
# config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

#
```

3.6.5 config lldp tx_delay

目的	LLDP ポートの最短時間 (遅延間隔) を変更します。 LLDP MIB コンテンツの変更のために、連続した LLDP 通知を遅延します。「tx delay」は、MIB コンテンツの頻繁な変更のために LLDP メッセージを送信する最小間隔を定義します。
構文	config lldp tx_delay <sec 1-8192>
説明	LLDP message_tx_interval (送信間隔) は 4 x tx_delay (遅延間隔) 以上である必要があります。
パラメーター	tx_delay - 範囲は 1 秒から 8192 秒です。デフォルト値は、2 秒です。 注意: Tx Delay は、0.25 * msgTxInterval 以下となる必要があります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 遅延時間を「8」設定するには

```
# config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

#
```

3.6.6 config lldp reinit_delay

目的	再初期化間隔の最小値を変更します。
構文	config lldp reinit_delay <sec 1-10>
説明	再度有効とされる LLDP ポートは、最後の「disable」(無効化)コマンドの後、reinit_delay(再初期化遅延)時間待機します。
パラメーター	reinit_delay - 範囲は 1 秒から 10 秒です。デフォルト値は、2 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 再初期化遅延間隔を「5」に変更するには

```
# config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

#
```


3.6.7 config lldp notification_interval

目的	定義済みの SNMP トラップレシーバに通知を送信する通知間隔のタイマーを設定します。
構文	config lldp notification_interval <sec 5 - 3600>
説明	スイッチによって生成される連続した LLDP 変更通知間の間隔をグローバルに変更します。
パラメーター	notification_interval - 範囲は 5 秒から 3600 秒です。デフォルト値は 5 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 通知間隔の値を「10」に変更するには

```
# config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

#
```

3.6.8 config lldp ports notification

目的	定義済みの SNMP トラップレシーバに通知を送信する各ポートを設定します。
構文	config lldp ports < <portlist> all > notification < enable disable >
説明	LLDP のデータの変更が LLDP ネイバーデバイスからポートに受信した通知の中に検出された場合、構成済みの SNMP トラップレシーバへの各ポートの変更通知の送信を「enable」（有効）または「disable」（無効）にします。変更の定義には、新しい有効な情報、タイムアウト情報、更新情報が含まれます。変更のタイプには、データの更新/挿入/削除が含まれます。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 notification - ネイバーのデバイスから受信した通知で検出された LLDP データ変更の SNMP トラップ通知を有効または無効にします。デフォルトでは、通知は無効です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート SNMP の通知状態を変更するには

```
# config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

#
```

3.6.9 config lldp ports admin_status

目的	各ポートごとの送信モードと受信モードを設定します。
構文	config lldp ports < <portlist> all > admin_status < tx_only rx_only tx_and_rx disable >
説明	これらのオプションは、どのポートが LLDP トラフィックに参加するのか、さらに参加ポートが、LLDP トラフィックを一方向または両方向許可するのかを制御します。
パラメーター	<p><portlist> - 設定するポート範囲を指定します。</p> <p>all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。</p> <p>tx_only - 指定ポートは LLDP パケットを送信しますが、ネイバーデバイスからの入力側パケットはブロックします。</p> <p>rx_only - 指定ポートはネイバーデバイスからの LLDP パケットを受信しますが、ネイバーデバイスへの出力側パケットはブロックします。</p> <p>tx_and_rx - 指定ポートは LLDP パケットの送受信両方を行います。</p> <p>disable - 指定ポートにおける LLDP パケットの送受信を無効にします。</p> <p>各ポートステータスはデフォルトにより tx_and_rx になっています。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1-5 の送信モードと受信モードを設定するには

```
# config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

#
```

3.6.10 config lldp ports mgt_addr

目的	管理アドレスのインスタンスを表す通知用に指定されたポートを「enable」(有効)または「disable」(無効)にします。
構文	config lldp ports < <portlist> all > mgt_addr ipv4 <ipaddr> < enable disable >
説明	本コマンドは、システムの IP アドレスが指定ポートから通知される必要があるかどうかを指定します。レイヤ 3 デバイスでは、各管理アドレスを個別に指定できます。リストに追加される管理アドレスは、各管理アドレスに対応付けされた特定のインターフェースからの LLDP に通知されます。さらに、その管理アドレスのインターフェースは ifindex 形式で通知されます。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 ipv4 - IPV4 の IP アドレス。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1-2 に対してアドレスエントリーの管理を有効にするには

```
# config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable
Command: config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable

Success

#
```

3.6.11 config lldp ports basic_tlvs

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上のオプションの TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> all > basic_tlvs < all < port_description system_name system_description system_capabilities > > < enable disable >
説明	スイッチのアクティブな LLDP ポートには、通常、出力側の通知に常に必須データを含んでいます。出力側 LLDP 通知からこれらのデータタイプを 1 個以上除外するために、個別のポートまたはポートグループに設定できる 4 つのオプションデータがあります。必須データタイプには、4 つの基本的な情報タイプ (end f LLDPDU TLV、chassis ID TLV、port ID TLV、Time to Live TLV) があります。必須データタイプを無効にすることはできません。さらに、オプションで選択可能な 4 つのデータタイプがあります。これらは、「port_description」、「system_name」、「system_description」、および「system_capability」です。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。

パラメーター	<p>port_description - この TLV のオプションデータタイプは、LLDP エージェントがポートの「Port Description TLV」を送信する必要があることを示します。デフォルトでは無効になっています。</p> <p>system_name - この TLV のオプションデータタイプは、LLDP エージェントが「System Name TLV」を送信する必要があることを示します。デフォルトでは無効になっています。</p> <p>system_description - この TLV のオプションデータタイプは、LLDP エージェントが「System Description TLV」を送信する必要があることを示します。デフォルトでは無効になっています。</p> <p>system_capabilities - この TLV のオプションデータタイプは、LLDP エージェントが「System Capabilities TLV」を送信する必要があることを示します。System capability は、デバイスがリピータ、ブリッジ、またはルーター機能を提供するかどうか、また提供された機能が現在有効であるかどうかを示します。デフォルトでは無効になっています。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: すべてのポートに対して出力側の LLDP 通知から、システム名 TLV を除外するには

```
# config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

#
```

3.6.12 config lldp ports dot1_tlv_pvid

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.1 準拠のポート vlan ID TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> all > dot1_tlv_pvid < enable disable >
説明	この TLV のオプションのデータタイプは、IEEE 802.1 準拠のポート VLAN TLV 送信が指定した LLDP 送信が可能なポートに許可されるかどうかを決定します。
パラメーター	<p><portlist> - 設定するポート範囲を指定します。</p> <p>all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。</p> <p>dot1_tlv_pvid - この TLV のオプションのデータタイプは、IEEE 802.1 準拠のポート VLAN ID TLV 送信が指定した LLDP 送信が可能なポートに許可されるかどうかを決定します。デフォルトでは無効になっています。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートに対して出力側の LLDP 通知から VLAN 名 TLV を設定するには

```
# config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

#
```

3.6.13 config lldp ports dot1_tlv_protocol_vid

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.1 準拠のポート ID TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> all > dot1_tlv_protocol_vid < vlan < all < vlan_name 32 > > vlanid <vlanid_list> > < enable disable >
説明	この TLV のオプションのデータタイプは、対応するローカルシステムのポート ID TLV のインスタンスがポートに送信されるかどうかを示します。ポート ID TLV は、ステーションにネットワークの操作に重要なプロトコルを通知する方法を提供します。スパニングツリープロトコル、リンクアグリゲーション制御プロトコルおよび多数のベンダが所有するプロトコルのバリエーションは、ネットワークのトポロジーと接続性を保持する責任があります。指定ポートで EAPOL、GVRP、STP (MSTP を含む)、および LACP プロトコル ID TLV を有効にすると、通知が有効になり、このポート ID TLV は通知を送信します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 dot1_tlv_protocol_vid - この TLV のオプションのデータタイプは、IEEE 802.1 準拠のポート ID TLV 送信が指定した LLDP 送信が可能なポートに許可されるかどうかを決定します。デフォルトでは無効になっています。 vlanid_list - このコマンド用に設定される VID のリスト。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートに対して出力側の LLDP 通知から VLAN 名 TLV を設定するには

```
#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

#
```

3.6.14 config lldp ports dot1_tlv_vlan_name

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.1 準拠の VLAN 名 TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> all > dot1_tlv_vlan_name < vlan < all <vlan_name 32> > vlanid <vidlist> > < enable disable >
説明	この TLV のオプションのデータタイプは、対応するローカルシステムの VLAN 名のインスタンスがポートに送信されるかどうかを示します。ポートが複数の VLAN に対応付けされた場合、有効な VLAN ID が通知されます。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 dot1_tlv_vlan_name - この TLV のオプションのデータタイプは、対応するローカルシステムの VLAN 名のインスタンスがポートに送信されるかどうかを示します。ポートが複数の VLAN に対応付けされた場合、有効な VLAN ID が通知されます。デフォルトでは無効になっています。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: すべてのポートに対して出力側の LLDP 通知から VLAN 名 TLV を設定するには

```
# config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable

Success.

#
```

3.6.15 config lldp ports dot1_tlv_protocol_identity

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.1 準拠のプロトコルアイデンティティ TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> all > dot1_tlv_protocol_identity < all [eapol lacp gvrp stp] > <enable disable>
説明	この TLV のオプションのデータタイプは、対応するローカルシステムのプロトコルアイデンティティのインスタンスがポートに送信されるかどうかを示します。プロトコルアイデンティティ TLV は、ステーションにネットワークの操作に重要なプロトコルを通知する方法を提供します。スパニングツリープロトコル、リンクアグリゲーション制御プロトコルおよび多数のベンダが所有するプロトコルのバリエーションは、ネットワークのトポロジーと接続性を保持する責任があります。指定ポートで EAPOL、GVRP、STP (MSTP を含む)、および LACP プロトコルアイデンティティを有効にすると、通知が有効になり、このプロトコルアイデンティティは通知を送信します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。

パラメーター	dot1_tlv_protocol_identity - この TLV のオプションのデータタイプは、対応するローカルシステムのプロトコルアイデンティティのインスタンスがポートに送信されるかどうかを示します。プロトコルアイデンティティ TLV は、ステーションにネットワークの操作に重要なプロトコルを通知する方法を提供します。スパニングツリープロトコル、リンクアグリゲーション制御プロトコルおよび多数のベンダが所有するプロトコルのバリエーションは、ネットワークのトポロジーと接続性を保持する責任があります。指定ポートで EAPOL、GVRP、STP (MSTP を含む)、および LACP プロトコルアイデンティティを有効にすると、通知が有効になり、このプロトコルアイデンティティは通知を送信します。デフォルトでは無効になっています。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: すべてのポートに対して出力側の LLDP 通知からプロトコルアイデンティティ TLV を設定するには

```
# config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success

#
```

3.6.16 config lldp ports dot3_tlvs

目的	各ポートまたはポートグループが、出力側の LLDP 通知から 1 つ以上の IEEE 802.3 準拠の組織固有の TLV データタイプを除外するように設定します。
構文	config lldp ports < <portlist> all > dot3_tlvs < all [mac_phy_configuration_status link_aggregation power_via_mdi maximum_frame_size] > < enable disable >
説明	この TLV のオプションの各 TLV を個別に有効にすることができます。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。 mac_phy_configuration_status - この TLV のオプションデータタイプは、LLDP エージェントが'MAC/PHY configuration/status TLV'を送信する必要があることを示します。このタイプは、IEEE 802.3 リンクの 2 つの終端が異なるデュプレックスおよび/または速度設定で、何らかの限定的なネットワークの接続性を確立することが可能であることを示しています。詳しく説明すると、情報はポートがオートネゴシエーション機能をサポートしているかどうか、機能が有効であるかどうか、自動通知機能、および操作可能な MAU タイプを含みます。デフォルトでは無効になっています。

パラメーター	<p>link_aggregation - この TLV のオプションデータタイプは、LLDP エージェントが「Link Aggregation TLV」を送信する必要があることを示します。このタイプは IEEE 802.3 MAC における現在のリンクアグリゲーションステータスを示します。情報は、ポートがリンクアグリゲーションできるかどうか、ポートが集約した1つのリンクにまとめられるかどうか、および束ねられたポートの ID を持っている必要があります。デフォルトでは無効になっています。</p> <p>power_via_mdi - この TLV のオプションデータタイプは、LLDP エージェントが「Power via MDI TLV」を送信する必要があることを示します。3つの IEEE 802.3 PMD インプリメンテーション (10BASE-T、100BASE-TX および 1000BASE-T) により、接続されている電力未供給システムに対してリンクを介して電力が供給されます。MDI TLV 経由の電力供給により、ネットワーク管理が通知を行い、送信する IEEE 802.3 LAN ステーション MDI 電力のサポート機能を検出します。デフォルトでは無効になっています。</p> <p>maximum_frame_size - この TLV のオプションデータタイプは、LLDP エージェントが「Maximum-frame-size TLV」を送信する必要があることを示します。デフォルトでは無効になっています。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートに対して出力側の LLDP 通知から MAC/PHY 設定/ステータスを設定するには

```
#config lldp ports all dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

#
```

3.6.17 config lldp forward_message

目的	LLDP が無効の際の LLDP DU パケットの転送を設定します。
構文	config lldp forward_message < enable disable >
説明	LLDP を無効にして、LLDP forward message を有効にしたとき、受信された LLDP DU パケットを転送します。デフォルトでは無効になっています。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:LLDP forward LLDPDU を設定するには

```
# config lldp forward_message enable
Command: config lldp forward_message enable

Success.

#
```


3.6.18 show lldp

目的	本コマンドは、スイッチの通常の LLDP 設定ステータスを表示します。
構文	show lldp
説明	本コマンドは、スイッチの通常の LLDP 設定ステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:LLDP 設定ステータスを表示するには

```
# show lldp
Command: show lldp

LLDP system information
  Chassis Id Subtype      : MAC Address
  Chassis Id              : 00-40-66-00-00-01
  System Name             :
  System Description      : Fast Ethernet Switch
  System Capabilities     : Repeater, Bridge,

LLDP Configurations
  LLDP Status             : Disable
  LLDP Forward Status    : Disable
  Message Tx Interval    : 30
  Message Tx Hold Multiplier : 4
  ReInit delay           : 2
  Tx Delay                : 2
  Notification Interval  : 5

#
```

3.6.19 show lldp mgt_addr

目的	LLDP の管理アドレス情報を表示します。
構文	show lldp mgt_addr [ipv4 <ipaddr>]
説明	本コマンドは、LLDP の管理アドレス情報を表示します。
パラメーター	ipv4 - IPV4 の IP アドレス。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: 管理アドレス情報を表示するには

```
#show lldp mgt_addr ipv4 192.168.254.10
Command: show lldp mgt_addr ipv4 192.168.254.10

Address 1 :
-----
Subtype                : IPv4
Address                : 192.168.254.10
IF Type                : Unknown
OID                    : 1.3.6.1.4.1.278.1.35.103
Advertising Ports      :

#
```

3.6.20 show lldp ports

目的	LLDP 通知オプションをポート設定ごとに表示します。
構文	show lldp ports [<portlist>]
説明	本コマンドは、LLDP 通知オプションをポート設定ごとに表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。 ポートリストを指定しない場合、すべてのポートの情報が表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ポートの TLV オプション設定ごとに LLDP を表示するには

```
# show lldp ports 1
Command: show lldp ports 1

Port ID                : 1
-----
Admin Status           : TX_and_RX
Notification Status    : Disable
Advertised TLVs Option :
  Port Description      Disable
  System Name           Disable
  System Description    Disable
  System Capabilities   Disable
  Enabled Management Address
    (NONE.)
  Port VLAN ID          Disable
  Enabled Port_and_protocol_VLAN_ID
    (NONE)
  Enabled VLAN Name     (NONE.)
  Enabled protocol_identity
```

(NONE.)	
MAC/PHY Configuration/Status	Disable
Power Via MDI	Disable
Link Aggregation	Disable
Maximum Frame Size	Disable
#	

3.6.21 show lldp local_ports

目的	出力側の LLDP 通知を組み込むためにポートごとの現在の情報を表示します。
構文	show lldp local_ports [<portlist>] [mode < brief normal detailed >]
説明	本コマンドは、出力側の LLDP 通知を組み込むためにポートごとの現在の情報を表示します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 ポートリストを指定しない場合、すべてのポートの情報が表示されます。 brief - brief(簡易)モードにおける情報を表示します。 normal - normal(通常)モードの情報を表示します。これはデフォルト値の表示モードです。 detailed - detailed(詳細)モードにおける情報を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: 各ポートの外出力側 LLDP 通知を detailed(詳細) モードで表示するには

```
# show lldp local_ports 1 mode detailed
Command: show lldp local_ports 1 mode detailed

Port ID : 1
-----
Port Id Subtype           : Local
Port Id                   : 1/1
Port Description          : Hitachi Cable APLFM108GTSS R1.07 Port 1
Port VLAN ID              : 1
Management Address Count : 1
    Subtype                : IPv4
    Address                 : 192.168.254.10
    IF Type                 : Unknown
    OID                     : 1.3.6.1.4.1.278.1.35.103

PPVID Entries Count      : 0
(NONE)
VLAN Name Entries Count  : 1
    Entry 1 :
        Vlan ID           : 1
        Vlan Name         : default

Protocol Identity Entries Count : 0
```

```

(NONE)
MAC/PHY Configuration/Status      :
  Auto-negotiation Support        : Supported
  Auto-negotiation Enabled        : Enabled
  Auto-negotiation Advertised Capability : 6c00(hex)
  Auto-negotiation Operational MAU Type : 0000(hex)

Power Via MDI                      : Not Supported

Link Aggregation                   :
  Aggregation Capability           : Aggregated
  Aggregation Status              : Not Currently In Aggregation
  Aggregation Port ID             : 1

Maximum Frame Size                 : 1536

#

```

使用例: 特定ポートの出力側 LLDP 通知を normal (通常) モードで表示するには

```

#show lldp local_ports 1 mode normal
Command: show lldp local_ports 1 mode normal

Port ID : 1
-----
Port Id Subtype                : Local
Port Id                        : 1/1
Port Description                : Hitachi Cable APLFM108GTSS R1.01 Port 1
Port VLAN ID                   : 1
Management Address Count       : 1
PPVID Entries Count            : 0
VLAN Name Entries Count        : 1
Protocol Identity Entries Count : 0
MAC/PHY Configuration/Status   : (See detail)
Power Via MDI                  : (See detail)
Link Aggregation               : (See detail)
Maximum Frame Size             : 1536

#

```

使用例: 特定ポートの出力側 LLDP 通知を brief (簡易) モードで表示するには

```

#show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief

Port ID : 1
-----

```

Port Id Subtype	: Local
Port Id	: 1/1
Port Description	: Hitachi Cable APLFM108GTSS R1.01 Port 1

#

3.6.22 show lldp remote_ports

目的	ネイバーから得た情報を表示します。
構文	show lldp remote_ports [<portlist>] [mode < brief normal detailed >]
説明	本コマンドは、ネイバーのパラメーターから得た情報を表示します。 32 個の VLAN 名エントリーと 10 個の管理アドレスエントリーを受信できます。
パラメーター	<portlist> - 設定するポート範囲を指定します。 ポートリストを指定しない場合、すべてのポートの情報が表示されます。 brief - brief(簡易)モードにおける情報を表示します。 normal - normal(通常)モードの情報を表示します。これはデフォルト値の表示モードです。 detailed - detailed(詳細)モードにおける情報を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: リモートテーブルエントリーを brief (簡易) モードで表示するには

```
#show lldp remote_ports 1 mode brief
Command: show lldp remote_ports 1 mode brief

Port ID : 1
-----
Remote Entities Count : 1
Entity 1
  Chassis Id Subtype      : MAC Address
  Chassis Id              : 00-40-66-10-27-00
  Port Id Subtype        : Local
  Port ID                 : 1/1
  Port Description        :

#
```

使用例: リモートテーブルエントリーを normal (通常) モードで表示するには

```
# show lldp remote_ports ports 1 mode normal
Command: show lldp remote_ports ports 1 mode normal

Port ID : 1
-----
Remote Entities Count : 1
Entity 1
  Chassis Id Subtype      : MAC Address
  Chassis Id              : 00-40-66-10-27-00
  Port Id Subtype        : Local
  Port ID                 : 1/1
  Port Description        :
  System Name             :
```

```

System Description          :
System Capabilities         :
Management Address Count   : 0
Port VLAN ID               : 0
PPVID Entries Count        : 0
VLAN Name Entries Count    : 0
Protocol ID Entries Count  : 0
MAC/PHY Configuration/Status : (None)
Power Via MDI               : (None)
Link Aggregation           : (None)
Maximum Frame Size         : 0
Unknown TLVs Count         : 0

```

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

使用例: リモートテーブルエントリを detailed (詳細) モードで表示するには

```

# show lldp remote_ports 1 mode detailed
Command: show lldp remote_ports 1 mode detailed

Port ID : 1
-----
Remote Entities Count : 1
Entity 1
  Chassis Id Subtype      : MAC Address
  Chassis Id              : 00-40-66-10-27-00
  Port Id Subtype         : Local
  Port ID                 : 1/1
  Port Description        :
  System Name             :
  System Description      :
  System Capabilities     :
  Management Address Count : 0
  (None)

  Port PVID               : 0
  PPVID Entries Count     : 0
  (None)

  VLAN Name Entries Count : 0
  (None)

```

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

3.6.23 show lldp statistics

目的	システムの LLDP 統計情報を表示します。
構文	show lldp statistics
説明	本コマンドは、スイッチのネイバーデバイスのアクティビティの概要を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: グローバル統計情報を表示するには

```
# show lldp statistics
Command: show lldp statistics

Last Change Time      : 6094
Number of Table Insert : 1
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0

#
```

3.6.24 show lldp statistics ports

目的	ポートの LLDP 統計情報を表示します。
構文	show lldp statistics ports [<portlist>]
説明	本コマンドは、ポートごとの LLDP 統計を表示します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 ポートリストを指定しない場合、すべてのポートの情報が表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート1の統計情報を表示するには

```
# show lldp statistics ports 1
```

```
Command: show lldp statistics ports 1
```

```
Port ID: 1
```

```
-----  
lldpStatsTxPortFramesTotal      : 27  
lldpStatsRxPortFramesDiscardedTotal : 0  
lldpStatsRxPortFramesErrors     : 0  
lldpStatsRxPortFramesTotal      : 27  
lldpStatsRxPortTLVsDiscardedTotal : 0  
lldpStatsRxPortTLVsUnrecognizedTotal : 0  
lldpStatsRxPortAgeoutsTotal     : 0
```

```
#
```

3.7 バナーとプロンプトの編集コマンド

3.7.1 config command_prompt

目的	コマンドプロンプトを設定します。
構文	config command_prompt < <string 16> username default >
説明	本コマンドを使用してコマンドプロンプトを変更できます。
パラメーター	string 16 - 半角英数字 16 文字以内の新しい名前を入力することで、コマンドプロンプトを変更できます。 username - コマンドプロンプトをログインユーザー名に変更します。 default - 工場出荷時コマンドプロンプトにリセットします。
制限事項	管理者アカウントのみ本コマンドを実行できます。 他の制限は以下の通りです。 「reset」コマンドが実行されると、変更されたコマンドプロンプトは変更された状態を維持します。ただし、「reset config/reset system」コマンドが実行されると、コマンドプロンプトは工場出荷時のバナーにリセットされます。
対応バージョン	1.00.00 以降

使用例: コマンドプロンプトを「HCL」に変更するには

```
#config command_prompt HCL
Command: config command_prompt HCL

Success.

HCL#
```

3.7.2 config greeting_message

目的	ログインバナーを設定します。
構文	config greeting_message [default]
説明	本コマンドは、ログインバナーを設定します。
パラメーター	default - default を入力すると、バナーコマンドを変更し、バナーは工場出荷時設定のバナーにリセットされます。 バナーエディタを開くには、「config greeting_message」コマンドの後に、<Enter>をクリックします。情報を入力し、バナーエディタに記述されているコマンドを使用してバナーを表示します。 Quit without save: Ctrl+C Save and quit: Ctrl+W Move cursor: Left/Right/Up/Down Delete line: Ctrl+D Erase all setting: Ctrl+X Reload original setting: Ctrl+L

制限事項	<p>管理者アカウントのみ本コマンドを実行できます。 他の制限は以下の通りです。 「reset」コマンドが実行されると、変更されたバナーは変更された状態を維持します。ただし、「reset config/reset system」コマンドが実行されると、変更されたバナーは工場出荷時のバナーにリセットされます。 バナーの最大容量は、6行*80文字/各行です。(1行に80文字で6行まで)。 Ctrl+W はDRAMに変更されたバナーを保存するだけです。「save config/save all」コマンドをタイプしてフラッシュメモリーに保存する必要があります。 閾値内でのみ有効です。</p>
対応バージョン	1.00.00以降

使用例:バナーを編集するには

```
#config greeting_message
Command: config greeting_message

Greeting Messages Editor
=====

                ApresiaLightFM108GT-SS Fast Ethernet Switch
                  Command Line Interface

                        Firmware: 1.08.00
                Copyright(C) 2014 Hitachi Metals, Ltd. All rights reserved.
=====

<Function Key>          <Control Key>
Ctrl+C      Quit without save    left/right/
Ctrl+W      Save and quit        up/down   Move cursor
                                           Ctrl+D     Delete line
                                           Ctrl+X     Erase all setting
                                           Ctrl+L     Reload original setting
=====
```

3.7.3 show greeting_message

目的	スイッチに現在設定されているログインバナーを参照します。
構文	show greeting_message
説明	本コマンドは、スイッチに現在設定されているのログインバナーを参照します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00以降

使用例:現在、設定されているログインバナーを参照するには

```
#show greeting_message
```

```
Command: show greeting_message
```

```
=====
```

```
                ApresiaLightFM108GT-SS Fast Ethernet Switch
```

```
                Command Line Interface
```

```
                Firmware: 1.08.00
```

```
                Copyright(C) 2014 Hitachi Metals, Ltd. All rights reserved.
```

```
=====
```

```
#
```

3.8 ネットワーク管理 (SNMP) コマンド

本スイッチは、Simple Network Management Protocol (SNMP) バージョン 1、2c および 3 をサポートしています。ユーザーは、SNMP のどのバージョンでスイッチを監視および制御するか指定できます。SNMP の 3 つのバージョンは、管理ステーションとネットワークデバイス間に提供するセキュリティーレベルが異なります。SNMP バージョンのセキュリティー機能は以下の表の通りです。

SNMP バージョン	認証方法	説明
v1	コミュニティ文字列	コミュニティ文字列は認証に使用されず- NoAuthNoPriv
v2c	コミュニティ文字列	コミュニティ文字列は認証に使用されず- NoAuthNoPriv
v3	ユーザー名	ユーザー名は認証に使用されず- NoAuthNoPriv
v3	MD5 または SHA	認証は HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて行われます- AuthNoPriv
v3	MD5 DES または SHA DES	認証は HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて行われます- AuthPriv DES 56 ビット暗号方式が CBC-DES(DES-56)標準規格に基づいて追加されます

3.8.1 create snmp user

目的	新しい SNMP ユーザーを作成し、作成した SNMP グループにユーザーを追加します。
構文	<code>create snmp user <SNMP_name 32> <groupname 32> [encrypted < by_password auth <md5 <auth_password 8-16> sha <auth_password 8-20> > priv < none des <priv_password 8-16> > by_key auth < md5 <auth_key 32-32> sha <auth_key 40-40> > priv < none des <priv_key 32-32> > >]</code>
説明	本コマンドは、新しい SNMP ユーザーを作成し、作成した SNMP グループにユーザーを追加します。SNMP は以下の項目を保証します。 メッセージの保全- パケットが送信中に変更されていないことを保証します。 認証- SNMP メッセージが有効な送信元から来ているかどうかを判断します。 暗号化- 未認証の送信元に参照されることを防ぐために、メッセージの内容にスクランブルをかけます。
パラメーター	<SNMP_name 32> - 新しい SNMP ユーザーを識別する半角英数字 32 文字以内の名前。 <groupname 32> - 新しい SNMP ユーザーが対応付けされる SNMP グループを識別する半角英数字 32 文字以内の名前。 encrypted - SNMP を使用した認証のタイプを選択します。ユーザーは以下の選択ができます。 by_password - 認証とプライバシーのために SNMP ユーザーにパスワードを入力するように要求します。パスワードは、以下で「auth_password」を指定することによって定義されます。この方式を推奨します。 by_key - 認証とプライバシーのために SNMP ユーザーに暗号化キーを入力するように要求します。キーは、16 進形式により指定することによって定義されます。この方式を推奨します。

パラメーター	<p>auth - SNMP ユーザーを認証するために使用される認証アルゴリズムのタイプを選択します。以下の選択があります。</p> <p>md5 - HMAC-MD5-96 認証レベルを指定します。md5 は、以下の1つを入力することによって、利用されます。</p> <p><auth password 8-16> - ホストに対するパケットが受信できるようエージェントを認可するために使用される半角英数字 8 ~ 16 文字列。</p> <p><auth_key 32-32> - ホストに対するパケットが受信できるようエージェントを認可するために使用される半角英数字 32 文字の文字列を 16 進数形式で入力します。</p> <p>sha - HMAC-SHA-96 認証レベルを使用します。</p> <p><auth password 8-20> - ホストに対するパケットが受信できるようエージェントを認可するために使用される半角英数字 8 ~ 20 文字の文字列。</p> <p><auth_key 40-40> - ホストに対するパケットが受信できるようエージェントを認可するために使用される半角英数字 40 文字のキーを 16 進数形式で入力します。</p> <p>priv - priv (プライバシー)パラメーターを追加すると、より高いセキュリティのために認証アルゴリズムに加えて、暗号化も可能になります。ユーザーは以下の選択ができます。</p> <p>des - 本パラメーターを追加すると、56 ビットの暗号化のための DES-56 標準の使用が可能となります。</p> <p><priv_password 8-16> - ホストがエージェントに送信するメッセージの内容を暗号化するために使用する半角英数字 8 ~ 16 文字の文字列。</p> <p><priv_key 32-32> - ホストがエージェントに送信するメッセージの内容を暗号化するために使用される半角英数字 32 文字のキーを 16 進数形式で入力します。</p> <p>none - 本パラメーターを追加すると、暗号化を行いません。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチの SNMP ユーザーを作成するには

```
#create snmp user HCL default encrypted by_password auth md5 knickerbockers priv none
Command: create snmp user HCL default encrypted by_password auth md5 knickerbockers priv none

Success.

#
```

3.8.2 delete snmp user

目的	SNMP グループから SNMP ユーザーを削除し、また対応付けされた SNMP グループも削除します。
構文	delete snmp user <SNMP_name 32>
説明	本コマンドは、SNMP グループから SNMP ユーザーを削除し、また対応付けされた SNMP グループも削除します。
パラメーター	<SNMP_name 32> - 削除される SNMP ユーザーを識別する半角英数字 32 文字以内の文字列。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチに入力済みの SNMP ユーザーを削除するには

```
#delete snmp user HCL
Command: delete snmp user HCL

Success.

#
```

3.8.3 show snmp user

目的	SNMP グループのユーザー名テーブル内の各 SNMP ユーザー名に関する情報を表示します。
構文	show snmp user
説明	本コマンドは、SNMP グループのユーザー名テーブル内の各 SNMP ユーザー名に関する情報を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに現在設定されている SNMP ユーザーを表示するには

```
#show snmp user
Command: show snmp user

Username          Group Name        SNMP Version Auth-Protocol PrivProtocol
-----
initial          initial          V3             None           None

Total Entries: 1

#
```

3.8.4 create snmp view

目的	MIB オブジェクトと SNMP マネージャーのアクセスを制限するために、コミュニティ文字列にビューを割り当てます。
構文	create snmp view <view_name 32> <oid> view_type < included excluded >
説明	本コマンドは、MIB オブジェクトと SNMP マネージャーのアクセスを制限するために、コミュニティ文字列にビューを割り当てます。
パラメーター	<p><view_name 32> - 作成される SNMP ビューを識別する半角英数字 32 文字以内の文字列。</p> <p><oid> - SNMP マネージャーによってアクセス可能な範囲であるかを指定されるオブジェクトツリー (MIB ツリー) を識別するオブジェクト ID。</p> <p>view type - 以下のビュータイプを選択します。</p> <p>included - SNMP マネージャーがアクセスできるオブジェクトのリストにこのオブジェクトを含めます。</p> <p>excluded - SNMP マネージャーがアクセスできるオブジェクトのリストからこのオブジェクトを除外します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。

使用例: SNMP ビューを作成するには

```
#create snmp view HCL 1.3.6 view_type included
Command: create snmp view HCL 1.3.6 view_type included

Success.

#
```

3.8.5 delete snmp view

目的	スイッチに作成済みの SNMP ビューエントリを削除します。
構文	delete snmp view <view_name 32> < all <oid> >
説明	本コマンドは、スイッチに作成済みの SNMP ビューエントリを削除します。
パラメーター	<p><view_name 32> - 作成される SNMP ビューを識別する半角英数字 32 文字以内の文字列。</p> <p>all - 削除するスイッチの SNMP ビューすべてを指定します。</p> <p><oid> - スイッチから削除されるオブジェクトツリー (MIB ツリー) を識別するオブジェクト ID。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:設定済みの SNMP ビューをスイッチから削除するには

```
#delete snmp view HCL all
Command: delete snmp view HCL all

Success.

#
```

3.8.6 show snmp view

目的	スイッチに作成済みの SNMP ビューを表示します。
構文	show snmp view [<view_name 32>]
説明	本コマンドは、スイッチに作成済みの SNMP ビューエントリを表示します。
パラメーター	<view_name 32> - 表示される SNMP ビューを識別する半角英数字 32 文字以内の文字列。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:SNMP ビュー設定を表示するには

```
#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name          Subtree              View Type
-----
restricted         1.3.6.1.2.1.1       Included
restricted         1.3.6.1.2.1.11      Included
restricted         1.3.6.1.6.3.10.2.1  Included
restricted         1.3.6.1.6.3.11.2.1  Included
restricted         1.3.6.1.6.3.15.1.1  Included
CommunityView     1                    Included
CommunityView     1.3.6.1.6.3          Excluded
CommunityView     1.3.6.1.6.3.1       Included
Total Entries   : 8

#
```

3.8.7 create snmp community

目的	SNMP マネージャーとエージェントとの関係を定義するために SNMP コミュニティの文字列を作成します。コミュニティ文字列は、スイッチ上のエージェントへのアクセスを行う際のパスワードのような役割をします。以下の特性はコミュニティ文字列に対応付けできます。 SNMP コミュニティにアクセス可能な全 MIB オブジェクトのサブセットを定義する MIB ビュー。 SNMP コミュニティにアクセス可能な MIB オブジェクトには、「read_write」(読み書き可能) または「read_only」(読み出しのみ) レベルがあります。
構文	create snmp community <community_string 32> view <view_name 32> < read_only read_write >
説明	本コマンドは、SNMP コミュニティ文字列を作成し、このコミュニティ文字列にアクセス制限を行う文字列を割り当てます
パラメーター	<community_string 32> - SNMP コミュニティのメンバーを識別する 32 文字までの半角英数文字列。この文字列は、リモートの SNMP マネージャーが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。 view <view_name 32> - リモート SNMP マネージャーがスイッチにアクセスできる MIB オブジェクトのグループの識別に使用される 32 文字までの半角英数文字列。 read_only - 本コマンドで作成されたコミュニティ文字列を使用して、SNMP コミュニティのメンバーはスイッチの MIB コンテンツを読み出しのみできます。 read_write - 本コマンドで作成されたコミュニティ文字列を使用して、SNMP コミュニティメンバーはスイッチの MIB コンテンツを読み書きできます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP コミュニティ文字列「HCL」を作成するには

```
#create snmp community HCL view ReadView read_write
Command: create snmp community HCL view ReadView read_write

Success.

#
```



工場出荷時の設定状態においては、コミュニティ名が一致する全ての 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、delete snmp community 設定を行なう必要があります。

3.8.8 delete snmp community

目的	スイッチから特定の SNMP コミュニティ文字列を削除します。
構文	delete snmp community <community_string 32>
説明	本コマンドは、スイッチから定義済みの SNMP コミュニティ文字列を削除します。
パラメーター	<community_string 32> - SNMP コミュニティのメンバを識別する 32 文字までの半角英数文字列。この文字列は、リモートの SNMP マネージャーが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP コミュニティ文字列「HCL」を削除するには

```
#delete snmp community HCL
Command: delete snmp community HCL

Success.

#
```

3.8.9 show snmp community

目的	スイッチに設定されている SNMP コミュニティ文字列を表示します。
構文	show snmp community [<community_string 32>]
説明	本コマンドは、スイッチに設定されている SNMP コミュニティ文字列を表示します。
パラメーター	<community_string 32> - SNMP コミュニティのメンバを識別する 32 文字までの半角英数文字列。この文字列は、リモートの SNMP マネージャーが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:現在入力した SNMP コミュニティ文字列を表示するには

```
#show snmp community
Command: show snmp community

SNMP Community Table

Community Name      View Name           Access Right
-----
private             CommunityView       read_write
public              CommunityView       read_only
HCL                 ReadView            read_write

Total Entries: 3

#
```

3.8.10 config snmp engineID

目的	スイッチの SNMP エンジンの識別子を設定します。
構文	config snmp engineID <snmp_engineID 10-64>
説明	本コマンドは、スイッチの SNMP エンジンの識別子を設定します。
パラメーター	<snmp_engineID 10-64> - スwitchの SNMP エンジンを指定する半角英数字の文字列。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの SNMP engineID に「0035636666」を付与するには

```
#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

#
```

3.8.11 show snmp engineID

目的	スイッチの SNMP エンジンの識別子を表示します。
構文	show snmp engineID
説明	本コマンドは、スイッチの SNMP エンジンの識別子を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチの SNMP engineID を表示するには

```
#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 80000116030040664599a6

#
```

3.8.12 create snmp group

目的	新しい SNMP グループまたは SNMP ビューに SNMP ユーザーをマッピングするテーブルを作成します。
構文	create snmp group <groupname 32> < v1 v2c v3 < noauth_nopriv auth_nopriv auth_priv > > < read_view <view_name 32> write_view <view_name 32> notify_view <view_name 32> >
説明	本コマンドは、SNMP ビューに SNMP ユーザーをマッピングする新しい SNMP グループまたはテーブルを作成します。
パラメーター	<p><groupname 32> - 新しい SNMP ユーザーが対応付けされる SNMP グループを識別する半角英数字 32 文字以内の名前。</p> <p>v1 - SNMP バージョン 1 を使用する場合に指定します。 Simple Network Management Protocol (SNMP) バージョン 1 は、モニタする手段と制御ネットワークデバイスを提供するネットワーク管理プロトコルです。</p> <p>v2c- SNMP バージョン 2 を使用する場合に指定します。 SNMP v2c は、ネットワークマネジメント管理を中央に集結して、提供します。 SMI (Structure of Management Information) およびセキュリティー機能において強化されています。</p> <p>v3 - SNMP バージョン 3 を使用する場合に指定します。 SNMP v3 は、ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。 SNMP v3 以下のパラメーターを追加します。</p> <p>メッセージの保全- パケットが送信中に変更されていないことを保証します。</p> <p>認証- SNMP メッセージが有効な送信元から来ているかどうかを判断します。</p> <p>暗号化- 未認証の送信元に参照されることを防ぐために、メッセージの内容にスクランブルをかけます。</p> <p>noauth_nopriv - スイッチとリモート SNMP マネージャー間に送信されるパケットには許可も暗号化もありません。</p> <p>auth_nopriv - スイッチとリモート SNMP マネージャー間には認証は必要ですが、送信パケットには暗号化はありません。</p> <p>auth_priv - スイッチとリモート SNMP マネージャー間には認証と送信パケットの暗号化が必要です。</p> <p>read_view - 作成された SNMP グループが、SNMP メッセージを要求する場合に指定します。</p> <p>write_view - 作成された SNMP グループに、書き込み権を持たせる場合に指定します。</p> <p>notify_view - 作成された SNMP グループが、スイッチの SNMP エージェントによって生成された SNMP トラップメッセージを受信する場合に指定します。</p>

パラメーター	view <view_name 32> - リモート SNMP マネージャーがスイッチにアクセスできる MIB オブジェクトのグループの識別に使用される 32 文字までの半角英数字列。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP グループ名「HCL」を作成するには

```
#create snmp group HCL v3 noauth_nopriv read_view v1 write_view v1 notify_view v1
Command: create snmp group HCL v3 noauth_nopriv read_view v1 write_view v1 notify_view v1

Success.

#
```

3.8.13 delete snmp group

目的	スイッチから SNMP グループを削除します。
構文	delete snmp group <groupname 32>
説明	本コマンドは、スイッチから SNMP グループを削除します。
パラメーター	<groupname 32> - 新しい SNMP ユーザーが対応付けされる SNMP グループを識別する半角英数字 32 文字以内の名前。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:「HCL」という名前の SNMP グループを削除するには :

```
#delete snmp group HCL
Command: delete snmp group HCL

Success.

#
```

3.8.14 show snmp groups

目的	スイッチに現在設定されている SNMP グループのグループ名を表示します。また、各グループのセキュリティーモデル/レベルおよびステータスを表示します。
構文	show snmp groups
説明	本コマンドは、スイッチに現在設定されている SNMP グループのグループ名を表示します。また、各グループのセキュリティーモデル/レベルおよびステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに現在設定されている SNMP グループを表示するには

```
#show snmp groups
Command: show snmp groups
Vacm Access Table Settings

Group Name      : Group3
ReadView Name   : ReadView
WriteView Name  : WriteView
Notify View Name : NotifyView
Security Model  : SNMPv3
Security Level  : NoAuthNoPriv

Group Name      : Group4
ReadView Name   : ReadView
WriteView Name  : WriteView
Notify View Name : NotifyView
Security Model  : SNMPv3
Security Level  : authNoPriv

Group Name      : Group5
ReadView Name   : ReadView
WriteView Name  : WriteView
Notify View Name : NotifyView
Security Model  : SNMPv3
Security Level  : authNoPriv

Group Name      : initial
ReadView Name   : restricted
WriteView Name  :
Notify View Name : restricted
Security Model  : SNMPv3
Security Level  : NoAuthNoPriv

Group Name      : ReadGroup
ReadView Name   : CommunityView
WriteView Name  :
Notify View Name : CommunityView
Security Model  : SNMPv1
Security Level  : NoAuthNoPriv

Total Entries: 5
```

#

3.8.15 create snmp host

目的	スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を作成します。
構文	create snmp < host <ipaddr> > < v1 v2c v3 < noauth_nopriv auth_nopriv auth_priv > <auth_string 32>
説明	本コマンドは、スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を作成します。
パラメーター	<p><ipaddr> - SNMP トラップの送信先 IP アドレス。</p> <p>v1 - SNMP バージョン 1 を使用する場合に指定します。</p> <p>v2c- SNMP バージョン 2c を使用する場合に指定します。</p> <p>v3 - SNMP バージョン 3 を使用する場合に指定します。 SNMP v3 は、ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。 SNMP v3 以下のパラメーターを追加します。</p> <p>メッセージの保全- パケットが送信中に変更されていないことを保証します。</p> <p>認証- SNMP メッセージが有効な送信元から来ているかどうかを判断します。</p> <p>暗号化- 未認証の送信元に参照されることを防ぐために、メッセージの内容にスクランブルをかけます。</p> <p>noauth_nopriv - スイッチとリモート SNMP マネージャー間に送信されるパケットは認証も暗号化も行いません。</p> <p>auth_nopriv - スイッチとリモート SNMP マネージャー間には認証は必要ですが、送信パケットには暗号化は行いません。</p> <p>auth_priv - スイッチとリモート SNMP マネージャー間および送信パケットは認証と暗号化が必要です。</p> <p><auth_string 32> - スイッチの SNMP エージェントをアクセスするためにリモート SNMP マネージャーを認証する半角英数文字列。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP メッセージを受信する SNMP ホストを作成するには

```
#create snmp host 10.48.74.100 v3 auth_priv public
Command: create snmp host 10.48.74.100 v3 auth_priv public

Success.

#
```

3.8.16 delete snmp host

目的	スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を削除します。
構文	delete snmp < host <ipaddr> >
説明	本コマンドは、スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を削除します。
パラメーター	<ipaddr> - SNMP トラップの送信先 IP アドレス。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP ホストエントリーを削除するには

```
#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

#
```

3.8.17 show snmp host

目的	スイッチの SNMP エージェントによって生成される SNMP トラップの送信先を表示します。
構文	show snmp host [<ipaddr>]
説明	本コマンドは、スイッチの SNMP エージェントによって生成される SNMP トラップの送信先として指定されたリモート SNMP マネージャーの IP アドレスおよび設定情報を表示します。
パラメーター	<ipaddr> - SNMP トラップの送信先 IP アドレス。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている SNMP ホストを表示するには

```
#show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version      Community Name / SNMPv3 User Name
-----
10.48.76.23     V3 noauthnopriv   initial
10.48.74.100    V2c                public

Total Entries  : 2

#
```

3.8.18 create trusted_host

目的	トラストホストを作成します。
構文	create trusted_host < <ipaddr> network <network_address> >
説明	本コマンドは、トラストホストを作成します。10 個までの IP アドレスが SNMP または Telnet ベースの管理ソフトウェア経由でスイッチを管理することができます。これらの IP アドレスは、マネジメント VLAN に所属する必要があります。IP アドレスが指定されない場合、ユーザーがユーザー名およびパスワードを知っていても、どの IP アドレスからもスイッチへのアクセスはできません。
パラメーター	<ipaddr> - 指定した IP アドレスのトラストホストを作成します。 <network_address> - 作成されるトラストホストの IP アドレスとネットワーク。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:トラストホストを作成するには

```
#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

#
```

使用例: トラストホストネットワークを作成するには

```
#create trusted_host network 10.48.0.0/16
Command: create trusted_host network 10.48.0.0/16

Success.

#
```

3.8.19 delete trusted_host

目的	上記「create trusted_host」コマンドで作成したトラストホストエントリーを削除します。
構文	delete trusted_host < ipaddr <ipaddr> network <network_address> all >
説明	本コマンドは、上記「create trusted_host」コマンドで作成したトラストホストエントリーを削除します。
パラメーター	<ipaddr> - トラストホストの IP アドレス。 <network_address> - トラストネットワークのネットワークアドレス。 all - トラストホストのすべてが削除されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: IP アドレス「10.48.74.121」のトラストホストを削除するには

```
#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

#
```

使用例: ネットワークアドレス「10.62.0.0/16」のトラストホストネットワークを削除するには

```
#delete trusted_host network 10.62.0.0/16
Command: delete trusted_host network 10.62.0.0/16

Success.

#
```

使用例: トラストホストエントリーを削除するには

```
#delete trusted_host all
Command: delete trusted_host all

Success.

#
```

3.8.20 show trusted_host

目的	「create trusted_host」コマンドでスイッチに作成したトラストホストのリストを表示します。
構文	show trusted_host
説明	本コマンドは、「create trusted_host」コマンドでスイッチに作成したトラストホストのリストを表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：トラストホストのリストを表示するには

```
#show trusted_host
Command: show trusted_host

Management Stations

IP Address/Netmask
-----
10.53.13.94/32

Total Entries: 1

#
```

3.8.21 enable snmp

目的	SNMP トラップを有効にします。
構文	enable snmp < authenticate_traps linkchange_traps traps login_trap login_fail_trap logout_trap >
説明	本コマンドは、スイッチの SNMP トラップを有効にします。
パラメーター	authenticate_traps - SNMP 認証トラップを有効にします。 linkchange_traps - SNMP リンクチェンジトラップを有効にします。 traps - SNMP トラップを有効にします。 login_trap - SNMP ログイントラップを有効にします。 login_fail_trap - SNMP ログインフェイルトラップを有効にします。 logout_trap - SNMP ログアウトトラップを有効にします。 ログイン、ログアウト、ログインフェイルの 3 種のトラップは、1.07 以降でサポートされます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチの SNMP トラップを有効にするには

```
#enable snmp traps
Command: enable snmp traps

Success.

#
```

使用例: スイッチの SNMP リンクチェンジトラップサポートを有効にするには

```
#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

#
```

使用例: SNMP 認証トラップサポートを有効にするには

```
#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

#
```

3.8.22 disable snmp

目的	スイッチの SNMP トラップを無効にします。
構文	disable snmp < authenticate_traps linkchange_traps traps login_trap login_fail_trap logout_trap >
説明	本コマンドは、スイッチの SNMP トラップを無効にします。
パラメーター	authenticate_traps - SNMP 認証トラップを無効にします。 linkchange_traps - SNMP リンクチェンジトラップを無効にします。 traps - SNMP トラップを無効にします。 login_trap - SNMP ログイントラップを無効にします。 login_fail_trap - SNMP ログインフェイルトラップを無効にします。 logout_trap - SNMP ログアウトトラップを無効にします。 ログイン、ログアウト、ログインフェイルの3種のトラップは、1.07以降でサポートされます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNMP 認証トラップを無効にするには

```
#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

#
```

使用例:SNMP リンクチェンジトラップを無効にするには

```
#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

#
```

使用例:SNMP トラップのスイッチからの送信を防ぐには

```
#disable snmp traps
Command: disable snmp traps

Success.

