

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326
Management Guide

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide

本マニュアルについて

- 本マニュアルでは、FXC3326 の各種設定およびシステムの監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末接続して、CLI（コマンドラインインタフェース）または Web ブラウザで行います。
- 本マニュアルに記載している機能は、ファームウェアバージョン 1.1.0.3 以降の製品に対応しています。



製品取り扱い時のご注意

この度は、お買い上げいただきましてありがとうございます。製品を安全にお使いいただくため、必ず最初にお読みください。

・下記事項は、安全のために必ずお守りください。



- 安全のための注意事項を守る
注意事項をよくお読みください。製品全般の注意事項が記載されています。
- 故障したら使わない
すぐに販売店まで修理をご依頼ください。
- 万一異常が起きたら
 - ・煙が出たら
 - ・異常な音、においがしたら
 - ・内部に水・異物が入ったら
 - ・製品を高所から落としたり、破損したとき

- ①電源を切る（電源コードを抜く）
 - ②接続ケーブルを抜く
 - ③販売店に修理を依頼する
-

- ・下記の注意事項を守らないと、火災・感電などにより死亡や大けがの原因となります。



- 電源ケーブルや接続ケーブルを傷つけない
 - ・電源ケーブルを傷つけると火災や感電の原因となります。
 - ・重いものをのせたり、引っ張ったりしない。
 - ・加工したり、傷つけたりしない。
 - ・熱器具の近くに配線したり、加熱したりしない。
 - ・電源ケーブルを抜くときは、必ずプラグを持って抜く。
 - 内部に水や異物を入れない
 - ・火災や感電の原因となります。
 - ・万一、水や異物が入ったときは、すぐに電源を切り（電源ケーブルを抜き）、販売店に点検・修理をご依頼ください。
 - 内部をむやみに開けない

本体及び付属の機器（ケーブル含む）をむやみに開けたり改造したりすると、火災や感電の原因となります。
 - 落雷が発生したらさわらない

感電の原因となります。また、落雷の恐れがあるときは、電源ケーブルや接続ケーブルを事前に抜いてください。本機が破壊される原因となります。
 - 油煙、湯気、湿気、ほこりの多い場所には設置しない

本書に記載されている使用条件以外の環境でのご使用は、火災や感電の原因となります。
-

製品取り扱い時のご注意

- ・下記の注意事項を守らないとけがをしたり周辺の物品に損害を与える原因となります。



- ぬれた手で電源プラグやコネクタに触らない
感電の原因となります。
 - 指定された電源コードや接続ケーブルを使う
マニュアルに記載されている電源ケーブルや接続ケーブルを使わないと、火災や感電の原因となります。
 - 指定の電圧で使う
マニュアルに記されている電圧の範囲で使わないと、火災や感電の原因となります。
 - コンセントや配線器具の定格を超えるような接続はしない
発熱による火災の原因となります。
 - 通風孔をふさがない
 - ・通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。また、風通しをよくするために次の事項をお守りください。
 - ・毛足の長いジュウタンなどの上に直接設置しない。
 - ・布などでくるまない。
 - 移動させるときは、電源ケーブルや接続ケーブルを抜く
接続したまま移動させると、電源ケーブルが傷つき、火災や感電の原因となります。
-

目次

1. イントロダクション	1
1.1 主な機能.....	1
1.2 ソフトウェア機能.....	2
2. 本機の管理.....	6
2.1 本機への接続.....	6
2.1.1 設定方法	6
2.1.2 接続手順	7
2.1.3 リモート接続	8
2.2 基本設定.....	9
2.2.1 コンソール接続	9
2.2.2 パスワードの設定	9
2.2.3 IP アドレスの設定	10
手動設定	10
動的設定	13
2.2.4 SNMP 管理アクセスを有効にする	16
コミュニティ名 (Community Strings)	16
トラップ・レシーバ (Trap Receivers)	17
2.3 システムファイルの管理.....	18
2.3.1 設定情報の保存または復元	18
3. Web インタフェース	20
3.1 Web インタフェースへの接続	20
3.2 Web インタフェースの操作方法.....	21
3.2.1 ホームページ	21
3.2.2 設定オプション	22
3.2.3 パネルの表示	22
3.3 基本設定.....	23
3.3.1 システム情報の表示	23
3.3.2 ハードウェア及びソフトウェアバージョンの表示	24
3.3.3 Jumbo フレームの有効化	25
3.3.4 ブリッジ拡張機能の表示	26
3.3.5 ファームウェアの管理.....	28
FTP/TFTP、HTTP 経由のファイルコピー	28
現在の設定をローカルファイルへ保存	30
起動ファイルの設定	31

システムファイルの表示	32
オペレーションコードの自動アップグレード	33
3.3.6 システムクロックの設定	36
手動設定	36
SNTP 設定	37
SNTP タイムサーバの設定	38
タイムゾーンの設定	39
3.3.7 コンソールポートの設定	40
3.3.8 Telnet の設定	42
3.3.9 CPU 使用率の表示	43
3.3.10 メモリ使用率の表示	44
3.3.11 再起動	45
3.4 インタフェース設定	48
3.4.1 ポート設定	48
ポートリストによる設定	48
ポート範囲による設定	50
接続状況の表示	51
ポートミラーリングの設定	52
リモートポートミラーリングの設定	54
ポート・トランク統計情報表示	58
ケーブル診断の実行	61
3.4.2 トランクグループの設定	63
静的トランクの設定	64
動的トランク設定	66
LACP ポートカウンタの表示	70
ローカル側の LACP 設定及びステータスの表示	71
リモート側の LACP 設定及びステータスの表示	73
3.4.3 パワーセービング	74
3.4.4 トラフィックセグメンテーション	76
トラフィックセグメンテーションの有効化	76
アップリンク / ダウンリンクポートの設定	77
3.4.5 VLAN トランキング	78
3.5 VLAN	80
3.5.1 IEEE802.1Q VLAN	80
VLAN グループの設定	83
VLAN への静的メンバーの追加	85
動的 VLAN 登録の設定	89
3.5.2 802.1Q トンネリングの設定	92
QinQ トンネリングの有効	96
インタフェースを QinQ トンネリングへ追加	97
3.5.3 プロトコル VLAN	98
プロトコル VLAN グループ設定	98
プロトコルグループをインタフェースへマッピング	100
3.5.4 IP サブネット VLAN	102

目次

3.5.5	MAC ベース VLAN.....	104
3.5.6	VLAN ミラーリング.....	106
3.6	アドレステーブル.....	108
3.6.1	静的アドレスの設定.....	108
3.6.2	エージングタイムの変更.....	110
3.6.3	動的アドレステーブルの表示.....	111
3.6.4	動的アドレステーブルの消去.....	111
3.6.5	MAC アドレスミラーリングの設定.....	113
3.7	スパニングツリーアルゴリズム.....	115
3.7.1	ループバック検出.....	116
3.7.2	グローバル設定.....	118
3.7.3	グローバル設定の表示.....	122
3.7.4	インタフェース設定.....	123
3.7.5	インタフェース設定の表示.....	126
3.7.6	MSTP 設定.....	128
3.7.7	MSTP インタフェースの設定.....	131
3.8	帯域制御.....	133
3.8.1	ストームコントロール.....	134
3.9	Class of Service (CoS).....	136
3.9.1	レイヤ 2 キュー設定.....	136
	インタフェースへのデフォルトプライオリティの設定.....	136
	キューモードの選択.....	137
	Egress キューへの CoS 値のマッピング.....	139
3.9.2	レイヤ 3/4 プライオリティの設定.....	141
	CoS 値へのレイヤ 3/4 プライオリティのマッピング.....	141
	優先処理を DSCP または CoS へ設定.....	141
	イングレス DSCP 値を内部 DSCP 値へマッピング.....	143
	CoS プライオリティを内部 DSCP 値へマッピング.....	145
3.10	Quality of Service.....	147
3.10.1	Quality of Service の設定.....	147
	クラスマップの設定.....	148
	QoS ポリシーの作成.....	151
	ポリシーマップをポートへ適用.....	158
3.11	VoIP 設定.....	159
	VoIP トラフィックの設定.....	159
	テレフォニー OUI の設定.....	161
	VoIP トラフィックポートの設定.....	163
3.12	セキュリティ.....	165
3.12.1	AAA 許可とアカウントिंग.....	165
	ローカル / リモートログオン認証設定.....	167

	リモートログオン認証サーバの設定	168
	AAA アカウンティングの設定	172
	AAA 認可設定	177
3.12.2	ユーザアカウントの設定	180
3.12.3	Web 認証	182
	Web 認証のグローバル設定	182
	Web 認証の設定（ポート）	184
3.12.4	ネットワークアクセス（MAC アドレス認証）	185
	ネットワークアクセスのグローバル設定	187
	ポートのネットワークアクセス設定	188
	ポートリンク検出	190
	MAC アドレスフィルタ	191
	セキュア MAC アドレス情報の表示	193
3.12.5	HTTPS 設定	194
	サイト証明書の置き換え	195
3.12.6	Secure Shell 設定	197
	SSH サーバ設定	199
	ホストキーペアの生成	200
	ユーザパブリックキーのインポート	202
3.12.7	ACL（Access Control Lists）	204
	タイムレンジの設定	205
	TCAM 使用率の表示	207
	ACL 名およびタイプの設定	208
	スタンダード IPv4 ACL の設定	209
	拡張 IPv4 ACL の設定	211
	MAC ACL の設定	214
	ARP ACL の設定	216
	ACL へのポートのバインド	218
3.12.8	ARP インスペクション	219
	ARP インスペクションのグローバル設定	220
	ARP インスペクション VLAN 設定	222
	ARP インスペクションインタフェース設定	224
	ARP インスペクション統計値の表示	225
	ARP インスペクションログの表示	226
3.12.9	管理アドレスのフィルタリング	227
3.12.10	ポートセキュリティの設定	229
3.12.11	802.1x ポート認証	231
	802.1x グローバル設定	232
	802.1x 認証ポート設定	233
	802.1x ポートサブリカント設定	236
	IEEE802.1x 統計情報の表示	238
3.12.12	IP ソースガード	240
	IP ソースガードポート設定	240
	IP ソースガード静的バインディング設定	242
	動的 IP ソースガードバインディング情報の表示	244

目次

3.12.13	DHCP スヌーピング	245
	DHCP スヌーピング設定	246
	DHCP スヌーピング VLAN 設定	248
	DHCP スヌーピングポート設定	249
	DHCP スヌーピングバインディング情報	250
3.13	基本管理プロトコル	251
3.13.1	Event Logging の設定	251
	syslog の設定	251
	リモートログの設定	253
	SMTP (Simple Mail Transfer Protocol)	254
3.13.2	LLDP	256
3.13.3	LLDP タイム属性の設定	256
3.13.4	LLDP インタフェースの設定	258
3.13.5	LLDP ローカルデバイス情報の表示	260
3.13.6	LLDP リモートポート情報の表示	263
3.13.7	デバイス統計値の表示	268
3.13.8	SNMP	270
3.13.9	SNMP グローバル設定	272
	ローカルエンジン ID の設定	273
	リモートエンジン ID の設定	274
	SNMPv3 ビューの設定	276
	SNMPv3 グループの設定	279
3.13.10	コミュニティ名の設定	282
	SNMPv3 ローカルユーザーの設定	283
	SNMPv3 リモートユーザーの設定	285
	トラップマネージャの指定	287
3.13.11	リモートモニタリング	292
	RMON アラームの設定	292
	RMON イベントの設定	295
	RMON 履歴サンプルの設定	297
	RMON 統計サンプルの設定	300
3.13.12	スイッチクラスタリング	303
	クラスタ設定	303
	クラスタメンバー設定	305
	クラスタメンバーの管理	307
3.14	IP 設定	308
3.14.1	PING	308
3.14.2	ARP	309
	ARP タイムアウトの設定	310
	ARP エントリの表示	310
3.14.3	IP アドレスの設定 (IP Version4)	311
3.14.4	IP アドレスの設定 (IP Version6)	313
	IPv6 デフォルトゲートウェイの設定	313
	IPv6 インタフェース設定	314

IPv6 アドレスの設定	317
IPv6 アドレスの表示	320
IPv6 近隣キャッシュの表示	321
IPv6 統計の表示	322
応答側ディスティネーションの MTU を表示	327
3.15 IP サービス	328
3.15.1 DNS (Domain Name Service)	329
DNS サービスの一般設定	329
ドメインネームリストの設定	330
ネームサーバリストの設定	331
静的 DNS ホストのアドレスエントリ	332
DNS キャッシュの表示	333
3.16 マルチキャストフィルタリング	334
3.16.1 レイヤ 2 IGMP (Snooping and Query)	334
IGMP Snooping とクエリパラメータの設定	335
マルチキャストルータの静的インタフェースを設定	338
マルチキャストサービスインタフェースをアサイン	340
インタフェース毎の IGMP Snooping 設定	342
IGMP Snooping で発見されたマルチキャストグループを表示	346
3.16.2 IGMP フィルタリング / スロットリング	347
IGMP フィルタリング / スロットリングの有効	347
IGMP フィルタプロファイルの設定	348
IGMP フィルタリング / スロットリングの設定 (ポート)	351
3.17 MVR (Multicast VLAN Registration)	353
グローバル MVR 設定	354
MVR インタフェースの設定	355
静的マルチキャストグループをインタフェースへ追加	357
4. コマンドラインインタフェース	358
4.1 コマンドラインインタフェースの利用	358
4.1.1 コマンドラインインタフェースへのアクセス	358
4.1.2 コンソール接続	358
4.1.3 Telnet 接続	359
4.2 コマンド入力	360
4.2.1 キーワードと引数	360
4.2.2 コマンドの省略	360
4.2.3 コマンド上でのヘルプの表示	361
コマンドの表示	361
4.2.4 キーワードの検索	362
4.2.5 コマンドのキャンセル	362
4.2.6 コマンド入力履歴の利用	362
4.2.7 コマンドモード	363

目次

4.2.8	Exec コマンド	363
4.2.9	Configuration コマンド	364
4.2.10	コマンドラインプロセス	365
4.3	コマンドグループ.....	366
4.4	General (一般コマンド).....	368
	prompt	368
	reload (Global Configuration)	369
	enable	370
	quit	371
	show history.....	372
	configure.....	373
	disable	373
	reload (Privileged Exec)	374
	show reload	374
	end.....	375
	exit	375
4.5	システム管理.....	376
4.5.1	Device Designation コマンド	377
	hostname	377
4.5.2	システム情報の表示	378
	show access-list tcam-utilization	378
	show memory	379
	show process cpu	379
	show running-config	380
	show startup-config	382
	show system	383
	show users	384
	show version.....	385
4.5.3	フレームサイズコマンド	386
	jumbo frame.....	386
4.5.4	ファイル管理 (Flash/File)	387
	boot system	388
	copy	389
	delete	392
	dir	393
	whichboot	394
	upgrade opcode auto.....	395
	upgrade opcode path.....	397
4.5.5	Line (ラインコマンド)	398
	Line	399
	databits.....	400
	exec-timeout	401
	login	402
	parity	403

	password	404
	password-thresh	405
	silent-time	406
	speed	407
	stopbits	408
	timeout login response	409
	disconnect	410
	show line	411
4.5.6	Event Logging コマンド	412
	logging facility	412
	logging history	413
	logging host	414
	logging on	415
	logging trap	416
	clear log	417
	show log	418
	show logging	419
4.5.7	SMTP アラートコマンド	421
	logging sendmail	421
	logging sendmail host	422
	logging sendmail level	423
	logging sendmail destination-email	424
	logging sendmail source-email	425
	show logging sendmail	425
4.5.8	Time コマンド	426
	sntp client	427
	sntp poll	428
	sntp server	429
	show sntp	430
	clock timezone	431
	calendar set	432
	show calendar	433
4.5.9	タイムレンジ	434
	time-range	434
	absolute	435
	periodic	436
	show time-range	437
4.5.10	スイッチクラスター	438
	cluster	439
	cluster commander	440
	cluster ip-pool	441
	cluster member	442
	rcommand	443
	show cluster	443
	show cluster members	444
	show cluster candidates	444

4.6	SNMP	445
	snmp-server.....	446
	snmp-server community	447
	snmp-server contact	448
	snmp-server location	448
	show snmp	449
	snmp-server enable traps.....	450
	snmp-server host.....	451
	snmp-server engine-id.....	453
	snmp-server group	454
	snmp-server user.....	455
	snmp-server view	456
	show snmp engine-id.....	457
	show snmp group	458
	show snmp user	460
	show snmp view	461
	nlm.....	462
	snmp-server notify-filter	463
	show nlm oper-status	464
	show snmp notify-filter	464
4.7	リモートモニタリング	465
	rmon alarm	466
	rmon event.....	467
	rmon collection history.....	468
	show rmon alarm	469
	show rmon event	469
	show rmon history	470
	show rmon statistics	470
4.8	認証コマンド	471
4.8.1	ユーザーアカウント	471
	enable password	472
	username.....	473
4.8.2	認証シーケンス	474
	authentication enable	474
	Authentication login	475
4.8.3	Radius クライアントコマンド	476
	radius-server acct-port.....	476
	radius-server auth-port	477
	radius-server host.....	478
	radius-server key	479
	radius-server retransmit.....	479
	radius-server timeout.....	480
	show radius-server	480
4.8.4	TACACS+ クライアントコマンド	481

	tacacs-server	481
	tacacs-server host	482
	tacacs-server key	482
	tacacs-server port	483
	show tacacs-server	483
4.8.5	AAA（認証・許可・アカウントिंग）コマンド	484
	aaa accounting dot1x	485
	aaa accounting exec	486
	aaa accounting update	487
	aaa authorization exec	487
	aaa group server	488
	server	488
	accounting dot1x	489
	accounting exec	490
	authorization exec	491
	show accounting	492
4.8.6	Web サーバーコマンド	493
	ip http port	493
	ip http server	494
	ip http secure-server	495
	ip http secure-port	495
4.8.7	Telnet サーバーコマンド	497
	ip telnet max-sessions	497
	ip telnet port	498
	ip telnet server	498
	show ip telnet	499
4.8.8	Secure Shell コマンド	500
	ip ssh authentication-retries	503
	ip ssh server	504
	ip ssh server-key size	505
	ip ssh timeout	506
	delete public-key	507
	ip ssh crypto host-key generate	508
	ip ssh crypto zeroize	509
	ip ssh save host-key	509
	show ip ssh	510
	show public-key	511
	show ssh	512
4.8.9	802.1x ポート認証コマンド	513
	dot1x default	514
	dot1x eapol-pass-through	514
	dot1x system-auth-control	515
	dot1x intrusion-action	515
	dot1x max-req	516
	dot1x operation-mode	517
	dot1x port-control	518

dot1x re-authentication	519
dot1x timeout quiet-period	519
dot1x timeout re-authperiod.....	520
dot1x timeout supp-timeout	521
dot1x timeout tx-period	522
dot1x re-authenticate.....	522
dot1x identity profile.....	523
dot1x max-start.....	524
dot1x pae supplicant.....	525
dot1x timeout auth-period.....	526
dot1x timeout held-period	527
dot1x timeout start-period.....	527
show dot1x	528
4.8.10 管理 IP フィルターコマンド	531
management.....	531
show management	532
4.9 セキュリティ	533
4.9.1 ポートセキュリティコマンド	533
port security	534
4.9.2 ネットワークアクセス (MAC アドレス認証)	535
network-access aging	536
network-access mac-filter.....	537
mac-authentication reauth-time	538
network-access dynamic-qos	539
network-access dynamic-vlan	540
network-access guest-vlan	541
network-access link-detection	542
network-access link-detection link-down	542
network-access link-detection link-up	543
network-access link-detection link-up-down	544
network-access max-mac-count.....	545
network-access mode mac-authentication	546
network-access port-mac-filter	547
mac-authentication intrusion-action	547
mac-authentication max-mac-count	548
show network-access	549
show network-access mac-address-table	550
show network-access mac-filter	551
4.9.3 Web 認証	552
web-auth login-attempts	553
web-auth quiet-period	554
web-auth session-timeout.....	554
web-auth system-auth-control	555
web-auth.....	555
web-auth re-authenticate (Port)	556

	web-auth re-authenticate (IP)	556
	show web-auth	557
	show web-auth interface.....	558
	show web-auth summary.....	559
4.9.4	DHCP スヌーピング	560
	ip dhcp snooping	561
	ip dhcp snooping database flash	562
	ip dhcp snooping information option	563
	ip dhcp snooping information policy	564
	ip dhcp snooping verify mac-address	565
	ip dhcp snooping vlan.....	566
	ip dhcp snooping trust	567
	clear ip dhcp snooping database flash	568
	show ip dhcp snooping	568
	show ip dhcp snooping binding	569
4.9.5	IP ソースガード	570
	ip source-guard binding	570
	ip source-guard.....	572
	show ip source-guard	573
	show ip source-guard binding.....	574
4.9.6	ARP インスペクション	575
	ip arp inspection	576
	ip arp inspection filter.....	577
	ip arp inspection log-buffer logs.....	578
	ip arp inspection validate	579
	ip arp inspection vlan.....	580
	ip arp inspection limit.....	581
	ip arp inspection trust	582
	show ip arp inspection configuration	582
	show ip arp inspection interface	583
	show ip arp inspection log	583
	show ip arp inspection statistics	584
	show ip arp inspection vlan	584
4.10	ACL (Access Control Lists)	585
4.10.1	IPv4 ACL	585
	access-list ip	586
	permit,deny (Standard IP ACL)	587
	permit,deny (Extended IPv4 ACL)	588
	ip access-group	590
	show ip access-group.....	591
	show ip access-list.....	591
4.10.2	MAC ACL.....	592
	access-list mac	592
	permit,deny (MAC ACL)	593
	mac access-group	595

目次

	show mac access-group	595
	show mac access-list	596
4.10.3	ARP ACL	597
	access-list arp	597
	permit,deny (ARP ACL)	598
	show arp access-list	599
4.10.4	ACL 情報の表示	600
	show access-group	600
	show access-list	600
4.11	インタフェース	601
	interface	602
	alias	603
	capabilities	604
	description	605
	flow control	606
	media-type	607
	negotiation	608
	shutdown	609
	speed-duplex	610
	switchport packet-rate	611
	clear counters	612
	show interfaces brief	613
	show interfaces counters	614
	show interfaces status	616
	show interfaces switchport	617
	test cable-diagnostics	619
	show cable-diagnostics	620
	power-save	621
	show power-save	622
4.12	リンクアグリゲーション	623
	channel-group	624
	lacp	625
	lacp admin-key (Ethernet Interface)	627
	lacp port-priority	628
	lacp system-priority	629
	lacp admin-key (Port Channel)	630
	show lacp	631
4.13	ポートミラーリング	634
4.13.1	ローカルポートミラーリング	634
	port monitor	635
	show port monitor	636
4.13.2	RSPAN ミラーリング	637
	rspan source	639
	rspan destination	640
	rspan remote vlan	641

no rspan session	642
show rspan	643
4.14 帯域制御.....	644
rate-limit.....	644
4.15 自動トラフィック制御	645
auto-traffic-control apply-timer	648
auto-traffic-control release-timer.....	649
auto-traffic-control.....	650
auto-traffic-control action	651
auto-traffic-control alarm-clear-threshold.....	652
auto-traffic-control alarm-fire-threshold	653
auto-traffic-control control-release	654
auto-traffic-control auto-control-release.....	654
snmp-server enable port-traps atc broadcast-alarm-clear.....	655
snmp-server enable port-traps atc broadcast-alarm-fire	656
snmp-server enable port-traps atc broadcast-control-apply	657
snmp-server enable port-traps atc broadcast-control-release	658
snmp-server enable port-traps atc multicast-alarm-clear	659
snmp-server enable port-traps atc multicast-alarm-fire	660
snmp-server enable port-traps atc multicast-control-apply.....	661
snmp-server enable port-traps atc multicast-control-release	662
show auto-traffic-control	663
show auto-traffic-control interface	663
4.16 アドレステーブル.....	664
mac-address-table aging-time	664
mac-address-table static	665
clear mac-address-table dynamic.....	666
show mac-address-table	667
show mac-address-table aging-time.....	668
4.17 スパニングツリー.....	669
spanning-tree.....	671
spanning-tree forward-time.....	672
spanning-tree hello-time	673
spanning-tree max-age.....	674
spanning-tree mode.....	675
spanning-tree pathcost method	676
spanning-tree priority.....	677
spanning-tree mst configuration	677
spanning-tree transmission-limit.....	678
max-hops	679
mst priority	680
mst vlan	681
name.....	682

revision	683
spanning-tree bpdu-filter.....	684
spanning-tree bpdu-guard	685
spanning-tree cost.....	686
spanning-tree edge-port	687
spanning-tree link-type	688
spanning-tree loopback-detection	689
spanning-tree loopback-detection release-mode	690
spanning-tree loopback-detection trap	691
spanning-tree mst cost	692
spanning-tree mst port-priority.....	694
spanning-tree port-priority	695
spanning-tree root-guard	696
spanning-tree spanning-disabled	697
spanning-tree loopback-detection release.....	698
spanning-tree protocol-migration.....	699
show spanning-tree	700
show spanning-tree mst configuration.....	702
4.18 VLAN.....	703
4.18.1 GVRP の設定.....	703
bridge-ext gvrp.....	704
garp timer	705
switchport forbidden vlan.....	706
switchport gvrp	707
show bridge-ext	707
show garp timer	708
show gvrp configuration.....	709
4.18.2 VLAN グループの設定	710
vlan database	710
vlan	711
4.18.3 VLAN インタフェースの設定	712
interface vlan	713
switchport acceptable-frame-types.....	714
switchport allowed vlan.....	715
switchport ingress-filtering	716
switchport mode	717
switchport native vlan	718
vlan-trunking	719
4.18.4 VLAN 情報の表示	721
show vlan.....	721
4.18.5 IEEE802.1Q トンネリングの設定	722
dot1q-tunnel system-tunnel-control	723
switchport dot1q-tunnel mode	724
switchport dot1q-tunnel tpid.....	725
show dot1q-tunnel	726
4.18.6 ポートベーストラフィックセグメンテーション	727

traffic-segmentation	728
show traffic-segmentation.....	729
4.18.7 プロトコル VLAN の設定.....	730
protocol-vlan protocol-group (Configuring Groups)	731
protocol-vlan protocol-group (Configuring Interface)	732
show protocol-vlan protocol-group	733
show interfaces protocol-vlan protocol-group	733
4.18.8 IP サブネット VLAN	734
subnet-vlan	735
show subnet-vlan.....	736
4.18.9 MAC ベース VLAN.....	737
mac-vlan	738
show mac-vlan.....	739
4.18.10 Voice VLAN	740
voice vlan.....	741
voice vlan aging.....	741
voice vlan mac-address.....	742
switchport voice vlan	743
switchport voice vlan priority.....	743
switchport voice vlan rule	744
switchport voice vlan security	745
show voice vlan	746
4.19 Class Of Service	747
4.19.1 プライオリティコマンド (Layer 2).....	747
queue mode.....	748
queue weight	749
switchport priority default.....	750
show queue mode	751
show queue weight.....	751
4.19.2 プライオリティコマンド (Layer 3 and 4).....	752
qos map cos-dscp	753
qos map dscp-mutation	755
qos map phb-queue.....	756
qos map trust-mode.....	757
show qos map dscp-mutation	758
show qos map phb-queue	759
show qos map cos-dscp	760
show qos map trust-mode	761
4.20 Quality of Service	762
class-map	764
description	765
match.....	766
rename	767
policy-map	768

class	769
police flow	770
police srtcm-color	771
police trtcm-color	773
set cos	775
set ip dscp	776
set php	777
service-policy	778
show class-map	779
show policy-map	780
show policy-map interface	781
4.21 マルチキャストフィルタリング	782
4.21.1 IGMP Snooping コマンド	782
ip igmp snooping	784
ip igmp snooping proxy-reporting	785
ip igmp snooping querier	786
ip igmp snooping router-alert-option-check	787
ip igmp snooping router-port- expire-time.....	788
ip igmp snooping tcn-flood.....	789
ip igmp snooping tcn-query-solicit	790
ip igmp snooping unregistered-data-flood	791
ip igmp snooping unsolicited-report-interval	792
ip igmp snooping version.....	793
ip igmp snooping version-exclusive	794
ip igmp snooping vlan general-query-suppression	795
ip igmp snooping vlan immediate-leave	796
ip igmp snooping vlan last-memb-query-count.....	797
ip igmp snooping vlan last-memb-query-intvl	798
ip igmp snooping vlan mrd.....	799
ip igmp snooping vlan proxy-address	800
ip igmp snooping vlan proxy-query-interval	801
ip igmp snooping vlan proxy-query-resp-intvl	802
ip igmp snooping vlan static	803
show ip igmp snooping	804
show ip igmp snooping group.....	805
4.21.2 静的マルチキャストルーティングコマンド	806
ip igmp snooping vlan mrouter	806
show ip igmp snooping mrouter.....	807
4.21.3 IGMP Filtering/Throttling コマンド	808
ip igmp filter (Global Configuration)	809
ip igmp profile	810
permit, deny.....	811
range	812
ip igmp filter (Interface Configuration)	813
ip igmp max-groups	814
ip igmp max-groups action	815

show ip igmp filter	816
show ip igmp profile	817
show ip igmp throttle interface	818
4.21.4 MVR の設定	819
mvr	820
mvr immediate-leave	821
mvr type	822
mvr vlan group	823
show mvr	824
4.22 LLDP コマンド	826
lldp	827
lldp holdtime-multiplier	828
lldp notification-interval	829
lldp refresh-interval	829
lldp reinit-delay	830
lldp tx-delay	830
lldp admin-status	831
lldp basic-tlv management-ip-address	831
lldp basic-tlv port-description	832
lldp basic-tlv system-capabilities	832
lldp basic-tlv system-description	833
lldp basic-tlv system-name	834
lldp dot1-tlv proto-ident	834
lldp dot1-tlv proto-vid	835
lldp dot1-tlv pvid	835
lldp dot1-tlv vlan-name	836
lldp dot3-tlv link-aggr	836
lldp dot3-tlv mac-phy	837
lldp dot3-tlv max-frame	837
lldp notification	838
show lldp config	839
show lldp info local-device	840
show lldp info remote-device	841
show lldp info statistics	842
4.23 DNS (Domain Name Server)	843
ip domain-list	844
ip domain-lookup	845
ip domain-name	846
ip host	847
ip name-server	848
ipv6 host	849
clear dns cache	849
clear host	850
show dns	850
show dns cache	851

目次

show hosts.....	852
4.24 DHCP	853
4.24.1 DHCP クライアント	853
ip dhcp client class-id	854
ip dhcp restart client	855
ipv6 dhcp restart client vlan	856
show ipv6 dhcp duid	857
show ipv6 dhcp vlan	857
4.25 IP インタフェース.....	858
4.25.1 IPv4 インタフェース設定	858
ip address	859
ip default-gateway	860
show ip default-gateway	860
show ip interface.....	861
traceroute	862
ping.....	863
4.25.2 ARP 設定	864
arp timeout.....	864
clear arp-cache.....	865
show arp.....	865
4.25.3 IPv6 インタフェース設定	866
ipv6 default-gateway.....	867
ipv6 address	868
ipv6 address autoconfig.....	870
ipv6 address eui-64	871
ipv6 address link-local	873
ipv6 enable	874
ipv6 mtu	875
show ipv6 default-gateway	876
show ipv6 interface.....	877
show ipv6 mtu.....	879
show ipv6 traffic.....	880
clear ipv6 traffic	885
ping6.....	886
ipv6 nd dad attempts	887
ipv6 nd ns-interval	889
ipv6 nd reachable-time	890
clear ipv6 neighbors	890
show ipv6 neighbors.....	891

1. イントロダクション

1.1 主な機能

本機はレイヤ 2 スイッチとして豊富な機能を搭載しています。

本機は管理エージェントを搭載し、各種設定を行うことができます。
ネットワーク環境に応じた適切な設定を行うことや、各種機能を有効に設定することで、機能を最大限に活用できます。

機能	解説
Configuration Backup and Restore	管理ステーションまたは FTP/TFTP サーバを使用
Authentication	Console, Telnet, web ユーザ名 / パスワード, RADIUS, TACACS+ Web - HTTPS Telnet - SSH SNMPv1/2c - コミュニティ名 SNMPv3 - MD5、SHA パスワード Port - IEEE802.1x 認証、MAC アドレスフィルタリング
General Security Measures	プライベート VLAN、ポート認証、ポートセキュリティ、 DHCP スヌーピング、IP ソースガード
Access Control Lists	最大 512 ルール、64ACL をサポート (1 つの ACL に最大 32 ルール)
DHCP	クライアント
DNS	クライアントおよび Proxy サービス
Port Configuration	スピード、通信方式、フローコントロール
Port Trunking	Static 及び LACP による最大 8 トランク
Port Mirroring	1 つの分析ポートに対する、1 つまたは複数ポートのミラーリング (5 セッション)
Rate Limiting	ポートごとの入力・出力帯域制御 ブロードキャスト、マルチキャスト、未知のユニキャストストーム の調節
Address Table	最大登録可能 MAC アドレス数：8k、1K 静的 MAC アドレス、255 L2 マルチキャストグループ
IP Version 4 and 6	IPv4 および IPv6 アドレスおよび管理をサポート
IEEE802.1D Bridge	動的スイッチング及び MAC アドレス学習
Store-and-Forward Switching	ワイヤスピードスイッチング
Spanning Tree Algorithm	STP、Rapid STP (RSTP)、Multiple STP (MSTP)
Virtual LANs	IEEE802.1Q タグ付 VLAN/ ポートベース VLAN/ プロトコル VLAN/ プライベート VLAN、voiceVLAN、QinQ トンネルをサポート (最大 255 グループ)
Traffic Prioritization	ポートプライオリティ、トラフィッククラスマッピング、キュースケ ジューリング、IP Precedence、DSCP をサポート
Quality of Service	DiffServ サポート
Link Layer Discovery Protocol	隣接するデバイスの基本情報を発見するために使用
Multicast Filtering	IGMP Snooping、Query、MVR

1.2 ソフトウェア機能

本機はレイヤ 2 イーサネットスイッチとして多くの機能を有し、それにより効果的なネットワークの運用を実現します。

ここでは、本機の主要機能を紹介します。

設定のバックアップ及び復元

TFTP サーバを利用して現在の設定情報を保存することができます。

また、保存した設定情報を本機に復元することも可能です。

認証 /Authentication

本機はコンソール、Telnet、Web ブラウザ経由の管理アクセスに対する本機内又はリモート認証サーバ (RADIUS/TACACS+) によるユーザ名とパスワードベースでの認証を行います。また、Web ブラウザ経由では HTTPS を、Telnet 経由では SSH を利用した認証オプションも提供しています。

SNMP、Telnet、Web ブラウザでの管理アクセスに対しては IP アドレスフィルタリング機能も有しています。

各ポートに対しては IEEE802.1x 準拠のポートベース認証をサポートしています。本機能では、EAPOL(Extensible Authentication Protocol over LANs) を利用し、IEEE802.1x クライアントに対してユーザ名とパスワードを要求します。その後、認証サーバにおいてクライアントのネットワークへのアクセス権を確認します。

その他に、HTTPS によるセキュアなマネジメントアクセスや、Telnet アクセスを安全に行う SSH もサポートしています。また、各ポートへのアクセスには MAC アドレスフィルタリング機能も搭載しています。

ACL/Access Control Lists

ACL は IP アドレス、プロトコル、TCP/UDP ポート番号による IP フレームのフィルタリングもしくは、MAC アドレス、イーサネットタイプによるフレームのフィルタリングを提供します。ACL を使用することで、不要なネットワークトラフィックを抑制し、パフォーマンスを向上させることができます。

また、ネットワークリソースやプロトコルによるアクセスの制限を行うことでセキュリティのコントロールが行えます。

ポート設定 /Port Configuration

本機ではオートネゴシエーション機能により対向機器に応じて各ポートの設定を自動的に行える他、手動で各ポートの通信速度、通信方式及びフローコントロールの設定を行うことができます。

通信方式を Full-Duplex にすることによりスイッチ間の通信速度を 2 倍にすることができます。IEEE802.3x に準拠したフローコントロール機能では通信のコントロールを行い、パケットバッファを越えるパケットの損失を防ぎます。

ポートミラーリング /Port Mirroring

本機は任意のポートからモニターポートに対して通信のミラーリングを行うことができます。ターゲットポートにネットワーク解析装置（Sniffer 等）又は RMON プロブを接続し、トラフィックを解析することができます。

ポートトランク /Port Trunking

複数のポートをバンド幅の拡大によるボトルネックの解消や、障害時の冗長化を行うことができます。本機で手動及び IEEE802.3ad 準拠の LACP を使用した動的設定で行うことができます。

帯域制御 /Rate Limiting

各インタフェースにおいて、受信トラフィックの最大帯域の設定を行うことができます。設定範囲内のパケットは転送されますが、設定した値を超えたパケットは転送されずにパケットが落とされます。

ストームコントロール /Storm Control

ストームコントロール機能は、ブロードキャスト、マルチキャスト、未知のユニキャスト通信によりネットワークの帯域が占有されることを防ぎます。ポート上で本機能を有効にした場合、ポートを通過するブロードキャスト、マルチキャスト、未知のユニキャストパケットを制限することができます。パケットが設定しているしきい値を超えた場合、しきい値以下となるよう制限を行います。

静的アドレス /Static Addresses

特定のポートに対して静的な MAC アドレスの設定を行うことができます。設定された MAC アドレスはポートに対して固定され、他のポートに移動することはできません。設定された MAC アドレスの機器が他のポートに接続された場合、MAC アドレスは無視され、アドレステーブル上に学習されません。

静的 MAC アドレスの設定を行うことにより、指定のポートに接続される機器を制限し、ネットワークのセキュリティを提供します。

IEEE802.1D ブリッジ /IEEE 802.1D Bridge

本機では IEEE802.1D ブリッジ機能をサポートします。

MAC アドレステーブル上で MAC アドレスの学習を行い、その情報に基づきパケットの転送を行います。本機では最大 8K 個の MAC アドレスの登録を行うことが可能です。

ストア & フォワード スイッチング /Store-and Forward Switching

本機ではスイッチング方式としてストア&フォワードをサポートします。

本機では 4Mbit のバッファを有し、フレームをバッファにコピーをした後、他のポートに対して転送します。これによりフレームがイーサネット規格に準拠しているかを確認し、規格外のフレームによる帯域の占有を回避します。また、バッファにより通信が集中した場合のパケットのキューイングも行います。

スパニングツリーアルゴリズム / Spanning Tree Algorithm

本機は 3 種類のスパニングツリープロトコルをサポートしています。

Spanning Tree Protocol (STP, IEEE 802.1D) —

本機能では、LAN 上の通信に対して複数の通信経路を確保することにより冗長化を行うことができます。

複数の通信経路を設定した場合、1 つの通信経路のみを有効とし、他の通信経路はネットワークのループを防ぐため無効にします。但し、使用している通信経路が何らかの理由によりダウンした場合には、他の無効とされている通信経路を有効にして通信を継続して行うことを可能とします。

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) —

既存の IEEE802.1D 準拠の STP に比べ約 10 分の 1 の時間でネットワークの再構築を行うことができます。

RSTP は STP の完全な後継とされていますが、既存の STP のみをサポートしている製品と接続され STP に準拠したメッセージを受信した場合には、STP 互換モードとして動作することができます。

Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) —

本機能は RSTP の拡張機能です。本機能により各 VLAN 単位での STP 機能を提供することが可能となります。VLAN 単位にすることにより、各 VLAN 単位でネットワークの冗長化を行えるほか、ネットワーク構成が単純化され RSTP よりさらに早いネットワークの再構築を行うことが可能となります。

VLAN/Virtual LANs

本機は最大 255 グループの VLAN をサポートしています。VLAN は物理的な接続に関わらず同一のコリジョンドメインを共有するネットワークノードとなります。

本機では IEEE802.1Q 準拠のタグ付 VLAN をサポートしています。VLAN グループメンバーは GVRP を利用した動的な設定及び手動での VLAN 設定を行うことができます。VLAN の設定を行うことにより指定した通信の制限を行うことができます。

VLAN によりセグメントを分ける事で以下のようなメリットがあります。

- 細かいネットワークセグメントにすることによりブロードキャストストームによるパフォーマンスの悪化を回避します。
- 物理的なネットワーク構成に関わりなく、VLAN の設定を変更することでネットワークの構成を簡単に変更することが可能です。
- 通信を VLAN 内に制限することでセキュリティが向上します。
- プライベート VLAN を利用することにより設定可能な VLAN 数に制限がある中で、同一 VLAN 内の各ポート間の通信を制限し、アップリンクポートとの通信のみを行うことが可能となります。
- プロトコルベース VLAN により、プロトコルタイプに基づいたトラフィックの制限を行うことが可能です。

IEEE 802.1Q トンネリング /IEEE 802.1Q TUNNELING (QINQ)

IEEE802.1Q トンネリング (QinQ) は、ネットワークで複数のカスタマーのトラフィックを送送するサービスプロバイダを対象に設計された機能です。
QinQ トンネリングは、フレームがサービスプロバイダのネットワークに入る時にサービスプロバイダ VLAN (SPVLAN) タグをカスタマーのフレームに挿入し、フレームがネットワークを去る時タグを取り去ることで実現します。

プライオリティ /Traffic Prioritization

本機ではキューと Strict 又は WRR キューイング機能によりサービスレベルに応じた各パケットに優先順位を設定することができます。これらは、入力されるデータの IEEE802.1p 及び 802.1Q タグにより優先順位付けが行われます。

本機能により、アプリケーション毎に要求される優先度を個別に設定することができます。

また、本機では IP フレーム上の ToS オクテット内のプライオリティビットを利用した優先順位の設定など、いくつかの方法により L3/L4 レベルでの優先順位の設定も行うことができます。

マルチキャストフィルタリング /Multicast Filtering

正常なネットワークの通信に影響させず、リアルタイムでの通信を確保するために、VLAN のプライオリティレベルを設定し、マルチキャスト通信を特定し各 VLAN に対して割り当てることができます。

本機では IGMP Snooping 及び Query を利用し、マルチキャストグループの登録を管理します。

2. 本機の管理

2.1 本機への接続

2.1.1 設定方法

FXC3326 は、ネットワーク管理エージェントを搭載し SNMP、RMON、及び Web インタフェースによるネットワーク経由での管理を行うことができます。また、PC から本機に直接接続しコマンドラインインタフェース (Command Line Interface/CLI) を利用した設定及び監視を行うことも可能です。

[注意] 初期設定状態では、DHCP サーバによる IP アドレスの取得を行うよう設定されています。この設定の変更を行うには 2.2.3 項「IP アドレスの設定」を参照して下さい。

本機には管理用の Web サーバが搭載されています。Web ブラウザから設定を行ったり、ネットワークの状態を監視するための統計情報を確認したりすることができます。ネットワークに接続された PC 上で動作する、Internet Explorer 5.0 以上から、Web インタフェースにアクセスすることができます。

本機の CLI へは本体のコンソールポートへの接続及びネットワーク経由での Telnet による接続によりアクセスすることができます。

本機には SNMP (Simple Network Management Protocol) に対応した管理エージェントが搭載されています。ネットワークに接続されたシステムで動作する、SNMP に対応した管理ソフトから、本機の SNMP エージェントにアクセスし設定などを行うことが可能です。

本機の CLI、Web インタフェース及び SNMP エージェントからは以下の設定を行うことが可能です。

- ・ ユーザ名、パスワードの設定
- ・ 管理 VLAN の IP インタフェースの設定
- ・ SNMP パラメータの設定
- ・ 各ポートの有効 / 無効
- ・ 各ポートの通信速度及び Full/Half Duplex の設定
- ・ 帯域制御による各ポートの入力及び出力帯域の設定
- ・ IEEE802.1X セキュリティ、静的アドレスフィルタリングのコントロール
- ・ ACL を使用したパケットのフィルタ
- ・ 最大 255 (VLAN4093 は予約済みとなり削除はできません) の IEEE802.1Q VLAN 設定
- ・ GVRP 有効
- ・ IGMP マルチキャストフィルタリング設定

- HTTP、FTP/TFTP 経由のファームウェアまたは設定ファイルのアップロード及びダウンロード
- スパニングツリーの設定
- Class of Service (CoS) の設定
- 静的トランク及び LACP 設定 (最大 12)
- ポートミラーリングの有効
- 各ポートのブロードキャストストームコントロールの設定
- システム情報及び統計情報の表示

2.1.2 接続手順

本機のシリアルポートと PC を RS-232C ケーブルを用いて接続し、本機の設定及び監視を行うことができます。

PC 側では VT100 準拠のターミナルソフトウェアを利用して下さい。PC を接続するための RS-232C ケーブルは、本機に同梱されているケーブルを使用して下さい。

手順：

- (1) RS-232C ケーブルの一方を PC のシリアルポートに接続し、コネクタ部分のねじを外れないように止めます。
- (2) RS-232C ケーブルのもう一方を本機のコンソールポートに接続します。
- (3) パソコンのターミナルソフトウェアの設定を以下の通り行ってください。

通信ポート ----- RS-232C ケーブルが接続されているポート
(COM ポート 1 又は COM ポート 2)

通信速度 ----- 9600bps

データビット ----- 8bit

ストップビット ---- 1bit

パリティ ----- なし

フロー制御 ----- なし

エミュレーション -- VT100

- (4) 上記の手順が正しく完了すると、コンソールログイン画面が表示されます。

コンソール接続に関する設定の詳細は P398 「Line (ラインコマンド)」を参照して下さい。
CLI の使い方は P358 「コマンドラインインタフェース」を参照して下さい。
また、CLI の全コマンドと各コマンドの使い方は P366 「コマンドグループ」を参照して下さい。

2.1.3 リモート接続

ネットワークを経由して本機にアクセスする場合は、事前にコンソール接続又は DHCP により本機の IP アドレス、サブネットマスク、デフォルトゲートウェイを設定する必要があります。

初期設定では本機は DHCP を用いて自動的に IP アドレスを取得します。手動で IP アドレスの設定を行う場合の設定方法は P10 「IP アドレスの設定」を参照して下さい。

[注意] 本機は同時に最大 4 セッションまでの Telnet または SSH 接続が行えます。

IP アドレスの設定が完了すると、ネットワーク上のどの PC からでも本機にアクセスすることができます。PC 上からは Telnet、Web ブラウザ、ネットワーク管理ソフトを使うことにより本機にアクセスすることができます (対応 Web ブラウザは Internet Explorer 5.0、又は Netscape Navigator 6.2 以上です)。

本機に搭載された管理エージェントでは SNMP 管理機能の設定項目に制限があります。すべての SNMP 管理機能を利用する場合は SNMP に対応したネットワーク管理ソフトウェアを使用して下さい。

2.2 基本設定

2.2.1 コンソール接続

CLI ではゲストモード (normal access level/Normal Exec) と管理者モード (privileged access level/Privileged Exec) の 2 つの異なるコマンドレベルがあります。ゲストモード (Normal Exec) を利用した場合、利用できる機能は本機の設定情報などの表示と一部の設定のみに制限されます。本機のすべての設定を行うためには管理者モード (Privileged Exec) を利用し CLI にアクセスする必要があります。

2 つの異なるコマンドレベルは、ユーザ名とパスワードによって区別されています。初期設定ではそれぞれに異なるユーザ名とパスワードが設定されています。

管理者モード (Privileged Exec) の初期設定のユーザ名とパスワードを利用した接続方法は以下の通りです。

- (1) コンソール接続を初期化し、<Enter> キーを押します。ユーザ認証が開始されます。
- (2) ユーザ名入力画面で "admin" と入力します。
- (3) パスワード入力画面で "admin" と入力します。
(入力したパスワードは画面に表示されません)
- (4) 管理者モード (Privileged Exec) でのアクセスが許可され、画面上に "Console#" と表示が行われます。