#
```

3.8.23 config snmp linkchange_traps ports

目的	リンクチェンジトラップの送信制御を設定します。
構文	config snmp linkchange_traps ports <all <portlist>> <enable disable >
説明	本コマンドは、リンクチェンジトラップの送信制御を設定します。各ポートごとに設定可能です。
パラメーター	all - すべてのポートを指定します。 <portlist> - ポート範囲を指定します。 enable - このポートのリンクチェンジトラップの送信を有効にします。 disable - このポートのリンクチェンジトラップの送信を無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1~4 の SNMP リンクチェンジトラップサポートを設定するには

<pre>#config snmp linkchange_traps ports 1-4 enable Command: config snmp linkchange_traps ports 1-4 enable Success. #</pre>

3.8.24 show snmp traps

目的	スイッチの SNMP トラップサポートを表示します。
構文	show snmp traps [linkchange_traps [ports <portlist>]]
説明	本コマンドは、スイッチに現在設定した SNMP トラップサポートステータスを表示します。 ログイン、ログアウト、ログインフェイルの 3 種のトラップステータスは 1.07 以降でサポートされます。
パラメーター	linkchange_traps - 現在の SNMP リンクチェンジトラップステータスを表示します。 <portlist> - SNMP トラップサポートを表示するポートのリストを指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:現在のSNMPトラップサポートを参照するには

```
#show snmp traps
Command: show snmp traps

SNMP Trap      : Enabled
Authenticate Traps : Enabled
Linkchange Traps : Enabled
Login Trap     : Disabled
Logout Trap    : Disabled
Login Fail Trap : Disabled

#
```

使用例:現在のリンクチェンジSNMPトラップステータスを参照するには

```
#show snmp traps linkchange_traps
Command: show snmp traps linkchange_traps

Linkchange Traps : Enabled
Port 1: Enabled
Port 2: Enabled
Port 3: Enabled
Port 4: Enabled
Port 5: Enabled
Port 6: Enabled
Port 7: Enabled
Port 8: Enabled
Port 9: Enabled
Port 10: Enabled
Port 11: Enabled
Port 12: Enabled
Port 13: Enabled
Port 14: Enabled
Port 15: Enabled
Port 16: Enabled
Port 17: Enabled
Port 18: Enabled

#
```


3.8.25 config snmp system_contact

目的	スイッチを管理する連絡担当者名を入力します。
構文	config snmp system_contact [<sw_contact>]
説明	本コマンドは、スイッチを管理する連絡担当者を識別するために名前および/または他の情報を入力します。 最大 128 文字を使用できます。
パラメーター	<sw_contact> - 最大 128 文字を使用できます。 連絡担当者を指定しない場合は、NULL を使用できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチの連絡担当者に「HCL」を設定するには

<pre>#config snmp system_contact HCL Command: config snmp system_contact HCL Success. #</pre>

3.8.26 config snmp system_location

目的	スイッチの設置場所の説明を入力します。
構文	config snmp system_location [<sw_location>]
説明	本コマンドは、スイッチの設置場所の説明を入力します。 最大 128 文字を使用できます。
パラメーター	<sw_location> - 最大 128 文字を使用できます。 場所を指定しない場合は、NULL を使用できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 「5F」のスイッチ場所を設定するには

```
#config snmp system_location 5F
Command: config snmp system_location 5F

Success.

#
```

3.8.27 config snmp system_name

目的	スイッチの名前を設定します。
構文	config snmp system_name [<sw_name>]
説明	このコマンドは、スイッチの名前を設定します。
パラメーター	<sw_name> - 最大 128 文字を使用できます。名前を指定しない場合は、NULLを使用できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 「ApresiaLightFM108GT-SS」のスイッチ名を設定するには

```
#config snmp system_name ApresiaLightFM108GT-SS
Command: config snmp system_name ApresiaLightFM108GT-SS

Success.

#
```

3.8.28 enable rmon

目的	スイッチの RMON を有効にします。
構文	enable rmon
説明	本コマンドは、下記の「disable rmon」コマンドと共に使用して、スイッチのリモートモニタリング(RMON)を有効・無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: RMON を有効にするには

```
#enable rmon
Command: enable rmon

Success.

#
```

3.8.29 disable rmon

目的	スイッチの RMON を無効にします。
構文	disable rmon
説明	本コマンドは、上記の enable rmon コマンドと共に使用して、スイッチのリモートモニタリング(RMON)を有効・無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：RMON を無効にするには

```
#disable rmon
Command: disable rmon

Success.

#
```

3.9 ネットワーク監視コマンド

3.9.1 show packet ports

目的	スイッチが送受信したパケットに関する統計情報を表示します。
構文	show packet ports <portlist>
説明	<portlist>で指定されたポートごとに送受信されたパケットに関する統計情報を表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ポート 2 のパケット統計情報を表示するには

```
#show packet ports 2
Command: show packet ports 2

Port Number : 2
Frame Size      Frame Counts  Frames/sec    Frame Type    Total        Total/sec
-----
64              0             0             RX Bytes     0            0
65-127          0             0             RX Frames    0            0
128-255         0             0
256-511         0             0             TX Bytes     0            0
512-1023        0             0             TX Frames    0            0
1024-1518       0             0

Unicast RX      0             0
Multicast RX    0             0
Broadcast RX    0             0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

3.9.2 show error ports

目的	ポート毎のエラー統計情報を表示します。
構文	show error ports <portlist>
説明	本コマンドは、スイッチが指定ポートに対して収集した、パケットエラー統計情報を表示します。 なお、Drop Pkts カウンタについては、未対応のためカウントされません。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート3のエラー統計情報を表示するには

```
#show error ports 3
Command: show error ports 3

Port Number : 3

          RX Frames                                TX Frames
          -----                                -----
CRC Error    0                                Excessive Deferral  0
Undersize    0                                CRC Error            0
Oversize     0                                Late Collision       0
Fragment     0                                Excessive Collision  0
Jabber       0                                Single Collision     0
Drop Pkts    -                                Collision            0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

3.9.3 config utilization notify

目的	装置のCPUおよびメモリ使用率通知機能を設定します。
構文	config utilization notify <cpu dram> [state<enable disable>] threshold <20-100> [polling_interval <10-300> trap_state <enable disable> log_state <enable disable>]
説明	本コマンドは、装置のCPUおよびメモリ使用率通知を設定します。 CPU&DRAM使用率表示コマンドは、CPUおよびDRAMの使用状態を周期的に監視することにより指定閾値を超過した場合に、ログやトラップによりユーザーへ通知する機能です。
パラメーター	<cpu dram> - 使用率通知設定を指定します。 state<enable disable> - 閾値の監視を有効または無効で指定します。 threshold <20-100> - 通知する場合の閾値を20%から100%の範囲で指定します。この閾値を超えた場合、"OVERLOADING utilization status"のログを出力します。また、閾値を超えた状態から閾値より小さくなった場合、"NORMAL utilization status"のログを出力します。デフォルト値は100%です。 polling_interval <10-300> - 閾値の監視間隔を10秒から300秒で指定します。デフォルト値は60秒です。 trap_state <enable disable> - 閾値を超えた場合のSNMPトラップ出力を有効または無効で指定します。デフォルト値は無効(disable)です。 log_state <enable disable> - 閾値を超えた場合のシステムログ出力を有効または無効で指定します。デフォルト値は有効(enable)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.07.00以降

使用例: CPU 使用率通知を閾値 100%、ポーリング間隔 10 秒で設定するには

```
#config utilization notify cpu threshold 100 polling_interval 10
Command: config utilization notify cpu threshold 100 polling_interval 10

Success.

#
```

3.9.4 clear utilization

目的	装置の CPU および DRAM 使用率統計情報をクリアします。
構文	clear <cpu dram>
説明	本コマンドは、装置の CPU および DRAM 使用率統計情報をクリアします。
パラメーター	<cpu dram> - クリアする使用率統計情報を指定します。 cpu - CPU 使用率に関する情報をクリアします。 dram - DRAM 使用率に関する情報をクリアします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.07.00 以降

使用例: CPU 使用率統計情報をクリアするには

```
#clear utilization cpu
Command: clear utilization cpu

Success.

#
```

3.9.5 show utilization

目的	リアルタイムで使用率統計情報を表示します。
構文	show utilization <cpu dram flash ports [<portlist>] >
説明	本コマンドは、リアルタイムでスイッチの使用率統計情報を表示します。
パラメーター	cpu - このパラメーターを入力すると、スイッチの現在の CPU 使用率を表示します。 dram - このパラメーターを入力すると、スイッチの現在の DRAM 使用率を表示します。 flash - このパラメーターを入力すると、スイッチの現在のフラッシュ使用率を表示します。 ports - このパラメーターを入力すると、スイッチの現在のポート使用率を表示します。 <portlist> - 表示するポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:現在のCPU使用率を表示するには

```
#show utilization cpu
Command: show utilization cpu

CPU Utilization :
-----
Five Seconds - 11 %           One Minute - 11 %           Five Minutes - 10 %
Maximum      - 27 %           Minimum      - 0 %

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

使用例:現在のDRAM使用率を表示するには

```
#show utilization dram
Command: show utilization dram

DRAM Utilization :

Total DRAM      : 131,072   KB
Used DRAM       : 65,604    KB
Utilization     : 50%

Utilization(max) : 50 %
Utilization(min) : 50 %

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

使用例:現在のフラッシュメモリー使用率を表示するには

```
#show utilization flash
Command: show utilization flash

FLASH Memory Utilization :

Total FLASH     : 16,384    KB
Used FLASH      : 7,371     KB
Utilization     : 44%

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

使用例:ポート使用統計を表示するには

```
#show utilization ports
```

```
Command: show utilization ports
```

Port	TX/sec	RX/sec	Util	Port	TX/sec	RX/sec	Util
1	148810	148810	100	22	0	0	0
2	148810	148810	100	23	0	0	0
3	0	148810	50	24	0	0	0
4	0	0	0	25	0	0	0
5	0	0	0	26	0	0	0
6	0	0	0	27	0	0	0
7	0	37	1	28	0	0	0
8	0	0	0				
9	0	0	0				
10	0	0	0				
11	36	0	1				
12	0	0	0				
13	0	0	0				
14	0	0	0				
15	0	0	0				
16	0	0	0				
17	0	0	0				
18	0	0	0				
19	0	0	0				
20	0	0	0				
21	0	0	0				

```
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```



TX/sec、RX/sec の単位は packet/sec です。

Util は TX/sec、RX/sec それぞれの最大転送レートに対する割合を最大 50%とし、合計値を表示します。

3.9.6 show utilization notify

目的	CPU および DRAM 使用率通知機能の設定状態を表示します。
構文	show utilization notify <cpu dram>
説明	本コマンドは、CPU および DRAM 使用率通知機能の設定を表示します。
パラメーター	cpu - CPU 使用率通知機能に関する設定状態を表示します。 dram - DRAM 使用率通知機能に関する設定状態を表示します。
制限事項	なし。
対応バージョン	1.07.00 以降

使用例:現在の CPU 使用率通知機能の設定を表示するには

<pre>#show utilization notify cpu Command: show utilization notify cpu CPU Utilization Notify Information ----- Current Status : NORMAL State : Enabled Threshold : 100% Polling Interval : 10 sec Trap State : Disabled Log State : Enabled #</pre>

3.9.7 clear counters

目的	スイッチの統計カウンタをクリアします。
構文	clear counters [ports <portlist>]
説明	本コマンドは、スイッチが使用するカウンタをクリアし統計をコンパイルします。
パラメーター	<portlist> - ポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:カウンタをクリアするには

```
#clear counters ports 2-9
Command: clear counters ports 2-9

Success.

#
```

3.9.8 clear log

目的	スイッチの履歴ログをクリアします。
構文	clear log
説明	本コマンドは、スイッチの履歴ログをクリアします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ログ情報をクリアするには

```
#clear log
Command: clear log

Success.

#
```

3.9.9 show log

目的	スイッチの履歴ログを表示します。
構文	show log [index <value_list X-Y>]
説明	本コマンドは、スイッチの履歴ログの内容を表示します。 最大表示件数は 6,000 件です。
パラメーター	index <value_list X-Y> - 本コマンドは、<value_list X-Y>フィールドでユーザーが指定した開始と終了の値間の履歴ログを表示します。 パラメーターを指定しない場合、すべての履歴ログエントリーが表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチの履歴ログを表示するには

```
#show log index 1-5
Command: show log index 1-5

Index  Data          Time      Log Text
-----  -
5      00000-00-00 01:01:09 Successful login through Console (Username: adpro)
4      00000-00-00 00:00:14 System warm start
3      00000-00-00 00:00:06 Port 25 link up, 1000Mbps FULL duplex
2      00000-00-00 00:00:01 Port 25 link down
1      00000-00-00 00:06:31 Port 25 link up, 1000Mbps FULL duplex

#
```

3.9.10 enable syslog

目的	システムログをリモートホストに送信する機能を有効にします。
構文	enable syslog
説明	本コマンドは、システムログをリモートホストに送信する機能を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチの syslog 機能を有効にするには

```
#enable syslog
Command: enable syslog

Success.

#
```

3.9.11 disable syslog

目的	システムログをリモートホストに送信する機能を無効にします。
構文	disable syslog
説明	本コマンドは、システムログをリモートホストに送信する機能を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの syslog 機能を無効にするには

```
#disable syslog
Command: disable syslog

Success.

#
```

3.9.12 show syslog

目的	syslog のステータスが有効または無効であるか表示します。
構文	show syslog
説明	本コマンドは、syslog のステータスが有効または無効であるか表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:syslog 機能の現在のステータスを表示するには

```
#show syslog
Command: show syslog

Syslog Global State : Disabled

#
```

3.9.13 create syslog host

目的	新たに syslog の送信内容を設定します。					
構文	create syslog host <index 1-4> [severity < informational warning all > facility < local0 local1 local2 local3 local4 local5 local6 local7 > udp_port <udp_port_number> ipaddress <ipaddr> state < enable disable >]					
説明	本コマンドは、新たに syslog の送信内容を設定します。					
パラメーター	<index 1-4> - コマンドを適用するホストのインデックスを指定します。 1~4 の番号のついた 4 つの利用可能なインデックスがあります。					
	severity - 重度レベルのインジケータ。以下の説明を参考にしてください。					
	<table border="1"> <thead> <tr> <th>数値</th> <th>重度</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>Warning(警告) : 警告の状態</td> </tr> <tr> <td>6</td> <td>Informational(情動的) : 情報を伝えるメッセージ</td> </tr> </tbody> </table>	数値	重度	4	Warning(警告) : 警告の状態	6
数値	重度					
4	Warning(警告) : 警告の状態					
6	Informational(情動的) : 情報を伝えるメッセージ					

パラメーター	数値 コード	ファシリティ
	16	ローカル使用 0 (local0)
	17	ローカル使用 1 (local1)
	18	ローカル使用 2 (local2)
	19	ローカル使用 3 (local3)
	20	ローカル使用 4 (local4)
	21	ローカル使用 5 (local5)
	22	ローカル使用 6 (local6)
	23	ローカル使用 7 (local7)
		<p>local0 - ローカル使用 0 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 16 番に対応します。</p> <p>local1 - ローカル使用 1 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 17 番に対応します。</p> <p>local2 - ローカル使用 2 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 18 番に対応します。</p> <p>local3 - ローカル使用 3 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 19 番に対応します。</p> <p>local4 - ローカル使用 4 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 20 番に対応します。</p> <p>local5 - ローカル使用 5 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 21 番に対応します。</p> <p>local6 - ローカル使用 6 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 22 番に対応します。</p> <p>local7 - ローカル使用 7 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 23 番に対応します。</p> <p>udp_port <udp_port_number> - syslog プロトコルがメッセージをリモートホストに送信するために使用する UDP ポート番号を指定します。</p> <p>ipaddress <ipaddr> - syslog メッセージが送信されるリモートホストの IP アドレスを指定します。</p> <p>state <enable disable> - リモートホストへの syslog メッセージの送信を「enable」(有効)または「disable」(無効)にします。</p>
制限事項		管理者アカウントのみ本コマンドを実行できます。
対応バージョン		1.00.00 以降

使用例:syslog ホストを作成するには

```
#create syslog host 1 ipaddress 10.68.88.1 severity all facility local0
Command: create syslog host 1 ipaddress 10.68.88.1 severity all facility local0

Success.

#
```

3.9.14 config syslog

目的	syslog の送信内容を変更します。																								
構文	config syslog host < all <index 1-4> > severity < informational warning all > [facility < local0 local1 local2 local3 local4 local5 local6 local7 > udp_port <udp_port_number> ipaddress <ipaddr> state < enable disable >]																								
説明	本コマンドは、syslog プロトコルを設定し、システムログ情報をリモートホストに送信します。																								
パラメーター	<p>all - 利用可能なすべてのインデックスを指定します。</p> <p><index 1-4> - コマンドを適用するホストのインデックスを指定します。 1~4 の番号のついた 4 つの利用可能なインデックスがあります。</p> <p>severity - 重度レベルのインジケータ。以下の説明を参考にしてください。</p> <table border="1"> <thead> <tr> <th>数値</th> <th>重度</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>Warning(警告) : 警告の状態</td> </tr> <tr> <td>6</td> <td>Informational(情報的) : 情報を伝えるメッセージ</td> </tr> </tbody> </table> <p>informational - 情報的なメッセージをリモートホストに送信する場合に指定します。これは上記リストの 6 番に対応します。</p> <p>warning - 警告的なメッセージをリモートホストに送信する場合に指定します。これは上記リストの 4 番に対応します。</p> <p>all - スイッチに生成される現在サポートしている Syslog メッセージのすべてをリモートホストに送信します。</p> <p>facility - 指定できるファシリティは以下の通りです。</p> <table border="1"> <thead> <tr> <th>数値</th> <th>ファシリティ</th> </tr> </thead> <tbody> <tr> <td>16</td> <td>ローカル使用 0 (local0)</td> </tr> <tr> <td>17</td> <td>ローカル使用 1 (local1)</td> </tr> <tr> <td>18</td> <td>ローカル使用 2 (local2)</td> </tr> <tr> <td>19</td> <td>ローカル使用 3 (local3)</td> </tr> <tr> <td>20</td> <td>ローカル使用 4 (local4)</td> </tr> <tr> <td>21</td> <td>ローカル使用 5 (local5)</td> </tr> <tr> <td>22</td> <td>ローカル使用 6 (local6)</td> </tr> <tr> <td>23</td> <td>ローカル使用 7 (local7)</td> </tr> </tbody> </table> <p>local0 - ローカル使用 0 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 16 番に対応します。</p> <p>local1 - ローカル使用 1 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 17 番に対応します。</p> <p>local2 - ローカル使用 2 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 18 番に対応します。</p> <p>local3 - ローカル使用 3 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 19 番に対応します。</p> <p>local4 - ローカル使用 4 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 20 番に対応します。</p>	数値	重度	4	Warning(警告) : 警告の状態	6	Informational(情報的) : 情報を伝えるメッセージ	数値	ファシリティ	16	ローカル使用 0 (local0)	17	ローカル使用 1 (local1)	18	ローカル使用 2 (local2)	19	ローカル使用 3 (local3)	20	ローカル使用 4 (local4)	21	ローカル使用 5 (local5)	22	ローカル使用 6 (local6)	23	ローカル使用 7 (local7)
数値	重度																								
4	Warning(警告) : 警告の状態																								
6	Informational(情報的) : 情報を伝えるメッセージ																								
数値	ファシリティ																								
16	ローカル使用 0 (local0)																								
17	ローカル使用 1 (local1)																								
18	ローカル使用 2 (local2)																								
19	ローカル使用 3 (local3)																								
20	ローカル使用 4 (local4)																								
21	ローカル使用 5 (local5)																								
22	ローカル使用 6 (local6)																								
23	ローカル使用 7 (local7)																								

パラメーター	<p>local5 - ローカル使用 5 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 21 番に対応します。</p> <p>local6 - ローカル使用 6 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 22 番に対応します。</p> <p>local7 - ローカル使用 7 のメッセージをリモートホストに送信する場合に指定します。これは上記リストの 23 番に対応します。</p> <p>udp_port <udp_port_number>- syslog プロトコルがメッセージをリモートホストに送信するために使用する UDP ポート番号を指定します。</p> <p>ipaddress <ipaddr> - syslog メッセージが送信されるリモートホストの IP アドレスを指定します。</p> <p>state <enable disable> - リモートホストへの syslog メッセージの送信を「enable」(有効)または「disable」(無効)にします。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:syslog ホストを設定するには

```
#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

Success.

#
```

使用例すべてのホストに対して syslog ホストを設定するには

```
#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

Success.

#
```

3.9.15 delete syslog host

目的	設定済みの syslog ホストをスイッチから削除します。
構文	delete syslog host < <index 1-4> all >
説明	本コマンドは、設定済みの syslog ホストをスイッチから削除します。
パラメーター	<p><index 1-4> - コマンドを適用するホストのインデックスを指定します。 1~4 の番号のついた 4 つの利用可能なインデックスがあります。</p> <p>all - コマンドをすべてのホストに適用する場合に指定します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:設定済みの syslog ホストを削除するには

```
#delete syslog host 4
Command: delete syslog host 4

Success.

#
```

3.9.16 show syslog host

目的	現在スイッチで設定されている syslog ホストを表示します。
構文	show syslog host [<index 1-4>]
説明	本コマンドは、スイッチに現在設定されている syslog ホストを表示します。
パラメーター	<index 1-4> - コマンドを適用するホストのインデックスを指定します。 1 ~ 4 の番号のついた 4 つの利用可能なインデックスがあります。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:syslog ホスト情報を表示するには

```
#show syslog host
Command: show syslog host

Syslog Global State : Enabled

Host 1
  IP Address       : 10.0.0.5
  Severity         : All
  Facility         : Local0
  UDP port         : 514
  Status           : Disabled

Total Entries : 1

#
```


3.9.17 config log_save_timing

目的	スイッチのフラッシュメモリーへログを保存する方法を設定します。
構文	config log_save_timing < time_interval <min 1-65535> on_demand log_trigger >
説明	本コマンドは、スイッチのフラッシュメモリーへログを保存する方法を設定します。
パラメーター	time_interval <min 1-65535> - ログファイルの保存を実行する間隔を設定します。 ログファイルは、ここで設定した時間 (X分) ごとに保存されます。 on_demand - 「save all」または「save log」コマンドを使用して、手動でスイッチに保存すると指定した場合にだけログファイルを保存します。 log_trigger - スイッチにログイベント起こるたびにスイッチにログを保存します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ログファイルの保存を 30 分間隔に設定するには

```
#config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.

#
```

3.9.18 show log_save_timing

目的	スイッチのフラッシュメモリーへログファイルを保存する設定方法を表示します。
構文	show log_save_timing
説明	本コマンドは、スイッチのフラッシュメモリーへログファイルを保存する設定方法を参照します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ログファイルを保存する方法を表示するには

```
#show log_save_timing
Command: show log_save_timing

Saving log method: on_demand

#
```

3.9.19 delete ipif System

目的	IPv6 アドレスを削除します。
構文	delete ipif System < ipv6address <ipv6networkaddr> >
説明	本コマンドは、IPv6 アドレスを削除します。
パラメーター	<ipv6networkaddr> - IPv6 ネットワークアドレスを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: システムインターフェースの IPv6 アドレスを削除するには

```
#delete ipif System ipv6address FE80::200:1FF:FE02:303/128
Command: delete ipif System ipv6address FE80::200:1FF:FE02:303/128

Success.

#
```

3.9.20 enable ipif_ipv6_link_local_auto

目的	IPv6 アドレスが設定されていない場合、リンクローカルアドレスの自動設定を有効にします。
構文	enable ipif_ipv6_link_local_auto <System>
説明	本コマンドは、IPv6 アドレスが明確に設定されていない場合、リンクローカルアドレスの自動設定を有効にします。 IPv6 アドレスが明確に設定されている場合は、リンクローカルアドレスは自動的に設定され、IPv6 処理が開始します。 IPv6 アドレスが明確に設定されていない場合、デフォルトにより、リンクローカルアドレスは設定されず、IPv6 処理は無効になります。 この自動設定を有効にすることによって、リンクローカルアドレスは自動的に設定され、IPv6 処理が開始します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: インターフェースのリンクローカルアドレスの自動設定を有効にするには

```
#enable ipif_ipv6_link_local_auto System
Command: enable ipif_ipv6_link_local_auto System

Success.

#
```

3.9.21 disable ipif_ipv6_link_local_auto

目的	IPv6 アドレスが設定されていない場合、リンクローカルアドレスの自動設定を無効にします。
構文	disable ipif_ipv6_link_local_auto <System>
説明	本コマンドは、IPv6 アドレスが明確に設定されていない場合、リンクローカルアドレスの自動設定を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: インターフェースのリンクローカルアドレスの自動設定を無効にするには

```
#disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System

Success.

#
```

3.9.22 show ipif_ipv6_link_local_auto

目的	リンクローカルアドレス自動設定の状態を表示します。
構文	show ipif_ipv6_link_local_auto
説明	本コマンドは、リンクローカルアドレス自動設定の状態を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: インターフェース情報を表示するには

```
#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

IPIF: System          Automatic Link Local Address: Disabled

#
```

3.10 SMTP コマンド

SMTP (Simple Mail Transfer Protocol) は、電子メールのアドレスに基づき下記のコマンドを使用してスイッチのイベントをメールの受信者に送信するスイッチの機能です。スイッチは SMTP のクライアントとして設定され、一方サーバーはスイッチからのメッセージを受信し、電子メールに適切な情報を記載し、スイッチに設定した受信者に送信します。これにより小規模のワークグループや配線の管理が簡素化され、スイッチの緊急イベントで処理速度が向上し、スイッチに発生した問題イベントの記録によりセキュリティが強化されます。

SMTP 機能におけるクライアントとしてのスイッチの重要な役割:

この機能を適切に動作させるには、SMTP サーバーの IP アドレスと TCP ポートは正しく設定されている必要があります。「server」と「server_port」のパラメーターを適切に設定することによって「config smtp」コマンドが機能します。

メール受信者をスイッチに設定しておく必要があります。サーバーに受信者の情報が送信され、情報が処理され、スイッチ情報が受信者にメールされます。「config smtp」コマンドの「add mail_receiver」と「delete mail_receiver」のパラメーターを使用して、最大 8 人までのメール受信者をスイッチに登録できます。

管理者は、設定した受信者に送信されるメッセージの送信元アドレスを設定することができます。これによりスイッチの機能や問題などについてより詳細な情報を得ることができます。「config smtp」コマンドを使用したり、「self_mail_addr」パラメーターを設定して、プライベートの電子メールを設定することもできます。

受信者が SMTP サーバーからの電子メールを受信できるか、スイッチにテストメール送信の設定をすることができます。テストメールの設定には、まず「enable smtp」コマンドを使用して SMTP 機能を有効にし、次に「smtp send_testmsg」コマンドを入力します。SMTP を設定したすべての受信者が、SMTP サーバーからのサンプルテストメッセージを受信し、この機能の信頼性が確認できます。

次のイベントのどれかひとつでも発生した場合、スイッチは受信者にメールを送信します。

スイッチにコールドスタートまたはウォームスタートが発生した時。

ポートがリンクダウン状態になった時。

ポートがリンクアップ状態になった時。

SNMP 認証がスイッチによって拒否された時。

スイッチ構成エントリがスイッチによって NVRAM に保存された時。

ファームウェアのダウンロードイベント中に TFTP サーバーに異常が発生した時。

これには、TFTP サーバーからの「invalid-file (無効なファイル)」、「file-not-found (ファイルが見つかりません)」、「complete (完了)」、「time-out (j タイムアウト)」のメッセージを含みます。

スイッチにシステムリセットが発生した時。

SMTP サーバーが送信する電子メールには次のスイッチイベント情報が含まれます。

メール送信機器のモデル名と IP アドレス

SMTP サーバーとメッセージを送信したクライアントを識別するタイムスタンプ。スイッチからメッセージを受信した日付も含まれます。中継されたメッセージには各中継ごとにタイムスタンプが付きます。

電子メール送信の要因となるスイッチに発生したイベント。

ファームウェアの保存またはアップグレードなどユーザーによってイベントが処理されたとき、タスクを処理したユーザーの IP アドレス、MAC アドレス、ユーザー名がイベント発生時のシステムメッセ

ージと共に送信されます。

複数回同じイベントが発生した時、2 通目からのメッセージはシステムエラーメッセージが件名に表示されます。

「Delivery Process (配信中)」中に発生したイベント詳細について

優先度の高いの緊急メールは送信待ちの通常メールに差し置いて送信されます。

送信待ちの未送信メールは最大 30 件まで保存されます。30 件まで保存されると新規メールは廃棄されます。

初期のメッセージが受信者に届いていない場合、送信待ちメールの順番に入れられ、再送信が実行されます。

再送信の最大限度は 3 回です。3 回まで 5 分おきに再送信が実行されます。限度数に達してもメッセージが受信されない場合、メールは破棄されます。

スイッチがシャットダウンや再起動した場合、送信待ちメールは破棄されます。

3.10.1 enable smtp

目的	SMTP クライアントとしてスイッチを有効にします。
構文	enable smtp
説明	本コマンドは「disable smtp コマンド」と共に設定を変更せずに、スイッチを SMTP クライアントとして有効/無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スwitchの SMTP を有効にするには

<pre>#enable smtp Command: enable smtp Success. #</pre>

3.10.2 disable smtp

目的	SMTP クライアントとしてスイッチを無効にします。
構文	disable smtp
説明	本コマンドは「enable smtp コマンド」と共に設定を変更せずに、スイッチを SMTP クライアントとして有効/無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチのSMTPを無効にするには

```
#disable smtp
Command: disable smtp

Success.

#
```

3.10.3 config smtp

目的	スイッチのSMTPクライアントとして必要な設定を行います。
構文	config smtp <server <ipaddr> server_port <tcp_port_number 1-65535> self_mail_addr <mail_addr 64> add mail_receiver <mail_addr 64> delete mail_receiver <index 1-8> >
説明	本コマンドはSMTPサーバーやメール受信者の設定を行うために必要なパラメータを設定します。本コマンドは、スイッチのSMTP機能が正常に作動するために、正しく全て設定する必要があります。
パラメーター	server <ipaddr> - リモートデバイス上のSMTPサーバーのIPアドレスを指定します。 server_port <tcp_port_number 1-65535> - SMTPサーバーに接続するTCPポート番号を入力します。SMTPの一般的なポート番号は、「25」です。 self_mail_addr <mail addr 64> - 送信元の電子メールアドレスを入力します。このアドレスは受信者に送信された電子メールアドレスになります。このスイッチでは、メールアドレスを1つだけ設定することができます。文字列は最大64文字までの半角英数字が使用できます。 add mail_receiver <mail_addr 64> - このパラメータを選択することにより、スイッチからの電子メールメッセージの受信者を追加できます。各スイッチごとに8つまでの電子メールアドレスを追加できます。 delete mail_receiver <index 1-8> - このパラメータを選択すると、設定リストからメール受信者を削除できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:SMTP設定を行うには

```
#config smtp server 10.48.74.100 server_port 25 add mail_receiver smtp@hitachi-metals.com
Command: config smtp server 10.48.74.100 server_port 25 add mail_receiver
smtp@hitachi-metals.com

Success.

#
```

3.10.4 show smtp

目的	スイッチの SMTP 機能の設定パラメーターの内容について参照します。
構文	show smtp
説明	本コマンドは、「server information (サーバー情報)」「mail recipients (メール受信者)」やスイッチの SMTP 機能の現在の状態を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに現在設定されている SMTP パラメーターを参照するには

```
#show smtp
Command: show smtp

smtp status: Enabled
smtp server address : 10.48.74.100
smtp server port : 25
self mail address: smtp@hitachi-metals.com

Index          Mail Receiver Address
-----          -
1              smtp@hitachi-metals.com
2
3
4
5
6
7
8

#
```

3.10.5 smtp send_testmsg

目的	スイッチで設定したメール受信者にテストメールを送信します。
構文	smtp send_testmsg
説明	本コマンドは設定された全ての受信者にテストメールを送信します。テストメール送信は SMTP サーバーの設定内容に従い行われます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 設定したメール受信者全員にテストメールを送信するには

```
# smtp send_testmsg
```

```
Command: smtp send_testmsg
```

```
Subject: This is a SMTP test.
```

```
Content: Hello everybody!!
```

```
Sending mail, please wait...
```

```
Success.
```

```
#
```


3.11 スイッチポートコマンド

3.11.1 config ports

目的	スイッチのイーサネットポートを設定します。
構文	<pre>config ports < <portlist> all > < medium_type speed flow_control <enable disable> state <enable disable> learning <enable disable> <description <desc 32> clear_description> mdix < auto normal cross > > medium_type = medium_type <fiber copper> speed = speed <auto 10_half 10_full 100_half 100_full 1000_full [< master slave >] ></pre>
説明	本コマンドは、スイッチのイーサネットポートを設定します。 <portlist> でリストされたポートのみが影響を受けます。
パラメーター	<p>all - スイッチのすべてのポートを設定します。</p> <p><portlist> - 設定するポートまたはポート範囲を指定します。</p> <p>medium_type <fiber copper> - コンボポートを設定する場合、使用している通信メディアのタイプを指定します。</p> <p>speed - ポートの速度を調節します。 ユーザーは以下の選択ができます。</p> <p>auto - ポートのオートネゴシエーションを有効にします。</p> <p><10 100 1000> - ポートの送信速度 (Mbps) を設定します。</p> <p><half full> - ポートをフルデュプレックスまたはハーフデュプレックスとして設定します。</p> <p><master slave> - copper ポートでは、マスター設定(1000M/Full_M)によりデュプレックス、速度および物理レイヤタイプに関連する情報を通知することができます。マスター設定は、さらに2つの接続している物理レイヤ間のマスター・スレーブ関係を決定します。この関係は2つの物理レイヤ間のタイミング制御を確立するために必要です。タイミング制御はローカルソースによってマスター物理レイヤ上に設定されます。スレーブ設定 (1000M/Full_S) は、マスターから受信したデータストリームよりタイミング合わせるループタイミングを使用します。一方の接続に 1000M/Full_M を設定した場合、もう一方の接続は 1000M/Full_S に設定する必要があります。それ以外の設定をすると両ポートにリンクダウンを引き起こします。IEEE 802.3-2005 1000BASE-T 仕様に準拠した装置との接続が可能です。</p> <p>flow_control <enable disable> -特定ポートのフロー制御を「enable」(有効)または「disable」(無効)にします。</p> <p>state <enable disable> - ポートを有効または無効にします。</p> <p>learning <enable disable> - ポートの MAC アドレスの学習を有効または無効にします。</p> <p>description <desc 32> - 選択したポートを説明するために 32 文字以下の半角英数字の文字列を入力します。</p> <p>clear_description - 選択したポートの説明をクリアします。</p> <p>mdix - ポートの MDIX を設定します。MDIX 設定は「auto (自動)」、「normal (通常)」、「cross (クロス)」から選択できます。</p> <p>「normal (通常)」に設定した場合 MDIX モードのポートはストレートケーブルを使用した PC NIC への接続が可能です。「cross (クロス)」に設定した場合、他のスイッチの MDIX モードのポートにストレートケーブルで接続することが可能です。</p>

制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 25 ~ 28 の速度を 10Mbps、フルデュプレックス、ステータスを有効にするには

```
#config ports 25-28 speed 10_full state enable
Command: config ports 25-28 speed 10_full state enable

Warning: For combo ports, the configuration is set to medium_type copper
Success.

#
```

注意事項



相手装置との通信モードは、オートネゴシエーションもしくは固定モードに合わせて下さい。

固定モードでは、通信速度や全二重および半二重モードを合わせる必要があります。双方で一致しないと、リンク確立されない場合やリンク確立してもエラー率の高い通信となる場合があります。

3.11.2 show ports

目的	ポートの設定を表示します。
構文	show ports [<portlist>] [description err_disabled]
説明	本コマンドは、ポートの設定を表示します。パラメーターがない場合は、すべてのポートを表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。 description - 本パラメーターを「show ports」コマンドに追加すると、入力済みのポート説明が表示されます。 err_disabled - 接続状態と無効になった原因を含む無効ポートのリストを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: すべてのポート設定を表示するには

```
#show ports
Command show ports

Port  State/      Settings          Connection        Address
      MDIX      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning
-----
1     Enabled    100M/Full/Disabled  LinkDown          Enabled
      Auto
2     Enabled    100M/Full/Disabled  LinkDown          Enabled
      Auto
```

3	Enabled Auto	100M/Full/Disabled	LinkDown	Enabled
4	Enabled Auto	100M/Full/Disabled	LinkDown	Enabled
5	Enabled Auto	100M/Full/Disabled	LinkDown	Enabled
6	Enabled Auto	100M/Full/Disabled	LinkDown	Enabled
7	Enabled Auto	100M/Full/Disabled	LinkDown	Enabled
8	Enabled Auto	100M/Full/Disabled	LinkDown	Enabled

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh

使用例: すべてのポート設定を説明と併せて表示するには

```
# show ports description

Command: show ports description

Port  State/      Settings          Connection        Address
      MDIX    Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning
-----
1     Enabled   Auto/Disabled    LinkDown          Enabled
      Auto
Desc:
2     Enabled   Auto/Disabled    LinkDown          Enabled
      Auto
Desc:
3     Enabled   Auto/Disabled    LinkDown          Enabled
      Auto
Desc:
4     Enabled   Auto/Disabled    LinkDown          Enabled
      Auto
Desc:
5     Enabled   Auto/Disabled    LinkDown          Enabled
      Auto
Desc:
6     Enabled   Auto/Disabled    LinkDown          Enabled
      Auto
Desc:

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

3.12 Time と SNTP コマンド

3.12.1 config sntp

目的	SNTP サービスを設定します。
構文	config sntp < primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999> >
説明	本コマンドは、SNTP サーバーから SNTP 情報を取得する設定をします。SNTP を使用するためには、本コマンドで SNTP を有効にする必要があります (「enable sntp」を参照してください)。
パラメーター	primary - SNTP 情報を取得するプライマリサーバーの IP アドレス。 <ipaddr> - プライマリサーバーの IP アドレス。 secondary - プライマリサーバーが使用できない場合に SNTP 情報を取得するセカンダリサーバー。 <ipaddr> - セカンダリサーバーの IP アドレス。 poll-interval <int 30-99999> - SNTP の更新情報をリクエストする間隔。ポーリング間隔は、30 ~ 99999 秒の範囲です。
制限事項	管理者アカウントのみ本コマンドを実行できます。 SNTP サーバーを使用するためには、本コマンドで SNTP を有効にする必要があります (「enable sntp」を参照してください)。
対応バージョン	1.00.00 以降

使用例:SNTP 設定を行うには

```
#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

#
```

3.12.2 show sntp

目的	SNTP 情報を表示します。
構文	show sntp
説明	本コマンドは、送信元 IP アドレス、時間、およびポーリング間隔を含む SNTP 設定情報を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:SNTP 設定情報を表示するには

```
#show sntp
Command: show sntp

Current Time Source      : System Clock
SNTP                     : Disabled
SNTP Primary Server     : 10.1.1.1
SNTP Secondary Server   : 10.1.1.2
SNTP Poll Interval      : 30 sec

#
```

3.12.3 enable sntp

目的	SNTP を有効にします。
構文	enable sntp
説明	本コマンドは、SNTP を有効にします。SNTP のパラメータは別途設定する必要があります(「config sntp」を参照してください)。SNTP を有効にして設定すると、手動で設定したすべてのシステム時間設定が上書きされます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。SNTP 設定はSNTP が機能するように設定される必要があります(「config sntp」を参照してください)。
対応バージョン	1.00.00 以降

使用例:SNTP 機能を有効にするには

```
#enable sntp
Command: enable sntp

Success.

#
```

3.12.4 disable sntp

目的	SNTP を無効にします。
構文	disable sntp
説明	本コマンドは、SNTP を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SNTP を無効にするには

```
#disable sntp
Command: disable sntp

Success.

#
```

3.12.5 config time

目的	手動でシステム時間と日付の設定を行います。
構文	config time <date ddmmmyyyy> <time hh:mm:ss>
説明	本コマンドは、システム時間と日付の設定を行います。SNTP が設定され有効にされると、上書きされます。
パラメーター	date - 日付には 2 桁の数字、月には英字 3 文字、年には 4 桁の数字を使用して表します。例：03aug2010 time - システム時間は hh:mm:ss 形式で表します (hh:時、mm:分、ss:秒は 2 桁の数字、24 時制)。例：19:42:30.
制限事項	管理者アカウントのみ本コマンドを実行できます。 SNTP が設定され有効にされると、手動で設定したシステム時間と日付設定は上書きされます。
対応バージョン	1.00.00 以降

使用例:手動でシステム時間と日付の設定を行うには

```
#config time 03aug2010 16:30:30
Command: config time 03aug2010 16:30:30

Success.

#
```

3.12.6 config time_zone

目的	使用するタイムゾーンを決定し、システムクロックを調整します。
構文	config time_zone < operator < + - > hour <gmt_hour 0-13> min <minute 0-59> >
説明	本コマンドは、タイムゾーンに従ってシステムクロック設定を調整します。タイムゾーン設定により SNTP 情報が調整されます。
パラメーター	operator - UTC に対するタイムゾーンの調整で時間を追加 (+) または減算 (-) します。 hour - UTC との差分の時間を指定します。 min - 追加または減算した差分の時間(分)を指定し、タイムゾーンを調整します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: タイムゾーン設定を行うには

```
#config time_zone operator + hour 9 min 00
Command: config time_zone operator + hour 9 min 00

Success.

#
```

3.12.7 config dst

目的	サマータイム(DST : Daylight Savings Time)を有効にし、時間調整を設定します。
構文	<pre>config dst < disable <i>repeating</i> annual > <i>Repeating</i> =repeating < <s_week <start_week 1-5,last> s_day <start_day sun-sat> s_mth <start_mth 1-12> s_time <start_time hh:mm> e_week <end_week 1-5,last> e_day <end_day sun-sat> e_mth <end_mth 1-12> e_time <end_time hh:mm> offset < 30 60 90 120 > > annual < <s_date start_date 1-31> s_mth <start_mth 1-12> s_time <start_time hh:mm> e_date <end_date 1-31> e_mth <end_mth 1-12> e_time <end_time hh:mm> offset < 30 60 90 120 > ></pre>
説明	本コマンドは、DST を有効にして設定します。本コマンドを有効にする場合、どのDST 要求にも応じるようにシステムクロックの調整をします。DST 調整は手動で設定した時間およびSNTP サービスを利用して設定した時間の両方のシステム時間に作用します。
パラメーター	<p>disable - スイッチの DST 季節時間の調整を無効にします。</p> <p>repeating - リpeatモードを使用すると、DST の季節の時間調整が有効になります。リpeatモードでは、計算式を使用して DST (サマータイム) の開始日と終了日を指定する必要があります。例えば、DST (サマータイム) を4月の第2週の日曜日から、10月の最終週の日曜日までと指定します。</p> <p>annual - アニュアルモードを使用すると、DST(サマータイム)の季節の時間調整が有効になります。アニュアルモードでは、DST (サマータイム) の開始日と終了日を詳細に指定する必要があります。例えば、DST (サマータイム) を4月3日から、10月14日までと指定します。</p> <p>s_week - DST(サマータイム)が開始する週を設定します。 <start_week 1-5,last> - DST が開始する週の番号。1 は第1週目、2 は第2週目と続き、last は月の最終週。</p> <p>e_week - DST(サマータイム)が終了する週を設定します。 <end_week 1-5,last> - DST(サマータイム)が終了する週の番号。1 は第1週目、2 は第2週目と続き、last は月の最終週。</p> <p>s_day - DST (サマータイム) が開始する曜日を設定します。 <start_day sun-sat> - 3文字の英字を使用して表された DST(サマータイム)が開始する曜日。(sun, mon, tue, wed, thu, fri, sat)</p> <p>e_day - DST(サマータイム)が終了する曜日を設定します。 <end_day sun-sat> - 3文字の英字を使用して表された DST(サマータイム)が終了する曜日。(sun, mon, tue, wed, thu, fri, sat)</p>

パラメーター	<p>s_mth - DST(サマータイム)が開始する月を設定します。 <start_mth 1-12> - DST(サマータイム)が開始する月番号。 e_mth - DST(サマータイム)が終了する月番号。 <end_mth 1-12> - DST(サマータイム)が終了する月番号。 s_time - DST (サマータイム) が開始する時刻を設定します。 <start_time hh:mm> - 24 時制で時刻 (hh:時、mm:分) を表します。 e_time - DST(サマータイム)が終了する時刻を設定します。 <end_time hh:mm> - 24 時制で時刻 (hh:時、mm:分) を表します。 s_date - DST(サマータイム)が開始する特定日(月日)を設定します。 <start_date 1-31> - 開始日を数字で表します。 e_date - DST(サマータイム)が開始する特定日(月日)を設定します。 <end_date 1-31> - 終了日を数字で表します。 offset <30 60 90 120> - サマータイム間の追加または減算分を示します。 可能なオフセット時間は、30、60、90、120 です。デフォルト値は、60 です。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチのサマータイムを設定するには

```
#config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e_day wed e_mth 10 e_time
15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e_day wed e_mth
10 e_time 15:30 offset 30

Success.

#
```

3.12.8 show time

目的	現在の時刻設定と状態を表示します。
構文	show time
説明	本コマンドは、現在のシステム時間と共に日付と時刻のコンフィギュレーションを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチのシステムクロックに現在設定されている時刻を表示するには

```
#show time
Command: show time

Current Time Source : System Clock
Current Time       : 1 Days 01:39:17
Time Zone         : UTC +02:30
Daylight Saving Time: Repeating
Offset in minutes : 30
  Repeating From  : Apr 2nd Tue 15:00
  To              : Oct 2nd Wed 15:30
  Annual From    : 29 Apr 00:00
  To             : 12 Oct 00:00

#
```

3.13 Asymmetric VLAN コマンド

3.13.1 enable asymmetric_vlan

目的	スイッチの asymmetric VLAN を有効にします。
構文	enable asymmetric_vlan
説明	本コマンドは、スイッチの asymmetric VLAN 機能を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: asymmetric VLAN を有効にするには

<pre>#enable asymmetric_vlan Command: enable asymmetric_vlan Success. #</pre>

3.13.2 disable asymmetric_vlan

目的	スイッチの asymmetric VLAN を無効にします。
構文	disable asymmetric_vlan
説明	本コマンドは、スイッチの asymmetric VLAN 機能を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: asymmetric VLAN を無効にするには

<pre>#disable asymmetric_vlan Command: disable asymmetric_vlan Success. #</pre>

3.13.3 show asymmetric_vlan

目的	スイッチの asymmetric VLAN 状態を参照します。
構文	show asymmetric_vlan
説明	本コマンドは、スイッチの asymmetric VLAN 状態を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定されている asymmetric VLAN 状態を表示するには

```
#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN: Enabled

#
```

3.14 BPDU ガードコマンド

3.14.1 enable bpdu_guard

目的	スイッチの BPDU ガード機能を有効にします。
構文	enable bpdu_guard
説明	本コマンドは、スイッチの BPDU ガード機能を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.04.00 以降

使用例:BPDU ガード機能を有効にするには

```
#enable bpdu_guard
Command: enable bpdu_guard

Success.

#
```

3.14.2 disable bpdu_guard

目的	スイッチの BPDU ガード機能を無効にします。
構文	disable bpdu_guard
説明	本コマンドは、スイッチの BPDU ガード機能を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.04.00 以降

使用例:BPDU ガード機能を無効にするには

```
#disable bpdu_guard
Command: disable bpdu_guard

Success.

#
```

3.14.3 config bpdu_guard ports

目的	スイッチのポートに BPDU ガード機能を設定します。
構文	config bpdu_guard ports <<portlist> all> [state <enable disable> mode <shutdown>]
説明	BPDU ガードを有効にしたポートでは、BPDU パケットを受信すると err-disable 状態となりポートを shutdown にします。
パラメーター	ports <<portlist> all> - BPDU ガード機能を設定するポートまたはポートリストを入力します。all パラメーターを入力すると、スイッチのすべてのポートが対象となります。 state <enable disable> - 指定されたポートの BPDU ガード機能を enable で有効、disable で無効にします。デフォルトでは無効になっています。 mode <shutdown> - BPDU パケットを受信したポートを shutdown にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.04.00 以降



使用例: ポートの BPDU ガードを有効にして、状態モードを shutdown に設定するには

```
#config bpdu_guard ports 1 state enable mode shutdown
Command: config bpdu_guard ports 1 state enable mode shutdown

Success.

#
```

注意事項

-  スパニングツリーが有効になっているポートでは、本 BPDU ガード機能を設定することができません。また、BPDU ガード機能が有効になっているポートでは、スパニングツリーを設定することができません。
-  BPDU ガード機能は、スイッチでサポートされた IEEE802.1d BPDU(STP, RSTP, MSTP) のパケットが対象となります。

3.14.4 config bpdu_guard recovery_time

目的	BPDU ガードのリカバリー時間を設定します。
構文	config bpdu_guard recovery_time <<sec 60-1000000> infinite>
説明	BPDU ガードのリカバリー時間を設定します。
パラメーター	recovery_time <<sec 60-1000000> infinite> - 自動復帰に関する BPDU ガードリカバリータイムを 60 ~ 1000000 秒の範囲または無限に設定します。デフォルトの値は 60 秒です。 Infinite パラメーターを指定するとリカバリータイムが無限に設定され、自動復帰をしなくなります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.04.00 以降

使用例: スイッチの BPDU ガード機能リカバリー時間を 120 秒に設定するには

<pre>#config bpdu_guard recovery_time 120 Command: config bpdu_guard recovery_time 120 Success. #</pre>

3.14.5 config bpdu_guard log

目的	スイッチの BPDU ガードに関するログ状態を設定します。
構文	config bpdu_guard log <none attack_detected attack_cleared both>
説明	スイッチの BPDU ガードに関するログ状態を設定します。
パラメーター	<none> - ログへの書き込みをしません。 <attack_detected> - BPDU パケットを検出した場合に、ログへの書き込みをします。 <attack_cleared> - リカバリー時間による自動復旧、またはコマンドによる手動復旧を行った場合に、ログへの書き込みをします。 <both> - BPDU パケット検知および復旧した場合に両方のログを書き込みます。デフォルトでは both が設定されています。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.04.00 以降

使用例: BPDU ガードログ状態を both として設定するには

<pre>#config bpdu_guard log both Command: config bpdu_guard log both Success. #</pre>

3.14.6 show bpdu_guard

目的	スイッチおよびポートのBPDUガード状態を表示します。
構文	show bpdu_guard [ports [<portlist>]]
説明	スイッチおよびポート毎のBPDUガード状態を表示します。
パラメーター	ports - ポートのBPDUガード状態を表示させませす。 <portlist> - 表示させたいポートリストを入力します。
制限事項	なし。
対応バージョン	1.04.00 以降

使用例: スイッチのBPDUガード設定を表示するには

```
#show bpdu_guard
Command: show bpdu_guard

BPDU Guard Global Settings
-----
BPDU Guard Status      : Enabled
BPDU Guard Recovery Time : 120 seconds
BPDU Guard Trap Status  : None
BPDU Guard Log Status   : Both

#
```

使用例: ポートの BPDU ガード設定を表示するには

```
#show bpdu_guard ports
```

```
Command: show bpdu_guard ports
```

Port	State	Mode	Status
1	Enabled	Shutdown	Normal
2	Disabled	Shutdown	Normal
3	Disabled	Shutdown	Normal
4	Disabled	Shutdown	Normal
5	Disabled	Shutdown	Normal
6	Disabled	Shutdown	Normal
7	Disabled	Shutdown	Normal
8	Disabled	Shutdown	Normal
9	Disabled	Shutdown	Normal
10	Disabled	Shutdown	Normal
11	Disabled	Shutdown	Normal
12	Disabled	Shutdown	Normal
13	Disabled	Shutdown	Normal
14	Disabled	Shutdown	Normal
15	Disabled	Shutdown	Normal
16	Disabled	Shutdown	Normal
17	Disabled	Shutdown	Normal
18	Disabled	Shutdown	Normal
19	Disabled	Shutdown	Normal
20	Disabled	Shutdown	Normal

```
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.15 フォワーディングデータベースコマンド

3.15.1 create fdb

目的	ユニキャスト MAC アドレスフォワーディングテーブル (データベース) にスタティックエントリーを作成します。
構文	create fdb <vlan_name 32> <macaddr> port <port>
説明	本コマンドは、スイッチのユニキャスト MAC アドレスフォワーディングテーブルにエントリーを作成します。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名。 <macaddr> - フォワーディングテーブルに追加される MAC アドレス。 port <port> - MAC 送信先アドレスに対応するポート番号。スイッチはこのポートを介して、常に指定されたデバイスにトラフィックを転送します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ユニキャスト MAC FDB エントリーを作成するには

```
#create fdb default 00-40-66-00-00-01 port 5
Command: create fdb default 00-40-66-00-00-01 port 5

Success.

#
```

3.15.2 create multicast_fdb

目的	マルチキャスト MAC アドレスフォワーディングテーブル (データベース) にスタティックエントリーを作成します。
構文	create multicast_fdb <vlan_name 32> <macaddr>
説明	本コマンドは、スイッチのマルチキャスト MAC アドレスフォワーディングデータベースにエントリーを作成します。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名。 <macaddr> - フォワーディングテーブルに追加される MAC アドレス。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:マルチキャスト MAC フォワーディングエントリーを作成するには

```
#create multicast_fdb default 01-00-5E-00-00-01
Command: create multicast_fdb default 01-00-5E-00-00-01

Success.

#
```


3.15.3 config multicast_fdb

目的	スイッチのマルチキャスト MAC アドレスフォワーディングデータベースを設定します。
構文	config multicast_fdb <vlan_name 32> <macaddr> < add delete > <portlist>
説明	本コマンドは、マルチキャスト MAC アドレスフォワーディングテーブルを構成します。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名。 <macaddr> - マルチキャストフォワーディングテーブルに追加される MAC アドレス。 <add delete> - add は、ポートをテーブルに追加します。delete は、マルチキャストフォワーディングテーブルからポートを削除します。 <portlist> - 設定するポートまたはポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: マルチキャスト MAC フォワーディングを設定するには

```
#config multicast_fdb default 01-00-5E-00-00-01 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-01 add 1-5

Success.

#
```

3.15.4 config fdb aging_time

目的	フォワーディングデータベースのエージングタイムを設定します。
構文	config fdb aging_time <sec 10-1000000>
説明	エージングタイムは、スイッチの学習プロセスに影響します。送信元 MAC アドレスと対応するポート番号から構成されるダイナミックフォワーディングテーブルエントリが、エージングタイム内にアクセスされないと、テーブルから削除されます。エージングタイムは 10 ~ 1000000 秒で指定します。デフォルトでは 300 秒に設定されています。エージングタイムが非常に長い場合、古いか既に存在しないダイナミックフォワーディングテーブルエントリとなります。これは、不正パケットの送信を引き起こす原因となります。しかし、エージングタイムが短すぎると多くのエントリが非常に早く削除されてしまいます。これは送信元アドレスがフォワーディングテーブルで見つけられないパケットを受信する高い確率をもたらし、その場合、スイッチはすべてのポートにパケットをブロードキャストするため、スイッチが持つ利点の多くを無駄にしまいます。
パラメーター	<sec 10-1000000> - MAC アドレスフォワーディングデータベース値のエージングタイム。10 ~ 1000000 秒を設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降


使用例: fdb エージングタイムを設定するには

```
#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

#
```

注意事項

 実際に FDB のエントリーが削除されるのは、<SEC> ÷ 2 ~ <SEC> - 1 までの時間幅があります。

3.15.5 delete fdb

目的	スイッチのフォワーディングデータベースのエントリーを削除します。
構文	delete fdb <vlan_name 32> <macaddr>
説明	本コマンドは、スイッチの MAC アドレスフォワーディングデータベースに作成したエントリーを削除します。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名。 <macaddr> - フォワーディングテーブルから削除する MAC アドレス。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: FDB を永久に削除するには

```
#delete fdb default 00-40-66-00-00-01
Command: delete fdb default 00-40-66-00-00-01

Success.

#
```

使用例: マルチキャスト FDB エントリーを削除するには

```
#delete fdb default 01-00-5E-00-00-01
Command: delete fdb default 01-00-5E-00-00-01

Success.

#
```

3.15.6 clear fdb

目的	すべての動的に学習された MAC アドレスをスイッチのフォワーディングデータベースからクリアします。
構文	clear fdb < vlan <vlan_name 32> port <port> all >
説明	本コマンドは、スイッチのフォワーディングデータベースにダイナミックに学習されたエントリをクリアします。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名。 port <port> - MAC 送信先アドレスに対応するポート番号。 all - スwitchのフォワーディングデータベースのすべてのダイナミックエントリをクリアします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: すべての FDB ダイナミックエントリをクリアするには

<pre>#clear fdb all Command: clear fdb all Success. #</pre>

3.15.7 show multicast_fdb

目的	スイッチのマルチキャストフォワーディングデータベースの内容を表示します。
構文	show multicast_fdb [vlan <vlan_name 32> mac_address <macaddr>]
説明	本コマンドは、スイッチのマルチキャスト MAC アドレスフォワーディングデータベースの現在の内容を表示します。
パラメーター	<vlan_name 32> - MAC アドレスが存在する VLAN 名。 <macaddr> - FDB エントリが表示される MAC アドレスを指定します。 パラメーターを指定しない場合、すべてのマルチキャスト FDB エントリが表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MAC アドレステーブルを表示するには

```
#show multicast_fdb vlan default
Command: show multicast_fdb vlan default

VLAN Name      : default
MAC Address     : 01-00-5E-00-00-01
Egress Ports    : 1-5
Mode            : Static

Total Entries   : 1

#
```

3.15.8 show fdb

目的	現在のユニキャストMACアドレスフォワーディングデータベースを表示します。
構文	show fdb [port <port> vlan <vlan_name 32> vlanid <vidlist> mac_address <macaddr> static aging_time]
説明	本コマンドは、スイッチのフォワーディングデータベースの現在の内容を表示します。
パラメーター	port <port> - MAC送信先アドレスに対応するポート番号。スイッチはこのポートを介して、常に指定されたデバイスにトラフィックを転送します。 <vlan_name 32> - MACアドレスが存在するVLAN名。 <vidlist> - VIDリストによって示されたVLANのエントリーを表示します。 <macaddr> - フォワーディングデータベーステーブルに存在するMACアドレス。 static - スタティックMACアドレスエントリーを表示します。 aging_time - MACアドレスフォワーディングデータベースのエイジングタイムを表示します。
制限事項	なし。
対応バージョン	1.00.00以降

使用例:ユニキャストMACアドレステーブルを表示するには

```
#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID  VLAN Name                MAC Address          Port Type
-----
1    default                    00-40-66-00-00-01  CPU   Self

Total Entries : 1

#
```

3.15.9 config multicast port_filtering_mode

目的	ポートのマルチキャストパケットフィルタリングモードを設定します。
構文	config multicast port_filtering_mode < <portlist> all > < forward_unregistered_groups filter_unregistered_groups >
説明	本コマンドは、スイッチの特定ポートに対するマルチキャストパケットフィルタリングモードを設定します。
パラメーター	<<portlist> all> - マルチキャストポートフィルタリングモードを設定するポートまたはポートリストを入力します。all パラメーターを入力すると、スイッチのすべてのポートが対象となります。 <forward_unregistered_groups filter_unregistered_groups> - これらの2つのオプションのいずれにもフィルタリングモードを設定することができます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1~4 のすべてのグループを転送するマルチキャストフィルタリングモードを設定するには

<pre>#config multicast port_filtering_mode 1-4 forward_unregistered_groups Command: config multicast port_filtering_mode 1-4 forward_unregistered_groups Success. #</pre>

3.15.10 show multicast port_filtering_mode

目的	ポートのマルチキャストパケットフィルタリングモードを表示します。
構文	show multicast port_filtering_mode
説明	本コマンドは、スイッチのポートに対する現在のマルチキャストパケットフィルタリングモードを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: すべてのポートのマルチキャストポートフィルタリングモードを参照するには

<pre>#show multicast port_filtering_mode Command: show multicast port_filtering_mode Multicast Filter Mode For Unregistered Group: Forwarding List: 1-28 Filtering List: #</pre>
--

3.16 IGMP スヌープコマンド

3.16.1 config igmp_snooping

目的	スイッチの IGMP スヌープを設定します。
構文	config igmp_snooping < vlan_name <vlan_name 32> vlanid <vidlist> all > < state < enable disable > fast_leave < enable disable > >
説明	本コマンドは、スイッチの IGMP スヌープを設定します。
パラメーター	<vlan_name 32> - IGMP スヌープを設定する VLAN 名。 <vidlist> - 設定する VLAN のリストを指定します。 All - スイッチが設定されるすべての VLAN を指定します。 Fast_leave <enable disable> - IGMP スヌープの fast-leave (直ぐに離脱) 機能を「enable」(有効)または「disable」(無効)にします この機能を有効にすると、システムが IGMP Leave メッセージを受信し、Leave メッセージを送信するホストがグループの最後のホストである場合、メンバーは直ぐに離脱されます。 State <enable disable> - 指定した VLAN の IGMP スヌープを「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: IGMP スヌープを設定するには

```
#config igmp_snooping vlan_name default state enable
Command: config igmp_snooping vlan_name default state enable

Success.

#
```

3.16.2 config igmp_snooping querier

目的	通常のクエリ送信の間隔 (秒)、メンバーからのレポートを待つ最大時間 (秒) および IGMP スヌープを保証する許容パケット損失を設定します。
構文	config igmp_snooping querier < vlan_name <vlan_name 32> vlanid <vidlist> all > < query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state < enable disable > version <value 1-3> >
説明	本コマンドは、IGMP スヌープクエリアを設定します。
パラメーター	<p><vlan_name 32> - 設定する IGMP スヌープクエリアに対する VLAN 名。</p> <p><vidlist> - IGMP スヌープクエリアが設定される VID 範囲。</p> <p>All - スイッチが設定されるすべての VLAN を指定します。</p> <p>Query_interval - 一般的なクエリア送信間隔を秒単位で指定します。デフォルト値は、125 秒です。</p> <p>Max_response_time - メンバからのレポートを待つ最大時間(秒)。デフォルト値は 10 秒です。</p> <p>Robustness_variable - 予想されるサブネット上のパケットの損失に応じてこの変数を微調整します。Robustness variable (堅牢性変数) の値は以下の IGMP メッセージ間隔を計算する場合に使用されます。</p> <ul style="list-style-type: none"> ・ Group membership interval - マルチキャストルーターがネットワーク上のグループにメンバがいないと判断するまでの時間。間隔の計算は以下の通りです。(堅牢性変数 x クエリ間隔) + (1 x クエリ応答間隔)。 ・ Other querier present interval- マルチキャストルーターがクエリアである他のマルチキャストルーターがないと判断するまでの時間。間隔の計算は以下の通りです。(堅牢性変数 x クエリ間隔) + (0.5 x クエリ応答間隔)。 ・ Last member query count - ルーターがグループ内にローカルメンバーがいないと見なす前に送信された Group-Specific Query 数。デフォルト値は Robustness Variable (堅牢性変数) の値です。 ・ デフォルトにより、robustness variable (堅牢性変数) は「2」に設定されています。サブネットのパケット損失が高くなると予想する場合には、この値を増やします。 <p>Last_member_query_interval - Leave-group メッセージへの応答として送信したメッセージを含む group-specific query メッセージ間の最大時間。この間隔を短くして、ルーターがラストグループメンバ損失の検出時間を減少させることができます。</p> <p>State - 状態が enable の場合、IGMP Querier として選択できます (IGMP クエリパケットを送信します)。「disable (無効)」の場合、スイッチはクエリアとして機能しません。スイッチに接続したレイヤ 3 ルーターが IGMP プロキシ機能のみを提供し、マルチキャストルーティング機能を提供しない場合、この状態は無効として設定されます。そうでない場合、レイヤ 3 ルーターがクエリアとして選択しないと、IGMP クエリパケットを送信しません。マルチキャストルーティングプロトコルパケットを送信しないため、ポートはルーターポートとしてタイムアウトになります。</p> <p>Version - この VLAN が送信する IGMP パケットのバージョンを指定します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。

対応バージョン	1.00.00 以降
---------	------------

使用例: IGMP スヌープクエリアを設定するには

```
#config igmp_snooping querier vlan_name default query_interval 125 state enable
Command: config igmp_snooping querier vlan_name default query_interval 125 state enable

Success.

#
```

3.16.3 config router_ports

目的	ポートをルーターポートとして設定します。
構文	config router_ports <vlan_name 32> vlanid <vidlist> > <add delete> > <portlist>
説明	本コマンドは、マルチキャストイネーブルのルーターに接続するポート範囲を指定します。これは、プロトコルの種類にかかわらず送信先としてルーターが持つすべてのパケットをマルチキャストイネーブルのルーターに到達するように設定します。
パラメーター	<vlan_name 32> - ルーターポートが存在する VLAN 名。 <vidlist> - 設定するルーターポートの VID 範囲。 <add delete> - 設定するルーターポートを追加するか削除するか指定します。 <portlist> - 設定するポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スタティックルーターポートを設定するには

```
#config router_ports_forbidden default add 1-10
Command: config router_ports_forbidden default add 1-10

Success.

#
```


3.16.4 config_router_ports_forbidden

目的	ポートを forbidden (禁止)ルーターポートとして設定します。
構文	config router_ports_forbidden < <vlan_name 32> vlanid <vidlist> > < add delete > <portlist>
説明	本コマンドは、マルチキャストイネーブルのルーターへの接続を禁止するポート範囲を指定します。これは、禁止ルーターポートがルーティングパケットを伝播しないようにします。
パラメーター	<vlan_name 32> - ルーターポートが存在する VLAN 名。 <vidlist> - 禁止ポートとして設定するポートの VID 範囲。 <add delete> - 指定した VLAN の禁止ポートを追加または削除するかどうか指定します。 <portlist> - 禁止ルーターポートとして設定されるポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:禁止ルーターポートを設定するには

```
#config router_ports_forbidden default add 2-10
Command: config router_ports_forbidden default add 2-10

Success.

#
```

3.16.5 enable_igmp_snooping

目的	スイッチの IGMP スヌープを有効にします。
構文	enable igmp_snooping [forward_mcrouter_only]
説明	本コマンドは、スイッチの IGMP スヌープを有効にします。 「forward_mcrouter_only」が指定されると、スイッチはマルチキャストルーティングプロトコルパケットと IGMP 制御パケットの識別に基づいたルーターポートを学習します。
パラメーター	forward_mcrouter_only - 本コマンドにこのパラメーターを追加すると、スイッチはマルチキャストルーティングプロトコルパケットと IGMP 制御パケットの識別に基づいたルーターポートを学習します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの IGMP スヌープを有効にするには

```
#enable igmp_snooping
Command: enable igmp_snooping

Success.

#
```

3.16.6 disable igmp_snooping

目的	スイッチの IGMP スヌープを無効にします。
構文	disable igmp_snooping [forward_mcrouter_only]
説明	本コマンドは、スイッチの IGMP スヌープを無効にします。 「forward_mcrouter_only」が指定されると、スイッチはユニキャストルーティングプロトコルパケット、マルチキャストルーティングプロトコルパケット、および IGMP 制御パケットの識別に基づいたルーターポートを学習します。コマンドの上位互換性について、本コマンドは CLI でサポートされますがルーターポート学習のシステム動作は無効になります。
パラメーター	Forward_mcrouter_only - このパラメーターを本コマンドに追加すると、スイッチはユニキャストルーティングプロトコルパケット、マルチキャストルーティングプロトコルパケット、および IGMP 制御パケットの識別に基づいたルーターポートを学習し、disable igmp_snooping forward_mcrouter_only コマンドは無効になります。スイッチはマルチキャストルーティングプロトコルパケットと IGMP 制御パケットの識別に基づいたルーターポートを学習します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スwitchの IGMP スヌープを無効にするには

```
#disable igmp_snooping
Command: disable igmp_snooping

Success.

#
```

3.16.7 show igmp_snooping

目的	スイッチ上の IGMP スヌープの現在のステータスを表示します。
構文	show igmp_snooping [vlan <vlan_name 32> vlanid <vidlist>]
説明	本コマンドは、スイッチの現在の IGMP スヌープステータスとコンフィギュレーションを表示します。
パラメーター	<vlan_name 32> - IGMP スヌープコンフィギュレーションを参照する VLAN 名。 <vidlist> - 表示するコンフィギュレーションの VID 範囲。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: IGMP スヌープを表示するには

```
#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State      : Disabled
Multicast Router Only           : Disabled

VLAN Name                        : default
Query Interval                   : 125
Max Response Time                : 10
Robustness Value                 : 2
Last Member Query Interval      : 1
Querier State                    : Disabled
Querier Role                     : Non-Querier
Querier IP                       : 0.0.0.0
Querier Expiry Time              : 0 secs
State                            : Disabled
Fast Leave                       : Disabled
Version                          : 3

Total Entries : 1

#
```

3.16.8 show router_ports

目的	現在スイッチで設定されているルーターポートを表示します。
構文	show router_ports [< vlan <vlan_name 32> vlanid <vidlist> >] [<static dynamic forbidden >]
説明	本コマンドは、スイッチに現在設定されているルーターポートを表示します。
パラメーター	<vlan_name 32> - ルーターポートが存在する VLAN 名。 <vidlist> - 表示するルーターポートの VID 範囲。 static - 静的に設定されているルーターポートを表示します。 dynamic - 動的に設定されているルーターポートを表示します。 forbidden - 静的に設定されている forbidden (禁止)ルーターポートを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ルーターポートを表示するには

```
#show router_ports
Command: show router_ports

VLAN Name      : default
Static Router Port :
Dynamic Router Port:
Forbidden Router Port:

Total Entries: 1

#
```

3.16.9 show igmp_snooping_group

目的	スイッチ上の現在の IGMP スヌープグループのコンフィギュレーションを表示します。
構文	show igmp_snooping_group [< vlan <vlan_name 32> vlanid <vidlist> >]
説明	本コマンドはスイッチ上の現在の IGMP スヌープグループのコンフィギュレーションを表示します。
パラメーター	<vlan_name 32>- IGMP スヌープグループ情報を参照する VLAN 名。 <vidlist> - IGMP スヌープグループ情報を参照する VID リスト。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:現在の IGMP スヌープグループを参照するには

```
#show igmp_snooping_group
Command: show igmp_snooping_group

Source/Group    : NULL/239.255.255.255
VLAN Name/VID   : default/1
Reports        : 1
Member Ports    : 4
Router Ports    : 8
Up time        : 122
Expire Time     : 260
Filter Mode     : EXCLUDE

Total Entries   : 1

#
```

3.16.10 show igmp_snooping host

目的	特定のポートまたは VLAN にグループを登録した IGMP ホストを表示します。
構文	show igmp_snooping host [<vlan_name <vlan_name 32> vlanid <vidlist> ports <portlist> group <ipaddr>>]
説明	本コマンドは、特定のポートまたは特定の VLAN にグループを登録した IGMP ホストを表示します。
パラメーター	<vlan_name 32> - VLAN を指定してホスト情報を表示します。VLAN またはポートを指定しない場合、すべての登録ホストが表示されます。 <vlanid>- VLAN ID を指定します。 <portlist>- ポートのリストを指定してホスト情報を表示します。VLAN またはポートを指定しない場合、すべての登録ホストが表示されます。 <ipaddr> - グループの IP アドレスを指定してホスト情報を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: IGMP スヌープ高速脱退 (Fast Leave) 機能を表示するには

```
# show igmp_snooping host
Command: show igmp_snooping host
```

VLAN ID	Group	Port No	IGMP Host
1	225.0.1.0	2	10.0.0.1
1	225.0.1.0	2	10.0.0.2
1	225.0.1.0	3	10.0.0.3
1	225.0.1.2	2	10.0.0.4
1	225.0.2.3	3	10.0.0.5
1	225.0.3.4	3	10.0.0.6
1	225.0.4.5	5	10.0.0.7
1	225.0.5.6	5	10.0.0.8
1	225.0.6.7	4	10.0.0.9
1	225.0.7.8	4	10.0.0.10
1	239.255.255.250	7	10.0.0.11

```
Total Entries : 11
#
```

3.17 リンクアグリゲーションコマンド

3.17.1 create link_aggregation

目的	スイッチのリンクアグリゲーショングループを作成します。
構文	<code>create link_aggregation group_id <value> [type<lacp static>]</code>
説明	本コマンドは、固有の識別子を有するリンクアグリゲーショングループを作成します。
パラメーター	<p><value> - グループ ID を指定します。最大 14(各装置で最大ポート数の半分)までのリンクアグリゲーショングループを設定できます。グループ ID によって各グループを識別します。</p> <p>type - グループに使用するリンクアグリゲーションのタイプを指定します。タイプを指定しない場合は、デフォルトタイプは「static」になります。</p> <p>lacp - ポートグループを LACP 準拠として指定します。LACP は集約されたポートグループに動的な調整を行います。LACP 準拠のポートは、詳細設定が必要になります (config lacp_ports を参照のこと)。LACP 準拠のポートは LACP 準拠のデバイスに接続する必要があります。</p> <p>static - アグリゲーションポートグループをスタティックとして指定します。スタティックポートグループは、トランクグループのコンフィギュレーションを変更した場合、リンクされた両デバイスを手動で設定する必要があるため、LACP 準拠のポートグループとして容易に変更することができません。スタティックリンクアグリゲーションを使用する場合、接続の両端が適切に設定され、すべてのポートが同一の速度/デュプレックス設定であることを確認してください。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: リンクアグリゲーショングループを作成するには

```
#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.
#
```



FM シリーズではリンクアグリゲーショングループ数最大は各製品搭載ポート数 ÷ 2 となります。GM シリーズにおいては APLGM118GTSS と APLGM124GTSS のみ最大 8、それ以外は製品搭載ポート数 ÷ 2 となります。
メンバーポートとして、ユーザーポートとコンボポートを組み合わせることは出来ません。

3.17.2 delete link_aggregation group_id

目的	設定済みのリンクアグリゲーショングループを削除します。
構文	delete link_aggregation group_id <value>
説明	本コマンドは、設定済みのリンクアグリゲーショングループを削除します。
パラメーター	<value> - グループ ID を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: リンクアグリゲーショングループを削除するには

```
#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

#
```

3.17.3 config link_aggregation group_id

目的	作成済みのリンクアグリゲーショングループを設定します。
構文	config link_aggregation group_id <value> < master_port <port> ports <portlist> state < enable disable > >
説明	本コマンドは、上記の create link_aggregation コマンドと併せて作成されたリンクアグリゲーショングループを設定します。
パラメーター	group_id <value> - グループ ID を指定します。最大 14 までのリンクアグリゲーショングループを設定できます。グループ ID によって各グループを識別します。 master_port <port> - マスタポート番号。マスタポートになるリンクアグリゲーショングループのポート (ポート番号 による) を指定します。リンクアグリゲーショングループのすべてのポートは、マスタポートと共にポートコンフィギュレーションを共有します。 ports <portlist> - リンクアグリゲーショングループに所属するポートまたはポート範囲を指定します。 state <enable disable> - 指定されたリンクアグリゲーショングループを「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。 リンクアグリゲーショングループは重複できません。 リンクアグリゲーションの所属ポートと認証機能 (802.1x 認証、MAC 認証、WEB 認証) のポート併用はできません。
対応バージョン	1.00.00 以降

使用例: ポートの負荷分散グループ、グループ ID1、マスタポート 1 をグループメンバポート 1-4 と共に定義するには :

```
#config link_aggregation group_id 1 master_port 1 ports 1-4
Command: config link_aggregation group_id 1 master_port 1 ports 1-4

Success.

#
```

3.17.4 config link_aggregation algorithm

目的	リンクアグリゲーションアルゴリズムを設定します。
構文	config link_aggregation algorithm < mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest >
説明	本コマンドは、負荷分散データの送信に対し、egress ポートを選択する際、スイッチによって検証されるパケットの部分を設定します。本機能は、アドレスベースの負荷分散アルゴリズムを使用したときのみ有効です。
パラメーター	mac_source - スイッチは送信元 MAC アドレスを検証します。 mac_destination - スイッチは送信先 MAC アドレスを検証します。 mac_source_dest - スイッチは送信元および送信先 MAC アドレスを検証します。 ip_source - スイッチは送信元 IP アドレスを検証します。 ip_destination - スイッチは送信先 IP アドレスを検証します。 ip_source_dest - スイッチは送信元および送信先 IP アドレスを検証します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 送信先および送信元 MAC のリンクアグリゲーションアルゴリズムを設定するには

```
#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

#
```

注意事項



Unknown unicast/Broadcast/Multicast の分散動作は下記を KEY としたアルゴリズムで振り分けられます。

Unknown unicast、Broadcast、L2 Multicast : MAC_DA、MAC_SA、SRC_PORT

IP Multicast : SIP、DIP、SRC_PORT

MAC_DA : 宛先 MAC アドレス

MAC_SA : 送信元 MAC アドレス

SRC_PORT : 送信元 TCP/UDP ポート番号

SIP : 送信元 IP アドレス

DIP : 宛先 IP アドレス

3.17.5 show link_aggregation

目的	スイッチ上の現在のリンクアグリゲーションのコンフィギュレーションを表示します。
構文	show link_aggregation [group_id <value> algorithm]
説明	本コマンドは、スイッチ上の現在のリンクアグリゲーションのコンフィギュレーションを表示します。
パラメーター	<value> - グループ ID を指定します。 algorithm - 使用中のアルゴリズムによって指定するリンクアグリゲーションを表示することができます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: リンクアグリゲーションのコンフィギュレーションを表示するには

```
#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source

Group ID      : 1
Type:         : Static
Master Port   :
Member Port   :
Active Port   :
Status        : Disabled
Flooding Port : 0

Total Entries : 1

#
```

3.17.6 config lacp_ports

目的	LACP 準拠のポートを設定します。
構文	config lacp_ports <portlist> mode < active passive >
説明	本コマンドは、LACP ポートとして指定済みのポートを設定します (create link_aggregation を参照のこと)。
パラメーター	<p><portlist> - 設定するポートまたはポート範囲を指定します。</p> <p>mode - LACP ポートが LACP 制御フレームを処理するかどうかを決定するモードを選択します。</p> <p>active - Active LACP ポートは、LACP 制御フレームの処理と送信を行うことが可能です。これにより LACP 準拠のデバイスはリンクの集約をネゴシエートし、グループは必要に応じてダイナミックに変更されます。グループへのポート追加、または削除などの集約ポートグループの変更を行うためには、少なくともいずれかのデバイスの LACP ポートを「Active」として設定する必要があります。デバイスは両方とも LACP をサポートしている必要があります。</p> <p>passive - 「Passive」として設定された LACP ポートは、LACP 制御フレームの処理ができません。リンクされたポートグループがネゴシエーションを行い、調整をネゴシエートし、動的に変更を行うには、接続のどちらか一端が「active」LACP ポートである必要があります (上記を参照のこと)。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: LACP ポートモード設定を行うには

```
#config lacp_ports 1-12 mode active
Command: config lacp_ports 1-12 mode active

Success.

#
```

3.17.7 show lacp_ports

目的	現在の LACP ポートモード設定を表示します。
構文	show lacp_ports [<portlist>]
説明	本コマンドは、現在の LACP モード設定を表示します。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 パラメーターを指定しない場合、システムはすべてのポートについて現在の LACP 設定を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:LACP ポートモード設定を表示するには

```
#show lacp_ports 1-10  
Command: show lacp_ports 1-10
```

```
Port      Activity  
-----  -  
1         Active  
2         Active  
3         Active  
4         Active  
5         Active  
6         Active  
7         Active  
8         Active  
9         Active  
10        Active
```

```
#
```

3.18 ループ防止コマンド

3.18.1 config looopdetect

目的	スイッチにループ防止機能を設定します。
構文	config looopdetect < recover_timer < 0 <value 60-1000000> > interval <value 1-32767> >
説明	本コマンドは、スイッチ全体にループ防止機能 (LBD) を設定します。
パラメーター	recover_timer - ループ状態がなくなったかをチェックする時間を決定するために自動リカバリーメカニズムが使用する間隔 (秒)。「0」は特別な値であり、自動リカバリーメカニズムが無効であることを意味します。従って、手動で無効なポートを復旧しなければなりません。手動で復旧させる場合には、ポートステータスを無効にしてから有効にすることで復旧します。 「config looopdetect ports <portlist> state disable」 「config looopdetect ports <portlist> state enable」 復旧タイマーのデフォルト値は 60 (秒) です。有効な範囲は、60 ~ 1000000 です。 interval - デバイスがループイベントを検出するためにすべてのコンフィギュレーションテストプロトコル(CTP : Configuration Test Protocol)パケットを送信する間隔(秒)。有効範囲は、1 ~ 32767 です。デフォルト値は 10 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 復旧タイマーを 0、CTP 送信間隔を 20 に設定するには

```
#config looopdetect recover_timer 0 interval 20
Command: config looopdetect recover_timer 0 interval 20

Success.

#
```

注意事項



ループ防止機能にてループ検知した場合、速やかにループ原因を取り除いて下さい。ループ状態では、リカバリー時間(デフォルト 60 秒)経過すると自動復旧が行われ次のループ検知までループが再発し、ネットワーク全体が不安定な状態になります。ループ発生源を早期に特定できない場合、リカバリー時間(0 秒)による手動復旧を設定されることを推奨します。

3.18.2 config loopdetect ports

目的	スイッチのポートにループ防止機能を設定します。
構文	config loopdetect ports <portlist> all > state <enable disable> method <shutdown drop >
説明	本コマンドは、スイッチのポートコンフィギュレーションでループ防止機能を設定します。enable に設定したポート配下に接続したスイッチにおいて生じたループの検知が有効になります。
パラメーター	<p><portlist> - ループ検知ステータスを設定するポート範囲を指定します。</p> <p>all - すべてのポートに設定を適用します。</p> <p>state - ポートリストに指定されたポートにループ防止機能を「enable」(有効)または「disable」(無効)にします。デフォルトでは無効になっています。</p> <p>enable - ループ防止機能のステータスを「enable」(有効)に設定します。</p> <p>disable - ループ防止機能のステータスを「disable」(無効)に設定します。</p> <p>method - ループ防止機能設定をしたポートに対して、shutdown 動作または drop 動作のどちらかを定義します。デフォルト値は shutdown です。</p> <p>shutdown - ポートに shutdown 設定を適用します。</p> <p>drop - ポートに drop 設定を適用します。drop 設定ではループバック検知しパケット転送は行われず。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.05.00 以降

使用例:ループ防止機能を有効にするには

```
# config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

#
```

注意事項



LBD 動作は、機器毎に識別されたループ監視専用フレームを受信することでループ発生と判断します。

- ・ ver.1.04.00 までの LBD は、ループ監視専用フレームを「自送出ポートで受信」することでループを検知します。
- ・ ver.1.05.00 以降の LBD では、ループ監視専用フレームを「自装置内ポートで受信」することでループ検知します。

このループ監視専用フレームは、Tag VLAN には対応しておりません。

(Tag ポートでも Tag 付与されずに送出されます)

そのため、対向機器で転送するには Native VLAN を設定する必要があります。

3.18.3 enable loopdetect

目的	スイッチのループ防止機能を装置単位で有効にします。
構文	enable loopdetect
説明	本コマンドは、スイッチのループ防止機能を装置単位で「enable」(有効)にします。デフォルト値は「disable」(無効)です。 1.07以降からループ防止機能によりループを検知した場合に、本装置の console LED を高速に点滅させる LED 点滅可視化機能を追加しました。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ループ防止機能を装置単位で有効にするには

```
# enable loopdetect
Command: enable loopdetect

Success.

#
```

注意事項



ループ検知時の LED 点滅可視化機能により、本装置の console LED 点滅状態が変わります。

- ・ ver.1.07.00 以降では、ループ検知している状態で console LED が点滅します。(ループ検知が解除された場合には LED 点滅も同時に解除されます。)
- ・ ver.1.06.00 以前では、ループ検知しても console LED は点滅しません。

3.18.4 disable loopdetect

目的	スイッチのループ防止機能を装置単位で無効にします。
構文	disable loopdetect
説明	本コマンドは、スイッチのループ防止機能を装置単位で無効にします。デフォルト値は「disable」(無効)です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ループ防止機能を装置単位で無効にするには

```
# disable loopdetect
Command: disable loopdetect

#
```

3.18.5 show loopdetect

目的	スイッチの現在のループ防止機能のコンフィギュレーションを表示します。
構文	show loopdetect
説明	本コマンドは、スイッチのループ防止機能のコンフィギュレーションを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ループ防止機能のコンフィギュレーションを表示するには

```
#show loopdetect
Command: show loopdetect

Loopdetect Global Settings
-----
Loopdetect Status      : Enabled
Loopdetect Interval    : 20
Recover Time           : 0

#
```

3.18.6 show loopdetect ports

目的	スイッチのポートごとにループ防止機能のコンフィギュレーションを表示します。
構文	show loopdetect ports < <portlist> all >
説明	本コマンドは、スイッチのポートごとの現在のループ防止機能のコンフィギュレーションとステータスを表示します。
パラメーター	<portlist> - 設定するポート範囲を指定します。 all - システムのすべてのポートを設定する場合は、「all」のパラメーターを使用します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ポート 1~9 のループ防止機能のコンフィギュレーションを表示するには

```
#show loopdetect ports 1-9
```

```
Command: show loopdetect ports 1-9
```

Port	Loopdetect State	Method	Loop Status
1	Disabled	Shutdown	Normal
2	Disabled	Shutdown	Normal
3	Disabled	Shutdown	Normal
4	Disabled	Shutdown	Normal
5	Disabled	Shutdown	Normal
6	Disabled	Shutdown	Normal
7	Disabled	Shutdown	Normal
8	Disabled	Shutdown	Normal
9	Disabled	Shutdown	Normal

3.19 MAC ベース VLAN コマンド

3.19.1 create mac_based_vlan

目的	スタティック MAC ベース VLAN エントリーを作成します。
構文	create mac_based_vlan mac_address <macaddr> vlan <vlan_name 32>
説明	本コマンドは、スタティック MAC ベース VLAN エントリーを作成します。 スタティック MAC ベース VLAN エントリーがユーザーに対して作成されると、このユーザーからのトラフィックはこのポートで動作する PVID に関係なく指定した VLAN の下で、実行されます。 スタティック MAC ベース VLAN エントリーに対しては、サポートされる最大エントリーにグローバル限界があります。
パラメーター	mac - MAC アドレス。 vlan - MAC アドレスに対応付けされる VLAN。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベース VLAN ローカルエントリーを作成するには

```
# create mac_based_vlan mac_address 00-40-66-00-00-01 vlan default
Command: create mac_based_vlan mac_address 00-40-66-00-00-01 vlan default

Success.

#
```

3.19.2 delete mac_based_vlan

目的	スタティック MAC ベース VLAN エントリーを削除します。
構文	delete mac_based_vlan [mac_address <macaddr> vlan <vlan_name 32>]
説明	本コマンドは、データベースエントリーを削除します。MAC アドレスおよび VLAN を指定しない場合、ポートに対応付けされたスタティックエントリーのすべてが削除されます。
パラメーター	mac - MAC アドレス。 vlan - MAC アドレスに対応付けされる VLAN。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スタティック MAC ベース VLAN エントリーを削除するには

```
# delete mac_based_vlan mac_address 00-40-66-00-00-01 vlan default
Command: delete mac_based_vlan mac_address 00-40-66-00-00-01 vlan default

Success.

#
```

3.19.3 show mac_based_vlan

目的	スタティック MAC ベース VLAN エントリーを表示します。
構文	show mac_based_vlan [mac <macaddr> vlan <vlan_name 32>]
説明	本コマンドは、スタティック MAC ベース VLAN エントリーを表示します。
パラメーター	mac - 表示するエントリーの MAC アドレス。 vlan - 表示するエントリーの VLAN。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: MAC ベース VLAN エントリーを表示するには

```
# show mac_based_vlan
Command: show mac_based_vlan

  MAC Address      VLAN    Status    Type
  -----
00-80-e0-14-a7-57  200     Active    Static
00-80-c2-33-c3-45  300     Inactive  Static
00-80-c2-33-c3-45  400     Active    802.1X

Total Entries: 3

#
```

3.20 MLD スヌープコマンド

3.20.1 config mld_snooping

目的	スイッチに MLD スヌープを設定します。
構文	config mld_snooping < vlan <vlan_name 32> vlanid <vidlist> all > < state <enable disable> fast_done < enable disable > >
説明	本コマンドは、スイッチに MLD スヌープを設定します。
パラメーター	<vlan_name 32> - 設定する MLD スヌープに対する VLAN 名。 <vidlist> - 設定される VID の範囲。 all- スwitchのすべての VLAN を設定します。 state - 選択した VLAN の MLD スヌープ機能を「enable」(有効)または「disable」(無効)にします。 fast_done - MLD スヌープ Fast done 機能を「enable」(有効)または「disable」(無効)にします。この機能を「enable」(有効)にするとメンバは MLD の完了メッセージがシステムに受信されるとすぐにグループから抜けることができます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MLD スヌープのステートを有効にしてデフォルトの VLAN に設定するには

<pre>#config mld_snooping vlan default state enable Command: config mld_snooping vlan default state enable Success. #</pre>

3.20.2 config mld_snooping querier

目的	MLD スヌープクエリアのタイマーと属性を設定します。
構文	config mld_snooping querier < vlan <vlan_name 32> vlanid <vidlist> all > < query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_listener_query_interval <sec 1-25> >
説明	本コマンドは、一般的なクエリ送信の間隔 (秒)、リスナーからのレポートを待つ最大時間(秒)を設定し、MLD スヌープによって保証されるパケットの損失を許容します。
パラメーター	<vlan_name 32> - 設定する MLD スヌープに対する VLAN 名。 <vidlist>- VID のリスト。 all- スwitchのすべての VLAN を設定します。 query_interval - 一般的なクエリア送信間隔を秒単位で指定します。デフォルト値は 125 秒です。 max_reponse_time - リスナーからのレポートを待つ最大時間 (秒)。デフォルト値は 10 秒です。

パラメーター	<p>robustness_variable - 予想されるサブネット上のパケットの損失に応じてこの変数を微調整します。Robustness Variable (堅牢性変数) の値は以下のMLD メッセージ間隔を計算する場合に使用されます。</p> <p>Group listener interval-マルチキャストルーターがネットワーク上のグループにメンバがいないと判断するまでの時間。 間隔の計算は以下の通りです。 (堅牢性変数 x クエリ間隔) + (1 x クエリ応答間隔)。</p> <p>Other querier present interval-マルチキャストルーターがクエリアである他のマルチキャストルーターがないと判断するまでの時間。間隔の計算は以下の通りです。 (堅牢性変数 x クエリ間隔) + (0.5 x クエリ応答間隔)。</p> <p>Last listener query count-ルーターがグループ内にローカルリスナーがいないと見なす前に送信されたグループに固有なクエリ数。 デフォルト値は Robustness Variable (堅牢性変数)の値です。</p> <p>デフォルトにより、robustness variable (堅牢性変数)は「2」に設定されています。サブネットのパケット損失が高くなると予想する場合には、この値を増やします。</p> <p>last_listener_query_interval - Done-group メッセージへの応答として送信したメッセージを含む group-specific query メッセージ間の最大時間。この間隔を短くして、ルーターがラストグループリスナー損失の検出時間を減少させることができます。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:クエリ間隔を 125 秒、状態を有効にして MLD スヌープクエリアを設定するには

<pre>#config mld_snooping querier vlan default query_interval 125 Command: config mld_snooping querier vlan default query_interval 125 state enable Success. #</pre>
--

3.20.3 config mld_snooping mrouter_ports

目的	ポートをルーターポートとして設定します。
構文	config mld_snooping mrouter_ports <vlan_name 32> < add delete > <portlist>
説明	本コマンドは、マルチキャストイネーブルのルーターに接続するポート範囲を指定します。これは、プロトコルの種類にかかわらず送信先としてルーターが持つすべてのパケットをマルチキャストイネーブルのルーターに到達するように設定します。
パラメーター	<p><vlan_name 32> - ルーターポートが存在する VLAN 名。</p> <p><add delete> - ルーターポートを追加または削除します。</p> <p><portlist> - 設定するポート範囲を指定します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ルーターポートに 1~10 のポート範囲を設定するには

```
# config mld_snooping mrouter_ports default add 1-10
Command: config mld_snooping mrouter_ports default add 1-10

Success.

#
```

3.20.4 config mld_snooping mrouter_ports_forbidden

目的	ポートを forbidden (禁止) ルーターポートとして設定します。
構文	config mld_snooping mrouter_ports_forbidden <vlan_name 32> < add delete > <portlist>
説明	本コマンドは、マルチキャストイネーブルのルーターに接続しないポート範囲を指定します。これは、禁止ルーターポートがルーティングパケットを伝播しないようにします。
パラメーター	<vlan_name 32> - 禁止ルーターポートが存在する VLAN 名。 <add delete> - 禁止ルーターポートを追加または削除します。 <portlist> - 設定するポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 禁止ルーターポートに 1~10 のポート範囲を設定するには

```
#config mld_snooping mrouter_ports_forbidden default add 1-10
Command: config mld_snooping mrouter_ports_forbidden default add 1-10

Success.

#
```

3.20.5 enable mld_snooping

目的	スイッチの MLD スヌープを有効にします。
構文	enable mld_snooping
説明	本コマンドは、スイッチの MLD スヌープを有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

注意事項



MLD スヌーピングバージョン 2 のソースフィルタリング機能は未サポートです。

使用例:スイッチのMLD スヌープを有効にするには

```
# enable mld_snooping
Command: enable mld_snooping

Success.

#
```

3.20.6 disable mld_snooping

目的	スイッチのMLD スヌープを無効にします。
構文	disable mld_snooping
説明	本コマンドは、スイッチのMLD スヌープを無効にします。MLD スヌープを無効にすると、デフォルトによりすべてのMLD とIPv6 マルチキャストトラフィックがスイッチ内でフラッドします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチのMLD スヌープを無効にするには

```
# disable mld_snooping
Command: disable mld_snooping

Success.