2.2.2 パスワードの設定

[注意] 安全のため、最初に CLI にログインした際に "username" コマンドを用いて両方のアクセスレベルのパスワードを変更するようにしてください。

パスワードは最大 32 文字の英数字です。大文字と小文字は区別されます。

パスワードの設定方法は以下の通りです。

- (1) コンソールにアクセスし、初期設定のユーザ名とパスワード "admin" を入力して管理者モード (Privileged Exec) でログインします。
- (2) "configure" と入力し <Enter> キーを押します。
- (3) "username guest password 0 password" と入力し、<Enter> キーを押します。Password 部分には新しいパスワードを入力します。
- (4) "username admin password 0 password" と入力し、<Enter> キーを押します。Password 部分には新しいパスワードを入力します。

```
Username: admin
Password:

      CLI session with the FXC3326 is opened.
      To end the CLI session, enter [Exit].

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

2.2.3 IP アドレスの設定

本機の管理機能にネットワーク経由でアクセスするためには、IP アドレスを設定する必要があります。

IP アドレスの設定は下記のどちらかの方法で行うことができます。

手動設定

IP アドレスとサブネットマスクを手動で入力し、設定を行います。本機に接続する PC が同じサブネット上にない場合には、デフォルトゲートウェイの設定も行う必要があります。

動的設定

ネットワーク上の BOOTP 又は DHCP サーバに対し、IP アドレスのリクエストを行い自動的に IP アドレスを取得します。

手動設定

IP アドレスを手動で設定します。セグメントの異なる PC から本機にアクセスするためにはデフォルトゲートウェイの設定も必要となります。

[注意] 工場出荷時の状態で、本機は DHCP を用いて自動的に IP アドレスを取得します。本機の管理機能にネットワーク経由でアクセスするためには、IP アドレスを設定する必要があります。

IPv4 アドレス

IP アドレスの設定を行う前に、必要な下記の情報をネットワーク管理者から取得して下さい

- (本機に設定する) IP アドレス
- ネットワークのデフォルトゲートウェイ
- ネットワークのマスク

IPv4 アドレスを設定するための手順は以下の通りです。

- (1) interface モードにアクセスするために、Global Configuration モードで "interface vlan 1" と入力し、<Enter> キーを押します。
- (2) "ip address *ip-address netmask*" と入力し、<Enter> キーを押します。
"*ip-address*" には本機の IP アドレスを、"*netmask*" にはネットワークのサブネットマスクを入力します。
- (3) Global Configuration モードに戻るために、"exit" と入力し、<Enter> キーを押します。
- (4) 本機の所属するネットワークのデフォルトゲートウェイの IP アドレスを設定するために、"ip default-gateway *gateway*" と入力し、<Enter> キーを押します。
"*gateway*" にはデフォルトゲートウェイの IP アドレスを入力します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```


IPv6 アドレス

ここでは、"リンクローカル"アドレスの設定方法および、複数セグメントのネットワークで使用されるネットワークプレフィックスと、アドレスのホスト部を含む、"グローバルユニキャスト"アドレスの設定方法を解説します。

IPv6 プレフィックスまたはアドレスは、RFC2373"IPv6 Addressing Architecture"に従ってフォーマットされなくてはなりません。8つの16ビット16進数をコロンで区切った値を使用します。アドレス内の不適格なフィールドを満たす為に必要とされるゼロの適切な数を示すために1つのダブルコロンが使用されます。

IPv6 アドレスを割り当てるその他の方法についての詳細は P313 「IP アドレスの設定 (IP Version6)」を参照してください。

リンクローカルアドレス

全てのリンクローカルアドレスはFE80のプレフィックスで設定される必要があります。このアドレスタイプが同じローカルサブネットに接続されている全ての装置にのみIPv6上のスイッチアクセスを可能にします。

スイッチが、設定されたアドレスと、サブネット上の他の装置で使用されている物に矛盾を検出した場合、それは問題アドレスの使用を停止し、自動でローカルサブネット上の他の装置と矛盾の無いリンクローカルアドレスを生成します。

スイッチのIPv6リンクローカルアドレスの設定

- (1) Global Configuration モードプロンプトで、" interface vlan 1" と入力し < Enter > を押します。interface-configuration モードへ入ります。
- (2) " ipv6 address" とタイプし、例のように最大8つのコロンによって区切られた16ビット16進数値、それに続き "link-local" コマンドパラメータを入力し、< Enter > を押します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::260:3EFF:FE11:6700 link-
local
Console(config-if)#end
Console#show ipv6 interface
IPv6 is stale.
Link-local address:
    FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
(None)
Joined group address(es):
FF02::1:FF11:6700
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

マルチセグメントネットワークのアドレス

マルチセグメントネットワークへの接続に使用されるスイッチへ IPv6 アドレスを割り当てる前に、ネットワーク管理者より以下の情報を入手してください。

◆ このネットワークのプレフィックス

◆ スwitchの IP アドレス

◆ ネットワークのデフォルトゲートウェイ

いくつかの異なるサブネットをカバーするネットワークのために、スイッチのネットワークプレフィックスとホストアドレスを含む、フルアドレスを定義する必要があります。

フル IPv6 アドレスまたは IPv6 アドレスとプレフィックス長を指定することが可能です。IPv6 ネットワークのプレフィックス長はネットワークアドレスを形成する接頭辞のビット数であり、10 進数として表現されます。

例えば、73 の最初のバイト（16 進数）で始まる全ての IPv6 アドレスが 73:0:0:0:0:0:0/8 または 73::/8 として表現されます。スイッチのグローバルユニキャスト IPv6 アドレスを生成するには、以下のステップを完了してください。

- (1) global configuration モードプロンプトから、interface-configuration モードにアクセスするため、" interface vlan 1" を入力し < Enter > を押します。
- (2) interface プロンプトから、" ipv6 address ipv6-address" または " ipv6 address ipv6-address/prefix-length" を入力します。"prefix-length" はアドレスのネットワーク部の形成に使用されるアドレスビットを示します。（ネットワークアドレスはプレフィックスの左から始まり、IPv6 アドレスビットの若干をカバーします）残りのビットはホストインタフェースに割り当てられます。 < Enter > を押します。
- (3) "exit" を入力し、global configuration モードプロンプトに戻ります。 < Enter > をクリックします。
- (4) " ipv6 default-gateway gateway," をタイプし、スイッチが属するネットワークの IPv6 デフォルトゲートウェイの IPv6 アドレスを設定します。" gateway" はデフォルトゲートウェイの IPv6 アドレスです。 <Enter> をクリックします。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::/64
Console(config-if)#exit
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is stale.
Link-local address:
    FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
    2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
Joined group address(es):
    FF02::1:FF00:0
    FF02::1:FF11:6700
    FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.

Console#show ipv6 default-gateway
ipv6 default gateway: 2001:DB8:2222:7272::254
Console#
```

動的設定

IPv4 アドレス

"bootp" 又は "dhcp" を選択した場合、BOOTP 又は DHCP からの応答を受け取るまで IP アドレスは有効になりません。IP アドレスを取得するためには "ip dhcp restart client" コマンドを使用してブロードキャストサービスリクエストを行う必要があります。リクエストは IP アドレスを取得するために周期的に送信されます (BOOTP と DHCP から取得する値には IP アドレス、サブネットマスクおよびデフォルトゲートウェイが含まれます)

IP アドレスの取得方法として "bootp" 又は "dhcp" が起動ファイルに設定されている場合、本機は電源投入時に自動的にブロードキャストリクエストを送信します。

"BOOTP" 又は "DHCP" サーバを用いて動的に IP アドレスの取得を行う場合は、下記の手順で設定を行います。

- (1) interface configuration モードにアクセスするために、global configuration モードで "interface vlan 1" と入力し <Enter> キーを押します。
- (2) interface configuration モードで、下記のコマンドを入力します。
 - DHCP で IP アドレスを取得する場合 : "ip address dhcp" と入力し <Enter> キーを押します。
 - BOOTP で IP アドレスを取得する場合 : "ip address bootp" と入力し <Enter> キーを押します。
- (3) Privileged Exec モードに戻るために、"end" と入力し、<Enter> キーを押します。
- (4) 数分待った後、IP 設定を確認するために、"show ip interface" と入力し、<Enter> キーを押します。
- (5) 設定を保存するために、"copy running-config startup-config" と入力し、<Enter> キーを押します。起動ファイル名を入力し、<Enter> キーを押します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart
Console#show ip interface
IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

IPv6 アドレス

リンクローカルアドレス

IPv6 アドレスの設定にはいくつかの方法があります。

一番シンプルな方法はリンクローカルアドレスの自動的生成です。(FE80 のアドレスプレフィックスで識別)

このアドレスタイプは、同じローカルサブネットに接続された全ての装置のために、IPv6 上のアクセスを可能にします。

IPv6 リンクローカルアドレスを生成するには、以下のステップを行ってください。

- (1) Global Configuration モードプロンプトにて、"interface vlan 1" を入力し、interface-configuration モードへアクセスします。＜ Enter ＞を押します。
- (2) "ipv6 enable" と入力し、＜ Enter ＞を押します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
    FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
    2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
Joined group address(es):
FF02::1:FF00:0
FF02::1:FF11:6700
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

マルチセグメントネットワークのアドレス

1 つ以上のサブネットを含むネットワークで利用できる IPv6 アドレスを生成するために、スイッチは自動的に、ルータアドバタイズメントメッセージで受信された、ローカルサブネットアドレスプレフィックスを基に、一意のホストアドレスを生成するよう設定が可能です。スイッチの IPv6 ホストアドレスを動的に生成するには、以下のステップを行ってください。

- (1) Global Configuration モードプロンプトにて、"interface vlan 1" を入力し、interface-configuration モードへアクセスします。 < Enter > を押します。
- (2) interface プロンプトにて、"ipv6 address autoconfig" と入力し < Enter > を押します。

```
Console(config-if)#interface vlan 1
Console(config-if)#ipv6 address autoconfig
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
    FE80::212:CFFF:FE0B:4600/64
Global unicast address(es):
    2005::212:CFFF:FE0B:4600, subnet is 2005:0:0:0::/64
    3FFE:501:FFFF:100:212:CFFF:FE0B:4600, subnet is 3FFE:501:FFFF:100::/64
Joined group address(es):
    FF01::1/16
    FF02::1/16
    FF02::1:FF0B:4600/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

2.2.4 SNMP 管理アクセスを有効にする

本機は、SNMP(Simple Network Management Protocol) ソフトウェア経由での管理コマンドによる設定が行えます。

本機では (1)SNMP リクエストへの応答、及び (2)SNMP トラップの生成、が可能です。

SNMP ソフトウェアが本機に対し情報の取得や設定のリクエストを出した場合、本機はリクエストに応じて情報の提供や設定を行います。また、あらかじめ設定することによりリクエストがなくても決められた出来事が発生した場合にトラップ情報を SNMP ソフトウェアに送ることが可能です。

コミュニティ名 (Community Strings)

コミュニティ名 (Community Strings) は、本機からトラップ情報を受け取る SNMP ソフトウェアの認証と、SNMP ソフトウェアからのアクセスをコントロールするために使用されます。指定されたユーザもしくはユーザグループにコミュニティ名を設定し、アクセスレベルを決定することができます。

初期設定でのコミュニティ名は以下のとおりです。

- public — 読み取り専用のアクセスが可能です。public に設定された SNMP 管理ソフトウェアからは MIB オブジェクトの閲覧のみが行えます。
- private — 読み書き可能なアクセスができます。private に設定された SNMP 管理ソフトウェアからは MIB オブジェクトの閲覧及び変更を行うことが可能です。

SNMP 経由での不正なアクセスを防ぐため、コミュニティ名は初期設定から変更して下さい。コミュニティ名の変更は以下の手順で行います。

- (1) 管理者モード (Privileged Exec) の global configuration モードから "snmp-server community string mode" と入力し <Enter> キーを押します。
"string" にはコミュニティ名 "mode" には rw (read/wirte、読み書き可能)、ro (read only、読み取り専用) のいずれかを入力します (初期設定では read only となります)
- (2) (初期設定などの) 登録済みのコミュニティ名を削除するために、"no snmp-server community string" と入力し <Enter> キーを押します。
"string" には削除するコミュニティ名を入力します。

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

[注意] SNMP を利用しない場合には、初期設定のコミュニティ名を削除して下さい。
コミュニティ名が設定されていない場合には、SNMP 管理アクセス機能は無効となります。

トラップ・レシーバ (Trap Receivers)

本機からのトラップを受ける SNMP ステーション (トラップ・レシーバ) を設定することができます。

トラップを設定するには、管理者モード (Privileged Exec) の global configuration モードから以下のコマンドを入力後、Enter を押してください。

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

"host-address" にはトラップ・レシーバの IP アドレスを、"community-string" にはバージョン 1/2c ホストのアクセス権か、バージョン 3 のユーザ名を入力します。

"version" では、SNMP クライアントバージョンを指定します。

"auth | noauth | priv" は、v3 クライアントで使用される " 認証 / 認証無し / 認証とプライバシー " を意味します。

これらのパラメータの詳細については P451 「snmp-server host」を参照してください。

以下の例は、SNMP クライアントのそれぞれのタイプにトラップホストを作成しています。

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

2.3 システムファイルの管理

本機のフラッシュメモリ上に CLI、Web インタフェース、SNMP から管理可能な 3 種類のシステムファイルがあります。これらのファイルはファイルのアップロード、ダウンロード、コピー、削除、及び起動ファイルへの設定を行うことができます。

3 種類のファイルは以下の通りです。

- **Configuration(設定ファイル)** — このファイルはシステムの設定情報が保存されており、設定情報を保存した際に生成されます。保存されたシステム起動ファイルに設定することができる他、サーバに FTP/TFTP 経由でアップロードしバックアップを取ることができます。
"Factory_Default_Config.cfg" というファイルはシステムの初期設定が含まれており、削除することはできません。
詳細に関しては 28 ページの「ファームウェアの管理」を参照して下さい。
- **Operation Code(オペレーションコード)** — 起動後に実行されるシステムソフトウェアでランタイムコードとも呼ばれます。オペレーションコードは本機のオペレーションを行なう他、CLI、Web インタフェースを提供します。
詳細に関しては 28 ページの「ファームウェアの管理」を参照して下さい。
- **Diagnostic Code(診断コード)** — POST(パワー・オン・セルフテスト) として知られているソフトウェア (システム・ブートアップ時の実行プログラム)。

本機はオペレーションコードを 2 つまで保存することができます。診断コードと設定ファイルに関しては、フラッシュメモリの容量の範囲内で無制限に保存することができます。

フラッシュメモリでは、各種類のそれぞれ 1 つのファイルが起動ファイルとなります。

システム起動時には診断コードファイルとオペレーションコードファイルが実行されます。その後設定ファイルがロードされます。設定ファイルは、ファイル名を指定してダウンロードされます。

実行中の設定ファイルをダウンロードした場合、本機は再起動されます。実行中の設定ファイルを保存用ファイルに保存しておく必要があります。

2.3.1 設定情報の保存または復元

configuration command を使用しての設定変更は、実行中の設定ファイルが変更されるだけとなります。本機の再起動を行った場合には設定情報が保存されません。

変更した設定を保存するためには "copy" コマンドを使い、実行中の設定ファイルを起動設定ファイルにコピーする必要があります。

新しい起動設定ファイルには指定された名前を付けられなければなりません。
ファイル名は 1 ～ 31 文字で設定でき、大文字小文字を区別されます。 ("¥" または "/" は使用出来ず、最初の文字を "." には出来ません。)

スイッチ内には 1 つ以上のユーザ定義の設定ファイルを保存できますが、スイッチブート時に使用される "startup" として指定できるのは 1 ファイルのみです。

" copy running-config startupconfig" コマンドは常に新しいファイルを起動ファイルとして設定します。

以前に保存された設定ファイルを起動システムに使用するには "config:<filename>" コマンドを使用してください。

保存される設定ファイルの最大数は、利用可能なフラッシュメモリの容量に依存します。
利用可能なフラッシュメモリの合計量は "dir" コマンドを使用して確認出来ます。

現在の設定を保存するには以下の手順を行ってください。

- (1) Privileged Exec モードにて、"copy running-config startup-config" と入力し "Enter" を押します。
- (2) 起動ファイルの名前を入力し、"Enter" を押します。

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

\Write to FLASH finish.
Success.

Console#
```

バックアップサーバから設定を復元するには以下の手順を行って下さい。

- (1) Privileged Exec モードにて、"ccopy tftp startup-config" と入力し "Enter" を押します。
- (2) TFTP サーバのアドレスを入力し、"Enter" を押します。
- (3) サーバに保存されている起動ファイルの名前を入力し "Enter" を押します。
- (4) スイッチの起動ファイルの名前を入力し "Enter" を押します。