#
```

3.20.7 show mld_snooping

目的	スイッチ上の現在のMLD スヌープコンフィギュレーションを表示します。
構文	show mld_snooping [vlan <vlan_name 32> vlanid <vidlist>]
説明	本コマンドは、スイッチの現在のMLD スヌープコンフィギュレーションを表示します。
パラメーター	<vlan_name 32> - MLD スヌープコンフィギュレーションを参照するVLAN名。 <vidlist> - VIDのリスト。 パラメーターを指定しない場合、システムはすべてのMLD スヌープの現在のコンフィギュレーションを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MLD スヌープを表示するには

```
# show mld_snooping
Command: show mld_snooping

MLD Snooping Global State      : Enabled

VLAN Name                       : default
Query Interval                  : 125
Max Response Time               : 10
Robustness Value                : 2
Last Listener Query Interval   : 1
Querier Router Behavior        : Non-Querier
State                           : Disabled
Fast Done                       : Disabled
Receive Query Count             : 0

Total Entries: 1

#
```

3.20.8 show mld_snooping group

目的	スイッチ上の現在の MLD スヌープグループコンフィギュレーションを表示します。
構文	show mld_snooping group [vlan <vlan_name 32> vlanid <vidlist>]
説明	本コマンドは、スイッチの現在の MLD スヌープコンフィギュレーションを表示します。
パラメーター	<vlan_name 32>- MLD スヌープグループコンフィギュレーション情報を参照する VLAN 名。 <vidlist> - MLD スヌープグループコンフィギュレーション情報を参照する VID。 パラメーターを指定しない場合、システムはすべての MLD グループスヌープコンフィギュレーションを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MLD スヌープを表示するには

```
#show mld_snooping group
Command: show mld_snooping group

Source/Group      : FE80::100:10:10:5/FF02::1000:0:0:20
VLAN Name/VID     : default/1
Port Member       : 1-2
Mode              : INCLUDE

Source/Group      : FE80::100:10:10:5/FF02::1000:0:0:20
VLAN Name/VID     : default/1
Port Member       : 3
Mode              : EXCLUDE

Source/Group      : NULL/ FF02::1000:0:0:21
VLAN Name/VID     : default/1
Port Member       : 4-5
Mode              : EXCLUDE

#
```

3.20.9 show mld_snooping mrouter_ports

目的	現在スイッチで設定されているルーターポートを表示します。
構文	show mld_snooping mrouter_ports [vlan <vlan_name 32> vlanid <vidlist>] [static dynamic forbidden]
説明	本コマンドは、スイッチに現在設定されているルーターポートを表示します。
パラメーター	<vlan_name 32> - 情報を表示するルーターポートが存在する VLAN 名。 <vidlist> - 情報を表示する設定済みルーターの VID 範囲。 static - 静的に設定されているルーターポートを表示します。 dynamic - 動的に設定されているルーターポートを表示します。 forbidden - 静的に設定されている forbidden (禁止)ルーターポートを表示します。 パラメーターを指定しない場合、システムはスイッチに現在設定されているすべてのルーターポートを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ルーターポートを表示するには

```
# show mld_snooping mrouter_ports  
Command: show mld_snooping mrouter_ports
```

```
VLAN Name           : default  
Static Router Port  : 1-10  
Dynamic Router Port :  
Forbidden Router Port :
```

```
VLAN Name           : vlan2  
Static Router Port  :  
Dynamic Router Port :  
Forbidden Router Port :
```

```
Total Entries : 2
```

```
#
```

3.21 マルチプルスパニングツリープロトコル (MSTP) コマンド

本スイッチは3種類のバージョンのスパニングツリープロトコル (802.1D STP、802.1w Rapid STP、802.1s MSTP) をサポートしています。マルチプルスパニングツリープロトコル (MSTP) はIEEE 委員会により定義された標準規格で、複数の VLAN を1つのスパニングツリーインスタンスにマッピングし、ネットワーク中に複数の経路を提供します。従って、これらの MSTP コンフィギュレーションはトラフィックロードのบาลancingを行い、単一のスパニングツリーインスタンスに障害が発生した場合でも、広い範囲で影響を与えないようにすることができます。これにより、障害が発生したインスタンスに代わって新しいトポロジーを素早く収束します。これら VLAN 用のフレームは、これらの3つのスパニングツリープロトコル (STP、RSTP、MSTP) のいずれかを使用して、素早く適切に相互接続されたブリッジを通して処理されます。本プロトコルでは、BPDU (Bridge Protocol Data Unit) パケットにタグ付けを行い、受信するデバイスが、スパニングツリーインスタンス、スパニングツリーリージョン、およびそれらに対応づけられた VLAN を区別できるようにしています。これらのインスタンスは Instance_ID によって分類されます。MSTP では、複数のスパニングツリーを CIST (Common and Internal Spanning Tree) で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を決定し、1つのスパニングツリーを構成する1つの仮想ブリッジのように見せかけます。そのため、異なる VLAN を割り当てられたフレームは、ネットワーク上の管理用に設定されたリージョン中の異なるデータ経路を通ります。

ネットワーク上の MSTP を使用しているスイッチは、以下の3つの属性を持つ1つの MSTP コンフィギュレーションを持ちます。

- (1) 32文字までの半角英数字で定義された「コンフィギュレーション名」(「config stp mst_config_id」コマンドでの name <string>として設定済み)。
- (2) 「コンフィギュレーションリビジョン番号」(「revision_level」として設定済み)。
- (3) 4094件のエレメントテーブル(「VID range」として設定済み)。
- (4) スイッチがサポートする4094件までのVLANとインスタンスとの対応づけです。

スイッチで MSTP 機能を利用するためには、以下の手順を実行します。

スイッチに MSTP 設定を行います (「config stp version」コマンド)。

MSTP インスタンスに適切なスパニングツリープライオリティを設定します (「config stp priority」コマンド)。

共有する VLAN を MSTP Instance ID に追加する必要があります (config stp instance_id コマンド)。

3.21.1 enable stp

目的	スイッチのスパニングツリープロトコルをグローバルで有効にします。
構文	enable stp
説明	本コマンドは、スイッチのスパニングツリープロトコルをグローバルで有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例: スイッチのスパニングツリープロトコルをグローバルで有効にするには

```
#enable stp
Command: enable stp

Success.

#
```

注意事項



認証機能 (MAC 認証、WEB 認証、802.1x 認証) とのポート併用はできません。

3.21.2 disable stp

目的	スイッチのスパニングツリープロトコルをグローバルで無効にします。
構文	disable stp
説明	本コマンドは、スイッチのスパニングツリープロトコルをグローバルで無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチのスパニングツリープロトコルを無効にするには

```
#disable stp
Command: disable stp

Success.

#
```

3.21.3 config stp version

目的	スイッチのスパニングツリープロトコルのバージョンをグローバルに設定します。
構文	config stp version < mstp rstp stp >
説明	本コマンドは、スイッチに組み込まれるスパニングツリーのバージョンを選択します。
パラメーター	mstp - 本パラメーターを選択すると、スイッチのマルチプルスパニングツリープロトコル(MSTP)をグローバルに設定します。 rstp - 本パラメーターを選択すると、スイッチのラピッドスパニングツリープロトコル(RSTP)をグローバルに設定します。 stp - 本パラメーターを選択すると、スイッチのスパニングツリープロトコル(STP)をグローバルに設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチをマルチプルスパニングツリープロトコル (MSTP) 用にグローバルに設定するには

```
#config stp version mstp
Command: config stp version mstp

Success.

#
```

3.21.4 config stp

目的	スイッチに STP、RSTP、および MSTP を設定します。
構文	config stp [maxage <value 6-40> maxhops <value 6-40> hellotime <value 1-2> forwarddelay <value 4-30> txholdcount <value 1-10> fbpdu <enable disable>] (1)
説明	本コマンドは、スイッチ全体にスパニングツリープロトコル (STP) を設定します。STP バージョン用に実行される以下のすべてのコマンドは、現在スイッチに設定されています。
パラメーター	<p>maxage <value 6-40> - 本値は古い情報がネットワークにある冗長パスを永遠に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN (ブリッジで相互接続された LAN) 内のデバイスが持っているスパニングツリーコンフィギュレーション値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6~40 秒の範囲で時間を選択できます。デフォルト値は 20 です。</p> <p>maxhops <value 6-40> - スイッチが送信した BPDU (bridge protocol data unit) パケットが破棄される前のスパニングツリー範囲内のデバイス間のホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。スイッチは、その後 BPDU パケットを破棄し、ポートに保持していた情報を解放します。ホップカウントは 6~40 で指定します。デフォルト値は「20」です。</p> <p>hellotime <value 1-2> - ルートデバイスによるコンフィギュレーションメッセージの送信間隔を設定し、スイッチがまだ機能していることを知らせます。1~2 秒の間の時間を選択します。デフォルト値は、2 秒です。</p> <p>forwarddelay <value 4-30> - 状態を変更する前にルートデバイスが待機する最大時間(秒)。4~30 秒の範囲で時間を選択できます。デフォルト値は 15 秒です。</p> <p>txholdcount <value 1-10> - 間隔ごとに送信される BPDU Hello パケットの最大数。デフォルト値は 6 です。</p> <p>fbpdu <enable disable> - STP を無効にすると、STP BPDU パケットが他のネットワークデバイスから送信されます。デフォルト値は「enable」です。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降


使用例:Maxage を 18、Maxhops を 15 にして STP を設定するには

```
#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

#
```

注意事項

- 
 マルチプルスパニングツリープロトコル (MSTP) では、スパニングツリーがポートごとに設定されるため、MSTP を使用するスイッチには「configure stp ports」コマンドを使用して「hellotime」を設定する必要があります。

3.21.5 config stp ports

目的	ポートレベルで STP を設定します。
構文	<pre>config stp ports <portlist> < externalCost < auto <value 1-200000000> > hellotime <value 1-2> migrate < yes no > edge < true false auto > restricted_role < true false > restricted_tcn < true false > p2p < true false auto > state < enable disable > fbpdu < enable disable > ></pre>
説明	本コマンドは、ポートグループに対して STP を作成および設定します。
パラメーター	<p><portlist> - 設定するポート範囲を指定します。</p> <p>externalCost - 指定したポートリストに対し、パケットの転送にかかるコストを表すメトリックを定義します。ポートコストは、自動的に設定するかメトリック値を設定できます。デフォルト値は「auto (自動)」です。</p> <p>auto - 本パラメーターを設定すると、リストに指定したポートに対して、最適な効率でパケット転送スピードを自動的に設定します。 Default port cost: 100Mbps port = 200000. Gigabit port = 20000.</p> <p><value 1-200000000> - 1~200000000 の範囲で値を定義し、外部コストを決定します。小さい数字を指定すると、パケット転送ポートとして選出される確率が上がります。</p> <p>hellotime <value 1-2> - 指定ポートが Bridged ブリッジにより接続される LAN 上の他のデバイスにコンフィギュレーションメッセージを送信する間隔。このようにしてスイッチがまだ機能していることを知らせます。1~2 秒の範囲で時間を選択できます。デフォルト値は 2 秒です。</p>

パラメーター	<p>migrate <yes no> - 「Yes」を設定すると、STP 設定に関する情報をリクエストする他のブリッジに BPDU パケットをポートが送信する場合に設定します。スイッチが RSTP に設定されると、ポートは 802.1D STP から 802.1w RSTP まで移行することができます。スイッチが MSTP に設定されると、ポートは 802.1D STP から 802.1s MSTP まで移行することができます。RSTP と MSTP は標準の STP と共存できますが、RSTP と MSTP の利点は 802.1D ネットワークが 802.1w または 802.1s が有効なネットワークに接続するポート上では実現されません。セグメントのすべてまたは一部において 802.1w RSTP または 802.1s にアップグレード可能なネットワークステーションまたはセグメントに接続したポートでは本パラメーターを「Yes」とします。</p> <p>edge <true false auto> - true は、選択ポートをエッジポートとして指定します。しかし、トポロジの変更によってループ発生の可能性が生じると、エッジポートはエッジポートとしての資格を失います。エッジポートは通常 BPDU パケットを受け取りません。もし、BPDU パケットが受信されると、そのポートはエッジポートの資格を失います。false は、そのポートにエッジポートの資格がないことを示しています。</p> <p>p2p <true false auto> - true は、選択ポートを P2P ポートとして指定します。P2P ポートはエッジポートと似ていますが、P2P ポートは全二重モードでのみ動作する点で異なります。RSTP の特長として、エッジポート同様、P2P ポートは迅速にフォワーディング状態に遷移します。P2P の値が false の場合は、そのポートに P2P ポートの資格がないことを示しています。Auto にすると、ポートはいつでも可能な時に（「true」を指定した時と同様に）P2P ポートとして動作します。ポートの資格を失う時（例えば、半二重モードを指定された時など）、自動的に「false」を指定した時と同様になります。本パラメーターのデフォルト値は、「auto」です。</p> <p>state <enable disable> - ポートリストに指定されたポートに STP を「enable」（有効）または「disable」（無効）にします。デフォルト値は「enable」です。</p> <p>restricted_role - ルートポートとして選択するかどうかを決定します。デフォルト値は「false」（偽）です。</p> <p>restricted_tcn - このポートがトポロジの変更を伝播するかどうかを決定します。デフォルト値は「false」（偽）です。</p> <p>fbpdu <enable disable> - 有効にすると、STP が指定したポートで無効になっている場合に STP BPDU パケットが他のネットワークデバイスから転送されます。ユーザーがポートごとに BPDU パケットの転送を有効にしたい場合、最初に次の設定を有効にする必要があります。1. STP をグローバルに無効にする必要があります。2. BPDU の転送をグローバルで有効にする必要があります。グローバルに STP を無効化するには、「disable stp」コマンドを使用します。「fbpdu」をグローバルに有効化するには、「config stp」コマンドを使用します。デフォルト値は「enable」（有効）です。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: Path cost auto、hellotime 2秒、migration enable、ポート 1~2 の state enable で STP を設定するには

```
#config stp ports 1-2 externalCost auto hellotime 2 migrate yes state enable
Command: config stp ports 1-2 externalCost auto hellotime 2 migrate yes state enable

#
```

3.21.6 create stp instance_id

目的	MSTP に STP インスタンス ID を作成します。
構文	create stp instance_id <value 1-4>
説明	本コマンドは、マルチプルスパニングツリープロトコル (MSTP) の STP インスタンス ID を作成します。スイッチには 5 個のインスタンス (1 つは CIST で変更できません。) があり、4 個のインスタンス ID を作成することができます。
パラメーター	<value 1-4> - スイッチに STP インスタンスを指定するために 1~4 の範囲から指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スパニングツリーインスタンス 2 を作成するには

```
#create stp instance_id 2
Command: create stp instance_id 2

Success.

#
```

3.21.7 config stp instance_id

目的	STP インスタンス ID を追加または削除します。
構文	config stp instance_id <value 1-4> < add_vlan remove_vlan > <vidlist>
説明	本コマンドは、スイッチに「instance_id」を作成することによって、VID (VLANID) を設定済みの STP インスタンスにマップします。STP インスタンスは、同じ MSTP コンフィギュレーションを持つ複数メンバーを持っています。ネットワークにおける、STP 範囲の数には制限はありませんが、各範囲は、最大 5 個の STP インスタンス (1 つは変更できないデフォルトエントリー) をサポートしています。VID は一度に 1 つの STP インスタンスにだけ所属することができます。
パラメーター	<value 1-4> - スイッチに instance_id を指定するために 1~4 の範囲から指定します。スイッチは「0」として設定されている変更できないデフォルトインスタンス ID 1 個を含め 5 個の STP 範囲をサポートしています。 add_vlan - vid_range <vidlist>パラメーターと共に、設定済みの STPinstance_id に VID を追加します。

パラメーター	remove_vlan - vid_range <vidlist>パラメーターと共に、設定済みの STPinstance_id から VID を削除します。 <vidlist> - スイッチに設定済みの VLAN の中から、VID の範囲を指定します。ID 番号が 1 ~ 4094 の範囲でスイッチの VID をサポートします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: インスタンス ID 2 を設定して VID 10 を追加するには

```
#config stp instance_id 2 add_vlan 10
Command: config stp instance_id 2 add_vlan 10

Success.

#
```

使用例: インスタンス ID 2 から VID 10 を削除するには

```
#config stp instance_id 2 remove_vlan 10
Command: config stp instance_id 2 remove_vlan 10

Success.

#
```

注意事項



同じ STP instance_id を持つ同じ STP 範囲にあるスイッチがマップされ、同じコンフィギュレーションの revision_level 番号と同じ name (名前) を持つ必要があります。

3.21.8 delete stp instance_id

目的	スイッチから STP インスタンス ID を削除します。
構文	delete stp instance_id <value 1-4>
説明	本コマンドは、スイッチから設定済みの STP インスタンス ID を削除します。
パラメーター	<value 1-4> - スイッチにスパニングツリーインスタンスを指定するために 1 ~ 4 の範囲から指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチから STP インスタンス ID 2 を削除するには

```
#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

#
```

3.21.9 config stp priority

目的	STP インスタンスコンフィギュレーションを更新します。
構文	config stp priority <value 0-61440> instance_id <value 0-4>
説明	本コマンドは、スイッチの STP インスタンスコンフィギュレーション設定を更新します。 MSTP は、ルートブリッジ、ルートポート、指定ポートの選択に優先度を使用します。 STP 領域に高い優先度を割り当てることにより、スイッチに転送パケット用として選択した instance_id に優先権を与えます。優先度の設定値が低いほど、優先度は高くなります。
パラメーター	priority <value 0-61440> - 0~61440 の値を選択し、転送パケットに対して指定されたインスタンス ID に優先度を指定します。数字が低いほど、優先度は高くなります。このエントリーは 4096 の倍数とする必要があります。 instance_id <value 0-4> - 設定済みのインスタンス ID に対応する優先度の値を入力します。0 のインスタンス ID は、スイッチに内部設定されたデフォルトの instance_id (CIST) であることを示します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: Instance_id 2 に対する優先度値に 4096 を設定するには

```
#config stp priority 4096 instance_id 2
Command: config stp priority 4096 instance_id 2

Success.

#
```

3.21.10 config stp mst_config_id

目的	MSTP コンフィギュレーション ID を更新します。
構文	config stp mst_config_id < revision_level <int 0-65535> name <string> >
説明	本コマンドは、スイッチに現在設定されている MSTP コンフィギュレーションを一意に識別します。ここに入力された情報は、それが属する MSTP 範囲の識別子として BPDU パケットに添付されます。同じ revision_level と名前を持つスイッチは、同じ MSTP 範囲の一部であると見なされます。
パラメーター	revision_level <int 0-65535> - 0 ~ 65535 の値を入力し、MSTP 領域を識別します。この値は名前と共に、スイッチに設定した MSTP 領域を識別します。デフォルト値は「0」です。 name <string> - 32 文字以内の半角英数字の文字列を入力して、スイッチの MSTP 領域を一意に識別します。この name (名前) は、revision_level の値と共に、スイッチに設定した MSTP 領域を識別します。name (名前) が入力されないと、デフォルト名はデバイスの MAC アドレスになります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:

リビジョンレベルを 10 にし、名前を「HCL」にしてスイッチの MSTP 領域を設定するには

<pre>#config stp mst_config_id revision_level 10 name HCL Command: config stp mst_config_id revision_level 10 name HCL Success. #</pre>

3.21.11 config stp mst_ports

目的	MSTP インスタンスのポートコンフィギュレーションを更新します。
構文	config stp mst_ports <portlist> instance_id <value 0-4> < internalCost < auto <value 1-200000000> > priority <value 0-240> >
説明	本コマンドは、STP instance_id のポートコンフィギュレーションを更新します。ループが発生すると、MSTP 機能はポートの優先度を使用して、フォワーディング状態に遷移させるインターフェースを選択します。最初に転送させるために選択するインターフェースには高い優先度を付与します。優先値が同じインスタンスでは、MSTP 機能は最小のポート番号をフォワーディング状態にし、他のインターフェースをブロックします。低優先度値が転送パケットのために、より高い優先度を意味することにご注意ください。
パラメーター	<p><portlist> - 設定するポートまたはポート範囲を指定します。</p> <p>instance_id <value 0-4> - スイッチに設定済みの instance_id を指定するために 0~4 の範囲から数値を入力します。0 のエントリは CIST (Common and Internal Spanning Tree) を示します。</p> <p>internalCost - 本パラメーターは、インターフェースが STP インスタンス内で選択される場合、指定ポートへの転送パケットの相対的なコストを設定します。デフォルト値は「auto」です。次の 2 つのオプションがあります：</p> <p>auto - internalCost に本パラメーターを選択すると、インターフェースに自動的に最適な最速ルートを設定します。デフォルト値はインターフェースのメディアスピードに基づきます。</p> <p>value 1-200000000 - ループが発生した場合、1~200000000 の範囲の値を持つコストを使用して最速ルートを設定します。internalCost の値が低いほど、高速で伝送されます。</p> <p>priority <value 0-240> - ポートインターフェースの優先度を 0~240 の範囲から指定します。最初に転送させたいインターフェースには高い優先度 (小さい数値) を与え、最後に転送させたいインターフェースには低い優先度 (大きい数値) を与えます。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: インスタンス ID 2、自動 internalCost、優先度 16 でポート 1~5 を指定するには

```
#config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16
Command : config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16

Success.

#
```

3.21.12 show stp

目的	スイッチに現在設定されている STP コンフィギュレーションを表示します。
構文	show stp
説明	本コマンドは、スイッチの現在の STP コンフィギュレーションを表示します。
パラメーター	なし
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スwitchの STP のステータスを表示するには

ステータス 1: STP 互換バージョンで有効にされた STP

```
#show stp
Command: show stp

STP Bridge Global Settings
-----
STP Status      : Enabled
STP Version     : STP compatible
Max Age        : 20
Hello Time     : 2
Forward Delay  : 15
Max Hops       : 20
TX Hold Count  : 6
Forwarding BPDU : Enabled

#
```

ステータス 2: RSTP に対し有効にされた STP

```
#show stp
Command: show stp

STP Bridge Global Settings
-----
STP Status      : Enabled
STP Version     : RSTP
Max Age         : 20
Hello Time      : 2
Forward Delay   : 15
Max Hops        : 20
TX Hold Count   : 6
Forwarding BPDU : Enabled

#
```

ステータス 3: MSTP に対し有効にされた STP

```
#show stp
Command: show stp

STP Bridge Global Settings
-----
STP Status      : Enabled
STP Version     : MSTP
Max Age         : 20
Forward Delay   : 15
Max Hops        : 20
TX Hold Count   : 6
Forwarding BPDU : Enabled

#
```

3.21.13 show stp ports

目的	スイッチ現在設定されている STP ポートコンフィギュレーションを表示します。
構文	show stp ports [<portlist>] [instance <value 0-4>]
説明	本コマンドは、特定のポートまたはポートグループに対する STP ポート設定を表示します。
パラメーター	<p><portlist> - 表示するポートまたはポート範囲を指定します。1つのポート情報が表示されます。ポートを指定しない場合、ポート1のSTP情報が表示されます。スペースバー、「p」および「n」キーを使用して、残りのポートの情報を表示します。</p> <p>instance <value 0-4> - 事前に設定した instance_id に対応する ID を 0 ~ 4 の間で入力します。0 のインスタンスは、スイッチの内部に設定したデフォルトの instance_id (CIST) を示します。</p>
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ポート1のSTPポート情報を表示するには (スイッチに有効なSTP)

```
#show stp ports
Command: show stp ports

MSTP Port Information
-----
Port Index      : 1      , Hello Time: 2 /2 , Port STP Enabled  ,
Restricted role  : False, Restricted TCN : False
External PathCost : Auto/200000  , Edge Port : Auto /No , P2P : Auto /Yes
Port Forward BPDU : Enabled
MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
-----
0      N/A                  200000            128   Disabled    Disabled

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

3.21.14 show stp instance

目的	スイッチの STP インスタンスコンフィギュレーションを表示します。
構文	show stp instance [<value 0-4>]
説明	本コマンドは、スイッチの現在の STP インスタンス設定と STP インスタンスの動作状態を表示します。
パラメーター	<value 0-4> - スイッチに設定済みの instance_id を入力します。0のエントリーは、スイッチの内部に設定されている CIST の STP コンフィギュレーションを表示します。
制限事項	なし
対応バージョン	1.00.00 以降

使用例: スイッチのインスタンス 0 (内部 CIST) に対する STP インスタンスコンフィギュレーションを表示するには

```
#show stp instance 0
Command: show stp instance 0

STP Instance Settings
-----
Instance Type      : CIST
Instance Status    : Enabled
Instance Priority   : 32768(Bridge Priority : 32768, sys ID ext : 0 )

STP Instance Operational Status
-----
Designated Root Bridge : 32766/00-40-66-39-78-E2
External Root Cost      : 200012
Regional Root Bridge    : 32768/00-40-66-1A-33-24
Internal Root Cost      : 0
Designated Bridge       : 32768/00-40-66-71-20-D6
Root Port                : 1
Max Age                 : 20
Forward Delay           : 15
Last Topology Change    : 856
Topology Changes Count  : 2987

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

3.21.15 show stp mst_config_id

目的	MSTP コンフィギュレーション ID を表示します。
構文	show stp mst_config_id
説明	本コマンドは、スイッチの現在の MSTP コンフィギュレーション ID を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに現在設定されている MSTP コンフィギュレーション ID を表示するには

```
#show stp mst_config_id
```

```
Command: show stp mst_config_id
```

```
Current MST Configuration Identification
```

```
-----
```

```
Configuration Name : 00:40:66:1A:33:24          Revision Level :0
```

```
MSTI ID          VID list
```

```
-----
```

```
    CIST          1-4094
```

```
#
```


3.22 パケットストーム制御コマンド

コンピュータネットワーク上にはマルチキャストやブロードキャストなどのパケットが絶えずあふれています。このトラフィックはネットワーク上の端末の不良や、故障したネットワークカードなどの誤動作によって増加することもあります。その結果、スイッチの処理能力問題が発生し、ネットワーク全体のパフォーマンスに影響を与えることがあります。本スイッチではこのパケットストーム状況を監視し制御することが可能です。

パケットストーム制御では、スイッチに入力されたパケットのスキャンを行い、ユーザーが指定した閾値を監視し制御します。動作モードには「drop」または「shutdown」を指定することができます。

「drop」オプションでは、スイッチのチップカウンタをインターバル時間毎に監視し、閾値を超えた分のパケットは次に監視する間まで破棄されます。監視の対象となるパケットストームは、ブロードキャストとマルチキャスト、宛先不明のユニキャストパケットです。

「Shutdown」オプションでは、ブロードキャストとマルチキャストを対象にスイッチのチップカウンタをインターバル時間毎に監視し、「countdown」オプションで指定した時間内（0秒～1800秒）にパケットストームが継続すると、ポート閉塞し、警告メッセージを出力します。

閉塞したポートの復旧には、(1)10秒から300秒後の自動リカバリーを待つか、(2)手動コマンドにより復旧させる方法があります。手動コマンドで復旧するには、対象ポートのステータスを無効、有効に切り替える必要があります。

3.22.1 config traffic control

目的	ブロードキャスト/マルチキャスト/宛先不明のユニキャストパケットストーム制御を設定します。ハードウェアストーム制御に加え、ソフトウェアメカニズムがトラフィックレートのモニタリングをします。
構文	config traffic control <portlist> all > <broadcast <enable disable> multicast <enable disable> unicast <enable disable> action <drop shutdown> threshold <value 64-1000000> countdown <secs 0-1800> time_interval <secs 5-30> recover_time<secs 10-300> >
説明	本コマンドは、ブロードキャスト/マルチキャスト/宛先不明のユニキャストパケットストーム制御を設定します。ソフトウェアトラフィック制御メカニズムを追加することで、ハードウェアとソフトウェアの両メカニズムが使用できます。ソフトウェアの制御により、シャットダウン機能とスイッチのリカバリーを提供します。
パラメーター	<p><portlist> - トラフィック制御のために設定するポート範囲を指定します。</p> <p>all - スwitchのトラフィック制御のためにすべてのポートを設定するよう指定します。</p> <p>broadcast <enable disable> - ブロードキャストストーム制御を「enable」（有効）または「disable」（無効）にします。</p> <p>multicast <enable disable> - マルチキャストストーム制御を「enable」（有効）または「disable」（無効）にします。</p> <p>unicast <enable disable> - 宛先不明のユニキャストトラフィック制御を「enable」（有効）または「disable」（無効）にします。</p> <p>action - スwitchでパケットストームを検知した際の動作モードを設定します。動作モードには、「drop」または「shutdown」を指定することができます。</p> <p>drop - スwitchのハードウェアによるトラフィック制御により、パケットストームの発生を検知します。パケットストームが検知されると、状態が改善するまで閾</p>

	<p>値を超えた分のパケットを廃棄します。</p> <p>shutdown - スイッチのソフトウェアによるトラフィック制御により、パケットストームの発生を検知します。パケットストームが検出されると、ブロードキャストとマルチキャストを対象にスイッチのチップカウンタをカウントダウン時間監視します。さらにカウントダウンタイマー経過後もパケットストームが続く場合には、そのポートを閉塞します。閉塞したポートの復旧には、(1) 指定時間後の自動リカバリーを待つか、(2) 「config ports 1 state disable」および「config ports 1 state enable」コマンドを使用して手動でポートをリセットすることで復旧できます。</p> <p>threshold <value 64-1000000> - 指定されたトラフィックを制御する閾値です。drop モードの単位は Kbit/秒です。shutdown モードでの単位は packets/秒です。デフォルト値は drop モードで 64Kbit/秒です。</p> <p>time_interval - スイッチのチップ情報からトラフィック制御機能に送られるマルチキャストおよびブロードキャストパケットのカウント監視間隔を設定します。このパケットカウンタを監視することで、入力トラフィックが閾値を超過したことを検知します。</p> <p><secs 5-30> - Interval を 5~30 秒間隔に設定します。デフォルト値は 5 秒です。</p> <p>countdown - トラフィックストームが継続しているポートをシャットダウンするまでの時間(秒)を指定します。本パラメーターは、action フィールドで shutdown を指定し、ソフトウェアによるトラフィック制御を行う場合に有効です。</p> <p><secs 0-1800> - デフォルト値は「0」で、ポートはシャットダウンされません。シャットダウンするまでのスイッチが待機する時間(秒)を 1~1800 で指定します。1.07 以降から指定可能な時間が分から秒に変更されました。</p> <p>recover_time - shutdown モードにおけるストームの検知により閉塞されたポートを自動的に復旧するまでの待機時間を設定します。</p> <p><secs 10-300> - 自動復旧待機時間を 10 秒~300 秒に設定します。デフォルト値は「300」です。action パラメーターで drop モードを指定した場合には適用できません。</p> <p>1.07 以降から自動復旧待機時間を 10 秒~300 秒の範囲でユーザーが設定できるように変更されました。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート1~12に対してブロードキャストストーム閾値 64Kbit/秒・監視間隔 10 秒・カウンタダウン時間 0 秒・自動復旧時間 60 秒のトラフィック制御を設定するには

```
#config traffic control 1-12 broadcast enable action shutdown threshold 64 countdown 0
time_interval 10 recover_time 60
Command: config traffic control 1-12 broadcast enable action shutdown threshold 64 countdown
0 time_interval 10 recover_time 60

Success.

#
```

3.22.2 show traffic control

目的	現在のトラフィック制御設定を表示します。
構文	show traffic control [<portlist>]
説明	本コマンドは、スイッチの現在のストームトラフィック制御の設定を表示します。 1.07以降から Recover time のパラメータ追加により表示が追加されました。
パラメーター	<portlist> - トラフィック制御を表示するポートまたはポートリストを指定します。ポートリスト範囲の最初と最後の間に - を使用します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート1~4のトラフィック制御設定を表示するには

```
#show traffic control 1-4
Command: show traffic control 1-4

Port Thres   Broadcast Multicast Unicast  Action  Count Time   Recover
  hold   Storm    Storm    Storm          down  Interval time
-----
1    64     Enabled  Disabled  Disabled shutdown 0    10    60
2    64     Enabled  Disabled  Disabled shutdown 0    10    60
3    64     Enabled  Disabled  Disabled shutdown 0    10    60
4    64     Enabled  Disabled  Disabled shutdown 0    10    60

Total Entries : 4

#
```

3.23 ポートミラーリングコマンド

3.23.1 config mirror port

目的	スイッチにミラーポートを設定し、ネットワークスニファアや他のデバイスで指定したポートを通過するトラフィックを通信に全く影響することなく監視することができます。
構文	config mirror port <port> [<add delete> source ports <portlist> < rx tx both >]
説明	本コマンドは、ポート範囲が指定ポートに送信されるすべてのトラフィックを持つことを可能にし、ネットワークスニファアや他のデバイスがネットワークトラフィックをモニタリングすることができます。さらに、1方向または両方向に送受信されるトラフィックだけが受信ポートにミラーリングされるような指定も可能です。
パラメーター	<port> - Target ポート(ミラーパケットを送信するポート)を指定します。 <add delete> - source ports パラメーターに指定されるミラーポートを追加または削除する場合に指定します。 source ports - ミラーされるポートまたはポート範囲。 <portlist> - ミラーされるポートまたはポート範囲を指定します。すべてのトラフィックがコピーされ、Target ポートに送信されるポート範囲です。 rx - ポートまたはポートリスト内のポート範囲が受信するパケットのみをミラーリングします。 tx - ポートまたはポートリスト内のポート範囲が送信するパケットのみをミラーリングします。 both - ポートまたはポートリスト内のポートが送受信するすべてのパケットをミラーリングします。
制限事項	管理者アカウントのみ本コマンドを実行できます。 Target ポートは送信元ポートとして指定できません。
対応バージョン	1.00.00 以降



使用例: ミラーリングポートを追加するには

```
#config mirror port 1 add source ports 2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

#
```

注意事項

-  リンクアグリゲーションポートをミラーリングする場合、LAG 所属ポートの全てをミラー元として設定してください。
-  送信フレームのミラーリングでは、タグなしフレームの場合も送信フレームの VLAN タグ付きフレームでミラーリングします。



Target ポートに VLAN がアサインされている場合、Target ポートに接続したデバイスからのフレームは VLAN 内に送出されます。アサイン VLAN を削除することにより Target ポートからのフレーム送出を回避することができます。

3.23.2 enable mirror

目的	指定済みポートミラーリングコンフィギュレーションを有効にします。
構文	enable mirror
説明	本コマンドは以下の「disable mirror」と組み合わせて、スイッチにポートミラーリングコンフィギュレーションを入力した後に、ポートミラーリングコンフィギュレーションを変更せずにミラーリングを有効または無効にすることができます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例ミラーリングコンフィギュレーションを有効にするには

```
#enable mirror
Command: enable mirror

Success.

#
```

3.23.3 disable mirror

目的	指定済みポートミラーリングコンフィギュレーションを無効にします。
構文	disable mirror
説明	本コマンドは上記の「enable mirror」と組み合わせて、スイッチにポートミラーリング設定コンフィギュレーションを入力した後に、ポートミラーリングコンフィギュレーションを変更せずにミラーリングを有効または無効にすることができます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ミラーリングコンフィギュレーションを無効にするには

```
#disable mirror
Command: disable mirror

Success.

#
```

3.23.4 show mirror

目的	スイッチ上の現在のポートミラーリングコンフィギュレーションを表示します。
構文	show mirror
説明	本コマンドは、スイッチ上の現在のポートミラーリングコンフィギュレーションを表示します。
パラメーター	なし
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ミラーリングコンフィギュレーションを表示するには

```
#show mirror
Command: show mirror

Current Settings
Mirror Status : Enabled
Target Port   : 1
Mirrored Port :
                RX :
                TX : 5-7

#
```

3.24 ポートセキュリティコマンド

3.24.1 config port_security ports

目的	ポートのセキュリティを設定します。
構文	config port_security ports < <auth_portlist> all > < admin_state < enable disable > max_learning_addr <max_lock_no 0-64> lock_address_mode < DeleteOnTimeout DeleteOnReset Permanent> >
説明	本コマンドは、ポートのセキュリティ機能を設定します。 <auth_portlist>で指定されたポートのみが影響を受けます。
パラメーター	<auth_portlist> - 設定するポートまたはポート範囲を指定します。 all - スイッチのすべてのポートに対しポートセキュリティを設定します。 admin_state <enable disable> - リスト内のポートに対しポートセキュリティを「enable」（有効）または「disable」（無効）にします。 max_learning_addr <max_lock_no 0-64> - ポートへの FDB 内で動的にリストされる MAC アドレス数を制限します。 lock_address_mode <DeleteOnTimeout DeleteOnReset Permanent> - アドレスをロックする方法を示します。 次の3つのオプションがあります： DeleteOnTimeout - ロックされたアドレスは、エイジングタイム経過後に削除されます。 DeleteOnReset - ロックされたアドレスは、リセットが再起動されるまで削除されません。 Permanent - ロックされたアドレスは、エージアウトしません。
制限事項	管理者アカウントのみ本コマンドを実行できます。 ポートセキュリティ機能と WEB 認証機能のポート併用はできません。
対応バージョン	1.00.00 以降

使用例: ポートセキュリティを設定するには

```
#config port_security ports 1-5 admin_state enable max_learning_addr 5 lock_address_mode DeleteOnReset
Command: config port_security ports 1-5 admin_state enable max_learning_addr 5 lock_address_mode DeleteOnReset

Success.

#
```

注意事項



認証機能（MAC 認証、WEB 認証、802.1x 認証）とのポート併用はできません。

3.24.2 delete port_security_entry vlan_name

目的	MAC アドレス、ポート番号、および VLAN ID からポートセキュリティエントリを削除します。
構文	delete port_security_entry vlan_name <vlan_name 32> mac_address <macaddr> port <auth_port>
説明	学習済みの単一ポートセキュリティエントリをポート番号、VLAN 名および MAC アドレスごとに削除します。
パラメーター	<p>vlan name <vlan_name 32> - 削除するポートの対応する VLAN 名を入力します。</p> <p>mac_address <macaddr> - 学習済みで削除するポートに対応する MAC アドレスを入力します。</p> <p>port <auth_port> - 前に入力した MAC アドレスを学習しているポート番号を入力します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポートセキュリティを削除するには

<pre>#delete port_security_entry vlan_name default mac_address 00-04-66-10-2C-C7 port 6 Command: delete port_security_entry vlan_name default mac_address 00-04-66-10-2C-C7 port 6 Success. #</pre>

3.24.3 clear port_security_entry port

目的	学習したポートセキュリティ機能が動作している MAC アドレスを指定のポートからクリアします。
構文	clear port_security_entry port <auth_portlist>
説明	本コマンドは、指定のポート別にスイッチが学習した MAC アドレスエントリをクリアします。本コマンドは、ポートのセキュリティ機能のみに関係します。
パラメーター	<auth_portlist> - クリアするポートまたはポート範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポートごとにポートセキュリティエントリをクリアするには

<pre># clear port_security_entry port 6 Command: clear port_security_entry port 6 Success. #</pre>
--

3.24.4 show port_security

目的	現在のポートセキュリティ情報を表示します。
構文	show port_security [ports <auth_portlist>]
説明	本コマンドは、スイッチのポートのポートセキュリティ情報を表示します。表示される情報は、ポートセキュリティ、管理者の状態、学習するアドレスの最大数、およびロックモードを含みます。
パラメーター	<auth_portlist> - 参照するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: ポートセキュリティ情報を表示するには

```
#show port_security ports 1-10
Command: show port_security ports 1-10

Port_security Trap/Log : Disabled

Port   Admin State   Max. Learning Addr.   Lock Address Mode
----   -
1      Disabled      1                      DeleteOnTimeout
2      Disabled      1                      DeleteOnTimeout
3      Disabled      1                      DeleteOnTimeout
4      Disabled      1                      DeleteOnTimeout
5      Disabled      1                      DeleteOnTimeout
6      Disabled      1                      DeleteOnTimeout
7      Disabled      1                      DeleteOnTimeout
8      Disabled      1                      DeleteOnTimeout
9      Disabled      1                      DeleteOnTimeout
10     Disabled      1                      DeleteOnTimeout

#
```

3.25 プロトコル VLAN コマンド

3.25.1 create dot1v_protocol_group

目的	プロトコル VLAN 機能のプロトコルグループを作成します。
構文	create dot1v_protocol_group group_id <int 1-16> [group_name <name 32>]
説明	本コマンドは、プロトコル VLAN 機能のプロトコルグループを作成します。
パラメーター	group_id - プロトコルのセットを他のセットと識別するために使用するプロトコルグループの ID。 group_name - プロトコルグループ名。最大長は、半角英数字 32 文字です。グループ名が指定されないと、「ProtocolGroup+group_id」というグループ名が自動的に生成されます。例えば、group_id が 2 の場合に自動生成される名前は、「ProtocolGroup2」となります。自動生成された名前が既存のグループと重複すると、「ProtocolGroup+group_id+ALT+num」という代替名が使用されます。「num」は 1 から開始します。さらに重複すると、その次の数が代わりに使用されます。例： Group ID が 1 の場合、自動生成される名前は、「ProtocolGroup1」となります。 この名前が既に存在していると、「ProtocolGroup1ALT1」が代わりに使用されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: プロトコルグループを作成するには

```
# create dot1v_protocol_group group_id 1 group_name General_Group
Command: create dot1v_protocol_group group_id 1 group_name General_Group

Success.

#
```

3.25.2 config dot1v_protocol_group

目的	プロトコルグループにプロトコルを追加します。
構文	config dot1v_protocol_group < group_id <int 1-16> group_name <name 32> > < add protocol <ethernet_2 ieee802.3_snap> <hex> delete protocol <ethernet_2 ieee802.3_snap > <hex> >
説明	本コマンドは、プロトコルグループにプロトコルを追加します。
パラメーター	group_id - プロトコルのセットを他のセットと識別するために使用するプロトコルグループの ID。 Group_name - プロトコルグループ名。 protocol - フレームタイプおよびプロトコル値を指定します。 フレームタイプは、ethernet_2 または ieee802.3_snap を選択できます。 (フレームタイプ ieee802.3_11c には対応しておりません) プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。入力形式は16 ビット(2オクテット)の16進法で、0x0 から 0xFFFF です。 例： IPv4 は0x0800、IPv6 は0x86DD、ARP は0x0806 など。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: プロトコルグループ 1 にプロトコル IPv6 を追加するには

```
#config dot1v_protocol_group group_id 1 add protocol ethernet_2 0x86DD
Command: config dot1v_protocol_group group_id 1 add protocol ethernet_2 0x86DD

The protocol value configured to add will take effect on both frame types ethernet_2 and
ieee802.3_snap.

Success.

#
```

3.25.3 delete dot1v_protocol_group

目的	プロトコルグループからプロトコルを削除します。
構文	delete dot1v_protocol_group < group_id <int 1-16> group_name <name 32> all >
説明	本コマンドは、プロトコルグループからプロトコルを削除します。
パラメーター	group_id - 削除するグループ ID を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: プロトコルグループ 1 を削除するには

```
# delete dot1v_protocol_group group_id 1
Command: delete dot1v_protocol_group group_id 1

Success.

#
```

3.25.4 show dot1v_protocol_group

目的	プロトコルグループで定義されたプロトコルを表示します。
構文	show dot1v_protocol_group <group_id <int 1-16> group_name <name 32> >
説明	本コマンドは、プロトコルグループで定義されたプロトコルを表示します。
パラメーター	Group_id - 表示するグループ ID を指定します。グループ ID を指定しない場合、設定したすべてのプロトコルグループが表示されます。 Group_name - プロトコルグループ名。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: プロトコルグループ ID 1 を表示するには

```
# show dot1v_protocol_group group_id 1
Command: show dot1v_protocol_group group_id 1

Protocol Group ID Protocol Group Name          Frame Type      Protocol Value
-----
1                General_Group   EthernetII      86dd
1                General_Group   IEEE802.3 SNAP 86dd

Total Entries: 1

#
```

3.25.5 config port dot1v ports

目的	設定されているプロトコルグループに基づきポートリストから入力するタグなしパケットのために VLAN を割り当てます。
構文	config port dot1v ports <all> < add protocol_group < group_id <int 1-16> group_name <name 32> > < vlan <vlan_name 32> vlanid <int> > [priority <value 0-7>] delete protocol_group < group_id <int 1-16> all > >
説明	本コマンドは、設定されているプロトコルグループに基づきポートリストから入力するタグなしパケットのための VLAN を割り当てます。この割り当ては、「delete protocol_group」オプションを使用して削除できます。 優先度をコマンドで指定しない場合、デフォルトのポート優先度は、プロトコル VLAN によって分類されるタグなしパケットの優先度になります。
パラメーター	Group_id - プロトコルグループのグループ ID。 Group_name - プロトコルグループ名。 Vlan - ポートに本プロトコルグループを対応づける VLAN。 Vlan_id - VLAN ID を指定します。 Priority - プロトコルによって指定される VLAN に分類されたパケットに対応づけられる優先度を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: VLAN default を割り当てた全ポートにグループ ID 1 を設定するには

```
# config port dot1v ports all add protocol_group group_id 1 vlan default
Command: config port dot1v ports all add protocol_group group_id 1 vlan default

Success.

#
```

3.25.6 show port dot1v

目的	プロトコルグループに基づいたポートから入力するタグなしパケットに対応づけられる VLAN を表示します。
構文	show port dot1v [ports <portlist>]
説明	本コマンドは、プロトコルグループに基づいたポートから入力するタグなしパケットに対応付けられる VLAN を表示します。
パラメーター	Portlist - 表示するポート範囲を指定します。 指定しない場合、すべてのポートの情報が表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート1~2のプロトコルVLAN情報を表示するには

```
# show port dot1v ports 1-2
```

```
Command: show port dot1v ports 1-2
```

```
Port: 1
```

Protocol Group ID	VLAN Name	Protocol Priority
-----	-----	-----
3	default	-
4	VLAN300	-
5	marketing-1	-

```
Port: 2
```

Protocol Group ID	VLAN Name	Protocol Priority
-----	-----	-----
3	default	-
4	VLAN300	-
5	marketing-1	-

```
Total Entries: 6
```

```
#
```

3.26 Q-in-Q コマンド

3.26.1 enable qinq

目的	本コマンドは、Q-in-Q モードを有効にします。
構文	enable qinq
説明	本コマンドは、Q-in-Q モードを有効にします。 Q-in-Q を有効にすると、すべてのネットワークポートの役割が NNI ポートとなり、外部 TPID が 88a8 に設定されます。既存のスタティック VLAN はすべて SP-VLAN となります。動的に学習したすべての L2 アドレスは、クリアされます。GVRP および STP は手動で無効にする必要があります。 スイッチの GVRP を実行する必要がある場合は、まず最初に、手動で GVRP を有効にします。Q-in-Q のデフォルト値は、「disable」（無効）です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Q-in-Q を有効にするには

```
#enable qinq
Command: enable qinq

Success.

#
```

3.26.2 disable qinq

目的	本コマンドは、Q-in-Q モードを無効にします。
構文	disable qinq
説明	本コマンドは、Q-in-Q モードを無効にします。 動的に学習したすべての L2 アドレスは、クリアされます。動的に登録したすべての VLAN エントリーはクリアされ、GVRP は「disable」（無効）になります。 スイッチの GVRP を実行する必要がある場合は、まず最初に、手動で GVRP を有効にします。既存の SP-VLAN はすべてスタティック IQ VLAN として実行します。 Q-in-Q のデフォルト値は、「disable」（無効）です。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:Q-in-Q を無効にするには

```
#disable qinq
Command: disable qinq

Success.

#
```

3.26.3 show qinq

目的	グローバル Q-in-Q を表示します。
構文	show qinq
説明	本コマンドは、グローバル Q-in-Q ステータスを表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: グローバル Q-in-Q のステータスを表示するには

```
#show qinq
Command: show qinq

QinQ Status: Enabled

#
```

3.26.4 show qinq ports

目的	グローバル Q-in-Q およびポート Q-in-Q モードのステータスを表示します。
構文	show qinq ports [<portlist>]
説明	本コマンドは、以下を含むグローバル Q-in-Q ステータスを表示します。 Q-in-Q モードでのポートの役割およびポート外部 TPID。
パラメーター	<portlist> - 表示するポート範囲を指定します。 パラメーターを指定しない場合、システムはすべての Q-in-Q ポート情報を表示します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1~4 の Q-in-Q ステータスを表示するには

```
#show qinq ports 1-4
Commands: show qinq ports 1-4

Port  Role  Outer  TPID  Trust_CVID  VLAN  Translation
-----
1      NNI    0x88a8  Disabled  Disabled
2      NNI    0x88a8  Disabled  Disabled
3      NNI    0x88a8  Disabled  Disabled
4      NNI    0x88a8  Disabled  Disabled

Total Entries   : 4

#
```


3.26.5 config qinq ports

目的	Q-in-Q ポートを設定します。
構文	config qinq ports < <portlist> all > [role < nni uni > outer_tpid <hex 0x1 - 0xffff> trust_cvid < enable disable > vlan_translation < enable disable > >
説明	本コマンドは、VLAN 機能のポートレベル設定を行います。Q-in-Q モードが無効であるとき、本設定は有効ではありません。
パラメーター	<portlist> - 設定するポート範囲。 role - Q-in-Q モードでのポートの役割。UNI ポートまたは NNI ポートのいずれかを選択します。 outer_tpid - SP-VLAN タグの TPID。 trust_cvid - C-Tag パケットに対し、C-VID は S-VID が有効かどうかを判断します。デフォルトでは「disable」（無効）に設定されています。 vlan_translation - 有効と指定された場合、VLAN トランスレーションがそのポートで実行されます。設定値は、デフォルトにより「disable」（無効）です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1~4 を NNI ポートとして設定し、アウターTPID を 0x88a8 に設定するには

```
#config qinq ports 1-4 role nni outer_tpid 0x88a8
Command: config qinq ports 1-4 role nni outer_tpid 0x88a8

Warning: The outer TPID will be globally applied to all ports!

Success.

#
```

3.26.6 create vlan_translation

目的	新しいルールとして追加される VLAN トランスレーションルールを作成するか、現在のルールを置換します。
構文	create vlan_translation < add cvid <vidlist> svid <vlanid 1-4094> replace cvid <vlanid 1-4094> svid <vlanid 1-4094> >
説明	本コマンドは、VLAN トランスレーションルールを作成して単一 S タグの送信パケットを追加または置換します (C-VID は S-VID に変更し、パケットの TPID はアウターTPID に変更します)。
パラメーター	cvid - UNI ポートからインGRESSするパケットの C-VLAN ID。 svid - C-VLAN ID を置換する、またはパケットに挿入される S-VLAN ID。 <vlanid 1-4094> - 1 ~ 4094 の範囲の VLAN ID。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:S-VLAN 100 を C-VLAN 1-10 に追加の割り当てをする VLAN トランスレーションルールを作成するには

```
#create vlan_translation add cvid 1-10 svid 100
Command: create vlan_translation add cvid 1-10 svid 100

Success.

#
```

3.26.7 delete vlan_translation cvid

目的	VLAN トランスレーションルールを削除します。
構文	delete vlan_translation cvid < <vidlist> all >
説明	本コマンドは、VLAN トランスレーションルールを削除します。
パラメーター	cvid - VLAN トランスレーションの C-VID ルールを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべての C-VID VLAN トランスレーションルールを削除するには

```
#delete vlan_translation cvid all

Command: delete vlan_translation cvid all

Success.

#
```

3.26.8 show vlan_translation cvid

目的	VLAN トランスレーションルールを表示します。
構文	show vlan_translation cvid [<vidlist>]
説明	本コマンドは、設定済み VLAN トランスレーションコンフィギュレーションを表示します。
パラメーター	cvid - 指定した C-VID リストの Q-in-Q トランスレーションルール。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:C-VID 10~C-VID 40のVLANトランスレーションルールを表示するには

```
#show vlan_translation cvid 10-40  
Command: show vlan_translation cvid 10-40
```

CVID	SVID	Action
-----	-----	-----
10	100	Add
20	100	Add
30	200	Add
40	400	Replace

Total Entries: 4

```
#
```

3.27 トラフィックセグメンテーションコマンド

トラフィックセグメンテーションで、細分化した VLAN をさらに小さいポートグループに分割することで VLAN のトラフィックを軽減します。VLAN ルールが優先され、次に、トラフィックセグメンテーションルールが適用されます。

3.27.1 config traffic_segmentation

目的	スイッチのトラフィックセグメンテーションを設定します。
構文	config traffic_segmentation <portlist> forward_list < null <portlist> >
説明	本コマンドは、スイッチにトラフィックセグメンテーションを設定します。
パラメーター	<portlist> - トラフィックセグメンテーションを設定するポートまたはポート範囲を指定します。 forward_list - 上で指定されたポートから転送されたフレームを受信するポートまたはポート範囲を指定します。 null - ポートは指定されません。 <portlist> - 転送リストのポート範囲を指定します。このリストはトラフィックセグメンテーション用として指定済みの同一スイッチ上にある必要があります (例: 上の config traffic_segmentation で指定した<portlist>)。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 11~15 にフレームを転送するために、ポート 1~10 を設定するには

```
#config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

#
```

3.27.2 show traffic_segmentation

目的	スイッチ上の現在のトラフィックセグメンテーションのコンフィギュレーションを表示します。
構文	show traffic_segmentation [<portlist>]
説明	本コマンドは、スイッチの現在のトラフィックセグメンテーションのコンフィギュレーションを表示します。
パラメーター	<portlist> - スwitchの現在のトラフィックセグメンテーションコンフィギュレーションが表示されるポートまたはポート範囲を指定します。
制限事項	セグメンテーション用ポートリストおよび転送リストは同一スイッチ上になければなりません。

使用例: スイッチ上の現在のトラフィックセグメンテーションのコンフィギュレーションを表示するには

```
#show traffic_segmentation
```

```
Command: show traffic_segmentation
```

```
Traffic Segmentation Table
```

```
Port      Forward Portlist
```

```
-----
```

```
1         1-28
```

```
2         1-28
```

```
3         1-28
```

```
4         1-28
```

```
5         1-28
```

```
6         1-28
```

```
7         1-28
```

```
8         1-28
```

```
9         1-28
```

```
10        1-28
```

```
11        1-28
```

```
12        1-28
```

```
13        1-28
```

```
14        1-28
```

```
15        1-28
```

```
16        1-28
```

```
17        1-28
```

```
18        1-28
```

```
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.28 VLAN コマンド

3.28.1 create vlan

目的	スイッチの VLAN を作成にします。
構文	create vlan <vlan_name 32> tag <vlanid 1-4094> [advertisement]
説明	本コマンドは、スイッチに VLAN を作成します。
パラメーター	<vlan_name 32> - 作成する VLAN 名。 <vlanid 1-4094> - 作成する VLAN の VLAN ID(1-4094)。 advertisement - VLAN が GVRP に連携できるように指定します。本パラメーターが設定されないと、スイッチは VLAN に関するすべての GVRP メッセージを送信することができません。
制限事項	管理者アカウントのみ本コマンドを実行できます。 各 VLAN 名は 32 文字以内で指定します。コンフィギュレーションごとに最大 4094 まで VLAN を作成できます。
対応バージョン	1.00.00 以降

使用例: VLAN 「v1」、 「tag 2」を作成するには

```
#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

#
```

3.28.2 delete vlan

目的	スイッチに設定済みの VLAN を削除します。
構文	delete vlan <vlan_name 32> vlanid <vidlist>
説明	本コマンドは、スイッチに設定済みの VLAN を削除します。
パラメーター	<vlan_name 32> - 削除する VLAN の VLAN 名。 <vidlist> - 削除する複数の VLAN ID 範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: VLAN 「v1」を削除するには

```
#delete vlan v1
Command: delete vlan v1

Success.

#
```

3.28.3 config vlan

目的	設定済みの VLAN にポートを追加します。
構文	config vlan <vlan_name 32> << add < tagged untagged forbidden > delete > <portlist> advertisement < enable disable > >
説明	本コマンドは、設定済み VLAN のポートリストにポートを追加します。追加ポートに「tagging」（タグ付き）、「untagging」（タグなし）、「forbidden」（禁止）の指定ができます。デフォルトによりポートは「untagging」（タグなし）として割り当てられます。
パラメーター	<p><vlan_name 32> - ポートを追加する VLAN 名。</p> <p>add - 「add」パラメーターを入力すると、VLAN にポートを追加します。追加するポートには3つのタイプがあります。</p> <p>tagged - 追加ポートをタグ付きとして指定します。</p> <p>untagged - 追加ポートをタグなしとして指定します。</p> <p>forbidden - 追加ポートを禁止ポートとして指定します。</p> <p>delete - 指定した VLAN からポートを削除します。</p> <p><portlist> - 指定した VLAN に追加する、または削除するポートまたはポート範囲を指定します。</p> <p>advertisement <enable disable> - 指定した VLAN 上の GVRP を「enable」（有効）または「disable」（無効）にします。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:4~8 のポートをタグ付きポートとして VLAN 「v1」に追加するには

```
#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

#
```

使用例:VLAN からポートを削除するには

```
#config vlan v1 delete 6-8
Command: config vlan v1 delete 6-8

Success.

#
```

注意事項



ポートには複数のタグなし VLAN を割り当てることができます。複数の VLAN がアサインされたポートでは、タグなしフレームを受信した場合にポート VLAN ID(PVID)により送信する VLAN を決めます。

3.28.4 create vlan vlanid

目的	スイッチに複数の VLAN ID を作成して VLAN を作成します。
構文	create vlan vlanid <vidlist> [advertisement]
説明	本コマンドは、スイッチに複数の VLAN を作成します。
パラメーター	<vidlist> - 作成する複数の VLAN ID 範囲を指定します。 advertisement - GVRP に連携するかどうか指定します。連携しない場合、VLAN は動的に連携できません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチに VLAN ID を作成するには

```
#create vlan vlanid 5-6 advertisement
Command: create vlan vlanid 5-6 advertisement

Success

#
```

3.28.5 delete vlan vlanid

目的	スイッチに設定された複数の VLAN を VLAN ID によって削除します。
構文	delete vlan vlanid <vidlist>
説明	本コマンドは、スイッチに設定済みの複数の VLAN を削除します。
パラメーター	<vidlist> - 削除する複数の VLAN ID 範囲を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチの VLAN ID を削除するには

```
#delete vlan vlanid 5-6
Command: delete vlan vlanid 5-6

Success

#
```


3.28.6 config vlan vlanid

目的	設定済みの VLAN にポートを追加します。
構文	config vlan vlanid <vidlist> < <add < tagged untagged forbidden > delete > <portlist> advertisement < enable disable > name <vlan_name 32> >
説明	本コマンドは、設定済み VLAN のポートリストにポートを追加または削除します。追加ポートに「tagged」（タグ付き）、「untagged」（タグなし）、「forbidden」（禁止）の指定をします。同一ポートを「untagged」（タグなし）として複数の VLAN のメンバポートにすることもできます。 advertisement パラメータを使用してポートが GVRP に連携するかどうかも指定できます。「name」パラメータで変更の必要のある VLAN の名前を設定します。
パラメーター	<vidlist> - 設定する複数 VLAN ID の範囲を設定します。 tagged - 追加ポートをタグ付きとして指定します。 untagged - 追加ポートをタグなしとして指定します。 forbidden - 追加ポートを禁止ポートとして指定します。 <portlist> - VLAN に追加するポート範囲。 advertisement - ポートを GVRP に連携させる場合、「advertisement」パラメータを入力します。次の 2 つのパラメータがあります： enable - ポートを GVRP に連携させます。 disable - ポートを GVRP に連携させません。 name - 「name」のパラメータを入力し、変更する VLAN の名前を設定します。 <vlan_name 32> - VLAN の名前を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチに設定済みの VLAN にポートを追加するには

```
#config vlan vlanid 5 add tagged 7 advertisement enable name HCL
Command: config vlan vlanid 5 add tagged 7 advertisement enable name HCL

Success.

#
```

注意事項



同一ポートにアサインするタグなし VLAN が 1 つだけの場合、PVID を意識する必要はありません。明示的に 1 つのアサインをお勧めします。非対称 VLAN やプロトコル VLAN などの機能においては、複数のタグなし VLAN をアサインするため、PVID を意識する必要があります。

3.28.7 enable pvid auto_assign

目的	PVIDの自動割り当てを有効にします。
構文	enable pvid auto_assign
説明	本コマンドは、PVIDの自動割り当てを有効にします。
パラメーター	なし。 デフォルト値は有効(enable)です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:PVIDの自動割り当てを有効にするには

```
#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

#
```

3.28.8 disable pvid auto_assign

目的	PVIDの自動割り当てを無効にします。
構文	disable pvid auto_assign
説明	本コマンドは、PVIDの自動割り当てを無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:PVIDの自動割り当てを無効にするには

```
#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

#
```

3.28.9 show pvid auto_assign

目的	PVIDの自動割り当てステータスを表示します。
構文	show pvid auto_assign
説明	本コマンドは、PVIDの自動割り当てステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00以降

使用例:PVIDの自動割り当てステータスを表示するには

```
#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

#
```

3.28.10 config gvrp

目的	スイッチに GVRP を設定します。
構文	config gvrp < <portlist> all > < state < enable disable > ingress_checking < enable disable > acceptable_frame < tagged_only admit_all > pvid <vlanid 1-4094> >
説明	本コマンドは、スイッチに Group VLAN Registration Protocol を設定します。 イングレスチェック、GVRP 情報の送受信、およびポート VLAN ID (PVID) を設定できます。
パラメーター	<portlist> - GVRP を有効にするポートまたはポート範囲を指定します。 all - スイッチのすべてのポートを設定します。 state <enable disable> - ポートリストで指定したポートに GVRP 機能を「enable」(有効)または「disable」(無効)にします。 ingress_checking <enable disable> - 指定されたポートリストに対するイングレスチェックを「enable」(有効)または「disable」(無効)にします。 acceptable_frame <tagged_only admit_all> - 本機能のためにスイッチが受け入れるフレームタイプを示します。tagged_only は、タグ付きの VLAN フレームだけを受け入れることを示します。一方、admit_all は、タグ付きおよびタグなしフレームを受け入れることを示します。 pvid <vlanid 1-4094> - ポートに関連するデフォルトの VLAN ID を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:イングレスチェック状態および GVRP 情報の送受信を設定するには

```
#config gvrp 1-4 state enable ingress_checking enable acceptable_frame tagged_only pvid 2
Command: config gvrp 1-4 state enable ingress_checking enable acceptable_frame tagged_only pvid 2

Success.

#
```

3.28.11 enable gvrp

目的	スイッチの GVRP を有効にします。
構文	enable gvrp
説明	下の disable gvrp を併せた本コマンドは、スイッチの GVRP コンフィギュレーションを変更しないで、スイッチの GVRP を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:一般的な VLAN Registration Protocol (GVRP) を有効にするには

```
#enable gvrp
Command: enable gvrp

Success.

#
```

3.28.12 disable gvrp

目的	スイッチの GVRP を無効にします。
構文	disable gvrp
説明	enable gvrp を併せた本コマンドは、スイッチの GVRP コンフィギュレーションを変更しないで、スイッチの GVRP を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:一般的な VLAN Registration Protocol (GVRP) を無効にするには

```
#disable gvrp
Command: disable gvrp

Success.

#
```

3.28.13 show vlan

目的	スイッチに設定された現在の VLAN 設定を表示します。
構文	show vlan < <vlan_name 32> vlanid <vidlist> ports <portlist> >
説明	本コマンドは、VLAN ID、VLAN 名、VLAN タイプ、タグ付き/タグなしステータス、および VLAN のメンバである各ポートの Member/Non-member/Forbidden ステータスを含む各 VLAN に関するサマリー情報を表示します。
パラメーター	<vlan_name 32> - サマリー設定を表示する VLAN 名。 vlanid <vidlist> - 表示する複数の VLAN ID 範囲を指定します。 ports <portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチの現在の VLAN 設定を表示するには

```
#show vlan
Command: show vlan
VID          : 1          VLAN Name     : default
VLAN Type    : Static    Advertisement : Enabled
Member Ports : 1-10
Static Ports : 1-10
Current Tagged Ports :
Current Untagged Ports : 1-10
Static Tagged Ports :
Static Untagged Ports : 1-10
Forbidden Ports :

Total Entries : 1

#
```

使用例: スイッチの現在の VLAN 設定を表示するには

```
#show vlan port 1
Command: show vlan ports 1

Port 1
VLAN ID  Untagged  Tagged  Forbidden  Dynamic
-----  -
1         X         -         -         -

#
```

3.28.14 show gvrp

目的	スイッチのポートリストの GVRP ステータスを表示します。
構文	show gvrp [<portlist>]
説明	本コマンドは、スイッチのポートリストの GVRP ステータスを表示します。
パラメーター	<portlist> - GVRP ステータスが表示されるポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:GVRP ポートステータスを表示するには

```
#show gvrp 1-10
Command: show gvrp 1-10

Global GVRP : Disabled

Port  PVID  Reassigned  GVRP      Ingress   Acceptable Frame Type
      PVID                State      Checking
-----
1     1     -           Disabled  Enabled   All Frames
2     1     -           Disabled  Enabled   All Frames
3     1     -           Disabled  Enabled   All Frames
4     1     -           Disabled  Enabled   All Frames
5     1     -           Disabled  Enabled   All Frames
6     1     -           Disabled  Enabled   All Frames
7     1     -           Disabled  Enabled   All Frames
8     1     -           Disabled  Enabled   All Frames
9     1     -           Disabled  Enabled   All Frames
10    1     -           Disabled  Enabled   All Frames

Total Entries : 10
```

3.29 ARP コマンド

3.29.1 create arpentry

目的	ARP テーブルにスタティックエントリーを作成します。
構文	create arpentry <ipaddr> <macaddr>
説明	本コマンドは、スイッチの ARP テーブルに IP アドレスと対応する MAC アドレスを入力します。
パラメーター	<ipaddr> - ARP テーブルに登録する IP アドレス。 <macaddr> - 上記 IP アドレスに対応する MAC アドレス。
制限事項	管理者アカウントのみ本コマンドを実行できます。 スイッチは、255 までのスタティック ARP エントリーをサポートします。
対応バージョン	1.00.00 以降

使用例: IP アドレス「10.48.74.121」と MAC アドレス「00-40-66-00-07-36」のスタティック ARP エントリーを作成するには

```
#create arpentry 10.48.74.121 00-40-66-00-07-36
Command: create arpentry 10.48.74.121 00-40-66-00-07-36

Success.

#
```

3.29.2 config arpentry

目的	ARP テーブルにスタティックエントリーを設定します。
構文	config arpentry <ipaddr> <macaddr>
説明	本コマンドは、ARP テーブルにスタティックエントリーを設定します。スイッチの ARP テーブルのエントリーに IP アドレスと対応する MAC アドレスを指定できます。
パラメーター	<ipaddr> - ARP テーブルに登録する IP アドレス。 <macaddr> - 上記 IP アドレスに対応する MAC アドレス。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: IP アドレス「10.48.74.12」と MAC アドレス「00-40-66-00-07-36」のスタティック ARP エントリーを設定するには

```
#config arpentry 10.48.74.12 00-40-66-00-07-36
Command: config arpentry 10.48.74.12 00-40-66-00-07-36

Success.

#
```

3.29.3 delete arpentry

目的	ARP テーブルからスタティックエントリーを削除します。
構文	delete arpentry < <ipaddr> all >
説明	上記「create arpentry」コマンドで作成したスタティック ARP エントリーを、エントリーの IP アドレスまたは「all」を指定することにより削除します。 「all」を指定すると、スイッチの ARP テーブルはすべてクリアされます。
パラメーター	<ipaddr> - ARP テーブルから削除する IP アドレス。 all - ARP エントリーをすべて削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：IP アドレス「10.48.74.121」を ARP テーブルから削除するには

```
#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

#
```

3.29.4 config arp_aging time

目的	スイッチの ARP テーブルエントリーにエージアウトタイマーを設定します。
構文	config arp_aging time <value 0-65535>
説明	本コマンドは、ARP エントリーがアクセスされない状態で、スイッチの ARP テーブルに保存される最大時間(分)を設定します。
パラメーター	time <value 0-65535> - ARP エージングタイム(分)。値は 0 ~ 65535 の範囲から指定できます。デフォルト値は 20 分です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：ARP エージングアウトタイマーを設定するには

```
#config arp_aging time 30
Command: config arp_aging time 30

Success.

#
```


3.29.5 show arpentry

目的	ARP テーブルを表示します。
構文	show arpentry ipif System [ipaddress <ipaddr> static]
説明	本コマンドは、スイッチの ARP テーブルの現在の内容を表示します。
パラメーター	ipaddress <ipaddr> - 上記 IP インターフェースに対応するネットワークアドレス。 static - ARP テーブルのスタティックエントリーを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例：ARP テーブルを表示するには

```
#show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface      IP Address      MAC Address      Type
-----
System         10.0.0.0        FF-FF-FF-FF-FF-FF Local/Broadcast
System         10.6.51.15     00-40-66-E7-B5-CD Dynamic
System         10.73.21.11    00-40-66-EF-78-B5 Local
System         10.255.255.255 FF-FF-FF-FF-FF-FF Local/Broadcast

Total Entries  : 4

#
```

3.29.6 clear arptable

目的	ダイナミック ARP テーブルエントリーをすべて削除します。
構文	clear arptable
説明	本コマンドは、スイッチの ARP テーブルからダイナミックエントリーを削除します。スタティック ARP テーブルエントリーは影響を受けません。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：ARP テーブルからダイナミックエントリーを削除するには

```
#clear arptable
Command: clear arptable

Success.

#
```

3.30 ルーティングテーブルコマンド

3.30.1 create iproute

目的	スイッチの IP ルーティングテーブルにデフォルト IP ルートエントリーを作成します。
構文	create iproute default <ipaddr> [<metric 1-65535>]
説明	本コマンドは、スイッチの IP ルーティングテーブルにデフォルトのスタティック IP ルートエントリーを作成します。
パラメーター	<ipaddr> - ネクストホップルーターのゲートウェイ IP アドレス。 <metric 1-65535> - スイッチと上記 IP アドレス間のルーターの数を表すルーティングプロトコルのメトリックエントリーを入力します。デフォルト値は「1」です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:メトリック値に「1」を使用して、スタティックアドレス「10.48.74.121」をルーティングテーブルに追加するには

<pre>#create iproute default 10.48.74.121 1 Command: create iproute default 10.48.74.121 1 Success. #</pre>

3.30.2 delete iproute

目的	スイッチの IP ルーティングテーブルからデフォルト IP ルートエントリーを削除します。
構文	delete iproute default
説明	本コマンドは、スイッチの IP ルーティングテーブルからデフォルトのスタティック IP ルートエントリーを削除します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:デフォルト IP ルートを削除するには

<pre>#delete iproute default Command: delete iproute default Success. #</pre>

3.30.3 show iproute

目的	スイッチ上の現在の IP ルーティングテーブルを表示します。
構文	show iproute [<network_address> static]
説明	本コマンドは、スイッチの現在の IP ルーティングテーブルを表示します。
パラメーター	<network_address> - ネットワーク IP アドレス。 static - スタティック IP ルートを選択します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: IP ルーティングテーブルの内容を表示するには

```
#show iproute
Command: show iproute

Routing Table

IP Address/Netmask      Gateway          Interface        Hops    Protocol
-----
0.0.0.0                 10.1.1.254      System           1       Default
10.0.0.0/8              10.48.74.122    System           1       Local

Total Entries: 2

#
```

3.30.4 create ipv6 neighbor_cache ipif

目的	IPv6 インターフェースにスタティックネイバーを追加します。
構文	create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
説明	本コマンドは、IPv6 インターフェースにスタティックネイバーを追加します。
パラメーター	<ipif_name> - インターフェース名を入力します。 <ipv6addr> - ネイバーのアドレスを入力します。 <macaddr> - ネイバーの MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: IPv6 インターフェースにスタティックネイバーを追加するには

```
#create ipv6 neighbor_cache ipif System fe80::20b:6aff:fece:7ec6 00-04-66-03-04-05
Command: create ipv6 neighbor_cache ipif System fe80::20b:6aff:fece:7ec6 00-04-66-03-04-05

Success.

#
```

3.30.5 delete ipv6 neighbor_cache ipif

目的	インターフェースネイバーアドレスキャッシュから IPv6 ネイバーを削除します。
構文	delete ipv6 neighbor_cache ipif < <ipif_name 12> all > < <ipv6addr> static dynamic all >
説明	本コマンドは、IPv6 インターフェースのネイバーキャッシュエントリー、もしくはスタティックネイバーキャッシュエントリーを削除します。スタティックもダイナミックも削除することができます。
パラメーター	<ipif_name> - IPv6 インターフェース名を入力します。 <ipv6addr> - ネイバーのアドレスを入力します。 all - スタティックおよびダイナミックエントリーを含むすべてのエントリーが削除されます。 static - スタティックエントリーを削除します。 dynamic - ダイナミックエントリーを削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ネイバーキャッシュを削除するには

<pre>#delete ipv6 neighbor_cache ipif System fe80::20b:6aff:fecf:7ec6 Command: delete ipv6 neighbor_cache ipif System fe80::20b:6aff:fecf:7ec6 Success. #</pre>

3.30.6 show ipv6 neighbor_cache ipif

目的	IPv6 ネイバーキャッシュを表示します。
構文	show ipv6 neighbor_cache ipif < <ipif_name 12> all > <ipv6address <ipv6addr> static dynamic all >
説明	本コマンドは、指定したインターフェースのネイバーキャッシュエントリーを表示します。指定したエントリー、すべてのエントリー、およびすべてのスタティックエントリーを表示します。
パラメーター	<ipif_name 12> - インターフェース名を入力します。 <ipv6addr> - アドレスを入力します。 static - スタティックエントリーを表示します。 dynamic - ダイナミックエントリーを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: インターフェースシステムのネイバーを表示するには

```
#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

Neighbor                Linklayer Address    Interface    State
-----
fe80::20b:6aff:feef:7ec6  00:40:66:cf:7e:c6   System      R

State :
(I) means Incomplete State. (R) means Reachable State.
(S) means Stale State.      (D) means Delay State.
(P) means Probe State.     (T) means Static State.

#
```

3.30.7 create ipv6route

目的	IPv6 スタティックルートを作成します。
構文	create ipv6route <default> < <ipif_name 12> <ipv6addr> > [<metric 1-65535>]
説明	本コマンドは、IPv6 スタティックルートに使用します。ネクストホップがグローバルアドレスの場合、インターフェース名を指定する必要はありません。ネクストホップがリンクローカルアドレスの場合、インターフェース名を指定する必要があります。
パラメーター	default - デフォルトルートを指定します。 <ipif_name 12> - ルートのインターフェースを指定します。 <ipv6addr> - 本ルートのネクストホップアドレスを指定します。 <metric 1-65535> - スイッチと上記 IP アドレス間のルーターの数を表すルーティングプロトコルのメトリックエントリを入力します。 デフォルト値は「1」です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: メトリック値に「1」を使用して、スタティックアドレス「fe80::20b:6aff:feef:7ec6」をルーティングテーブルに追加するには

```
#create ipv6route default System fe80::20b:6aff:feef:7ec6
Command: create ipv6route default System fe80::20b:6aff:feef:7ec6

Success.

#
```

3.30.8 delete ipv6route

目的	IPv6 ルートを削除します。
構文	delete ipv6route < <default> < <ipif_name 12> <ipv6addr> all >
説明	本コマンドは、IPv6 スタティックルートに使用します。ネクストホップがグローバルアドレスの場合、インターフェース名を指定する必要はありません。ネクストホップがリンクローカルアドレスの場合、インターフェース名を指定する必要があります。
パラメーター	default - デフォルトルートを指定します。 <ipv6addr> - デフォルトルートのネクストホップアドレスを指定します。 all - 作成されたスタティックルートをすべて削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: IPv6 スタティックルートを削除するには

<pre>#delete ipv6route default fe80::20b:6aff:fece:7ec6 Command: delete ipv6route default fe80::20b:6aff:fece:7ec6 Success. #</pre>

3.30.9 show ipv6 nd

目的	インターフェースの情報を表示します。
構文	show ipv6 nd [ipif <ipif_name 12>]
説明	本コマンドは、IPv6 ND に関連した情報を表示します。
パラメーター	<ipif_name> - インターフェースの名前。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: インターフェースの情報を表示するには

<pre>#show ipv6 nd ipif System Command: show ipv6 nd ipif System Interface Name : System NS Retransmit Time : 0(ms) #</pre>

3.30.10 show ipv6route

目的	IPv6 ルートを表示します。
構文	show ipv6route
説明	本コマンドは、IPv6 ルートを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: すべての IPv6 ルートを表示するには

```
#show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                Protocol: Static  Metric: 1
Next Hop   : fe80::20b:6aff:fe6f:7ec6    IPIF   : System

Total Entries: 1

#
```

3.30.11 config ipv6 nd ns ipif

目的	ネイバーのソリシエーションに関連した引数を設定します。
構文	config ipv6 nd ns ipif <ipif name 12> retrans_time <uint 0-4294967295>
説明	本コマンドは、ネイバーのソリシエーションに関連した引数を設定します。
パラメーター	<ipif_name> - インターフェースの名前。 retrans_timer - ネイバーのソリシエーションを再送するまでの遅延時間(ミリ秒)。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: IPv6 nd ns インターフェースを設定するには

```
#config ipv6 nd ns ipif System retrans_time 10000
Command: config ipv6 nd ns ipif System retrans_time 100000

Success.

#
```

3.31 QoS コマンド

スイッチは、802.1p 優先キューをサポートします。スイッチには4つの優先キューがあります。これらの優先キューには、最高レベルの3番キュー（クラス3）から最低レベルの0番キュー（クラス0）までがあります。IEEE 802.1p (p0 から p7) に規定される8つの優先度タグはスイッチの優先度タグと以下のように関連付けされます。

- 優先度0は、スイッチのQ1キューに割り当てられます。
- 優先度1は、スイッチのQ0キューに割り当てられます。
- 優先度2は、スイッチのQ0キューに割り当てられます。
- 優先度3は、スイッチのQ1キューに割り当てられます。
- 優先度4は、スイッチのQ2キューに割り当てられます。
- 優先度5は、スイッチのQ2キューに割り当てられます。
- 優先度6は、スイッチのQ3キューに割り当てられます。
- 優先度7は、スイッチのQ3キューに割り当てられます。

優先度スケジューリングは上記の優先キューによって実装されます。スイッチは4個の優先キューを空にします。その順番は、最も高い優先キューの3から最も低い優先キューの0となります。各ハードウェアキューは次に低い優先度にパケットを送信する前にバッファのすべてのパケットを送信します。最も低いハードウェア優先キューがすべてのパケットの送信を完了すると、最も高いハードウェア優先キューは、受信しているすべてのパケットを再送信できるようになります。

3.31.1 config bandwidth_control

目的	ポートベースで帯域幅制御を設定します。
構文	config bandwidth_control <portlist> < rx_rate < no_limit <value 64-1024000> > > tx_rate < no_limit <value 64-1024000> > >
説明	本 コマンドは、ポートベースで帯域幅制御を設定します。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 rx_rate - 下のパラメーター(no_limit または<value 64-1024000>)を指定し、上で指定したポートがパケットを受信できる速度に適用させます。 no_limit - 指定ポートが受信するパケットの速度を制限しません。 <value 64-1024000> - 上記ポートで受信するトラフィック制限(Kbps)を指定します。 tx_rate - 下のパラメーター(no_limit または<value 64-1024000>)を指定し、上で指定したポートがパケットを送信できる速度に適用させます。 no_limit - 指定ポートが受信するパケットの速度を制限しません。 <value 64-1024000> - 上記ポートで受信するトラフィック制限(Kbps)を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 帯域幅制御を設定するには

```
#config bandwidth_control 1 rx_rate 64
```

```
Command: config bandwidth_control 1 rx_rate 64
```

Note: To perform precise bandwidth control, it is required to enable the flow control to mitigate the retransmission of TCP traffic.

The specified RX rate is not a multiple of 62.5, thus the closest smaller multiple 62.5 is chosen.

Success.

```
#
```

注意事項



設定範囲は 64-1024000Kbps となりますが、実際に設定される値は 62.5Kbps の倍数となるように自動的に調整されます。

3.31.2 show bandwidth_control

目的	帯域幅制御テーブルを表示します。
構文	show bandwidth_control [<portlist>]
説明	本コマンドは、スイッチの現在の帯域幅制御の設定をポート別に表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: 帯域幅制御設定を表示するには

```
#show bandwidth_control 1-5
```

```
Command: show bandwidth_control 1-5
```

Bandwidth Control Table

Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
1	no_limit	no_limit	no_limit	no_limit
2	no_limit	no_limit	no_limit	no_limit
3	no_limit	no_limit	no_limit	no_limit
4	no_limit	no_limit	no_limit	no_limit
5	no_limit	no_limit	no_limit	no_limit

```
#
```

3.31.3 config scheduling

目的	各 COS キューにトラフィックスケジューリングメカニズムを設定します。
構文	config scheduling <class_id 0-3> weight <value 1-55>
説明	スイッチには4つのハードウェア優先キューがあります。これら4つのキューのうち1つに入力パケットをマッピングする必要があります。本コマンドは、これらの4つのハードウェア優先キューが空にされている順番を指定します。スイッチのデフォルト値（「config scheduling」コマンドが使用されない場合）では、最も高い優先キュー（ハードウェアキュー3）から最も低い優先キュー（ハードウェアキュー0）まで順番にハードウェア優先キューを空にしていきます。各ハードウェアキューは、次に低い優先キューがパケット送信を許可するまで、バッファにすべてのパケットを送信します。最も低いハードウェア優先キューがすべてのパケットの転送を完了すると、最も高いハードウェア優先キューは、受信しているすべてのパケットの送信を開始します。 weight <value 1-55> - 重み付けされた COS キューのウェイトを指定します。1 ~ 55 の範囲で値を指定できます。
パラメーター	<class_id 0-3> - 「config scheduling」コマンドが4つのハードウェア優先キューのどれに適用されるかを指定します。4つのハードウェア優先キューは、最も低い優先度である0キューを持つ0から3の番号によって識別されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:各キューにトラフィックスケジューリングメカニズムを設定するには

```
# config scheduling 0 weight 55
Command: config scheduling 0 weight 55

Success.

#
```

3.31.4 show scheduling

目的	スイッチに現在設定されているトラフィックスケジューリングを表示します。
構文	show scheduling
説明	本コマンドは、スイッチの現在のトラフィックスケジューリングメカニズムを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:現在のスケジューリング設定を表示するには

```
#show scheduling
Command: show scheduling

QoS Output Scheduling

Class ID      Weight
-----      -
Class-0       1
Class-1       2
Class-2       4
Class-3       8

#
```

3.31.5 config scheduling_mechanism

目的	QoS 機能のスケジューリングメカニズムを設定します。
構文	config scheduling_mechanism < strict weight_fair >
説明	<p>本コマンドは、QoS 機能サービスの優先度クラスを空にするために weight fair と strict メカニズムから選択します。スイッチには 4 つのハードウェア優先度 CoS を含みます。これら 4 つのハードウェア優先度 CoS の 1 つに入力パケットをマップする必要があります。このコマンドは、これらの 4 つのハードウェア優先度 CoS が送信されるという循環を指定します。</p> <p>スイッチのデフォルト値は、最も高い優先キュー（キュー3）から-最も低い優先キュー（キュー0）まで順番にハードウェア優先度 CoS を送信していきます。各キューは、次に低い優先度 CoS がパケット送信を許可するまで、バッファにすべてのパケットを送信します。パケットがより高いサービスクラスで受信されると、次に低い CoS がパケットをキューに送信するように差し替えられます。より高い CoS に受信されるパケットは、より低いクラスがキューの送信が完了するまで送信されません。</p>
パラメーター	<p>strict - strict パラメーターを指定すると、上位の CoS キューからトラフィックを処理します。上位キューの送信が完了するまで下位キューからはパケットは送信されません。</p> <p>weight_fair - 「Weight fair」パラメーターを入力すると、優先度 CoS が重み付けされた順でパケットを処理します。パケットは均一に処理されることとなります。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 各 QoS キューにトラフィックスケジューリングメカニズムを設定するには

```
#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

#
```

3.31.6 show scheduling_mechanism

目的	スイッチの現在のトラフィックスケジューリングメカニズムを表示します。
構文	show scheduling_mechanism
説明	本コマンドは、スイッチの現在のトラフィックスケジューリングメカニズムを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スケジューリングメカニズムを表示するには

```
#show scheduling_mechanism
Command: show scheduling_mechanism

QoS Scheduling mechanism
CLASS ID  Mechanism
-----  -
Class-0   strict
Class-1   strict
Class-2   strict
Class-3   strict

#
```

3.31.7 config 802.1p user_priority

目的	スイッチで利用可能な4個のハードウェアキューの1つに入力パケットの802.1p ユーザー優先度をマップします。																											
構文	config 802.1p user_priority <priority 0-7> <class_id 0-3>																											
説明	<p>本コマンドは、802.1p ユーザー優先度に基づいて、入力パケットを4つの有効なハードウェア優先キューの1つにマップする方法を設定します。スイッチの初期状態では、以下の通り入力する802.1p ユーザー優先度の値を4つのハードウェア優先キューにマップします。</p> <table border="1"> <thead> <tr> <th>802.1p</th> <th>ハードウェアキュー</th> <th>備考</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>1</td> <td>中-低</td> </tr> <tr> <td>1</td> <td>0</td> <td>最低</td> </tr> <tr> <td>2</td> <td>0</td> <td>最低</td> </tr> <tr> <td>3</td> <td>1</td> <td>中-低</td> </tr> <tr> <td>4</td> <td>2</td> <td>中-高</td> </tr> <tr> <td>5</td> <td>2</td> <td>中-高</td> </tr> <tr> <td>6</td> <td>3</td> <td>最高</td> </tr> <tr> <td>7</td> <td>3</td> <td>最高</td> </tr> </tbody> </table> <p>このマッピングスキームは、IEEE 802.1Dに含まれる勧告に基づいています。このマッピングは、<class_id 0-3> (ハードウェアキューの番号) に対して802.1p ユーザー優先度を指定することで変更できます。</p>	802.1p	ハードウェアキュー	備考	0	1	中-低	1	0	最低	2	0	最低	3	1	中-低	4	2	中-高	5	2	中-高	6	3	最高	7	3	最高
802.1p	ハードウェアキュー	備考																										
0	1	中-低																										
1	0	最低																										
2	0	最低																										
3	1	中-低																										
4	2	中-高																										
5	2	中-高																										
6	3	最高																										
7	3	最高																										
パラメーター	<p><priority 0-7> - class_id (ハードウェアキューの番号)に連携させる802.1p ユーザー優先度。</p> <p><class_id 0-3> - スwitchのハードウェア優先キューの番号。本スイッチには、4個のハードウェア優先キューがあります。これらのキューは0(最も低い優先度)と3(最も高い優先度)の間で番号を付与されます。</p>																											
制限事項	管理者アカウントのみ本コマンドを実行できます。																											
対応バージョン	1.00.00以降																											

使用例: スwitchに802.1p ユーザー優先度を設定するには

```
#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

#
```

3.31.8 show 802.1p user_priority

目的	入力パケットの 802.1p ユーザー優先値とスイッチの 4 個のハードウェア優先キューとの現在のマッピングを表示します。
構文	show 802.1p user_priority
説明	本コマンドは、入力パケットの 802.1p 優先値とスイッチの 4 個のハードウェア優先キューの 1 つとの現在のマッピングを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:802.1p ユーザー優先度を表示するには

```
#show 802.1p user_priority
Command: show 802.1p user_priority
```

QoS Class of Traffic

```
Priority-0 -> <Class-1>
Priority-1 -> <Class-0>
Priority-2 -> <Class-0>
Priority-3 -> <Class-1>
Priority-4 -> <Class-2>
Priority-5 -> <Class-2>
Priority-6 -> <Class-3>
Priority-7 -> <Class-3>
```

#

3.31.9 config 802.1p default_priority

目的	スイッチに 802.1p デフォルトの優先度を設定します。 タグなしパケットをスイッチが受信すると、本コマンドで設定した優先度は、パケットの優先度フィールドに記載されます。
構文	config 802.1p default_priority <<portlist> all> <priority 0-7>
説明	本コマンドは、スイッチが受信したタグなしパケットのデフォルトの優先度処理に関する指定をします。本コマンドで入力された優先値は、パケットが 4 個のハードウェア優先キューのうちのどれに転送されるかを決定するために使用されます。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - スwitchのすべてのポートに適用します。 <priority 0-7> - スwitchまたはスSwitchのポート範囲が受信したタグなしパケットに割り当てる優先値。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチに 802.1p デフォルトの優先度を設定するには

```
#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

#
```

3.31.10 show 802.1p default_priority

目的	送信先に転送される前に入力するタグなしパケットに割り当てられている現在の 802.1p 優先値を表示します。
構文	show 802.1p default_priority [<portlist>]
説明	本コマンドは、送信先に転送される前に入力するタグなしパケットに割り当てられている現在の 802.1p 優先値を表示します。
パラメーター	<portlist> - 表示するポートまたはポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに 802.1p デフォルトの優先度コンフィギュレーションを表示するには

```
# show 802.1p default_priority
Command: show 802.1p default_priority

Port  Priority
----  -
1     0
2     0
3     0
4     0
5     0
6     0
7     0
8     0
9     0
10    0
11    0
12    0
13    0
14    0
15    0
16    0
17    0
18    0
19    0
20    0
```

21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0
#	

3.31.11 config cos mapping

目的	スイッチに適用する CoS ポートマッピング方法を設定します。
構文	config cos mapping ports < <portlist> all > < none < ethernet <802.1p> ip < tos dscp > > >
説明	本コマンドは、スイッチの Cos とポートのマッピング機能に対し、入力パケットが識別される方法を設定します。識別されたパケットは、適切な CoS キューに転送されます。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - すべてのポートを設定する場合に指定します。 none - 優先度ベースの CoS 機能をすべて無効にします。 ethernet - イーサネットフレームベースの優先度を有効にします。 802.1p - 「802.1p CoS」を有効にします。 ip - イーサネットフレームベースの優先度を有効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1 を CoS イネーブルとして設定するには

#config cos mapping ports 1 ethernet 802.1p Command: config cos mapping ports 1 ethernet 802.1p Success. #

3.31.12 show cos mapping

目的	CoS マッピングを表示します。
構文	show cos mapping [port <portlist>]
説明	本コマンドは、CoS マッピングの有効ポートと方法について表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。パラメーターを指定しない場合は、すべてのポートの優先度設定が表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:CoS マッピング情報を表示するには

```
#show cos mapping
Command: show cos mapping

Port  Ethernet_priority  IP_priority
-----
1      802.1p              off
2      802.1p              off
3      802.1p              off
4      802.1p              off
5      802.1p              off
6      802.1p              off
7      802.1p              off
8      802.1p              off
9      802.1p              off
10     802.1p              off
11     802.1p              off
12     802.1p              off
13     802.1p              off
14     802.1p              off
15     802.1p              off
16     802.1p              off
17     802.1p              off
18     802.1p              off
19     802.1p              off
20     802.1p              off

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.31.13 config cos tos value

目的	スイッチで利用可能な4つのハードウェアキューの1つに入力パケットのIPヘッダのToS値をマップします。
構文	config cos tos value <value 0-7> <class <class_id 0-3>>
説明	本コマンドは、ToSをトラフィッククラスマッピングに設定します。
パラメーター	<value 0-7> - トラフィッククラスに関連付けする入力パケットのToS値。 <class_id 0-3> - スイッチのハードウェア優先キューの番号。本スイッチには、4個のハードウェア優先キューがあります。これらのキューは0(最も低い優先度)と3(最も高い優先度)の間で番号を付与されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:TOS 5 をトラフィッククラス 1 マッピングに設定するには

```
#config cos tos value 5 class 1
Command: config cos tos value 5 class 1

Success.

#
```

注意事項



本コマンドには「cos」の記載がありますが、「cos」に関する設定は出来ません。

3.31.14 show cos tos

目的	トラフィッククラスマッピングをする TOS の値を表示します。
構文	show cos tos [value <value 0-7>]
説明	本コマンドは、ToS とトラフィッククラス マッピングの情報を表示します。
パラメーター	<value 0-7> - 入力パケットの TOS 値。パラメーターが指定されないと、トラフィッククラスマッピングのすべての ToS 値が表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:TOS 5 の TOS トラフィッククラスマッピングを表示するには

```
#show cos tos value 5
Command: show cos tos value 5

TOS value          Class
-----
5                   2

#
```

3.31.15 config dscp_mapping

目的	スイッチで利用可能な 4 個のハードウェアキューの 1 つに入力パケットの IP ヘッダの DSCP 値をマップします。
構文	config dscp_mapping dscp_value <value 0-63> < class <class_id 0-3> >
説明	本コマンドは、DSCP マッピングをトラフィッククラスに設定します。
パラメーター	<value 0-63> - クラス ID と関連付けする入力パケットの DSCP 値。 <class_id 0-3> - スイッチのハードウェア優先キューの番号。本スイッチには、4 個のハードウェア優先キューがあります。これらのキューは 0 (最も低い優先度) と 3(最も高い優先度)間で番号を付与されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:DSCP のトラフィッククラスマッピングを設定するには

```
#config dscp_mapping dscp_value 8 class 1
Command: config dscp_mapping dscp_value 8 class 1

Success.