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

Success.
Console#
```

3. Web インタフェース

3.1 Web インタフェースへの接続

本機には管理用の Web サーバが搭載されています。Web ブラウザから設定を行ったり、ネットワークの状態を監視するための統計情報を確認したりすることができます。

ネットワークに接続された PC 上で動作する、Internet Explorer 5.0、又は Netscape Navigator 6.2 以上から、Web インタフェースにアクセスすることができます。

[注意] Web インタフェース以外に、ネットワーク経由での Telnet 及びシリアルポート経由のコンソール接続でコマンドラインインタフェース (CLI) を使用し本機の設定を行うことができます。

CLI の使用に関する詳細は 4 章コマンドラインインタフェースを参照して下さい。

Web インタフェースを使用する場合は、事前に下記の設定を行って下さい。

- (1) コンソール接続、BOOTP 又は DHCP プロトコルを使用して本機に IP アドレス、サブネットマスク、デフォルトゲートウェイを設定します (詳細は P311 ページの「IP アドレスの設定 (IP Version4)」を参照して下さい)
- (2) コンソール接続で、ユーザ名とパスワードを設定します。Web インタフェースへの接続はコンソール接続の場合と同じユーザ名とパスワード使用します。
- (3) Web ブラウザからユーザ名とパスワードを入力すると、アクセスが許可され、本機のホームページが表示されます。

[注意] パスワードは 3 回まで再入力することができます。3 回失敗すると接続は切断されます。

[注意] ゲストモード (Normal Exec) で Web インタフェースにログインする場合、ページ情報の閲覧と、ゲストモードのパスワードの変更のみ行えます。管理者モード (Privileged Exec) でログインする場合は全ての設定変更が行えます。

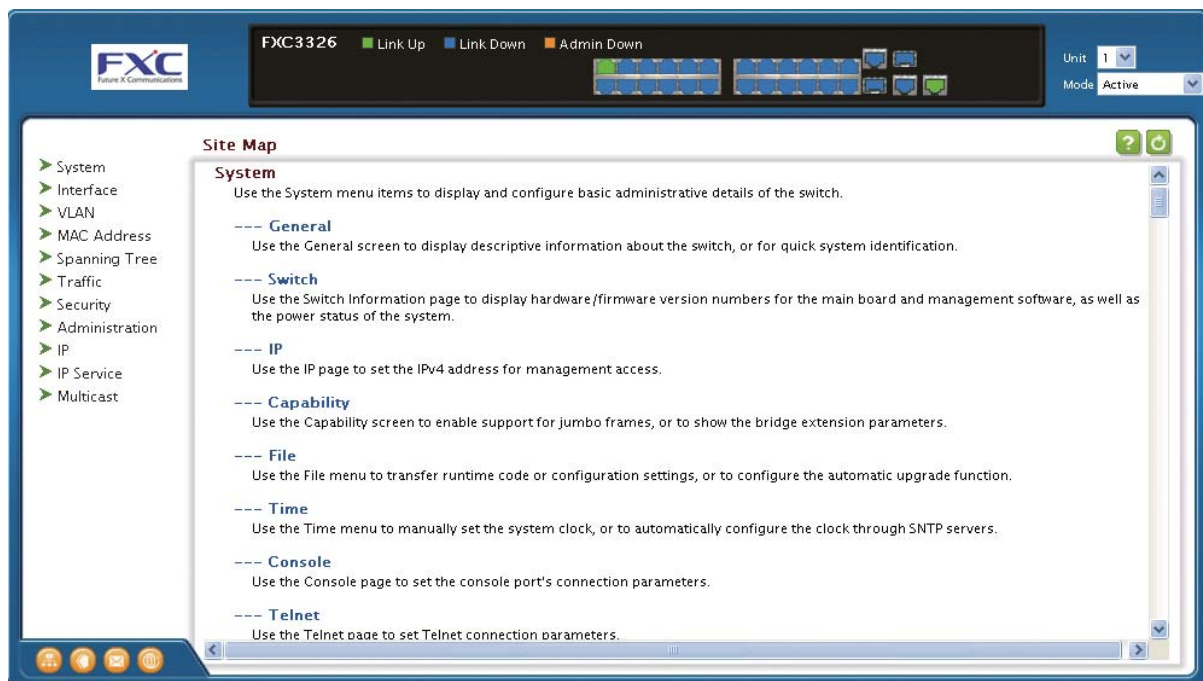
[注意] 管理用 PC と本機の間でスパニングツリーアルゴリズム (STA) が使用されていない場合、管理用 PC に接続されたポートをファストフォワーディングにする (Admin Edge Port の有効化) ことにより、Web インタフェースからの設定に対する本機の応答速度を向上させることができます (詳細は P123 「インタフェース設定」を参照して下さい)

3.2 Web インタフェースの操作方法

Web インタフェースへアクセスする際は、初めにユーザ名とパスワードを入力する必要があります。管理者モード (Privileged Exec) では全ての設定パラメータの表示 / 変更と統計情報の表示が可能です。管理者モード (Privileged Exec) の初期設定のユーザ名とパスワードは "admin" です

3.2.1 ホームページ

Web インタフェースにアクセスした際の本機の管理画面のホームページは以下の通り表示されます。画面の左側にメインメニュー、右側にはシステム情報が表示されます。メインメニューからは、他のメニューや設定パラメータ、統計情報の表示されたページへリンクしています。



3.2.2 設定オプション

設定パラメータにはダイアログボックスとドロップダウンリストがあります。

ページ上で設定変更を行った際は、必ず新しい設定を反映させるために、[Apply] ボタンをクリックしてください。

次の表は Web ページに表示される設定ボタンの内容を解説しています。

ボタン	操作
Revert	入力した値をキャンセルし、[Apply] 又は [Apply Changes] をクリックする前に表示されていた元の値に戻す
Apply	入力した値を本機に反映させる
Help	Web ヘルプにリンクしています

[注意] ページ内容の更新を確実に行うため、Internet Explorer 5.x ではメニューから [ツール] → [インターネットオプション] → [全般] → [インターネット一時ファイル] を選択し、[設定で保存しているページの新しいバージョンの確認] の [ページを表示するごとに確認する] をチェックして下さい。

3.2.3 パネルの表示

Web インタフェースではポートの状態が画像で表示されます。各ポートのリンク状態、Duplex、フローコントロールなどの状態を確認することができます。また、各ポートをクリックすることで P48 「ポート設定」で解説している各ポートの設定ページが表示されます。



3.3 基本設定

3.3.1 システム情報の表示

System>General ページを使用し、本機の名前、設置場所及びコンタクト情報等を表示することができます。

設定・表示項目

System Description

デバイスタイプの説明

System Object ID

本機のネットワーク管理サブシステムの MIBII オブジェクト ID

System Up Time

管理システムを起動してからの時間

System Name

本機に設定した名前

System Location

本機の設置場所

System Contact

管理者のコンタクト情報

設定方法

- (1) [System] → [General] をクリックします。
- (2) システム管理者の System Name、Location、Contact 情報を指定し、< Apply >をクリックします。

System > General

System Description	FXC3326
System Object ID	1.3.6.1.4.1.25574.11
System Up Time	0 days, 4 hours, 54 minutes, and 30.97 seconds
System Name	
System Location	
System Contact	

3.3.2 ハードウェア及びソフトウェアバージョンの表示

System > Switch ページを使用し、メインボードと管理ソフトウェアのハードウェア / ファームウェアバージョン、システムの電源ステータスを確認できます。

設定・表示項目

Main Board（ハードウェア本体）

Serial Number

ご購入いただきました製品につきましては、製品底面に添付された serialNumber をご参照下さい。

Number of Ports

搭載された RJ-45 ポートの数

Hardware Version

ハードウェアのバージョン

Internal Power Status

内部電源のステータスを表示

Management Software（管理ソフトウェア）

Role

本機が Master、Slave どちらで動作しているかを表示

EPLD Version

EPLD（Electronically Programmable Logic Device）コードのバージョン

Loader Version

Loader コードのバージョン

Diagnostics Code Version

Power-On Self-Test (POST) 及び boot コードのバージョン

Operation Code Version

runtime コードのバージョン

設定方法

(1) [System] → [Switch] をクリックします。

System > Switch	
Main Board Information	
Serial Number	LN10220064
Number of Ports	26
Hardware Version	R01A
Internal Power Status	Active
Management Software Information	
Role	Master
EPLD Version	0.00
Loader Version	1.0.1.5R01
Diagnostics Code Version	0.0.0.1
Operation Code Version	1.1.0.1

3.3.3 Jumbo フレームの有効化

Jumbo フレームを有効を有効化することにより、ギガビットイーサネット使用時に、最大 10240 バイトの Jumbo フレームパケットをサポートできます。

機能解説

- Jumbo フレームを使用するためには、ソース・ディスティネーション両方の終端ノード（PC またはサーバ）がこの機能をサポートしている必要があります。
同じく、接続が全二重で稼動している際には、2つの終端のノード間のネットワークにある全てのスイッチが拡張フレームサイズを受け取れなくてはなりません。
半二重接続時は、コリジョンドメインの全てのデバイスが Jumbo フレームをサポートしている必要があります。

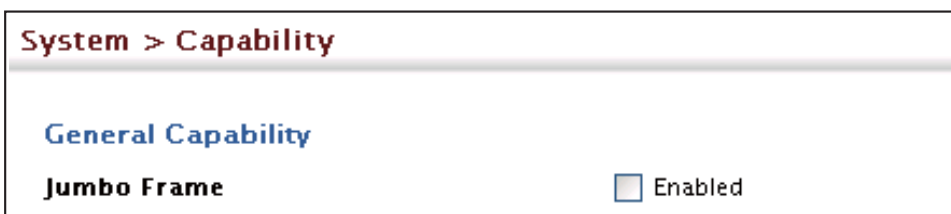
設定・表示項目

Jumbo Frame

Jumbo フレームサポートを設定します。（初期設定：無効）

設定方法

- (1) [System] → [Capability] をクリックします。
- (2) Jumbo Frame サポートの「Enable」チェックマークにチェックを入れます。
チェックを外すことで無効に出来ます。



3.3.4 ブリッジ拡張機能の表示

ブリッジ MIB には、トラフィッククラス、マルチキャストフィルタリング、VLAN に対応した管理装置用の拡張情報が含まれます。

System > Capability ページを使用することで、これらの設定を確認することが出来ます。

設定・表示項目

Extended Multicast Filtering Services

GARP Multicast Registration Protocol(GMRP) を使用した個々のマルチキャストアドレスのフィルタリングが行われないことを表します（現在のファームウェアでは使用できません）

Traffic Classes

ユーザプライオリティが複数のトラフィッククラスにマッピングされていることを表します。（詳細は、P136 「Class of Service (CoS)」を参照して下さい）

Static Entry Individual Port

ユニキャスト及びマルチキャストアドレスの静的フィルタリングが行なわれていることを表します。

VLAN Version Number

"1" は 1 つのスパニングツリー（SST）、"2" がマルチプルスパニングツリー（MST）を示します。

VLAN Learning

本機は各ポートが独自のフィルタリングデータベースを保有する Independent VLAN Learning(IVL) を使用していることを表しています。

Local VLAN Capable

本機は複数のローカルブリッジ（マルチプルスパニングツリー）をサポートしていることを表しています。

Configurable PVID Tagging

本機は各ポートに対して初期ポート VLAN ID（フレームタグで使用する PVID）と、その出力形式（タグ付又はタグなし VLAN）が設定可能であることを表しています（P80 「VLAN」を参照して下さい）

Max Supported VLAN Numbers

本機でサポートされる VLAN の最大数

Max Supported VLAN ID

本機でサポートされる設定可能な VLAN 識別子

GMRP

GMRP を使用することで、マルチキャストグループ内の終端端末をネットワーク機器に登録することができます。本機では GMRP に対応していません。本機は自動的なマルチキャストフィルタリングを行う Internet Group Management Protocol (IGMP) を使用しています。

設定方法

(1) [System] → [Capability] をクリックします。

System > Capability

General Capability

Jumbo Frame	☐ Enabled

Bridge Extension

Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Version Number	1
VLAN Learning	IVL
Local VLAN Capable	No
Configurable PVID Tagging	Yes
Max Supported VLAN Numbers	256
Max Supported VLAN ID	4093
GMRP	Disabled

3.3.5 ファームウェアの管理

本項では、本機のオペレーティングソフトウェアまたは設定ファイルのアップグレード方法および、システム起動ファイルの設定方法について解説します。

FTP/TFTP、HTTP 経由のファイルコピー

System>File (Copy) ページにて、FTP/TFTP、HTTP を使用してファームウェアまたは設定ファイルのアップロード / ダウンロードを行うことが出来ます。

ファイルをダウンロードした際、保存先ファイル名は、現在のファイルと置き換えるように設定することが可能です。または、ファイルを現在の Run-time コードファイルと異なる名前を使用してダウンロードを行い、その後に新しいファイルをスタートアップファイルとして設定することも可能です。

設定・表示項目

Copy Type

ファームウェアコピーの操作方法。下記のオプションがあります。

- － FTP Upgrade — FTP サーバからスイッチへファイルをコピーします。
- － FTP Download — スイッチから FTP サーバへファイルをコピーします。
- － TFTP Upgrade — TFTP サーバからスイッチへファイルをコピーします。
- － TFTP Download — スイッチから TFTP サーバへファイルをコピーします。
- － HTTP Upgrade — 管理ステーションからスイッチへファイルをコピーします。
- － HTTP Download — スイッチから管理ステーションへファイルをコピーします。

FTP/TFTP Server IP Address

FTP/TFTP サーバの IP アドレス

User Name

FTP サーバアクセスのためのユーザ名

Password

FTP サーバアクセスのためのパスワード

File Type

ファームウェアコピーのための opcode (オペレーションコード)

File Name

ファイル名は大文字と小文字が区別され、スラッシュ及びバックスラッシュを使用することはできません。また、ファイル名の頭文字にはピリオド (.) は使用できません。TFTP サーバ上のファイル名は最長 127 文字、本機内では最長 31 文字です (利用できる文字 :A-Z, a-z,0-9, ".", "-", "_")

Auto reboot after opcode upgrade completed

オペレーションコードのアップグレードが行われた後、自動的にスイッチを再起動します。

[注意] スイッチのファイルディレクトリに保存できるシステムソフトウェア(ランタイムファームウェア等) の最大数は 2 つです。

[注意] ユーザ定義設定ファイルの最大数は使用可能なフラッシュメモリスペースに依存します。

[注意] "Factory_Default_Config.cfg" ファイルは、TFTP サーバまたは管理ステーションにコピーすることが可能ですが、スイッチの宛先ファイル名として使用することは出来ません。

設定方法

ファームウェアのコピー

- (1) [System] → [File] をクリックします。
- (2) 「Action」 から「Copy」を選択します。
- (3) トランスファメソッドとして「FTP Upgrade」、「HTTP Upgrade」、「TFTP Upgrade」のいずれかを選択します。
- (4) FTP または TFTP アップグレードを使用する際、ファイルサーバの IP アドレスを入力します。
- (5) FTP アップグレードを使用する際、FTP サーバアカウントのユーザ名とパスワードを入力します。
- (6) 「File Type」を「Operation Code」に設定します。
- (7) ダウンロードするファイルの名前を入力します。
- (8) スイッチ上のファイルを上書きを選択するか、新しいファイル名を入力します。
- (9) < Apply > をクリックします。

The screenshot shows a web interface titled "System > File". Under the "Action:" dropdown, "Copy" is selected. Below this, the "Copy Type" is set to "TFTP Upgrade". The "TFTP Server IP Address" field is empty. The "File Type" is set to "Operation Code". The "Source File Name" field is empty. The "Destination File Name" section has two radio buttons; the first is selected and points to a dropdown menu showing "es3526ma-7lf-xc_v1.1.0.1.bix". The second radio button points to an empty text field. Below these fields is a checkbox labeled "Auto reboot after opcode upgrade completed." which is currently unchecked. A note states: "Note: If you do not specify a file name, above source file name will be used." At the bottom right are "Apply" and "Revert" buttons.

現在使用しているファイルを置き換え、新しいファイルを使用したい場合は System>Reset メニューでシステムの再起動を行ってください。

現在の設定をローカルファイルへ保存

System > File (Copy) ページを使用し、スイッチ上のローカルファイルへ現在の設定を保存することが出来ます。この設定は、スイッチリブート時にシステムによる自動保存はされません。これらの設定は、現在の起動ファイルまたは、起動ファイルとして設定可能なその他のファイルへ保存する必要があります。

設定・表示項目

Copy Type

コピーの操作方法。下記のオプションがあります。

- － Running-Config －現在の設定をスイッチ上のローカルファイルへコピー

Destination File Name

ファイル名は大文字と小文字が区別され、スラッシュ及びバックスラッシュを使用することはできません。また、ファイル名の頭文字にはピリオド (.) は使用できません。TFTP サーバ上のファイル名は最長 127 文字、本機内では最長 31 文字です（利用できる文字 :A-Z, a-z, 0-9, ".", "-", "_"）

[注意] ユーザ定義設定ファイルの最大数は使用可能なフラッシュメモリスペースに依存します。

設定方法

現在の設定ファイルを保存

- (1) [System] → [File] をクリックします。
- (2) 「Action」 から「Copy」を選択します。
- (3) 「Copy Type」 から「Running-Config」を選択します。
- (4) スイッチ上のファイルを上書きを選択するか、新しいファイル名を入力します。
- (5) < Apply > をクリックします。

System > File

Action: Copy

Copy Type: Running-Config

Destination File Name: ☒ startup1.cfg ☐

Apply Revert

現在使用しているファイルを置き換え、新しいファイルを使用したい場合は System>Reset メニューでシステムの再起動を行ってください。

起動ファイルの設定

System > File (Set Start-Up) ページを使用し、システム初期時に使用するファームウェアまたは設定ファイルを指定することが出来ます。

設定方法

- (1) [System] → [File] をクリックします。
- (2) 「Action」 から 「Set Start-Up」 を選択します。
- (3) スタートアップに使用するオペレーションコードまたは設定ファイルにマークします。
- (4) < Apply > をクリックします。

System > File

Action: Set Start-Up

File List Max: 18 Total: 3

	File Name	File Type	Start-Up	Size (bytes)
☒	es3526ma-7lf-xc_v1.1.0.1.bix	Operation Code	Y	11474116
☐	Factory_Default_Config.cfg	Config File	N	509
☒	startup1.cfg	Config File	Y	4587

Apply
Revert

新しいファームウェアまたは設定ファイルを使用するには System > Reset メニューからシステムを再起動してください。

システムファイルの表示

System > File (Show) ページを使用し、システムディレクトリのファイルを表示または削除を行うことができます。

[注意] スタートアップに指定されたファイルと、Factory_Default_Config.cfg ファイルは削除することが出来ません。

設定方法

システムファイルを表示

- (1) [System] → [File] をクリックします。
- (2) 「Action」 から「Show」を選択します。
- (3) ファイルを削除するには、ファイルリストのファイル名にマークし、< Delete >をクリックします。

System > File

Action: Show

File List Max: 18 Total: 3

☐	File Name	File Type	Start-Up	Size (bytes)
☐	es3526ma-7lf-xc_v1.1.0.1.bix	Operation Code	Y	11474116
☐	Factory_Default_Config.cfg	Config File	N	509
☐	startup1.cfg	Config File	Y	4587

Delete Revert

オペレーションコードの自動アップグレード

本システムはオペレーションコードの自動ダウンロードを設定できます。
現在インストールされているファイルよりも、新しいバージョンのファイルがサーバーに発見された時に、オペレーションコードファイルの自動ダウンロードを行います。
ファイルがサーバーから転送され、ファイルシステムへの書き込みが成功した後、新しいファイルを自動的にスタートアップファイルとして設定し、スイッチの再起動を行います。

機能解説

- この機能が有効の際、スイッチはブートアップシーケンスの間に一度、定義された URL を検索します。
- アップグレードファイルロケーションの URL のホスト部分は、有効な IPv4 IP アドレスに設定してください。DNS ホスト名は認識されません。
有効な IP アドレスは、ピリオドで分けられた 0-255 の 4 つの数から成ります。
- ディレクトリへのパスも同じく定義してください。
もしファイルが TFTP/FTP サービスのルートディレクトリに保存されている場合、"/" を使用して指定してください。(例: ftp://192.168.0.1/)
- ファイル名は、アップグレードファイルロケーション URL に含まれなくてはなりません。リモートサーバに保存されたコードのファイル名は FXC3326.bix になります。
- TFTP 接続は、PASV モードが有効時に確立されます。PASV モードは、FTP トラフィックがブロックされないとしても、ファイアウォールを横断するために必要となります。PASV モードは無効にできません。
- 大文字あるいは小文字のファイル名を受け入れるという点で (例: 本機はサーバーへ "fxc3326.bix" を要求しても、"FXC3326.BIX" を受け取ることができます)、スイッチベースの検索機能は大文字小文字の区別を無視します。しかしながら、Unix 等の多くの Unix ライクシステム (FreeBSD、NetBSD、OpenBSD 等) が、大文字小文字の違いを識別し、同じディレクトリの 2 つのファイル、fxc3326.bix と FXC3326.BIX が別の名前であると認識するということを念頭に置いてください。もし FXC3326.BIX (または fxc3326.bix) として保存されたアップグレードファイルが大文字小文字の違いを識別するサーバに置かれている場合、スイッチ (fxc3326.bix を要求) はアップグレードを行えません。サーバはリクエストされたファイル名と保存されているファイルが同じ物だと認識が出来ないからです。
大文字小文字の違いを識別する Unix ライクオペレーティングシステムの顕著な例外は Mac OS X です。MAC OS X は大文字小文字の違いを無視します。
もし、サーバのオペレーティングシステムの仕様が不確かな場合は、マニュアル等でチェックをしてください。
- もし既に 2 つのオペレーションコードイメージファイルが本機のファイルシステムに保存されている場合、アップグレードイメージが転送される前に、スタートアップイメージ以外のファイルを削除して下さい。
- 自動アップグレードプロセスは、バックグラウンドで行われ、本機の通常のオペレーションを妨げません。
- 自動検索と転送のプロセスの間、管理者は他のオペレーションコードイメージ、設定ファイル、パブリックキー、HTTPS 証明書等の転送またはアップグレードを行うことができません。

- アップグレードオペレーションコードイメージは、ファイルシステムへの書き込みが成功した後、スタートアップファイルとして設定されます。
- 全てのアップグレードの成功 / 失敗後、スイッチは SNMP トラップを送信し、ログエントリを作成します。
- アップグレードファイルのファイルシステムへの書き込みに成功し、スタートアップイメージへ設定された後、スイッチはただちに再起動を行います。

設定・表示項目

Automatic Opcode Upgrade

スイッチブートアッププロセス時に、アップグレードオペレーションコードファイルの検索を有効にします。(初期設定：無効)

Automatic Upgrade Location URL

スイッチブートアッププロセス時にスイッチがオペレーションコードアップグレードファイルを検索する場所を定義します。URL の最後の文字は ("/") になります。

スイッチによって自動的に付加される為、FXC3326.bix ファイル名は含みません。

(オプション：ftp、tftp)

tftp://host[/filedir]/

tftp:// - サーバ接続の TFTP プロトコルを定義します。

host - TFTP サーバの IP アドレスを定義します。有効な IP アドレスは、ピリオドで分けられた 0-255 の 4 つの数から成ります。DNS ホスト名は認識されません。

filedir - ディレクトリを定義します。

/ - URL の最後の文字であることを示します。

ftp://[username[:password@]][host[/filedir]]/

ftp:// - サーバ接続の FTP プロトコルを定義します。

Username - FTP 接続のユーザ名を定義します。入力を省略した場合、仮ユーザ名は "anonymous" になります。

Password - FTP 接続のパスワードを定義します。パスワードを、URL のホスト部分とユーザ名から区別するために、パスワードの前にはコロン (:) を付けて下さい。また、パスワードの後にはアットマーク (@) を付けて下さい。

host - FTP サーバの IP アドレスを定義します。有効な IP アドレスは、ピリオドで分けられた 0-255 の 4 つの数から成ります。DNS ホスト名は認識されません。

filedir - ディレクトリを定義します。

/ - URL の最後の文字であることを示します。

例

- 次の例は、様々な場所に保存されたオペレーションコードイメージと、IP アドレス 192.168.0.1 の TFTP サーバを示す URL 構文です。

— tftp://192.168.0.1/

イメージファイルは TFTP ルートディレクトリにあります。

— tftp://192.168.0.1/switch-opcode/

イメージファイルは TFTP ルートに相対的な "switch-opcode" ディレクトリにあります。

— tftp://192.168.0.1/switches/opcode/

イメージファイルは "opcode" ディレクトリにあり、それは TFTP ルートに相対的な "switches" 親ディレクトリの中にあります。

- 次の例は、様々なユーザ名、パスワード、ロケーションと IP アドレス 192.168.0.1 の FTP サーバを示す URL 構文です。

- ftp://192.168.0.1/
ユーザ名とパスワードは空です。ユーザ名は "anonymous"、パスワードはブランクになります。イメージファイルは FTP ルートディレクトリにあります。
- ftp://switches:upgrade@192.168.0.1/
ユーザ名は "switches"、パスワードは "upgrade" です。イメージファイルは FTP ルールにあります。
- ftp://switches:upgrade@192.168.0.1/switches/opcode/
ユーザ名は "switches"、パスワードは "upgrade" です。イメージファイルは "opcode" ディレクトリにあり、それは TFTP ルートに相対的な "switches" 親ディレクトの中にあります。

設定方法

システムファイルを表示

- (1) [System] → [File] をクリックします。
- (2) 「Action」 から 「Automatic Operation Code Upgrade」 を選択します。
- (3) 「Automatic Opcode Upgrade」 の Enable チェックボックスにチェックを入れます。
- (4) FTP または TFTP サーバの URL とオペレーティングコードがあるパスとディレクトリを入力します。
- (5) < Apply > をクリックします。

System > File

Action: Automatic Operation Code Upgrade ▼

Automatic Opcode Upgrade ☐ Enabled

Automatic Upgrade Location
URL

Note: The last character of this URL must be a forward slash ("/").
For automatic upgrades, the operation code file name must be set as ES3526ma.bix.

Apply Revert

3.3.6 システムクロックの設定

SNTP(Simple Network Time Protocol) 機能は、タイムサーバ (SNTP/NTP) からの周期的なアップデートにより本機内部の時刻設定を行うことができます。本機の内部時刻の設定を正確に保つことにより、システムログの保存の際に日時を正確に記録することができます。また、手動で時刻の設定を行うこともできます。

時刻の設定がされていない場合、初期設定の時刻が記録され本機起動時からの時間となります。本機は SNTP クライアントとして有効な場合、設定してあるタイムサーバに対して時刻の取得を要求します。最大 3 つのタイムサーバの IP アドレスを設定することができます。各サーバに対して時刻の取得を要求します。

手動設定

本機では、SNTP を使用せず手動でシステムを時間を設定することも可能です。

設定・表示項目

Current Time

スイッチに設定された、現在の時刻を表示

Hours

時を設定 (範囲: 0-23 初期設定: 0)

Minutes

分を設定 (範囲: 0-59 初期設定: 0)

Seconds

秒を設定 (範囲: 0-59 初期設定: 0)

Month

月を設定 (範囲: 1-12 初期設定: 1)

Day

日を設定 (範囲: 1-31 初期設定: 1)

Year

年を設定 (範囲: 2001-2100 初期設定: 2001)

設定方法

- (1) [System] → [Time] をクリックします。
- (2) 「Action」 から「Configure General」を選択します。
- (3) 「Maintain Type」 リストから「Maintain Type」を選択します。
- (4) 時刻と日付を設定します。
- (5) < Apply > をクリックします。

System > Time

Step: 1. Configure General

Current Time 2010-3-29 16:18:18

Maintain Type Manually

16 Hours 18 Minutes 18 Seconds

3 Month 29 Day 2010 Year

Apply Revert

SNTP 設定

本機では、特定のタイムサーバに対して時間の同期リクエストを送信します。

設定・表示項目

Current Time

スイッチに設定された、現在の時刻を表示

SNTP Poll Interval

SNTP クライアントモード時のタイムサーバに対する時刻更新リクエストの送信間隔を設定します（範囲：16-16384 秒、初期設定：16 秒）

設定方法

- (1) [System] → [Time] をクリックします。
- (2) 「Action」 から「Configure General」を選択します。
- (3) 「Maintain Type」 リストから「SNTP」を選択します。
- (4) 必要の応じ、「polling interval」を編集します。
- (5) < Apply > をクリックします。

System > Time

Step: 1. Configure General

Current Time 2010-3-29 16:18:18

Maintain Type SNTP

SNTP Configuration

SNTP Polling Interval (16-16384) 16 sec

Apply Revert

SNTP タイムサーバの設定

System > Time (Configure Time Server) ページを使用し、最大 3 つのタイムサーバアドレスを指定出来ます。

設定・表示項目

SNTP Server IP Address

最大 3 つのタイムサーバアドレスを設定できます。

設定方法

- (1) [System] → [Time] をクリックします。
- (2) 「Action」 から「Configure Time Server」を選択します。
- (3) 最大 3 つのタイムサーバ IP アドレスを入力します。
- (4) < Apply > をクリックします。

System > Time

Step: 2. Configure Time Server ▼

SNTP Server IP Address 1	10.1.0.19
SNTP Server IP Address 2	137.82.140.80
SNTP Server IP Address 3	128.250.36.2

Apply Revert

タイムゾーンの設定

SNTP では UTC(Coordinated Universal Time: 協定世界時間。別名：GMT/Greenwich Mean Time) を使用します。本機を設置している現地時間に対応するために UTC からの時差（タイムゾーン）の設定を行う必要があります。
80 の既定義タイムゾーンから 1 つを選択、あるいは手動でローカルタイムのパラメータを設定することが出来ます。

設定・表示項目

Direction

UTC からのタイムゾーンの差がプラスかマイナスかを設定します。

Name

UTC からのタイムゾーンの差がプラスかマイナスかを設定します。

Hours (0-13)

UTC からの時間の差を設定します。

Minutes (0-59)

UTC からの時間（分数）の差を設定します。

設定方法

- (1) [System] → [Time] をクリックします。
- (2) 「Action」 から「Configure Time Zone」を選択します。
- (3) タイムゾーンとオフセットを設定してください。
- (4) < Apply > をクリックします。

System > Time

Step: 3. Configure Time Zone

DirectionAfter UTC

NameUTC

Hours (0-13)0

Minutes (0-59)0

Note: The maximum value before UTC is 12:00.
The maximum value after UTC is 13:00.

ApplyRevert

3.3.7 コンソールポートの設定

VT100 端末を本機のシリアル（コンソール）ポートに接続し、本機の設定を行うことができます。コンソール経由での管理機能の利用は、パスワード、タイムアウト、その他の基本的な通信条件など、数々のパラメータにより可能となります。CLI または Web インタフェースからパラメータ値の設定を行うことができます。

設定・表示項目

Login Timeout

CLI でのログインタイムアウト時間。設定時間内にログインが行われない場合、その接続は切断されます（範囲：0-300 秒、初期設定：0 秒）

Exec Timeout

ユーザ入力のタイムアウト時間。設定時間内に入力が行われない場合、その接続は切断されます（範囲：0-65535 秒、初期設定：600 秒）

Password Threshold

ログイン時のパスワード入力のリトライ回数。リトライ数が設定値を超えた場合、本機は一定時間（Silent Time パラメータで指定した時間）、ログインのリクエストに応答しなくなります（範囲：0-120 回、初期設定：3 回）

Quiet Period

パスワード入力のリトライ数を超えた場合に、コンソールへのアクセスができなくなる時間（範囲：0-65535 秒、初期設定：30 秒）

Data Bits

コンソールポートで生成される各文字あたりのデータビットの値。パリティが生成されている場合は 7 データビットを、パリティが生成されていない場合 (no parity) は 8 データビットを指定して下さい（初期設定：8 ビット）

Stop Bits

送信するストップビットの値（範囲：1-2、初期設定：1 ストップビット）

Parity

パリティビット。接続するターミナルによっては個々のパリティビットの設定を要求する場合があります。Even(偶数)、Odd(奇数)、None(なし) から設定します（初期設定：None）

Speed

ターミナル接続の送信（ターミナルへの）/ 受信（ターミナルからの）ボーレート。シリアルポートに接続された機器でサポートされているボーレートを指定して下さい。（範囲：9600、19200、38400、57600、115200baud 初期設定：9600baud）

[注意] コンソール接続のパスワードは CLI からのみ設定出来ます。（P404 「password」を参照）

[注意] コンソール接続ログインのパスワードチェックは有効または無効に出来ます。（P402 「login」を参照）

[注意] "password" コマンドで設定されたシングルグローバルパスワードによる認証または、ユーザネームアカウントのために設定されたパスワードによる認証から選択が可能です。スイッチ上に設定されている初期設定はローカルパスワードです。

設定方法

- (1) [System] → [Console] をクリックします。
- (2) 必要な接続パラメータを指定します。
- (3) < Apply > をクリックします。

System > Console

Login Timeout (0-300)	0	sec (0: Disabled)
Exec Timeout (0-65535)	0	sec (0: Disabled)
Password Threshold (0-120)	3	(0: Disabled)
Quiet Period (0-65535)	0	sec (0: Disabled)
Data Bits	8	
Stop Bits	1	
Parity	None	
Speed	115200	baud

3.3.8 Telnet の設定

ネットワーク経由、Telnet (仮想ターミナル) で本機の設定を行うことができます。Telnet 経由での管理機能利用の可 / 不可、または TCP ポート番号、タイムアウト、パスワードなど数々のパラメータの設定が可能です。CLI または Web インタフェースからパラメータ値の設定を行うことができます。

設定・表示項目

Telnet Status

本機への Telnet 接続の有効 / 無効 (初期設定 : 有効)

TCP Port

本機へ Telnet 接続する場合の TCP ポート番号 (初期設定 : 23)

Login Timeout

CLI でのログインタイムアウト時間。設定時間内にログインが行われない場合、その接続は切断されます (範囲 : 0-300 秒、初期設定 : 300 秒)

Exec Timeout

ユーザ入力のタイムアウト時間。設定時間内に入力が行われない場合、その接続は切断されます (範囲 : 0-65535 秒、初期設定 : 600 秒)

Password Threshold

ログイン時のパスワード入力のリトライ回数。

(範囲 : 0-120 回、初期設定 : 3 回)

Quiet Period

パスワード入力のリトライ数を超えた場合に、管理インタフェースへのアクセスができなくなる時間 (範囲 : 0-65535 秒、初期設定 : 30 秒)

設定方法

- (1) [System] → [Telnet] をクリックします。
- (2) 必要な接続パラメータを指定します。
- (3) < Apply > をクリックします。

System > Telnet

Telnet Status	☒ Enabled
TCP Port (1-65535)	23
Login Timeout (1-300)	300
Exec Timeout (1-65535)	600
Password Threshold (0-120)	3 (0: Disabled)
Quiet Period (0-65535)	0 sec (0: Disabled)

3.3.9 CPU 使用率の表示

System > CPU Utilization ページを使用し、CPU 使用率を表示します。

設定・表示項目

Time Interval

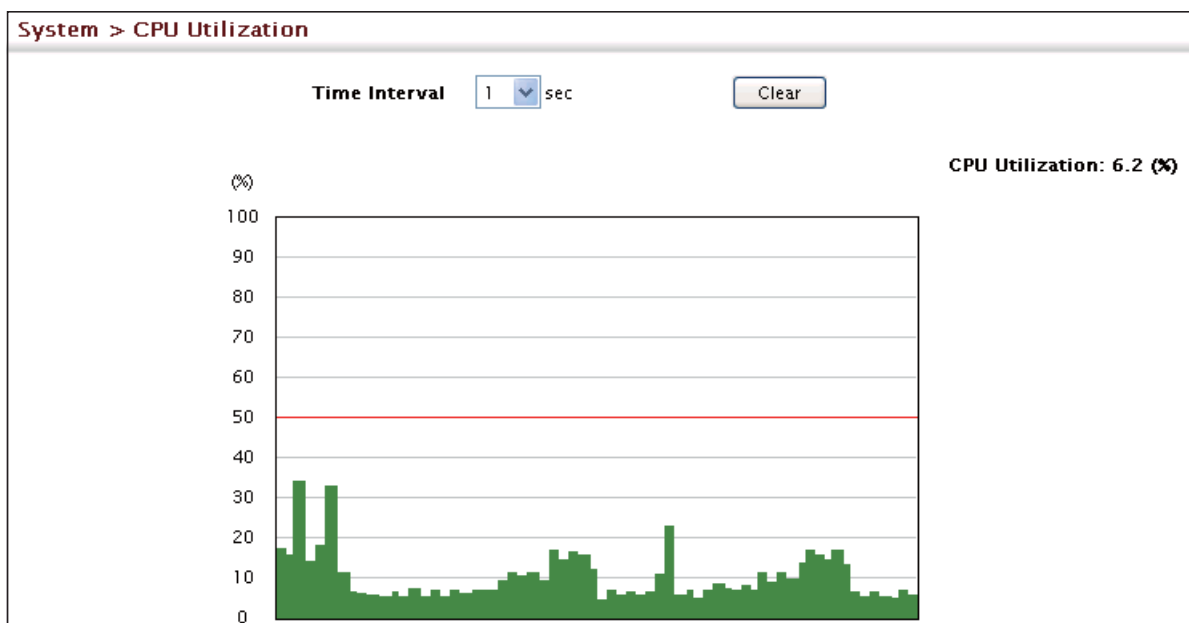
表示する使用率を更新する間隔。(オプション: 1、5、10、30、60 秒 初期設定: 1 秒)

CPU Utilization

指定した間隔の CPU 使用率

設定方法

- (1) [System] → [CPU Utilization] をクリックします。
- (2) 必要に応じ、「Time Interval」を変更します。



3.3.10 メモリ使用率の表示

System > Memory Status ページを使用し、メモリ使用率パラメータを表示します。

設定・表示項目

Free Size

現在の空きメモリ容量

Used Size

アクティブな処理に割り当てられたメモリの容量

Total

システムメモリの合計容量

設定方法

(1) [System] → [Memory Status] をクリックします。

System > Memory Status	
Memory Status	
Free Size	51830784 bytes
Used Size	82386944 bytes
Total	134217728 bytes

3.3.11 再起動

System > Reset メニューを使用し、スイッチを即座に、または指定した時刻、指定した時間経過後、定期的な間隔で再起動することが出来ます。

機能解説

- 本コマンドは全てのシステムをリセットします。
- システム再起動実行時、常に Power-On Self テストが実行されます。"copy running-config startup-config" コマンドによって、非揮発性メモリに保存された全ての設定情報は維持されます（P389 「copy」を参照）。

設定・表示項目

システム再起動設定

Reset Mode

スイッチをただちに、または指定した時間に再起動します。

- Immediately –システムをただちに再起動します。
- In –スイッチの再起動を行うまでの時間を指定します。（時間の指定は 24 日かそれ以下にしてください）
 - hours –時間（時）を指定。（分）と組み合わせてスイッチ再起動までの時間（範囲：0-576）
 - minutes –時間（分）を指定。（時）と組み合わせてスイッチ再起動までの時間（範囲：0-59）
- At –スイッチの再起動を行う日時を指定します。
 - DD –日付を指定（範囲：1-31）
 - MM –月を指定（範囲：january ... december）
 - YYYY –年を指定（範囲：2001-2050）
 - HH –時間（時）を指定。（範囲：0-23）
 - MM –時間（分）を指定。（範囲：0-59）
- Regularly –スイッチの再起動を行う間隔を指定します。
- 時間
 - HH –再起動を行う時間（時）（範囲：0-23）
 - MM –再起動を行う時間（分）（範囲：0-59）
- 間隔
 - Daily –毎日
 - Weekly –再起動を行う曜日を指定（Sunday – Saturday）
 - Monthly –再起動を行う月（範囲：1-31）

設定方法

スイッチの再起動（即時）

- (1) [System] → [Restart] をクリックします。
- (2) リセットモードを選択します。
- (3) 「reset immediately」 以外の場合は必要なオプションパラメータを入力します。
- (4) < Apply > をクリックします。
- (5) プロンプトが表示されるので、確認後「OK」をクリックしてください。

System > Reset

System Reload Information:
No configured settings for reloading.

Refresh Cancel

System Reload Configuration:

Reset Mode

Apply Revert

Microsoft Internet Explorer

Note: It takes around 100~120 seconds to finish system reboot.
Do you want to reset the switch immediately?

OK キャンセル

スイッチの再起動（再起動までの時間を指定）

System > Reset

System Reload Information:
No configured settings for reloading.

Refresh Cancel

System Reload Configuration:

Reset Mode

Reload switch in hours minutes.

Note: The specified time must be equal to or less than 24 days.

Apply Revert

スイッチの再起動（時刻を指定）

System > Reset

System Reload Information:
No configured settings for reloading.

Refresh
Cancel

System Reload Configuration:
Reset Mode At

Reload switch at 19/05/2010 (DD/MM/YYYY) 15:00 (HH:MM)
Warning: You have to setup system time first.Otherwise this function won't work.

Apply
Revert

スイッチの再起動（定期的に実行）

System > Reset

System Reload Information:
Warning: Because you don't setup system time first, the reload function won't work properly!
Reloading switch at time: October 19 05:00 2010.

Refresh
Cancel

System Reload Configuration:
Reset Mode Regularly

Time 05:30 (HH:MM)
Period ☒ Daily ☐ Weekly Sunday ☐ Monthly 1
Warning: You have to setup system time first.Otherwise this function won't work.

Apply
Revert

3.4 インタフェース設定

3.4.1 ポート設定

ポート接続、1つのポートから他のポートへのトラフィックミラー、ケーブル解析の設定について解説します。

ポートリストによる設定

Interface > Port > General (Configure by Port List ページを使用し、インタフェースの有効 / 無効、オートネゴシエーションおよびインタフェースキャパビリティのアドバタイズへの設定、手動固定スピード、デュプレックスモード、フローコントロールの設定を行います。

機能解説

- ポートの設定を手動で行ない、Speed/Duplex モード 及び Flow Control の設定を反映させるためには、Autonegotiation（オートネゴシエーション）は Disabled（無効）にする必要があります。
- オートネゴシエーション使用時、リンクパートナーとの間で、それらのアドバタイズ能力をベースに最適な設定が交渉されます。スピード、デュプレックスモード、オートネゴシエーション下のフローコントロールを設定するために、必要なオペレーションモードをインタフェースのキャパビリティリストで指定してください。

設定・表示項目

Port

ポート識別子（範囲：1-26）

Type

ポートの種類 (100Base-TX 又は 1000BASE-T, SFP) の表示

Name

ポート名（範囲：1-64 文字）

Admin

インタフェースの有効 / 無効

Media Type

メディアタイプ（ポート 25-26）

- Copper-Forced — 常に RJ-45 ポートを使用。
- SFP-Forced — 常に SFP ポートを使用。
(モジュールがインストールされていなくても)
- SFP-Preferred-Auto — 両方が作用しており、SFP ポートのリンクが確立していれば SFP を使用。(初期設定)

Autonegotiation (Port Capabilities)

オートネゴシエーションの有効 / 無効を設定。オートネゴシエーションが使用可能時、アドバタイズされるキャパビリティを指定する必要があります。
オートネゴシエーションが無効時、スピード、モードおよびフローコントロールを固定で設定することが出来ます。

- 10half — 10 Mbps half-duplex をサポート
- 10full — 10 Mbps full-duplex をサポート

- 100half – 100 Mbps half-duplex をサポート
- 100full – 100 Mbps full-duplex をサポート
- 1000full – 1000 Mbps full-duplex をサポート (port25、26 のみ)
- Sym (Gigabit のみ) – ポーズフレームの送受信を行うチェック
- FC – フローコントロールは、バッファが満杯になった時に、エンドステーションまたはスイッチに直接接続されたセグメントからの "blocking" トラフィックによってフレーム損失を排除することが可能です。有効時、プレッシャーは half-duplex オペレーションと Ifullduplex オペレーションの IEEE 802.3-2005 (formally IEEE 802.3x) に使用されます。
問題を解決する必要がある場合以外、ハブへ接続されたポートでフローコントロールを使用するのは避けてください。さもなければ、バックプレッシャーのジャム信号は、ハブに接続されたセグメントの全体的なパフォーマンスを落すかもしれません。
初期設定：
オートネゴシエーション 有効
アドバイズド能力
 - 100Base-TX=10half、10full、100half、100full
 - 1000Base-SX/LX/LH=1000full)

Speed/Duplex

オートネゴシエーションを無効にした場合に、ポートの通信速度及び通信方式を手動で設定できます。

Flow Control

フローコントロールを自動設定又は手動設定で行うことができます

設定方法

- (1) [Interface] → [Port] → [General] をクリックします。
- (2) 「Step」 リストから「Configure by Port List」を選択します。
- (3) 必要な設定を編集します。
- (4) < Apply >をクリックします。

Interface > Port > General

Action: Configure by Port List

Port List Max: 26 Total: 26

Port	Type	Name	Admin	Media Type	Autonegotiation				Speed Duplex	Flow Control
1	100Base-TX		☒ Enabled	Copper-Forced	☒ 10h	☒ 100h	☐ 1000h	☐ Sym	100full	☒ Enabled
2	100Base-TX		☒ Enabled	Copper-Forced	☒ 10h	☒ 100h	☐ 1000h	☐ Sym	100full	☒ Enabled
3	100Base-TX		☒ Enabled	Copper-Forced	☒ 10h	☒ 100h	☐ 1000h	☐ Sym	100full	☒ Enabled
4	100Base-TX		☒ Enabled	Copper-Forced	☒ 10h	☒ 100h	☐ 1000h	☐ Sym	100full	☒ Enabled

ポート範囲による設定

Interface > Port > General (Configure by Port Range) ページを使用し、インタフェースの有効 / 無効、オートネゴシエーションおよびインタフェースキャパビリティのアドバタイズへの設定、手動固定スピード、デュプレックスモード、フローコントロールの設定を行います。コマンド使用に関する情報とパラメータの解説の詳細は P48 「ポートリストによる設定」を参照してください。

設定方法

- (1) [Interface] → [Port] → [General] をクリックします。
- (2) 「Step」 リストから「Configure by Port Range」を選択します。
- (3) 設定変更を行うポートの範囲を入力します。
- (4) 必要な設定を編集します。
- (5) < Apply > をクリックします。

Interface > Port > General

Action: Configure by Port Range ▾

Port Range (1-10)

1 - 5

Admin

☒ Enabled

Autonegotiation

☒ Enabled

☐ 10h ☒ 100h ☐ 1000h ☐ Sym

☒ 10f ☒ 100f ☐ 1000f ☐ FC

Speed Duplex

10half ▾

Flow Control

☐ Enabled

Apply

Revert

接続状況の表示

接続状態の情報・速度及び通信方式・フロー制御そして、オートネゴシエーションを含む現在の接続情報を表示するために Interface > Port > General ページを使用することができます。

設定・表示項目

Port

ポート識別子

Type

ポートの種類 (100Base-TX 又は 1000BASE-T, SFP) の表示

Name

インタフェースラベルの表示

Admin

インタフェースの有効 / 無効の表示

Oper Status

リンクアップ / リンクダウンの表示

Media Type

メディアタイプの表示（オプション：RJ-45 - Copper-Forced、SFP -Copper-Forced、SFP-Forced、SFP-Preferred-Auto 初期設定：RJ-45 - Copper-Forced、SFP-Preferred-Auto）

Autonegotiation

オートネゴシエーションの有効 / 無効の表示

Oper Speed Duplex

現在のスピードと通信モードを表示

Oper Flow Control

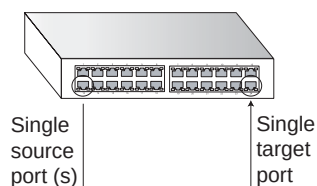
フローコントロールの有効 / 無効を表示

設定方法

- (1) [Interface] → [Port] → [General] をクリックします。
- (2) 「Step」 リストから「Show Information」を選択します。

Interface > Port > General								
Action: Show Information								
Port List Max: 26 Total: 26 1 2 3								
Port	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	100Base-TX		Enabled	Up	Copper-Forced	Enabled	100full	None
2	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
3	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
4	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
5	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
6	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
7	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
8	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
9	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None
10	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None

ポートミラーリングの設定



リアルタイムで通信の解析を行うために、ソースポートからターゲットポートへ通信のミラーリングをする事ができます。それにより、ターゲットポートにネットワーク解析装置（Sniffer 等）又は RMON プローブを接続し、通信に影響を与えずにソースポートのトラフィックを解析することができます。

機能解説

- ・ トラフィックは、同じスイッチ 1 つ以上のソースポートからディスティネーションポートへのミラー（ローカルポートミラーリングについては本項にて説明しています）、またはリモートスイッチ上の 1 つ以上のソースポートから本機のディスティネーションポートへミラーを行うことが可能です（リモートポートミラーリングについては P54 「リモートポートミラーリングの設定」を参照）。
- ・ ソースポートとターゲットポートの通信速度は同じでなければいけません。通信速度が異なる場合には、通信がターゲットポート側で落とされます。
- ・ VLAN トラフィック（P106 「VLAN ミラーリング」を参照）、またはソース MAC アドレスを基にしたパケットのミラー時（P113 「MAC アドレスミラーリングの設定」を参照）、ターゲットポートは、このコマンドによってポートミラーリングに使用されているターゲットポートに設定することは出来ません。
- ・ トラフィックがポートミラーリングと VLAN トラフィックまたは MAC アドレスベースパケットのミラーリングの両方にマッチした際、マッチしたパケットはポートミラーリングで指定されたターゲットポートに送信されません。

設定・表示項目

Source Port

通信がモニターされるソースポート

Target Port

ソースポートの通信のミラーリングがされるターゲットポート

Type

モニターを行う通信の種類。

Rx（受信）、Tx（送信）、Both（送・受信）（初期設定：Rx）

設定方法

ローカルミラーセッションの設定

- (1) [Interface] → [Port] → [Mirror] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) 必要な設定を編集します。
- (4) < Apply >をクリックします。

Interface > Port > Mirror

Action: Add ▼

Source Port

Unit 1 ▼ Port 7 ▼

Target Port

Unit 1 ▼ Port 8 ▼

Type

Rx ▼

Apply Revert

ローカルミラーセッションの設定を表示

- (1) [Interface] → [Port] → [Mirror] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

Interface > Port > Mirror

Action: Show ▼

Mirror Session List Max: 10 Total: 1

	Source (Unit/Port)	Target (Unit/Port)	Type
☐	1 / 6	1 / 8	Rx

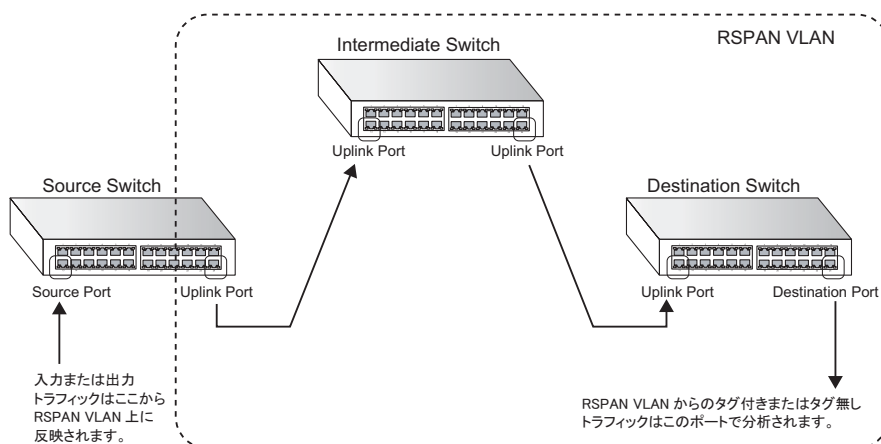
Delete Revert

リモートポートミラーリングの設定

Interface > Port > RSPAN ページを使用し、分析の為、ローカルスイッチのディスティネーションポートでリモートスイッチのトラフィックをミラーすることが出来ます。

この機能は Remote Switched Port Analyzer (RSPAN) と呼ばれ、全ての参加スイッチの RSPAN セッションを専用するユーザ指定 VLAN 上の、指定されたソースポートで生成されたトラフィックを運びます。

下の図で示されるように、1 つまたはそれ以上のソースポートの被監視トラフィックは、RSPAN をモニタする、RSPAN ディスティネーションポートへ運ばれる IEEE802.1Q トランクまたはハイブリッドポートを通して RSPAN VLAN 上にコピーされます。



機能解説

- ・ トラフィックは 1 つまたはそれ以上のソースポートから同じスイッチのディスティネーションポート（52 ページの「ポートミラーリングの設定」を参照）へ、またはリモートスイッチの 1 つまたはそれ以上のソースポートから本機のディスティネーションポート（リモートポートミラーリングとして本項で解説）へミラーが出来ます。

設定ガイドライン

RSPAN セッションを設定するには、以下のステップを実行してください。

- (1) VLAN Static List（83 ページの「VLAN グループの設定」を参照）を使用し、RSPAN で使用する VLAN を確保してください。（このページで "Remote VLAN" にマークします。）デフォルト VLAN 1 は禁止です。
- (2) "RSPAN configuration" ページでミラーセッションを指定し、スイッチのロール (Source)、RSPAN VLAN、アップリンクポート等ソーススイッチをセットアップします。その後、ソースポートとモニタを行うトラフィックタイプ (Rx, Tx or Both) を指定します。
- (3) "RSPAN configuration" ページでミラーセッションを入力し、スイッチロール (Intermediate)、RSPAN VLAN、アップリンクポート等全ての中間スイッチのセットアップを行います。
- (4) "RSPAN configuration" ページでミラーセッション指定し、スイッチロール (Destination)、ディスティネーションポート、このポートを出るトラフィックにタグが付けられるか否か、RSPAN VLAN 等ディスティネーションスイッチのセットアップをします。その後、ミラーされるトラフィックが受信されるそれぞれのアップリンクポートを指定します。

RSPAN 制限事項

本機の RSPAN 機能には以下の制限があります。

- RSPAN Ports –ポートのみが RSPAN ソース、ディスティネーションまたはアップリンクに設定できます。静的または動的トラフィックは許可されません。また、ソースポートとディスティネーションは同じスイッチ上で設定することは出来ません。
- Local/Remote Mirror –ローカルモニタセッションのディスティネーション（Interface > Port > Mirror ページで作成された）は RSPAN トラフィックのディスティネーションには使用できません。
- Spanning Tree –スパンニングツリー無効時、BPDU は RSPAN VLAN 上にはフラッドされません。
- MAC address learning – RSPAN がスイッチで有効時、MAC アドレス学習は RSPAN アップリンクポートではサポートされません。そのため、たとえ RSPAN が設定された後にスパンニングツリーが有効になっても MAC アドレス学習は RSPAN アップリンクポート上で再開されません。
- IEEE 802.1X – RSPAN と 802.1X は相互に排他的な機能です。802.1X がグローバルで有効時、RSPAN ソースおよびディスティネーションポートは設定可能ですが、RSPAN アップリンクポートは設定できません。
RSPAN アップリンクポートがスイッチで有効時、802.1X はグローバルで有効に出来ません。
- Port Security –ポートでポートセキュリティが有効時、RSPAN ソースまたはディスティネーションポートとして設定は出来ませんが、RSPAN アップリンクポートとして設定できません。また、ポートが RSPAN アップリンクポートとして設定されている時、このポートでポートセキュリティは有効にできません。

設定・表示項目

Session

RSPAN セッションを指定（範囲：1-2）

ローカルとリモートモニタリング両方を含む、2つのミラーセッションのみが許可されます。ローカルミラーリングが有効時（P52）、RSPAN で使用可能な1つのセッションのみがあります。

Operation Status

RSPAN が現在機能しているかどうかを示します。

Switch Role

本機がミラーリングトラフィックで行う役割を指定します。

- None –スイッチは RSPAN に参加しません。
- Source –デバイスをリモートミラーリングトラフィックのソースとして指定
- Intermediate –デバイスを、1つまたはそれ以上のソースから1つまたはそれ以上のディスティネーションへ、ミラーリングトラフィックを透過的に渡す中間スイッチとして指定します。
- Destination –デバイスをこのセッションでミラーリングトラフィックを受信するディスティネーションとして設定します。

Remote VLAN

ソースポートからミラーされたトラフィックがフラッドされる VLAN。このフィールドで指定された VLAN は最初に VLAN > Static ページ（P85）で RSPAN アプリケーション用に確保します。

Uplink Port

アップリンクポートを指定します。

ソーススイッチには1つのアップリンクポートのみ設定できますが、中間またはディスティネー

セッションスイッチで設定されたアップリンクポートの数には制限がありません。ディスティネーションおよびアップリンクポートのみがスイッチによって RSPAN VLAN のメンバーとして割り当てられます。ポートを VLAN > Static ページにて、手作業で RSPAN VLAN に割り当てすることは出来ません。同様に、GVRP は動的に RSPAN VLAN にポートメンバを追加することは出来ません。また、VLAN > Static (Show) ページは RSPAN VLAN のメンバーを表示しませんが、設定された RSPAN VLAN 識別子のみ表示します。

Type

リモートでミラーされるトラフィックのタイプを指定します。(オプション: Rx, Tx, Both)

Destination Port

ソースポートからミラーされるトラフィックをモニタするディスティネーションポートを指定します。1つのディスティネーションポートのみ同じスイッチのセッションごとに設定できますが、ディスティネーションポートは同じセッションの1つ以上のスイッチには設定できません。また、ディスティネーションポートは依然スイッチされたトラフィックの送受信と、アサインされたレイヤ2プロトコルに参加が可能です。

Tag

ディスティネーションポートを出て、管理デバイスへ行くトラフィックに RSPAN VLAN タグが付加されるかどうかを指定します。

設定方法

リモートミラーセッションの設定 (ソース)

- (1) [Interface] → [RSPAN] をクリックします。
- (2) 「Switch Role」を「None」、「Source」、「Intermediate」、「Destination」のいずれかに設定します。
- (3) 必要な項目の設定を行い、< Apply >をクリックします。

Interface > RSPAN

Session

Operation Status Up

Switch Role

Remote VLAN

Uplink Port

Source Port Configuration List Max: 10 Total: 10

Source Port	Type
1	None
2	Both
3	None
4	None
5	None
6	None
7	None

リモートミラーセッションの設定（中間）

Interface > RSPAN

Session

1

Operation Status

Down

Switch Role

Intermediate

Remote VLAN

5

Uplink Port List

Max: 26

Total: 26

123

Port	Uplink
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐

リモートミラーセッションの設定（ディスティネーション）

Interface > RSPAN

Session

1

Operation Status

Down

Switch Role