#
```

3.31.16 show dscp_mapping

目的	トラフィッククラスマッピングをする DSCP の値を表示します。
構文	show dscp_mapping [dscp_value <value 0-63>]
説明	本コマンドは、DSCP トラフィッククラスマッピングの設定を表示します。
パラメーター	<value 0-63> - 入力パケットの DSCP 値。パラメーターの設定がされていない場合、トラフィッククラスへに全ての DSCP マッピングが表示されます。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:DSCP のトラフィッククラスマッピングを表示するには

```
#show dscp_mapping
Command: show dscp_mapping

DSCP   Class
-----
0       0
1       0
2       0
3       0
4       0
5       0
6       0
7       0
8       0
9       0
10      0
11      0
12      0
13      0
14      0
15      0
16      0
17      0
18      0
19      0

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.32 アクセス制御リスト (ACL) コマンド

スイッチはアクセス制御リストを使用して、IP アドレスおよび MAC アドレスに基づき特定のデバイスやデバイスグループへのネットワークアクセスを拒否できるようにします。

アクセスプロファイルを作成すると、各パケットヘッダの中の情報に従い、スイッチがパケット転送を決定するための基準を設定できるようになります。

アクセスプロファイルの作成は基本的に 2 つの部分に分かれます。最初に「create access_profile」コマンドを使用してアクセスプロファイルを作成します。例えば、サブネット 10.42.73.0 ~ 10.42.73.255 に対して全トラフィックを制限したい場合、はじめにスイッチに対して各フレームの関連フィールドすべてを調査するアクセスプロファイルを作成します。

最初に調査の基準として IP アドレスを使用するアクセスプロファイルを作成します。

```
create access_profile ip source_ip_mask 255.255.255.0 profile_id 1
```

この例では、スイッチが受信した各フレームの IP フィールドを調査するアクセスプロファイルを作成しました。スイッチが検出した各送信元 IP アドレスを論理積により source_ip_mask と照合します。profile_id パラメータを使用してアクセスプロファイルに識別番号を設定します。ここでは 1 を設定します。これは競合が生じたとき優先度を割り当てるために使用します。profile_id は、プロファイルリスト内で優先度を設定します。数字の小さい access_id ほど高い優先度が付与されます。アクセスプロファイルに登録したルール内に競合がある場合、最も高い優先度 (最も低い access_id) のルールが優先されます。アクセスプロファイルとアクセスルールの制限に関する情報は下記を参照してください。

スイッチは deny パラメータを使用して規準に合うフレームを廃棄します。ここでは、次のステップで指定する IP アドレスと ip_source_mask 照合の AND オペレーションです。

スイッチのアクセスプロファイルの初期値は、トラフィックフローを permit (許可) しています。トラフィックを制限するためには、deny (拒否) パラメータを使用する必要があります。

アクセスプロファイルの作成後、スイッチがある特定フレームの転送またはフィルタリングを決定するために基準を追加する必要があります。config access_profile コマンドを使用して、希望する基準を定義する新しいルールを作成します。さらに新しいルールで各ポートからある IP アドレスの範囲にアクセスを拒否するように指定する例を見てみましょう。この例では、10.42.73.0 ~ 10.42.73.255 の IP 送信元アドレスを持つパケットをフィルタリングし、許可しないポートを指定します。

```
config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny
```

アクセスプロファイルを作成したときに指定した「profile_id 1」を使用します。「add」パラメータはアクセスプロファイル 1 と関連付けられるルールリストに従う基準をスイッチに追加します。アクセスプロファイルに登録した各ルールに、ルールを識別し、ルールリスト内に優先度を設定する access_id を割り当てることができます。access_id はインデックス番号のみを意図し、profile_id 内での優先度に影響を与えません。access_id はユーザーがプロファイルから個々のルールを解除する場合に、後で使用できます。

ip パラメータはこの新しいルールが各フレームヘッダ内の IP アドレスに適用されるようにします。source_ip はこのルールを各フレームヘッダの送信元 IP アドレスに適用するようにスイッチに指示します。最後に、IP アドレス 10.42.73.1 は source_ip_mask 255.255.255.0 に統合し、10.42.73.0 と 10.42.73.255 の間の送信元 IP アドレスに IP アドレス 10.42.73.0 を与えます。最後に制限付きポート (ポート番号 7) が指定されます。

3.32.1 create access_profile

目的	<p>スイッチにアクセスプロファイルを作成し、入力するフレームの各ヘッダのどの部分をスイッチが調査するか定義します。スイッチが特定のフレームヘッダフィールドで見つける値と組み合わせてマスクを入力することができます。ルールに対する具体的な値は、下記の「config access_profile」コマンドを入力して指定します。</p>
構文	<pre>create access_profile < ethernet ip packet_content_mask ipv6 > profile_id <value 1-512> ethernet =ethernet < vlan [<hex 0x0-0x0fff>] source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type > ip =ip < vlan [<hex 0x0-0x0fff>] source_ip_mask <netmask> destination_ip_mask <netmask> dscp < icmp [type code] igmp [type] tcp [src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask < all < urg ack psh rst syn fin > >] udp < src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> > protocol_id_mask <0x0-0xff> > > packet_content_mask = packet_content_mask < destination_mac <macmask> source_mac <macmask> c_tag <hex 0x0-0xffff> s_tag <hex 0x0-0xffff> offset1 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset2 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset3 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset4 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset5 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset6 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset7 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset8 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset9 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset10 <12 13 14> <value 0-31> <hex 0x0-0xffff> offset11 <12 13 14> <value 0-31> <hex 0x0-0xffff> > > ipv6 =ipv6 < class flowlabel source_ipv6_mask< ipv6mask ::-::FFF:FFFF:FFFF> < tcp [src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>] udp [src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>] > ></pre>
説明	<p>本コマンドはスイッチにアクセスプロファイルを作成し、入力するフレームの各ヘッダのどの部分をスイッチが調査するか定義します。スイッチが特定のフレームヘッダフィールドで見つける値と組み合わせてマスクを入力することができます。ルールに対する具体的な値は、下記の「config access_profile」コマンドを入力して指定します。</p>

<p>パラメーター</p>	<p>ethernet - スイッチが各パケットヘッダのレイヤ 2 の部分を調査する場合に指定します。</p> <p>vlan - VLAN マスクを調査指定します。マスクの最後の 12 ビットのみが対象になります。</p> <p>source_mac <macmask> - 送信元 MAC アドレスの MAC アドレスマスクを指定します。このマスクは 16 進数形式入力されます。</p> <p>destination_mac <macmask> - 送信先 MAC アドレスの MAC アドレスマスクを指定します。</p> <p>802.1p - スイッチがフレームヘッダの 802.1p 優先値を調査する場合に指定します。</p> <p>ethernet_type - スイッチが各フレームヘッダのイーサネットタイプ値を調査する場合に指定します。</p> <p>ip - スイッチが各フレームヘッダの IP フィールドを調査する場合に指定します。</p> <p>source_ip_mask <netmask> - 送信元 IP アドレスの IP アドレスマスクを指定します。</p> <p>destination_ip_mask <netmask> - 送信先 IP アドレスの IP アドレスマスクを指定します。</p> <p>ip - スイッチが各フレームヘッダの DiffServ Code Point (DSCP) フィールドを調査する場合に指定します。</p> <p>icmp - スイッチが各フレームヘッダの Internet Control Message Protocol (ICMP) フィールドを調査する場合に指定します。</p> <p>type - スイッチが各フレームの ICMP タイプフィールドを調査する場合に指定します。</p> <p>code - スイッチが各フレームの ICMP Code フィールドを調査する場合に指定します。</p> <p>igmp - スイッチが各フレームの Internet Group Management Protocol (IGMP) フィールドを調査する場合に指定します。</p> <p>type - スイッチが各フレームの IGMP タイプフィールドを調査する場合に指定します。</p> <p>tcp - スイッチが各フレームの Transport Control Protocol (TCP) フィールドを調査する場合に指定します。</p> <p>src_port_mask <hex 0x0-0xffff> - 送信元ポートの TCP ポートマスクを指定します。</p> <p>dst_port_mask <hex 0x0-0xffff> - 送信先ポートの TCP ポートマスクを指定します。</p> <p>flag_mask - 適切な flag_mask パラメーターを入力します。すべての入力パケットは転送基準として TCP ポート番号を持っており、これらの番号はパケットをどうするかを決定するパケットの一部に関連する flag bit を持っています。パケット内の特定の flag bit を調査して、パケットを拒否します。all、urg (urgent)、ack (acknowledgement)、psh (push)、rst (reset)、syn (synchronize)、および fin (finish) から選択できます。</p> <p>udp - スイッチが各フレームの Universal Datagram Protocol (UDP) フィールドを調査する場合に指定します。</p>
---------------	---

パラメーター	<p>src_port_mask <hex 0x0-0xffff> - 送信元ポートの UDP ポートマスクを指定します。</p> <p>dst_port_mask <hex 0x0-0xffff> - 送信先ポートの UDP ポートマスクを指定します。</p> <p>protocol_id_mask - スイッチが各パケットのプロトコル ID フィールドを調査する場合に指定します。このフィールドにここで入力した値が含まれている場合は、以下のルールを適応します。</p> <p>ipv6 - IPv6 フィルタリングマスクを指定します。</p> <p>class - IPv6 クラスを指定します。</p> <p>flowlabel - IPv6 フローラベルを指定します。</p> <p>source_ipv6_mask - IPv6 送信元サブマスクを指定します。デバイスは、送信元 IPv6 アドレスの最後の 44 ビット (LSB)のフィルタリングのみをサポートします。</p> <p>src_port_mask - IPv6 L4 (TCP/UDP) 送信元ポートのサブマスクを指定します。</p> <p>dst_port_mask - IPv6 L4 (TCP/UDP) 送信先ポートサブマスクを指定します。</p> <p>packet_content_mask - 最大 11 のオフセットを指定できます。単一の UDF フィールドとして認識される 2 バイトのデータが各オフセットで設定できます。オフセットリファレンスも同様に設定可能です。タグの最後、タイプの最後または IP ヘッダの最後のいずれかから開始を指定できます。タグの最後の前でフィールドを許可するためには、送信先アドレス、送信元アドレス、VLAN タグも含まれます。</p> <p>source_mac - 送信元 MAC アドレスの MAC アドレスマスクを指定します。</p> <p>destination_mac - 送信先の MAC マスクを指定します。</p> <p>c_tag - マスクにパケットの 16 ビット内部 VLAN タグを指定します。これは 3 ビットの PCP、1 ビットの CFI、12 ビットの VID フィールドから構成されます。</p> <p>s_tag - マスクにパケットの 16 ビット外部 VLAN タグを指定します。これは 3 ビットの PCP、1 ビットの CFI、12 ビットの VID フィールドから構成されます。</p> <p>offset1 - offset11 - デバイスによってフィルタリングされる UDF フィールドを指定します。各 UDF フィールドはオフセットリファレンスから「n」バイト離れた 2 バイトのデータになります（「n」はオフセット値）。T オフセットは 0 から 31 の間で設定可能です。オフセットリファレンスは次のどれかになります。</p> <p>12 - オフセットは VLAN タグの後のバイトからカウントを開始します。(ether type」の始め)</p> <p>13 - オフセットは「ether type」フィールドのの後からカウントを開始します。パケットには有効な L2 ヘッダがあり識別順に「ether type」が判別されている必要があります。</p> <p>14 - オフセットは「ip header」の後からカウントを開始します。パケットは有効な IP ヘッダが識別順にある必要があります。</p> <p>例：「offset1 12 0 0xFFFF」は「ether type」の最初の 2 バイトがマスクされます。</p> <p>profile_id <value 1-512> - プロファイルに対応する優先度を設定します。優先度は他のプロファイルと比較して設定され、最も低いプロファイル ID が最も高い優先度を持ちます。1~512 の範囲でプロファイル ID を入力できます。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: アクセスリストルールを作成するには

```
#create access_profile ethernet vlan source_mac 00-00-00-00-00-01 destination_mac
00-00-00-00-00-02 802.1p ethernet_type profile_id 1
Command: create access_profile ethernet vlan source_mac 00-00-00-00-00-01 destination_mac
00-00-00-00-00-02 802.1p ethernet_type profile_id 1

Success.

#create access_profile ip vlan source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp
type code profile_id 2
Command: create access_profile ip vlan source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0
dscp icmp type code profile_id 2

Success.

#
```

3.32.2 delete access_profile

目的	作成済みのアクセスプロファイルを削除します。
構文	delete access_profile < profile_id <value 1-512> all >
説明	本コマンドは、スイッチに作成済みのアクセスプロファイルを削除します。
パラメーター	profile_id <value 1-512> - 本コマンドで削除するアクセスプロファイルを識別する番号を1～512の範囲で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。1～512の範囲でプロファイル ID 番号を入力できます。 all - 削除するすべてのアクセスリストプロファイルを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: プロファイル ID が 1 のアクセスプロファイルを削除するには

```
# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

#
```


3.32.3 config access_profile

<p>目的</p>	<p>スイッチにアクセスプロファイルを設定し、受信パケットを転送するか、フィルタリングするかを決めるためにスイッチが使用する値を定義します。</p> <p>「create access_profile」コマンドを使用して入力したマスクは論理積を使用し、指定したフレームのヘッダフィールド内にスイッチが検出した値と統合します。</p>
<p>構文</p>	<pre> config access_profile profile_id <value 1-512> < add access_id < auto_assign <value 1-65535> > < ethernet ip packet_content ipv6 > > delete access_id <value 1-65535> > ethernet =ethernet < < vlan <vlan_name 32> vlan_id <vid> > [mask <hex 0x0-0x0fff>] source_mac <macaddr> [mask <macmask>] destination_mac <macaddr> [mask <macmask>] 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff> > ip =ip [< vlan <vlan_name 32> vlan_id <vid> > [mask <hex 0x0-0x0fff>] destination_ip <ipaddr> [mask <netmask>] dscp <value 0-63> < icmp [type <value 0-255> code <value 0-255>] igmp [type <value 0-255>] tcp udp < src_port <value 0-65535> dst_port <value 0-65535>] protocol_id <value 0-255> > >] tcp =tcp [src_port <value 0-65535> [mask <hex 0x0-0xffff>] dst_port <value 0-65535> [mask <hex 0x0-0xffff>] flag < all < urg ack psh rst syn fin > >] udp =udp [src_port <value 0-65535> dst_port <value 0-65535>] packet_content =packet_content [destination_mac <macaddr> [mask <macmask>] source_mac <macaddr> [mask <macmask>] c_tag <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] s_tag <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset1 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset2 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset3 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset4 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset5 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset6 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset7 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset8 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset9 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset10 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>] offset11 <hex 0x0-0xffff> [mask <hex 0x0-0xffff>]] ipv6 =ipv6 [class <value 0-255> flowlabel <hex 0x0-0xffff> source_ipv6 <ipv6addr> [mask <ipv6mask>] < tcp [src_port < value 0-65535> [mask <hex 0x0-0xffff>] dst_port < value 0-65535>[mask <hex 0x0-0xffff>]] udp < src_port <value 0-65535> [mask <hex 0x0-0xffff>] dst_port <value 0-65535> [mask <hex 0x0-0xffff>] > >] > < port < <portlist> all > > < permit [priority <value 0-7> [replace_priority] replace_dscp_with <value0-63> counter < enable disable >] deny mirror > </pre>
<p>説明</p>	<p>本コマンドは、スイッチにアクセスプロファイルを設定し、上の「create access_profile」コマンドを使用して入力したマスク値は論理積を使用し、特定値を組み合わせて入力します。</p>

パラメーター	<p>profile_id <value 1-512> - 本コマンドで設定するアクセスプロファイルを識別する整数を入力します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。プロファイル ID は、他のプロファイルと比較した相対的な優先度を設定し、インデックス番号を指定します。このインデックス番号は本コマンドと共に作成され、アクセスプロファイルを識別します。優先度は他のプロファイルと比較して設定され、最も低いプロファイル ID が最も高い優先度を持ちます。1～512 の範囲でプロファイル ID 番号を入力できます。</p> <p>add access_id <value 1-65535> - 上で指定したアクセスプロファイルにルールを追加します。値は作成したルールのインデックスに使用されます。ポートに作成できるルールの数についての詳細は、本章のイントロダクションの項を参照してください。</p> <p>auto_assign - 本パラメーターは、設定するルールに自動的に数字（1～65535 の範囲）を割り当てます。</p> <p>ethernet - 以下のパラメーターに基づきパケットの廃棄または送信を決定するために各パケットのレイヤ 2 部分をスイッチが調査します。</p> <p>vlan <vlan_name 32> - 既に作成しているこの VLAN だけにアクセスプロファイルを適用します。</p> <p>vlan_id <vid> - 既に作成しているこの VLAN だけにアクセスプロファイルを適用します。</p> <p>source_mac <macaddr> - 送信元 MAC アドレスを持つパケットだけにアクセスプロファイルを適用します。</p> <p>destination_mac <macaddr> - 送信元 MAC アドレスを持つパケットだけにアクセスプロファイルを適用します。</p> <p>802.1p <value 0-7> - 802.1p 優先値を持つパケットだけにアクセスプロファイルを適用します。</p> <p>ethernet_type <hex 0x0-0xffff> - パケットヘッダ内に 16 進数の 802.1Q イーサネットタイプを持つパケットだけにアクセスプロファイルを適用します。</p> <p>ip - スイッチが各パケットの IP フィールドを調査する場合に指定します。</p> <p>vlan <vlan_name 32> - 既に作成しているこの VLAN だけにアクセスプロファイルを適用します。</p> <p>vlan_id <vid> - 本 VLAN ID を持つ VLAN だけにアクセスプロファイルを適用します。</p> <p>source_ip <ipaddr> - 送信元 IP アドレスを持つパケットだけにアクセスプロファイルを適用する場合に指定します。</p> <p>destination_ip <ipaddr> - アクセスプロファイルをこの送信先 IP アドレスを持つパケットにだけ適用します。</p> <p>type - スイッチが各フレームの IGMP タイプフィールドを調査する場合に指定します。</p> <p>tcp - 各パケット内の Transmission Control Protocol (TCP) フィールドを調査する場合に指定します。</p>
--------	---

<p>パラメーター</p>	<p>src_port <value 0-65535> - アクセスプロファイルを TCP ヘッダにこの TCP 送信元ポートを持つパケットにだけ適用します。</p> <p>dst_port <value 0-65535> - アクセスプロファイルを TCP ヘッダにこの TCP 送信先ポートを持つパケットにだけ適用します。</p> <p>flag - 対応する TCP フラグのタイプを入力します。</p> <p>all : すべてのフラグが選択されます。</p> <p>urg : TCP 制御フラグ(urgent : 緊急)</p> <p>ack : TCP 制御フラグ(acknowledgement : 承認)</p> <p>psh : TCP 制御フラグ(push : プッシュ)</p> <p>rst : TCP 制御フラグ(reset : リセット)</p> <p>syn : TCP 制御フラグ(synchronize : 同期化)</p> <p>fin : TCP 制御フラグ(finish : 終了)</p> <p>udp - 各パケットの Universal Datagram Protocol(UDP)フィールドを調査します。</p> <p>src_port <value 0-65535> - アクセスプロファイルはヘッダ内に本 UDP 送信元ポートを持つパケットにだけ適用します。</p> <p>dst_port <value 0-65535> - アクセスプロファイルはヘッダ内に本 UDP 送信先ポートを持つパケットにだけ適用します。</p> <p>protocol_id <value 0-255> - スイッチが各パケットのプロトコル ID フィールドを調査するように指定し、このフィールドにここで入力した値が含まれている場合、以下のルールを適用します。</p> <p>ipv6 - IPv6 フィルタリングマスクを指定します。</p> <p>class - IPv6 クラスを指定します。</p> <p>flowlabel - IPv6 フローラベルを指定します。</p> <p>source_ipv6_mask - IPv6 送信元アドレスを指定します。</p> <p>src_port_mask - IPv6 L4 (TCP/UDP) 送信元ポートのサブマスクを指定します。</p> <p>dst_port_mask - IPv6 L4 (TCP/UDP) 送信先ポートサブマスクを指定します。</p> <p>packet_content - 最大 11 のオフセットを指定できます。単一の UDF フィールドとして認識される 2 バイトのデータが各オフセットで設定できます。オフセットリファレンスも同様に設定可能です。タグの最後、タイプの最後または IP ヘッダの最後のいずれかから開始を指定できます。タグの最後の前でフィールドを許可するためには、送信先アドレス、送信元アドレス、VLAN タグも含まれます。</p> <p>source_mac - 送信元 MAC アドレスを持つパケットだけにアクセスプロファイルを適用する場合に指定します。</p> <p>destination_mac - 送信先 MAC アドレスを持つパケットだけにアクセスプロファイルを適用する場合に指定します。</p> <p>c_tag - 一致するパケットの 16 ビット内部 VLAN タグを指定します。これは 3 ビットの PCP、1 ビットの CFI、12 ビットの VID フィールドから構成されます。</p> <p>s_tag - 一致するパケットの 16 ビット外部 VLAN タグを指定します。これは 3 ビットの PCP、1 ビットの CFI、12 ビットの VID フィールドから構成されます。</p> <p>offset1 - offset11 - プロファイルで定義した各 UDF フィールドデータにマッチするデータを指定します。</p> <p>例 : offset1 が「offset1 0 L2 0x00FF」としてプロファイルで定義され、本コマンドに指定されるデータが「offset1 0x00AA」の場合、スイッチはいずれかのタイプの二番目のバイトを見ます。バイトが 0xAA と一致する場合、デバイスは設定に従ってパケットを処理します。</p>
---------------	---

パラメーター	<p>port <portlist> - スイッチのポート番号を指定し、ルールに従ってアクセスを許可または拒否します。「all」をすべてのポートに指定することもできます。</p> <p>permit - スイッチによる転送を許可するアクセスプロファイルに適合するパケットを指定します。</p> <p>priority <value 0-7> - スイッチに既に設定している 802.1p デフォルトの優先度を書き換えたい場合に、このパラメーターを指定します。本フィールドを指定すると、スイッチが受信したパケットの中のこの優先度に一致するパケットは、既に指定した CoS キューに転送されます。</p> <p>replace_priority <value 0-7> - 指定した CoS キューにパケットを転送する前に、このコマンドで既に指定している基準に適合するパケットの 802.1p デフォルトの優先度を優先度フィールドに入力した値に書き換えたい場合に、このパラメーターを入力します。指定しない場合は、パケットは転送される前に、入力用の 802.1p ユーザー優先度を元の値に書き換えられます。</p> <p>replace_dscp_with - コマンドの最初の部分で指定した基準に適合する入力パケットの「DSCP」フィールドに記述される値を指定します。</p> <p>counter - カウンター機能を有効または無効にします。これはオプションです。デフォルトでは無効になっています。ルールがフローメーターに拘束されない場合、適合するパケットがカウントされます。ルールがフローメーターに拘束される場合、カウンターは上書きされます。</p> <p>deny - アクセスプロファイルに適合しないパケットはスイッチによって転送することを許可されずフィルタリングされます。</p> <p>mirror - アクセスプロファイルに一致するパケットをポートにミラーリングします。</p> <p>mask - これらのオプションは、各フィールドに対し追加のマスクを提供します。追加のマスクはプロファイルで指定されたフィールドマスクのサブセットである必要があります。この最終マスクはプロファイルマスクか各ルールマスクの論理積になります。</p> <p>delete access_id <value 1-65535> - 本コマンドを使用して、イーサネットプロファイル、IP プロファイル、または packet_content プロファイルから指定 ACL ルールを削除します。最大 512 のルールがすべてのアクセスプロファイルに指定できます。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 10.42.73.0 ~ 10.42.73.255 の範囲内で IP アドレスを持つポート 7 のフレームをフィルタリングするためにプロファイル ID が 1 のアクセスプロファイルを設定するには

```
# config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny
Command: config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny

Success.

#
```

注意事項



APLFM では ethernet、ip、ipv6 で 1 グループ、packet_content_mask で 1 グループそれぞれ ACL ルールを書き込むグループが装置内部で割り当てられています。同一グループに共通するパケットを受信した場合、最も低いプロファイル ID 及びアクセス ID をもつ ACL が優先と判断されます。異なるグループに共通するパケットを受信した場合、最終的な優先順位は permit 及び deny (deny が上位) によって判断されます。

3.32.4 show access_profile

目的	スイッチに現在設定されているアクセスプロファイルを表示します。
構文	show access_profile [profile_id <value 1-512>]
説明	本コマンドは、現在設定されているアクセスプロファイルを表示します。
パラメーター	profile_id <value 1-512> - プロファイル ID を指定して1つのプロファイル ID に対するアクセスフルコンフィギュレーションのみを表示します。 プロファイル ID 番号を1～512の範囲で入力します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに現在設定されているすべてのアクセスプロファイルを表示するには

```
#show access_profile
Command: show access_profile

Access Profile Table

=====
Profile ID: 1                               Type: Ethernet Frame Filter
=====
Owner: ACL
Masks Option
VLAN      Source MAC      Destination MAC  802.1P Eth Type
-----
0xFFFF    00-00-00-00-00-01 00-00-00-00-00-02

=====
Profile ID: 2                               Type: IPv4 Frame Filter - ICMP
=====
Owner: ACL
Masks Option
VLAN      Source IP      Dest. IP      DSCP Prot Type Code
-----
0xFFFF    20.0.0.0      10.0.0.0      ICMP

=====
Total Profile Entries: 2

Total Used Rule Entries: 0

Total Unused Rule Entries: 512

#
```

3.33 フローメーターコマンド

3.33.1 config flow_meter profile_id

目的	アクセスプロファイルとルールに基づいたパケットフローベースのメータリング機能を設定します。
構文	<pre>config flow_meter profile_id <value 1-512> access_id <access_id> < < rate <value 64-1024000> burst_size <value 0-1016> rate_exceed <drop_packet remark_dscp <value 0-63> > > delete ></pre>
説明	<p>本コマンドは、フローベースメータリングを設定します。メータリング機能は、「シングルレート2カラーモード」(single-rate two-color mode)のみをサポートします。本機能のパラメーターを適用するには、アクセスルールを最初に作成する必要があります。</p> <p>帯域幅を Kbps の単位で設定できますが、帯域幅を超過した場合、コンフィギュレーションに従って、超過パケットは破棄、または DSCP フィールドを割り当てられます。</p> <p>設定レートを遵守するために、パケットは ACL ルールに従い処理されます。本フローメータリング機能は ACL ルールが「permit」か「mirror」の場合のみ有効です。</p>
パラメーター	<p>profile_id - プロファイル ID を指定します。</p> <p>access_id - アクセス ID を指定します。</p> <p>flow meter - シングルレート2カラーフローメーターを設定します。</p> <p>rate - シングルレート2カラーモードのレートを指定します。フローの認定帯域幅を Kbps で指定します。最小レートは 64 Kbps で、設定可能な最大レートは 1024000 です。</p> <p>burst_size - シングルレート2カラーモードのバーストサイズを指定します。単位は、Kbytes です。バーストサイズの最小値は 0 K バイトで、最大値は 1016 K バイトです。バーストサイズの有効値は 8K バイトの倍数です。</p> <p>rate_exceed - シングルレート2カラーモードの認定レートを超過したパケットの処理について設定します。この処理は以下の方法のいずれかを指定できます。</p> <p>drop_packet: 超過パケットを破棄する。</p> <p>remark_dscp: DSCP の割り当てをパケットにマークする。超過したパケットはまた破棄優先値を高く設定されます。</p> <p>delete - 指定したフローメーターを削除します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ACL ルールに一致する入力パケットのレートとバーストを設定するには

```
# config flow_meter profile_id 1 access_id 1 rate burst_size 64 rate_exceed drop_packet
Command: config flow_meter profile_id 1 access_id 1 rate burst_size 64 rate_exceed drop_packet

Success.

#
```

3.33.2 show flow_meter

目的	フローベースのメータリング設定を表示します。
構文	show flow_meter [profile_id <value 1-512> [access_id <access_id>]]
説明	本コマンドは、フローメーターの設定を表示します。
パラメーター	profile_id - プロファイル ID を指定します。 access_id - アクセス ID を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:フローメーターの設定を表示するには

```
# show flow_meter
Command: show flow_meter

Flow Meter information:
-----
Profile ID : 1           Access ID : 1           Mode : Single-rate Two-color
Rate:  2000(Kbps)       Burst Size:1000(Kbyte)
Actions:
Conform : Permit
Violate : Drop

Profile ID : 1           Access ID : 2           Mode : Single-rate Two-color
Rate:  2000(Kbps)       Burst Size:1016(Kbyte)
Actions:
Conform : Permit
Violate : Permit         Replace_dscp : 20

Total Flow Meter Entries: 2
#
```


3.34 802.1X コマンド

本スイッチは、IEEE 802.1X ポートベースおよびホストベースアクセス制御機能が搭載されています。このメカニズムは、ポートがフレームを送受信する前に満たさなければならない各ポートの条件を各ポートに設定することにより、認証ユーザーまたは他のネットワークデバイスがネットワークリソースにアクセスできる許可を与えることを意図します。

3.34.1 enable 802.1x

目的	スイッチの 802.1X サーバーを有効にします。
構文	enable 802.1x
説明	本コマンドは、スイッチの 802.1X ネットワークアクセス制御アプリケーションを有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:802.1X を有効にするには

```
#enable 802.1x
Command: enable 802.1x

Success.

#
```

3.34.2 disable 802.1x

目的	スイッチの 802.1X サーバーを無効にします。
構文	disable 802.1x
説明	本コマンドは、スイッチの 802.1X ネットワークアクセス制御アプリケーションを無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:802.1X を無効にするには

```
#disable 802.1x
Command: disable 802.1x

Success.

#
```

3.34.3 show 802.1x

目的	スイッチで 802.1X サーバーの現在の認証状態と認証設定を表示します。
構文	show 802.1x < auth_state auth_configuration > [ports <portlist>]
説明	本コマンドは、スイッチで 802.1X サーバーの現在の認証状態と認証設定を表示します。
パラメーター	<p>auth_state - 802.1X サーバーの現在認証状態を表示します。</p> <p>auth_configuration - 802.1X サーバーの現在の認証設定を表示します。</p> <p>ports <portlist> - 参照するポートまたはポート範囲を指定します。以下に認証設定の詳細を示します。</p> <p>802.1x Enabled / Disabled - スイッチの 802.1X 機能の現在のステータスを表示します。</p> <p>Authentication Mode - MAC アドレスによるかまたはポートによるか、認証モードを表示します。</p> <p>Authentication Protocol - スイッチと RADIUS サーバー間で使用する認証プロトコルスイートを表示します。「Radius_Eap」または「local」を指定することができます。</p> <p>Port number - スイッチの物理的なポート数を表示します。</p> <p>機能： Authenticator/None - 上に表示されたポート数の 802.1X 機能を表示します。スイッチに設定できる 802.1X 機能が 2 つあります。「Authenticator」および「None」。</p> <p>AdminCtIDir: Both / In - 未認証の制御ポートが送受両方向または受信方向だけで通信に制御を行うかどうかを表示します。</p> <p>OpenCtIDir: Both / In - 未認証の制御ポートが送受両方向または受信方向だけで通信に制御を行うかどうかを表示します。</p> <p>Port Control: ForceAuth / ForceUnauth / Auto - ポートの認証状態の管理者制御を指定します。「ForceAuth」はポートのオーセンティケータを認証済みに強制します。「ForceUnauth」はポートを非認証に強制します。</p> <p>QuietPeriod - QuietPeriod タイマーの初期設定値です。デフォルト値は 60 秒ですが、0 ~ 65535 秒の範囲で変更できます。</p> <p>TxPeriod - Tx タイマーの初期設定値です。デフォルト値は 30 秒ですが、1 ~ 65535 秒の範囲で変更できます。</p> <p>SuppTimeout - Request / Identity パケットを除くすべての EAP パケットに対するサブリカント（ユーザー）からの応答を待つ時間を表示します。</p> <p>ServerTimeout - RADIUS サーバーからの応答を待つ時間の長さを表示します。</p> <p>MaxReq - サブリカントへのパケットの再送信回数を表示します。</p> <p>ReAuthPeriod - 連続する再認証の間隔を表示します。</p> <p>ReAuthenticate: Enabled / Disabled - 再認証を行うかどうかを表示します。以下の詳細を表示して現在の認証状態が示されます。</p> <p>Port number - スイッチの物理的なポート数を表示します。</p> <p>Auth PAE State: Initalize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth - Authenticator PAE の現在の状態を表示します。</p>

パラメーター	Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout - Backend Authenticator の現在の状態を表示します。 Port Status: Authorized / Unauthorized - 認証プロセスの結果を表示します。Authorized は、ユーザーが認証され、ネットワークにアクセスできることを意味します。Unauthorized は、ユーザーが認証されず、ネットワークにアクセスできないことを意味します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:802.1X 認証の状態を表示するには

```
#show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

802.1X                : Enabled
Authentication Mode   : Port_based
Authentication Protocol : Radius_EAP

Port Number           : 1
Capability             : None
AdminCrIDir           : Both
OpenCrIDir            : Both
Port Control          : Auto
QuietPeriod           : 60   sec
TxPeriod              : 30   sec
SuppTimeout           : 30   sec
ServerTimeout         : 30   sec
MaxReq                : 2    times
ReAuthPeriod          : 3600 sec
ReAuthenticate        : Disabled

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

使用例: ホストベースの 802.1X の 802.1X 認証の状態を表示するには

```
#show 802.1x auth_state
```

```
Command: show 802.1x auth_state
```

```
Port Number : 1
```

Index	MAC Address	Auth PAE State	Backend State	Port Status
1	00-40-66-4D-4E-0A	Connecting	Idle	Unauthorized
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

```
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

3.34.4 config 802.1x capability ports

目的	スイッチのポート範囲の 802.1X 認証を設定します。
構文	config 802.1x capability ports <portlist> all > <authenticator none >
説明	本コマンドには、「authenticator」と「none」の2つの機能があり、ポートごとに設定できます。
パラメーター	<portlist> - 設定するポートまたはポート範囲を指定します。 all - スイッチのすべてのポートを設定します。 authenticator - ネットワークのアクセス権を取得するために認証プロセスを通過する必要があります。 none - ポートは 802.1X 機能によって制御されません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート 1 ~ 10 に 802.1X 機能を設定するには

```
#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

#
```

3.34.5 config 802.1x auth_parameter ports

目的	ポート範囲内の 802.1X 認証パラメータを設定します。デフォルトのパラメータは、指定した範囲内のすべてのポートをデフォルトの 802.1X 設定に戻します。
構文	config 802.1x auth_parameter ports < <portlist> all > < default direction < both in > port_control < force_unauth auto force_auth > quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> enable_reauth < enable disable > >
説明	本コマンドは、ポート範囲内の 802.1X 認証パラメータを設定します。デフォルトのパラメータは、指定した範囲内のすべてのポートをデフォルトの 802.1X 設定に戻します。
パラメーター	<p><portlist> - 設定するポートまたはポート範囲を指定します。</p> <p>all - スイッチのすべてのポートを設定します。</p> <p>default - 指定した範囲内のすべてのポートをデフォルトの 802.1X 設定に戻します。</p> <p>direction <both in> - 制御されたポートが送受信両方または受信方向だけの通信をブロックするかどうかを決定します。</p> <p>port_control - ポート範囲の認証処理における管理用の制御を設定します。以下の認証オプションがあります。</p> <p>force_auth - ポートの認証を Authorized 状態にします。ネットワークアクセスは許可されます。</p> <p>auto - ポートステータスに認証プロセスの結果を反映します。</p> <p>force_unauth - ポートの認証を Unauthorized 状態にします。ネットワークアクセスはブロックされます。</p> <p>quiet_period <sec 0-65535> - 認証に失敗した後、新しく認証を開始するまでの間隔を設定します。</p> <p>tx_period <sec 1-65535> - EAP Request/Identity パケットを送信するためにサブリカント(ユーザー)からの応答を待つ時間を設定します。</p> <p>supp_timeout <sec 1-65535> - Request / Identity パケットを除くすべての EAP パケットに対するサブリカント(ユーザー)からの応答を待つ時間を設定します。</p> <p>ServerTimeout - RADIUS サーバーからの応答を待つ時間の長さを表示します。</p> <p>max_req <value 1-10> - サブリカント(ユーザー)へのパケットの再送信回数を設定します。</p> <p>reauth_period <sec 1-65535> - 連続する再認証の間隔を設定します。</p> <p>enable_reauth <enable disable> - スイッチが再認証するかどうかを決定します。有効にすると、上記「Re-authentication Period (再認証間隔時間)」フィールドで指定した間隔でユーザーを再認証します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1 ~ 20 に 802.1X 認証パラメータを設定するには

```
#config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

#
```

3.34.6 config 802.1x auth_protocol

目的	スイッチの 802.1X 認証プロトコルを設定します。
構文	config 802.1x auth_protocol < local radius_eap >
説明	本コマンドは、認証プロトコルを設定します。
パラメーター	local radius_eap - 希望する認証プロトコルのタイプを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:スイッチの認証プロトコルを設定するには

```
# config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

#
```

3.34.7 config 802.1x init

目的	ポート範囲内の 802.1X 機能を初期化します。
構文	config 802.1x init < port_based ports < <portlist> all > mac_based ports <<portlist> all > [mac_address <macaddr>] >
説明	本コマンドは、指定したポート範囲または指定したポート範囲から動作する MAC アドレスの 802.1X 機能をただちに初期化します。
パラメーター	port_based - スイッチがポート番号のみに基づいた 802.1X 機能を初期化するように指定します。初期化を承認されるポートを指定することができます。 mac_based - スイッチがポート番号のみに基づいた 802.1X 機能を初期化するように指定します。初期化を承認される MAC アドレスを指定することができます。 ports <portlist> - ポートまたはポート範囲を指定します。 all - スイッチのすべてのポートを指定します。 mac_address <macaddr> - 初期化する MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:すべてのポートの認証状態マシンを初期化するには

```
# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

#
```

3.34.8 config 802.1x reauth

目的	スイッチの 802.1X 再認証機能を設定します。
構文	config 802.1x reauth < port_based ports < <portlist> all > mac_based ports < <portlist> all > [mac_address <macaddr>] >
説明	本コマンドは、ポート番号に基づいて認証済みデバイスを再認証します。
パラメーター	port_based - スイッチがポート番号のみに基づいた 802.1X 機能を再認証するように指定します。再認証を承認されるポートを指定することができます。 mac_based - スイッチがポート番号または MAC アドレスのみに基づいた 802.1X 機能を初期化するように指定します。再認証を承認される MAC アドレスを指定することができます。 ports <portlist> - 再認証するポートまたはポート範囲を指定します。 all - スイッチのすべてのポートを指定します。 mac_address <macaddr> - 再認証する MAC アドレスを入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:ポート 1～18 に 802.1X 再認証を設定するには

```
#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

#
```


3.34.9 config radius add

目的	スイッチが RADIUS サーバーと通信するための設定をします。
構文	config radius add <server_index 1-3> <server_ip> key <passwd 32> <default <auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535> > >
説明	本コマンドは、スイッチが RADIUS サーバーと通信するための設定をします。
パラメーター	<p><server_index 1-3> - RADIUS サーバーのインデックス番号を割り当てます。最大 3 つまでの RADIUS サーバーをスイッチに登録できます。</p> <p>スイッチでは登録したインデックス番号の若い順に RADIUS の応答を確認し、最初に応答した RADIUS を認証サーバーとして認識します。</p> <p><server_ip> - RADIUS サーバーの IP アドレス。</p> <p>key <passwd 32> - RADIUS サーバーとスイッチが使用する共有秘密鍵を 32 文字以内で指定します。</p> <p>default - 「auth_port」と「acct_port」設定の両方にデフォルト UDP ポート番号を設定します。</p> <p>auth_port <udp_port_number 1-65535> - 認証リクエストに対する UDP ポート番号を設定します。デフォルト値は「1812」です。</p> <p>acct_port <udp_port_number 1-65535> - アカウンティングリクエストに対する UDP ポート番号を設定します。デフォルト値は「1813」です。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:RADIUS サーバー通信設定を行うには

```
#config radius add 1 10.48.74.121 key HCL default
Command: config radius add 1 10.48.74.121 key HCL default

Success.

#
```

3.34.10 config radius delete

目的	入力済み RADIUS サーバー設定を削除します。
構文	config radius delete <server_index 1-3>
説明	本コマンドは、入力済み RADIUS サーバー設定を削除します。
パラメーター	<server_index 1-3> - 削除したい RADIUS サーバーの番号を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:設定済み RADIUS サーバ設定を削除するには

```
#config radius delete 1
Command: config radius delete 1

Success.

#
```

3.34.11 config radius

目的	登録した RADIUS サーバの設定を変更します。
構文	config radius <server_index 1-3> < ipaddress <server_ip> key <passwd 32> < auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535> > >
説明	登録した RADIUS サーバの設定を変更します。
パラメーター	<p><server_index 1-3> - 登録した RADIUS サーバのインデックス番号を指定します。</p> <p>ipaddress <server_ip> - RADIUS サーバの IP アドレスを変更します。</p> <p>key <passwd 32> - RADIUS サーバとスイッチが使用する共有秘密鍵を 32 文字以内で変更します。</p> <p>auth_port <udp_port_number 1-65535> - 認証リクエストに対する UDP ポート番号を変更します。</p> <p>acct_port <udp_port_number 1-65535> - アカウンティングリクエストに対する UDP ポート番号を変更します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:RADIUS サーバ設定を変更するには

```
#config radius 1 10.1.1.1 key HCL-1
Command: config radius 1 10.1.1.1 key HCL-1

Success.

#
```

3.34.12 config radius parameter

目的	RADIUS サーバーのパラメータを設定します。
構文	config radius parameter < timeout <int 1-255> retransmit <int 1-255> >
説明	本コマンドは、RADIUS サーバーのパラメータを設定します。
パラメーター	timeout <int 1-255> - サーバーの応答を待つ時間。デフォルト値は 5 秒です。 retransmit <int 1-255> - 再送回数。デフォルト値は 2 です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: RADIUS サーバーのタイムアウトオプションを設定するには

```
# config radius parameter timeout 3
Command: config radius parameter timeout 3

Success.

#
```

3.34.13 show radius

目的	スイッチに設定された現在の RADIUS 設定を表示します。
構文	show radius
説明	本コマンドは、スイッチの現在の RADIUS 設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに設定された現在の RADIUS 設定を表示するには

```
#show radius
Command: show radius

Timeout      : 5 seconds
Retransmit   : 2

Index  IP Address          Auth-Port  Acct-Port  Status      Key
-----  -----
1      10.1.1.1            1812       1813       Active      HCL1
2      10.2.1.1            1800       1813       Active      HCL2
3      10.3.1.1            1812       1813       Active      HCL3

Total Entries : 3

#
```

3.34.14 show acct_client

目的	現在の RADIUS アカウンティングクライアントを表示します。
構文	show acct_client
説明	本コマンドは、スイッチに現在設定されている現在の RADIUS アカウンティングクライアントを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: RADIUS アカウンティングクライアントを参照するには

```
#show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses    0
radiusAcctClientIdentifier                 Hitachi Cable

radiusAuthServerEntry ==>
radiusAccServerIndex : 1

radiusAccServerAddress                     10.53.13.199
radiusAccClientServerPortNumber           1813
radiusAccClientRoundTripTime              0
radiusAccClientRequests                    0
radiusAccClientRetransmissions            0
radiusAccClientResponses                   0
radiusAccClientMalformedResponses         0
radiusAccClientBadAuthenticators          0
radiusAccClientPendingRequests            0
radiusAccClientTimeouts                   0
radiusAccClientUnknownTypes               0
radiusAccClientPacketsDropped             0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.15 show auth_client

目的	現在の RADIUS 認証クライアントを表示します。
構文	show auth_client
説明	本コマンドは、スイッチに現在設定されている現在の RADIUS 認証クライアントを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:RADIUS 認証クライアントを参照するには

```
#show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses    0
radiusAuthClientIdentifier                 Hitachi Cable

radiusAuthServerEntry ==>
radiusAuthServerIndex   :1

radiusAuthServerAddress                0.0.0.0
radiusAuthClientServerPortNumber       0
radiusAuthClientRoundTripTime          0
radiusAuthClientAccessRequests         0
radiusAuthClientAccessRetransmissions  0
radiusAuthClientAccessAccepts          0
radiusAuthClientAccessRejects          0
radiusAuthClientAccessChallenges       0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators       0
radiusAuthClientPendingRequests        0
radiusAuthClientTimeouts                0
radiusAuthClientUnknownTypes            0
radiusAuthClientPacketsDropped          0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.16 show auth_diagnostics

目的	現在の認証診断を表示します。
構文	show auth_diagnostics [ports <portlist>]
説明	ポートベースでスイッチの現在の認証診断を表示します。
パラメーター	ports <portlist> - ポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート1の現在の認証診断を表示するには

```
#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Port number : 1
MAC address: 00-40-66-5D-60-02

EntersConnecting          3
EapLogoffsWhileConnecting 0
EntersAuthenticating     2
SuccessWhileAuthenticating 2
TimeoutsWhileAuthenticating 0
FailWhileAuthenticating  0
ReauthsWhileAuthenticating 0
EapStartsWhileAuthenticating 0
EapLogoffWhileAuthenticating 0
ReauthsWhileAuthenticated 0
EapStartsWhileAuthenticated 1
EapLogoffWhileAuthenticated 0
BackendResponses         4
BackendAccessChallenges  2
BackendOtherRequestsToSupplicant 0
BackendNonNakResponsesFromSupplicant 2
BackendAuthSuccesses     2
BackendAuthFails         0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.17 show_auth_session_statistics

目的	現在の認証セッション統計情報を表示します。
構文	show_auth_session_statistics [ports <portlist>]
説明	ポートベースでのスイッチの現在の認証セッション統計情報を表示します。
パラメーター	ports <portlist> - ポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00以降

使用例:ポート 16 の現在の認証セッション統計情報を表示するには

```
#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port number : 1
MAC address: 00-40-66-5D-60-02

SessionOctetsRx          7808
SessionOctetsTx          469102741
SessionFramesRx          122
SessionFramesTx          4196211
SessionId                 ether1_2-1
SessionAuthenticMethod    Remote Authentication Server
SessionTime                70803
SessionTerminateCause     NotTerminatedYet
SessionUserName            456
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.18 show auth_statistics

目的	現在の認証統計を表示します。
構文	show auth_statistics [ports <portlist>]
説明	ポートベースでのスイッチの現在の認証統計情報を表示します。
パラメーター	ports <portlist> - ポート範囲を指定します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:ポート1の現在の認証統計を表示するには

```
#show auth_statistics ports 1
Command: show auth_statistics ports 1

Port number : 1
MAC address: 00-40-66-5D-60-02

EapolFramesRx          6
EapolFramesTx          7
EapolStartFramesRx    2
EapolReqIdFramesTx    3
EapolLogoffFramesRx   0
EapolReqFramesTx      2
EapolRespIdFramesRx   2
EapolRespFramesRx     2
InvalidEapolFramesRx  0
EapLengthErrorFramesRx 0

LastEapolFrameVersion  1
LastEapolFrameSource   00-40-66-5D-60-02
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3.34.19 create 802.1x user

目的	新しい802.1Xユーザーを作成します。
構文	create 802.1x user <username 15>
説明	本コマンドは、新しい802.1Xユーザーを作成します。
パラメーター	<username 15> - 半角英数字15文字以内でユーザー名を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例:802.1Xユーザーを作成するには

```
#create 802.1x user HCL
Command: create 802.1x user HCL

Enter a case-sensitive new password:*****
Enter the new password again for confirmation:*****
Success.

#
```


3.34.20 show 802.1x user

目的	スイッチの 802.1X ユーザーアカウントを表示します。
構文	show 802.1x user
説明	本コマンドは、スイッチに現在設定されている 802.1X ポートベースまたはホストベースのネットワークアクセス制御ローカルユーザーを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに現在設定されている 802.1X ユーザーを参照するには

```
#show 802.1x user
Command: show 802.1x user

Index  UserName
----  -
1      ctsnow

Total Entries: 1

#
```

3.34.21 delete 802.1x user

目的	スイッチの 802.1X ユーザーアカウントを削除します。
構文	delete 802.1x user <username 15>
説明	本コマンドは、スイッチに現在設定されている 802.1X ポートベースまたはホストベースのネットワークアクセス制御ローカルユーザーを削除します。
パラメーター	<username 15> - ユーザー名は 15 文字までの半角英数字で指定できます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 802.1X ユーザーを削除するには

```
#delete 802.1x user ctsnow
Command: delete 802.1x user ctsnow

Success.

#
```

3.35 アクセス認証制御コマンド

アクセス認証制御は、TACACS/XTACACS/TACACS+/RADIUS プロトコルを使用してスイッチへの安全なアクセスを可能にします。ユーザーがスイッチへのログインや、管理者レベルの特権へのアクセスを行うおうとする時、パスワードの入力を求められます。TACACS/ XTACACS/ TACACS+/ RADIUS 認証がスイッチで有効になると、スイッチはTACACS/XTACACS/TACACS+/RADIUS サーバーと連絡し、ユーザーの確認をします。確認が行われたユーザーは、スイッチへのアクセスを許可されます。

現在 TACACS セキュリティープロトコルには異なるエンティティを持つ3つのバージョンが存在します。本スイッチのソフトウェアはTACACS の以下のバージョンをサポートします。

TACACS(Terminal Access Controller Access Control System) - セキュリティーのためのパスワードチェック、認証、およびユーザーアクションの通知を、1 台またはそれ以上の集中型の TACACS サーバーを使用して行います。パケットの送受信には UDP プロトコルを使用します。

XTACACS(拡張型 TACACS) - TACACS プロトコルの拡張版で、TACACS プロトコルより多種類の認証リクエストとレスポンスコードに対応します。パケットの送受信には UDP プロトコルを使用します。

TACACS+(Terminal Access Controller Access Control System plus) - ネットワークデバイスの認証のために詳細なアクセス制御を提供します。TACACS+は、1 台またはそれ以上の集中型のサーバーを経由して認証コマンドを使用することができます。TACACS+プロトコルは、スイッチとTACACS+デーモンの間のすべてのトラフィックを暗号化します。また、TCP プロトコルを使用して信頼性の高い伝達を行います。

スイッチは、アクセス認証制御コマンドを使用して認証するための RADIUS プロトコルもサポートします。RADIUS (Remote Authentication Dial In User Server)は、認証用にリモートサーバーを使用し、ユーザーによる接続要求の受信、ユーザーの認証、クライアントがユーザーにサービスを提供するために必要なコンフィギュレーション情報すべての提供を行う役割も持ちます。RADIUS は本セクションにリストされたコマンドを使用してスイッチで活用できます。

TACACS/XTACACS/TACACS+/RADIUS のセキュリティー機能が正常に動作するためには、スイッチ以外の認証サーバーと呼ばれるデバイス上で 認証用のユーザー名とパスワードを含む

TACACS/XTACACS/TACACS+/ RADIUS サーバーの設定を行う必要があります。スイッチがユーザーにユーザー名とパスワードの要求を行う時、スイッチは、TACACS/XTACACS/TACACS+/RADIUS サーバーにユーザー認証の問い合わせを行います。サーバーは以下の3つのうちの1つの応答を返します。

- (1) サーバーは、ユーザー名とパスワードを認証し、ユーザーにスイッチへの通常のアクセス権を与えます。
- (2) サーバーは、入力されたユーザー名とパスワードを受け付けず、スイッチへのアクセスを拒否します。
- (3) サーバーは、認証の問い合わせに応じません。この時点でスイッチはサーバーからタイムアウトを受け取り、メソッドリスト中に設定された次の認証方法へと移行します。

本スイッチには TACACS、XTACACS、TACACS+、RADIUS の各プロトコル用に4つの認証サーバーグループがあらかじめ組み込まれています。これらのビルトインサーバーグループは、スイッチにアクセスを試みるユーザーの認証に使用されます。認証サーバーグループ内に任意の順番で認証サーバーを設定し、ユーザーがスイッチへのアクセス権を取得する場合、1 番目の認証サーバーに認証を依頼します。

認証が行われなければ、リストの2番目のサーバーに依頼し、以下同様の処理が続きます。

実装されている認証サーバーグループには、特定のプロトコルが動作するホストのみを登録できます。例えば TACACS 認証サーバーグループは、TACACS 認証サーバーのみを登録できます。

スイッチの管理者は、ユーザー定義のメソッドリストに6種類の異なる認証方法 (TACACS/XTACACS/TACACS+/RADIUS/local/none) を設定できます。これらの方法は、任意に並べ替えることが可能で、スイッチ上での通常のユーザー認証に使用されます。リストには最大8つの認証方法を登録できます。ユーザーがスイッチにアクセスしようとする時、スイッチはリストの1番目の認証方法を選択して認証を行います。1番目の方法で認証サーバーを通過しても認証が返ってこなければ、スイッチはリストの次の方法を試みます。この手順は、認証が成功するか、拒否されるか、またはリストのすべての認証方法を試し終わるまで繰り返されます。

スイッチへのアクセス権を取得したユーザーは、通常のアクセス権を与えられていることにご注意ください。管理者特権レベルの権利を取得するためには、ユーザーは「enable admin」コマンドにアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。

注意事項



TACACS、XTACACS、TACACS+、RADIUS は独立したエンティティであり、互換性はありません。スイッチとサーバー間は、同じプロトコルを使用した全く同じ設定を行う必要があります(例えば、スイッチに TACACS 認証を設定した場合、ホストサーバーにも同様の設定を行います)。

3.35.1 enable_authen_policy

目的	システムアクセス認証ポリシーを有効にします。
構文	enable_authen_policy
説明	本コマンドは、管理者が定義するスイッチにアクセスするユーザーのための認証ポリシーを有効にします。有効にすると、デバイスはログインメソッドリストをチェックし、ログイン時のユーザー認証に使用する認証方法を選択します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: システムアクセス認証ポリシーを有効にするには

```
#enable_authen_policy
Command: enable_authen_policy

Success.

#
```

3.35.2 disable authen_policy

目的	システムアクセス認証ポリシーを無効にします。
構文	disable authen_policy
説明	本コマンドは、管理者が定義するスイッチにアクセスするユーザーのための認証ポリシーを無効にします。無効になると、スイッチはユーザー名とパスワード検証のためにローカルユーザーアカウントデータベースにアクセスします。さらに、スイッチは、現在、管理者レベルの権限にアクセスを試みる普通のユーザーのために認証としてローカルイネーブルパスワードを受け入れます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: システムアクセス認証ポリシーを無効にするには

```
#disable authen_policy
Command: disable authen_policy

Success.

#
```

3.35.3 show authen_policy

目的	スイッチ上のシステムアクセス認証ポリシーのステータスを表示します。
構文	show authen_policy
説明	スイッチ上のアクセス認証ポリシーの現在のステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: システムアクセス認証ポリシーを表示するには

```
#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

#
```

3.35.4 create_authen_login_method_list_name

目的	ユーザーがスイッチにログインする際の認証方法のユーザー定義メソッドリストを作成します。
構文	create_authen_login_method_list_name <string 15>
説明	本コマンドは、ユーザーがログインする際の認証方法リストを作成します。本スイッチは、最大 8 個のメソッドリストをサポートしていますが、1 つはデフォルトとして予約されているため、削除できません。複数のメソッドリストは、別々に作成および設定される必要があります。
パラメーター	<string 15> - 15 文字以内の半角英数字の文字列を入力して、メソッドリストを定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:メソッドリスト「HCL」を作成するには

```
#create_authen_login_method_list_name HCL
Command: create_authen_login_method_list_name HCL

Success.