Destination

Destination Port

1

Tag

Untagged

Remote VLAN

5

Uplink Port List

Max: 26

Total: 26

123

Port	Uplink
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐

ポート・トランク統計情報表示

RMON MIB をベースとした通信の詳細情報の他、Ethernet-like MIB やインタフェースグループからのネットワーク通信の標準的な統計情報の表示を行うことができます。

インタフェース及び Ethernet-like 統計情報は各ポートの通信エラー情報を表示します。これらの情報はポート不良や、重負荷などの問題点を明確にすることができます。

RMON 統計情報は各ポートのフレームタイプ毎の通信量を含む幅広い統計情報を提供します。すべての値はシステムが再起動された時からの累積数となり、毎秒単位 (per second) で表示されます。初期設定では統計情報は 60 秒ごとに更新されます。

[注意] RMONグループ2、3、9は、SNMP管理ソフトウェアを使用しないと利用できません。

パラメータ	解説
インタフェース統計	
Received Octets	フレーム文字を含むインタフェースで受信されたオクテットの数
Transmitted Octets	フレーム文字列を含むインタフェースから送信されたオクテットの数。
Received Errors	受信パケットで、上層位プロトコルへ届けることを妨げるエラーを含んでいたパケットの数。
Transmitted Errors	エラーにより送信されなかったアウトバウンドパケットの数
Received Unicast Packets	層位プロトコルで受信したサブネットワークユニキャストパケットの数
Transmitted Unicast Packet	上層位プロトコルがサブネットワークユニキャストアドレスに送信するよう要求したパケットの数。(削除されたパケット及び送信されなかったパケットを含む)
Received Discarded Packets	ラー以外の理由で削除された受信パケットの数。パケットが削除された理由は、バッファスペースを空けるためです
Transmitted Discarded Packets	エラー以外の理由で削除されたアウトバウンドパケットの数。パケットが削除された理由は、バッファスペースを空けるためです。
Received Multicast Packets	このサブレイヤから送信され、高層のレイヤで受信されたパケットで、このサブレイヤのマルチキャストアドレス宛てのパケットの数
Transmitted Multicast Packets	上層位プロトコルが要求したパケットで、このサブレイヤのマルチキャストアドレスに宛てられたパケットの数。(削除されたパケット及び送信されなかったパケットを含む)
Received Broadcast Packets	このサブレイヤから送信され、高層のレイヤで受信されたパケットで、このサブレイヤのブロードキャストアドレス宛てのパケットの数
Transmitted Broadcast Packets	上層位プロトコルが要求したパケットで、このサブレイヤのブロードキャストアドレスに宛てられたパケットの数。(削除されたパケット及び送信されなかったパケットを含む)
Received Unknown Packets	インタフェースから受信したパケットで、未知又は未対応プロトコルのために削除されたパケットの数。
Etherlike 統計	
Single Collision Frames	1つのコリジョンで転送が妨げられたフレームで、送信に成功したフレーム数
Multiple Collision Frames	2つ以上のコリジョンで転送が妨げられたフレームで、送信に成功したフレーム数
Late Collisions	512 ビットタイムより後にコリジョンが検出された回数

Excessive Collisions	特定のインタフェースでコリジョンの多発によりエラーを起こしたパケット数。full-duplex モードでは動作しません。
Deferred Transmissions	メディアが使用中のため、特定のインタフェース上で最初の送信試みが遅延したフレーム数
Frames Too Long	特定のインタフェースで受信したフレームで許容最大フレームサイズを超えたフレームの数
Alignment Errors	整合性エラー数 (同期ミスデータパケット)
FCS Errors	特定のインタフェースで受信したフレームで、完全なオクテットの長さで、FCS チェックにパスしなかったフレームの数。frame-too-long frame-too-short エラーと共に受信したフレームは除きます。
SQE Test Errors	特定のインタフェースの PLS サブレイヤで SQE TEST ERROR メッセージが生成された回数
Carrier Sense Errors	フレームを送信しようとした際、キャリアセンスの状況が失われたり、機能しなかった回数
Internal MAC Receive Errors	内部の MAC サブレイヤーエラーにより特定のインタフェースへの受信に失敗したフレーム数
Internal MAC Transmit Errors	内部の MAC サブレイヤーエラーにより特定のインタフェースへの送信に失敗したフレーム数
RMON 統計	
Drop Events	ソースの不足によりパケットがドロップした数
Jabbers	フレーミングビットを除き、FCS オクテットは含む)1518 オクテットより長いフレームで、FCS 又は配列エラーを含む受信フレーム数で
Fragments	フレーミングビットを除き、FCS オクテットは含む)64 オクテットよりも小さい長さで FCS もしくは配列エラーがあった受信フレーム数
Collisions	本 Ethernet セグメント上のコリジョンの総数の最良推定数
Received Octets	ネットワーク上で受信したデータのオクテットの合計数
Received Packets	受信したパケットの合計数 (不良、ブロードキャスト、マルチキャスト)
Broadcast Packets	受信した正常なパケットのうちブロードキャストアドレスに転送したパケット数。マルチキャストパケットは含まない。
Multicast packets	受信した正常なパケットのうち、このマルチキャストアドレスに転送したパケット数
Undersize Packets	フレーミングビットを除き、FCS オクテットは含む)64 オクテットより短い長さの受信パケット数で、その他の点では正常な受信パケット数
Oversize Packets	フレーミングビットを除き、FCS オクテットは含む)1518 オクテットよりも長い受信パケットで、その他の点では正常な受信パケット数
64 Bytes Packets	不良パケットを含む送受信トータルパケット数 (フレーミングビットを除き、FCS オクテットは含みます。)
65-127 Byte Packets 128-255 Byte Packets 256-511 Byte Packets 512-1023 Byte Packets 1024-1518 Byte Packets 1519-1536 Byte Packets	不良パケットを含む送受信トータルパケット数で、各オクテット数の範囲に含まれるもの (フレーミングビットを除き、FCS オクテットは含みます。)

設定方法

ポート統計の表示（テーブル）

- (1) [Interface] → [Port] → [Statistics] をクリックします。
- (2) 表示する統計モードを選択します。（Interface、Etherlike、RMON）
- (3) ドロップダウンリストからポートを選択します。
- (4) < Refresh > ボタンを使用して表示の更新が行えます。

Interface > Port > Statistics

Mode

☒ Interface ☐ Etherlike ☐ RMON

Port

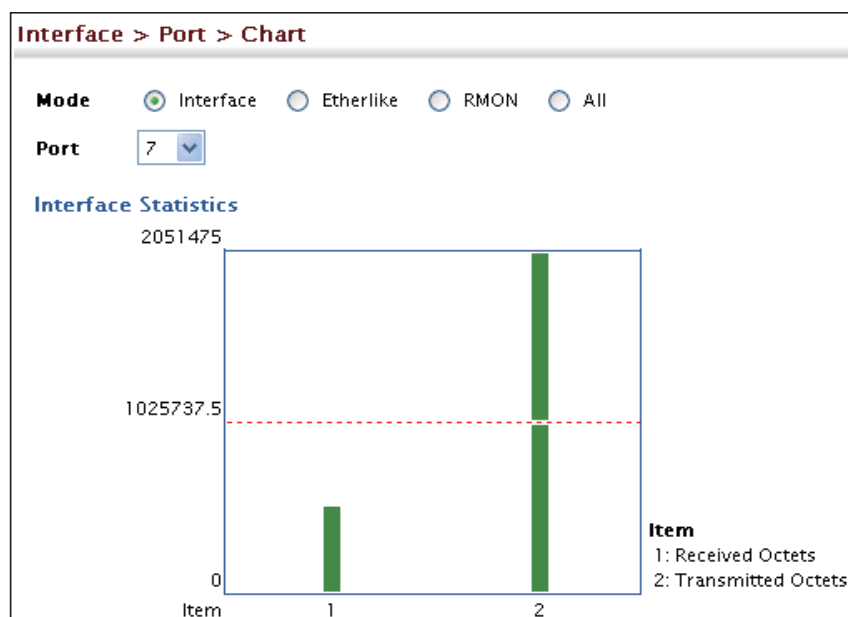
7

Interface Statistics

Received Octets	515372	Transmitted Octets	1993394
Received Errors	0	Transmitted Errors	0
Received Unicast Packets	3123	Transmitted Unicast Packets	3642
Received Discarded Packets	0	Transmitted Discarded Packets	0
Received Multicast Packets	2	Transmitted Multicast Packets	1355
Received Broadcast Packets	19	Transmitted Broadcast Packets	0
Received Unknown Packets	0		

ポート統計の表示（チャート）

- (1) [Interface] → [Port] → [Chart] をクリックします。
- (2) 表示する統計モードを選択します。（Interface、Etherlike、RMON、All）
- (3) Interface、Etherlike、RMON を選択した場合、ドロップダウンリストからポートを選択します。All 統計モードが選択されている際には表示する統計タイプを選択してください。



ケーブル診断の実行

Interface > Port > Cable Test ページを使用し、ポートに接続されているケーブルのテストを行います。ケーブルテストはケーブルの欠陥（ショート、オープン他）をチェックします。欠陥が見つかった際、スイッチは欠陥までのケーブル長もしくはケーブルの実長を報告します。これはケーブル、コネクタ、端子の品質を決定するために使用されます。オープン、ショート、ケーブルインピーダンス不整合のような問題は、このテストで診断をすることが可能です。

機能解説

- ケーブル診断は Time Domain Reflectometry（TDR）テストメソッドを使用して実行されます。TDR はパルス信号をケーブルに送り、このパルスのリフレクションを調べることでケーブルを分析します。
- 本テストは 7-140m のケーブルでのみ正確です。
- テストには約 5 秒がかかります。スイッチはすぐに、ステータス、欠陥までのおよそのケーブル長、ケーブル診断、通常のケーブル欠陥等の結果を表示します。
- 診断によってリストされる潜在的な状態
 - OK：正確に終端されるペア
 - Open：オープンペア、リンクパートナー無し
 - Short：ショートしたペア
 - Not Supported：1000Mbps 以下のスピードでリンクアップしている Fast Ethernet ポートまたは Gigabit Ethernet に表示されます。
 - Impedance mismatch：ターミネーティングインピーダンスがリファレンスレンジではありません。
- ケーブル診断の実行中、ポートはリンクダウンします。

設定・表示項目

Port

スイッチポート識別子

Type

メディアタイプを表示（FE-Fast Ethernet、GE-Gigabit Ethernet）

Link Status

ポートのリンクアップまたはリンクダウンを表示

Test Result

通常のケーブル欠陥、ステータス、欠陥までの距離またはおよそのケーブル長を表示

Last Updated

このポートで前回テストが行われた時を表示

設定方法

ケーブルテストの実行

- (1) [Interface] → [Port] → [Cable Test] をクリックします。
- (2) テストを行うポートの「Test」をクリックしてください。

Interface > Port > Cable Test						
Cable Test Port List Max: 26 Total: 26						
Port	Type	Link Status	Test Result (Cable/Fault Distance in Meters)		Last Updated	Action
			Pair A (meters)	Pair B (meters)		
1	FE	Up	Not Tested	Not Tested		Test
2	FE	Down	Not Tested	Not Tested		Test
3	FE	Down	Not Tested	Not Tested		Test
4	FE	Down	Not Tested	Not Tested		Test
5	FE	Down	Not Tested	Not Tested		Test

3.4.2 トランクグループの設定

ネットワーク接続におけるバンド幅の拡大によるボトルネックの解消や障害の回避のために複数のポートは束ねるトランク機能を利用することができます。最大 12 トランクを同時に設定することができます。

本機は、静的トランク及び動的な Link Aggregation Control Protocol (LACP) の両方をサポートしています。静的トランクでは、接続の両端において手動で設定する必要があり、また Cisco EtherChannel に準拠している必要があります。一方 LACP では LACP に設定したポートが、対向の LACP 設定ポートと連携し、自動的にトランクの設定を行ないます。静的トランクポートとして設定していない場合には、すべてのポートが LACP ポートに設定することができます。もし、8 つ以上のポートにより LACP トランクを形成している場合、8 つのポート以外はスタンバイモードとなります。トランクしている 1 つのポートに障害が発生した場合には、スタンバイモードのポートの 1 つが自動的に障害ポートと置き換わります。

機能解説

トランク内の各ポートで通信を分散すること及び、トランク内のポートで障害が発生した場合に他のポートを使用し通信を継続させる機能を提供します。

なお、設定を行なう場合には、デバイス間のケーブル接続を行なう前に両端のデバイスにおいてトランクの設定を行なって下さい。

トランクの設定を行なう場合には以下の点に注意して下さい：

- ループを回避するため、スイッチ間のネットワークケーブルを接続する前にポートトランクの設定を行なって下さい。
- 1 トランク最大 8 ポート、最大 12 トランクを作成することができます。
- 両端のデバイスのポートをトランクポートとして設定する必要があります。
- 異なる機器同士で静的トランクを行なう場合には、Cisco EtherChannel と互換性がなければなりません。
- トランクの両端のポートは通信速度、通信方式、及びフロー制御の通信モード、VLAN 設定、及び CoS 設定等に関して同じ設定を行なう必要があります。
- トランクの全てのポートは VLAN の移動、追加及び削除を行なう際に 1 つのインタフェースとして設定する必要があります。
- STP、VLAN 及び IGMP の設定はトランク全体への設定のみが可能です。

静的トランクの設定

Interface > Trunk > Static ページを使用し、トランクの作成、ポートメンバーの割り当て、接続パラメータの設定を行います。

機能解説

- ・ メーカー独自の機能の実装により、異なる機種間ではトランク接続ができない可能性があります。本機の静的トランクは Cisco EtherChannel に対応しています。
- ・ ネットワークのループを回避するため、ポート接続前静的トランクを設定し、静的トランクを解除する前にポートの切断を行なって下さい。

設定・表示項目

Trunk ID

トランク識別子（範囲：1-12）

Member

トランクの初期メンバー（Add Member ページを使用して追加メンバーを編集できます）

- － Unit － ユニット識別子（範囲：1）
- － Port － ポート識別子（範囲：1-26）

設定方法

静的トランクの作成

- (1) [Interface] → [Trunk] → [Static] をクリックします。
- (2) 「Step」 リストから「Configure Trunk」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) トランク識別子を入力します。
- (5) トランクの初期メンバーとなるポートの、ユニットおよびポート番号を設定します。
- (6) < Apply > をクリックします。

Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add

Trunk ID (1-12)

Member Unit 1 Port 5

Apply Revert

静的トランクメンバーを追加

- (1) [Interface] → [Trunk] → [Static] をクリックします。
- (2) 「Step」 リストから「Configure Trunk」を選択します。
- (3) 「Action」 リストから「Add Member」を選択します。
- (4) トランク識別子を選択します。
- (5) 追加するポートのユニットおよびポート番号を設定します。
- (6) < Apply > をクリックします。

Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add Member

Trunk 1

Member Unit 1 Port 2

Apply Revert

静的トランク接続パラメータの設定

- (1) [Interface] → [Trunk] → [Static] をクリックします。
- (2) 「Step」 リストから「Configure General」を選択します。
- (3) 「Action」 リストから「Configure」を選択します。
- (4) 必要な項目の設定を行い、< Apply > をクリックします。パラメータについての詳細は P48 「ポートリストによる設定」を参照してください。

Interface > Trunk > Static

Step: 2. Configure General Action: Configure

Static Trunk List Max: 12 Total: 1

Trunk	Type	Name	Admin	Media Type	Autonegotiation				Speed Duplex	Flow Control
1	100Base-TX		☒ Enabled	Copper-Forced	☒ 10h	☒ 100h	☐ 1000h	☐ Sym	100full	☐ Enabled
					☒ 10f	☒ 100f	☐ 1000f	☐ FC		

Apply Revert

スイッチの静的トランク設定情報を表示

- (1) [Interface] → [Trunk] → [Static] をクリックします。
- (2) 「Step」 リストから「Configure General」を選択します。
- (3) 「Action」 リストから「Show Interface」を選択します。

Interface > Trunk > Static

Step: 2. Configure General Action: Show Information

Static Trunk List Max: 12 Total: 1

Trunk	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	100Base-TX		Enabled	Down	Copper-Forced	Enabled	100full	None

動的トランク設定

Interface > Trunk > Dynamic (Configure Aggregator) ページを使用し、アグリゲーショングループの管理キーの設定、ポート上で LACP を有効、ローカルおよびパートナーポートのプロトコルパラメータの設定を行います。

機能解説

- ネットワークのループを回避するため、ポート接続前に LACP を有効にし、LACP を無効にする前にポートの切断を行って下さい。
- 対向のスイッチのポートが LACP を有効に設定している場合、トランクは自動的にアクティブになります。
- LACP により対向のスイッチと構成されたトランクには、自動的に次の番号のトランク ID が割り当てられます。
- 8 つ以上のポートにより LACP トランクを有効にした場合、8 つのポート以外はスタンバイモードとなります。トランクしている 1 つのポートに障害が発生した場合には、スタンバイモードのポートの 1 つが自動的に障害ポートと置き換わります。
- LACP トランクの両端のポートは固定又はオートネゴシエーションにより full duplex に設定する必要があります。

[注意] チャンネルグループが形成され、port channel admin key が設定されていない場合、このキーはグループに参加しているインタフェースのポートアドミンキーと同じ値に設定されます。

設定・表示項目

アグリゲータ設定

Admin Key

LACP 管理キーは、同じ LAG に属するポートと同じ値に設定する必要があります
(範囲：0-65535)

アグリゲーションポートの設定 - 通常

Port

ポート番号 (範囲：1-26)

LACP Status

ポートの LACP を有効 / 無効

アグリゲーションポートの設定 - Actor/Partner

Port

ポート番号 (範囲：1-26)

Admin Key

LACP 管理キーは、同じ LAG に属するポートと同じ値に設定する必要があります (範囲：0-65535、初期設定：1)

System Priority

LACP システムプライオリティは、リンク集合グループ (LAG) メンバーを決定し、且つ LAG 間での設定の際に、他のスイッチが本機を識別するために使用されます (範囲: 0-65535、初期設定: 32768)

- ー同じ LAG に参加するポートは同じシステムプライオリティを設定する必要があります。
- ーシステムプライオリティはスイッチの MAC アドレスと結合し、LAG の ID となります。
この ID は LACP が他のシステムとネゴシエーションをする際に特定の LAG を示す ID となります。

Port Priority

リンクが落ちた場合、LACP ポートプライオリティはバックアップリンクを選択するために使用されます (範囲: 0-65535、初期設定: 32768)

[注意] ポートの LACP 設定は、その管理ステータスへのみ適用され、機能ステータスへは適用されません。
また、次にポートとアグリゲートリンクが確立した時のみ効果を発します。

設定方法

動的トランクの Admin key を設定

- (1) [Interface] → [Trunk] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Aggregator」を選択します。
- (3) 必要とされる LACP グループに Admin key を設定します。
- (4) < Apply > をクリックします。

Interface > Trunk > Dynamic

Step: 1. Configure Aggregator

Trunk List Max: 12 Total: 12

Trunk	Admin Key (0-65535)
1	0
2	0
3	0
4	0
5	0

ポートで LACP を有効化

- (1) [Interface] → [Trunk] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Aggregation Port」を選択します。
- (3) 「Action」 リストから「Configure」を選択します。
- (4) 「General」 をクリックします。
- (5) 必要とされるポートで LACP を有効にします。
- (6) < Apply > をクリックします。

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Configure

☒ General ☐ Actor ☐ Partner

Port List Max: 26 Total: 26

Port	LACP Status
1	☐ Enabled
2	☒ Enabled
3	☐ Enabled
4	☐ Enabled
5	☐ Enabled

グループメンバーの LACP パラメータを設定

- (1) [Interface] → [Trunk] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Aggregation Port」を選択します。
- (3) 「Action」 リストから「Configure」を選択します。
- (4) 必要な項目の編集を行い、< Apply > をクリックします。

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Configure

☐ General ☒ Actor ☐ Partner

Port List Max: 26 Total: 26

Port	Admin Key (0-65535)	System Priority (0-65535)	Port Priority (0-65535)
1	3	32768	32768
2	1	32768	32768
3	1	32768	32768
4	1	32768	32768
5	1	32768	32768

動的トランクのアクティブメンバーを表示

- (1) [Interface] → [Trunk] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Trunk」を選択します。
- (3) 「Action」 リストから「Show」を選択します。
- (4) トランクを選択します。

Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Show Member

Trunk 1

Member List Max: 8 Total: 2

Member (Unit/Port)
1/1
1/2

動的トランクの接続パラメータを設定

- (1) [Interface] → [Trunk] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Trunk」を選択します。
- (3) 「Action」 リストから「Configure」を選択します。
- (4) 必要な項目の編集を行います。
- (5) < Apply > をクリックします。

Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Configure

Dynamic Trunk List Max: 32 Total: 1

Trunk	Type	Name	Admin	Media Type	Autonegotiation	Speed Duplex	Flow Control
2	100Base-TX		☒ Enabled	Copper-Forced	☒ 10h ☒ 100h ☐ 1000h ☒ 10f ☒ 100f ☐ 1000f	☒ Enabled 100full	☐ Enabled

Apply Revert

動的トランクの接続パラメータを表示

- (1) [Interface] → [Trunk] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Trunk」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Show

Dynamic Trunk List Max: 32 Total: 1

Trunk	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control
2	100Base-TX		Enabled	Up	Copper-Forced	Enabled	100full	None

LACP ポートカウンタの表示

LACP プロトコルメッセージの統計情報の表示を行ないます。

カウンタ情報

項目	解説
LACPDUs Sent	チャンネルグループから送信された有効な LACPDU の数
LACPDUs Received	チャンネルグループが受信した有効な LACPDU の数
Marker Sent	本チャンネルグループから送信された有効な Marker PDU の数
Marker Received	本チャンネルグループが受信した有効な Marker PDU の数
Marker Unknown Pkts	以下のフレームの受信数 (1) スロープロトコル・イーサネット・タイプ値を運び、未知の PDU を含んでいるフレーム (2) スロープロトコルグループ MAC アドレスに属し、スロープロトコル・イーサネット・タイプ値を運んでいないフレーム
Marker Illegal Pkts	不正な PDU 又はプロトコルサブタイプが不正な値を含むスロープロトコルイーサネットパケットを運ぶフレーム数

設定方法

- (1) [Interface] → [Trunk] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Aggregation Port」を選択します。
- (3) 「Action」 リストから「Show Information」を選択します。
- (4) 「Counters」をクリックします。
- (5) ポートリストからグループメンバーを選択します。

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

☒ Counters ☐ Internal ☐ Neighbors

Port 1

Trunk ID 2

Port Counters Information

LACPDUs Sent	29	LACPDUs Received	25
Marker Sent	0	Marker Receive	0
Marker Unknown Pkts	0	Marker Illegal Pkts	0

Refresh

ローカル側の LACP 設定及びステータスの表示

Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Internal) ページを使用し、LACP のローカル側の設定及びステータスの表示を行なうことができます。

内部設定情報

項目	解説
LACP System Priority	本ポートチャンネルグループに割り当てられた LACP システムプライオリティ
LACP Port Priority	本ポートチャンネルグループに割り当てられた LACP ポートプライオリティ
Admin Key	現在のアグリゲーションポートのキーの管理値
Oper Key	現在のアグリゲーションポートのキーの運用値
LACPDUs Interval	受信した LACPDU 情報を無効にするまでの秒数
Admin State, Oper State	Actor の管理値又は運用値の状態のパラメータ。 ♦ Expired — Actor の受信機器は失効状態です ♦ Defaulted — Actor の受信機器は初期設定の運用 partner の情報を使用しています ♦ Distributing — 誤りの場合、このリンク上の出力フレームの配信は無効になります。配信は現在無効状態で、受信プロトコル情報の管理上の変更、又は変更がない状態で有効にはなりません。 ♦ Collecting — このリンク上の入力フレームの収集は可能な状態です。収集は現在可能な状態で、受信プロトコル情報の管理上の変化、又は変化がない状態で無効にはなりません。 ♦ Synchronization — システムはリンクを IN_SYNC と認識します。それにより正しいリンクアグリゲーショングループに属することができます。グループは互換性のある Aggregator に関係します。リンクアグリゲーショングループの ID はシステム ID と送信されたオペレーショナルキー情報から形成されます。 ♦ Aggregation — システムは、アグリゲーション可能なリンクと認識しています。アグリゲーションの存在的な候補です。 ♦ Long timeout — LACPDU の周期的な送信にスロー転送レートを使用します。 ♦ LACP-Activity — 本リンクに関するアクティブコントロール値 (0 : Passive、1 : Active)

設定方法

- (1) [Interface] → [Trunk] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Aggregation Port」を選択します。
- (3) 「Action」 リストから「Show Information」を選択します。
- (4) 「Internal」 をクリックします。
- (5) ポートリストからグループメンバーを選択します。

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

☐ Counters ☒ Internal ☐ Neighbors

Port 1

Trunk ID 2

Port Internal Information

LACP System Priority	32768
LACP Port Priority	32768
Admin Key	3
Oper Key	3
LACPDUs Interval	30 sec
Admin State	Defaulted, Aggregation, Long timeout, LACP-activity
Oper State	Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

リモート側の LACP 設定及びステータスの表示

Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Neighbors) ページを使用し、LACP のリモート側の設定及びステータスの設定を行なうことができます。

LACP 内部設定情報

項目	解説
Partner Admin System ID	ユーザにより指定された LAG partner のシステム ID
Partner Oper System ID	LACP プロトコルにより指定された LAG partner のシステム ID
Partner Admin Port Number	プロトコル partner のポート番号の現在の管理値
Partner Oper Port Number	ポートのプロトコル partner によりアグリゲーションポートに指定された運用ポート番号
Port Admin Priority	プロトコル partner のポートプライオリティの現在の管理値
Port Oper Priority	partner により指定された本アグリゲーションポートのプライオリティ
Admin Key	プロトコル partner のキーの現在の管理値
Oper Key	プロトコル partner のキーの現在の運用値
Admin State	partner のパラメータの管理値（前の表を参照）
Oper State	partner のパラメータの運用値（前の表を参照）

設定方法

- (1) [Interface] → [Trunk] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Aggregation Port」を選択します。
- (3) 「Action」 リストから「Show Information」を選択します。
- (4) 「Partner」 をクリックします。
- (5) ポートリストからグループメンバーを選択します。

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

☐ Counters ☐ Internal ☒ Neighbors

Port 3

Trunk ID 2

Port Neighbors Information

Partner Admin System ID	32768, 00-00-00-00-00-00
Partner Oper System ID	32768, 00-12-CF-61-24-2F
Partner Admin Port Number	3
Partner Oper Port Number	3
Port Admin Priority	32768
Port Oper Priority	32768
Admin Key	0
Oper Key	3
Admin State	Defaulted, Distributing, Collecting, Synchronization, Long timeout
Oper State	Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

3.4.3 パワーセービング

Interface > Green Ethernet ページを使用し、選択されたポートのパワーセービングモードを有効にします。

機能解説

- IEEE802.3 は 100m で稼動しているケーブル接続に基づき、イーサネットスタンダードと続く電源条件を定義しています。パワーセービングモードの有効は 60m またはそれ以下の長さのケーブル使用時の電力を削減、20m またはそれ以下のケーブル使用時には更に削減し、信号保全性の保証は維持されます。
- リンクパートナーが無い状態でのパワーセービング
標準的なオペレーション下では、リンクパートナーを見つけるためスイッチは継続してオートネゴシエートを行い、接続が存在しない場合にも MAC インタフェースはパワーアップを維持し続けます。パワーセービングモードの使用時、スイッチはリンクパートナーの有無をサーキットのエネルギーをチェックすることで決定します。もし何も検出されない場合、スイッチは自動的に発信機と受信回路の大部分をオフにします。(スリープモードへ入ります)
このモードでは、ローパワーエネルギー検索回路はケーブル上のエネルギーをチェックし続けます。なにも検出されない場合、MAC インタフェースもまた余分なエネルギーを節約するためにパワーをダウンします。エネルギーが検出された場合、スイッチはただちに発信機と受信機能用法でターンオンされ、MAC インタフェースがパワーアップします。
- リンクパートナーが有る状態でのパワーセービング
従来のイーサネット接続は、一般に少なくとも 100m ケーブルの十分な電力をサポートして稼動しますが、ネットワークケーブルの長さの平均はそれより短いです。ケーブルが短い場合、信号減衰はケーブルの長さに比例するので、電力消費量を減少することが可能です。パワーセービングモードが有効の際、スイッチは特定のリンクに使用される信号出力レベルを減らすことが出来るか否か決定するために、ケーブルの長さを分析します。

[注意] パワーセービングはツイストペア配線使用時のギガビットイーサネットポートでのみ実行されます。アクティブリンクのパワーセービングモードは接続スピードが 1Gbps であり、ラインの長さが 60m 以下の場合にのみ動作します。

設定・表示項目

Port

パワーセービングモードは銅メディアを使用するギガビットイーサネットポートにのみ適用されます。

Power Saving Status

他のデバイスへの接続に使用されるケーブルの長さに基づき、ポートに提供される電力を調整します。(初期設定：ギガビット RJ-45 ポートで有効)

設定方法

- (1) [Interface] → [Green Ethernet] をクリックします。
- (2) 有効にするポートのチェックボックスをクリックします。
- (3) < Apply > をクリックします。

Interface > Green Ethernet

Port Green Ethernet List Max: 26 Total: 26 1 2 3

Port	Power Saving Status
21	☐ Enabled
22	☐ Enabled
23	☐ Enabled
24	☐ Enabled
25	☒ Enabled
26	☒ Enabled

3.4.4 トラフィックセグメンテーション

ローカルネットワークおよびサービスプロバイダへのアップリンクポート上で、異なるクライアントからダウンリンクポートを通過するトラフィックに、より厳しいセキュリティが必要とされる際、個々のクライアントセッションのトラフィックを隔離するためにポートベーストラフィックセグメンテーションを使用できます。

トラフィックセグメンテーションの有効化

Interface > Traffic Segmentation (Configure Global) ページを使用して、トラフィックセグメンテーションを有効にすることができます。

設定・表示項目

Status

ポートベーストラフィックセグメンテーションを有効にします（初期設定：無効）

設定方法

- (1) [Interface] → [Traffic Segmentation] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Enable」 チェックボックスにチェックを入れます。
- (4) < Apply > をクリックします。

Interface > Traffic Segmentation

Step: 1. Configure Global ▼

Status ☒ Enabled

Uplink-to-Uplink Blocking ▼

Apply Revert

アップリンク / ダウンリンクポートの設定

アップリンクポートをアサインします。ダウンリンクポートとして指定されたポートはアップリンクポートを除く、スイッチの他のポートとのコミュニケーションできません。アップリンクポートはその他のスイッチ上のポートおよび、ダウンリンクポートに指定されたポートとコミュニケーションが可能です。

設定・表示項目

Interface

ポートまたはトランクのリストを表示

Port

ポート識別子（範囲：1-26）

Trunk

トランク識別子（範囲：1-12）

Direction

インタフェースをアップリンクまたはダウンリンクに設定されたグループに追加

設定方法

- (1) [Interface] → [Traffic Segmentation] をクリックします。
- (2) 「Step」 リストから「Configure Session」を選択します。
- (3) ディレクションリストから、グループメンバーに追加するアップリンクまたはダウンリンクを選択します。
- (4) < Apply > をクリックします。

Interface > Traffic Segmentation

Step: 2. Configure Session

Interface ☒ Port ☐ Trunk

Port Configuration List Max: 10 Total: 10

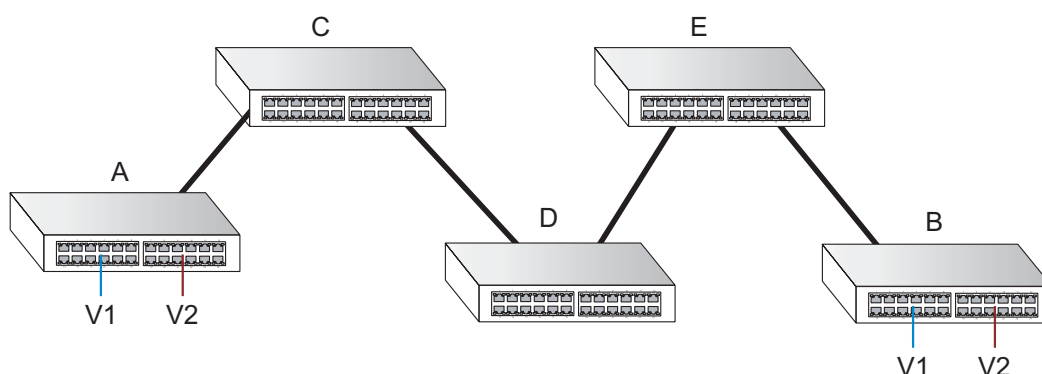
Port	Direction
1	None
2	None
3	None
4	None
5	None

3.4.5 VLAN トランキング

Interface > VLAN Trunking ページを使用し、未知の VLAN グループが指定されたインタフェースを通過することを許可します。

コマンド解説

- 本コマンドは、それらが属さない VLAN グループのトラフィックを渡す 1 つ以上の中間スイッチを横切るトンネルを設定します。
以下の図は VLAN1 と 2 をスイッチ A と B へ VLAN トランキングと共に設定し、スイッチ C,D および E を横断するこれらの VLAN グループがトラフィックを渡すために使用されます。 .



VLAN トランキングが無い場合、全ての中間スイッチへ VLAN1 と 2 を設定する必要があります。さもなければこれらのスイッチは未知の VLAN グループタグのついたフレームを破棄します。VLAN トランキングを有効にすれば、スイッチ A と B へのみ、これらの VLAN グループを作成するだけで中間スイッチポートは経路に沿って VLAN1 と VLAN2 の接続が行えます。

D と E は、VLAN グループタグ 1 と 2 が付いたフレームを自動的に許可し、VLAN トランキングポートを通過することが可能になります。

- VLAN トランキングは "access" スイッチポートモード（717 ページの「switchport mode」を参照）と相互に排他的です。もし VLAN トランキングがインタフェースで有効の場合、このインタフェースはアクセスモードには設定することが出来ません。その逆もまた同様です。
- スパニングツリー構成からのループを防ぐ為、全ての未知の VLAN は一つのインスタンス（STP/RSTP または MSTP インスタンス、選択された STA モードに依存）へバインドされます。
- ポートで、VLAN トランキングとイングレスフィルタリングの両方が無効の場合、未知のタグが付いたパケットはこのインタフェースへ入ることを許可され、VLAN トランキングが有効であるその他全てのポートへフラッドされます。（VLAN トランキングの効果は未知の VLAN で依然有効です。）

設定・表示項目

Interface

ポートまたはトランクのリストを表示

Port

ポート識別子（範囲：25-26）

[注意] VLAN トランキングはギガビットポートでのみ有効に出来ます。

Trunk

トランク識別子（範囲：1-12）

VLAN Trunking Status

選択されたインタフェースで VLAN トランキングを有効化

設定方法

- (1) [Interface] → [VLAN Trunking] をクリックします。
- (2) ポートまたはトランクをクリックし、インタフェースタイプを指定します。
- (3) ギガビットポートまたはギガビットポートを含むトランクの VLAN トランキングを有効にします。
- (4) < Apply > をクリックします。

Interface > VLAN Trunking

Interface ☒ Port ☐ Trunk

Port VLAN Trunking List Max: 26 Total: 26 1 2 3

Port	VLAN Trunking Status
21	☐ Enabled
22	☐ Enabled
23	☐ Enabled
24	☐ Enabled
25	☒ Enabled
26	☐ Enabled

3.5 VLAN

3.5.1 IEEE802.1Q VLAN

大規模なネットワークでは、ブロードキャストトラフィックを分散させるためにルータにより各サブネットを異なるドメインに分割します。本機では同様のサービスをレイヤ 2 の VLAN 機能によりブロードキャストドメインを分割させたネットワークのグループを作成させることができます。VLAN は各グループでブロードキャストトラフィックを制限し、大規模ネットワークにおけるブロードキャストストームを回避します。

また、VLAN により安全で快適なネットワーク環境の構築も行なうことができます。

IEEE 802.1Q VLAN は、ネットワーク上どこにでも配置することができ、物理的に離れていても同じ物理的なセグメントに属するように通信を行うことができます。

VLAN は物理的な接続を変更することなく新しい VLAN ヘドバイスを追加することによりネットワーク管理を簡単に行うことができます。VLAN はマーケティング、R&D 等の部門別のグループ、e-mail やマルチメディアアプリケーションなどの使用方法ごとにグループ分けを行うことができます。

VLAN はブロードキャスト通信を軽減することにより巨大なネットワーク能力効率を実現し、IP アドレス又は IP サブネットを変更することなくネットワーク構成の変更を可能にします。VLAN は本質的に異なる VLAN への通信に、設定されたレイヤ 3 による転送が必要となるため、高水準のネットワークセキュリティを提供します。

本機では以下の VLAN 機能をサポートしています。

- IEEE802.1Q 準拠の最大 255VLAN グループ
- GVRP プロトコルを利用した、複数のスイッチ間での動的な VLAN ネットワーク構築
- 複数の VLAN に参加できるオーバーラップポートの設定が可能なマルチプル VLAN
- エンドステーションは複数の VLAN へ所属可能
- VLAN 対応と VLAN 非対応デバイス間での通信が可能
- プライオリティタギング

VLAN ヘポートの割り当て

VLAN を有効にする前に、各ポートを参加する VLAN グループに割り当てる必要があります。初期設定では全てのポートが VLAN 1 にタグなしポートとして割り当てられています。1 つ又は複数の VLAN で通信を行う場合や、VLAN に対応したネットワーク機器、ホストと通信を行う場合には、タグ付ポートとして設定を行います。その後、手動又は GVRP による動的な設定により、同じ VLAN 上で通信が行われる他の VLAN 対応デバイス上でポートを割り当てます。

しかし、1 つ又は複数の VLAN にポートが参加する際に、対向のネットワーク機器、ホストが VLAN に対応していない場合には、このポートをタグなしポートとして設定を行う必要があります。

[注意] タグ付 VLAN フレームは VLAN 対応及び VLAN 非対応のネットワーク機器を通ることができますが、VLAN タグに対応していない終端デバイスに到達する前にタグを外す必要があります。

VLAN の分類 — フレームを受信した際、スイッチは 2 種類のうち 1 種類のフレームとして認識します。タグなしフレームの場合、受信したポートの PVID に基づいた VLAN にフレームを割り当てます。タグ付フレームの場合、VLAN ID タグを使用してフレームのポートブロードキャストドメインを割り当てます。

ポートのオーバーラップ — ポートのオーバーラップは、ファイルサーバ又はプリンタのように異なった VLAN グループ間で共有されるネットワークリソースへのアクセスを許可するために使用します。

オーバーラップを行わない VLAN を設定し、VLAN 間での通信を行う必要がある場合にはレイヤ 3 ルータ又はスイッチを使用することにより通信が行えます。

タグなし VLAN — タグなし又は静的 VLAN はブロードキャストトラフィックの軽減及びセキュリティのため、使用されます。

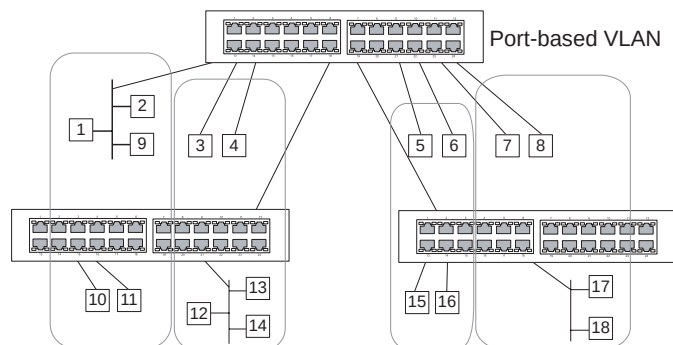
VLAN に割り当てられたユーザグループが、他の VLAN と分けられたブロードキャストドメインとなります。パケットは同じ VLAN 内の指定されたポート間でのみ送信されます。タグなし VLAN は手動でのユーザグループ又はサブネットの分割が行えます。また、GVRP を使用した IEEE802.3 タグ VLAN により、完全に自動化した VLAN 登録を行うことも可能となります。

自動 VLAN 登録 — GVRP (GARP VLAN Registration Protocol) は各終端装置が VLAN を割り当てられる必要がある場合に、VLAN を自動的に学習し設定を行います。終端装置 (又はそのネットワークアダプタ) が IEEE802.1Q VLAN プロトコルに対応している場合、参加したい VLAN グループを提示するメッセージをネットワークに送信するための設定を行うことができます。本機がこれらのメッセージを受信した際、指定された VLAN の受信ポートへ自動的に追加し、メッセージを他の全てのポートへ転送します。

メッセージが他の GVRP 対応のスイッチに届いたときにも、同様に指定された VLAN の受信ポートへ追加され、他の全てのポートへメッセージが送られます。VLAN の要求はネットワークを通じて送られます。GVRP 対応デバイスは、終端装置の要求に基づき自動的に VLAN グループの構成を行うことが可能となります。

ネットワークで GVRP を使用するために、最初に要求された VLAN へ (OS 又はアプリケーションを使用して) ホストデバイスを追加します。その後、この VLAN 情報がネットワーク上へ伝達されます。ホストに直接接続されたエッジスイッチおよびネットワークのコアスイッチにおいて GVRP を有効にします。また、ネットワークのセキュリティ境界線を決め、通知の伝送を防ぐためポートの GVRP を無効にするか、ポートの VLAN への参加を禁止する必要があります。

[注意] GVRP に対応していないホストデバイスでは、デバイスへ接続するポートで静的 VLAN を設定する必要があります。また、コアスイッチとエッジスイッチにおいて GVRP を有効にする必要があります。



タグ付き・タグなしフレームの送信— 1 台のスイッチでポートベースの VLAN を構成する場合、同じタグなし VLAN にポートを割り当てることで構成できます。しかし、複数のスイッチ間での VLAN グループに参加するためには、全てのポートをタグ付ポートとする VLAN を作成する必要があります。

各ポートは複数のタグ付又はタグなし VLAN に割り当てることができます。また、各ポートはタグ付及びタグなしフレームを通過させることができます。

VLAN 対応機器に送られるフレームは、VLAN タグを付けて送信されます。VLAN 未対応機器（目的ホストを含む）に送られるフレームは、送信前にタグを取り除かなければなりません。タグ付フレームを受信した場合は、このフレームをフレームタグにより指示された VLAN へ送ります。VLAN 非対応機器からタグなしフレームを受信した場合は、フレームの転送先を決め、進入ポートのデフォルト VID を表示する VLAN タグを挿入します。

VLAN グループの設定

VLAN > Static (Add) ページを使用し、VLAN の作成と削除を行います。

設定・表示項目

Add

VLAN ID

VLAN ID または VLAN 範囲 (1-4093)

最大 255VLAN グループを定義できます。VLAN1 はデフォルトタグ無し VLAN になります。

Status

指定した VLAN を有効 / 無効にします。

Remote VLAN

この VLAN を RSPAN 用に確保します。(詳細は P54 「リモートポートミラーリングの設定」を参照してください)

Modify

VLAN ID

設定された VLAN ID (1-4093)

VLAN Name

VLAN 名 (1-32 文字)

Status

指定した VLAN を有効 / 無効にします。

show

VLAN ID

設定された VLAN ID

VLAN Name

VLAN 名

Status

設定された VLAN のステータス

Remote VLAN

この VLAN で RSPAN が有効時に表示 (詳細は P54 「リモートポートミラーリングの設定」を参照してください)

設定方法

VLAN の作成

- (1) [VLAN] → [Static] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) VLAN ID または ID の範囲を入力します。
- (4) "Enable" にチェックを入れ VLAN を動作させます。
- (5) < Apply > をクリックします。

VLAN > Static

Action: Add

VLAN ID (1 - 4093) 2 -

Status ☒ Enabled

Remote VLAN ☐ Enabled

Apply Revert

VLAN の編集

- (1) [VLAN] → [Static] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) 設定された VLAN の ID を選択します。
- (4) 必要に応じ、VLAN 名、ステータス等の編集を行います。
- (5) < Apply > をクリックします。

VLAN > Static

Action: Modify

VLAN ID (1 - 4093) 1

VLAN Name DefaultVlan

Status ☒ Enabled

Apply Revert

VLAN 設定の表示

- (1) [VLAN] → [Static] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

VLAN > Static

Action: Show

Static VLAN List Max: 26 Total: 3

☐	VLAN ID	VLAN Name	Status	Remote VLAN
☐	1	DefaultVlan	Enabled	Disabled
☐	2		Enabled	Disabled
☐	4093		Enabled	Disabled

Delete Revert

VLAN への静的メンバーの追加

VLAN > Static ページを使用し、選択した VLAN のポートメンバーの設定を行ないます。

IEEE802.1Q VLAN 準拠の機器と接続する場合にはポートはタグ付として設定し、VLAN 非対応機器と接続する場合にはタグなしとして設定します。また、GVRP による自動 VLAN 登録から回避するためポートの設定を行ないます。

設定・表示項目

VLAN によるメンバー編集

VLAN

設定された VLAN ID (1-4093)

Interface

ポートまたはトランクのリストを表示

Port

ポート識別子 (範囲: 1-26)

Trunk

トランク識別子 (範囲: 1-12)

Mode

ポートの VLAN メンバーシップモードを表示します: (初期設定: Hybrid)

- Access — ポートをタグ無しインタフェースとして動作するように設定します。全てのフレームはタグ無しになります。
- Hybrid — ハイブリッド VLAN インタフェースを指定します。ポートはタグ付又はタグなしフレームを送受信します。
- 1Q Trunk — VLAN トランクの終端となっているポートを指定します。トランクは 2 台のスイッチの直接接続となり、ポートは発信元 VLAN のタグ付フレームを送信します。しかし、ポートのデフォルト VLAN に属したフレームはタグなしフレームが送信されます。

PVID

タグなしフレームを受信した際に付ける VLAN ID (初期設定: 1)

インタフェースが VLAN 1 のメンバーでない場合に、この VLAN へ PVID "1" を割り当てた場合、インタフェースは自動的にタグなしメンバーとして VLAN 1 に参加します。その他の VLAN に関しては、まず「Static table」(85 ページの「VLAN への静的メンバーの追加」を参照) にて、各 VLAN に所属しているポートごとに Tag 付き、Tag なしの設定を行う必要があります。

Acceptable Frame Type

全てのフレーム又はタグ付フレームのみのどちらか受け入れ可能なフレームの種類を設定します。全てのフレームを選択した場合には、受信したタグなしフレームはデフォルト VLAN に割り当てられます。(選択肢: 全て又はタグ付き、初期設定: 全て (all))

Ingress Filtering

入力ポートがメンバーでない VLAN のタグ付フレームを受信した場合の処理を設定します (初期設定: 有効 (Enabled))

- イングレスフィルタリングはタグ付フレームでのみ機能します。
- イングレスフィルタリングが有効で、ポートがメンバーでない VLAN のタグ付フレームを受信した場合、受信フレームを破棄します。
- イングレスフィルタリングは GVRP 又は STP 等の VLAN と関連しない BPDU フレームに機能しません。しかし、GMRP のような VLAN に関連する BPDU フレームには機能します。

Membership Type

ラジオボタンをマークすることにより、各インタフェースへの VLAN メンバーシップを選択します。

- **Tagged** — インタフェースは VLAN のメンバーとなります。ポートから送信される全てのパケットにタグがつけられます。タグにより VLAN 及び CoS 情報が運ばれます。
- **Untagged** — インタフェースは VLAN のメンバーとなります。ポートから転送された全てのパケットからタグがはずされます。タグによる VLAN 及び CoS 情報は運ばれません。各インタフェースはタグなしポートとして最低 1 つのグループに割り当てなければいけません。
- **Forbidden** — GVRP を使用した VLAN への自動的な参加を禁止します。詳細は P80 を参照して下さい。
- **None** — インタフェースは VLAN のメンバーではありません。この VLAN に関連したパケットは、インタフェースから送信されません。

[注意] VLAN1 はアクセスモードを使用するスイッチ上の全てのポートを含む、デフォルトタグ無し VLAN です。

インタフェースによるメンバ編集

全てのパラメータは、前の項「VLAN によるメンバー編集」で解説されている内容と同じです。

インタフェース範囲によるメンバ編集

以下の 2 項目以外の全てのパラメータは、前の項「VLAN によるメンバー編集」で解説されている内容と同じです。

- ◆ Port Range — ポートのリストを表示（範囲：1-26）
- ◆ Trunk Range . ポートのリストを表示（範囲：1-12）

設定方法

VLAN インデックスで静的メンバーを設定

- (1) [VLAN] → [Static] をクリックします。
- (2) 「Action」 リストから「Edit Member by VLAN」を選択します。
- (3) ポートまたはトランクとして表示するインタフェースタイプを設定します。
- (4) その他必要な項目の設定を行い、< Apply >をクリックします。

VLAN > Static

Action: Edit Member by VLAN

VLAN: 1

Interface: ☒ Port ☐ Trunk

Static VLAN Port Member List Max: 26 Total: 26 1 2 3

Port	Mode	PVID	Acceptable Frame Type	Ingress Filtering	Membership Type			
					Tagged	Untagged	Forbidden	None
1	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐
2	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐
3	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐
4	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐
5	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐

インタフェースで静的メンバーを設定

- (1) [VLAN] → [Static] をクリックします。
- (2) 「Action」 リストから「Edit Member by Interface」を選択します。
- (3) ポートまたはトランク設定を選択します。
- (4) その他必要な項目の設定を行い、< Apply >をクリックします。

VLAN > Static

Action: Edit Member by Interface

Interface: ☒ Port 1 ☐ Trunk

Mode: Access

PVID: 1

Acceptable Frame Type: All

Ingress Filtering: ☐ Enabled

Static VLAN Membership List Max: 26 Total: 3

VLAN	Membership Type			
	Tagged	Untagged	Forbidden	None
1	☐	☒	☐	☐
2	☐	☐	☐	☒
4093	☐	☐	☐	☒

Apply Revert

インタフェースの範囲で静的メンバーを設定

- (1) [VLAN] → [Static] をクリックします。
- (2) 「Action」 リストから「Edit Member by Interface Range」を選択します。
- (3) ポートまたはトランク設定を選択します。
- (4) その他必要な項目の設定を行い、< Apply >をクリックします。

VLAN > Static

Action: Edit Member by Interface Range ▼

Interface

☒ Port ☐ Trunk

Port Range (1-10)

8 - 10

Mode

Hybrid ▼

VLAN ID (1-4093)

2 -

Membership Type

☐ Tagged ☒ Untagged ☐ Forbidden ☐ None

Apply

Revert

動的 VLAN 登録の設定

VLAN > Dynamic ページを使用して、GVRP をスイッチのグローバルで有効にします。また、インタフェース毎での GVRP の有効、プロトコルタイマーの調整も行えます。

設定・表示項目

一般設定

GVRP Status

GVRP はネットワーク全体のポートの登録 VLAN メンバーのために、VLAN 情報を交換する方法を定義します。VLAN は、ホストデバイスから発行されネットワーク全体に伝えられる join メッセージを基に、動的に設定されます。(初期設定：無効)

インタフェース設定

Interface

ポートまたはトランクのリストを表示

Port

ポート識別子 (範囲：1-26)

Trunk

トランク識別子 (範囲：1-12)

GVRP Status

インタフェース GVRP を有効又は無効にします。GVRP はこの設定が実施される前にスイッチを全体的に有効にする必要があります (26 ページの「ブリッジ拡張機能の表示」を参照して下さい)。無効な時、このポートで受信された GVRP パケットは放棄されどの GVRP 登録も他のポートから伝搬されなくなります (初期設定：無効)

GVRP Timers

タイマー設定は以下のルールに従ってください。

$2 \times (\text{join timer}) < \text{leave timer} < \text{leaveAll timer}$

- Join – VLAN グループに参加するために送信される要求またはクエリの送信間隔 (範囲：20-1000 センチセカンド、初期設定：20)
- Leave – VLAN グループを外れる前にポートが待機する間隔。この時間は Join Timer の 2 倍以上の時間を設定する必要があります。これにより、Leave 又は LeaveAll メッセージが発行された後、ポートが実際にグループを外れる前に再び VLAN に参加できます (範囲：60-3000 センチセカンド、初期設定：60)
- Leave All – VLAN グループ参加者への LeaveAll クエリメッセージの送信からポートがグループを外れるまでの間隔。この間隔はノードが再び参加することによるトラフィックの発生量を最小限にするための Leave Timer よりも大幅に大きい値を設定する必要があります (範囲：500-18000 センチセカンド、初期設定：1000)

動的 VLAN の表示 – Show VLAN

VLAN ID

GVRP を通して加入した VLAN の識別子。

VLAN Name

GVRP を通して加入した VLAN の名前。

Status

この VLAN が現在稼動中か否かを示します。(Enable/Disable)

動的 VLAN の表示 – Show VLAN Member

VLAN

GVRP を通して加入した VLAN の識別子。

Interface

ポートまたはトランクのリスト。

設定方法

スイッチの GVRP を設定

- (1) [VLAN] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure General」を選択します。
- (3) GVRP を有効 / 無効に設定します。
- (4) < Apply > をクリックします。

VLAN > Dynamic

Step: 1. Configure General

GVRP Status

☒

Enabled

Apply
Revert

ポートまたはトランクの GVRP ステータスとタイマーの設定

- (1) [VLAN] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) ポートまたはトランクとして表示するインタフェースタイプを指定します。
- (4) いずれかのインタフェースの GVRP ステータスまたはタイマを編集します。
- (5) < Apply > をクリックします。

VLAN > Dynamic

Step: 2. Configure Interface

Interface ☒ Port ☐ Trunk

Port List Max: 26 Total: 26

Port	GVRP Status	GARP Timer (centiseconds)		
		Join (20-1000)	Leave (60-3000)	LeaveAll (500-18000)
1	☐ Enabled	20	60	1000
2	☐ Enabled	20	60	1000
3	☒ Enabled	20	60	1000
4	☐ Enabled	20	60	1000
5	☐ Enabled	20	60	1000

動的 VLAN の表示

- (1) [VLAN] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Show Dynamic VLAN」を選択します。
- (3) 「Action」 リストから「Show VLAN」を選択します。

VLAN > Dynamic

Step: 3. Show Dynamic VLAN Action: Show VLAN

Dynamic VLAN List Max: 256 Total: 2

VLAN ID	VLAN Name	Status
120		Enabled
150		Enabled

動的 VLAN のメンバーを表示

- (1) [VLAN] → [Dynamic] をクリックします。
- (2) 「Step」 リストから「Show Dynamic VLAN」を選択します。
- (3) 「Action」 リストから「Show VLAN Members」を選択します。

VLAN > Dynamic

Step: 3. Show Dynamic VLAN Action: Show VLAN Member

VLAN 120

Dynamic VLAN Member List Max: 64 Total: 10

Interface
Unit 1 / Port 1
Unit 1 / Port 4
Unit 1 / Port 10
Unit 1 / Port 16
Unit 1 / Port 19

3.5.2 802.1Q トンネリングの設定

IEEE802.1Q トンネリング (QinQ) は、ネットワークで複数のカスタマーのトラフィックを送信するサービスプロバイダを対象に設計された機能です。サービスプロバイダは、他のカスタマーのトラフィックに影響を与えずに、各カスタマーの VLAN およびレイヤ 2 プロトコル設定を維持する必要があります。QinQ トンネリングは、それらがサービスプロバイダのネットワークに入る時にサービスプロバイダ VLAN (SPVLAN) タグをカスタマーのフレームに挿入し、フレームがネットワークを去る時タグを取り去ることで実現します。

多くの場合、サービスプロバイダのカスタマーには、VLAN ID と、サポートの対象となる VLAN 数についての特定の要件があります。

同じサービスプロバイダネットワーク内の様々なカスタマーが必要とする VLAN の範囲は重複する場合があります。インフラストラクチャを介したカスタマーのトラフィックが混在する場合もあります。各カスタマーに、固有の範囲の VLAN ID を割り当てると、カスタマーの設定を制限することになり、IEEE802.1Q 仕様の 4096 という VLAN の制限を容易に超える可能性があります。

IEEE802.1Q トンネリング機能を使用することにより、サービスプロバイダは複数の VLAN を設定しているカスタマーを、1 つの VLAN を使用してサポートできます。カスタマーの VID は保持されるため、様々なカスタマーからのトラフィックは、同じ VLAN 内に存在するように見える場合でも、サービスプロバイダのインフラストラクチャ内では分離されています。

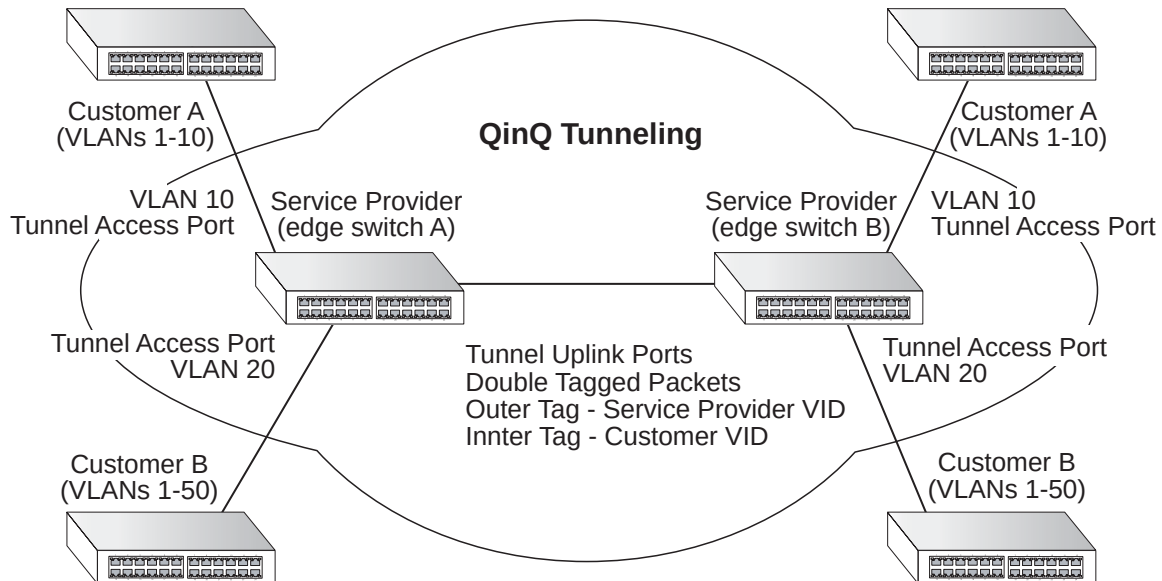
IEEE802.1Q トンネリングでは、VLAN 内 VLAN 階層を使用して、タグ付きパケットに再度タグ付けを行うことによって、VLAN スペースを拡張します。

ポートに QinQ トンネリングをサポートさせるには、トンネルポートモードに設定する必要があります。特定のカスタマーのサービスプロバイダ VLAN (SPVLAN) ID は、カスタマーのトラフィックがサービスプロバイダのネットワークへ入るエッジスイッチの QinQ トンネルアクセスポートにアサインします。それぞれのカスタマーは別々の SPVLAN を必要としますが、VLAN は全てのカスタマーの内部 VLAN をサポートします。

エッジスイッチからサービスプロバイダのメトロネットワークへトラフィックを渡す QinQ トンネリングアップリンクポートは、同じくこの SPVLAN へ加えられなくてはなりません。アップリンクポートは、インバウンドトラフィックをサービスプロバイダネットワークへの異なるカスタマに運ぶ為に、複数の VLAN へ付加されることが可能です。

二重タグ付き (ダブルタギング) パケットが、サービスプロバイダの本機にある別のトランクポートに入ると、スイッチ内でパケットが処理される時に、外側のタグが外されます。同じコアスイッチの別のトランクポートからパケットが送出される時には、同じ SPVLAN タグがパケットに再度追加されます。

パケットがサービスプロバイダ出力スイッチのトランクポートに入ると、スイッチでパケットが内部処理される時に、外側のタグが再度除去されます。ただし、パケットがエッジスイッチのトンネルポートからカスタマーネットワークに送信される時には、SPVLAN タグは追加されません。カスタマーネットワーク内の元の VLAN 番号を保持するために、パケットは通常の IEEE802.1Q タグ付きフレームとして送信されます。



トンネルアクセスポートへ入るパケットのレイヤ 2 フロー

QinQ トンネルポートはタグ付きまたはタグ無しパケットのいずれかを受信します。入力パケットがいくつかのタグを持つかには関わらず、タグ付きポートとして扱われます。入力プロセスはソースとディスティネーションを検索します。両方の検索が成功したら、入力プロセスはパケットをメモリへ書き込み、出力プロセスへパケットを伝えます。

QinQ トンネルポートへ入ったパケットは以下の方法で処理されます。

- (1) 既にいくつかのタグを保持しているかに関わらず、新しい SPVLAN タグは全ての入力パケットに付加されます。
この入力プロセスは外のタグ (SPVLAN) を組み立て、デフォルト VLAN ID とタグ識別子に基づき挿入します。
この外側のタグはパケットの学習とスイッチングに使用されます。もしこれがタグ付きまたはプライオリティタグ付きパケットである場合、内側のタグのプライオリティは外側のタグにコピーされます。
- (2) ソース、ディスティネーション検索が成功した後、入力プロセスは、2 つのタグと共にスイッチングプロセスへパケットを送ります。
もし入力パケットがタグ無しの場合、外側のタグは SPVLAN タグとなり、内側のタグはダミーとなります。(8100 0000)
もし入力パケットがタグ付きである場合、外側のタグは SPVLAN タグになり、内側のタグは CVLAN タグとなります。
- (3) スwitchングプロセスを通るパケット分類の後、パケットは 1 つのタグ (外側のタグ) または 2 つのタグと共にメモリへ書き込まれます。
- (4) スイッチはパケットを適切な出力ポートへ送ります。
- (5) もし出力ポートが SPVLAN のタグ無しメンバーである場合、外側のタグは取り外されます。タグ付きメンバーである場合、発信パケットは 2 つのタグを持ちます。

トンネルアップリンクポートへ入るパケットのレイヤ 2 フロー

アップリンクポートは以下のパケットの 1 つを受け取ります。

- タグ無し
- 1 つのタグ付き (CVLAN または SPVLAN)
- 2 つのタグ付き (CVLAN+SPVLAN)

入力プロセスはソースとディスティネーションを検索します。

両方の検索が成功したら、入力プロセスはパケットをメモリへ書き込み、出力プロセスへパケットを伝えます。

QinQ アップリンクポートへ入ったパケットは以下の方法で処理されます。

- (1) 入力パケットがタグ無しである場合、PVID VLAN ネイティブタグが付加されます。
- (2) 入力パケット (1 つまたは 2 つのタグ付き) イーサタイプがアップリンクポートの TPID と一致しない場合、VLAN タグはカスタマ VLAN (CVLAN) タグであると決定されます。アップリンクポートの PVID VLAN ネイティブタグがパケットに付加されます。
この外側のタグは、サービスプロバイダネットワークで、パケットの学習とスイッチングに使われます。TPID はポートベースで設定され、検証は無効にすることができません。
- (3) 入力パケット (1 つまたは 2 つのタグ付き) のイーサタイプがアップリンクポートの TPID と一致する場合、新しい VLAN タグは付加されません。
アップリンクポートが入ってきたパケットの外側の VLAN のメンバーでない場合、インgress フィルタリング有効時であればパケットは破棄されます。
インgress フィルタリングが有効でない場合、パケットはフォワードされます。
VLAN が VLAN テーブル上に無い場合、パケットは破棄されます。
- (4) ソース、ディスティネーション探索に成功後、パケットは 2 つのタグが付けられます。スイッチは、0x8100 の TPID を、入力パケットに二重のタグが付けられていることを示す為に使用します。
二重タグ付き入力パケットの外側のタグがポートの TPID と一致し、内側のタグが 0x8100 である場合、これは二重タグ付きパケットとして取り扱われます。
シングルタグ付きパケットが、TPID として 0x8100 を持ち、ポート TPID が 0x8100 ではない場合、新しい VLAN タグが付加され、これもまた二重タグ付きパケットとして取り扱われます。
- (5) ディスティネーション検索が失敗した場合、パケットは、外タグの VLAN の全てのメンバーポートへ送信されます。
- (6) パケット分類の後、パケットは、シングルタグ付きまたは二重タグ付きパケットとして処理されるために、メモリへ書き込まれます。
- (7) スイッチはパケットを適切な出力ポートへ送信します。
- (8) 出力ポートが SPVLAN のタグ無しメンバーである場合、外側のタグは取り外されます。タグ付きメンバーである場合、出て行くパケットは 2 つのタグを持ちます。

QinQ の設定制限

- アップリンクポートのネイティブ VLAN は SPVLAN としては使用できません。
SPVLAN がアップリンクポートのネイティブ VLAN である場合、アップリンクポートは SPVLAN のタグ無しメンバーになります。パケットが送信される時、外側の SPVLAN タグは取り外されます。
- QinQ 設定がトランクポートグループと整合性がある限り、静的トランクポートグループは、QinQ トンネルポートと両立できます。
- ネイティブ VLAN (VLAN1) は通常、転送されたフレームに付加されません。
設定不良の危険を減少する為、カスタマトラフィックの SPVLAN タグを VLAN1 にするのは避けてください。サービスプロバイダネットワークのデータ VLAN の代わりに、VLAN 1 を管理 VLAN として使用してください。
- レイヤ 2 とレイヤ 3 スイッチングには若干の固有互換性があります。
 - ー トンネルポートは IP アドレスコントロールリストをサポートしません。
 - ー レイヤ 3 Quality of Service (QoS) ACL とレイヤ 3 情報に関連するその他の QoS 機能はトンネルポートでサポートされません。
 - ー ポートが IEEE802.1Q トランクポートとして設定されている場合、スパンニングツリーの BPDU フィルタリングは、インタフェースで自動的に無効となります。

QinQ の一般的な設定ガイドライン

- (1) トンネルステータスを有効にし、トンネルアクセスポートの Tag Protocol Identifier (TPID) 値を設定します。このステップは接続されているクライアントが 802.1Q タグ付きフレームの識別に、非標準 2 バイトイーサタイプを使用している場合に必要となります。デフォルトイーサタイプ値は 0x8100 です。(P96 を参照)
- (2) SPVLAN として定義されたカスタマサービスプロバイダ VLAN を作成します。(P83 を参照)
- (3) QinQ トンネルアクセスポートを 802.1Q トンネルモードに設定します。(P97 を参照)
- (4) QinQ トンネルアクセスポートをタグ無しとして SPVLAN に加入させます (P85 を参照)
- (5) QinQ トンネルアクセスポートに SPVLAN ID をネイティブ VID として設定します。(P85 を参照)
- (6) QinQ トンネルアップリンクポートを 802.1Q トンネルアップリンクモードに設定します。(P97 を参照)
- (7) QinQ トンネルアップリンクポートをタグ付きメンバーとして SPVLAN に加入させます。(P85 を参照)

QinQ トンネリングの有効

スイッチは通常の VLAN か、サービスプロバイダのメトロポリタンエリアネットワーク上のレイヤ 2 トラフィックを通過させるために IEEE802.1Q (QinQ) トンネリングで動作するように構成することができます。

設定・表示項目

Tunnel Status

スイッチを QinQ モードに設定します。

802.1Q Ethernet Type

タグプロトコル識別子 (TPID) (範囲 ; 16 進 0800-FFFF 初期設定 : 8100)

設定方法

- (1) [VLAN → [Tunnel] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) トンネルステータスを有効にし、TPID を指定します。
- (4) < Apply > をクリックします。

VLAN > Tunnel

Step: 1. Configure Global ▼

Tunnel Status

☒ Enabled

Ethernet Type

(800-FFFF, hexadecimal value)

9100

Apply

Revert

インタフェースを QinQ トンネリングへ追加

前のセクションに従い、QinQ トンネルの準備を行ってください。

機能解説

- VLAN ポート設定または VLAN トランク設定画面を使用し、エッジスイッチのアクセスポートを 802.1Q トンネルモードに設定してください。
- トンネルポートの設定を行う前に 802.1Q トンネル設定画面を使用し、スイッチを QinQ モードに設定してください。(P96 「QinQ トンネリングの有効」を参照)

設定・表示項目

Interface

ポートまたはトランクのリストを表示

Port

ポート識別子（範囲：1-26）

Trunk

トランク識別子（範囲：1-12）

Mode

ポートの VLAN モードを設定します（初期設定：無効）

- None – 通常 VLAN モードで動作
- Tunnel – サービスプロバイダのネットワークを横断するカスタマーの VLAN ID を分離し、保つためにクライアントのアクセスポートに IEEE802.1Q トンネリング（QinQ）を設定します。
- Tunnel Uplink – サービスプロバイダのネットワーク内のもう1つのデバイスに向けたアップリンクポートとして IEEE802.1Q トンネリング（QinQ）を設定します。

設定方法

- (1) [VLAN → [Tunnel]] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) トンネルアクセスポートにモードを設定します。
- (4) < Apply > をクリックします。

VLAN > Tunnel

Step: 2. Configure Interface

Interface ☒ Port ☐ Trunk

802.1Q Tunnel Port List Max: 26 Total: 26 1 2 3

Port	Mode
1	Tunnel Uplink
2	Tunnel
3	None
4	None
5	None

3.5.3 プロトコル VLAN

多数のプロトコルをサポートすることを要求されるネットワーク装置は、通常の VLAN では容易にグループ分けをおこなうことができません。
これには、非標準のデバイスが特定のプロトコルに参加する全てのデバイスをカバーするように、異なった VLAN 間へトラフィックを渡すことが要求されます。
この種類の設定はセキュリティ、アクセシビリティといった VLAN の基本的な利益をユーザから奪います。

これらの問題を避けるために、本機ではプロトコルベース VLAN を設定できます。
これにより物理的ネットワークをそれぞれ必要とされるプロトコルの論理 VLAN グループへ分けます。ポートでフレームが受信された時、その VLAN メンバーシップはインバウンドパケットで使われているプロトコルタイプによって決定されます。

機能解説

- ・ プロトコルベース VLAN の設定は以下のステップでおこなってください。
 - (1) 最初に使用したいプロトコルの VLAN グループを設定します。(P710 参照)
それぞれの主要なプロトコルがネットワーク上で送受信される VLAN は別個の VLAN 設定をおこなうことを推奨します。(これは必須ではないです)
この段階ではポートメンバーの追加を行わないで下さい。
 - (2) "Configure Protocol" ページ (P98) で、VLAN へ割り当てたいプロトコルそれぞれのプロトコルグループを作成します。
 - (3) "Configure Interface (Add) " ページ (P100) を使用し、それぞれのインタフェースのプロトコルを適切な VLAN へマップします。
- ・ MAC ベース、IP サブネットベース、プロトコルベース VLAN が同時にサポートされる場合、プライオリティはこの順番に適用され、最後にポートベース VLAN になります。

プロトコル VLAN グループ設定

VLAN > Protocol (Configure Protocol - Add) ページを使用し、プロトコルグループを作成します。

設定・表示項目

Frame Type

このプロトコルで使用されるフレームタイプを選択してください。
(範囲：Ethernet、RFC1042、LLC Other)

Protocol Type

マッチするプロトコルタイプを指定します。(利用可能なオプション：IP、ARP、RARP、IPv6)
フレームタイプに LLC Other が選択される場合、利用可能なプロトコル種別は IPX Raw のみです。

Protocol Group ID

プロトコル VLAN グループに割り当てられる、プロトコルグループ ID
(範囲：1-2147483647)

設定方法

プロトコルグループの設定

- (1) [VLAN → [Protocol]] をクリックします。
- (2) 「Step」 リストから「Configure Protocol」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) フレームタイプリストからエントリを選択します。
- (5) プロトコルタイプリストからエントリを選択します。
- (6) プロトコルグループの識別子を入力します。
- (7) < Apply > をクリックします。

VLAN > Protocol

Step: 1. Configure Protocol ▼ Action: Add ▼

Frame Type Ethernet ▼

Protocol Type 08 00 (IP) ▼

Protocol Group ID (1 - 2147483647) 1

Apply Revert

プロトコルグループの表示

- (1) [VLAN → [Protocol]] をクリックします。
- (2) 「Step」 リストから「Configure Protocol」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

VLAN > Protocol

Step: 1. Configure Protocol ▼ Action: Show ▼

Protocol to Group Mapping Table Max: 12 Total: 1

☐	Frame Type	Protocol Type	Protocol Group ID
☐	Ethernet	08 00	1

Delete Revert

プロトコルグループをインタフェースへマッピング

プロトコルグループを VLAN にマッピングします。

機能解説

- プロトコルベース VLAN を作成する際、この設定画面を使用してのみインタフェースの割り当てが行えます。もし、"VLAN Static Table" や "VLAN Static Membership "(P85 参照) 等他の VLAN メニューを使用してインタフェースを割り当てた場合、これらインタフェースは関連付けられた VLAN の全てのトラフィックタイプを受け入れます。
- プロトコル VLAN へアサインされたポートへフレームが入ってくる時、次の方法で処理されます。
 - －フレームがタグ付きの場合、タグフレームに適用された標準ルールに従い処理されます。
 - －フレームがタグ無しで、プロトコルタイプが一致した場合、フレームは適切な VLAN へ転送されます。
 - －フレームがタグ無しで、プロトコルタイプが一致しない場合、フレームはインタフェースのデフォルト VLAN へ転送されます。

設定・表示項目

Interface

リストまたはポートのリストを表示

Port

ポート識別子（範囲：1-26）

Trunk

トランク識別子（範囲：1-12）

Protocol Group ID

プロトコル VLAN グループに割り当てられたプロトコルグループ ID
（範囲：1-2147483647）

VLAN ID

一致したプロトコルトラフィックがフォワードされる VLAN（範囲：1-4093）

設定方法

プロトコルグループを VLAN ヘマッピング

- (1) [VLAN → [Protocol]] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) ポートまたはトランクを選択します。
- (5) プロトコルグループの識別子を入力します。
- (6) 対応する VLAN ID を入力します。
- (7) < Apply >をクリックします。

VLAN > Protocol

Step: 2. Configure Interface Action: Add

Interface ☒ Port 2 ☐ Trunk

Protocol Group ID 1

VLAN ID (1-4093)

Apply Revert

ポートまたはトランクヘマッピングされたプロトコルグループを表示

- (1) [VLAN → [Protocol]] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

VLAN > Protocol

Step: 2. Configure Interface Action: Show

Interface ☒ Port 2 ☐ Trunk

Port To Protocol Group Mapping Table Max: 528 Total: 1

	Protocol Group ID	VLAN ID
☐	1	3

Delete Revert

3.5.4 IP サブネット VLAN

ポートベースの分類を使用する際、ポートで受信された全てのタグ無しフレームはその VID (PVID) がポートと結び付けられる VLAN に属しているとして分類されます。

IP サブネットベース VLAN 分類が有効である時、タグ無し入力フレームのソースアドレスは、IP サブネットから VLAN へのマッピングテーブルと照らし合わされます。

サブネットのエントリが発見された場合、これらのフレームはエントリで示された VLAN に割り当てられます。

IP サブネットがマッチしない場合、タグ無しフレームは受信ポートの VLAN ID (PVID) に属すると分類されます。

機能解説

- それぞれのサブネットは 1 つの VLAN ID にのみマップされることが可能です。
IP サブネットは IP アドレスとマスクから成ります。
- ポートでタグ無しフレームが受信された場合、ソース IP アドレスは IP サブネットから VLAN へのマッピングテーブルと照らし合わされ、エントリが見つかるに対応する VLAN ID がフレームに割り当てられます。マッピングが見つからない場合、受信ポートの PVID がフレームに割り当てられます。
- IP サブネットはブロードキャストまたはマルチキャスト IP アドレスにはなれません。
- MAC ベース、IP サブネットベース、プロトコル VLAN が同時にサポートされる時、このシーケンスではプライオリティが適用され、最後にポートベース VLAN になります。

設定・表示項目

IP Address

サブネットの IP アドレス。

Subnet Mask

IP サブネットのホストアドレスビットを識別します。

VLAN

IP サブネットとマッチしたトラフィックは VLAN に転送されます。(範囲：1-4093)

Priority

タグ無しイングレストラフィックに割り当てられたプライオリティ
(範囲：0-7 7 が最高プライオリティ。 初期設定：0)

設定方法

IP サブネットを VLAN ヘマップ

- (1) [VLAN → [IP Subnet] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) IP アドレスフィールドにアドレスを入力します。
- (4) サブネットマスクフィールドにマスクを入力します。
- (5) VLAN フィールドに識別子を入力します。
- (6) プライオリティフィールドに、タグ無しフレームに割り当てる値を入力します。
< Apply >をクリックします。

VLAN > IP Subnet

Action:

IP Address

Subnet Mask

VLAN (1-4093)

Priority (0-7)

IP サブネット VLAN 設定の表示

- (1) [VLAN → [IP Subnet] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

VLAN > IP Subnet

Action:

IP Subnet to VLAN Mapping Table Max: 256 Total: 1

☐	IP Address	Subnet Mask	VLAN	Priority
☐	192.168.1.0	255.255.255.0	10	0

3.5.5 MAC ベース VLAN

MAC ベース VLAN 機能は、ソース MAC アドレスに従って VLAN ID を入力タグ無しフレームへ割り当てます。

MAC ベース VLAN 分類が有効である場合、ポートで受信されたタグ無しフレームは、フレームのソース MAC アドレスにマップされる VLAN へ割り当てられます。

MAC アドレスが一致しない時、タグ無しフレームは受信ポートのネイティブ VLAN ID (PVID) が割り当てられます。

機能解説

- MAC-to-VLAN マッピングは本機の全てのポートへ適用されます。
- ソース MAC アドレスは 1 つの VLAN ID へのみマップされることが可能です。
- 設定された MAC アドレスはブロードキャストまたはマルチキャストアドレスにはなれません。
- MAC ベース、IP サブネットベース、プロトコル VLAN が同時にサポートされる時、このシーケンスではプライオリティが適用され、最後にポートベース VLAN になります。

設定・表示項目

MAC Address

特定の VLAN にマップされるソース MAC アドレス

VLAN

指定されたソース MAC アドレスと一致する入力トラフィックが転送される VLAN
(範囲：1-4093)

Priority

タグ無しイングレストラフィックに割り当てられたプライオリティ
(範囲：0-7 7 が最高プライオリティ。 初期設定：0)

設定方法

MAC アドレスを VLAN ヘマップ

- (1) [VLAN] → [MAC-Based] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) MAC アドレスフィールドにアドレスを入力します。
- (4) VLAN フィールドに識別子を入力します。
- (5) プライオリティフィールドに、タグ無しフレームに割り当てる値を入力します。
- (6) < Apply >をクリックします。

VLAN > MAC-Based

Action: Add ▼

MAC Address

VLAN (1-4093)

Priority (0-7)

Apply Revert

VLAN ヘマップされた MAC アドレスの表示

- (1) [VLAN] → [MAC-Based] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

VLAN > MAC-Based

Action: Show ▼

MAC-Based VLAN List Max: 32 Total: 1

☐	MAC Address	VLAN	Priority
☐	00-AB-CD-11-22-33	10	0

Delete Revert

3.5.6 VLAN ミラーリング

リアルタイム解析のため、1 つまたはそれ以上のソース VLAN から、ターゲットポートへトラフィックをミラーリングを行うことができます。
ターゲットポートにネットワーク解析装置（Sniffer 等）又は RMON プローブを接続し、ソース VLAN のトラフィックを調査することが可能です。

機能解説

- ソース VLAN の全てのアクティブポートは入力トラフィックのみモニタされます。
- 全ての VLAN ミラーセッションは、同一のターゲットポートを共有します。
- VLAN ミラーリングとポートミラーリングの両方が有効である場合、それらは同一のターゲットポートを使用します。
- VLAN ミラーリングとポートミラーリングの両方が有効である場合、ターゲットポートは、2 倍のミラーされたパケットを受信します。1 つはソースミラーポートで、ソースミラー VLAN から再度受信します。

設定・表示項目

Source VLAN

トラフィックのモニタがおこなわれる VLAN（範囲：1 - 4093）

Target Port

ソース VLAN からミラートラフィックを受信する行先ポート（範囲：1-26）

設定方法

VLAN ミラーリングの設定

- (1) [VLAN] → [Mirror] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) ソース VLAN、ターゲットポートを選択します。
- (4) < Apply > をクリックします。

VLAN > Mirror

Action: Add

Source VLAN: 1

Target Port: 2

Apply Revert

ミラーされた VLAN の表示

- (1) [VLAN] → [Mirror] をクリックします。

(2) 「Action」 リストから「Show」を選択します。

VLAN > Mirror

Action: Show ▼

VLAN Mirror List Max: 26 Total: 1

☐	Source (VLAN)	Target (Unit/Port)
☐	1	1/2

DeleteRevert

3.6 アドレステーブル

本機には認知されたデバイスの MAC アドレスが保存されています。この情報は受送信ポート間での通信の送信に使用されます。通信の監視により学習された全ての MAC アドレスは動的アドレステーブルに保存されます。また、手動で特定のポートに送信する静的なアドレスを設定することができます。

3.6.1 静的アドレスの設定

静的アドレスは本機の指定されたインタフェースに割り当てることができます。静的アドレスは指定したインタフェースに送信され、他へは送られません。静的アドレスが他のインタフェースで見つかった場合は、アドレスは無視されアドレステーブルには登録されません。

機能解説

- ホストデバイスの静的アドレスは、特定の VLAN の特定のポートに割り当てられることが可能です。このコマンドを MAC アドレスへの静的アドレスの追加に使用できます。静的アドレスは以下の特徴を持ちます。
 - 静的アドレスは有り当てられ、動かされていないインタフェースにバウンドします。静的アドレスが他のインタフェースで見つかった時、アドレスは無視されアドレステーブルへは書き込まれません。
 - 所定のインタフェースリンクがダウンしている時、静的アドレスをアドレステーブルから削除することはできません
 - 静的アドレスはテーブルから削除されるまで、他のポートで学習されることはできません。

設定・表示項目

VLAN

VLAN ID(1-4093)

Interface

静的アドレスと関連したポート又はトランク

MAC Address

インタフェースの MAC アドレス

Static Status

指定されたアドレスを維持する時間

- Delete-on-reset – スイッチがリセットされるまで割り当てを維持
- Permanent – 恒久に割り当てを維持（初期設定）

設定方法

静的 MAC アドレスの設定

- (1) [MAC Address] → [Static] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) 必要な項目の設定を行い、< Apply >をクリックします。

MAC Address > Static

Action: Add

VLAN 1

Interface ☒ Port 1 ☐ Trunk

MAC Address 00-12-cd-94-34-da

Static Status Permanent

Apply Revert

MAC アドレステーブルの静的アドレスを表示

- (1) [MAC Address] → [Static] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

MAC Address > Static

Action: Show

Static MAC Address to Interface Mapping Table Max: 1024 Total: 1

☐	MAC Address	VLAN	Interface	Type	Life Time
☐	00-12-CD-94-34-DA	1	Unit 1 / Port 1	Config	Permanent

Delete Revert

3.6.2 エージングタイムの変更

動的アドレステーブルに学習されたアドレスが削除されるまでの時間（エージングタイム）を設定することができます。

設定・表示項目

Aging Status

エージングタイムの機能の有効 / 無効

Aging Time

MAC アドレスエージングタイム（範囲：10-844 秒、初期設定：300 秒）

設定方法

エージングタイムの設定

- (1) [MAC Address] → [Dynamic] をクリックします。
- (2) 「Action」 リストから「Configure Aging」を選択します。
- (3) 必要に応じ、エージングタイムを編集します。
- (4) < Apply > をクリックします。

The screenshot shows a web interface for configuring MAC addresses. The breadcrumb is "MAC Address > Dynamic". Below this, there is a section for "Configure Aging". The "Action:" dropdown is set to "Configure Aging". Underneath, "Aging Status" is checked and labeled "Enabled". "Aging Time (10-844)" is set to "300" seconds. At the bottom right, there are "Apply" and "Revert" buttons.

MAC Address > Dynamic	
Action:	Configure Aging
Aging Status	☒ Enabled
Aging Time (10-844)	300 sec
Apply Revert	

3.6.3 動的アドレステーブルの表示

動的アドレステーブルには、入力された通信の送信元アドレスの監視により学習した MAC アドレスが保存されています。入力された通信の送信先アドレスがアドレステーブル内で発見された場合、パケットはアドレステーブルに登録された関連するポートへ直接転送されます。アドレステーブルに見つからなかった場合には全てのポートに送信されます。

設定・表示項目

Sort Key

リストの並びを MAC アドレス、VLAN、インタフェースから選択

MAC Address

インタフェースの MAC アドレス

VLAN

VLAN ID (1-4093)

Interface

ポート又はトランク

Type

このテーブルの学習されるエントリを表示

Life Time

指定したアドレスが維持される時間を表示

設定方法

エージングタイムの設定

- (1) [MAC Address] → [Dynamic] をクリックします。
- (2) 「Action」 リストから「Show Dynamic MAC」を選択します。
- (3) ソートキーを選択します。
- (4) それぞれのパラメータを入力します。
- (5) < Query > をクリックします。

MAC Address > Dynamic

Action: Show Dynamic MAC

Query by:

Sort Key: MAC Address

☐ MAC Address

☐ VLAN

☐ Interface

☐ Port

☐ Trunk

Query

Dynamic MAC Address List Max: 8192 Total: 1

MAC Address	VLAN	Interface	Type	Life Time
00-0A-E4-33-CD-26	1	Unit 1 / Port 1	Learn	Delete on Timeout

3.6.4 動的アドレステーブルの消去

MAC Address > Dynamic (Clear Dynamic MAC) ページを使用し、転送データベースから学習されたエントリを消去することができます。

設定・表示項目

Clear by

全てのエントリまたは、指定した MAC アドレス、VLAN の全てのエントリ、ポートまたはトランクに関連付けられる全てのエントリをクリアすることができます。

設定方法

- (1) [MAC Address] → [Dynamic] をクリックします。
- (2) 「Action」 リストから「Clear Dynamic MAC」を選択します。
- (3) 消去を行うメソッドを選択します。(All、MAC Address、VLAN、Interface)
- (4) < Apply > をクリックします。

MAC Address > Dynamic

Action:

Clear by:

3.6.5 MAC アドレスミラーリングの設定

本機では、リアルタイム分析の為に、スイッチのターゲットポート以外の全てのポートから、指定した特定のソースアドレスのトラフィックをターゲットポートへミラーリングすることが可能です。
ターゲットポートにネットワーク解析装置（Sniffer 等）又は RMON プローブを接続し、通信に影響を与えずにソースポートのトラフィックを解析することができます。

機能解説

- MAC アドレスからのトラフィックのミラーリングを行う際、ターゲットポート以外のスイッチの全てのポートへ入る、指定したソースアドレスを持つ入力トラフィックはディスティネーションポートへミラーされます。
- 全てのミラーセッションは同じディスティネーションポートを共有します。
- スパニングツリー BPDU パケットはターゲットポートへミラーされません。
- ポートトラフィックのミラーリング時に MSTP を使用する際、ターゲットポートはソースポートと同じ VLAN に含まれなくてはなりません。（詳細は P115 を参照してください）

設定・表示項目

Source MAC

通信がモニターされる MAC アドレスを指定します。

XX-XX-XX-XX-XX-XX または XXXXXXXXXXXX の形式で入力してください。

Target Port

ソースポートからトラフィックのミラーを行うポートを指定します。（範囲：1-26）

設定方法

MAC アドレスベースの packets ミラー

- (1) [MAC Address] → [Mirror] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) ソース MAC アドレスとディスティネーションポートを指定します。
- (4) < Apply > をクリックします。

MAC Address > Mirror

Action: Add

Source MAC 11-22-33-44-55-66

Target Port 2

Apply Revert

Web インタフェース アドレステーブル

ミラーされた MAC アドレスの表示

- (1) [MAC Address] → [Mirror] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

MAC Address > Mirror

Action: Show ▼

MAC Mirror List Max: 10 Total: 1

☐	Source (MAC)	Target (Unit/Port)
☐	11-22-33-44-55-66	1/2

Delete Revert

3.7 スパニングツリーアルゴリズム

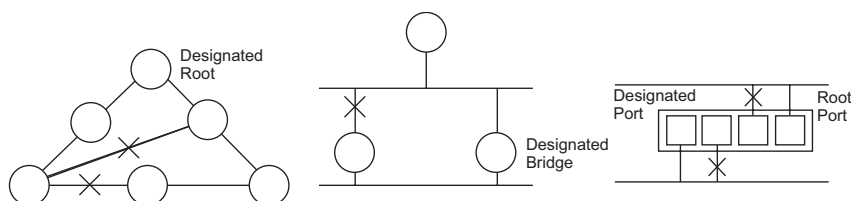
スパニングツリープロトコル STP はネットワークのループを防ぎ、また、スイッチ、ブリッジ及びルータ間のバックアップリンクを確保するために使用します。

STP 機能を有するスイッチ、ブリッジ及びルータ間で互いに連携し、各機器間のリンクで 1 つのルートがアクティブになるようにします。また、別途バックアップ用のリンクを提供し、メインのリンクがダウンした場合には自動的にバックアップを行います。

本機は、以下の規格に準拠した STP に対応しています。

- STP — Spanning Tree Protocol (IEEE 802.1D)
- RSTP — Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP — Multiple Spanning Tree Protocol (IEEE 802.1s)

STP はスパニングツリーネットワークの経路となる STP 対応スイッチ・ブリッジ又はルータを選択するために分散アルゴリズムを使用します。それにより、デバイスからルートデバイスにパケットを送信する際に最小のパスコストとなるようにルートデバイスを除く各デバイスのルートポートの設定を行います。これにより、ルートデバイスから LAN に対し最小のパスコストにより各 LAN の指定されたデバイスに対してパケットが転送されます。その後、指定のポートとして各関連する LAN 又はホストデバイスと通信する指定ブリッジ上のポートを選択します。



最小コストのスパニングツリーが決定した後、すべてのルートポートと指定ポートが有効となり、他のポートは無効となります。それによりパケットはルートポートから指定ポートにのみ送信され、ネットワークのループが回避されます。

安定したネットワークポロジが確立された後、ルートブリッジから送信される Hello BPDU(Bridge Protocol Data Units) をすべてのブリッジが受信します。定められた間隔（最大値）以内にブリッジが Hello BPDU を確認できない場合、ルートブリッジへの接続を行っているリンクを切断します。そして、このブリッジはネットワークの再設定を行ない有効なネットワークポロジを回復するために、他のブリッジとネゴシエーションを開始します。

RSTP は既存の遅い STP に代わる機能とされています。RSTP は MSTP にも組み込まれています。RSTP はあらかじめ障害時の代替ルートを定め、ツリー構造に関連のない転送情報を区別することにより、STP に比べ約 10 分の 1 の速さでネットワークの再構築が行えます。

STP 又は RSTP を利用した場合、すべての VLAN メンバー間での安定的なパスの提供が難しくなります。ツリー構造の頻繁な変更により一部のグループメンバーが孤立してしまうことがあります。(RSTP の拡張である) MSTP では、VLAN グループ毎に独立したスパニングツリーを提供することができます。特定の VLAN を Multiple Spanning Tree インスタンス (MSTI) に含むように指定すると、MSTI ツリーが自動的に構成され、各 VLAN の接続状況が維持されます。

各インスタンスは、Common Spanning Tree (CST) 内の RSTP ノードとして扱われるので、MSTP は、ネットワーク全体との接続を行なうことができます。

3.7.1 ループバック検出

ポートループバック検出が有効であり、ポートがそれ自身の BPUD を受信した際、ディテクションエージェントはループバック BPDU を破棄、SNMP トラップを送信し、ポートを Discard（パケット破棄）モードにします。

このループバックステータスは自動または手動でリリースすることができます。

ポートが自動ループバックリリースに設定されている場合、以下の条件の内 1 つが満たされるとポートは転送状態に戻ります。

- ・ ポートがポート自身以外の BPUD を受信する。
- ・ ポートのリンクステータスが一旦リンクダウンになった後、再びリンクアップになる。
- ・ ポートがフォワード遅延インターバルでポート自身の BPUD の受信を終了。

[注意] ポートループバックディテクションが有効でなく、ポートが自身の BPUD を受信した場合、ポートは IEEE 標準の 802.1w-2001 9.3.4 に従ってループバック BPDU を破棄します。

[注意] スパニングツリーがスイッチで無効になっている場合、ポートループバックディテクションはアクティブになりません。

[注意] 手動リリースモードに設定時、Link down/Up イベントはポートをリリースしません。

設定・表示項目

Interface

ポートまたはトランクのリストを表示。

Status

このインタフェースでループバックディテクションを有効化。（初期設定：有効）

Trap

このインタフェースでループバックイベントの SNMP トラップ通知を有効化。（初期設定：無効）

Release Mode

ポートを自動または手動ループバックリリースに設定。

Release

ポートが Discard モードから手動でリリースされることを許可。ポートが手動リリースモードに設定時のみ利用可能。

設定方法

- (1) [Spanning Tree] → [Loopback Detection] をクリックします。
- (2) 必要なインタフェースタイプを表示するため、ポートまたはトランクをクリックします。
- (3) 必要に応じ、設定を修正します。
- (4) < Apply > をクリックします。

Spanning Tree > Loopback Detection

Interface ☒ Port ☐ Trunk

Loopback Detection Port List Max: 26 Total: 26 1 2 3

Port	Status	Trap	Release Mode	Release
1	☒ Enabled	☐ Enabled	Auto ▼	Release
2	☒ Enabled	☐ Enabled	Auto ▼	Release
3	☒ Enabled	☒ Enabled	Manual ▼	Release
4	☒ Enabled	☐ Enabled	Auto ▼	Release
5	☒ Enabled	☐ Enabled	Auto ▼	Release

3.7.2 グローバル設定

Spanning Tree > STA ページを使用し、スパニングツリーのグローバル設定を行います。
ここでの設定は本機全体に適用されます。

機能解説

- Spanning Tree Protocol
本機の初期設定では RSTP に指定されていますが、STP に設定し IEEE802.1D に準拠した BPDU のみを送信することができます。この場合、ネットワーク全体に対して 1 つの SpanningTree のみの設定が行なえます。もしネットワーク上に複数の VLAN を設定する場合、一部の VLAN メンバー間はネットワークのループを回避するため無効となる場合があります。複数の VLAN を構成する場合には MSTP を使用することを推奨します。
- Rapid Spanning Tree Protocol
RSTP は、以下のそれぞれの着信プロトコルメッセージを監視し動的に各プロトコルメッセージに適合させることにより、STP と RSTP ノードのどちらへの接続もサポートします。
 - － STP Mode － ポートの移動遅延タイマーが切れた後に IEEE802.1D BPDU を受け取ると、本機は IEEE802.1D ブリッジと接続していると判断し、IEEE802.1D BPDU のみを使用します。
 - － RSTP Mode － RSTP において、ポートで IEEE802.1D BPDU を使用しポート移動遅延タイマーが切れた後に RSTP BPDU を受け取ると、RSTP は移動遅延タイマーを再スタートさせそのポートに対し RSTP BPDU を使用します。
- Multiple Spanning Tree Protocol
MSTP はそれぞれのインスタンスのためにユニークなスパニングツリーを生成します。これはネットワーク中に複数のパスウェイを提供し、それによってトラフィック付加のバランスを取り、1 つのインスタンスのブリッジノードで不具合が発生した時に広範囲の中断を防ぎます。また、失敗したインスタンスのため、新しいトポロジのより早い輻輳を可能にします。
 - － ネットワーク上で MSTP を有効にするには、接続された関連するブリッジにおいても同様の MSTP の設定を行ない、スパニングツリーインスタンスに参加することを許可する必要があります。
 - － スパニングツリーインスタンスは互換性のある VLAN インスタンス割り当てを持つブリッジ上にのみ存在出来ます。
 - － スパニングツリーモードを変更する場合、変更前のモードのスパニングツリーインスタンスをすべて止め、その後新しいモードにおいて通信を再開します。スパニングツリーのモード変更時には通信が一時的に遮断されるので注意して下さい。

設定・表示項目

基本設定

Spanning Tree Status

スパニングツリーを有効又は無効にします。(初期設定:有効)

Spanning Tree Type

使用されるスパニングツリープロトコルの種類を指定します。(初期設定:RSTP)

- － **STP** — Spanning Tree Protocol (IEEE 802.1D。STP を選択すると、本機は RSTP の STP 互換モードとなります)
- － **RSTP** — Rapid Spanning Tree Protocol(IEEE 802.1w)
- － **MSTP** — Multiple Spanning Tree Protocol(IEEE 802.1s)

Priority

ルートデバイス、ルートポート、指定ポートの識別に使用される、デバイスプライオリティを設定できます。最上位のプライオリティを持つ機器が STP ルート機器になります（値が小さいほどプライオリティが高くなります）。すべての機器のプライオリティが同じ場合は、最小の MAC アドレスを持つ機器がルート機器になります。（初期設定 :32768、範囲 :0-61440 の値で 4096 ずつ (0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440)）

アドバンスド

Path Cost Method

パスコストはデバイス間の最適なパスを決定するために使用されます。パスコスト方式は各インタフェースに割り当てることができる値の範囲を決定するのに使用されます。

- － Long — 32 ビットの 1-200,000,000 の値 (初期値)
- － Short — 16 ビットの 1-65535 の値

Transmission Limit

継続的なプロトコルメッセージの最小送信間隔の設定による BPDU の最大転送レートの設定を行います（範囲 :1-10（秒）、初期設定 :3）

ルート時

Hello Time

ルートデバイスが設定メッセージを送信する間隔（秒）を設定できます（初期設定 :2（秒）、最小値 :1、最大値 :10 又は $[(\text{Maximum Age}/2)-1]$ の小さい方の値）

Maximum Age

機器が再設定される前に設定メッセージを待ち受ける、最大の時間を秒で設定できます。指定ポートを除く全機器のポートで、通常のインターバル内に設定メッセージが受信される必要があります。STP 情報がエージアウトしたポートは接続されている LAN の指定ポートに変更されます。ルートポートの場合、ネットワークに接続されている機器のポートから新たなルートポートが選択されます。（初期設定 :20（秒）、最小値 :6 又は $[2 \times (\text{Hello Time}+1)]$ の大きい方の値、最大値 :40 もしくは $[2 \times (\text{Forward Delay}-1)]$ の小さい方の値）

Forward Delay

機器状態の遷移に対してルート機器が待機する最大の時間（秒）が設定できます。フレームの転送が開始される前に、トポロジの変更を機器に認識させるため、遅延を設定する必要があります。さらに各ポートでは、一時的なデータのループを防ぐため、ポートをブロック状態に戻す競合情報のリスニングを行う時間が必要になります（初期設定 :15（秒）、最小値 :4 又は $[(\text{Maximum Age}/2)+1]$ の大きい方の値、最大値 :30）

MSTP 設定

Max Instance Numbers

本機で設定可能な MST インスタンスの最大数

Configuration Digest

VLAN ID から MST ID へのマッピングテーブルを含む MD5 署名キー。つまりこのキーは全ての VLAN から CIST へのマッピングです。

Region Revision

MST インスタンスのリビジョン（設定範囲：0-65535、初期設定：0）

Region Name

MST インスタンス名（最大値：32 文字、スイッチの MAC アドレス）

Maximum Hop Count

BPDU が破棄される前の MST 内での最大ホップ数（設定範囲：1-40、初期設定：20）

設定方法

- (1) [Spanning Tree] → [STA] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Configure」を選択します。
- (4) 必要な設定項目を変更し、< Apply >をクリックします。

(STP)

Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status ☒ Enabled

Spanning Tree Type STP

Priority (0-61440, in steps of 4096) 32768

Advanced:

Path Cost Method Long

Transmission Limit (1-10) 3

When the Switch Becomes Root:

Hello Time (1-10) 2 sec

Maximum Age (6-40) 20 sec

Forward Delay (4-30) 15 sec

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

Apply Revert

(RSTP)

Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status ☒ Enabled

Spanning Tree Type RSTP

Priority (0-61440, in steps of 4096) 32768

Advanced:

Path Cost Method Long

Transmission Limit (1-10) 3

When the Switch Becomes Root:

Hello Time (1-10) 2 sec

Maximum Age (6-40) 20 sec

Forward Delay (4-30) 15 sec

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

Apply Revert

(MSTP)

Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status ☒ Enabled

Spanning Tree Type MSTP

Priority (0-61440, in steps of 4096) 32768

Advanced:

Path Cost Method Long

Transmission Limit (1-10) 3

When the Switch Becomes Root:

Hello Time (1-10) 2 sec

Maximum Age (6-40) 20 sec

Forward Delay (4-30) 15 sec

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

MSTP Configuration

Max Instance Numbers 32

Configuration Digest 0xAC36177F50283CD4B83821D8AB26DE62

Region Revision (0-65535) 0

Region Name 00 1a 7e ab fd 12

Max Hop Count (1-40) 20

Apply Revert

3.7.3 グローバル設定の表示

Spanning Tree > STA (Configure Global - Show Information) 使用し、現在の STP の情報を確認することができます。

設定・表示項目

Bridge ID

STP で本機を認識するための一意の ID を表示します。ID は本機の STP プライオリティと MAC アドレスから算出されます。

Designated Root

ルートデバイスに設定された、スパニングツリー内の機器のプライオリティ及び MAC アドレスが表示されます。

Root Port

ルートの最も近い、スイッチ上のポートの番号。スイッチはこのポートを通して、ルートデバイスとコミュニケーションが可能です。ルートポートが無い場合、このスイッチがスパニングツリーのルートデバイスとしてアクセプトされます。

Root Path Cost

スイッチ上のルートポートからルートデバイスへのパスコスト。

Configuration Changes

スパニングツリーが再設定された回数が表示されます。

Last Topology Change

最後にスパニングツリーが再設定されてから経過した時間が表示されます。

設定方法

- (1) [Spanning Tree] → [STA] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Show Information」を選択します。

Spanning Tree > STA

Step: 1. Configure Global Action: Show Information

Spanning Tree Information

Spanning Tree Status	Enabled	Spanning Tree Type	RSTP
Designated Root	32768.0012CFF3DE46	Bridge ID	32768.0012CFF3DE46
Root Port	0	Max Age	20 sec
Root Path Cost	0	Hello Time	2 sec
Configuration Changes	0	Forward Delay	15 sec
Last Topology Change	0 days, 2 hours, 56 minutes, 9 seconds		

3.7.4 インタフェース設定

Spanning Tree > STA (Configure Interface - Configure) ページにて、ポートプライオリティ、パスコスト、リンクタイプ及びエッジポートを含む各インタフェースの RSTP 及び MSTP 属性を設定することができます。

ネットワークのパスを指定するために同じメディアタイプのポートに対し異なるプライオリティ又はパスコストを設定し、二点間接続または共有メディア接続を示すためリンクタイプを設定します。また、ファストフォワーディングをサポートした機器を接続した場合にはエッジポートの指定を行います。(本項での "ポート" とは "インタフェース" を意味するため、ポートとトランクの両方を示します)

設定・表示項目

以下の設定は変更することはできません。

Interface

ポートまたはトランクのリストを表示。

Interface

ポートまたはトランクのリストを表示。

Admin Edge Status for all ports

- Enabled — 手動でポートを Edge ポートとして設定します。
- Disabled — Edge ポート設定を無効にします。
- Auto — RSTP または MSTP BPDU を受信せずにエッジ遅延時間の期限が切れた際、ポートを自動でエッジポートとして設定します。

以下の条件では、インタフェースは Edge ポートとして機能しません。

- ・ スパニングツリーモードが STP (P118) に設定されている場合、エッジポートモードは手動で有効か、自動に設定できますが効果は発しません。
- ・ ループバック検索 (P116) が有効であり、とループバック BPDU が無効の場合、インスタンスはループバック状態が開放されるまでエッジポートとして機能出来ません。
- ・ インタフェースがフォワーディング状態で、ロールが変更された場合、エッジ遅延時間が期限切れになっていても、インスタンスはエッジポートとして動作を続けることが出来ません。
- ・ 遅延タイマーの期限が切れた後に、エッジポートが BPDUs を受信しない場合、designated ポートへロール変更され、すぐにフォワーディング状態に入ります。(126 ページの「インタフェース設定の表示」を参照)

Spanning Tree

このインタフェースの STA の有効 / 無効 (初期設定 : 有効)

Priority

STP での各ポートのプライオリティを設定します。本機の全てのポートのパスコストが同じ場合には、最も高いプライオリティ (最も低い設定値) がスパニングツリーのアクティブなリンクとなります。これにより、STP においてネットワークのループを回避する場合に、高いプライオリティのポートが使用されるようになります。2 つ以上のポートが最も高いプライオリティの場合には、ポート番号が小さいポートが有効になります (初期設定 : 128、範囲 : 0-240 の 16 ずつ)

Admin Path Cost

このパラメータは STP においてデバイス間での最適なパスを決定するために設定します。低い値がスピードの早いメディアのポートに割り当てられ、より高い値がより遅いメディアに割り当てられる必要があります (パスコストはポートプライオリティより優先されます)

推奨 STA パスコスト範囲

ポートタイプ	IEEE802.1D-1998	IEEE802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

推奨 STA パスコスト

ポートタイプ	リンクタイプ	IEEE802.1D-1998	IEEE802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

デフォルト STA パスコスト

ポートタイプ	リンクタイプ	IEEE802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Admin Link Type

インタフェースへ接続する接続方式（初期設定 :Auto）

- Point-to-Point — 他の 1 台のブリッジへの接続
- Shared — 2 台以上のブリッジへの接続
- Auto — Point-to-Point か Shared のどちらかを自動的に判断します。

Root Guard

STA はより低いブリッジ識別子（または同じ値と、より低い MAC アドレス）を持つブリッジがいつでも、ルートブリッジを引き継ぐことを許可します。Root Guard はルートブリッジが最適以下の場所において構成されないことを保証するために使用します。

（初期設定：無効）

Admin Edge Port

“Admin Edge Status for all ports” を参照してください。

BPDU Guard

BPDU の受信からエッジポートを保護します。（初期設定：無効）

BPDU Filter

最後のノードに接続される設定をされたエッジポートで BPUD の転送を無効にします。

（初期設定：無効）

Migration

設定およびトポロジ変更通知 BPDU を含む STP BPDU を検知することにより、自動的に STP 互換モードに変更することができます。

また、本機能のチェックボックスをチェックし機能を有効にすることにより、手動で適切な BPDU フォーマット（RSTP または STP 互換）の再確認を行うことができます。

設定方法

- (1) [Spanning Tree] → [STA] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Configure」を選択します。
- (4) 必要に応じて設定変更を行います。
- (5) < Apply > をクリックします。

Spanning Tree > STA

Step: 2. Configure Interface Action: Configure

Interface ☒ Port ☐ Trunk

Admin Edge Status for all ports ☐ Auto

Port List Max: 26 Total: 26 1 2 3

Port	Spanning Tree	Priority (0-240, in steps of 16)	Admin Path Cost (0-2000000000, 0: Auto)	Admin Link Type	Root Guard	Admin Edge Port	BPDU Guard	BPDU Filter	Migration
1	☒ Enabled	128	0	Auto	☐ Enabled	Disabled	☐ Enabled	☐ Enabled	☐ Enabled
2	☒ Enabled	128	0	Auto	☐ Enabled	Disabled	☐ Enabled	☐ Enabled	☐ Enabled
3	☒ Enabled	128	0	Auto	☐ Enabled	Disabled	☐ Enabled	☐ Enabled	☐ Enabled
4	☒ Enabled	128	0	Auto	☐ Enabled	Disabled	☐ Enabled	☐ Enabled	☐ Enabled
5	☒ Enabled	128	0	Auto	☐ Enabled	Disabled	☐ Enabled	☐ Enabled	☐ Enabled

3.7.5 インタフェース設定の表示

STA Port Information 及び STA Trunk Information 画面では STA ポート及び STA トランクの現在の状態を表示します。

設定・表示項目

Spanning Tree

STA の有効 / 無効が表示されます。

STA Status

スパニングツリー内での各ポートの現在の状態を表示します：

- － Discarding — STP 設定メッセージを受信しますが、パケットの送信は行っていません。
- － Learning — 矛盾した情報を受信することなく、Forward Delay で設定した間隔で設定メッセージを送信しています。ポートアドレステーブルはクリアされ、アドレスの学習が開始されています。
- － Forwarding — パケットの転送が行われ、アドレスの学習が継続されています。

ポート状態のルール

- ・ STP 準拠のブリッジデバイスが接続されていないネットワークセグメント上のポートは、常に転送状態 (Forwarding) にあります。
- ・ 他の STP 準拠のブリッジデバイスが接続されていないセグメント上に、2 個のポートが存在する場合は、ID の小さい方でパケットの転送が行われ (Forwarding)、他方ではパケットが破棄されます (Discarding)。
- ・ 起動時にはすべてのポートでパケットが破棄されます (Discarding)。その後学習状態 (Learning)、フォワーディング (Forwarding) へと遷移します。

Forward Transitions

ポートが転送状態 (Forwarding) に遷移した回数が表示されます。

Designated Cost

スパニングツリー設定における、本ポートからルートへのコストが表示されます。媒体が遅い場合、コストは増加します。

Designated Bridge

スパニングツリーのルートに到達する際に、本ポートから通信を行うデバイスのプライオリティと MAC アドレスが表示されます。

Designated Port

スパニングツリーのルートに到達する際に、本機と通信を行う指定ブリッジデバイスのポートのプライオリティと番号が表示されます。

Oper Path Cost

このポートを含むスパニングツリールートへ向かうパスのパスコストへの、このポートの貢献。

Oper Link Type

インタフェースの属する LAN セグメントの使用中の 2 点間の状況。この項目は STP Port/Trunk Configuration ページの Admin Link Type に記載されているように手動設定又は自動検出により決定されます。

Oper Edge Port

この項目は STP Port/Trunk Configuration ページの Admin Edge Port の設定により設定のために初期化されます。しかし、このポートへの接続された他のブリッジを含め、BPDU を受信した場合は false に設定されます。

Port Role

実行中のスパニングツリーポートロジの一部であるかないかによって役割が割り当てられています。

- － Root ポート — ルートブリッジへのブリッジに接続します。
- － Designated ポート — ルートブリッジへのブリッジを通じて LAN に接続します。
- － Master ポート — MSTI regional ルート
- － Alternate 又は Backup ポート — 他のブリッジ、ブリッジポート又は LAN が切断または削除された場合に、接続を提供します。
- － Disabled ポート — スパニングツリー内での役割がない場合には無効 (Disabled) となります。

設定方法

- (1) [Spanning Tree] → [STA] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Show Information」を選択します。

Spanning Tree > STA

Step: 2. Configure Interface Action: Show Information

Interface ☒ Port ☐ Trunk

Spanning Tree Port List Max: 26 Total: 26

123

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Enabled	Forwarding	1	0	32768.001A7EABFD12	128.1	100000	Point-to-Point	Disabled	Designated
2	Enabled	Discarding	0	0	32768.001A7EABFD12	128.2	100000	Point-to-Point	Disabled	Disabled
3	Enabled	Discarding	0	0	32768.001A7EABFD12	128.3	100000	Point-to-Point	Disabled	Disabled
4	Enabled	Discarding	0	0	32768.001A7EABFD12	128.4	100000	Point-to-Point	Disabled	Disabled
5	Enabled	Discarding	0	0	32768.001A7EABFD12	128.5	100000	Point-to-Point	Disabled	Disabled

3.7.6 MSTP 設定

MSTP は各インスタンスに対し特定のスパニングツリーを生成します。これによりネットワーク上に複数のパスを構築し、通信のロードバランスを行い、単一のインスタンスに不具合が発生した場合に大規模なネットワークの障害が発生することを回避すると共に、不具合の発生したインスタンスの新しいトポロジーへの変更を迅速に行ないます。

初期設定ではすべての VLAN は、MST 内に接続されたブリッジおよび LAN はすべて内部スパニング・ツリー (MST インスタンス 0) に割り当てられます。

本機では最大 32 のインスタンスをサポートしています。ネットワークの同一エリアをカバーする VLAN をグループ化するように設定して下さい。

但し、同一インスタンスのセットにより同一 MSTI 内のすべてのブリッジ、及び同一 VLAN のセットにより同一インスタンスを形成する必要があります。RSTP は単一ノードとして各 MSTI を扱い、すべての MSTI を Common Spanning Tree として接続する点に注意して下さい。

MSTP を使用するには以下の手順で設定を行なってください。

- (1) スパニングツリータイプを MSTP に設定します (P118 「グローバル設定」参照)