#
```

3.35.5 config_authen_login

目的	ユーザーがログインする際の認証方法を規定するユーザー定義またはデフォルトのメソッドリストを設定します。
構文	config_authen_login < default method_list_name <string 15> > method < tacacs xtacacs tacacs+ radius server_group <string 15> local none >
説明	ユーザーがスイッチにログインする際の認証方法を規定するユーザー定義またはデフォルトのメソッドリストを設定します。本コマンドで設定した認証方法の順番で、認証結果に影響を与えます。例えば、ログインメソッドリストに「tacacs,xtacacs,local」の順番で認証方法を入力した場合、スイッチはまずサーバーグループ内の 1 番目の「tacacs」ホストに認証リクエストを送信します。そのサーバーから応答がない場合、2 番目の「tacacs」ホストに認証リクエストを送信し、リストが終了するまでこの手順を続けます。スイッチは、リストの次のプロトコル xtacacs を使用して、同じシーケンスを再開します。xtacacs リストを使用しても認証が行われない場合は、スイッチに設定された「local」アカウントのデータベースセットを使用して該当のユーザーを認証します。Local メソッドが使用される時、ユーザーの権限はスイッチに設定されたローカルアカウントの権限に依存します。 これらの方法によって、認証に成功したユーザーには「User」の権限のみが与えられます。ユーザーが管理者レベルの権限に更新したい場合、「enable_admin」コマンドを実行し、スイッチに管理者により事前に設定されているパスワードの入力が必要になります（「enable_admin」についての詳細は、このセクションの「enable_admin」の説明を参照してください）。

<p>パラメーター</p>	<p>default - ユーザー定義されたアクセス認証のデフォルトのメソッドリストを表示します。ユーザーは以下の認証方法を1つまたは組み合わせて最大4つまで選択できます。</p> <p>tacacs - 本パラメーターを追加する場合、TACACS server group リストのリモートの TACACS server hosts から TACACS プロトコルを使用してユーザー認証を行う必要があります。</p> <p>xtacacs - 本パラメーターを追加する場合、XTACACS server group リストのリモートの XTACACSserver hosts から XTACACS プロトコルを使用してユーザー認証を行う必要があります。</p> <p>tacacs+ - 本パラメーターを追加する場合、TACACS+ server group リストのリモートの TACACS+ server hosts から TACACS+プロトコルを使用してユーザー認証を行う必要があります。</p> <p>radius - 本パラメーターを追加する場合、RADIUS server group リストのリモートの RADIUS server hosts から RADIUS プロトコルを使用してユーザー認証を行う必要があります。</p> <p>server_group <string 15> - 本パラメーターを追加する場合、スイッチに設定済みのユーザー定義のサーバーグループを使用してユーザー認証を行う必要があります。</p> <p>local - 本パラメーターを追加する場合、スイッチ上のローカル user account データベースを使用してユーザー認証を行う必要があります。</p> <p>none - 本パラメーターを追加する場合、スイッチにアクセスするための認証は必要ありません。</p> <p>method_list_name - ユーザーによって定義されたメソッドリスト名を入力します。ユーザーは以下の認証方法を1つまたは組み合わせて本メソッドリストに最大4つまで追加できます。</p> <p>tacacs - 本パラメーターを追加する場合、リモートの TACACS サーバーから TACACS プロトコルを使用してユーザー認証を行う必要があります。</p> <p>xtacacs - 本パラメーターを追加する場合、リモートの XTACACS サーバーから XTACACS プロトコルを使用してユーザー認証を行う必要があります。</p> <p>tacacs+ - 本パラメーターを追加する場合、TACACS+サーバーから TACACS+プロトコルを使用してユーザー認証を行う必要があります。</p> <p>radius - 本パラメーターを追加する場合、リモートの RADIUS サーバーから RADIUS プロトコルを使用してユーザー認証を行う必要があります。</p> <p>server_group <string 15> - 本パラメーターを追加する場合、スイッチに設定済みのユーザー定義のサーバーグループを使用してユーザー認証を行う必要があります。</p> <p>local - 本パラメーターを追加する場合、スイッチ上のローカル user account データベースを使用してユーザー認証を行う必要があります。</p> <p>none - 本パラメーターを追加する場合、スイッチにアクセスするための認証は必要ありません。</p>
<p>制限事項</p>	<p>管理者アカウントのみ本コマンドを実行できます。</p>
<p>対応バージョン</p>	<p>1.00.00 以降</p>

使用例: 認証メソッド TACACS、XTACACS、および local をこの順番でユーザー定義メソッドリスト「HCL」に設定するには

```
#config authn_login method_list_name HCL method tacacs xtacacs local
Command: config authn_login method_list_name HCL method tacacs xtacacs local

Success.

#
```


使用例: デフォルトのメソッドリストを認証メソッド XTACACS、TACACS+、ローカルの順に設定するには

```
#config authn_login default method xtacacs tacacs+ local
Command: config authn_login default method xtacacs tacacs+ local

Success.

#
```

注意事項

 認証プロトコルとして「none」または「local」を入力すると、メソッドリストまたはデフォルトのメソッドリストに別の認証が上書きされます。

3.35.6 delete authn_login method_list_name

目的	ユーザーがスイッチにログインする際の認証方法を規定するユーザー定義のログインメソッドリストを削除します。
構文	delete authn_login method_list_name <string 15>
説明	本コマンドは、ユーザーがログインする際の認証方法リストを削除します。
パラメーター	<string 15> - 15文字以内の半角英数字の文字列を入力して、削除するメソッドリストを定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: メソッドリスト名「HCL」を削除するには

```
#delete authn_login method_list_name HCL
Command: delete authn_login method_list_name HCL

Success.

#
```

3.35.7 show authen_login

目的	ユーザーがスイッチにログインする際の認証方法の設定済みユーザー定義メソッドリストを表示します。
構文	show authen_login < default method_list_name <string 15> all >
説明	本コマンドは、ユーザーがログインする際の認証メソッドリストを表示します。
パラメーター	<p>default - 本パラメーターを入力すると、ユーザーがスイッチにログインする際のデフォルトメソッドリストを表示します。</p> <p>method_list_name <string 15> - 最大 15 文字までの半角英数字文字列を入力して、表示する「method list」を定義します。</p> <p>all - 本パラメーターを入力すると、現在スイッチに設定されているすべての認証ログインメソッドを表示します。</p> <p>ウィンドウは次のパラメーターを表示します。</p> <p>Method List Name - 設定済みメソッドリスト名。</p> <p>Priority - ユーザーがスイッチにログインする際、認証のために問い合わせられるメソッドリストプロトコルの順番を定義します。1(最も高い) から 4(最も低い)で優先順位が付けられます。</p> <p>Method Name - メソッドリスト名ごとに実行されるセキュリティープロトコルを定義します。</p> <p>Comment - メソッドのタイプを定義します。「User-defined Group」は、ユーザー定義されたサーバーグループを参照します。「Built-in Group」は、スイッチに普遍設定される TACACS、XTACACS、TACACS+および RADIUS セキュリティープロトコルを参照します。「Keyword」は、「local」(スイッチのユーザーアカウントを介した認証)と「none」(スイッチのすべての機能にアクセスするために認証する必要がない)という TACACS/XTACACS/TACACS+/RADIUS に代わる技術を使用した認証を参照します。</p>
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: 「HCL」という名の認証ログインメソッドリストを参照するには

```
#show authen_login method_list_name HCL
Command: show authen_login method_list_name HCL
```

Method List Name	Priority	Method Name	Comment
-----	-----	-----	-----
hcl	1	tacacs+	Built-in Group
	2	tacacs	Built-in Group
	3	HCL	User-defined Group
	4	local	Keyword

```
#
```


3.35.8 create authen_enable method_list_name

目的	スイッチでユーザーの権限を通常のユーザーレベルから管理者レベルに上げる認証メソッドのユーザー定義メソッドリストを設定します。
構文	create authen_enable method_list_name <string 15>
説明	本コマンドは、スイッチでユーザーを通常のユーザーレベル権限から管理者レベル権限に昇格する認証メソッドのユーザー定義メソッドリストを設定します。スイッチの通常のユーザーレベル権限を取得したユーザーが管理者レベル権限を得るためには、管理者が定義した方法により認証を受ける必要があります。スイッチに最大 8 件の「enable method list」が実行できます。
パラメーター	<string 15> - 15 文字以内の半角英数字の文字列を入力して、作成する「enable method list」を定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ユーザー権限を管理者権限に昇格するために「HCL」という名のユーザー定義メソッドリストを作成するには

```
#create authen_enable method_list_name HCL
Command: create authen_enable method_list_name HCL

Success.

#
```

3.35.9 config authen_enable

目的	スイッチでユーザーの権限を通常のユーザーレベルから管理者レベル権限に昇格する認証メソッドのユーザー定義メソッドリストを作成します。
構文	<pre>config authen_enable < default method_list_name <string 15> > method < tacacs xtacacs tacacs+ radius server_group <string 15> local_enable none ></pre>
説明	<p>本コマンドは、スイッチでユーザーを通常のユーザーレベル権限から管理者レベル権限に昇格する認証メソッドのユーザー定義メソッドリストを設定します。スイッチの通常のユーザーレベル権限を取得したユーザーが管理者レベル権限を得るためには、管理者が定義した方法により認証を受ける必要があります。最大 8 件の「enable method list」がスイッチに同時に実行できます。本コマンドで設定した認証方法の順番で、認証結果に影響を与えます。例えば、ログインメソッドリストに「tacacs,xtacacs,local_enable」の順番で認証方法を入力した場合、スイッチはまずサーバーグループ内の 1 番目の「TACACS」ホストに認証リクエストを送信します。認証が得られない場合、サーバーグループの 2 番目の「TACACS」ホストに認証リクエストを送信し、リストが終了するまでこの手順を続けます。スイッチは、リストの次のプロトコル xtacacs を使用して、同じシーケンスを再開します。xtacacs リストを使用しても認証が行われない場合は、スイッチに設定された「local_enable」のパスワードセットを使用して該当のユーザーを認証します。</p> <p>これらの中のいずれかの方法で認証されたユーザーは、「Admin」(管理者)レベルの権限を取得することができます。</p>
パラメーター	<p>default - ユーザー定義された管理者権限の認証のデフォルトのメソッドリストを表示します。ユーザーは以下の認証方法を 1 つまたは組み合わせて最大 4 つまで選択できます。</p> <p>tacacs - 本パラメーターを追加する場合、TACACS server group リストのリモートの TACACS server hosts から TACACS プロトコルを使用してユーザー認証を行う必要があります。</p> <p>xtacacs - 本パラメーターを追加する場合、XTACACS server group リストのリモートの XTACACS server hosts から XTACACS プロトコルを使用してユーザー認証を行う必要があります。</p> <p>tacacs+ - 本パラメーターを追加する場合、TACACS+ server group リストのリモートの TACACS+ server hosts から TACACS+プロトコルを使用してユーザー認証を行う必要があります。</p> <p>radius - 本パラメーターを追加する場合、TACACS server group リストのリモートの RADIUS server hosts から RADIUS プロトコルを使用してユーザー認証を行う必要があります。</p> <p>server_group <string 15> - 本パラメーターを追加する場合、スイッチに設定済みのユーザー定義のサーバーグループを使用してユーザー認証を行う必要があります。</p> <p>local_enable - 本パラメーターを追加する場合、スイッチ上のローカル user account データベースを使用してユーザー認証を行う必要があります。</p>

パラメーター	<p>none - 本パラメーターを追加する場合、スイッチにアクセスするための認証は必要ありません。</p> <p>method_list_name - ユーザーによって定義されたメソッドリスト名を入力します (create authen_enable)。ユーザーは以下の認証方法を1つまたは組み合わせて本メソッドリストに最大4つまで追加できます。</p> <p>tacacs - 本パラメーターを追加する場合、リモートのTACACSサーバーからTACACSプロトコルを使用してユーザー認証を行う必要があります。</p> <p>xtacacs - 本パラメーターを追加する場合、リモートのXTACACSサーバーからXTACACSプロトコルを使用してユーザー認証を行う必要があります。</p> <p>tacacs+ - 本パラメーターを追加する場合、TACACS+サーバーからTACACS+プロトコルを使用してユーザー認証を行う必要があります。</p> <p>radius - 本パラメーターを追加する場合、リモートのRADIUSサーバーからRADIUSプロトコルを使用してユーザー認証を行う必要があります。</p> <p>server_group <string 15> - 本パラメーターを追加する場合、スイッチに設定済みのユーザー定義のサーバーグループを使用してユーザー認証を行う必要があります。</p> <p>local_enable - 本パラメーターを追加する場合、スイッチ上のローカルuser accountデータベースを使用してユーザー認証を行う必要があります。デバイスのローカルイネーブルパスワードは、「config admin local_password」コマンドを使用して設定できます。</p> <p>none - 本パラメーターを追加する場合、スイッチ上の管理者レベル権限にアクセスするための認証は必要ありません。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例: ユーザー定義のメソッドリスト「HCL」を認証メソッドTACACS、XTACACS、ローカルの順に設定するには

```
#config authen_enable method_list_name HCL method tacacs xtacacs local_enable
Command: config authen_enable method_list_name HCL method tacacs xtacacs local_enable

Success.

#
```

使用例: デフォルトのメソッドリストを認証メソッドXTACACS、TACACS+、ローカルの順に設定するには

```
#config authen_enable default method xtacacs tacacs+ local_enable
Command: config authen_enable default method xtacacs tacacs+ local_enable

Success.

#
```

3.35.10 delete authen_enable method_list_name

目的	通常のコユーザーレベル権限を管理者レベル権限に昇格するための認証方法を規定するユーザー定義のログインメソッドリストを削除します。
構文	delete authen_enable method_list_name <string 15>
説明	本コマンドは、通常のコユーザーレベルの権限を管理者レベル権限に昇格するための認証方法を規定するユーザー定義のログインメソッドリストを削除します。
パラメーター	<string 15> - 15文字以内の半角英数字の文字列を入力して、削除する「enable method list」を定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例: ユーザー定義のメソッドリスト「HCL」を削除するには

```
#delete authen_enable method_list_name HCL
Command: delete authen_enable method_list_name HCL

Success.

#
```

3.35.11 show authen_enable

目的	スイッチでユーザーの権限を通常のユーザーレベル権限から管理者レベル権限に昇格する認証メソッドのメソッドリストを表示します。
構文	show authen_enable < default method_list_name <string 15> all >
説明	本コマンドは、通常のユーザーレベルの権限を管理者レベル権限に昇格するための認証方法を規定するユーザー定義のログインメソッドリストを表示します。
パラメーター	<p>default - 本パラメーターを入力すると、ユーザーがスイッチの管理者レベル権限にアクセスする際のデフォルトメソッドリストを表示します。</p> <p>method_list_name <string 15> - 最大 15 文字までの半角英数字文字列を入力して、表示する「method list」を定義します。</p> <p>all - 本パラメーターを入力すると、現在スイッチに設定されているすべての認証ログインメソッドを表示します。</p> <p>ウィンドウは次のパラメーターを表示します。</p> <p>Method List Name - 設定済みメソッドリスト名。</p> <p>Priority - ユーザーがスイッチにログインする際、認証のために問い合わせされるメソッドリストプロトコルの順番を定義します。1(最も高い) から 4(最も低い) で優先順位が付けられます。</p> <p>Method Name - メソッドリスト名ごとに実行されるセキュリティープロトコルを定義します。</p> <p>Comment - メソッドのタイプを定義します。「User-defined Group」は、ユーザー定義されたサーバーグループを参照します。「Built-in Group」は、スイッチに普遍設定される TACACS、XTACACS、TACACS+および RADIUS セキュリティープロトコルを参照します。「Keyword」は、「local」(スイッチの local_enable パスワードを介した認証)と「none」(スイッチのすべての機能にアクセスするために認証する必要がない)という TACACS/XTACACS/TACACS+/RADIUS に代わる技術を使用した認証を参照します。</p>
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: 通常のユーザーレベル権限を管理者レベル権限に昇格するためにすべてのメソッドリストを表示するには

```
#show authn_enable all
```

```
Command: show authn_enable all
```

Method List Name	Priority	Method Name	Comment
-----	-----	-----	-----
Permit	1	tacacs+	Built-in Group
	2	tacacs	Built-in Group
	3	HCL	User-defined Group
	4	local_enable	Keyword
default	1	tacacs+	Built-in Group
	2	local_enable	Keyword

```
Total Entries : 2
```

```
#
```

3.35.12 config authen application

目的	設定済みのメソッドリストを使用して、認証のためにスイッチに様々なアプリケーションを設定します。
構文	config authen application < console telnet ssh http all > < login enable > < default method_list_name <string 15> >
説明	本コマンドは、作成済みのメソッドリストを使用して、ユーザーレベルおよび管理者レベル(authen_enable)でログインする際に使用するスイッチの設定用アプリケーション(コンソール、Telnet、SSH、Web)を設定します。
パラメーター	<p>application - 設定するアプリケーションを選択します。以下の5つのオプションの1つを選択します。</p> <p>console - コマンドラインインターフェースログインメソッドを設定します。</p> <p>telnet - Telnet ログインメソッドを設定します。</p> <p>ssh - Secure Shell ログインメソッドを設定します。</p> <p>http - Web インターフェースログインメソッドを設定します。</p> <p>all - すべてのアプリケーション(コンソール、Telnet、SSH、Web)ログインメソッドを設定します。</p> <p>login - 登録済みのメソッドリストを使用して、ユーザーレベルの通常ログインを行うアプリケーションを設定します。</p> <p>enable - 登録済みのメソッドリストを使用して、通常のユーザーレベルを管理者権限に昇格させるアプリケーションを設定します。</p> <p>default - デフォルトメソッドリストを使用して、ユーザー認証を行うアプリケーションを設定します。</p> <p>method_list_name <string 15> - 登録済みのメソッドリストを使用して、ユーザー認証用のアプリケーションを設定します。15文字以内の半角英数字の文字列を入力して、登録済みのメソッドリストを指定します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: Web インターフェースのためにデフォルトメソッドリストを設定するには

<pre>#config authen application http login default Command: config authen application http login default Success. #</pre>

3.35.13 show authen application

目的	スイッチの様々なアプリケーションのための認証方法を表示します。
構文	show authen application
説明	本コマンドは、スイッチに現在設定されているスイッチコンフィギュレーションアプリケーション(コンソール、Telnet、SSH、Web) に対するすべての認証メソッドリスト (ログイン、管理者特権の有効化など)を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スwitchのすべてのアプリケーションに対するログインと「enable method list」を表示するには

```
#show authen application
Command: show authen application

Application      Login Method List  Enable Method List
-----
Console          default             default
Telnet           default             default
SSH               default             default
HTTP              default             default

#
```


3.35.14 create_authen_server_host

目的	認証サーバーを作成します。
構文	create_authen_server_host <ipaddr> protocol < tacacs xtacacs tacacs+ radius > [port <int 1-65535> key <<key_string 254> none> timeout <int 1-255> retransmit < 1-255>]
説明	本コマンドは、スイッチに TACACS/ XTACACS/ TACACS+/ RADIUS セキュリティープロトコルに対応したユーザー定義の認証サーバーを作成します。ユーザーが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/ XTACACS/ TACACS+/ RADIUS サーバーに認証パケットを送信します。すると TACACS/XTACACS/TACACS+/RADIUS サーバーはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/XTACACS/TACACS+/RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。 サポート可能なサーバーは最大 16 台です。
パラメーター	server_host <ipaddr> - 追加するリモートサーバーの IP アドレス。 protocol - サーバーが使用するプロトコル。以下から選択します。 tacacs - サーバーが TACACS プロトコルを使用している場合に選択します。 xtacacs - サーバーが XTACACS プロトコルを使用している場合に選択します。 tacacs+ - サーバーが TACACS+プロトコルを使用している場合に選択します。 radius - サーバーが RADIUS プロトコルを使用している場合に選択します。 port <int 1-65535> - サーバー上で認証プロトコルに使用する 1～65535 の仮想ポート番号。ポート番号の初期値は、TACACS/XTACACS/TACACS+サーバーの場合は 49、RADIUS サーバーの場合は 1812 と 1813 です。独自の番号を設定してセキュリティを向上することも可能です。 key <key_string 254> - 設定した TACACS+または RADIUS サーバーのみと共有する認証キー。最大 254 文字までの半角英数字を指定します。 timeout <int 1-255> - スイッチが、サーバーからの認証リクエストへの応答を待つ時間(秒)を入力します。デフォルト値は 5 秒です。 retransmit <int 1-255> - サーバーからの応答がない場合に、デバイスが認証リクエストを再送する回数を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート番号が 1234、タイムアウトの値が 10 秒、再送回数が 5 である TACACS+認証サーバーを作成するには

<pre>#create_authen_server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10 retransmit 5 Command: create_authen_server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10 retransmit 5 5 Success. #</pre>

3.35.15 config authen server_host

目的	ユーザー定義の認証サーバーを設定します。
構文	config authen server_host <ipaddr> protocol < tacacs xtacacs tacacs+ radius> < port <int 1-65535> key <<key_string 254> none > timeout <int 1-255> retransmit < 1-255> >
説明	本コマンドは、スイッチに TACACS/XTACACS/TACACS+/RADIUS セキュリティープロトコルに対応したユーザー定義の認証サーバーを設定します。ユーザーが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/XTACACS/TACACS+/RADIUS サーバーに認証パケットを送信します。すると TACACS/XTACACS/TACACS+/RADIUS サーバーはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/XTACACS/TACACS+/RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバーは最大 16 台です。
パラメーター	server_host <ipaddr> - 変更するリモートサーバーの IP アドレス。 protocol - サーバーが使用するプロトコル。以下から選択します。 tacacs - サーバーが TACACS プロトコルを使用している場合に選択します。 xtacacs - サーバーが XTACACS プロトコルを使用している場合に選択します。 tacacs+ - サーバーが TACACS+プロトコルを使用している場合に選択します。 radius - サーバーが RADIUS プロトコルを使用している場合に選択します。 port <int 1-65535> - サーバー上で認証プロトコルに使用する 1~65535 の仮想ポート番号。ポート番号の初期値は、TACACS/XTACACS/TACACS+サーバーの場合は 49、RADIUS サーバーの場合は 1812 と 1813 です。独自の番号を設定してセキュリティを向上することも可能です。 key <key_string 254> - 設定した TACACS+または RADIUS サーバーのみと共有する認証キー。最大 254 文字までの半角英数字または「none」を指定します。 timeout <int 1-255> - スイッチが、サーバーからの認証リクエストへの応答を待つ時間(秒)を入力します。デフォルト値は 5 秒です。 retransmit <int 1-255> - サーバーからの応答がない場合に、デバイスが認証リクエストを再送する回数を入力します。本フィールドでは TACACS+プロトコルは操作できません。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ポート番号が 4321、タイムアウトの値が 12 秒、再送回数が 4 である TACACS+認証サーバーを設定するには

<pre>#config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12 retransmit 4 Command: config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12 retransmit 4 Success. #</pre>

3.35.16 delete authen server_host

目的	ユーザー定義の認証サーバーを削除します。
構文	delete authen server_host <ipaddr> protocol < tacacs xtacacs tacacs+ radius >
説明	本コマンドは、スイッチに作成済みのユーザー定義認証サーバーホストを削除します。
パラメーター	server_host <ipaddr> - 削除するリモートサーバーの IP アドレス。 protocol - ユーザーが削除したいサーバーに使用されるプロトコル。以下から選択します。 tacacs - サーバーが TACACS プロトコルを使用している場合に選択します。 xtacacs - サーバーが XTACACS プロトコルを使用している場合に選択します。 tacacs+ - サーバーが TACACS+プロトコルを使用している場合に選択します。 radius - サーバーが RADIUS プロトコルを使用している場合に選択します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: ユーザー定義の TACACS+認証サーバーを削除するには

<pre>#delete authen server_host 10.1.1.121 protocol tacacs+ Command: delete authen server_host 10.1.1.121 protocol tacacs+ Success. #</pre>

3.35.17 show authen server_host

目的	ユーザー定義の認証サーバーを参照します。
構文	show authen server_host
説明	本コマンドは、スイッチに作成済みのユーザー定義認証サーバーを参照します。 次のパラメーターが表示されます。 IP Address - 認証サーバーの IP アドレス。 Protocol - サーバーが使用するプロトコル。結果には TACACS、XTACACS、TACACS+または RADIUS が含まれる可能性が高くなります。 Port - サーバーの仮想ポート番号。デフォルト値は 49 です。 Timeout - スイッチが、サーバーからの認証リクエストへの応答を待つ時間 (秒)。 Retransmit - 再送信フィールドの値は TACACS サーバーからの応答がない場合に、デバイスが認証リクエストを再送する回数を示します。本フィールドでは TACACS+プロトコルは操作できません。 Key - 設定した TACACS+サーバーのみと共有する認証キー。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに現在設定されている認証サーバーを表示するには

```
#show authen server_host
Command: show authen server_host

IP Address      Protocol      Port  Timeout  Retransmit  Key
-----
10.53.13.94     TACACS       49    5         2           No Use

Total Entries : 1

#
```

3.35.18 create authen server_group

目的	ユーザー定義の認証サーバーグループを作成します。
構文	create authen server_group <string 15>
説明	本コマンドは、認証サーバーグループを作成します。認証サーバーグループを作成します。サーバーグループとは、TACACS/XTACACS/TACACS+/RADIUSのサーバーを、ユーザー定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。「config authen server_group」コマンドを使用して、8個までの認証サーバーをこのグループに追加できます。
パラメーター	<string 15> - 15文字以内の半角英数字の文字列を入力して、新しく作成するサーバーグループを定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例: サーバーグループ「group_1」を作成するには

```
#create authen server_group group_1
Command: create authen server_group group_1

Success.

#
```

3.35.19 config authen server_group

目的	ユーザー定義の認証サーバーグループを設定します。
構文	config authen server_group < tacacs xtacacs tacacs+ radius <string 15> > < add delete > server_host <ipaddr> protocol < tacacs xtacacs tacacs+ radius >
説明	本コマンドは、認証サーバーグループを設定します。認証サーバーグループを作成します。サーバーグループとは、TACACS/XTACACS/TACACS+/RADIUSのサーバーを、ユーザー定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。ユーザーはサーバーグループのタイプをプロトコルによって、または定義済みサーバーグループによって定義できます。本コマンドを使用して、最大8個までの認証サーバーをこのグループに追加することができます。
パラメーター	<p>server_group - スイッチに実装するプロトコルグループ (TACACS/XTACACS/TACACS+/RADIUS)、または「create authen server_group」コマンドで作成したユーザー定義グループによってグループを定義します。</p> <p>tacacs - スイッチに実装されている TACACS サーバープロトコルを使用します。TACACS プロトコルを使用するサーバーだけをこのグループに追加することができます。</p> <p>xtacacs - スイッチに実装されている XTACACS サーバープロトコルを使用します。XTACACS プロトコルを使用するサーバーだけをこのグループに追加することができます。</p> <p>tacacs+ - スイッチに実装されている TACACS+サーバープロトコルを使用します。TACACS+プロトコルを使用するサーバーだけをこのグループに追加することができます。</p> <p>radius - スイッチに実装されている RADIUS サーバープロトコルを使用します。RADIUS プロトコルを使用するサーバーだけをこのグループに追加することができます。</p> <p><string 15> - 15文字以内の半角英数字の文字列を入力して、作成済みのサーバーグループを定義します。本グループはプロトコルにかかわらずサーバーのどんな組み合わせも追加することができます。</p> <p>add/delete - サーバーグループからサーバーを追加または削除します。</p> <p>server_host <ipaddr> - 追加または削除するリモートサーバーの IP アドレスを入力します。</p> <p>protocol - サーバーが使用するプロトコルを入力します。次の4つのオプションがあります：</p> <p>tacacs - サーバーが TACACS 認証プロトコルを使用している場合に指定します。</p> <p>xtacacs - サーバーが XTACACS 認証プロトコルを使用している場合に指定します。</p> <p>tacacs+ - サーバーが TACACS+認証プロトコルを使用している場合に指定します。</p> <p>radius - サーバーが RADIUS 認証プロトコルを使用している場合に指定します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: サーバグループ「group_1」に認証ホストを追加するには

```
# config authn server_group group_1 add server_host 10.1.1.121 protocol tacacs+
Command: config authn server_group group_1 add server_host 10.1.1.121 protocol tacacs+

Success.

#
```

3.35.20 delete authn server_group

目的	ユーザー定義の認証サーバグループを削除します。
構文	delete authn server_group <string 15>
説明	本コマンドは、認証サーバグループを削除します。
パラメーター	<string 15> - 15文字以内の半角英数字の文字列を入力して、削除する作成済みのサーバグループを定義します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00以降

使用例: サーバグループ「group_1」を削除するには

```
#delete authn server_group group_1
Command: delete authn server_group group_1

Success.

#
```

3.35.21 show authn server_group

目的	スイッチの認証サーバグループを表示します。
構文	show authn server_group <string 15>
説明	本コマンドは、スイッチに現在設定されている認証サーバグループを表示します。 本コマンドは、次のフィールドを表示します。 Group Name - 実装されているグループおよびユーザー定義グループを含むスイッチに現在設定されているサーバグループの名前。 IP Address - サーバの IP アドレス。 Protocol - サーバが使用する認証プロトコル。
パラメーター	<string 15> - 15文字以内の半角英数字の文字列を入力して、表示する作成済みのサーバグループを定義します。 本コマンドを<string>パラメーターなしで入力すると、スイッチのすべての認証サーバグループを表示します。
制限事項	なし。
対応バージョン	1.00.00以降

使用例: スイッチに現在設定されている認証サーバーグループを表示するには

```
#show authen server_group
Command: show authen server_group

Group Name      IP Address      Protocol
-----
radius          -----
tacacs          -----
tacacs+         -----
xtacacs         -----

Total Entries : 4

#
```

3.35.22 config authen parameter response_timeout

目的	スイッチが、タイムアウトの前にユーザーからの認証のレスポンスを待つ時間を設定します。
構文	config authen parameter response_timeout <int 0-255>
説明	ユーザーからの認証のレスポンスに対するスイッチの待ち時間を指定します。
パラメーター	response_timeout <int 0-255> - コンソールまたは telnet からユーザーの認証レスポンスに対するスイッチの待ち時間を指定します。0 はタイムアウトにならないことを意味します。デフォルト値は 30 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: レスポンスのタイムアウトを 60 秒に設定するには

```
#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

#
```

3.35.23 config authen parameter attempt

目的	スイッチが認証の試みを許容する最大回数を設定します。
構文	config authen parameter attempt <int 1-255>
説明	本コマンドは、スイッチが認証の試みを許容する最大回数を設定します。ユーザーが認証を試みることができる最大回数。指定回数認証に失敗すると、そのユーザーはスイッチへのアクセスを拒否され、さらに認証を試みることができなくなります。コンソールの場合は、再度認証を行うために 60 秒待つ必要があります。Telnet の場合は、スイッチから切断されます。
パラメーター	parameter attempt <int 1-255> - ロックされる前にスイッチによる認証のために試みることができる最大回数を設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 認証試みの最大数に 5 を設定するには

<pre>#config authen parameter attempt 5 Command: config authen parameter attempt 5 Success. #</pre>

3.35.24 show authen parameter

目的	スイッチに現在設定されている認証パラメーターを表示します。
構文	show authen parameter
説明	本コマンドは、レスポンスタイムアウトおよびユーザー認証を試みる回数を含むスイッチに設定されている現在の認証パラメーターを表示します。 本コマンドは、次のフィールドを表示します。 Response timeout - コンソールまたは telnet からログインを試みるユーザーの認証レスポンスに対するスイッチの待ち時間に割り当てられる設定時間。 User attempts - ロックされる前にユーザーが認証を試みることができる最大回数。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに現在設定している認証パラメーターを参照するには

```
#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 5

#
```

3.35.25 enable admin

目的	ユーザーレベルから管理者レベルに権限を昇格します。
構文	enable admin
説明	本コマンドは、通常のユーザーレベルとしてスイッチにログインした後、管理者レベルに変更する場合に使用します。スイッチにログインした後のユーザーにはユーザーレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本コマンドを入力し、認証用パスワードを入力します。本機能における認証方法には、TACACS/XTACACS/TACACS+/RADIUS、ユーザー定義のサーバーグループ、local enable (スイッチのローカルアカウント) または、認証なし (none) があります。XTACACS と TACACS は local enable (スイッチのローカルアカウント) をサポートしていないため、ユーザーはサーバーに特別なアカウントを作成し、ユーザー名「enable」、および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「disable」(無効) である場合には実行できません。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチの管理者権限を有効にするには

```
#enable admin
Password: *****

#
```

3.35.26 config admin local_enable

目的	管理者レベルの権限のためのローカルイネーブルパスワードを設定します。
構文	config admin local_enable
説明	本コマンドは、「enable admin」コマンドのローカルで有効なパスワードを設定します。「local_enable」方式を選択してユーザーレベルの権限を管理者レベルの権限に上げると、このセクションに記載されるスイッチにローカルに登録したパスワードを入力するように要求されます。
パラメーター	<password 15> - 本コマンドを入力した後、ユーザーは元のパスワード、次に新しいパスワード、さらに確認のために再び新しいパスワードを入力します。パスワードは 15 文字以内の半角英数字で指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 「local_enable」認証方法のためのパスワードを設定するには

```
#config admin local_enable
Command: config admin local_enable

Enter the old password:
Enter the case-sensitive new password:*****
Enter the new password again for confirmation:*****
Success.

#
```

3.36 MAC ベースアクセス制御コマンド

3.36.1 enable mac_based_access_control

目的	MAC ベースアクセス制御を有効にします。
構文	enable mac_based_access_control
説明	本コマンドは、スイッチで MAC ベースアクセス制御を有効にします。デフォルトにより有効化されていません。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチに MAC ベースアクセス制御をグローバルで有効にするには

```
# enable mac_based_access_control
Command: enable mac_based_access_control

Success.

#
```

3.36.2 disable mac_based_access_control

目的	MAC ベースアクセス制御を無効にします。
構文	disable mac_based_access_control
説明	本コマンドは、スイッチの MAC ベースアクセス制御を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スイッチの MAC ベースアクセス制御をグローバルで無効にするには

```
# disable mac_based_access_control
Command: disable mac_based_access_control

Success.

#
```

3.36.3 config mac_based_access_control password

目的	MAC ベースアクセス制御のパスワードを設定します。
構文	config mac_based_access_control password <passwd 16>
説明	本コマンドは、RADIUS サーバー経由の認証に使用されるパスワードを設定します。
パラメーター	<password 16> - RADIUS モードでは、スイッチは RADIUS サーバーとの通信にパスワードを使用します。キーは 16 文字以内で指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御のパスワードを設定するには

```
#config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

#
```

3.36.4 config mac_based_access_control method

目的	MAC ベースアクセス制御の認証方法を設定します。
構文	config mac_based_access_control method < local radius >
説明	本コマンドは、認証方法をローカルデータベース経由か RADIUS 経由にするか設定します。
パラメーター	local - ローカルデータベースを経由した認証を指定します。 radius - RADIUS サーバーを経由した認証を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御メソッドを設定するには

```
#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

#
```

3.36.5 config mac_based_access_control auth_failover

目的	MAC ベースアクセス制御の failover を設定します。
構文	config mac_based_access_control auth_failover < enable disable >
説明	本コマンドは、radius サーバーからの認証応答がなく認証が失敗した際、認証方法をローカルデータベース経由へ切り替えるための failover 機能を設定します。
パラメーター	enable - RADIUS 認証サーバーの認証応答ない時 failover 機能を有効にします。 disable - RADIUS 認証サーバーの認証応答ない時 failover 機能を無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.07.00 以降

使用例:MAC ベースアクセス制御で failover 機能を有効にするには

```
#config mac_based_access_control auth_failover enable
Command: config mac_based_access_control auth_failover enable

Success.

#
```

3.36.6 config_mac_based_access_control_ports

目的	MAC ベースアクセス制御のパラメーターを設定します。
構文	config mac_based_access_control_ports < <portlist> all > < state < enable disable > mode < port_based host_based > aging_time < infinite <min 1-1440> > hold_time < infinite <sec 1-300> > max_users <no_limit <value 1-128> > >
説明	本コマンドは、MAC ベースアクセス制御設定のパラメーターを設定します。MAC アドレス認証機能がポートに対して有効で、ゲスト VLAN 機能が無効である場合、このポートに割り付けられているユーザーのトラフィックは、認証を通過しない限り転送されません。認証を通過しないユーザーは、スイッチによりサービスを提供されません。ユーザーが認証を通過すると、元の VLAN コンフィギュレーションのもとで操作されたトラフィックを転送することができます。
パラメーター	ports - MAC アドレス認証機能を有効または無効にするポート範囲を設定します。 state - MAC アドレス認証機能を有効または無効にします。 mode - ポートベースまたはホストベースのいずれかを指定します。ポートベースは、ポートに接続するすべてのユーザーがはじめての認証結果を共有することを意味します。 aging_time - 認証ホストが認証状態を保つ時間。aging_time がタイムアウトになると、ホストは未認証状態に戻ります。デフォルト値は 1440 分です。 hold_time - ホストが認証通過に失敗した場合に認証を開始できない時間。ユーザーがエントリー状態を手動でクリアしない限り、次の認証はこの時間内に開始しません。デフォルト値は 300 秒です。 max_users - ポート毎に収容可能な端末数を指定します。なお、ポート毎の収容数の総和は、装置全体の収容数(初期値128)設定の範囲内で制限されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御のポートの状態を設定するには

```
#config mac_based_access_control_ports 1-8 state enable
Command: config mac_based_access_control_ports 1-8 state enable

Success.

#
```

3.36.7 clear mac_based_access_control auth_mac

目的	ユーザーの現在の認証状態をリセットします。再認証は、再度ユーザートラフィックを受信した後に開始します。
構文	clear mac_based_access_control auth_mac < ports < all <portlist> > mac_addr <macaddr> >
説明	本コマンドは、ユーザー（またはポート）の認証状態をクリアします。ポート（またはユーザー）は未認証状態に戻ります。ポート(またはユーザー)に関連しているすべてのタイマーがリセットされます。
パラメーター	ports - MAC を削除するポート範囲を指定します。 <macaddr> - この MAC アドレスを持つホストを削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御により処理した MAC をクリアするには

```
#clear mac_based_access_control auth_mac ports all
Command: clear mac_based_access_control auth_mac ports all

Success.

#
```

3.36.8 create mac_based_access_control_local mac

目的	ローカルデータベースエントリーを作成します。
構文	create mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094>]
説明	本コマンドは、ローカルデータベースエントリーを作成します。
パラメーター	mac - ローカルモードでアクセスが許可される MAC アドレス。 vlan - MAC アドレスが認証されると、ポートはこの VLAN に割り当てられます。 vlanid - MAC アドレスが認証されると、ポートはこの VLAN に割り当てられます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御ローカルエントリーを作成するには

```
#create mac_based_access_control_local mac 00-40-66-00-00-01 vlan default
Command: create mac_based_access_control_local mac 00-40-66-00-00-01 vlan default

Success.

#
```

3.36.9 config mac_based_access_control_local mac

目的	MAC ベースアクセス制御ローカルデータベースエントリーを設定します。
構文	config mac_based_access_control_local mac <macaddr> <vlan <vlan_name 32> vlanid <vlanid 1-4094> >
説明	本コマンドは、「mac_based_access_control_local」コマンドを使用して、作成済みの MAC ベースアクセス制御ローカルデータベースエントリーを設定します。
パラメーター	mac - 認証ホストの MAC アドレスを指定します。 vlan - VLAN 名によってターゲット VLAN を指定します。このホストが認証されると、この VLAN に割り当てられます。 vlanid - VID によってターゲット VLAN を指定します。ホストが認証されると、ターゲット VLAN が存在する場合、この VLAN に割り当てられます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御ローカルデータベースエントリー 00-40-66-00-00-01 のターゲット VLAN 「default」を設定するには

```
# config mac_based_access_control_local mac 00-40-66-00-00-01 vlan default
Command: config mac_based_access_control_local mac 00-40-66-00-00-01 vlan default

Success.

#
```

3.36.10 delete mac_based_access_control_local

目的	ローカルデータベースエントリーを削除します。
構文	delete mac_based_access_control_local <mac <macaddr> <vlan <vlan_name 32> vlanid <vlanid 1-4094>>
説明	本コマンドは、ローカルデータベースエントリーを削除します。
パラメーター	mac - この MAC アドレスによってデータベースを削除します。 vlan - この VLAN 名のデータベースを削除します。 vlanid - この VLAN ID のデータベースを削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC アドレスによってローカルの MAC ベースアクセス制御を削除するには

```
#delete mac_based_access_control_local mac 00-40-66-00-00-01
Command: delete mac_based_access_control_local mac 00-40-66-00-00-01

Success.

#
```

使用例:VLAN 名によってローカルの MAC ベースアクセス制御を削除するには

```
#delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

#
```

3.36.11 show mac_based_access_control

目的	MAC ベースアクセス制御の設定を表示します。
構文	show mac_based_access_control [ports [<portlist>]]
説明	本コマンドは、MAC ベースアクセス制御の設定を表示します。
パラメーター	ports - MAC ベースアクセス制御のポートの状態を表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御を表示するには

```
#show mac_based_access_control
Command: show mac_based_access_control

MAC Based Access Control
-----
State           : Disabled
Method          : Local
Authentication Failover: Disabled
MAC Format Case  : Uppercase
MAC Format Delimiter : None
Password        : default
Password Type   : Manual String
Max Users       : 128

#
```

使用例:MAC ベースアクセス制御ポートを表示するには

```
#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4

Port  State      Aging Time  Hold Time  Auth Mode  Max Users
      (mins)    (secs)
-----
1     Enabled    100         100        Port_based 128
2     Enabled    100         200        Host_based 128
3     Enabled    50          300        Port_based 128
```


4	Enabled	200	100	Host_based	no limit
#					

3.36.12 show mac_based_access_control_local

目的	MAC ベースアクセス制御ローカルデータベースを表示します。
構文	show mac_based_access_control_local [< mac <macaddr> < vlan <vlan_name 32> vlanid <vlanid 1-4094> >]
説明	本コマンドは、MAC ベースアクセス制御ローカルデータベースを表示します。
パラメーター	mac - 本 MAC アドレスによって MAC ベースアクセス制御ローカルデータベースを表示します。 vlan - VLAN 名によって MAC ベースアクセス制御ローカルデータベースを表示します。 vlanid - VLAN ID によって MAC ベースアクセス制御ローカルデータベースを表示します。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御ローカルデータベースを表示するには

```
#show mac_based_access_control_local
Command: show mac_based_access_control_local

  MAC Address          VLAN Name          VID
  -----
00-40-66-00-00-01    default            1
00-40-66-00-00-02    v123               123
00-40-66-00-00-03    v123               123
00-40-66-00-00-04    default            1

Total Entries: 4

#
```

使用例:MAC アドレスから MAC ベースアクセス制御ローカルデータベースを表示するには

```
#show mac_based_access_control_local mac 00-40-66-00-00-01
Command: show mac_based_access_control_local mac 00-40-66-00-00-01

  MAC Address          VLAN Name          VID
  -----
00-40-66-00-00-01    default            1

Total Entries: 1

#
```

使用例:VLAN から MAC ベースアクセス制御ローカルデータベースを表示するには

```
#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address          VLAN Name          VID
-----
00-40-66-00-00-01   default           1
00-40-66-00-00-02   default           1

Total Entries: 2

#
```

3.36.13 show mac_based_access_control auth_mac

目的	MAC ベースアクセス制御の認証状態を表示します。
構文	show mac_based_access_control auth_mac [ports <portlist>]
説明	本コマンドは、MAC ベースアクセス制御の認証状態を表示します。
パラメーター	ports - ポートから認証ステータスを表示します。
制限事項	なし。

使用例:MAC ベースアクセス制御の状態を表示するには

```
# show mac_based_access_control auth_mac
Command: show mac_based_access_control auth_mac ports 9

Port Number : 9
Index MAC Address          Auth State          VID Aging Time/
                               Hold Time
-----
1      00-40-66-00-00-00   Authenticated      200 45
2      00-40-66-00-00-05   Failure             1   1

CTRL+C ESC q QUIT SPACE n Next Page ENTER Next Entry a All
```

3.36.14 config mac_based_access_control max_users

目的	認証クライアントの最大数を設定します。
構文	config mac_based_access_control max_users < no_limit <value 1-128> >
説明	本コマンドは、装置全体の収容可能な端末数を指定します。
パラメーター	no_limit - ポート毎の収容数(初期値 128)設定と併せて no_limit 指定した場合、FDB 最大登録数の 8K まで収容可能となります。 <value 1-128> - 装置全体の収容可能な端末数を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:MAC ベースアクセス制御の最大ユーザー数を設定するには

```
#config mac_based_access_control max_users 128
Command: config mac_based_access_control max_users 128

Success.

#
```

注意事項



MAC 認証の認証最大数を越えた場合、show fdb コマンドの Type 情報に BlockByMBA と表示されます。

BlockByMBA : MAC 認証許可されない場合に FDB 表示されます。

UnBlockByMBA : MAC 認証許可された場合に FDB 表示されます。

3.36.15 enable authorization network

目的	属性機能に対する認証をグローバルに有効化します。
構文	enable authorization network
説明	ネットワーク認証を有効にします。有効にすると、認証属性 (例: VLAN) が RADIUS サーバーまたはローカルデータベースによって割り当てられます。どの属性が許可されるかは、個々の設定に依存します。 属性の認証はデフォルトにより無効になっています。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:この例ではグローバル認証の状態を有効にするには

```
# enable authorization network
Command: enable authorization network

Success.

#
```

3.36.16 disable authorization network

目的	属性機能に対する認証をグローバルに無効化します。
構文	disable authorization network
説明	ネットワーク認証を無効にします。 属性の認証が無効になっている場合、RADIUS サーバーまたはローカルデータベースによって割り当てられた認証済み属性（例：VLAN）は、個々のモジュール設定が有効になっていても無視されます。 属性の認証はデフォルトにより無効になっています。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: この例ではグローバル認証の状態を無効にするには

```
# disable authorization network
Command: disable authorization network

Success.

#
```

3.36.17 show authorization

目的	認証ステータスを表示します。
構文	show authorization
説明	認証ステータスを表示します。
パラメーター	なし。
制限事項	なし。

使用例: この例は、認証ステータスを表示します。

```
#show authorization
Command: show authorization

Authorization : Enabled

#
```

3.36.18 config mac_based_access_control mac_format

目的	MAC ベースアクセス制御の MAC アドレスフォーマットを設定します。
構文	config mac_based_access_control mac_format < case [lowercase uppercase] delimiter [hyphen none] >
説明	本コマンドは、RADIUS サーバーを経由した MAC ベース認証時の MAC アドレスフォーマットを設定します。
パラメーター	case - MAC アドレスの大文字/小文字を選択するときに設定します。 lowercase - MAC アドレスを小文字に限定するときに設定します。

	uppercase - MAC アドレスを大文字に限定するときに設定します。 delimiter - MAC アドレスの区切り文字を使用するときに設定します。 hyphen - MAC アドレスの区切り文字としてハイフンを使用するときに設定します。 none - MAC アドレスの区切り文字を使用しないときに設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。

使用例: MAC アドレスフォーマットを大文字/区切り文字なしに設定するには

```
# config mac_based_access_control mac_format case uppercase delimiter none
Command: config mac_based_access_control mac_format case uppercase delimiter none

Success.

#
```

3.36.19 config mac_based_access_control password_type

目的	MAC ベースアクセス制御のパスワードタイプを設定します。
構文	config mac_based_access_control password_type < manual_string client_mac_address >
説明	本コマンドは、RADIUS サーバー認証時のパスワードタイプを設定します。
パラメーター	manual_string - RADIUS認証時に装置に設定したパスワードを使用します。 client_mac_address - RADIUS認証時にクライアントのMACアドレスをパスワードとして使用します。
制限事項	管理者アカウントのみ本コマンドを実行できます。

使用例: 認証パスワードタイプを入力文字列に設定するには

```
# config mac_based_access_control password_type manual_string
Command: config mac_based_access_control password_type manual_string

Success.

#
```

3.37 マルチプル認証コマンド

3.37.1 config authentication auth_mode

目的	ポートに設定された認証方式の認証モードを設定します。
構文	config authentication auth_mode <port_based host_based>
説明	本コマンドは、設定された MAC/802.1X/WEB 認証方式の認証モードを設定します。
パラメーター	auth_mode - 認証モードを指定します。 port_based - 1つのホストが認証された場合、同じポート上の全てのホストがアクセスを許可されます。認証に失敗した場合には、そのポートは次の認証の試みを継続します。 host_based - 全てのユーザーは個別に認証されます。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: 全ポートの認証モードをポートベースに設定するには

```
#config authentication auth_mode port_based
Command: config authentication auth_mode port_based

Success.