- (2) 選択した MST インスタンスにスパニングツリープライオリティを入力します。
- (3) MSTI を共有する VLAN を追加します。

[注意] すべての VLAN は自動的に IST (インスタンス 0) に追加されます。

MSTI をネットワーク上で有効にし、接続を継続するためには、同様の設定を関連するブリッジにおいて行なう必要があります。

設定・表示項目

MST ID

設定のためのインスタンス ID (設定範囲: 0-4094)

VLAN ID

MST インスタンスに指定する VLAN ID (設定範囲: 1-4093)

Priority

スパニングツリーインスタンスのプライオリティ (範囲: 4096 飛ばしの値で 0-61440、選択肢: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440、初期設定: 32768)

設定方法

MSTP インスタンスの作成

- (1) [Spanning Tree] → [MSTP] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) MST インスタンスと初期 VLAN メンバーを指定します。メンバーの追加は panning Tree > MSTP(Configure Global - Add Member) ページで行うことができます。プライオリティを指定しない場合、初期値の 32768 が使用されます。
- (5) < Apply > をクリックします。

Spanning Tree > MSTP

Step: 1. Configure Global Action: Add

MST ID (0-4094)

VLAN ID (1-4093)

Priority (0-61440, in steps of 4096)

Apply Revert

設定方法

MSTP インスタンスの表示

- (1) [Spanning Tree] → [MSTP] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Show Information」を選択します。表示項目の解説は P122 「グローバル設定の表示」を参照してください。

Spanning Tree > MSTP

Step: 1. Configure Global Action: Show Information

MST ID 0

Priority	32768	Designated Root	32768.0.001A7EABFD12
Bridge ID	32768.0.001A7EABFD12	Root Port	0
Max Age	20 sec sec	Root Path Cost	0
Hello Time	2 sec sec	Configuration Changes	0 sec
Forward Delay	15 sec	Last Topology Change	0 hrs 1 mins 31 seconds

MSTP インスタンスへ VLAN グループを追加

- (1) [Spanning Tree] → [MSTP] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Add Member」を選択します。
- (4) MST ID リストから MST インスタンスを選択します。
- (5) 「VLAN ID」フィールドへ、インスタンスへ追加する VLAN グループの VLAN ID を入力します。
- (6) < Apply > をクリックします。

Spanning Tree > MSTP

Step: 1. Configure Global Action: Add Member

MST ID 1

VLAN ID (1-4093) 2

Apply Revert

MSTP インスタンスの LAN メンバーを表示

- (1) [Spanning Tree] → [MSTP] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Show Member」を選択します。

Spanning Tree > MSTP

Step: 1. Configure Global Action: Show Member

MST ID 1

Member List Max: 4093 Total: 2

☐	VLAN
☐	1
☐	2

Delete Revert

3.7.7 MSTP インタフェースの設定

Spanning Tree > MSTP (Configure Interface - Configure) ページにて、MST インスタンスへの STA インタフェースの設定を行なうことができます。

設定・表示項目

MST Instance ID

設定を行うインスタンス ID（初期設定：0）

Interface

ポートまたはトランクリストの表示

STA Status

スパニングツリー内での各ポートの現在の状態を表示します：

（詳細は 126 ページの「インタフェース設定の表示」を参照して下さい）

- － Discarding — STP 設定メッセージを受信しますが、パケットの送信は行っていない。
- － Learning — 矛盾した情報を受信することなく、Forward Delay で設定した間隔で設定メッセージを送信しています。ポートアドレステーブルはクリアされ、アドレスの学習が開始されています。
- － Forwarding — パケットの転送が行われ、アドレスの学習が継続されています。

Priority

STP での各ポートのプライオリティを設定します。

本機の全てのポートのパスコストが同じ場合には、最も高いプライオリティ（最も低い設定値）がスパニングツリーのアクティブなリンクとなります。これにより、STP においてネットワークのループを回避する場合に、高いプライオリティのポートが使用されるようになります。2 つ以上のポートが最も高いプライオリティの場合には、ポート番号が小さいポートが有効印となります（初期設定：128、範囲：0-240 の 16 ずつ）

Admin MST Path Cost

このパラメータは MSTP においてデバイス間での最適なパスを決定するために設定します。低い値がスピードの早いメディアのポートに割り当てられ、より高い値がより遅いメディアに割り当てられる必要があります（パスコストはポートプライオリティより優先されます）

- －推奨設定範囲：P124 の表を参照してください。
- －推奨設定値：P124 の表を参照してください。
- －初期設定：P124 の表を参照してください。

設定方法

ポートまたはトランクの MSTP パラメータを設定。

- (1) [Spanning Tree] → [MSTP] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Configure」を選択します。
- (4) インタフェースのプライオリティとパスコストを入力します。
- (5) < Apply > をクリックします。

Spanning Tree > MSTP

Step: 2. Configure Interface Action: Configure

MST ID 0

Interface ☒ Port ☐ Trunk

Spanning Tree Port List Max: 26 Total: 26

Port	STA Status	Priority (0-240, in steps of 16)	Admin MST Path Cost (0-200000000, 0: Auto)
1	Forwarding	128	0
2	Discarding	128	0
3	Discarding	128	0
4	Discarding	128	0
5	Discarding	128	0

ポートまたはトランクの MSTP パラメータを表示。

- (1) [Spanning Tree] → [MSTP] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Show Information」を選択します。

Spanning Tree > MSTP

Step: 2. Configure Interface Action: Show Information

MST ID 0

Interface ☒ Port ☐ Trunk

Spanning Tree Port List Max: 26 Total: 26

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Forwarding	2	0	32768.0.001A7EABFD12	128.1	100000	Point-to-Point	Disabled	Designated
2	Discarding	0	0	32768.0.001A7EABFD12	128.2	100000	Point-to-Point	Disabled	Disabled
3	Discarding	0	0	32768.0.001A7EABFD12	128.3	100000	Point-to-Point	Disabled	Disabled
4	Discarding	0	0	32768.0.001A7EABFD12	128.4	100000	Point-to-Point	Disabled	Disabled
5	Discarding	0	0	32768.0.001A7EABFD12	128.5	100000	Point-to-Point	Disabled	Disabled

3.8 帯域制御

帯域制御機能では各インタフェースの送信及び受信の最大速度を設定することができます。帯域制御を有効にすると、通信はハードウェアにより監視され、設定を超える通信はドロップされます。設定範囲内の通信はそのまま転送されます。

設定・表示項目

Port

ポート番号

Type

ポートタイプ (100Base-TX、1000Base-T、SFP)

Status

帯域制御の有効 / 無効 (初期設定：無効)

Rate

帯域制御のレベルを設定

(範囲：Fast Ethernet 64 - 100,000 kilobits/ 秒 Gigabit Ethernet 64-1,000,000 kilobits/ 秒)

設定方法

- (1) [Traffic] → [Rate Limit] をクリックします。
- (2) 設定をおこなうポートの「Rate Limit Status」を有効にします。
- (3) 個々のポートへ「Rate」を設定します。
- (4) < Apply > をクリックします。

Traffic > Rate Limit					
Port Rate Limit List Max: 26 Total: 26					
Port	Type	Input		Output	
		Status	Rate (kbits/sec)	Status	Rate (kbits/sec)
1	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	100000 (64-100000)
2	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	100000 (64-100000)
3	100Base-TX	☐ Enabled	64 (64-100000)	☒ Enabled	100 (64-100000)
4	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	100000 (64-100000)
5	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	100000 (64-100000)

3.8.1 ストームコントロール

Traffic > Storm Control ページを使用し、ブロードキャストストームしきい値コントロールの設定が可能です。ブロードキャストストームは、ネットワーク上の装置が誤動作を起こすか、アプリケーションプログラムの不具合または適切に設定されていない時に発生します。ネットワーク上に過度のブロードキャストトラフィックが存在する場合、パフォーマンスは著しく落ちます。

ブロードキャストトラフィックのしきい値を設定することで、ブロードキャストストームからネットワークを保護することが可能です。指定したしきい値を超えたブロードキャストパケットは破棄されます。

機能解説

- ・ブロードキャストストームコントロールは初期設定で有効になっています。
- ・ブロードキャストコントロールは IP マルチキャストトラフィックに影響しません。

設定・表示項目

Interface

ポートまたはトランクのリストを表示。

Type

インタフェースタイプ (100Base-TX、100Base-T、SFP)

Unknown Unicast

未知のユニキャストトラフィックのストームコントロールを指定

Multicast

マルチキャストトラフィックのストームコントロールを指定

Broadcast

ブロードキャストトラフィックのストームコントロールを指定

Status

ストームコントロールの有効 / 無効 (初期設定: ブロードキャストストームコントロール有効、マルチキャスト / 未知のユニキャストストームコントロール無効)

Rate

レートとしてのしきい値 (パケット / 秒。範囲: 64-1,000,000 Kbits / 秒)

初期設定: 64 Kbits/second)

[注意] 1 つのレートのみ、インタフェース上の全てのトラフィックタイプでサポートされます。

設定方法

- (1) [Traffic] → [Storm Control] をクリックします。
- (2) しきい値を設定し、任意のポートの "Enable" フィールドへチェックを入れます。
- (3) [Apply] をクリックして下さい。

Traffic > Storm Control

Interface ☒ Port ☐ Trunk

Port Storm Control List Max: 26 Total: 26

1 2 3

Port	Type	Unknown Unicast		Multicast		Broadcast	
		Status	Rate (kbits/sec)	Status	Rate (kbits/sec)	Status	Rate (kbits/sec)
1	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	64 (64-100000)	☒ Enabled	64 (64-100000)
2	100Base-TX	☒ Enabled	128 (64-100000)	☐ Enabled	128 (64-100000)	☒ Enabled	128 (64-100000)
3	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	64 (64-100000)	☒ Enabled	64 (64-100000)
4	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	64 (64-100000)	☒ Enabled	64 (64-100000)
5	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	64 (64-100000)	☒ Enabled	64 (64-100000)

3.9 Class of Service (CoS)

Class of Service(CoS) は、ネットワークの混雑状態のために通信がバッファされる場合に、優先するデータパケットを指定することができます。本機では各ポートで 4 段階のキューの CoS をサポートしています。高いプライオリティのキューを持ったデータパケットを、より低いプライオリティのキューを持ったデータパケットよりも先に転送します。各インタフェースにデフォルトプライオリティを設定することができ、又本機のプライオリティキューに対し、フレームプライオリティタグのマッピングを行うことができます。

3.9.1 レイヤ 2 キュー設定

タグ無しフレームのデフォルトプライオリティ設定、キューモードの設定、それぞれのキューへのウェイトの割り当て等について解説します

インタフェースへのデフォルトプライオリティの設定

各インタフェースのデフォルトポートプライオリティを指定することが出来ます。スイッチへ入る全てのタグなしパケットは指定されたデフォルトポートプライオリティによりタグが付けられ、出力ポートでの適切なプライオリティキューが設定されます。

機能解説

- ・ 本機は各ポートで 4 つのプライオリティキューを提供します。head-of-queue blockage を防止するために重み付けラウンドロビン (WRR) を使用します。
- ・ デフォルトプライオリティは、"accept all frame type" に設定されたポートで受信したタグなしフレームの場合に適用されます。このプライオリティは IEEE 802.1Q VLAN タグ付フレームに対応していません。受信フレームが IEEE 802.1Q VLAN タグ付フレームの場合、IEEE 802.1Q VLAN User Priority ビットが使用されます。
- ・ 出力ポートが関連 VLAN のタグ無しメンバーの場合、これらのフレームは送信前に全ての VLAN タグを外します。

設定・表示項目

Interface

ポートまたはトランクのリストを表示。

CoS

指定されたインタフェースで受信されるタグ無しフレームに割り当てられるプライオリティ。(範囲：0-7 初期設定：0)

設定方法

- (1) [Traffic] → [Priority] → [Default Priority] をクリックします。
- (2) 表示するインタフェースのタイプを選択します。(ポートまたはトランク)
- (3) 各インタフェースのデフォルトプライオリティを編集します。
- (4) < Apply > をクリックします。

Traffic > Priority > Default Priority

Interface ☒ Port ☐ Trunk

Port to CoS Mapping Table Max: 26 Total: 26 1 2 3

Port	CoS (0-7)
1	0
2	0
3	0
4	0
5	0

キューモードの選択

本機では、すべての高プライオリティキューが低プライオリティキューに優先される strict ルール、又は各キューの重み付けを行う Weighted Round-Robin (WRR) を用いてキューイングを行います。WRR では、あらかじめ設定した重みに応じて各キューの転送時間の割合を決定します。それにより、Strict ルールによって生じる HOL Blocking を防ぐことができます。

機能解説

- Strict プライオリティははより高いプライオリティキューのすべてのトラフィックが、より低いキューがサービスされる前に処理されることを必要とします。
- 本機で使用されている WRR アルゴリズムは Shaped Deficit Weighted Round Robin (SDWRR) として知られています。
- 基本 WRR アルゴリズムはそれぞれのキューに、次のキューに映る前にスイッチが個々のキューを処理する、サービス時間のパーセンテージを決定する相対荷重を使います。これは strict priority キューイングで発生する head-of-line blocking を防ぎます。
- Strict および WRR モードが選択されている時、Strict サービスの組合せが高いプライオリティキューに使われ、残りのキューのサービスを加重します。
- 指定されたキューモードは全てのインタフェースに適用されます。

設定・表示項目

Queue Mode

- Strict
イングレスキューを順次処理します。すべての高プライオリティキューのトラフィックが低プライオリティキューのトラフィックより優先的に処理されます。
- WRR (SDWRR)
エグレスポートの帯域をスケジューリングウェイトを使用して共有し、Round-Robin 方式でそれぞれのキューを処理します。
- Strict and WRR
高プライオリティキューには Strict プライオリティを使用し、その他には SDWW を使用します。(初期設定)

Queue ID

プライオリティキューの ID (範囲：0-7)

Strict Mode

“Strict and WRR”モードが選択されている場合、Strict サービスの組合せが高いプライオリティキューに使用され、残りのキューのサービスを加重します。。"strict weighted queuing" モードが使用されている時、このパラメータは Strict プライオリティを使用するよう割り当てられたキューを指定するために使用します。(初期設定：無効)

Weight

SDWRR スケジューラで使用される、それぞれのキューにウェイトを設定 (範囲：1-255)
初期設定：Weights 1, 2, 4, 6 がキュー 0-3 へそれぞれ割り当てられます。

設定方法

キューモードの設定 (Strict)

- (1) [Traffic] → [Priority] → [Queue] をクリックします。
- (2) キューモードを設定します。
- (3) 設定の編集を行います。
- (4) < Apply > をクリックします。

Traffic > Priority > Queue

Queue Mode

キューモードの設定 (WRR)

Traffic > Priority > Queue

Queue Mode

Queue Setting Table Max: 4 Total: 4

Queue ID	Weight (1-255) in ascending order
0	1
1	2
2	4
3	6

キューモードの設定 (Strict and WRR)

Traffic > Priority > Queue

Queue Mode

Queue Setting Table Max: 4 Total: 4

Queue ID	Strict Mode	Weight (1-255) in ascending order
0	Disabled	1
1	Disabled	2
2	Disabled	4
3	Enabled	6

Egress キューへの CoS 値のマッピング

本機は各ポートの 8 つのプライオリティキューを使用することによる CoS プライオリティタグ付通信の処理を、重み付けラウンドロビン (Weighted Round Robin/WRR) に基づいたサービススケジュールにより行います。

最大 8 つに分けられた通信プライオリティは IEEE802.1p で定められます。デフォルトプライオリティレベルは次の表に記載されている IEEE802.1p の勧告に基づいて割り当てられています。

プライオリティ	0	1	2	3	4	5	6	7
キュー	1	0	0	1	2	2	3	3

様々なネットワークアプリケーションの IEEE 802.1p 標準で推奨されたプライオリティレベルが以下の表に記載されています。しかし、アプリケーションの通信に対して、自由にアウトプットキューのプライオリティレベルを設定することが可能です。

プライオリティレベル	トラフィックタイプ
1	Background
2	(Spare)
0 (初期設定)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

機能解説

- 出力パケットは、このコマンドによって定義されたマッピングに従って、ハードウェアキューの中へ置かれます。
- 初期設定の内部 PHB から出力キューへのマッピングは以下です。

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	1	0	0	1	2	2	3	3

- 指定されたマッピングは全てのインタフェースへ適用されます。

設定・表示項目

PHB

Per-hop behavior またはこのルータホップで使用されるプライオリティ (範囲：0-7、7 は最高プライオリティ)

Queue

出力キューバッファ (範囲：0-3、3 は最高 CoS プライオリティキュー)

設定方法

内部 PHB をハードウェアキューへマップ

- (1) [Traffic] → [Priority] → [PHB] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) "PHB" と "Queue" を入力し、< Apply >をクリックします。

Traffic > Priority > PHB to Queue

Action:

PHB (0-7)

Queue (0-3)

内部 PHB のハードウェアキューへのマップを表示

- (1) [Traffic] → [Priority] → [PHB to Queue] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。
- (3) インタフェースを選択します。

Traffic > Priority > PHB to Queue

Action:

PHB to Queue Mapping List Max: 8 Total: 8

☐	PHB	Queue
☐	0	1
☐	1	0
☐	2	0
☐	3	1
☐	4	2
☐	5	2
☐	6	3
☐	7	3

3.9.2 レイヤ 3/4 プライオリティの設定

CoS 値へのレイヤ 3/4 プライオリティのマッピング

本機はアプリケーションの要求を満たすため、レイヤ 3/4 プライオリティをサポートしています。通信プライオリティは Type of Service (ToS) オクテットのプライオリティビットや TCP ポート番号を使用しフレームの IP ヘッダで指定します。プライオリティビットを使用する場合、ToS オクテットは Differentiated Services Code Point(DSCP) サービスの 6 ビットを使用します。これらのサービスが有効な時、プライオリティは CoS 値へマッピングされ、該当する出力キューへ送られます。

[注意] 入力トラフィックから内部 DSCP 値へのマッピングプライオリティ値で使用されるデフォルト設定は、出力トラフィックで使われるハードウェアキューを決定するために使用され、プライオリティ値は置き換えません。これらの初期設定は大多数のネットワークアプリケーションのためのプライオリティサービスを最適化することを意図しています。特定のアプリケーションでキューの問題が発生しない限り、デフォルト設定を修正する必要はありません。

優先処理を DSCP または CoS へ設定

本機は DSCP または CoS プライオリティ処理メソッドのいずれかを選択して使用することが可能です。Priority > Trust Mode ページで必要なプロセッシングメソッドを選択します。

機能解説

- QoS マッピングモードが DSCP に設定されており、入力パケットタイプが IPv4 の場合、プライオリティ処理は入力パケットの DSCP 値を基にします。
- QoS マッピングモードが DSCP に設定されており、IP 以外のパケットが受信された場合、タグ付きの場合、パケットの CoS と CFI (Canonical Format Indicator) 値はプライオリティプロセッシングに使用されます。タグ無しパケットの場合、プライオリティ処理にはデフォルトポートプライオリティが使用されます。
- QoS マッピングモードが CoS に設定されており、入力パケットタイプが IPv4 の場合、プライオリティ処理は入力パケットの CoS と CFI 値を基にします。タグ無しパケットの場合、プライオリティ処理にはデフォルトポートプライオリティが使用されます。

設定・表示項目

Interface

ポートまたはトランクを指定。

Trust Mode

- － DSCP － Differentiated Services Code Point (DSCP) 値を使用してレイヤ 3/4 プライオリティをマップします。
- － CoS － Class of Service 値を使用してレイヤ 3/4 プライオリティをマップします。(初期設定)

設定方法

- (1) [Traffic] → [Priority] → [Trust Mode] をクリックします。
- (2) 表示するインタフェースタイプを選択します。(ポートまたはトランク)
- (3) 「Trust Mode」を設定します。
- (4) < Apply > をクリックします。

Traffic > Priority > Trust Mode

Interface ☒ Port ☐ Trunk

DSCP Trust Mode List Max: 26 Total: 26 1 2 3

Port	Trust Mode
1	CoS ▼
2	DSCP ▼
3	DSCP ▼
4	DSCP ▼
5	DSCP ▼

イングレス DSCP 値を内部 DSCP 値へマッピング

Traffic > Priority > DSCP to DSCP ページを使用して、入力パケットの DSCP 値を内部プライオリティ処理の per-hop behavior と drop precedence 値にマップします。

DSCP は 6 ビットで最大 64 個の異なった転送動作が可能です。DSCP は ToS ビットと置き換えることができ先行 3 ビットを使用して下位互換性を維持するので、DSCP 非対応で ToS 対応のデバイスは DSCP マッピングを使用することができます。DSCP では、ネットワークポリシーに基づき、異なる種類のトラフィックを異なる種類の転送とすることができます。

機能解説

- ・ プライオリティマッピングモードが DSCP にセットされており、入力パケットのタイプが IPv4 の時のみ使用出来ます。
- ・ バッファが 0x60 パケットで一杯になった時、Random Early Detection が黄と赤のパケットのドロップを開始し、バッファが 0x80 パケット一杯になった時には色に関係なく全てのパケットもドロップします。
- ・ 指定されたマッピングは全てのインタフェースに適用されます。

設定・表示項目

DSCP

イングレスパケットの DSCP 値 (範囲：0-63)

PHB

Per-hop behavior またはこのルータホップで使用されるプライオリティ (範囲：0-7)

Drop Precedence

トラフィック輻輳コントロールの Random Early Detection に使用されます。(範囲：0- 緑、3- 黄、1- 赤)

DSCP 値から内部 PHB/ ドロップ Precedence へのデフォルトマッピング

ingress-dscp1 ingress-dscp10	0	1	2	3	4	5	6	7	8	9
0	0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1	1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2	2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3,0	3,1
3	3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4,0	4,3
4	5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5	6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7,0	7,3
6	7,0	7,1	7,0	7,3						

* 入力 DSCP は ingress-dscp10 (左側の最も重要な列) と ingress-dscp1 (一番上の列 ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1) で構成されており、テーブルの重なるセルに対応する内部 DSCP を見れます。入力 DSCP はドロップ Precedence を決定するために、2 進法の 11 で ANDed を取られるビットワイズです。

設定方法

DSCP 値を内部 PHB/drop precedence ハマップ

- (1) [Traffic] → [Priority] → [DSCP to DSCP] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) DSCP 値の PHB と drop precedence を設定します。
- (4) < Apply > をクリックします。

Traffic > Priority > DSCP to DSCP

Action: Add ▼

DSCP (0-63) 1

PHB (0-7) 3

Drop Precedence 1: Red ▼

Apply Revert

DSCP 値の内部 PHB/drop precedence へのマップを表示

- (1) [Traffic] → [Priority] → [DSCP to DSCP] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

Traffic > Priority > DSCP to DSCP

Action: Show ▼

DSCP to DSCP Mapping List Max: 64 Total: 64 1 2 3 4 5 6 7

☐	DSCP	PHB	Drop Precedence
☐	0	0	0
☐	1	0	1
☐	2	0	0
☐	3	0	3
☐	4	0	0
☐	5	0	1

CoS プライオリティを内部 DSCP 値へマッピング

Traffic > Priority > CoS to DSCP ページを使用し、入力パケットの CoS/CFI 値を、プライオリティ処理の per-hop behavior と drop precedence 値へマップします。

機能解説

- CoS から PHB 値へのデフォルトマッピングは表 CoS/CFI から内部 PHB/ ドロップ Precedence へのデフォルトマッピングを参照してください。
- もし 802.1Q ヘッダを持つパケットが到着し、これが IP パケットでない場合、プライオリティを生成し、内部処理の precedence 値をドロップするために、CoS/CFI-to-PHB/Drop Precedence マッピングテーブルが使用されます。オリジナルパケットのプライオリティタグはこのコマンドでは修正されません。
- 内部 DSCP は、パケットが送られるキューを決定する per-hop behavior (PHB) の 3 ビットと、トラフィック輻輳コントロールを行う Random Early Detection (RED) に使用される drop precedence の 2 ビットで構成されています。
- バッファがファーストイーサネットポートで最高 16 パケット、またはギガビットイーサネットでは最高 72 パケットを満たした時、RED は黄と赤のパケットのドロップを開始します。また、バッファがファーストイーサネットポートで最高 58 パケット、またはギガビットイーサネットでは最高 80 パケットを満たした時、色に関係無く全てのパケットのドロップを開始します。
- 指定されたマッピングは全てのインタフェースに適用されます。

設定・表示項目

CoS

入力パケットの CoS 値 (範囲: 0-7)

CFI

Canonical Format Indicator (基準的なフォーマット指標)

このパラメータを "0" にセットすると、フレームで表された MAC アドレス情報が基準的なフォーマットであることを示します。(範囲: 0-1)

PHB

Per-hop behavior またはこのルータホップで使用されるプライオリティ (範囲: 0-7)

Drop Precedence

トラフィック輻輳コントロールの Random Early Detection に使用されます。(範囲: 0- 緑、3- 黄、1- 赤)

CoS/CFI から内部 PHB/ ドロップ Precedence へのデフォルトマッピング

CoS	CFI 0	CFI 1
0	(0,0)	(0,0)
1	(1,0)	(1,0)
2	(2,0)	(2,0)
3	(3,0)	(3,0)
4	(4,0)	(4,0)
5	(5,0)	(5,0)
6	(6,0)	(6,0)
7	(7,0)	(7,0)

入力 DSCP は ingress-dscp10 (左側の最も重要な列) と ingress-dscp1 (一番上の列) ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1 で構成されており、テーブルの重なるセルに対応する内部 DSCP を見れます。入力 DSCP はドロップ Precedence を決定するために、2 進法の 11 で ANDed を取られるビットワイズです。

設定方法

CoS/CFI 値を内部 PHB/drop precedence ハマップ

- (1) [Traffic] → [Priority] → [CoS to DSCP] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) PHB と drop precedence を設定します。
- (4) < Apply > をクリックします。

Traffic > Priority > CoS to DSCP

Action: Add ▼

CoS (0-7)

CFI (0-1)

PHB (0-7)

Drop Precedence

Apply Revert

CoS/CFI 値の内部 PHB/drop precedence へのマップを表示

- (1) [Traffic] → [Priority] → [CoS to DSCP] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。
- (3) インタフェースを選択します。

Traffic > Priority > CoS to DSCP

Action: Show ▼

CoS to DSCP Mapping List Max: 16 Total: 16 1 2

☐	CoS	CFI	PHB	Drop Precedence
☐	0	0	0	0
☐	0	1	0	0
☐	1	0	1	0
☐	1	1	1	0
☐	2	0	2	0
☐	2	1	2	0
☐	3	0	3	0

3.10 Quality of Service

3.10.1 Quality of Service の設定

ここで記載されているコマンドは QoS(Quality of Service) 機能の基準とサービスポリシーを構成するために使用されます。DiffServ(Differentiated Services) 機能は、ネットワーク上を流れるフレームの 1 つの単位を特定のトラフィックの要件に合致させるため、ネットワークリソースを優先する管理機能を提供します。それぞれのパケットはアクセスリスト、IP Precedence、DSCP、VLAN リストをベースにしたネットワークの中のエン트리によって分類されます。アクセスリストを使用することにより、それぞれのパケットが含んでいるレイヤ 2 ～ 4 の情報を元にトラフィックの選別を許可します。設定されたネットワークポリシーをベースにして、異なる種類のトラフィックに対し、異なる種類の転送のためにマークを付けることができます。

インターネットにアクセスするすべてのスイッチとルーターは、同じクラスのパケットには同じ方向への転送を行うためにクラス情報を使用します。クラス情報は、経路の終端のホスト、スイッチ、ルーターのいずれかから割り当てられます。そして、優先度は一般的なポリシー、もしくはパケット詳細調査によって割り当てられます。しかし、パケットの詳細調査はコアスイッチとルーターに負荷がかかり過ぎないようにするため、ネットワークのエッジ側に近いところで行われる必要があります。

経路に属するスイッチとルーターは、異なるクラスにリソースの割り当ての優先順位をつけるため、クラス情報を使用することができます。個々のデバイスが DiffServ 機能に基づいてトラフィックを扱う方法は、Per-Hop Behavior と呼ばれます。経路に属するすべてのデバイスは、エンド・トゥ・エンドの QoS ソリューションを構成するために矛盾のない方法で設定されます。

[注意] クラスマップごとに最大 16 個のルールを設定することができます。ポリシーマップには複数のクラスを設定することもできます。

[注意] ポリシーマップを作成する前にクラスマップを作成してください。作成しない場合、ポリシールールの設定画面からクラスマップを選択することはできません。

機能解説

特定のカテゴリや入力トラフィックのためのサービスポリシーを作成するには、下のステップを実施してください。

- (1) Configure Class (Add) ページを使用して、トラフィックの特定のカテゴリにクラスの名前を設定します。
- (2) Configure Class (Add Rule) ページを使用し、アクセスリスト、DSCP、IP Precedence の値、VLAN に基づいてトラフィックの種類を指定するために、それぞれのクラスのルールを編集します。
- (3) Configure Policy (Add) ページを使用して、入力トラフィックを取り扱う特定の方法のポリシーの名前を設定します。
- (4) Configure Policy (Add Rule) ページを使用し、ポリシーマップに 1 つ、もしくはそれ以上のクラスを追加します。トラフィックに合致するクラスに QoS の値を割り当てるため、setting 画面でそれぞれのクラスにルールを割り当てます。ポリシールールはフローレートとバーストレートの平均の監視、特定のレートを超えたトラフィックの破棄、特定のレートを超えたトラフィックの DSCP サービスレベルを減らすよう構成できます。
- (5) Configure Interface を使用して、特定のインターフェースにポリシーマップを割り当てます。

クラスマップの設定

クラスマップが指定されたクラスにパケットをマッチさせるために使用します。Traffic > DiffServ (Configure Class) ページを使用し、クラスマップの設定を行います。

機能解説

- クラスマップはポリシーマップで、パケット分類。サービスタギング、バンドワイズポリッシングを定義する特定のインタフェースのために、サービスポリシーを作成するために使用されます。
- 最大 32 のクラスマップを設定できます。

設定・表示項目

Add

Class Name

クラスマップ名（範囲：1-16 文字）

Type

タイプを指定します。

Description

クラスマップの簡単な説明（範囲：1-64 文字）

Add Rule

Class Name

クラスマップ名。

Type

タイプを指定します。

ACL List

ACL リスト名。

IP DSCP

IP DSCP 値（範囲：0-63）

IP Precedence

IP Precedence 値（範囲：0-7）

VLAN ID

VLAN（範囲：1-4093）

設定方法

クラスマップを設定

- (1) [Traffic] → [DiffServ] をクリックします。
- (2) 「Step」 リストから「Configure Class」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) "Class name" を入力します。
- (5) "Description" を入力します。
- (6) < Apply >をクリックします。

Traffic > DiffServ

Step: 1. Configure Class ▼ Action: Add ▼

Class Name:

Type: Match Any ▼

Description:

Apply Revert

設定したクラスマップを表示

- (1) [Traffic] → [DiffServ] をクリックします。
- (2) 「Step」 リストから「Configure Class」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Traffic > DiffServ

Step: 1. Configure Class ▼ Action: Show ▼

Class List Max: 32 Total: 1

☐	Class Name	Type	Description
☐	rd-class	Match Any	class of software group

Delete Revert

クラスマップのルールを編集

- (1) [Traffic] → [DiffServ] をクリックします。
- (2) 「Step」 リストから「Configure Class」を選択します。
- (3) 「Action」 リストから「Add Rule」を選択します。
- (4) クラスマップを選択します。
- (5) アクセスリスト DSCP または IP Precedence 値、VLAN に基づき、このクラスのトラフィックタイプを指定します。入力トラフィックをクラスマップに割り当て時、最大 16 アイテムを指定できます。
- (6) < Apply > をクリックします。

Traffic > DiffServ

Step: 1. Configure Class Action: Add Rule

Class Name: rd-class

Type: Match Any

Rule:

☐ ACL

☒ IP DSCP (0-63) 3

☐ IP Precedence (0-7)

☐ VLAN ID (1-4093)

Apply Revert

クラスマップのルールを表示

- (1) [Traffic] → [DiffServ] をクリックします。
- (2) 「Step」 リストから「Configure Class」を選択します。
- (3) 「Action」 リストから「Show Rule」を選択します。

Traffic > DiffServ

Step: 1. Configure Class Action: Show Rule

Class Name: rd-class

Type: Match Any

Rule List Max: 16 Total: 2

	Rule
☐	IP DSCP 3
☐	IP Precedence 3

Delete Revert

QoS ポリシーの作成

Traffic > DiffServ (Configure Policy) ページを使用し、複数のインタフェースを付加できるポリシーマップを作成します。

ポリシーマップは、1 つ以上のクラスマップステートメントの分類、サービスタグの修正、バンドワイズポリッシングに使用されます。

QoS ポリシーの設定にはいくつかの段階が必要です。

最初に、アクセスリスト、DSCP または IP Precedence 値または指定した VLAN のメンバーに従って、インバウンドパケットと一致する方法を示す class map の設定を行います。

次にインバウンドトラフィックのモニタリングに使用される境界パラメータを示す、ポリシーマップを設定し、順応と不適合なトラフィックにたいして取る行動を設定します。

ポリシーマップはあらかじめ作成したクラスマップの定義を基にし、1 つまたはそれ以上のクラスを含みます。

class of service または per-hop behavior (内部キュー処理に使用されるプライオリティ) はマッチするパケットに割り当てられます。加えて、インバウンドトラフィックのフローレートは監視されることが可能で、以下に解説する 3 つの異なるポリッシングメソッドの内 1 つを基にした順応と不適合なトラフィックへ返答します。

Police Flow Meter — 確約する情報レートを明確にし、(最大スループット) バーストサイズを確約し、(burst rate) 順応と不適合トラフィックにたいして取るべき行動を定義します。

srTCM Police Meter — RFC2697 で定義された、単速度三色パケットマーカ (srTCM) 方式に基づき、分類されたトラフィックされたトラフィックの施工を定義します。

srTCM はトラフィックをモニタし、committed information rate (CIR または最大スループット)、committed burst size (BC またはバーストレート)、excess burst size (BE) に従いパケットを処理します。

- PHB ラベルは per-hop behavior の 3 ビットとコントロールキュー輻輳で使用されるクラススキーマの 2 ビットの 5 ビットで構成されます。送信、DSCP サービス値のリマーク、またはパケットの破棄を行うこのコマンドに定義されたアクションに加え、スイッチは Random Early Detection パケットのドロップ Precedence のセットに仕様される 2 つのカラービットをマークします。
コミットされた情報レートとバーストサイズを超えない場合、パケットは緑にマークされます。コミットされた情報レートとバーストサイズを越えた場合、パケットは黄にマークされ、その他は赤にマークされます。
- メータは 2 つの内 1 つのモードで動作します。カラーバインドモードでは、パケットにマーキング (色付け) がされていないとみなします。カラーアウェアモードでは、あらかじめ何らかの前段の存在がパケットにマーキング (色付け) をしているとみなします。(パケットは既に緑・黄色・赤のいずれかである)
IP パケットのマーカー (再) 色付けはメータの結果に従います。カラーはパケットの DS フィールド (RFC2474) でコード化されます。
- メータのふるまいは、動作モードと、共通のレート CIR を共有する C と E のふたつのトークンパケツで規定されます。C の最大値は BS、E の最大値は BE です。
C と E は時刻 0 では、満杯です ($T_c(0)=BC$ 、 $T_e(0)=BE$)。
その後は以下のように毎秒 CIR 回ずつ更新されます。
 - T_c が BC より小さければひとつだけ増加される。
 - T_e が BE より小さければひとつだけ増加される。
 - T_c も T_e も増やされない。

- 時刻 t に B バイトのパケットが到着したら、パケットカラーバインドモードの場合は以下のように動作します：
 - $Tc(t)-B$ が 0 以上ならパケットは緑色にされ、 Tc が B だけ減少する (Tc の最低値は 0)
 - $Te(t)-B$ が 0 以上ならパケットは黄色にされ、 Te が B だけ減少する (Te の最低値は 0)
 - パケットは赤色にされ、 Tc も Te も減少しない
- 時刻 t に B バイトのパケットが到着したら、カラーアウェアモードの場合は以下のように動作します：
 - パケットが予め緑色であり、かつ $Tc(t)-B$ が 0 以上ならパケットは緑色にされ Tc が B だけ減らされる (Tc の最低値は 0)
 - パケットが予め緑色または黄色であり、 $Te(t)-B$ が 0 以上ならパケットは黄色にされ、 Te が B だけ減らされる (Te の最低値は 0)
 - パケットは赤色にされ、 Tc も Te も減らされない。

trTCM Police Meter — RFC2698 で定義された、二速度三色パケットマーカ (srTCM) 方式に基づき、分類されたトラフィックの施工を定義します。
trTCM はトラフィックを測定し、CIR または最大スループット、RIP、関連するバーストサイズに基づいてパケットを緑・黄色・赤に色付けします。

- PHB ラベルは per-hop behavior の 3 ビットとコントロールキュー輻輳で使用されるクラススキーマの 2 ビットの 5 ビットで構成されます。
送信、DSCP サービス値のリマーク、またはパケットの破棄を行うこのコマンドに定義されたアクションに加え、スイッチはまた、Random Early Detection パケットのドロップ Precedence のセットに仕様される 2 つのカラービットをマークします。
PIR を越えていれば赤であり、そうでなければ CIR を越えているかないかによって緑か黄色になります。
- メータは次の二つのモードのうちどちらかで動作します。カラーバインドモードではパケットにマーキング (色付け) がされていないとみなし、カラーアウェアモードではあらかじめ何らかの前段の存在がパケットにマーキング (色付け) をしているとみなします。(パケットは既に緑・黄色・赤のいずれか)。
- メータのふるまいは、モードの基準と、RIP と CIR を基にした P と C のふたつのトークンバケツで指定されます。 P の最大値は BP 、 C の最大値は BC です。
 P と C は時刻 0 では、満杯です ($Tp(0)=BP$ 、 $Tc(0)=BC$)。
その後 Tp は BP まで毎秒 $1RIP$ ずつ BP まで増加し、トークンカウント Tc は毎秒 $1CIR$ ずつ Bc まで増加します。
時刻 t に B バイトのパケットが到着したら、パケットカラーバインドモードの場合は以下のように動作します：
 - $Tp(t)-B$ が 0 より小さければパケットは赤に色付けされます。
 - $Tc(t)-B$ が 0 より小さければパケットは黄に色付けされ、 B によって減少します。
 - Tp と Tc の両方が B によって減少する場合、パケットは緑に色付けされます。
- 時刻 t に B バイトのパケットが到着したら、パケットカラーアウェアモードの場合は以下のように動作します：
 - $Tp(t)-B$ が 0 以下ならパケットは赤に色付けされます。
 - $Tc(t)-B$ が 0 以下ならパケットは黄に色付けされます。
 - Tp と Tc の両方が B によって減少する場合、パケットは緑に色付けされます。

Random Early Detection –バッファが 0 × 60 パケット一杯になった時、RED は黄と赤のパケットのドロップを開始し、0x80 パケットが一杯になった時、色に関わらず全てのパケットをドロップし始めます。

機能解説

- ・ ポリシーマップは同じインタフェースに適用できる 16 のクラスステートメントを含むことが可能です。(P158) 入力ポートに最大 32 のポリシーマップを設定できます。
- ・ ポリシーマップをパケット分類、サービススタギング、バンドワイズポリッシングの定義に使用した後、サービスポリシー (P158) によって指定のインタフェースにアサインしてください。

設定・表示項目

Add

Policy Name

ポリシー名 (範囲: 1-16 文字)

Description

ポリシーマップの解説 (範囲: 1-256 文字)

Add Rule

Policy Name

ポリシーマップの名前 (範囲: 1-16 文字)

Class Name

ポリシーが作用するトラフィック分類を定義したクラスマップの名前

Action

この属性はマッチングパケット用のハードウェアの内部 QoS 値を設定するために使用します。

PHB ラベルは 5 ビットで構成され、3 ビットは per-hop behavior、2 ビットは srTCM、trTCM メータリング機能と共にキュー輻輳をコントロールするために使用されるカラースキームです。

- Set CoS – マッチングパケット (クラスマップのルール設定で指定される) の内部 CoS 値をセットすることによって、入力トラフィックへ提供されるサービスを設定します。(範囲: 0-7)
- Set PHB – マッチングパケット (クラスマップのルール設定で指定される) の内部 per-hop behavior をセットすることによって、入力トラフィックへ提供されるサービスを設定します。(範囲: 0-7)

Meter

最大スループット、バーストレート、ポリシー違反の結果となるアクションを定義するためにチェックします。

Meter Mode

以下のポリッシングメソッドのいずれかを選択します。

- Flow (Police Flow) - committed information rate (CIR または最大スループット)、committed burst size (BC またはバーストレート)、適合と不適合トラフィックに対して取るアクションを定義します。

- Committed Information Rate (CIR) – レートを指定。(範囲: 64kbps の精度または最大ポートスピードで 64-10000000 kbps)
レートは設定されたインタフェーススピードを越えられません。
 - Committed Burst Size (BC) – バーストサイズを指定。(範囲: 4k バイトの精度で 4000-16000000)
バーストサイズは 16Mbytes を越えられません。
 - Conform – 最大レート (CIR) へ順応するトラフィックが DSCP サービスレベルの変更無しで転送されます。
 - Transmit – 不適合トラフィックが DSCP サービスレベルの変更無しで転送されます。
- Violate – 最大レート (CIR) 越えたトラフィックがドロップされるか、DSCP サービスレベルが減少するかを指定します。
- Set IP DSCP – 適合トラフィック外の DSCP プライオリティを減少 (範囲: 0-63)
 - Drop – 適合トラフィックをドロップします。
- srTCM (Police Meter) – committed information rate (CIR または最大スループット)、committed burst size (BC またはバーストレート)、excess burst size (BE) および最大スループットに適合したトラフィックを定義します。転送、DSCP サービス値のマーク、パケットのドロップを行うこのコマンドによって定義されるアクションに加え、スイッチはまた Random Early Detection のためのパケットのドロップ Precedence に使用される 2 つのカラービットをマークします。
カラーモードにはパケットストリームが色付けされていないと想定する " カラーバインド " と、入力パケットは既に色付けされていると想定する " カラーアウェア " の 2 つがあります。
- Committed Information Rate (CIR) – レートを指定 (範囲: 64kbps の精度または最大ポートスピードで 64-10000000kbps)
レートは設定されたインタフェーススピードを越えられません。
 - Committed Burst Size (BC) – バーストサイズを指定 (範囲: 4kbps の精度で 4000-16000000)
バーストサイズは 16Mbytes を越えられません。
 - Excess Burst Size (BE) – コミットされたバーストサイズを超過したバースト (範囲: 4kbps の精度で 4000-16000000)
バーストサイズは 16Mbytes を越えられません。
 - Conform – 最大レート (CIR) へ順応するトラフィックが DSCP サービスレベルの変更無しで転送されます。
 - Transmit – 不適合トラフィックが DSCP サービスレベルの変更無しで転送されます。
 - Exceed – 最大レート (CIR) を越えたが、超過バーストサイズ内であるトラフィックがドロップさえるか DSCP サービスレベルを減少するかを指定します。
 - Set IP DSCP – 適合トラフィック外の DSCP プライオリティを減少 (範囲: 0-63)
 - Drop – 適合トラフィックをドロップします。
 - Violate – 超過バーストサイズ (BE) を越えたトラフィックがドロップされるか、DSCP サービスレベルが減少するかを指定します。
 - Set IP DSCP – 適合トラフィック外の DSCP プライオリティを減少 (範囲: 0-63)
 - Drop – 適合トラフィックをドロップします。

- － trTCM (Police Meter) － committed information rate (CIR または最大スループット)、peak information rate (PIR)、それらに関するバーストサイズを定義します。－コミットされたバーストサイズ (BC またはバーストレート) と peak information rate (PIR)、トラフィックが最大スループットに適合した時取るアクション、最大スループットを越え、peak information rate (PIR) 内にあるまたは peak information rate (PIR) を超過、等を定義します。このコマンドで定義される、DSCP サービス値のリーマークまたはドロップパケット等に加え、スイッチはまた Random Early Detection のためのパケットのドロップ Precedence に使用される 2 つのカラービットをマークします。

カラーモードにはパケットストリームが色付けされていないと想定する " カラーバインド " と、入力パケットは既に色付けされていると想定する " カラーアウェア " の 2 つがあります。

- Committed Information Rate (CIR) －レートを指定 (範囲: 64kbps の精度または最大ポートスピードで 64-10000000kbps)
- Peak Information Rate (PIR) －レートを指定 (範囲: 64kbps の精度または最大ポートスピードで 64kbps の精度または最大ポートスピードで)
- Committed Burst Size (BC) －バーストサイズを指定 (範囲: 4kbps の精度で 4000-16000000)バーストサイズは 16Mbytes を越えられません。
- Peak Burst Size (BP) －バーストサイズを指定 (範囲: 4kbps の精度で 4000-16000000)バーストサイズは 16Mbytes を越えられません。
- Conform －最大レート (CIR) へ順応するトラフィックが DSCP サービスレベルの変更無しで転送されます。
 - Transmit －不適合トラフィックが DSCP サービスレベルの変更無しで転送されます。
- Exceed －大レート (CIR) を越えたが、peak information rate (PIR) 内であるトラフィックがドロップさえるか DSCP サービスレベルを減少するかを指定します。
 - Set IP DSCP －適合トラフィック外の DSCP プライオリティを減少 (範囲: 0-63)
 - Drop －適合トラフィックをドロップします。
- Violate － peak information rate (PIR) を越えたトラフィックがドロップされるか、DSCP サービスレベルが減少するかを指定します。
 - Set IP DSCP －適合トラフィック外の DSCP プライオリティを減少 (範囲: 0-63)
 - Drop －適合トラフィックをドロップします。

設定方法

ポリシーマップの設定

- (1) [Traffic] → [DiffServ] をクリックします。
- (2) 「Step」 リストから「Configure Policy」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) ポリシー名を入力します。
- (5) 解説を入力します。
- (6) < Add > をクリックします。

Traffic > DiffServ

Step: 2. Configure Policy ▼ Action: Add ▼

Policy Name:

Description:

Apply Revert

ポリシーマップ設定の表示

- (1) [Traffic] → [DiffServ] をクリックします。
- (2) 「Step」 リストから「Configure Policy」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Traffic > DiffServ

Step: 2. Configure Policy ▼ Action: Show ▼

Policy List Max: 32 Total: 1

☐	Policy Name	Description
☐	rd-policy	for the software group

Delete Revert

ポリシーマップのルールを編集

- (1) [Traffic] → [DiffServ] をクリックします。
- (2) 「Step」 リストから「Configure Policy」を選択します。
- (3) 「Action」 リストから「Add Rule」を選択します。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Traffic > DiffServ

Step: 2. Configure Policy Action: Add Rule

Policy Name: rd-policy

Rule:

Class Name: rd-class

Action: Set PHB (0-7) 3

☒ Meter

Meter Mode: Flow

Committed Information Rate (64-1000000): 1000000 kbps

Committed Burst Size (4000-16000000): 4000 bytes

Exceeded Burst Size (4000-16000000): bytes

Peak Information Rate (64-1000000): kbps

Peak Burst Size (4000-16000000): bytes

Conform: Transmit

Exceed: Set IP DSCP (0-63)

Violate: Drop

Apply Revert

ポリシーマップのルールを表示

- (1) [Traffic] → [DiffServ] をクリックします。
- (2) 「Step」 リストから「Configure Policy」を選択します。
- (3) 「Action」 リストから「Show Rule」を選択します。

Traffic > DiffServ

Step: 2. Configure Policy Action: Show Rule

Policy Name: rd-policy

Rule List Max: 128 Total: 1

	Class Name	Action	Meter									
			Meter Mode	Committed Information Rate (kbps)	Committed Burst Size (bytes)	Exceeded Burst Size (bytes)	Peak Information Rate (kbps)	Peak Burst Size (bytes)	Conform	Exceed	Violate	
☐	rd-class	Set CoS 3	Flow	1000000	4000					Transmit		Drop

Delete Revert

ポリシーマップをポートへ適用

ポリシーマップをポートへ適用します。

機能解説

- 最初にクラスマップの定義を行ってください。その後、ポリシーマップの定義を行い、最後にサービスポリシーをインタフェースへ適用します。
- 一つのインタフェースに一つのポリシーをバインド可能です。

設定・表示項目

Port

ポートを指定。

Ingress

入カトラフィックヘルールを適用します。

設定方法

ポリシーマップをポートへバインド

- (1) [Traffic] → [DiffServ] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) ポリシーマップを有効にするポートの、Ingress フィールドのチェックボックスをチェックします。
- (4) スクロールダウンボックスからポリシーマップを選択します。
- (5) < Apply > をクリックします。

Traffic > DiffServ

Step: 3. Configure Interface ▼

Port Service Policy List Max: 26 Total: 26 1 2 3

Port	Ingress
1	☒ rd-policy ▼
2	☐ rd-policy ▼
3	☐ rd-policy ▼
4	☐ rd-policy ▼
5	☐ rd-policy ▼

3.11 VoIP 設定

IP 電話がエンタープライズネットワークに配置される場合、他のデータトラフィックから VoIP ネットワークを分離することを推奨します。トラフィックの分離は極端なパケット到達遅延、パケットロス、ジッターを防ぎ、より高い音声品質を得ることにつながります。これは 1 つの Voice VLAN にすべての VoIP トラフィックを割り当てることで実現できます。

Voice VLAN を使用することにはいくつかの利点があります。他のデータトラフィックから VoIP トラフィックを分離することでセキュリティが保たれます。エンドツーエンドの QoS ポリシーと高い優先度の設定により、ネットワークを横断して VoIP VLAN トラフィックに必要な帯域幅を保証することができます。また、VLAN 分割は音声品質に重大な影響を及ぼすブロードキャストやマルチキャストからトラフィックを保護することができます。

スイッチはネットワーク間で Voice VLAN を設定し、VoIP トラフィックに CoS 値を設定することができます。VoIP トラフィックはパケットの送信先 MAC アドレス、もしくは接続された VoIP デバイスを発見するために LLDP (IEEE802.1AB) を使うことで、スイッチポート上において検出されます。VoIP トラフィックが設定されたポート上で検出されたとき、スイッチは自動的に Voice VLAN のタグメンバーとしてポートを割り当てます。

スイッチポートを手動で設定することもできます。

VoIP トラフィックの設定

VoIP 向けにスイッチを構成するため、最初にスイッチポートに接続された VoIP デバイスの Automatic Detection を有効にし、次にネットワーク中の Voice VLAN の ID を設定します。また Voice VLAN Aging Time は、VoIP トラフィックがポート上で受信されていないとき、Voice VLAN からポートを取り外すために設定します。

設定・表示項目

Auto Detection Status

スイッチポート上で VoIP トラフィックの自動検出を有効にします。(初期設定：無効)

Voice VLAN ID

ネットワーク中の Voice VLAN ID を設定します。1 つの Voice VLAN ID のみサポートします。またその VLAN ID は事前にスイッチ上で作成されていなければ行けません。
(範囲：1-4093)

Voice VLAN Aging Time

Voice VLAN Aging Time…ポート上で VoIP トラフィックが受信されていないとき、ポートが Voice VLAN から取り外されるまでの時間。(範囲：5-43200 秒 初期設定：1440 秒)

[注意] Auto Detection Statusが有効のとき、Voice VLAN IDを設定することができません。

設定方法

- (1) [Traffic] → [VoIP] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) "Auto Detection" を有効にします。
- (4) "Voice VLAN ID" を指定します。
- (5) 必要に応じ、"Voice VLAN Aging Time" を編集します。
- (6) < Apply > をクリックします。

Traffic > VoIP

Step: 1. Configure Global ▼

Auto Detection Status

☒ Enabled

Voice VLAN

1234 ▼