#
```

3.37.2 show authentication ports

目的	ポートに設定された認証方式の認証モードを表示します。
構文	show authentication ports [<portlist>]
説明	本コマンドは、ポートに設定された認証方式の認証モードを表示します。
パラメーター	<portlist> - 指定したポートの認証モードを表示します。ポートの指定が省略された場合には、全ポートの認証モードを表示します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: ポート1から5のセキュリティーモードを表示するには

```
#show authentication ports 1-5
Command: show authentication ports 1-5

Port Authorized Mode
-----
1   Port_based
2   Port_based
3   Port_based
4   Port_based
5   Port_based

#
```

3.38 SSH コマンド

リモート PC (SSH クライアント) とスイッチ (SSH サーバー) 間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

- (1) 「create account admin <username> <password>」コマンドで管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザーアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。
- (2) 「config ssh user authmode」コマンドを使用して、ユーザーアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザーの認証方法を指定します。この認証方法には、「password」、「publickey」、「hostbased」の 3 つがあります。
- (3) SSH クライアントとサーバー間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。
- (4) 「enable ssh」コマンドで、SSH を有効にします。

これらの手順が完了後、安全な帯域内の通信を使用してリモート PC からスイッチの管理を行うことができます。

3.38.1 enable ssh

目的	SSH を有効にします。
構文	enable ssh
説明	本コマンドは、スイッチの SSH を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：SSH を有効にするには

<pre>#enable ssh Command: enable ssh Success. #</pre>

3.38.2 disable ssh

目的	SSH を無効にします。
構文	disable ssh
説明	本コマンドは、スイッチの SSH を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：SSH を無効にするには

```
# disable ssh
Command: disable ssh

Success.

#
```

3.38.3 config ssh authmode

目的	SSH 認証モードの設定を行います。
構文	config ssh authmode < password publickey hostbased > < enable disable >
説明	本コマンドは、ユーザーがスイッチにアクセスするための SSH 認証モードを設定します。
パラメーター	password - 本パラメーターは、管理者がスイッチにおける認証にローカルに設定したパスワードを使用したいときに選択します。 publickey - 本パラメーターは、管理者が認証に SSH サーバーで設定した公開鍵のコンフィギュレーションセットを使用したいときに選択します。 hostbased - 本パラメーターは、管理者が認証にホストコンピュータを使用したいときに選択します。本パラメーターは SSH 認証機能を必要とする Linux ユーザー向けに設定され、ホストコンピュータには SSH プログラムがインストールされ、Linux オペレーティングシステムが起動している必要があります。 <enable disable> - スイッチに指定された SSH 認証を「enable」(有効)または「disable」(無効)にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:パスワードによる SSH 認証モードを有効にするには

```
#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

#
```

3.38.4 show ssh authmode

目的	SSH 認証モードの設定を表示します。
構文	show ssh authmode
説明	本コマンドは、スイッチに設定された現在の SSH 設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチに設定された現在の認証モードを表示するには

```
#show ssh authmode
Command: show ssh authmode

The SSH Authmode:
-----
Password   : Enabled
Publickey  : Enabled
Hostbased  : Enabled

#
```

3.38.5 config ssh server

目的	SSH サーバーを設定します。
構文	config ssh server < maxsession <int 1-8> contimeout <sec 120-600> authfail <int 2-20> rekey < 10min 30min 60min never > >
説明	本コマンドは、SSH サーバーを設定します。
パラメーター	maxsession <int 1-8> - スイッチに同時に接続できるユーザー数を設定します。デフォルト値は 8 です。 contimeout <sec 120-600> - 接続のタイムアウト時間を指定します。120 ~ 600 秒の範囲で時間を設定します。デフォルト値は 120 秒です。 authfail <int 2-20> - ユーザーが SSH 認証を使用してログインを試みることができる上限回数を管理者が指定します。指定した上限回数を超えるとスイッチは接続を切り、ユーザーは再度スイッチに再接続し、ログインをし直す必要があります。 rekey <10min 30min 60min never> - スイッチが SSH 暗号を変更する期間を設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: SSH サーバーを設定するには

```
#config ssh server maxsession 2 contimeout 300 authfail 2
Command: config ssh server maxsession 2 contimeout 300 authfail 2

Success.

#
```

3.38.6 show ssh server

目的	SSH サーバーの設定を表示します。
構文	show ssh server
説明	本コマンドは、SSH サーバーの設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例：SSH サーバーを表示するには

<pre>#show ssh server Command: show ssh server SSH Server Status : Disabled SSH Max Session : 8 Connection Timeout : 120 (sec) Authenticate Failed Attempts : 2 Rekey Timeout : never Listened Port Number : 22 #</pre>	
---	--

3.38.7 config ssh user

目的	SSH ユーザーを設定します。
構文	config ssh user <username 15> authmode < hostbased < hostname <domain_name 32> > < hostname_IP <domain_name 32> <ipaddr> > password publickey >
説明	本コマンドは、SSH ユーザー認証方法を設定します。
パラメーター	<p><username 15> - SSH ユーザーを識別するユーザー名を 15 文字までの半角英数字で指定します。</p> <p>authmode - スイッチへのログインを希望する SSH ユーザーの認証モードを指定します。管理者は以下のパラメーターを選択することができます。</p> <p>hostbased - 認証用にリモート SSH サーバーを使用する場合に選択します。本パラメーターを選択すると、SSH ユーザー識別のために以下の入力が必要になります。</p> <p>hostname <domain_name 32> - リモートの SSH ユーザーを識別する 32 文字以内の半角英数字の文字列を入力します。</p> <p>hostname_IP <domain_name 32> <ipaddr> - SSH ユーザーのホスト名と対応する IP アドレスを入力します。</p> <p>password - 管理者定義のパスワードを使用してユーザー認証を行う場合に選択します。本コマンドを入力すると、スイッチはユーザーにパスワードの入力を要求し、次にパスワードを再度タイプして確認するようプロンプトします。</p> <p>publickey - SSH サーバー上の公開鍵を使用して認証を行う場合に選択します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SSH ユーザーを設定するには

```
# config ssh user HCL authmode password
Command: config ssh user HCL authmode password

Success.

#
```

3.38.8 show ssh user authmode

目的	SSH ユーザーの設定を表示します。
構文	show ssh user authmode
説明	本コマンドは、SSH ユーザーの設定を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SSH ユーザーを表示するには

```
#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
Username    AuthMode   HostName           HostIP
-----
HCL         Password

Total Entries : 1

#
```

注意事項



SSH ユーザーを設定するには、管理者はスイッチにユーザーアカウントを作成する必要があります。ユーザーアカウント設定に関する情報については、本マニュアルの「create account」を参照してください。

3.38.9 config ssh algorithm

目的	SSH アルゴリズムを設定します。
構文	config ssh algorithm < 3DES AES128 AES192 AES256 arcfour blowfish cast128 twofish128 twofish192 twofish256 MD5 SHA1 RSA DSA > < enable disable >
説明	本コマンドは、認証の暗号化に使用される SSH アルゴリズムのタイプを設定します。
パラメーター	<p>3DES - Triple_Data Encryption Standard 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>AES128 - Advanced Encryption Standard AES128 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>AES192 - Advanced Encryption Standard AES192 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>AES256 - Advanced Encryption Standard AES256 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>arcfour - Arcfour 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>blowfish - Blowfish 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>cast128 - Cast128 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>twofish128 - Twofish 128 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>twofish192 - Twofish192 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>MD5 - MD5 Message Digest 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>SHA1 - Secure Hash Algorithm 暗号化を「enable」(有効)または「disable」(無効)にします。</p> <p>RSA - RSA 暗号化アルゴリズムを「enable」(有効)または「disable」(無効)にします。</p> <p>DSA - Digital Signature Algorithm 暗号化を「enable」(有効)または「disable」(無効)にします。</p> <p><enable disable> - スイッチに本コマンドで入力したアルゴリズムを「enable」(有効)または「disable」(無効)にします。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例：SSH アルゴリズムを設定するには

```
# config ssh algorithm blowfish enable
Command: config ssh algorithm blowfish enable

Success.

#
```

3.38.10 show ssh algorithm

目的	SSH アルゴリズムの設定を表示します。
構文	show ssh algorithm
説明	本コマンドは、SSH アルゴリズムの設定ステータスを表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例：スイッチに現在設定されている SSH アルゴリズムを表示するには

```
#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
-----
3DES      : Enabled
AES128    : Enabled
AES192    : Enabled
AES256    : Enabled
arcfour   : Enabled
blowfish  : Enabled
cast128   : Enabled
twofish128 : Enabled
twofish192 : Enabled
twofish256 : Enabled

Data Integrity Algorithm
-----
MD5       : Enabled
SHA1      : Enabled

Public Key Algorithm
-----
RSA       : Enabled

CTRL+C ESC q QUIT SPACE n Next Page ENTER Next Entry a All
```

3.39 SSL コマンド

Secure Sockets Layer (SSL) とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。

このセキュリティ機能は、認証セッションに使用する厳密な暗号パラメーター、特定の暗号化アルゴリズムおよびキー長を決定する、暗号スイートと呼ばれるセキュリティ文字列により実現しています。SSL は、以下の 3 つの段階で構成されます。

- (1) 鍵交換：暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA (Rivest Shamir Adleman) 公開鍵アルゴリズムとデジタル署名アルゴリズム (DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定) を使用します。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。
- (2) 暗号化：暗号スイートの次の段階は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
 - ・ ストリーム暗号 - スwitchは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。これらの鍵はメッセージの暗号化に使用され、最適な使用のためにはクライアントとホスト間で一致させる必要があります。
 - ・ CRC ブロック暗号 - CBC (Cipher Block Chaining : 暗号ブロック連鎖) とは、前に暗号化したブロックの暗号文を使用して現在のブロックの暗号化を行う方法です。本スイッチは、DES (Data Encryption Standard) で定義する 3 DES_EDE 暗号化コードをサポートし、暗号文を生成します。
- (3) ハッシュアルゴリズム：暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージで暗号化され、整合性を提供し、再送攻撃を防止します。本スイッチは、MD5(Message Digest 5)と SHA(Secure Hash Algorithm)の 2 種類のハッシュアルゴリズムをサポートします。

これら 3 つのパラメーターは、スイッチ上での 4 つの選択肢として独自に組み合わせられ、サーバーとホスト間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を変換させて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバーを使用してスイッチにダウンロードできます。本スイッチは、SSLv3 および TLSv1 をサポートしています。SSL の他のバージョンは本スイッチとは互換性がないおそれがあり、クライアントからホストへの認証やメッセージ転送時に問題が発生する場合があります。



3.39.1 enable ssl

目的	スイッチの SSL 機能を有効にします。
構文	enable ssl [ciphersuite < RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5 >]
説明	本コマンドは、スイッチにリストされた暗号スイートの 1 つ以上の組み合わせによりスイッチの SSL を有効にします。パラメーターなしで本コマンドを入力することによってスイッチの SSL ステータスを有効にします。SSL を無効にすると、スイッチの Web マネージャーが無効になります。
パラメーター	<p>ciphersuite - 暗号スイートは認証セッションに使用する、正確な暗号のパラメーター、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。ユーザーは以下のどの組み合わせも選択できます。</p> <p>RSA_with_RC4_128_MD5 - RSA key exchange、stream cipher C4(128-bit keys)、MD5 Hash Algorithm の組み合わせです。</p> <p>RSA_with_3DES_EDE_CBC_SHA - RSA key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。</p> <p>DHE_DSS_with_3DES_EDE_CBC_SHA - DSA Diffie Hellman key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。</p> <p>RSA_EXPORT_with_RC4_40_MD5 - RSA Export key exchange と stream cipher RC4 encryption (40 ビットキー) の組み合わせです。</p> <p>暗号スイートは、デフォルトでは有効になっていますが、SSL 機能はデフォルトにより無効になっています。暗号スイートを持つ SSL を有効にしてもスイッチの SSL ステータスは有効になりません。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: すべての暗号スイートに対し、スイッチの SSL 機能を有効にするには

<pre>#enable ssl Command: enable ssl Note: Web will be disabled if SSL is enabled. Success. #</pre>

注意事項

-  スwitchの SSL 機能を有効にするとすべての暗号スイートが有効になります。特定の暗号スイートを使用するには、適切な暗号スイートと共に無効 SSL コマンドを使用して他の暗号スイートを無効にする必要があります。
-  スwitchの SSL 機能を有効にすると、スイッチは Web マネージャー用のポート(ポート 80)を無効にします。Web マネージャーにログインするためには、URL のエントリーは「https://」で始まる必要があります(例: <https://10.90.90.90>)。

3.39.2 disable ssl

目的	スイッチの SSL 機能を無効にします。
構文	disable ssl [ciphersuite < RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5 >]
説明	本コマンドは、スイッチの SSL を無効にし、スイッチの暗号スイートのどんな組み合わせも無効にすることができます。
パラメーター	<p>ciphersuite - 暗号スイートは認証セッションに使用する、正確な暗号のパラメーター、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。ユーザーは以下のどの組み合わせも選択できます。</p> <p>RSA_with_RC4_128_MD5 - RSA key exchange、stream cipher C4(128-bit keys)、MD5 Hash Algorithm の組み合わせです。</p> <p>RSA_with_3DES_EDE_CBC_SHA - RSA key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。</p> <p>DHE_DSS_with_3DES_EDE_CBC_SHA - DSA Diffie Hellman key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。</p> <p>RSA_EXPORT_with_RC4_40_MD5 - RSA Export key exchange と stream cipher RC4 (40 ビットキー) の組み合わせです。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: スwitchの SSL ステータスを無効にするには

```
#disable ssl
Command: disable ssl

Success.

#
```

使用例: 暗号化スイート RSA_EXPORT_with_RC4_40_MD5 のみを無効にするには

```
#disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5

Success.

#
```


3.39.3 config ssl cachetimeout timeout

目的	SSL キャッシュタイムアウトを設定します。
構文	config ssl cachetimeout timeout <value 60-86400>
説明	本コマンドは、SSL 機能を使用してクライアントとホスト間の新しい鍵交換の間隔を設定します。クライアントとホストが鍵交換をすると常に新しい SSL セッションが確立します。この値を長くすると SSL セッションによる特定のホストとの再接続には主鍵が再利用されます。
パラメーター	timeout <value 60-86400> - 60 ~ 86400 の範囲でタイムアウト時間を入力して設定し、SSL モジュールが新しく完全な SSL ネゴシエーションを必要となる前に SSL 鍵 ID が有効性を維持する合計時間を指定します。デフォルトのキャッシュタイムアウトは、600 秒です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例:SSL キャッシュタイムアウトを 7200 秒に設定するには

<pre>#config ssl cachetimeout timeout 7200 Command: config ssl cachetimeout timeout 7200 Success. #</pre>

3.39.4 show ssl cachetimeout

目的	SSL キャッシュタイムアウトを表示します。
構文	show ssl cachetimeout
説明	本コマンドは、スイッチに現在設定されている SSL キャッシュタイムアウトを参照します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例:スイッチに設定されている SSL キャッシュタイムアウトを参照するには

<pre>#show ssl cachetimeout Command: show ssl cachetimeout Cache timeout is 600 second(s). #</pre>
--

3.39.5 show ssl

目的	スイッチ上の SSL ステータスと証明ファイルのステータスを表示します。
構文	show ssl
説明	本コマンドは、スイッチ上の SSL ステータスを参照します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチ上の SSL ステータスを参照するには

```
#show ssl
Command: show ssl

SSL Status                               Disabled
RSA_WITH_RC4_128_MD5                     0x0004 Enabled
RSA_WITH_3DES_EDE_CBC_SHA                 0x000A Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA            0x0013 Enabled
RSA_EXPORT_WITH_RC4_40_MD5               0x0003 Enabled

#
```

3.39.6 show ssl certificate

目的	スイッチ上の SSL 証明ファイルのステータスを参照します。
構文	show ssl certificate
説明	本コマンドは、スイッチ上の SSL 証明書ファイルの情報を参照します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.00.00 以降

使用例: スイッチ上の証明書ファイル情報を参照するには

```
# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

#
```

3.39.7 download ssl certificate

目的	スイッチ上の SSL 機能用証明ファイルをダウンロードします。
構文	download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>
説明	本コマンドは、スイッチで SSL 機能を使用するための証明書ファイルを TFTP サーバーからダウンロードするときに使用します。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータ記録であり、所有者の情報や認証のための鍵、またデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバーとクライアントが一致した証明書ファイルを持つ必要があります。本スイッチは、拡張子「.der」を持つ証明書を 1 つのみサポートします。
パラメーター	<ipaddr> - TFTP サーバーの IP アドレスを入力します。 certfilename <path_filename 64> - ダウンロードする証明書ファイルのパスとファイル名を入力します。 keyfilename <path_filename 64> - ダウンロードする秘密鍵交換ファイルのパスとファイル名を入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.00.00 以降

使用例: 証明書ファイルと秘密鍵ファイルをスイッチにダウンロードするには

```
#download ssl certificate 10.53.13.94 certfilename c:/cert.der keyfilename c:/pkey.der
Command: download ssl certificate 10.53.13.94 certfilename c:/cert.der keyfilename c:/pkey.der

Certificate Loaded Successfully!

#
```

3.40 WEB 認証コマンド

3.40.1 enable web_authentication

目的	WEB 認証機能を有効にします。
構文	enable web_authentication
説明	このコマンドは WEB 認証機能を有効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証機能を有効にするには

<pre>#enable web_authentication Command: enable web_authentication Success. #</pre>

3.40.2 disable web_authentication

目的	WEB 認証機能を無効にします。
構文	disable web_authentication
説明	このコマンドは WEB 認証機能を無効にします。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証機能を無効にするには

<pre>#disable web_authentication Command: disable web_authentication Success. #</pre>

3.40.3 create web_authentication user

目的	コマンドは WEB 認証のローカルユーザーを作成します。
構文	create web_authentication user <username 15> [vlan <vlan_name 32> vlanid <vlanid 1-4094>]
説明	WEB 認証のローカルユーザーを作成する時に使用するコマンドです。VLAN が指定されない場合又は割り当てられた VLAN が存在しない場合には、WEB 認証ユーザーはデフォルト VLAN のみアクセスすることが可能です。
パラメーター	User - WEB ベースのアクセス制御用のアカウントを作成します。 <username 15> - 半角英数字 15 文字以内でユーザー名を作成します。 Vlan - 認証 VLAN 名を指定します <vlan_name 32> - MAC アドレスが存在する VLAN 名。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証のローカルユーザーを作成するには

<pre>#create web_authentication user webuser vlan default Command: create web_authentication user webuser vlan default Enter a case-sensitive new password:***** Enter the new password again for confirmation:***** Success. #</pre>

3.40.4 config web_authentication user

目的	このコマンドは WEB 認証ローカルユーザーを設定します。
構文	config web_authentication user <username 15> [vlan clear_vlan] Vlan = vlan <vlan_name 32> vlanid <vlanid 1-4094>
説明	WEB 認証ローカルユーザーを設定する時に使用するコマンドです。VLAN が指定されない場合又は割り当てられた VLAN が存在しない場合、WEB 認証ユーザーはデフォルト VLAN のみにアクセスすることが可能です。
パラメーター	User - WEB ベースアクセス制御用のアカウントを指定します。 <username 15> - 半角英数字 15 文字以内でユーザー名を指定します。 Vlan - 認証 VLAN 名を指定します <vlan_name 32> - MAC アドレスが存在する VLAN 名。 Clear vlan - このアカウントにリンクされている VLAN 情報をクリアします
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証ローカルユーザーを設定するには

```
#config web_authentication user webuser clear_vlan
Command: config web_authentication user webuser clear_vlan

Success.

#
```

3.40.5 config web_authentication auth_failover

目的	WEB 認証の failover を設定します。
構文	config web_authentication auth_failover < enable disable >
説明	本コマンドは、radius サーバーからの認証応答がなく認証が失敗した際、認証方法をローカルデータベース経由へ切り替えるための failover 機能を設定します。
パラメーター	enable - RADIUS 認証サーバーの認証応答ない時 failover 機能を有効にします。 disable - RADIUS 認証サーバーの認証応答ない時 failover 機能を無効にします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証で failover 機能を有効にするには

```
#config web_authentication auth_failover enable
Command: config web_authentication auth_failover enable

Success.

#
```

3.40.6 config web_authentication authorization network

目的	ネットワークにおける認証の許可を有効にします。
構文	config web_authentication authorization network [radius <enable disable> local <enable disable>]
説明	Radius 認証が有効になると、RADIUS サーバーより割り当てられた認証データを受け取ります。 ローカル認証が有効になると、ローカルデータベースより割り当てられた認証データを受け取ります。
パラメーター	Radius - 有効になると、RADIUS サーバーにより割り当てられた認証データを受け取ります。デフォルト状態は有効です。 Local - 有効になると、ローカルデータベースにより割り当てられた認証データを受け取ります。デフォルト状態は有効です。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: ローカル認証の受け取りを有効にするには

```
#config web_authentication authorization network local enable
Command: config web_authentication authorization network local enable

Success.

#
```

3.40.7 config web_authentication clear_redir_url

目的	WEB 認証のリダイレクト URL を消去します。
構文	config web_authentication clear_redir_url
説明	リダイレクト URL がクリアされると、認証が成功した後にクライアントはログアウトページにリダイレクトされます。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証のデリダイレクト URL をクリアするには

```
#config web_authentication clear_redir_url
Command: config web_authentication clear_redir_url

Success.

#
```

3.40.8 config web_authentication method

目的	WEB 認証方法を設定します。
構文	config web_authentication method <local radius>
説明	このコマンドにより、WEB 認証に使用される RADIUS プロトコルをユーザーが指定することが可能です。 このコマンドにより RADIUS プロトコルが設定されると、WEB 認証は 802.1X 認証と同じく RADIUS 設定を共有します。“config radius”コマンドによって追加された RADIUS サーバーが当該プロトコルをサポートしている必要があります。
パラメーター	Local - ローカルデータベースを介して認証が行われることを指定します。 Radius - RADIUS サーバーを介して認証が行われることを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証方法を設定するには

```
#config web_authentication method radius
Command: config web_authentication method radius

Success.

#
```

3.40.9 config web_authentication ports

目的	ポートの WEB 認証パラメーターを設定します。
構文	config web_authentication ports <<portlist> all> [<i>state</i>] <i>State</i> =state <enable disable> aging_time <infinite <min 1-1440>> block_time <<sec 0-300>>
説明	このコマンドはポートの WEB 認証パラメーターを設定します。
パラメーター	ports - この設定に使用されるポート範囲を指定します。 <portlist> - この設定に使用されるポートリストを入力します。 all - この設定に使用される全てのポートを指定します。 state - WEB 認証のポート状態を指定します。 aging_time - 認証されたホストが認証状態を保持している間隔を指定します。 infinite - 認証されたホストがエージアウトされないように指定します。 block_time - 認証に失敗したホストをブロックさせる時間を指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: ポート 1-9 の WEB 認証状態を有効にするには

```
#config web_authentication ports 1-9 state enable
Command: config web_authentication ports 1-9 state enable

Success.

#
```

注意事項



WEB 認証が有効なポートで認証の対象となるフレームは、イーサネットフレームタイプが IP かつ IP プロトコルタイプが TCP のフレームとなります。
認証の対象外となるフレーム（例えば ICMP, UDP など）は、認証テーブルへ登録されませんが、認証による廃棄は行われませんのでご注意ください。
また、IPv6 についても認証の対象外フレームのため装置中継されます。

3.40.10 config web_authentication redir_url

目的	WEB 認証リダイレクト URL を設定します。
構文	config web_authentication redir_url <string 128>
説明	リダイレクト URL が設定された場合、ユーザーは認証が成功した後、このパスにリダイレクトされます。 このパスがクリアされると、クライアントは認証が成功した後、他の URL にリダイレクトされません。
パラメーター	<string 128> - 認証が成功した後のクライアントがリダイレクトされる URL を指定します。デフォルトではリダイレクト経路はクリアされています。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証デフォルトリダイレクト URL を設定するには

<pre>#config web_authentication redir_url http://www.website.com Command: config web_authentication redir_url http://www.website.com Success. #</pre>

3.40.11 config web_authentication switch_http_port

目的	WEB 認証が使用するスイッチの HTTP ポートを設定します。
構文	config web_authentication switch_http_port <tcp_port_number 1-65535> [<http https>]<="" td="" =""> </http>
説明	HTTP 又は HTTPS 用の TCP ポートは、HTTP 又は HTTPS パケットを認識するために使用されます。HTTP 又は HTTPS パケットは CPU の認証処理又はログインページにアクセスするために使用されます。 指定されない場合、HTTP のデフォルトポート番号は 80 です。そして HTTPS のデフォルトポート番号は 443 です。何もプロトコルが指定されない場合、デフォルトプロトコルは HTTP です。HTTP は TCP ポート 443 にて動作できません。また HTTPS は TCP ポート 80 にて動作できません。 ホストが HTTPS モード下で強制的に認証するようになりたい場合、WEB 認証パラメーター "switch_http_port" を "https" に設定する必要があります。そして "enable SSL" コマンドは最初に設定しなければなりません。
パラメーター	switch_http_port - WEB 認証スイッチが使用し、ユーザーが認証プロセスを終了する TCP ポートを指定します。ポート番号の範囲は 1 から 65535 です。 http - WEB 認証が当該 TCP ポート上で HTTP プロトコルで動作することを指定します。 https - WEB 認証が当該 TCP ポート上で HTTPS プロトコルで動作することを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証が使用するスイッチの HTTP ポートを 8888 に設定するには

```
#config web_authentication switch_http_port 8888 http
```

```
Command: config web_authentication switch_http_port 8888 http
```

```
Success.
```

```
#
```

3.40.12 config web_authentication auth_page

目的	WEB 認証で使用する認証画面にユーザーが表示させたい任意の文字列情報を設定します。
構文	config web_authentication auth_page <<login logout> <default customize_text_box line <value 1-8>> <content <multiword 70> clear>>
説明	本コマンドにより管理者はWEB 認証 login または logout 画面に任意の文字列情報をカスタマイズして表示させることが可能となります。
パラメーター	login - カスタマイズする WEB 認証 login 画面を指定します。 logout - カスタマイズする WEB 認証 logout 画面を指定します。 default - WEB 認証画面を初期値に戻します。カスタマイズされた内容をクリアします。 line - テキストボックスのカスタマイズを指定します。 <value 1-8> - カスタマイズするテキストボックス番号を指定します。 content - 選択したテキストボックスへカスタマイズする文字列登録を指定します。 <multiword 70> - 選択したテキストボックスへ登録するカスタマイズの任意文字列を最大で半角 70 文字にて入力します。全角の場合は最大 35 文字となります。登録対象となる文字列は先頭と最後尾に「」をおいて入力します。また、日本語を登録する場合は、使用するターミナルソフトウェアにてエンコード方式を Shift-JIS に設定してください。 clear - 選択したテキストボックスに登録されているカスタマイズ文字列をクリアします。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.07.00 以降

使用例: WEB 認証 login 画面に任意の文字列をカスタマイズ表示設定するには

```
#config web_authentication auth_page login customize_textbox_line 1 content "ご利用方法がわからない方は下記へご連絡ください。"
```

```
Command: config web_authentication auth_page login customize_textbox_line 1 content "ご利用方法がわからない方は下記へご連絡ください。"
```

```
#config web_authentication auth_page login customize_textbox_line 8 content "MAIL      : taro.densen@hitachi-metals.com"
```

```
Command: config web_authentication auth_page login customize_textbox_line 8 content "MAIL      : taro.densen@hitachi-metals.com"
```

```
#
```

使用例: WEB 認証 login 画面のカスタマイズ文字列をクリアするには

```
#config web_authentication auth_page login customize_textbox_line 1 clear
Command: config web_authentication auth_page login customize_textbox_line 1 clear

#
```

使用例: WEB 認証 login 画面のカスタマイズ文字列を default に戻すには

```
#config web_authentication auth_page login default
Command: config web_authentication auth_page login default

#
```

3.40.13 config web_authentication virtual_ip

目的	このコマンドは WEB 認証用の仮想 IP アドレスを設定します。
構文	config web_authentication virtual_ip <ipaddr>
説明	WEB 認証の仮想 IP アドレスは、認証されていないホストからの認証要求を受け付ける時に使用されます。この IP に送信された TCP パケット要求のみ正しく応答が返されます。 この IP アドレスは ARP パケット又は ICMP パケットに応答しません。この仮想 IP アドレスには同一サブネット内に存在するホスト PC や IP インターフェースに設定されたアドレスにしないようにしてください。
パラメーター	virtual_ip - 仮想 IP の IP アドレスを指定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。 仮想 IP に "0.0.0.0" を設定した場合、WEB 認証機能を有効にできません。
対応バージョン	1.03.00 以降

使用例: WEB 認証用仮想 IP アドレスを設定するには

```
#config web_authentication virtual_ip 1.1.1.1
Command: config web_authentication virtual_ip 1.1.1.1

Success.

#
```

3.40.14 clear web_authentication auth_state

目的	このコマンドは WEB 認証エントリーをクリアします。
構文	clear web_authentication auth_state <ports> Ports = ports <<portlist> all> [authenticated authenticating blocked] macaddr <macaddr>
説明	ポートがポートベースモードに設定された場合、そのポートは認証されない状態に戻ります。そのポートに関係する全てのタイマーはリセットされます。 ポートがホストベースモードに設定された場合、そのポート上のユーザーは全てクリアされます。 ユーザーはネットワークにアクセスするために再認証される必要があります。
パラメーター	ports - この設定に使用されるポートリストを指定します。 <portlist>この設定に使用されるポートリストをここに入力します。 all - この設定に使用される全てのポートを指定します。 authenticated - ある 1 ポートの全ての認証されたユーザーをクリアします。 authenticating - ある 1 ポートの全ての認証中のユーザーをクリアします。 blocked - ある 1 ポートの全てのブロックされたユーザーをクリアします。 macaddr - この設定に使用される MAC アドレスを指定します。 <macaddr>この設定に使用される MAC アドレスをここに入力します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: ポート 1-5 の WEB 認証エントリーをクリアするには

<pre>#clear web_authentication auth_state ports 1-5 Command: clear web_authentication auth_state ports 1-5 Success. #</pre>

3.40.15 delete web_authentication

目的	このコマンドは WEB 認証ローカルユーザーをクリアします。
構文	delete web_authentication <user <username 15> all_users>
説明	このコマンドは WEB 認証ローカルユーザーをクリアします。
パラメーター	user - 削除されるユーザー名を指定します。 <username 15> - 半角英数字 15 文字以内でユーザー名を指定します。 all user - ローカル DB にある全てのユーザーアカウントを削除します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: WEB 認証ローカルユーザーをクリアするには

```
#delete web_authentication user user1
Command: delete web_authentication user user1

Success.

#
```

3.40.16 show web_authentication

目的	このコマンドは WEB 認証のグローバル設定を表示します。
構文	show web_authentication
説明	このコマンドは WEB 認証のグローバル設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.03.00 以降

使用例: WEB 認証のグローバル設定を表示するには

```
#show web_authentication
Command: show web_authentication

Web-Base Access Control
-----
State                : Disabled
Method               : RADIUS
Authentication Failover : Enabled
Redirect Path        : http://www.website.com
Virtual IP           : 1.1.1.1
Switch HTTP Port     : 8888 (HTTP)
RADIUS Authorization : Enabled
Local Authorization  : Enabled

#
```

3.40.17 show web_authentication auth_state ports

目的	このコマンドはポートの認証状態を表示します。
構文	show web_authentication auth_state ports [<portlist>]
説明	このコマンドはポートの認証状態を表示します。
パラメーター	Ports - 表示されるポート範囲を指定します。
制限事項	なし。
対応バージョン	1.03.00 以降

使用例: ポートの認証状態を表示するには

```
# show web_authentication auth_state ports
Command: show web_authentication auth_state ports

H:Host-based P:Port-based

Port      MAC Address          Original State      VID Aging Time/
          RX VID              Block Time
-----
1         00-00-00-00-00-01(H) 20    Authenticated  4004 Infinite
1         00-00-00-00-00-03(H) 100    Blocked        -    60
2         00-00-00-00-00-02(H) 20    Authenticated  1234 Infinite
2         00-00-00-00-00-04(H) 110    Authenticating -    10

Total Authenticating Hosts :1
Total Authenticated Hosts  :2
Total Blocked Hosts       :1

#
```

3.40.18 show web_authentication ports

目的	このコマンドはWEB認証ポート設定を表示します。
構文	show web_authentication ports [<portlist>]
説明	このコマンドはWEB認証ポート設定を表示します。
パラメーター	Ports- 表示されるポート範囲を指定します
制限事項	なし。
対応バージョン	1.03.00以降

使用例: ポート 1-3 の WEB 認証ポート設定を表示するには

```
#show web_authentication ports 1-3
Command: show web_authentication ports 1-3
```

Port	State	Aging Time (Minutes)	Block Time (Seconds)	Auth Mode
-----	-----	-----	-----	-----
1	Enabled	60	120	Host-Based
2	Enabled	60	120	Host-Based
3	Enabled	120	120	Host-Based

```
#
```

3.40.19 show web_authentication user

目的	このコマンドはユーザーがWEB認証アカウントを表示します。
構文	show web_authentication user
説明	ユーザーがWEB認証アカウントを表示することを可能にするコマンドです パスワードは管理レベルの下に表示されます。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.03.00以降

使用例: WEB 認証アカウントを表示するには

```
#show web_authentication user
Command: show web_authentication user
```

Username	Password	VID
-----	-----	-----
webuser	webuser	-

```
Total Entries:1
#
```


3.40.20 show web_authentication auth_page

目的	WEB 認証で使用する認証画面に管理者がカスタマイズ登録した任意の文字列情報内容を表示します。
構文	show web_authentication auth_page
説明	本コマンドは、WEB 認証 login または logout 画面にカスタマイズ登録された文字列情報内容を表示します。日本語を表示させるには使用するターミナルソフトウェアにてエンコード方式を Shift-JIS に設定してください。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.07.00 以降

使用例: WEB 認証カスタマイズ文字列内容を表示するには

<pre>#show web_authentication auth_page Command: show web_authentication auth_page Login Page Customized Text Box: ----- 1.ご利用方法がわからない方は下記へご連絡ください。 2. 3. [問い合わせ先] 4. 5.情報システム統括部 ネットワーク運用担当 6.担当者名: 金属太郎 7.TEL : 123-4567 8.MAIL : taro.kinzoku.ab@hitachi-metals.com ----- Logout Page Customized Text Box: ----- 1.ご利用方法がわからない方は下記へご連絡ください。 2. 3. [問い合わせ先] 4. 5.情報システム統括部 ネットワーク運用担当 6.担当者名: 金属太郎 7.TEL : 123-4567 8.MAIL : taro.kinzoku.ab@hitachi-metals.com ----- #</pre>
--

3.41 POE コマンド

POE とは、TP ケーブルの特定の組み合わせのペアに直流電圧を重畳させ、通信をしながら受電機器に電源を供給する 802.3af の規格の機能です。この機能は APLFM108GT-POE および APLFM116GT-POE のみに提供されます。

3.41.1 config poe ports

目的	各ポートの PoE 設定を変更します。
構文	<pre>config poe ports <all <portlist>> state State =state <enable disable> priority <critical high low> power_limit <class_based user_define <value 1000-15400>></pre>
説明	<p>IEEE802.3af に規定された 4 つの PD Class (class 0, class 1, class 2, class 3) が使用できます。</p> <p>消費電力範囲はそれぞれ 0.44 ~ 12.95W, 0.44 ~ 3.84W, 3.84 ~ 6.49W, 6.49 ~ 12.95W です。</p> <p>4 つのクラスに対する供給電力制限値が既定してあります。各クラスの供給電力制限値は消費電力範囲よりも少し大きな値となっています。これは接続ケーブルにおける電力損失を考慮しているためです。下記の値が典型的な値として決められています。</p> <p style="padding-left: 40px;">Class 0: 15,400mW Class 1: 4,000mW Class 2: 7,000mW Class 3: 15,400mW</p> <p>これらの 4 つの既定値の他に、数値でも供給電力制限値を指定できます。IEEE802.3af 規格では、通常では最小値は 1,000mW、最大値は 15,400mW です。</p>
パラメーター	<p>ports - 対象となるポートを指定します。</p> <p>all - すべてのポートを設定する場合は、「all」のパラメーターを使用します。</p> <p><portlist> -設定するポート範囲を指定します</p> <p>state - 「disable」に設定すると、このポートから給電はされません。</p> <p>enable - state を「enable」に設定します。1.05 からデフォルト設定は enable に変更されました。</p> <p>disable - state を「disable」に設定します。</p> <p>priority - 給電ポートの優先順位を指定します。critical が最も高くなります。</p> <p>critical - 優先順位を critical に設定します。</p> <p>high - 優先順位を high に設定します。</p> <p>low - 優先順位を low に設定します。</p> <p>power_limit -各ポートの給電電力制限値を指定します。</p> <p>class_based - 接続される PD のクラスを自動検出して、そのクラスに応じた給電電力制限をします。</p> <p>user_define - 各ポートの給電電力制限を数値で指定します。</p> <p><value 1000-15400> - 給電電力制限値を 1000 ~ 15400 で指定します。</p>
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: ポート 1 から 4,5 の PoE 設定を変更するには

```
#config poe ports 1-4 state enable priority critical power_limit class_based
Command: config poe ports 1-4 state enable priority critical power_limit class_b
ased





Success.

#config poe ports 5 state enable priority critical power_limit user_define 1000
Command: config poe ports 5 state enable priority critical power_limit user_define 1000

Success.

#
```

注意事項

-  最大給電量を超えると、プライオリティレベルの高いポートから電力を供給します。プライオリティレベルが同じ場合には、若番ポートから優先的に電力を供給します。(新たに接続した受電機器によって最大給電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されるわけではありません)
-  power_limit でポートの供給制限を変更した場合、対象ポートの給電を一時的に停止した後に給電を再開します。
-  user_define で入力するポートの最大供給値は、100mW 単位での動作となります。(100mW 未満を入力しても切捨てた値で動作します)
-  config ports コマンドで、ポート設定を(disable)にしても電力供給は行われます。

3.41.2 show poe ports

目的	各ポートの PoE 設定と実際の値を表示します。
構文	show poe ports (portlist)
説明	各ポートの PoE 設定と実際の値を表示します。
パラメーター	<portlist> - 表示するポート範囲を指定します。 省略されたときは全ポートが対象となります。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: ポート 1 から 5 の PoE 設定を表示するには

```
#show poe ports 1-5
Command: show poe ports 1-5

Port   State   Priority   Power Limit(mW)
      Class   Power(mW)   Voltage(decivolt)   Current(mA)
      Status
=====
1      Enabled Critical   --- (Class-based)
      0       0         0                   0
      OFF : Interim state during line detection
2      Enabled Critical   --- (Class-based)
      0       0         0                   0
      OFF : Interim state during line detection
3      Enabled Critical   --- (Class-based)
      0       0         0                   0
      OFF : Interim state during line detection
4      Enabled Critical   --- (Class-based)
      0       0         0                   0
      OFF : Interim state during line detection
5      Enabled Critical   1000 (User-defined)
      0       0         0                   0
      OFF : Interim state during line detection

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

3.41.3 config poe system

目的	スイッチの PoE 設定を変更します。
構文	config poe system power_limit <value 20-125>
説明	本コマンドはスイッチの PoE 設定を変更します。
パラメーター	power_limit - スイッチ全体の供給電力制限値 <value 20-125> - 制限値を W 単位で入力します。範囲は 20 から 125。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.03.00 以降

使用例: 供給電力制限値を 37W に設定するには

```
# config poe system power_limit 37
Command: config poe system power_limit 37

Success.

#
```

注意事項

- ❗ ポートに電力供給を始めて給電電力制限を超過する場合には、PoE のコントローラは過負荷を回避するために他のポートの切断を試みます。このプロセスは deny_low_priority_port と呼ばれ、新しく供給を開始するポートよりもプライオリティが低く、かつ最も低いプライオリティのポートから優先的に切断するポートを選びます。過負荷状態が解消されるまで、この順番でポートの給電が切断されつづけます。
- ❗ 供給電力残量が 17W 以下の状態で新たにポート追加をする場合、パワーガードバンド機能により、LowPriorityDeny プロセスに従ったポート追加処理となります。

3.41.4 show poe system

目的	スイッチの PoE 設定を表示します。
構文	show poe system
説明	本コマンドはスイッチの PoE 設定を表示します。
パラメーター	無し
制限事項	無し
対応バージョン	1.03.00 以降

使用例: スイッチの PoE 設定を表示するには

```
#show poe system
Command: show poe system

PoE System Information
-----
Power Limit                : 37(Watts)
System Total Power Consumption : 0(Watts)
System Power Remained       : 42(Watts)
Power Disconnection Method   : Deny Low Priority Port

If System Power Remained is less than 17W (Power Guard Band), then there might
be no additional port supplied with power.
#
```

3.42 COMMAND LOGGING コマンド

COMMAND LOGGING コマンドは、コマンドラインインターフェース上で実行したコマンドの成功および失敗をログに出力するコマンドです。デフォルトでは「enable」有効となっています。

3.42.1 enable command logging

目的	コマンドログ機能を有効にします。
構文	enable command logging
説明	本コマンドは、コマンドログ機能を有効に設定します。 ただし、装置が起動中または設定を読み込んでいる間は動作しません。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.07.00 以降

使用例: コマンドログ機能を有効に設定するには

<pre>#enable command logging Command: enable command logging Success. #</pre>

3.42.2 disable command logging

目的	コマンドログ機能を無効にします。
構文	disable command logging
説明	本コマンドは、コマンドログ機能を無効に設定します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.07.00 以降

使用例: コマンドログ機能を無効に設定するには

<pre>#disable command logging Command: disable command logging Success. #</pre>

3.42.3 show command logging

目的	コマンドログ機能設定を表示します。
構文	show command logging
説明	本コマンドは、現在のコマンドログ機能設定を表示します。
パラメーター	なし。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.07.00 以降

使用例: 現在のコマンドログ機能設定を表示するには

```
#show command logging
Command: show command logging

Command Logging State : Enabled

#
```

3.43 Link Error Recovery コマンド

Link Error Recovery コマンドは、ポート接続状態監視の健全性が確認できない場合、装置内ログを保存して装置再起動により接続復旧を試みるためのコマンドです。デフォルトでは「disable」無効となっています。

3.43.1 config auto_recovery_mode

目的	スイッチのポート接続状態の健全性が2ポート以上確認できない場合、自動再起動により復旧を試みます。
構文	config auto_recovery_mode < enable disable >
説明	本コマンドは、ポート接続状態の健全性が2ポート以上確認できない場合、自動再起動により復旧を試みます。自動再起動した場合の起動ログには"System restart"ログが出力されます。
パラメーター	enable - 自動再起動を「enable」(有効)に設定します。 disable - 自動再起動を「disable」(無効)に設定します。
制限事項	管理者アカウントのみ本コマンドを実行できます。
対応バージョン	1.08.00 以降

使用例: オートリカバリー機能を有効にするには

```
# config auto_recovery_mode enable
Command: config auto_recovery_mode enable

Success.

#
```

3.43.2 show auto_recovery_mode

目的	オートリカバリーモード設定を表示します。
構文	show auto_recovery_mode
説明	本コマンドは、現在のオートリカバリーモード設定を表示します。
パラメーター	なし。
制限事項	なし。
対応バージョン	1.08.00 以降

使用例: 現在のオートリカバリー設定を表示するには

```
# show auto_recovery_mode
Command: show auto_recovery_mode
Auto Recovery Mode : Enabled

Success.

#
```


4. 使用上の注意事項

- (1) コンソールポートには、パラメータ設定時のみに 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。
- (2) ポートミラーリング機能は、source ポートとして設定したポートで送受信されたフレーム等を解析するための機能です。従って、Target ポートとして設定したポートには、アナライザ等ネットワークを解析する装置以外は接続しないでください。
- (3) ポート VLAN を設定する場合、ホスト(スイッチングハブ)が属していないグループのポートからホスト宛に通信を行うことはできません。またホストは複数のグループに属することはできません。

5. トラブルシューティング

5.1 表示 LED に関連する現象と対策

現象	対策
「PWR」 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。
ツイストケーブルを接続しても「LINK/ACT」 LED が点灯しない	ツイスト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。
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。	
「CONSOLE」 LED が点滅している。	当該装置またはその接続先ネットワークにてループが生じていないか確認してください。

5.2 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 9600bps、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。

5.3 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、デフォルトルート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、ツイスト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。

5.4 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ツイスト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。
パケットロスが発生する。	特定のポートから出力されるフレームの負荷が 100% を超えていないかどうか確認してください。(特定のポートに 100% を超える負荷が集中した場合、別ポートにも影響を及ぼし、パケットロスが発生する場合があります。)

5.5 VLAN に関連する現象と対策

現象	対策
VID を指定するとエラーメッセージが表示される。	指定した VID が、既に他の 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。VID の設定を修正してください。

5.6 SFP に関連する現象と対策

現象	対策
SFP を認識している状態で通信しない	SFP を認識している状態で通信しない場合は、SFP が不完全装着になっている可能性があります。SFP を再度装着し直してください。現象が再発する場合は SFP 又は装置の異常が考えられます。

5.7 PoE に関連する現象と対策

現象	対策
端末へ給電されない	給電の Status が Enable になっているかを確認してください。
	ツイストペアケーブルに異常がない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。
	端末の給電クラスと合致しているかを確認してください。
	スイッチの給電制限を超えていないかを確認してください。

5.8 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	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、お買い求めの販売店もしくは販売元にお問い合わせください。

6. 準拠規格

No.	項目	準拠規格
1	LAN インターフェース	IEEE802.3 : 10BASE-T IEEE802.3u : 100BASE-TX IEEE802.3u : Auto-Negotiation IEEE802.3z : 1000BASE-X IEEE802.3ab : 1000BASE-T
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	RFC1157 : Simple Network Management Protocol (SNMP) RFC1901 : Introduction to Community-based SNMPv2 RFC1905 : Protocol Operations for Version 2 of the Simple Network Management Protocol RFC1908 : Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework RFC2570 : Introduction to Version 3 of the Internet-standard Network Management Framework RFC2575 : View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
4	ネットワーク管理対象	RFC1213 : Internet 標準 MIB RFC1493 : Bridge MIB RFC2819 : RMON MIB 4 グループ RFC2021 : RMON2 MIB のうち Probe config の一部 RFC2233 : ifMIB
5	通信プロトコル	RFC793 : TCP(Transmission Control Protocol) RFC768 : UDP(User Datagram Protocol) RFC1350 : THE TFTP PROTOCOL (REVISION 2) RFC783 : TFTP Client RFC791 : IP(Internet Protocol) RFC792 : ICMP(Internet Control Message Protocol) RFC826 : ARP(Address Resolution Protocol) RFC854 : TELNET RFC1769 : SNTP(Simple Network Time Protocol) RFC3164 : SYSLOG RFC951/RFC1541 : BootP/DHCP Client
6	IGMP snooping	RFC1112 : IGMPv1 (snooping only) RFC2236 : IGMPv2 (snooping only) RFC3376 : IGMPv3 (awareness only)

No.	項 目	準 拠 規 格
7	セキュリティープロトコル	RFC2865 : RADIUS (client only) RFC1492 : TACACS+ Authentication For the Management Access RFC2138/RFC2139 : RADIUS Auth. For Management Access RFC2866 : RADIUS Accounting RFC4250 : The Secure Shell(SSH) Protocol Assigned Numbers RFC4251 : The Secure Shell(SSH) Protocol Architecture RFC4252 : The Secure Shell(SSH) Authentication Protocol RFC4253 : The Secure Shell(SSH) Transport Layer Protocol RFC4254 : The Secure Shell(SSH) Connection Protocol RFC4255 : Using DNS to Securely Publish Secure Shell(SSH) Key Fingerprints RFC4256 : Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)
8	その他	VCCI Class A 準拠 IEEE802.3ad : リンクアグリゲーション IEEE802.1Q : tag group VLAN, QoS(IEEE802.1Q priority mapping/queuing) IEEE802.1D : STP/RSTP IEEE802.1Q : MSTP IEEE802.3x : フロー制御 IEEE802.1AB : LLDP IEEE802.3af : PoE

ApresiaLightFM シリーズ Ver.1.08 CLI マニュアル

Copyright(c) 2014 Hitachi Metals, Ltd.

2014 年 1 月 初版

2016 年 11 月 第三版

日立金属株式会社

東京都港区港南一丁目 2 番 70 号

(品川シーズンテラス)