Voice VLAN Aging Time (5-43200)

3000 min

Apply

Revert

テレフォニー OUI の設定

スイッチに接続された VoIP デバイスは、受信したパケットの送信元 MAC アドレスの中の VoIP デバイス製造者の Organizational Unique Identifier (OUI) によって認識されます。OUI 番号は製造者によって割り当てられ、デバイスの MAC アドレスの最初の 3 オクテットを構成します。VoIP デバイスからのトラフィックを VoIP と認識するために、VoIP 機器の MAC アドレスの OUI 番号をスイッチ上で設定することができます。

設定・表示項目

Telephony OUI

リストに追加する MAC アドレスの範囲を指定します。「01-23-45-67-89-AB」というフォーマットで MAC アドレスを入力します。

Mask

VoIP デバイスの MAC アドレスの範囲を確定します。ここで「FF-FF-FF-00-00-00」を設定すると同じ OUI 番号（最初の 3 オクテットが同一）であるすべてのデバイスを VoIP デバイスとして認識します。他の値を指定することで MAC アドレスの範囲を制限することができます。ここで「FF-FF-FF-FF-FF-FF」を選択すると 1 つの MAC アドレスのみ VoIP デバイスとして設定します（初期設定：FF-FF-FF-00-00-00）

Description

VoIP デバイスの内容を説明するテキストを入力します。

設定方法

VoIP 装置の MAC OUI 番号を設定

- (1) [Traffic] → [VoIP] をクリックします。
- (2) 「Step」 リストから「Configure OUI」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) ネットワーク内の VoIP デバイスの OUI を指定する MAC アドレスを入力します。
- (5) MAC アドレス範囲を定義するマスクをプルダウンリストから選択します。
- (6) デバイスの説明を入力します。
- (7) < Apply > をクリックします。

Traffic > VoIP

Step: 2. Configure OUI Action: Add

Telephony OUI

Mask

Description

00-e0-bb-00-00-00

FF-FF-FF-00-00-00

oid phone

Apply Revert

VoIP 装置で使用されるの MAC OUI 番号を表示

- (1) [Traffic] → [VoIP] をクリックします。
- (2) 「Step」 リストから「Configure OUI」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Traffic > VoIP

Step: 2. Configure OUI Action: Show

Telephony OUI List Max: 16 Total: 1

	Telephony OUI	Mask	Description
☐	00-E0-BB-00-00-00	FF-FF-FF-00-00-00	oid phone

Delete Revert

VoIP トラフィックポートの設定

VoIP トラフィックのためにポートを構成するため、モード (Auto か Manual)、VoIP デバイスを発見する方法、トラフィックの優先度を設定する必要があります。また VoIP トラフィックのみ Voice VLAN 上を転送できることを保証するため、セキュリティフィルタを有効にすることができます。

設定・表示項目

Mode

ポートが Voice VLAN に加わった場合、VoIP トラフィックをどの時点で検出するかを設定します (初期設定: None)

- None — ポート上で Voice VLAN 機能は無効になります。ポートは VoIP トラフィックを検出せず、Voice VLAN にも追加されません。
- Auto — ポートが VoIP トラフィックを検出したとき、ポートは Voice VLAN のタグメンバーとして追加されます。VoIP トラフィックを検出する方法を、OUI か 802.1AB のどちらかから選択しなくてははいけません。OUI を選択した場合、Telephony OUI List で MAC アドレスの範囲を確認してください。
- Manual — Voice VLAN 機能はポート上で有効になりますが、ポートは手動で Voice VLAN に追加されます。

Security

ポート上で受信した Voice VLAN ID のタグの付いた非 VoIP パケットを破棄するために、セキュリティフィルタを有効にします。VoIP トラフィックは Telephony OUI List で構成された送信元 MAC アドレス、もしくはスイッチ上で接続された VoIP デバイスを発見する LLDP を通して認証されます。VoIP デバイスではない送信元から受信したパケットは破棄されます

(初期設定: 無効)

Discovery Protocol

ポート上で VoIP トラフィックを検出するために使う方式を選択します。(初期設定: OUI)

- OUI — VoIP デバイスからのトラフィックは送信元 MAC アドレスの Organizationally Unique Identifier (OUI) によって検出されます。OUI 番号は製造者によって割り当てられ、デバイスの MAC アドレスの最初の 3 オクテットを構成します。スイッチが VoIP デバイスからのトラフィックを認識するには、MAC アドレスの OUI 番号を Telephony OUI List で構成しなくてははいけません。
- LLDP — ポートに接続された VoIP デバイス発見するために LLDP を使用します。LLDP は System Capability TLV の中の Telephone Bit が有効であるかどうかをチェックします。LLDP (Link Layer Discovery Protocol) については本マニュアル 256 ページの「LLDP」を参照してください。

Priority

Voice VLAN 上のポートとトラフィックの CoS 優先度を定義します。Voice VLAN 機能がポート上で有効であるとき、受信したすべての VoIP パケットの優先度が新しい優先度で上書きされます。

Remaining Age

このエントリがエイジアウトするまでの秒数

設定方法

- (1) [Traffic] → [VoIP] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) それぞれのポートの VoIP 設定から必要な項目の編集を行います。
- (4) < Apply > をクリックします。

Traffic > VoIP

Step: 3. Configure Interface

VoIP Port List Max: 26 Total: 26

123

Port	Mode	Security	Discovery Protocol	Priority (0-6)	Remaining Age (minutes)
1	None	☐ Enabled	☒ OUI ☐ LLDP	6	NA
2	None	☐ Enabled	☒ OUI ☐ LLDP	6	NA
3	Manual	☒ Enabled	☒ OUI ☐ LLDP	0	NA
4	None	☐ Enabled	☒ OUI ☐ LLDP	6	NA
5	None	☒ Enabled	☒ OUI ☐ LLDP	6	NA

3.12 セキュリティ

本機は、それぞれのデータポートに接続されたクライアントのトラフィックの分離および、認証されたクライアントだけがアクセスを得ることを保証するための多数のメソッドをサポートします。

プライベート VLAN と IEEE802.1x を利用したポートベース認証は、一般的にこれらの目的のために使用されます。これらのメソッドに加え、その他いくつかの提供されているセキュリティのオプションもサポートされています。

[注意] フィルタリングコマンドの実行プライオリティは、ポートセキュリティ、ポート認証、ネットワークアクセス、Web 認証、アクセスコントロールリスト、IP ソースガード、DHCP スヌーピングです。

3.12.1 AAA 許可とアカウントिंग

オーセンティケーション、オーソライゼーション、アカウントिंग (AAA) 機能はスイッチ上でアクセス制御を行うための主要なフレームワークを規定します。この 3 つのセキュリティ機能は下のようによりまとめることができます。

- オーセンティケーション：ネットワークへのアクセスを要求するユーザーを認証します。
- オーソライゼーション：ユーザーが特定のサービスにアクセスできるかどうかを決定します。
- アカウントिंग：ネットワーク上のサービスにアクセスしたユーザーに関する報告、監査、請求を行います。

AAA 機能を使用するにはネットワーク上で RADIUS サーバー、もしくは TACACS+ サーバーを構成することが必要です。セキュリティサーバーはシークエンシャルグループとして定義され、特定のサービスへのユーザーアクセスを制御するために適用されます。例えば、スイッチがユーザーを認証しようと試みた場合、最初にリクエストが定義されたグループ内のサーバーに送信されます。応答がない場合、第 2 のサーバーにリクエストが送信され、さらに応答がない場合、次のサーバーにリクエストが送信されます。どこかの時点で認証が成功するか失敗した場合、プロセスは停止します。

本機は下記の AAA 機能をサポートしています。

- スイッチを通してネットワークにアクセスした IEEE802.1x で認証されたユーザーをアカウントングします。
- コンソールと Telnet を通してスイッチ上の管理インターフェースにアクセスするユーザーをアカウントングします。
- 特定の CLI 特権レベルに入ったユーザーにコマンドをアカウントングします。
- コンソールと Telnet を通してスイッチ上の管理インターフェースにアクセスするユーザーのオーソライゼーションを行います。

スイッチ上の AAA 機能の設定を行うために、下の手順を実行する必要があります。

- (1) RADIUS サーバー、TACACS+ サーバーへアクセスするための値を設定します。
- (2) サービスのアカウントिंग、オーソライゼーション機能をサポートするため、RADIUS サーバーと TACACS+ サーバーのグループを定義します。
- (3) 適用したいそれぞれのサービスのアカウントING、オーソライゼーションのメソッド名を定義し、使用する RADIUS サーバー、もしくは TACACS+ サーバーのグループを指定します。
- (4) ポートまたはラインインターフェースにメソッド名を適用します。

[注意] 上の説明は RADIUS サーバーと TACACS+ サーバーが既に AAA 機能をサポートしていることを前提にしています。RADIUS サーバーと TACACS+ サーバーの設定については、各サーバー、ソフトウェアのマニュアルを参照してください。

ローカル / リモートログオン認証設定

本機ではユーザ名とパスワードベースによる管理アクセスの制限を行うことができます。本機内部でのアクセス権の設定が行える他、RADIUS 及び TACACS+ によるリモート認証サーバでの認証も行うことができます。

RADIUS 及び TACACS+ は、ネットワーク上の RADIUS 対応及び TACACS+ 対応のデバイスのアクセスコントロールを認証サーバにより集中的に行うことができます。認証サーバは複数のユーザ名 / パスワードと各ユーザの本機へのアクセスレベルを管理するデータベースを保有しています。

機能解説

- ・ 初期設定では、管理アクセスは本機内部の認証データベースを使用します。外部の認証サーバを使用する場合、認証手順とリモート認証プロトコルの対応したパラメータの設定を行う必要があります。ローカル、RADIUS 及び TACACS+ 認証では、コンソール接続、Web インタフェース及び Telnet 経由のアクセス管理を行います。
- ・ 最大 3 つの認証方法を利用することができます。例えば (1) RADIUS、(2) TACACS、(3) Local と設定した場合、初めに RADIUS サーバでユーザ名とパスワードの認証を行います。RADIUS サーバが使用できない場合には、次に TACACS+ サーバを使用し、その後本体内部のユーザ名とパスワードによる認証を行います。

設定・表示項目

Authentication

認証方式を選択します。

- － Local － 本機内部においてユーザ認証を行います。
- － RADIUS － RADIUS サーバによるユーザ認証を行います。
- － TACACS － TACACS+ サーバによるユーザ認証を行います。
- － [authentication sequence] － ユーザ認証は、指定されたシーケンスの最大 3 つの認証メソッドによって実行されます。

設定方法

- (1) [Security] → [AAA] → [System Authentication] をクリックします。
- (2) “Authentication sequence” を指定します。
- (3) < Apply > をクリックします。

The screenshot shows a web interface window titled "Security > AAA > System Authentication". Inside the window, there is a label "Authentication Sequence" followed by a dropdown menu. The dropdown menu is open, showing the text "Local, RADIUS". Below the dropdown menu, there are two buttons: "Apply" and "Revert".

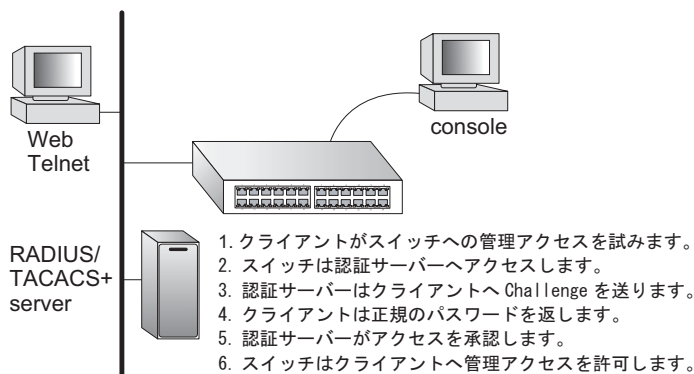
リモートログオン認証サーバの設定

本機ではユーザ名とパスワードベースによる管理アクセスの制限を行うことができます。本機内部でのアクセス権の設定が行える他、RADIUS 及び TACACS+ によるリモート認証サーバでの認証も行うことができます。

RADIUS 及び TACACS+ は、ネットワーク上の RADIUS 対応及び TACACS+ 対応のデバイスのアクセスコントロールを認証サーバにより集中的に行うことができます。認証サーバは複数のユーザ名 / パスワードと各ユーザの本機へのアクセスレベルを管理するデータベースを保有しています。

RADIUS ではベストエフォート型の UDP を使用しますが、

TACACS+ では接続確立型通信の TCP を使用します。また、RADIUS ではサーバへのアクセス要求パケットのパスワードのみが暗号化されますが、TACACS+ は全てのパケットが暗号化されます。



機能解説

- 外部の認証サーバを使用する場合、認証手順とリモート認証プロトコルの対応したパラメータの設定を行う必要があります。ローカル、RADIUS 及び TACACS+ 認証では、コンソール接続、Web インタフェース及び Telnet 経由のアクセス管理を行います。
- RADIUS 及び TACACS+ 認証では、各ユーザ名とパスワードに対し、アクセスレベル (Privilege Level) を設定します。ユーザ名、パスワード及びアクセスレベル (Privilege Level) は認証サーバ側で設定を行います。
設定

表示項目

RADIUS 設定

Global

RADIUS サーバの設定をグローバルに適用します。

Server Index

設定する RADIUS サーバを、5 つのうち 1 つ指定します。本機は、表示されたサーバの順に認証プロセスを実行します。認証プロセスは、サーバがそのユーザのアクセスを許可または拒否した時点で終了します。

Server IP Address

RADIUS サーバの IP アドレス

Accounting Server UDP Port

アカウンティングメッセージに使用される、認証サーバのネットワークポート (UDP) 番号 (1-65535、初期設定 :1813)

Authentication Server UDP Port

認証メッセージに使用される、認証サーバのネットワークポート (UDP) 番号 (1-65535、初期設定 :1812)

Authentication Timeout

スイッチがリクエストを再送信するまで、RADIUS サーバからの返答を待つ秒数。
(1-65535、初期設定 :5)

Authentication Retries

スイッチが認証サーバを経由して、認証ログオンアクセスを試みる回数。
(1-30、初期設定 :2)

Set Key

スイッチが認証サーバを経由して、認証ログオンアクセスを試みる回数。
(1-30、初期設定 :2)

Authentication Key

暗号鍵はクライアントのログオンアクセスに認証に使用されます。余白を使用しないでください。(最大値 : 48 文字)

Confirm Authentication Key

エラーがないことを確認する為に、前のフィールドに入力されたストリングを再タイプしてください。

TACACS+ 設定

Global

TACACS+ サーバの設定をグローバルに適用します。

Server Index

設定を行うサーバのインデックス番号を指定します。本機は 1 つの TACACS+ サーバのみサポートしています。

Server IP Address

TACACS+ サーバの IP アドレス

Authentication Server TCP Port

TACACS+ サーバで認証メッセージに使用される TCP ポート番号
(範囲 : 1-65535、初期設定 :49)

Set Key

暗号キーの設定または編集を行うためにこのボックスをマークします。

Authentication Key

クライアントのログオンの認証に使用されるアクセス暗号キー余白は使用しないでください。
(最大値 48 文字)

Confirm Authentication Key

エラーがないことを確認する為に、前のフィールドに入力されたストリングを再タイプしてください。

グループ設定

Server Type

RADIUS または TACACS+ サーバを選択

Group Name

RADIUS または TACACS+ サーバのグループ名を定義 (1-255 文字)

Sequence at Priority

グループで使用する RADIUS サーバとシーケンスを指定 (範囲 : 1-5)

設定方法

リモート認証サーバの設定（RADIUS）

- (1) [Security] → [AAA] → [Server] をクリックします。
- (2) 「Step」 リストから「Configure Server」を選択します。
- (3) RADIUS または TACACS+ からサーバタイプを選択します。
- (4) 必要に応じ、設定変更を行います。
- (5) < Apply > をクリックします。

Security > AAA > Server

Step: 1. Configure Server

Server Type ☒ RADIUS ☐ TACACS+

☐ Global | Server Index: ☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Server IP Address

Accounting Server UDP Port (1-65535)

Authentication Server UDP Port (1-65535)

Authentication Timeout (1-65535) sec

Authentication Retries (1-30)

☒ Set Key

Authentication Key

Confirm Authentication Key

リモート認証サーバの設定（TACACS+）

Security > AAA > Server

Step: 1. Configure Server

Server Type ☐ RADIUS ☒ TACACS+

☐ Global | Server Index: ☒ 1

Server IP Address

Authentication Server TCP Port (1-65535)

☒ Set Key

Authentication Key

Confirm Authentication Key

アカウントティングと許可に使用される RADIUS または TACACS+ サーバグループの設定

- (1) [Security] → [AAA] → [Server] をクリックします。
- (2) 「Step」 リストから「Configure Group」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) RADIUS または TACACS+ からサーバタイプを選択します。
- (5) 必要に応じ、設定変更を行います。
- (6) < Apply > をクリックします。

Security > AAA > Server

Step: 2. Configure Group Action: Add

Server Type ☒ RADIUS ☐ TACACS+

RADIUS Group Name

Sequence At Priority 1

Sequence At Priority 2

Sequence At Priority 3

Sequence At Priority 4

Sequence At Priority 5

Apply Revert

アカウントティングと許可に使用される RADIUS または TACACS+ サーバグループの表示

- (1) [Security] → [AAA] → [Server] をクリックします。
- (2) 「Step」 リストから「Configure Group」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Security > AAA > Server

Step: 2. Configure Group Action: Show

Server Type ☒ RADIUS ☐ TACACS+

RADIUS Group List Max: 5 Total: 1

	Group Name	Member Index
☐	radius	1

Delete Revert

AAA アカウンティングの設定

この画面では課金やセキュリティ目的でリクエストされたサービスのアカウンティングを有効にするかどうかを設定します。

機能解説

- アカウンティングを有効にする前に、RADIUS または TACACS+ 経由の AAA 認証を有効にしてください。

設定・表示項目

グローバル設定

Periodic Update

ローカルアカウンティングサービスが システム上の全てのユーザからアカウンティングサーバーへの情報をアップデートする間隔を指定。(範囲：1-2147483647 分 0 は無効を意味します)

メソッド設定

Accounting Type

- 802.1X - エンドユーザのアカウンティング
- Exec - ローカルコンソール、Telnet、SSH 用の管理アカウンティング

Method Name

サービス要求のオーソライゼーション方法を指定します。"default" メソッドは他のメソッドが定義されていない場合、リクエストされたサービスに使用されます (範囲：1 ~ 255 文字)

Accounting Notice

ログインからログオフポイントまでのユーザ活動を記録。

Server Group Name

アカウンティングサーバグループを指定 (範囲：1-255 文字)

グループ名 "radius" と "tacacs+" は設定された全ての RADIUS と TACACS+ ホスト (P167 「ローカル / リモートログオン認証設定」を参照) を指定します。その他のグループ名は Security > AAA > Server (Configure Group) ページで設定されたサーバグループを参照してください。

サーバ設定

Accounting Type

アカウンティングタイプを指定します。

802.1X

- Method Name - コンソール接続と Telnet 接続に割り当てるユーザー定義のメソッド名を指定します。(範囲：1-255 文字)

Exec

- Console Method Name - コンソール接続に割り当てられるユーザ定義メソッド名を指定。
- Telnet Method Name - Telnet 接続と Telnet 接続に割り当てるユーザー定義のメソッド名を指定します。

情報の表示－概要

Accounting Type

アカウントティングサービスを表示

Method Name

ユーザ定義またはデフォルトアカウントティングメソッドを表示。

Server Group Name

アカウントティングサーバグループを表示。

Interface

ルールが適用されるポート、コンソールまたは Telnet インタフェースを表示。

情報の表示－統計

User Name

登録されたユーザー名を表示。

Accounting Type

アカウントティングサービスを表示。

Interface

このユーザがスイッチにアクセスした受信ポート数。

Time Elapsed

このエントリが有効になった時間の長さを表示。

設定方法

AAA アカウンティングのグローバル設定

- (1) [Security] → [AAA] → [Accounting] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 適切なアップデートインターバルを入力します。
- (4) < Apply >をクリックします。

Security > AAA > Accounting

Step: 1. Configure Global

Periodic Update (1-2147483647) min (0: Disabled)

Apply Revert

アカウンティングメソッドの設定

- (1) [Security] → [AAA] → [Accounting] をクリックします。
- (2) 「Step」 リストから「Configure Method」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) アカウンティングタイプを選択します。
- (5) アカウンティングメソッド名とサーバグループ名を指定します。
- (6) < Apply >をクリックします。

Security > AAA > Accounting

Step: 2. Configure Method Action: Add

Accounting Type

Method Name

Accounting Notice

Server Group Name ☒ radius

Apply Revert

アカウンティングメソッドの表示

- (1) [Security] → [AAA] → [Accounting] をクリックします。
- (2) 「Step」 リストから「Configure Method」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Security > AAA > Accounting

Step: 2. Configure Method Action: Show

Method List Max: 26 Total: 2

☐	Accounting Type	Method Name	Accounting Notice	Server Group Name
☐	802.1X	default	Start-Stop	radius
☐	EXEC	default	Start-Stop	tacacs+

Delete Revert

指定されたインタフェース、コンソールコマンド、ローカルコンソール、Telnet、SSH 接続に適用されるアカウントングメソッドの設定

- (1) [Security] → [AAA] → [Accounting] をクリックします。
- (2) 「Step」 リストから「Configure Service」を選択します。
- (3) アカウントングタイプを選択します。(802.1X、Exec)
- (4) アカウントングメソッドを入力します。
- (5) < Apply >をクリックします。

Security > AAA > Accounting

Step: 3. Configure Service

Accounting Type ☒ 802.1X ☐ EXEC

Port Method List Max: 10 Total: 10

Port	Method Name
1	default
2	default
3	default
4	
5	

Eexec サービスのアカウントングサービスを設定

Security > AAA > Accounting

Step: 3. Configure Service

Accounting Type ☐ 802.1X ☒ EXEC

Console Method Name default

Telnet Method Name default

Apply Revert

指定されたサービスタイプに設定された、アカウントングメソッドとサーバグループの概要を表示

- (1) [Security] → [AAA] → [Accounting] をクリックします。
- (2) 「Step」 リストから「Show Information」を選択します。
- (3) 「Summary」をクリックします。

Security > AAA > Accounting

Step: 4. Show Information

☒ Summary ☐ Statistics

Method List Max: 26 Total: 2

Accounting Type	Method Name	Server Group Name	Interface
802.1X	default	radius	
EXEC	default	tacacs+	Console, Telnet

Web インタフェース セキュリティ

基本アカウント情報およびユーザセッションに記録された統計を表示

- (1) [Security] → [AAA] → [Accounting] をクリックします。
- (2) 「Step」 リストから「Show Information」を選択します。
- (3) 「Statistics」をクリックします。

Security > AAA > Accounting			
Step: 4. Show Information ▼			
☐ Summary ☒ Statistics			
Accounting Statistics Max: 26 Total: 2			
User Name	Accounting Type	Interface	Time Elapsed
Bob	802.1X	Eth1/1	3:44:55
Ted	802.1X	Eth1/5	1:24:51

AAA 認可設定

Security > AAA > Authorization ページを使用し、要求されるサービスの認可を有効にします。また、設定された認可メソッドの表示、指定したインタフェースへのメソッドの割り当ても行えます。

コマンド解説

- この機能は、ユーザが Exec シェルを実行することを可能にするかどうかを決定する認可を行います。
- アカウンティングを有効にする前に、RADIUS または TACACS+ 経由の AAA 認証を有効にしてください。

設定・表示項目

メソッドの設定

Authorization Type

オーソライゼーションサービスの種類を表示します。

Method Name

サービスリクエストのための認可メソッドを指定します。他のメソッドが定義されていない場合、"default" メソッドが要求されたサービスに使用されます。(範囲：1-255 文字)

Server Group Name

認可サーバグループを指定 (範囲：1-255 文字)

グループ名 "tacacs+" は、設定された TACACS+ ホスト (167 ページの「ローカル / リモートログオン認証設定」を参照) 全てを指定します。その他のグループ名は "TACACS+" 設定ページで設定されたサーバグループを参照してください。認可は TACACS+ サーバでのみサポートされます。

サービスの設定

Console Method Name

コンソール接続に割り当てる、ユーザー定義メソッド名を指定

Telnet Method Name

Telnet 接続に割り当てる、ユーザー定義メソッド名を指定

情報の表示

Authorization Type

オーソライゼーションサービスを表示

Method Name

ユーザ定義またはデフォルトアカウントメソッドを表示

Server Group Name

認可サーバグループを表示

Interface

オーソライゼーションメソッドを適用したコンソール、もしくは Telnet のインターフェースを表示します (この欄はオーソライゼーションメソッド、または関連付けられたサーバグループが割り当てられていない場合、空欄になります)

設定方法

Exec サービスタイプに適用された認可メソッドを設定

- (1) [Security] → [AAA] → [Authorization] をクリックします。
- (2) 「Step」 リストから「Configure Method」を選択します。
- (3) 認可メソッド名とサーバグループ名を指定します。
- (4) < Apply > をクリックします。

Security > AAA > Authorization

Step: 1. Configure Method Action: Add

Authorization Type: EXEC

Method Name: default

Server Group Name: ☒ radius ☐

Apply Revert

Exec サービスタイプに適用された認可メソッドを表示

- (1) [Security] → [AAA] → [Authorization] をクリックします。
- (2) 「Step」 リストから「Configure Method」を選択します。
- (3) 「Step」 リストから「Show」を選択します。

Security > AAA > Authorization

Step: 1. Configure Method Action: Show

Method List Max: 5 Total: 1

☐	Authorization Type	Method Name	Server Group Name
☐	EXEC	default	radius

Delete Revert

ローカルコンソール、Telnet、SSH 接続に適用された認可メソッドを設定

- (1) [Security] → [AAA] → [Authorization] をクリックします。
- (2) 「Step」 リストから「Configure Service」を選択します。
- (3) 必要とされる認可メソッドを入力します。
- (4) < Apply > をクリックします。

Security > AAA > Authorization

Step: 2. Configure Service ▼

Console Method Name tps-auth

Telnet Method Name tps-auth

Apply
Revert

設定された認可メソッドと Exec サービスタイプのアサインされたサーバグループを表示

- (1) [Security] → [AAA] → [Authorization] をクリックします。
- (2) 「Step」 リストから「Show Information」を選択します。

Security > AAA > Authorization			
Step: 3. Show Information ▼			
Method List Max: 5 Total: 2			
Authorization Type	Method Name	Server Group Name	Interface
EXEC	default	radius	
EXEC	tps-auth	radius	Console, Telnet

3.12.2 ユーザアカウントの設定

ゲストモードではほとんどの設定パラメータにおいて、表示しか行うことができません。管理者モードでは設定パラメータの変更も行うことができます。

安全のため、管理者用パスワードは初期設定からの変更を行ない、パスワードは安全な場所に保管して下さい。

初期設定では、ゲストモードのユーザ名・パスワードは共に「guest」、管理者モードのユーザ名・パスワードは「admin」です。

設定・表示項目

User Name

ユーザ名（最大文字数：32 文字、最大ユーザ数：16）

Access Level

ユーザのアクセスレベル（オプション：0：Normal、15：Privileged）

Password

ユーザのパスワード（範囲：0-32 文字、大文字と小文字は区別されます）

Confirm Password

確認のため、もう一度パスワードを入力。

設定方法

ユーザアカウントの設定

- (1) [Security] → [User Accounts] → をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) ユーザ名を指定し、ユーザのアクセスレベルを選択します。パスワードを入力後、確認の為もう一度パスワードを入力します。
- (4) < Apply > をクリックします。

The screenshot shows a web interface titled "Security > User Accounts". At the top, there is a section labeled "Action:" with a dropdown menu currently set to "Add". Below this, there are four input fields arranged in two columns. The first column contains labels: "User Name", "Access Level", "Password", and "Confirm Password". The second column contains the corresponding input values: "bob" for User Name, "15 (Privileged)" for Access Level (which is a dropdown menu), and two password fields, each filled with six dots. At the bottom right of the form, there are two buttons: "Apply" and "Revert".

ユーザアカウントの表示

- (1) [Security] → [User Accounts] →をクリックします。
- (2) 「Action」 リストから「Show」を選択します。
- (3) ユーザ名を指定し、ユーザのアクセスレベルを選択します。パスワードを入力後、確認

Security > User Accounts

Action: Show ▼

User Account List Max: 16 Total: 2

☐	User Name	Access Level
☐	admin	15
☐	guest	0

Delete Revert

3.12.3 Web 認証

Web 認証は、802.1x やネットワークアクセス認証が実行不可能であり実用的でない状況で、ネットワークへの認証とアクセスを行うことを端末に許可します。Web 認証機能は IP アドレスを割り当てる DHCP のリクエストと受信、DNS クエリの実行を、認証されていないホストに許可します。HTTP を除いたほかのすべてのトラフィックはブロックされます。スイッチは HTTP トラフィックを傍受し、RADIUS を通してユーザーネームとパスワードを入力するスイッチが生成した Web ページにリダイレクトします。一度認証に成功すると、Web ブラウザは元のリクエストされた Web ページに転送されます。認証が成功したポートに接続されたすべてのホストについて、認証が有効になります。

[注意] RADIUS 認証は適切に機能させるために、アクティベートし Web 認証のために適切に構成しなくてはなりません。(P231 「802.1x ポート認証」を参照)

[注意] Web 認証はトランクポート上で設定することはできません。

Web 認証のグローバル設定

Security > Web Authentication(Configure Global) ページを使用して、Web 認証のグローバルパラメータを編集できます。

設定・表示項目

Web Authentication Status

スイッチ上で Web 認証機能を有効にします (初期設定: 無効)

Session Timeout

ホストの再認証をする前に認証セッションをどのくらいの時間維持するかを設定します
(範囲: 300 – 3600 秒 初期設定: 3600 秒)

Quiet Period

ホストがログインの試行回数の上限を超えた後、再び認証ができるまでに待機する時間を設定します (範囲: 1 – 180 秒 初期設定: 60 秒)

Login Attempts

ログインの試行回数の上限を設定します。(範囲: 1 – 3 回 初期設定: 3 回)

設定方法

- (1) [Security] → [Web Authentication] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) Web 認証を有効にし、必要なパラメータの編集を行ってください。
- (4) < Apply >をクリックします。

Security > Web Authentication

Step: 1. Configure Global ▼

Web Authentication Status

☐ Enabled

Session Timeout (300-3600)

sec

Quiet Period (1-180)

sec

Login Attempts (1-3)

Apply

Revert

Web 認証の設定（ポート）

Security > Web Authentication (Configure Interface) ページを使用して、Web 認証をポートで有効化します。また、接続されたホストの情報を表示します。

設定・表示項目

Port

設定されるポート

Status

ポートの Web Authentication の状態を設定します。

Host IP Address

接続されたそれぞれのホストの IP アドレス。

Remaining Session Time

ホストの現在の認証セッションの期限が切れるまでの残り時間を表示します。

設定方法

- (1) [Security] → [Web Authentication] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) Web 認証を必要とするポートの「Status」チェックボックスにチェックを入れ、< Apply >をクリックします。

Security > Web Authentication

Step: 2. Configure Interface

Port 1

Status ☒ Enabled

Authenticated Host List Max: 8 Total: 2

☐	Host IP Address	Remaining Session Time (sec)
☐	10.1.1.1	300
☐	10.2.2.2	100

Apply Revert

3.12.4 ネットワークアクセス (MAC アドレス認証)

スイッチポートに接続するいくつかのデバイスは、ハードウェアやソフトウェアの制限により 802.1x 認証をサポートできないかもしれません。これはネットワークプリンタ、IP 電話、ワイヤレスアクセスポイントのようなデバイスでしばしば遭遇します。スイッチは、RADIUS サーバーでデバイスの MAC アドレスを認証し管理することで、これらのデバイスからのネットワークアクセスを可能にします。

[注意] RADIUS 認証は適切に機能させるために、アクティベートし Web 認証のために適切に構成しなくてははいけません。(P231 「802.1x ポート認証」を参照)

[注意] MAC 認証はトランクポート上で設定することはできません。

機能解説

- ネットワークアクセス機能は、ホストが接続されたスイッチポート上で MAC アドレスを認証することで、ホストのネットワークへのアクセスを管理しています。特定の MAC アドレスから受信したトラフィックは、送信元 MAC アドレスが RADIUS サーバーで認証された場合のみスイッチにより転送されます。MAC アドレスによる認証が進行しているとき、すべてのトラフィックは認証が完了するまでブロックされます。認証が成功した場合、RADIUS サーバーはスイッチポートに VLAN 設定を任意に割り当てる可能性があります。
- ポート上で有効にしたとき、認証プロセスは設定された RADIUS サーバーに Password Authentication Protocol (PAP) リクエストを送信します。ユーザーネームとパスワードは両方とも認証する予定の MAC アドレスと同じです。RADIUS サーバー上で PAP のユーザーネームとパスワードは MAC アドレスのフォーマット (xx-xx-xx-xx-xx-xx) で設定してください。
- 認証された MAC アドレスは、スイッチの保護された MAC アドレステーブルにダイナミックエントリとして保存され、エージングタイムが過ぎたときに取り除かれます。スイッチでサポートする保護された MAC アドレスの最大数は 1024 個です。
- 設定された静的 MAC アドレスがスイッチポートで見られた時、セキュアアドレステーブルに追加されます。静的アドレスは RADIUS サーバへのリクエスト送信無しで認証済みとして取り扱われます。
- ポートステータスがダウンへ変更した際、全ての MAC アドレスはセキュアアドレスからクリアされます。静的 VLAN 割り当ては保存されません。
- RADIUS サーバーはスイッチポートに適用するために VLAN ID のリストを任意に返すかもしれません。下記の設定は RADIUS サーバー上で設定するために必要です。

- Tunnel-Type = VLAN
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = 1u、2t (VLAN ID リスト)

VLAN ID リストは RADIUS の "Tunnel-Private-Group-ID" の中で維持されています。VLAN ID のリストは、"1u、2t、3u" といったフォーマットの複数の VLAN ID を含むことができます。"u" が付いているのはタグなしの VLAN ID で、"t" が付いているのはタグありの VLAN ID となります。

- RADIUS サーバはオプションとして、認証されたユーザのために、スイッチポートに適用された動的 QoS 割り当てを返します。"Filter ID" 属性は、以下の QoS 情報を渡すよう RADIUS サーバに設定することができます。

動的 QoS プロファイル

プロファイル	属性文法	例
DiffServ	service-policy-in=policy-map-name	service-policy-in=p1
Rate Limit	rate-limit-input=rate	rate-limit-input=100 (in units of Kbps)
802.1p	switchport-priority-default=value	switchport-priority-default=2

- 複数のプロファイルはセミコロンでそれぞれを区切るにより、Filter-ID 属性で指定することができます。
例えば、属性 “ service-policy-in=pp1;rate-limit-input=100 ”は "diffserv profile name is pp1, ”と "ingress rate limit profile value is 100 kbps" を指定しています。
- 重複したプロファイルが Filter-ID 属性でパスする際、最初のプロファイルのみ使用されます。例えば、もし属性が “ service-policy-in=p1;service-policy-in=p2 ” の場合、スイッチは "DiffServ profile p1." のみ適用します。
- Filter-ID 属性の未サポートプロファイルは無視されます。
例えば属性が “ map-ip-dscp=2:3;service-policy-in=p1, ”の場合、スイッチは “ map-ip-dscp ”を無視します。
- 認証成功時、動的 QoS 情報は以下のうちいずれかの状態により、RADIUS サーバからパスされないことがあります。
 - Filter-ID 属性ユーザプロファイルに見つけれない。
 - Filter-ID 属性がブランク。
 - 動的 QoS 割り当ての Filter-ID 属性フォーマットが認識不可 (Filter-ID 属性全体を認識不可)
- 以下の状態が起きた時、動的 QoS 割り当てが失敗し認証結果が成功から失敗へ変更されます。
 - プロファイル値にイリーガル文字を発見 (例：802.1p プロファイル値の非デジタル文字)
 - 認証ポートで受信されるプロファイル設定の失敗
- 動的 QoS にアサインする、最後のユーザがポートからログオフした時、スイッチはオリジナル QoS 設定をポートヘリストアします。
- ユーザが、既に同じポートへログオンしているユーザと異なる動的 QoS プロファイルでネットワークへのログインを試みた時、このユーザはアクセスを拒否されます。
- ポートが割り当てられた QoS プロファイルを持つ間、手動 QoS 設定は、全てのユーザがポートからログオフした後のみ効力を発します。

ネットワークアクセスのグローバル設定

MAC アドレス認証は基本的にポートごとに設定しますが、スイッチすべてのポートに適用する設定が 2 つあります。

Security > Network Access (Configure Global) ページを使用して、MAC アドレス認証エージングと再認証時間の設定を行います。

設定・表示項目

Aging Status

セキュア MAC アドレステーブルに保存された、認証 MAC アドレスのエージングを有効 / 無効にします。(初期設定：無効)

このパラメータは本セクションで説明する MAC アドレス認証プロセスによって設定され、認証された MAC アドレスと、同様に 802.1x によって認証されたセキュア MAC アドレスに、802.1X モード (P233 「802.1X 認証ポート設定」で解説される Single-Host、Multi-Host、MAC-Based 認証) にかかわらず適用されます。

認証された MAC アドレスは、スイッチのセキュア MAC アドレステーブル動的エントリとして保存され、エージングタイムの期限が切れた時に削除されます。

スイッチシステムにサポートされているセキュア MAC アドレス最大数は 1024 です。

Reauthentication Time

MAC アドレスが認証された後、再認証されるまでの期間を設定します。(範囲：120 秒 - 1,000,000 秒 初期設定：1800 秒)

設定方法

- (1) [Security] → [Network Access] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) セキュアアドレスのエージングを有効 / 無効にし、「Reauthentication Time」を編集します。
- (4) < Apply > をクリックします。

Security > Network Access

Step: 1. Configure Global

Aging Status ☒ Enabled

Reauthentication Time (120-1000000) sec

Apply Revert

ポートのネットワークアクセス設定

Security > Network Access (Configure Interface - General) ページを使用して、スイッチポートに MAC アドレス認証の設定を行います。

設定・表示項目

MAC Authentication

- Status —ポートで MAC 認証を有効にします。(初期設定：無効)
- Intrusion —ホスト MAC 認証が失敗した時に、ポートへのアクセスをブロックするか、あるいはトラフィックを渡すかを設定します。(オプション：Block、Pass 初期設定：Block)
- Max MAC Count* — MAC 認証経由で 認証されることが可能な MAC アドレスの最大数を設定 (範囲：1-1024 初期設定：1024)

Network Access Max MAC Count*

あらゆる形態の認証によってポートインタフェースが認証可能な MAC アドレスの最大数を設定します。(範囲：1-1024 初期設定：1024)

Guest VLAN

802.1x の認証が失敗したとき、ポートに割り当てる VLAN を指定します。VLAN は事前に作成し、有効にする必要があります。

Dynamic VLAN

認証されたポートへのダイナミック VLAN の割り当てを有効にします。有効にしたとき、RADIUS サーバーより返ってきた VLAN ID がポートに割り当てられ、スイッチ上で事前に作成した VLAN が規定されます (VLAN 作成に GVRP は使用できません)。VLAN の設定は最初に行ってください。

(初期設定：有効)

Dynamic QoS

認証ポートでの、動的 QoS 機能の有効 / 無効 (初期設定：無効)

* ポートごとの MAC アドレスの最大数は 1024 です。また、スイッチシステムでサポートされるセキュア MAC アドレスの最大数も 1024 です。上限に達した時、全ての新しい MAC アドレスは認証失敗として扱われます。

設定方法

- (1) [Security] → [Network Access] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「General」 ボタンをクリックします。
- (4) 必要な項目の編集を行います。
- (5) < Apply > をクリックします。

Security > Network Access

Step: 2. Configure Interface ▼

☒ General
 ☐ Link Detection

Port List Max: 26 Total: 26 1 2 3

Port	MAC Authentication			Network Access Max MAC Count (1-1024)	Guest VLAN (0-4093, 0: Disabled)	Dynamic VLAN	Dynamic QoS
	Status	Intrusion	Max MAC Count (1-1024)				
1	☒ Enabled	Block ▼	1024	1024	0	☐ Enabled	☐ Enabled
2	☐ Enabled	Block ▼	1024	1024	0	☒ Enabled	☐ Enabled
3	☐ Enabled	Block ▼	1024	1024	0	☒ Enabled	☐ Enabled
4	☐ Enabled	Block ▼	1024	1024	0	☒ Enabled	☐ Enabled
5	☐ Enabled	Block ▼	1024	1024	0	☒ Enabled	☐ Enabled

ポートリンク検出

ポートリンク検出機能はリンクイベント発生時に、SNMP トラップの送信とポートのシャットダウン（どちらかあるいは両方）を実行します。

設定・表示項目

Link Detection Status

ポートでリンク検出を有効 / 無効に設定

Condition

ポートアクションを引き起こすリンクイベントタイプ

- Link Up – リンクアップイベントのみポートアクションを発生
- Link Down – リンクダウンイベントのみポートアクションを発生
- Link Up and Down – 全てのリンクアップ・ダウンイベントでポートアクションを発生

Action

本機は以下の 3 通りの方法でリンクアップ・ダウンイベントに対応することが可能です。

- Trap – SNMP トラップを送信。
- Trap and Shutdown – SNMP トラップを送信し、ポートをシャットダウンします。
- Shutdown – ポートをシャットダウン。

設定方法

- (1) [Security] → [Network Access] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Link Detection」 ボタンをクリックします。
- (4) ポートごとに、「Link Detection Status」、「Condition」、「Action」 の編集を行います。
- (5) < Apply > をクリックします。

Security > Network Access

Step: 2. Configure Interface

☐ General ☒ Link Detection

Port List Max: 10 Total: 10

Port	Link Detection Status	Condition	Action
1	☐ Enabled	Link down	Trap
2	☒ Enabled	Link up and down	Trap
3	☐ Enabled	Link down	Trap
4	☐ Enabled	Link down	Trap
5	☐ Enabled	Link down	Trap

MAC アドレスフィルタ

それぞれのポートの MAC 認証は、独立して設定されます。

MAC 認証ポート設定ページでは、それぞれのポートで指定する MAC 認証の最大数と、侵入時のアクションを設定します。

機能解説

- 指定した MAC アドレスは認証を免除されます。
- 最大 65 フィルタテーブルの定義が可能です。
- フィルタテーブルで使われるエントリの数に制限はありません。

設定・表示項目

Filter ID

指定したフィルタのフィルタルールを追加。

MAC Address

フィルタルールは、入力パケットを MAC アドレスまたは MAC アドレス範囲（MAC アドレスマスクによって定義される）と照らし合わせてチェックします。

MAC Address Mask

フィルタルールは MAC ビットマスクで定義される MAC アドレス範囲とチェックされます。もしマスクを省略した場合、システムは完全一致のデフォルトマスクを割り当てます。（範囲：000000000000 - FFFFFFFF） 初期設定：FFFFFFFF

設定方法

MAC 認証の MAC アドレスフィルタを追加

- (1) [Security] → [Network Access] をクリックします。
- (2) 「Step」 リストから「Configure MAC Filter」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) Filter ID、MAC Address、マスク（オプション）を入力します。
- (5) < Apply > をクリックします。

Security > Network Access

Step: 3. Configure MAC Filter Action: Add

Filter ID (1-64) 22

MAC Address 11-22-33-44-55-66

MAC Address Mask FFFFFFFFFF

Apply Revert

Web インタフェース セキュリティ

MAC 認証の MAC アドレスフィルタテーブルを表示

- (1) [Security] → [Network Access] をクリックします。
- (2) 「Step」 リストから「Configure MAC Filter」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Security > Network Access

Step: 3. Configure MAC Filter Action: Show

MAC Filter List Max: 65 Total: 1

☐	Filter ID	MAC Address	MAC Address Mask
☐	22	11-22-33-44-55-66	FF-FF-FF-FF-FF-FF

Delete Revert

セキュア MAC アドレス情報の表示

Security > Network Access (Show Information) ページを使用し、セキュア MAC アドレステーブルに保存されている、認証済み MAC アドレスを表示します。ここでは保護された MAC エントリの情報を表示し、選択したエントリをテーブルから削除することができます。

設定・表示項目

Query By

MAC アドレスの検索に使用する値を指定します。

- Sort Key—MAC アドレス、ポートインタフェースまたはその他属性で表示された情報をソートします。
- MAC Address — MAC アドレスを指定
- Interface — ポートインタフェースを指定
- Attribute — スタティックアドレスかダイナミックアドレスかを表示

Authenticated MAC Address List

- MAC Address — 認証された MAC アドレス
- Interface — セキュア MAC アドレスに関連付けられたポートインタフェース
- RADIUS Server — MAC アドレスを認証した RADIUS サーバの IP アドレス
- Time—MAC アドレスが最後に認証された時間
- Attribute—静的または動的アドレスを指定

設定方法

- (1) [Security] → [Network Access] をクリックします。
- (2) 「Step」 リストから「Show Information」を選択します。
- (3) MAC アドレス、インタフェースまたはその他の属性を基にアドレスを表示するため、「Sort」キーを使用します。
- (4) 「MAC Address」フィールドに入力されたアドレスや、「Interface」フィールドで指定したポート、「Attribute」フィールドで指定した動的、静的アドレスタイプによって表示を限定します。
- (5) < Query > をクリックします。

Security > Network Access

Step: 4. Show Information

Query by:

Sort Key: MAC Address

☐ MAC Address

☐ Interface

☐ Attribute

Query

Authenticated MAC Address List Max: 2048 Total: 8

	MAC Address	Interface	RADIUS Server	Time	Attribute
☐	00-00-86-45-F2-23	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 16m 12s	Dynamic
☐	00-00-E8-5E-E1-DD	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 24s	Dynamic
☐	00-00-E8-81-93-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 40m 32s	Dynamic
☐	00-01-8C-31-B8-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 18m 51s	Dynamic
☐	00-01-8C-36-95-D8	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 22s	Dynamic

3.12.5 HTTPS 設定

Secure Socket Layer(SSL) を使った Secure Hypertext Transfer Protocol(HTTPS) によって本機の Web インタフェースへ、暗号化された安全な接続を行うことができます。

機能解説

- HTTP 及び HTTPS サービスは共に使用することはできます。但し、HTTP 及び HTTPS サービスで同じ UDP ポート番号を設定することはできません。
- HTTPS を使用する場合、URL は HTTPS: から始まる表示がされます。
例 :[https://device: ポート番号]
- HTTPS のセッションが開始されると以下の手順で接続が確立されます。
 - －クライアントはサーバのデジタル証明書を使用し、サーバを確認します。
 - －クライアントとサーバが接続用のセキュリティプロトコルの調整を行います。
 - －クライアントとサーバは、データを暗号化し解読するためのセッション・キーを生成します。
- HTTPS を使用した場合、クライアントとサーバは安全な暗号化された接続を行います。Internet Explorer 5.x 以上または NetscapeNavigator 6.2 以上、Mozilla Firefox 2.0.0.0 以上のステータスバーには鍵マークが表示されます。
- "HTTP をサポートしている Web ブラウザ及び OS は以下の通りです。

Web ブラウザ	OS
Internet Explorer 5.0 以上	Windows 98、Windows NT (サービスパック 6A)、Windows 2000、Windows XP、Windows 7
Netscape Navigator 6.2 以上	Windows 98、Windows NT (サービスパック 6A)、Windows 2000、Windows XP、Solaris 2.6
Mozilla Firefox 2.0.0.0 以上	Windows 2000、Windows XP、Linux

※ 安全なサイトの証明を指定するためには、P195 「サイト証明書の置き換え」を参照して下さい。

設定・表示項目

HTTPS Status

HTTPS サーバ機能を有効または無効に設定します（初期設定；無効）

HTTPS Port

HTTPS 接続に使用される UDP ポートを指定します（初期設定：443）

設定方法

- (1) [Security] → [HTTPS] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) HTTPS を有効にし、必要な場合はポート番号を指定します。
- (4) < Apply > をクリックします。

Security > HTTPS

Action: Configure Global ▼

HTTPS Status ☒ Enabled

HTTPS Port (1-65535)

Apply Revert

サイト証明書の置き換え

HTTPS を使用して Web インタフェースにログインする際に、SSL を使用します。初期設定では認証機関による認証を受けていないため、Netscape 及び Internet Explorer 画面で安全なサイトとして認証されていないという警告が表示されます。この警告を表示させないようにするためには、認証機関から個別の証明書入手し、設定を行う必要があります。

[注意] 初期設定の証明書は個々のハードウェアで固有の認証キーではありません。より高度なセキュリティ環境を実現するためには、できるだけ早くで独自の SSL 証明書を取得し設定を行う事を推奨します。

個別の証明書を取得した場合には、TFTP サーバを使用して既存の証明書と置き換えます。

設定・表示項目

TFTP Server IP Address

証明書ファイルを含む、TFTP サーバの IP アドレス。

Certificate Source File Name

TFTP サーバに保存されている証明書ファイル名。

Private Key Source File Name

TFTP サーバに保存されているプライベートキーファイル名。

Private Password

プライベートキーファイルに保存されているパスワード。

Confirm Password

確認のため、再度パスワードを入力してください。

設定方法

- (1) [Security] → [HTTPS] をクリックします。
- (2) 「Step」 リストから「Copy Certificate」を選択します。
- (3) 必要な項目を入力し、< Apply >をクリックします。

Security > HTTPS

Action: Copy Certificate ▼

TFTP Server IP Address	192.168.0.4
Certificate Source File Name	es-3026-site-certificate
Private Key Source File Name	es-3026-private-key
Private Password	•••••
Confirm Password	•••••

Apply Revert

3.12.6 Secure Shell 設定

Secure Shell (SSH) は、それ以前からあったバークレーリモートアクセスツールのセキュリティ面を確保した代替としてサーバ / クライアントアプリケーションを含んでいます。また、SSH は Telnet に代わる本機へのセキュアなリモート管理アクセスを提供します。

クライアントが SSH プロトコルによって本機と接続する場合、本機はアクセス認証のためにローカルのユーザ名およびパスワードと共にクライアントが使用する公開暗号キーを生成します。さらに、SSH では本機と SSH を利用する管理端末の間の通信をすべて暗号化し、ネットワーク上のデータの保護を行ないます。

[注意] SSH 経由での管理アクセスを行なうためには、クライアントに SSH クライアントをインストールする必要があります。

[注意] 本機では SSH Version1.5 と 2.0 をサポートしています。

機能解説

本機の SSH サーバはパスワード及びパブリックキー認証をサポートしています。SSH クライアントによりパスワード認証を選択した場合、認証設定ページで設定したパスワードにより本機内、RADIUS、TACACS+ のいずれかの認証方式を用います。クライアントがパブリックキー認証を選択した場合には、クライアント及び本機に対して認証キーの設定を行なう必要があります。

公開暗号キー又はパスワード認証のどちらかを使用するに関わらず、本機上の認証キー（SSH ホストキー）を生成し、SSH サーバを有効にする必要があります。

SSH サーバを使用するには以下の手順で設定を行ないます。

- (1) **ホストキーペアの生成** — SSH ホストキー設定ページでホスト パブリック / プライベートキーのペアを生成します。
- (2) **ホスト公開キーのクライアントへの提供** — 多くの SSH クライアントは、本機との自動的に初期接続設定中に自動的にホストキーを受け取ります。そうでない場合には、手で管理端末のホストファイルを作成し、ホスト公開キーを置く必要があります。ホストファイル中の公開暗号キーは以下の例のように表示されます。

```
10.1.0.54 1024 35
15684995401867669259333946775054617325313674890836547254150202455931998
68544358361651999923329781766065830956
1082591321289023376546801726272571413428762941301196195566782
59566410486957427888146206519417467729848654686157177393901647793559423
0357741309802273708779454524083971752646358058176716709574804776117
```

- (3) **クライアント公開キーの本機への取り込み** — 389 ページの「copy」を参照コマンドを使用し、SSH クライアントの本機の管理アクセスに提供される公開キーを含むファイルをコピーします。クライアントへはこれらのキーを使用し、認証が行なわれます。現在のファームウェアでは以下のような UNIX 標準フォーマットのファイルのみ受け入れることが可能です。

```
1024 351341081685609893921040944920155425347631641921872958921143173
88005553616163105177594083868631109291232226828519254374603100937187721
19969631781366277414168985132049117204830339254324101637997592371449011
93800609025394840848271781943722884025331159521348610229029789827213532
67131629432532818915045306393916643  steve@192.168.1.19
```

- (4) **オプションパラメータの設定** — SSH 設定ページで、認証タイムアウト、リトライ回数、サーバキーサイズなどの設定を行なってください。

(5) **SSH の有効化** — SSH 設定ページで本機の SSH サーバを有効にしてください。

(6) **認証** — 次の認証方法の内ひとつが使用されます。

パスワード認証 (SSH v1.5 または V2 クライアント)

- a. クライアントはサーバへパスワードを送信します。
- b. スイッチはクライアントのパスワードとメモリに保存されているものを比較します。
- c. もしマッチするならば、接続は許可されます。

[注意] パスワード認証と共に SSH を使用する場合にも、ホスト公開キーは初期接続時又は手動によりクライアントのホストファイルに与えられます。但し、クライアントキーの設定を行なう必要はありません。

パブリックキー認証 — SSH クライアントがスイッチへの接続を試みる時、SSH サーバはホストキーペアを使用し、セッションキーと暗号化方式のネゴシエートを行います。スイッチに保存されるパブリックキーに対応するプライベートキーを持つクライアントだけがアクセス可能です。以下のやり取りは、このプロセスの間に行われます。

SSH v1.5 クライアント認証

- a. クライアントはスイッチへ RSA パブリックキーを送信します。
- b. スイッチはクライアントのパスワードとメモリに保存されているものを比較します。
- c. 一致した場合、スイッチはそのシークレットキーを使用してランダムな 256-bit スtring を、challenge として生成します。この String をユーザパブリックキーで暗号化し、クライアントへ送信します。
- d. クライアントはプライベートキーを使用して challenge String を解読し、MD5 チェックサムを計算し、それをスイッチへチェックサムバックします。
- e. スイッチは、クライアントから送られたチェックサムと、計算されたオリジナル String を比較します。2つのチェックサムがマッチした場合、クライアントのプライベートキーが認証パブリックキーと一致したことを意味し、クライアントは認証されます。

SSH v2 クライアント認証

- a. クライアントは最初に、DSA パブリックキー認証が受容出来るかどうかを決定する為、スイッチへ問い合わせます。
- b. もし、指定されたアルゴリズムがスイッチでサポートされている場合、クライアントに認証プロセスを続けるよう知らせます。サポートされていない場合は要求は拒絶されます。
- c. クライアントはプライベートキーを使用して生成された署名をスイッチへ送信します。
- d. サーバがこのメッセージを受け取ると、供給されたキーが認証の為に受容できるかどうかをチェックします。可能な場合、署名が正しいかどうかをチェックします。両方のチェックがに成功すると、クライアントは認証されます。

[注意] SSHサーバはTelnetとあわせて最大4クライアントの同時セッションをサポートします。

SSH サーバ設定

Security > SSH (Configure Global) 認証用の SSH サーバの設定を行います。

[注意] SSH サーバを有効にする前に、スイッチでホストキーペアを設定してください。
(200 ページの「ホストキーペアの生成」を参照)

設定・表示項目

SSH Server Status

SSH サーバ機能を有効または無効にします (初期設定 : 無効)

Version

Secure Shell のバージョンナンバー。Version 2.0 と表示されていますが、Version1.5 と 2.0 の両方をサポートしています。

Authentication timeout

SSH サーバの認証時に認証端末からの応答を待つ待機時間 (1-120 (秒)、初期設定 :120 (秒))

Authentication Retries

認証に失敗した場合に、認証プロセスを再度行うことができる回数。設定した回数を超えると認証エラーとなり、認証端末の再起動を行う必要があります (1-5、初期設定 :3 回)

Server-Key Size

SSH サーバのキーサイズ (設定範囲 : 512-896 ビット、初期設定 :768 ビット)

- ー サーバキーはプライベートキーで、本機以外とは共有しません。
- ー SSH クライアントと共有されるホストキーは、1024 ビット固定です。

設定方法

- (1) [Security] → [SSH] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) SSH サーバを有効にします。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Security > SSH

Step: 1. Configure Global

SSH Server Status	☒ Enabled
Version	2.0
Authentication Timeout (1-120)	120 sec
Authentication Retries (1-5)	3
Server-Key Size (512-896)	768

Apply Revert

ホストキーペアの生成

ホスト公開 / プライベートキーペアは本機と SSH クライアント間のセキュアな接続のために使用されます。キーペアが生成された後、ホスト公開キーを SSH クライアントに提供し、上記の機能解説の通りにクライアントの公開キーを本機に取り込む必要があります。

[注意] SSH サーバを有効にする前に、スイッチでホストキーペアを設定してください。
P199 「SSH サーバ設定」を参照してください。

設定・表示項目

Host-Key Type

キータイプは（公開キー、プライベートキーの）ホストキーペアを生成するために使用されます（設定範囲：RSA, DSA, Both、初期設定：Both）
クライアントが本機と最初に接続を確立する場合、SSH サーバはキー交換のために RSA 又は DSA を使用します。その後、データ暗号化に DES(56-bit) 又は 3DES(168 -bit) のいずれかを用いるためクライアントと調整を行ないます。

[注意] 本機は SSHv1.5 クライアントの RSA バージョン 1 と、SSHv2 の DSA バージョン 2 のみ使用します。

Save Host-Key from Memory to Flash

ホストキーを RAM からフラッシュメモリに保存します。ホストキーペアは初期設定では RAM に保存されています。ホストキーペアを生成するには、事前にこのアイテムを選択する必要があります。（初期設定：無効）

設定方法

SSH ホストキーペアの生成

- (1) [Security] → [SSH] をクリックします。
- (2) 「Step」 リストから「Configure Host Key」を選択します。
- (3) 「Action」 リストから「Generate」を選択します。
- (4) ドロップダウンボックスから Host-Key タイプを選択します。
- (5) 必要な場合は、「Save Host-Key from Memory to Flash」にチェックを入れます。
- (6) < Apply > をクリックします。

Security > SSH

Step: 2. Configure Host Key Action: Generate

Host-Key Type Both

☒ Save Host-Key from Memory to Flash

Apply Revert

SSH ホストキーペアの表示

- (1) [Security] → [SSH] をクリックします。
- (2) 「Step」 リストから「Configure Host Key」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Security > SSH

Step: 2. Configure Host Key
Action: Show

Public-Key of Host-Key

☐ RSA

1024 65537
119609178702862888807237652467631858124905824865143258254314388024221765775676299623
464690441799771045913760314090236455706663236948641138707140372204227658717956318840
396770815797455038837438407535796048911157974587778604212269461563627625080602645930
674338102822374869171189489744655655281094211435737669447

☐ DSA

ssh-dss
AAAAB3NzaC1kc3MAAACBAOJW7HJsXcZJ7fvG9/U56/4r2y7z76JCWXBsamEe5T/mH44SHz7jreONzlrHtOpA
qakKG6z2qcReq8a/juV5pR3noL2XXE4Jmd4A4FRE2WKMO00iFvxHTGmrxeX1pzKdGH12HdQzOsNiH0gosgr6
CPpfX4ZNFoJhPNFmJ3b/AL1LAAAFQDQ7jZno19pjvNOwDQcELZeUBvcwAAAEAw3vILR1dyxYJJiG0moSK
emrxtPEIxIarY9xlarpxaPcmwCpNjUA8MDX6UVNZAP+WdC9CjTSHoRceSFZK/kDeJGR/a1mlR9zvfUXOughN

Clear

ユーザパブリックキーのインポート

ユーザの公開キーは、ユーザが公開キー認証メカニズムを使用してログインを行いことが可能になるために、スイッチへアップロードされる必要があります。

ユーザの公開キーがスイッチに存在しない場合、認証を完了するため、SSH は対話型のパスワード認証メカニズムに戻ります。

設定・表示項目

User Name

ドロップ - ダウンボックスで、管理したい公開キーのユーザを選択します。
(P180 「ユーザアカウントの設定」を参照してください)

Public-Key Type

ドロップ - ダウンボックスで、アップロードしたい公開キーを選択します。

- ー RSA: スイッチは SSH バージョン 1、RSA の暗号化された公開キーを受け入れます。
- ー DSA: スイッチは SSH バージョン 2 の、DSA の暗号化された公開キーを受け入れます。

TFTP Server IP Address

TFTP サーバの IP アドレス

Source File Name

ソースファイル名

設定方法

SSH ユーザパブリックキーのコピー

- (1) [Security] → [SSH] をクリックします。
- (2) 「Step」 リストから「Configure User Key」を選択します。
- (3) 「Action」 リストから「Copy」を選択します。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Security > SSH

Step: 3. Configure User Key ▼ Action: Copy ▼

User Name

guest ▼

User-Key Type

RSA ▼

TFTP Server IP Address

192.168.0.4

Source File Name

rsa pub

Apply

Revert

SSH ユーザパブリックキーの表示と消去

- (1) [Security] → [SSH] をクリックします。
- (2) 「Step」 リストから「Configure User Key」を選択します。
- (3) 「Action」 リストから「Show」を選択します。
- (4) 「User Name」 リストからユーザを選択します。
- (5) 消去するホストキータイプを選択します。
- (6) < Clear > をクリックします。

Security > SSH

Step: 2. Configure Host Key Action: Show

Public-Key of Host-Key

☐

RSA

1024 65537
1480220937772193109967882191897869076673078824151724992407025121828690162016474445339
1667942450570093339422932545152202043583189918588264701199521464739810320305865029839
8473670516025543210438660758858919850241166441730463579799255182511108846314033955899
732895735202234665421721768844978831196756189309582533

☐

DSA

ssh-dss
AAAAB3NzaC1kc3MAAACBAKM4i8EgUe89W+vh1+y4z12YpyK8cpCNz30rhCriv1ClKmdgE/fiZPsqrYH/C1AB/
sJ1rNax0sJTUxtb8e2GLk+x8UmQJVuSDdklwZ9ZRoFwWAl0Yyi57V1TK3tUnT9ocCbVJNGckJkXd1uac4OP09
tAPEAuXBuAWGpDAGSmg6pHAAAFQCpzwjn0rSaLiTq53jx1tsj0RILZwAAAIbiL0Cr7GC7ARztGE9dRkT9oh9
uhuiAzcXrAcZTmxhjGsEtMlAtxKm+r1O6pnz2aX9KEzMewJEMuDphOTRnSpMv39XtSW1aSXWtKoGAcQgDsFqK

Clear

3.12.7 ACL (Access Control Lists)

Access Control Lists (ACL) は IPv4 フレーム (IP アドレス、プロトコル、レイヤ 4 プロトコルポート番号、TCP コントロールコード) およびその他のフレーム (MAC アドレス、イーサネットタイプ) のパケットフィルタリングを提供します。

入力されるパケットのフィルタリングを行うには、初めにアクセスリストを作成し必要なルールを追加します。その後、リストに特定のポートをバインドします。

ACL の設定

ACL は IP アドレス、又は他の条件と一致するパケットに対し、アクセスを許可 (Permit) 又は拒否 (Deny) するためのリストです。

本機では入力及び出力パケットに対して ACL と一致するかどうか 1 個ずつ確認を行ないます。パケットが許可ルールと一致した場合には直ちに通信を許可し、拒否ルールと一致した場合にはパケットを破棄します。リスト上の許可ルールに一致しない場合、パケットは破棄され、リスト上の拒否ルールに一致しない場合、パケットは通信を許可されます。

機能解説

ACL は以下の制限があります。

- 最大 ACL 設定数は 64 個です。
- システムごとに設定できるルールは、512 ルールです。
- 各 ACL は最大 32 ルールまで設定可能ですが、リソース制限により、ポートにバウンドされたルールの平均は 20 以上にはできません

タイムレンジの設定

Security > ACL (Configure Time Range) ページでは、ACL 機能が適用される時間の範囲を設定します。

設定・表示項目

Add

Time-Range Name

タイムレンジ名（範囲：1-30 文字）

Add Rule

Time-Range

タイムレンジ名（範囲：1-30 文字）

Mode

- Absolute — 時間またはタイムレンジを指定
 - Start/End — 開始と終了の、時 (hours)、分 (minutes)、月 (month)、日 (day)、年 (year) を指定します。
- Periodic — 周期を指定
 - Start/To — 開始と終了の、曜日と時 (hours)、分 (minutes)、月 (month) を指定します。

設定方法

タイムレンジを設定

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure Time Range」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) タイムレンジの名前を入力します。
- (5) < Apply > をクリックします。

Security > ACL

Step: 1. Configure Time-Range Action: Add

Time-Range Name R&D

Apply Revert

タイムレンジのリストを表示

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure Time Range」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Security > ACL

Step: 1. Configure Time-Range Action: Show

Time-Range List Max: 16 Total: 1

	Time-Range Name
☐	R&D

Delete Revert

タイムレンジのルールを設定

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure Time Range」を選択します。
- (3) 「Action」 リストから「Add Rule」を選択します。
- (4) ドロップダウンリストから、タイムレンジの名前を選択します。
- (5) モードのオプションを "Absolute"、"Periodic" から選択します。
- (6) 必要な項目の編集を行います。
- (7) < Apply > をクリックします。

Security > ACL

Step: 1. Configure Time-Range Action: Add Rule

Time-Range R&D

Mode Periodic

Start To

Days of the week Weekend Days of the week Sunday

Hours (0-23) 5 Hours (0-23) 6

Minutes (0-59) 0 Minutes (0-59) 0

Apply Revert

設定されたタイムレンジのルールを表示

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure Time Range」を選択します。
- (3) 「Action」 リストから「Show Rule」を選択します。

Security > ACL

Step: 1. Configure Time-Range Action: Show Rule

Time-Range time1

Time-Range Rule List Max: 8 Total: 4

☐	Mode	Start	End
☐	Absolute	2009-01-01 10:05	2010-01-31 20:10
☐	Periodic	Daily 10:05	Daily 20:10
☐	Periodic	Monday 10:05	Tuesday 20:10
☐	Periodic	Monday 00:00	Tuesday 23:59

Delete Revert

TCAM 使用率の表示

Security > ACL (Configure ACL - Show TCAM) ページを使用し、使用するナンバーポリシー制御エントリ、フリーエントリの番号、全体的なパーセンテージを含む、TCAM (Ternary Content Addressable Memory) ユーティライゼーションパラメータを表示します。

機能解説

ポリシー制御エントリ (PCEs) は、Access Control Lists (ACLs)、IP Source Guard フィルタルール、Quality of Service (QoS) プロセス等、検索ベースのルールに頼る様々なシステムで使用されます。例えば、ポートに ACL をバインディングした時、ACL のそれぞれのルールは 2 つの PCE を使用し、ポートに IP ソースガードフィルタルールを設定する時にも同じく 2 つの PCE を使用します。

設定・表示項目

Total Policy Control Entries

使用するナンバーポリシー制御エントリ

Free Policy Control Entries

使用できるポリシー制御エントリの数

Entries Used by System

オペレーティングシステムによって使用されるポリシー制御エントリの数

Entries Used by User

ACL 等の設定によって使用されるポリシー制御エントリの数

TCAM Utilization

使用中の TCAM の全体的なパーセンテージ

設定方法

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure ACL」を選択します。
- (3) 「Action」 リストから「Show TCM」を選択します。

Security > ACL	
Step:	2. Configure ACL ▼
Action:	Show TCAM ▼
Total Policy Control Entries	512
Free Policy Control Entries	352
Entries Used by System	160
Entries Used by User	0
TCAM Utilization	31.25%

ACL 名およびタイプの設定

ACL Configuration ページでは、ACL の名前及びタイプを設定することができます。

設定・表示項目

ACL Name

ACL 名 (15 文字以内)

Type

- IP Standard — ソース IPv4 アドレスに基づくパケットフィルタリングを行います。
- IP Extended — ソース又はディステーション IPv4 アドレス、プロトコルタイプ、プロトコルポート番号、TCP コントロールコードに基づくフィルタリングを行ないます。
- MAC — ソース又はディステーション MAC アドレス、イーサネットフレームタイプ (RFC 1060) に基づくフィルタリングを行なう MAC ACL モード。
- ARP — ARP インспекション (詳細は 219 ページの「ARP インспекション」を参照) を使用した静的 IP-to-MAC アドレスバインディングを指定します。

設定方法

ACL の名前とタイプを設定

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure ACL」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) ACL 名を入力し、ACL タイプを選択します。
- (5) < Apply >をクリックします。

Security > ACL

Step: 2. Configure ACL Action: Add

ACL Name R&D

Type IP Standard

Apply Revert

ACL リストを表示

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure ACL」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Security > ACL

Step: 2. Configure ACL Action: Show

ACL List Max: 64 Total: 1

	ACL Name	Type
☐	R&D	IP Standard

Delete Revert

スタンダード IPv4 ACL の設定

Security > ACL (Configure ACL - Add Rule - IP Standard) ページを使用し、スタンダード IPv4 ACL の設定を行います。

設定・表示項目

Type

ネームリストに表示する ACL のタイプを選択します。

Name

選択したタイプにマッチする ACL の名前を表示します。

Action

ACL のルールが「permit (許可)」か「deny(拒否)」を選択します。

Address Type

ソース IP アドレスの指定を行いません。"any" ではすべての IP アドレスが対象となります。"host" ではアドレスフィールドのホストが対象となります。"IP" では、IP アドレスとサブネットマスクにより設定した IP アドレスの範囲が対象となります。

(オプション：Any, Host, IP、初期設定：Any)

Source IP Address

ソース IP アドレス

Source SubnetMask

ソースサブネットマスク

Time Range

タイムレンジ名

設定方法

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure ACL」を選択します。
- (3) 「Action」 リストから「Add Rule」を選択します。
- (4) タイプリストから "Standard IP" を選択します。
- (5) ネームリストから ACL 名を選択します。
- (6) 「Action」を指定します。
- (7) アドレスタイプを選択します。
- (8) "Host" が選択された場合、特定のアドレスを入力します。"IP" が選択された場合、アドレス範囲のサブネットアドレスとマスクを入力します。
- (9) < Apply > をクリックします。

Security > ACL

Step: 2. Configure ACL **Action:** Add Rule

Type ☒ IP Standard ☐ IP Extended ☐ MAC ☐ ARP

Name R&D

Action Permit

Address Type Host

Source IP Address 192.168.0.21

Source Subnet Mask 255.255.255.255

☒ **Time-Range** R&D

Apply Revert

拡張 IPv4 ACL の設定

Security > ACL (Configure ACL - Add Rule - IP Extended) ページを使用し、拡張 IPv4 ACL の設定を行います。

設定・表示項目

Type

ネームリストに表示する ACL のタイプを選択します。

Name

選択したタイプにマッチする ACL の名前を表示します。

Action

ACL のルールが「permit (許可)」か「deny(拒否)」を選択します。

Source/Destination Address Type

ソース又はディスティネーション IP アドレスの設定を行います。"any" ではすべての IP アドレスが対象となります。"host" ではアドレスフィールドのホストが対象となります。"IP" では、IP アドレスとサブネットマスクにより設定した IP アドレスの範囲が対象となります (オプション: Any, Host, IP、初期設定: Any)

Source/Destination IP Address

ソース又はディスティネーション IP アドレス

Source/Destination Subnet Mask

ソース又はディスティネーション IP アドレスのサブネットマスク

Source /Destination Port

プロトコルタイプに応じたソース / ディスティネーションポート番号 (範囲: 0-65535)

Source/Destination Port Bitmask

一致するポートビットを表す 10 進数 (範囲: 0-65535)

Protocol

TCP、UDP のプロトコルタイプの指定又はポート番号 (0-255)

(オプション: TCP, UDP, Others;、初期設定: TCP)

Service Type

以下の基準に基づいたパケットプライオリティセッティング

- ToS—Type of Service レベル (範囲: 0-15)
- Precedence—IP precedence レベル (範囲: 0-7)
- DSCP— DSCP priority レベル (範囲: 0-63)

Control Code

TCP ヘッダのバイト 14 内のフラグ・ビットを指定 (範囲: 0-63)

Control Code Bit Mask

一致するコードビットの値 (範囲: 0-63)

※コントロールビットマスクは、コントロールコードに使用される 10 進数の値です。
10 進数の値を入力し、等価な 2 進数のビットが "1" の場合、一致するビットであり、"0" の場合、拒否するビットとなります。

以下のビットが指定されます。

- 1 (fin) — Finish
- 2 (syn) — Synchronize
- 4 (rst) — Reset
- 8 (psh) — Push
- 16 (ack) — Acknowledgement
- 32 (urg) — Urgent pointer

例えば、コード値及びコードマスクを利用し、パケットをつかむには以下のフラグをセットします。

- 有効な SYN flag — コントロールコード：2、コントロールビットマスク：2
- 有効な SYN 及び ACK — コントロールコード：18、コントロールビットマスク：18
- 有効な SYN 及び無効な ACK — コントロールコード：2、コントロールビットマスク：18

Time Range

タイムレンジ名

設定方法

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure ACL」を選択します。
- (3) 「Action」 リストから「Add Rule」を選択します。
- (4) タイプリストから "Extended IP" を選択します。
- (5) ネームリストから ACL 名を選択します。
- (6) 「Action」を指定します。
- (7) アドレスタイプを選択します。
- (8) "Host" が選択された場合、特定のアドレスを入力します。"IP" が選択された場合、アドレス範囲のサブネットアドレスとマスクを入力します。
- (9) 必要な項目の入力・編集を行います。
- (10) < Apply >をクリックします。

Security > ACL

Step: 2. Configure ACL
Action: Add Rule

Type
☐ IP Standard
☒ IP Extended
☐ MAC
☐ ARP

Name
R&D2

Action
Permit

Source Address Type
IP

Source IP Address
10.7.1.0

Source Subnet Mask
255.255.255.0

Source Port (0-65535)

Source Port Bit Mask (0-65535)

Destination Address Type
Any

Destination IP Address
0.0.0.0

Destination Subnet Mask
0.0.0.0

Destination Port (0-65535)

Destination Port Bit Mask (0-65535)

Protocol
☒ TCP (6)
☐ UDP (17)
☐ Others

Control Code (0-63)

Control Code Bit Mask (0-63)

Service Type
☒ ToS (0-15)
☐ Precedence (0-7)
☐ DSCP (0-63)

☐ Time-Range
R&D

Apply
Revert

MAC ACL の設定

Security > ACL (Configure ACL - Add Rule - MAC) ページを使用し、ハードウェアアドレス、パケットフォーマット、イーサネットタイプを基にした ACL の設定をおこないます。

設定・表示項目

Type

ネームリストに表示する ACL のタイプを選択します。

Name

選択したタイプにマッチする ACL の名前を表示します。

Action

ACL のルールが「permit (許可)」か「deny (拒否)」を選択します。

Source/Destination Address Type

"Any" を使用した場合、全ての可能なアドレスを含み、"Host" を指定した場合はアドレスフィールドにホストアドレスを入れます。"MAC" を指定した場合、アドレスとビットマスクフィールドへアドレス範囲を入力します。(オプション: Any、Host、MAC 初期設定: Any)

Source/Destination MAC Address

ソース又はディスティネーション MAC アドレス

Source/Destination Bitmask

ソース又はディスティネーション MAC アドレスの 16 進数のマスク

Packet Format

本属性は次のパケット・タイプから選択できます。

- Any — すべてのイーサネットパケットタイプ
- Untagged-eth2 — タグなしイーサネット II パケット
- Untagged-802.3 — タグなしイーサネット IEEE802.3 パケット
- Tagged-eth2 — タグ付イーサネット II パケット
- Tagged-802.3 — タグ付イーサネット IEEE802.3 パケット

VID

VLAN ID (範囲: 1-4095)

VID Mask

VLAN ビットマスク (範囲: 1-4095)

Ethernet Type

この項目はイーサネット II フォーマットのパケットのフィルタリングに使用します (範囲: 600-fff hex) イーサネットプロトコルタイプのリストは RFC 1060 で定義されていますが、一般的なタイプとしては、0800(IP)、0806(ARP)、8137(IPX) 等があります。

Ethernet Type Bit mask

プロトコルビットマスク (範囲: 600-fff hex)

Time Range

タイムレンジ名

設定方法

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure ACL」を選択します。
- (3) 「Action」 リストから「Add Rule」を選択します。
- (4) タイプリストから "MAC" を選択します。
- (5) ネームリストから ACL 名を選択します。
- (6) 「Action」を指定します。
- (7) アドレスタイプを選択します。
- (8) "Host" が選択された場合、特定のアドレスを入力します。"MAC" が選択された場合、アドレス範囲のベースアドレスとビットマスクを入力します。
- (9) 必要な項目の入力・編集を行います。
- (10) < Apply >をクリックします。

Security > ACL

Step: 2. Configure ACL
Action: Add Rule

Type
☐ IP Standard
☐ IP Extended
☒ MAC
☐ ARP

Name
R&D3

Action
Permit

Source Address Type
Any
Destination Address Type
Any

Source MAC Address
00-00-00-00-00-00
Destination MAC Address
00-00-00-00-00-00

Source Bit Mask
00-00-00-00-00-00
Destination Bit Mask
00-00-00-00-00-00

Packet Format
Any

VID (1-4094)
12
Ethernet Type
(600-FFFF, hexadecimal value)

VID Bit Mask (1-4094)
4094
Ethernet Type Bit Mask
(600-FFFF, hexadecimal value)

☐ Time-Range
R&D

Apply
Revert

ARP ACL の設定

Security > ACL (Configure ACL - Add Rule - ARP) ページを使用し、ARP メッセージアドレスをベースにした ACL の設定をおこないます。

ARP インспекションはこれらの ACL を、疑わしいトラフィックのフィルタを行う為に使用することが出来ます。(詳細は 219 ページの「ARP インспекション」を参照してください)

設定・表示項目

Type

ネームリストに表示する ACL のタイプを選択します。

Name

選択したタイプにマッチする ACL の名前を表示します。

Action

ACL のルールが「permit (許可)」か「deny(拒否)」を選択します。

Packet Type

ARP リクエスト、ARP レスポンス、イーサタイプを指定します。

(範囲：Request、Response、All 初期設定：Request)

Source/Destination IP Address Type

ソースまたはディスティネーション IP v4 アドレスを指定します。îAnyî を使用することで、全ての可能なアドレスを含み、îHostî はアドレスフィールドに特定のホストアドレスを指定します。îIPî はアドレスとマスクフィールドへアドレスの範囲を指定します。(範囲：Any、Host、IP 初期設定：Any)

Source/Destination IP Address

ソースまたはディスティネーション IP アドレス

Source/Destination IP Subnet Mask

ソースまたはディスティネーションアドレスのサブネットマスク

Source/Destination MAC Address Type

ソースまたはディスティネーション IP v4 アドレスを指定します。"Any" を使用することで、全ての可能なアドレスを含み、"Host" はアドレスフィールドに特定のホストアドレスを指定します。"MAC" はアドレスとマスクフィールドへアドレスの範囲を指定します。(範囲：Any、Host、IP 初期設定：Any)

Source/Destination MAC Address

ソースまたはディスティネーション MAC アドレス

Source/Destination MAC Bit Mask

ソースまたはディスティネーション MAC アドレスの 16 進数マスク。

Log

アクセスコントロールエントリに一致したパケットのログ。

設定方法

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure ACL」を選択します。
- (3) 「Action」 リストから「Add Rule」を選択します。
- (4) タイプリストから "ARP" を選択します。
- (5) ネームリストから ACL 名を選択します。
- (6) 「Action」を指定します。
- (7) パケットタイプを選択します。
- (8) アドレスタイプを選択します。
- (9) "Host" が選択された場合、特定のアドレスを入力します。"IP" が選択された場合、アドレス範囲のベースアドレスとビットマスクを入力します。
- (10) 必要な項目の入力・編集を行います。
- (11) < Apply > をクリックします。

Security > ACL

Step: 2. Configure ACL
Action: Add Rule

Type
☐ IP Standard
☐ IP Extended
☐ MAC
☒ ARP

Name
ARP_ACL

Action
Permit

Packet Type
All

Source IP Address Type
Any

Destination IP Address Type
Any

Source IP Address
0.0.0.0

Destination IP Address
0.0.0.0

Source IP Subnet Mask
0.0.0.0

Destination IP Subnet Mask
0.0.0.0

Source MAC Address Type
Any

Destination MAC Address Type
Any

Source MAC Address
00-00-00-00-00-00

Destination MAC Address
00-00-00-00-00-00

Source MAC Bit Mask
00-00-00-00-00-00

Destination MAC Bit Mask
00-00-00-00-00-00

☐ Log

Apply
Revert

ACL へのポートのバインド

ACL の設定が完了後、フィルタリングを機能させるためにはポートをバインドする必要があります。

1 つの IP アクセスリストと MAC アクセスリストをポートに割り当てることができます。

機能解説

- ・ 本機は入力フィルタの ACL のみサポートしています。
- ・ 入力フィルタリングを行うポートに、1 つの ACL のみをバインドすることができます。

設定・表示項目

Type

ポートへバインドする ACL のタイプを選択

Port

ポート又は拡張モジュールスロット（範囲：1-26）

ACL

入力パケットに対する ACL

Time Range

タイムレンジ名

設定方法

- (1) [Security] → [ACL] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) タイプリストから "IP" または "MAC" を選択します。
- (4) ACL リストから ACL 名を選択します。
- (5) < Apply > をクリックします。

The screenshot shows the 'Security > ACL' configuration page. At the top, there is a 'Step:' dropdown menu set to '3. Configure Interface'. Below this, the 'Type' section has two radio buttons: 'IP' (selected) and 'MAC'. The 'Port' section has a dropdown menu showing '1'. The 'IN' section has a checked checkbox and a dropdown menu showing 'R&D'. The 'Time-Range' section has an unchecked checkbox and a dropdown menu showing 'R&D'. At the bottom right, there are 'Apply' and 'Revert' buttons.

3.12.8 ARP インスペクション

ARP インスペクションは、Address Resolution packet (ARP) プロトコルのため、MAC アドレスバインディングの妥当性の検査を行うセキュリティ機能です。

この機能により、ある種の man-in-the-middle 攻撃等からネットワークを保護できます。

これはローカル ARP キャッシュがアップデートされるか、またはパケットが適切な目的地に転送される前に、全ての ARP リクエストを途中で捕らえ、これらのパケットのそれぞれを照合することによって達成されます。無効な ARP パケットは破棄されます。

ARP インスペクションは、信頼できるデータベースに保存された正当な IP-to-MAC アドレスバインディングに基づいて ARP パケットの正当性を決定します。(245 ページの「DHCP スヌーピング」を参照)

このデータベースは、それがスイッチと VLAN で有効になっている時に DHCP スヌーピングによって構築されます。

また、ARP インスペクションはユーザで設定された ARP アクセスコントロールリスト (ACL) に対して、ARP パケットの妥当性を確認することも可能です。(216 ページの「ARP ACL の設定」を参照)

機能解説

ARP インスペクションの有効/無効

- ARP インスペクションはスイッチ全体および VLAN ベースでコントロールされます。
- 初期設定では ARP インスペクションはスイッチと全て VLAN の両方で無効になっています。
 - ARP インスペクションがグローバルで有効の場合、有効になっている VLAN 上でのみアクティブになります。
 - ARP インスペクションがグローバルで有効の場合、インスペクションが有効な VLAN の全ての ARP リクエストとリプライパケットは CPU ヘリダイレクトし、それらのスイッチング行為は ARP インスペクションエンジンによって処理されます。
 - ARP インスペクションがグローバルで無効の場合、有効になっている物も含め全ての VLAN で非アクティブになります。
 - ARP インスペクションが無効の場合、全ての ARP リクエストとリプライパケットは ARP インスペクションエンジンを回避し、それらのスイッチング行為はその他全てのパケットと同様になります。
 - グローバル ARP インスペクションの無効化とその後の再有効化は、VLAN の ARP インスペクション設定に影響を与えません。
 - ARP インスペクションがグローバルで無効の際、個々の VLAN の ARP インスペクション設定は可能です。グローバルで ARP インスペクションが再度有効になった時、これらの設定変更はアクティブになります。
- 現在のファームウェアバージョンの ARP インスペクションエンジンはトランクポートの ARP インスペクションをサポートしていません。

ARP インспекションのグローバル設定

ARP インспекションは、スイッチ全体と VLAN ごとの両方で動作し、インспекションパラメータはそれぞれの VLAN で設定します。

機能解説

ARP インспекション妥当性チェック

- 初期設定で、ARP インспекション妥当性チェックは無効になっています。
- 以下の妥当性検査の内、最低 1 つを指定することにより、ARP インспекション妥当性チェックをグローバルで有効にすることが可能です。以下の項目のいずれも、同時にアクティブにすることができます。
 - Destination MAC
ARP ボディのターゲット MAC アドレスにたいして、イーサネットヘッダの送信先 MAC アドレスをチェックします。このチェックは ARP レスポンスのために実行されます。
有効の際、異なる MAC アドレスを持つパケットは無効として分類され破棄されます。
 - IP
無効と予期せぬ IP アドレスの ARP ボディをチェックします。
これらのアドレスは 0.0.0.0、255.255.255.255 および全ての IP マルチキャストアドレスを含みます。セNDER IP アドレスは全ての ARP リクエストとレスポンスでチェックされ、ターゲット IP アドレスは ARP レスポンスのみチェックされます。
 - Source MAC
ARP ボディのセNDER MAC アドレスにたいし、イーサネットヘッダのソース MAC アドレスのチェックをおこないます。
このチェックは ARP リクエストとレスポンス両方に実行されます。
有効の際、異なる MAC アドレスを持つパケットは無効として分類され破棄されます。

ARP インспекションロギング

- 初期設定で、ARP インспекションのロギングはアクティブになっており無効にはできません。
- 管理者はログファシリティレートの設定をおこなえます。
- スイッチがパケットの破棄を行った時、スイッチはログバッファにエントリを置き、コントロールされたレートを基にシステムメッセージを生成します。システムメッセージが表示された後、エントリはログバッファからクリアされます。
- それぞれのログエントリは受信 VLAN、ポート番号、ソース・ディスティネーション IP アドレス、ソース・ディスティネーション MAC アドレスの情報を含みます。
- 複数、同一の不正な ARP パケットが同じ VLAN で連続して受信された場合、ロギングファシリティはログバッファの 1 つのエントリと、1 つの対応するシステムメッセージのみ生成します。
- ロギングバッファが一杯になると、最も古い項目から新しいエントリで置き換えられます。

設定・表示項目

ARP Inspection Status

ARP インスペクションをグローバルで有効にします。(初期設定：無効)

ARP Inspection Validation

以下のオプションの内いずれかが使用可能な場合、拡張 ARP インスペクション検査を有効にできます。(初期設定：無効)

- Dst-MAC
ARP レスポンスのボディ内のターゲット MAC アドレスに対し、イーサネットヘッダのディスティネーション MAC アドレスの妥当性検査をおこないます。
- IP
不正および予期せぬ IP アドレスの ARP ボディをチェックします。
セNDER IP アドレスは全ての ARP リクエストとレスポンスをチェックされます。
ターゲット IP アドレスは ARP レスポンスのみチェックされます。
- Src-MAC
ARP ボディ内のセNDER MAC アドレスに対し、イーサネットヘッダのソース MAC アドレスの妥当性検査をおこないます。このチェックは ARP リクエストとレスポンスの両方に実行されます。

Log Message Number

ログメッセージに保存するエントリの最大数 (範囲：0-256 初期設定：5)

Log Interval

ログメッセージが送信される間隔 (範囲：0-86400 秒 初期設定：1 秒)

設定方法

- (1) [Security] → [ARP Inspection] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) ARP インスペクションをグローバルで有効にし、その他必要な項目の設定を行います。
- (4) < Apply > をクリックします。

Security > ARP Inspection

Step: 1. Configure General

ARP Inspection Status

☒ Enabled

ARP Inspection Validate

☒ Dst-MAC
☐ IP
☐ Src-MAC

Log Message Number (0-256)

Log Interval (0-86400)

 sec

ARP インスペクション VLAN 設定

Security > ARP Inspection (Configure VLAN) ページを使用し、VLAN の ARP インスペクションの有効・使用 ARP ACL の指定を行います。

機能解説

ARP インスペクション VLAN フィルタ (ACL)

- 初期設定で、ARP インスペクション ACL は設定されておらず、この機能は無効です。
- ARP インスペクション ACL は ARP ACL Configuration ページで設定されます。(216 ページの「ARP ACL の設定」を参照)
- ARP インスペクション ACL は設定されたどの VLAN にも適用することが可能です。
- ARP インスペクションは、正当な IP-to-MAC アドレスバインディングのリストのために、DHCP スヌーピングバインディングデータベースを使用します。ARP ACL は DHCP スヌーピングバインディングデータベースのエントリに優先されます。スイッチは最初に、指定された ARP ACL と ARP パケットを比較します。
- "static が指定された場合、ARP パケットは選択された ACL パケットがいずれかのマッチングルールによってフィルタされることにたいしての、妥当性の検査のみ行われます。いずれのルールにもマッチングしないパケットは破棄され、DHCP スヌーピングバインディングデータベースチェックは回避されます。
- "static が指定されない場合、ARP パケットは最初に選択した ACL に対して妥当性を検査されます。ACL ルールとパケットが一致しない場合、DHCP スヌーピングバインディングデータベースはそれらの正当性を決定します。

設定・表示項目

ARP Inspection VLAN ID

VLAN を選択 (初期設定: 1)

ARP Inspection VLAN Status

選択した VLAN で ARP インスペクションを有効 (初期設定: 無効)

ARP Inspection ACL Name

— ARP ACL — 設定された ARP ACL の選択を許可

— Static — ARP ACL が選択され、また static mode もまた選択されている時、本機は ARP インスペクションのみ実行し、DHCP スヌーピングバインディングデータベースの妥当性検査を回避します。ARP ACL が選択が選択され、static mode が選択されていない時、本機は最初に ARP インスペクシ

設定方法

- (1) [Security] → [ARP Inspection] をクリックします。
- (2) 「Step」 リストから「Configure VLAN」を選択します。
- (3) 必要とされる VLAN で ARP インспекションを有効にし、その他項目の設定を行います。
- (4) < Apply > をクリックします。

Security > ARP Inspection

Step: 2. Configure VLAN ▼

ARP Inspection VLAN ID

1 ▼

ARP Inspection VLAN

☒ Enabled

Status

ARP Inspection ACL Name

☒ R&D4 ▼ ☐ Static

Apply

Revert

ARP インспекションインタフェース設定

Security > ARP Inspection (Configure Interface) ページを使用して、ARP インспекションを必要とするポートを指定し、パケットインспекションレートを調整します。

設定・表示項目

Port

ポート番号

Trust Status

ポートを Trusted または Untrusted に設定（初期設定：Untrusted）

Packet Rate Limit

Untrusted ポートで受信される ARP パケットのレート制限（範囲：0-2048 初期設定：15）
0 は制限無しを意味します。

設定方法

- (1) [Security] → [ARP Inspection] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) ARP インспекションを必要とする Trusted ポートを指定し、パケットレートを調整してください。
- (4) < Apply > をクリックします。

Security > ARP Inspection

Step: 3. Configure Interface

Port Configuration List Max: 26 Total: 26

Port	Trust Status	Packet Rate Limit (0-2048 pps)
1	☒ Enabled	☒ 15
2	☐ Enabled	☒ 15
3	☐ Enabled	☒ 15
4	☐ Enabled	☒ 15
5	☐ Enabled	☒ 15

ARP インспекション統計値の表示

ARP インспекションポート情報を表示します。

Trusted ポートのリスト、様々な理由で処理または破棄された ARP パケットの数に関する統計情報などが確認できます。

設定・表示項目

ARP Inspection Statistics

- Received ARP packets before ARP inspection rate limit
ARP インспекションレート制限を越えない受信 ARP パケットの数
- Dropped ARP packets in the process of ARP inspection rate limit
ARP レート制限を越えた（破棄された）ARP パケットの数
- Total ARP packets processed by ARP inspection
ARP インспекションエンジンに処理された全ての ARP パケット数
- ARP packets dropped by additional validation (Src-MAC)
ソース MAC アドレステストに落ちたパケット数
- ARP packets dropped by additional validation (Dst-MAC)
ディスティネーション MAC アドレステストに落ちたパケット数
- ARP packets dropped by additional validation (IP)
IP アドレステストに落ちた ARP パケット数
- ARP packets dropped by ARP ACLs
ARP ACL ルールに対する妥当性検査に落ちた ARP パケットの数
- ARP packets dropped by DHCP snooping
DHCP スヌーピングバインディングデータベースに対する妥当性検査に落ちたパケット数

設定方法

- (1) [Security] → [ARP Inspection] をクリックします。
- (2) 「Step」 リストから「Configure Information」を選択します。
- (3) 「Action」 リストから「Show Statistics」を選択します。

Security > ARP Inspection	
Step:	4. Show Information
Action:	Show Statistics
Received ARP packets before ARP inspection rate limit	0
Dropped ARP packets in processing ARP inspection rate limit	0
Total ARP packets processed by ARP inspection	0
ARP packets dropped by additional validation (Src-MAC)	0
ARP packets dropped by additional validation (Dst-MAC)	0
ARP packets dropped by additional validation (IP)	0
ARP packets dropped by ARP ACLs	0
ARP packets dropped by DHCP snooping	0

ARP インスペクションログの表示

Security > ARP Inspection (Show Information - Show Log) ページを使用し、関連付けられた VLAN、ポート、アドレスコンポーネント等、ログに保存されたエントリについての情報を表示します。

設定・表示項目

ARP Inspection Log

ARP インスペクションロギングパラメータを設定します。

- VLAN ID
- Port
- Src. IP Address
- Dst. IP Address
- Src. MAC Address
- Dst. MAC Address

設定方法

- (1) [Security] → [ARP Inspection] をクリックします。
- (2) 「Step」 リストから「Configure Information」を選択します。
- (3) 「Action」 リストから「Show Log」を選択します。

Security > ARP Inspection

Step: 4. Show Information Action: Show Log

ARP Inspection Log List Max: 256 Total: 2

VLAN ID	Port	Src. IP Address	Dst. IP Address	Src. MAC Address	Dst. MAC Address
1	15	192.168.1.1	192.168.1.5	11-22-33-44-55-66	AA-BB-CC-DD-EE-FF
1	17	192.168.1.3	192.168.1.23	11-4E-33-75-55-BB	A0-3B-C9-DD-4E-1F

3.12.9 管理アドレスのフィルタリング

Web インタフェース、SNMP、Telnet による管理アクセスが可能な IP アドレス又は IP アドレスグループを最大 15 個作成できます。

機能解説

- 管理インタフェースは、初期設定ではすべての IP アドレスに対して接続可能な状態になっています。フィルタリストに 1 つでも IP アドレスを指定すると、そのインタフェースは指定したアドレスからの接続のみを許可します。
- 設定以外の無効な IP アドレスから管理アクセスに接続された場合、本機は接続を拒否し、イベントメッセージをシステムログに保存し、トラップメッセージの送信を行います。
- SNMP、Web、Telnet アクセスへの IP アドレスまたは IP アドレス範囲の設定は合計で最大 5 つまで設定可能です。
- SNMP、Web、Telnet の同一グループに対して IP アドレス範囲を重複して設定することはできません。異なるグループの場合には IP アドレス範囲を重複して設定することは可能です。
- 設定した IP アドレス範囲から特定の IP アドレスのみを削除することはできません。IP アドレス範囲をすべて削除し、その後設定をし直して下さい。
- IP アドレス範囲の削除は IP アドレス範囲の最初のアドレスだけを入力しても削除することができます。また、最初のアドレスと最後のアドレスの両方を入力して削除することも可能です。

設定・表示項目

Mode

- Web — Web グループの IP アドレスを設定
- SNMP — SNMP グループの IP アドレスを設定
- Telnet — Telnet グループの IP アドレスを設定

Start IP Address

IP アドレス、又は IP アドレスを範囲で指定している場合の最初の IP アドレス

End IP Address

IP アドレスを範囲で指定している場合の最後の IP アドレス

設定方法

管理アクセスを許可される IP アドレスリストを作成

- (1) [Security] → [IP Filter] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) フィルタを行う管理インタフェースを選択します。(Web、SNMP、Telnet)
- (4) インタフェースへの管理アクセスが許可される IP アドレスまたは範囲を入力します。
- (5) < Apply > をクリックします。

Security > IP Filter

Action: Add ▼

Mode: ☒ Web ☐ SNMP ☐ Telnet

Start IP Address: 192.168.1.10

End IP Address: 192.168.1.20

Apply Revert

管理アクセスを許可される IP アドレスリストを表示

- (1) [Security] → [IP Filter] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

Security > IP Filter

Action: Show ▼

Mode: ☒ Web ☐ SNMP ☐ Telnet

Web IP Filter List Max: 5 Total: 1

	Start IP Address	End IP Address
☐	192.168.1.10	192.168.1.20

Delete Revert

3.12.10 ポートセキュリティの設定

ポートセキュリティはポートに対し、そのポートを使用してネットワークにアクセスすることができるデバイスの MAC アドレスを設定し、その他の MAC アドレスのデバイスではネットワークへのアクセスを行えなくする機能です。

ポートセキュリティを有効にした場合、本機は有効にしたポートにおいて MAC アドレスの学習を停止します。本機に入って来た通信のうち、ソースアドレスが動的・静的なアドレステーブルに登録済みの MAC アドレスの場合にのみ、そのポートを利用したネットワークへのアクセスを行うことができます。登録されていない不正な MAC アドレスのデバイスがポートを使用した場合、侵入は検知され自動的にポートを無効にし、トラップメッセージの送信を行います。

ポートセキュリティを使用する場合、ポートに許可する MAC アドレスの最大数を設定し、動的に < ソース MAC アドレス、VLAN > のペアをポートで受信したフレームから学習します。P108 「静的アドレスの設定」を使用し、入力により MAC アドレスを設定することもできます。ポートに設定された最大 MAC アドレス数に達すると、ポートは学習を終了します。アドレステーブルに保存された MAC アドレスは保持され、時間の経過により消去されることはありません。これ以外のデバイスがポートを利用しようとしても、スイッチにアクセスすることはできません。

機能解説

- セキュリティポートに設定できるポートは、以下の制限があります。
 - － LACP または静的トランクポートに設定できません。
 - － ハブなどネットワーク接続デバイスは接続しないで下さい。
- 初期設定では、セキュリティポートへのアクセスを許可している最大 MAC アドレス数は "0" です。セキュリティポートへのアクセスを許可するためには、最大 MAC アドレス数を 1-1024 のいずれかに設定する必要があります。
- セキュリティ違反によりポートが Disabled となった（シャットダウンした）場合、P48 「インタフェース設定」からポートの有効化を行ってください。

設定・表示項目

Port

ポート番号

Action

- － None — 動作が行なわれません（初期設定）
- － Trap — SNMP トラップメッセージを送信します。
- － Shutdown — ポートを無効にします。
- － Trap and Shutdown — ポートを無効にし、SNMP トラップメッセージを送信します。

Security Status

ポートセキュリティの有効 / 無効（初期設定：無効）

Max MAC Count

ポートが学習可能な MAC アドレス数（設定範囲：0-1024、0 は無効）

設定方法

管理アクセスを許可される IP アドレスリストを作成

- (1) [Security] → [Port Security] をクリックします。
- (2) ポートで無効なアドレスが検出された時にとる行動を設定し、「Security Status」チェックボックスで機能を有効にします。ポートで許可される MAC アドレスの最大数を入力し、< Apply > をクリックします。

Security > Port Security

Port Security List Max: 26 Total: 26 1 2 3

Port	Action	Security Status	Max MAC Count (0-1024)
1	Trap and Shutdown ▼	☒ Enabled	0
2	None ▼	☐ Enabled	0
3	None ▼	☐ Enabled	0
4	None ▼	☐ Enabled	0
5	None ▼	☐ Enabled	0

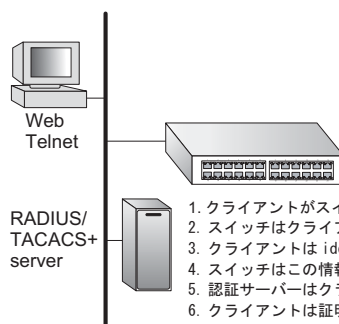
3.12.11 802.1x ポート認証

スイッチは、クライアント PC から容易にネットワークリソースにアクセスすることができません。しかし、それによりは好ましくないアクセスを許容し、ネットワーク上の機密のデータへのアクセスが行える可能性もあります。

IEEE802.1x(dot1x) 規格では、ユーザ ID 及びパスワードにより認証を行うことにより無許可のアクセスを防ぐポートベースのアクセスコントロールを提供します。

ネットワーク中のすべてのポートへのアクセスはセントラルサーバによる認証を行うことで、どのポートからでも 1 つの認証用のユーザ ID 及びパスワードによりユーザの認証が行えます。

本機では Extensible Authentication Protocol over LAN (EAPOL) によりクライアントの認証プロトコルメッセージの交換を行います。RADIUS サーバによりユーザ ID とアクセス権の確認を行います。



1. クライアントがスイッチへのアクセスを試みます。
2. スイッチはクライアントへ identity リクエストを送ります。
3. クライアントは identity 情報を送り返します。
4. スイッチはこの情報を認証サーバへ転送します。
5. 認証サーバはクライアントへ Challenge を送ります。
6. クライアントは証明書を送り返します。
7. 認証サーバがアクセスを承認します。
8. スイッチがクライアントへアクセスを許可します。

クライアント（サブリカント）がポートに接続されると、本機では EAPOL の ID のリクエストを返します。クライアントは ID をスイッチに送信し、RADIUS サーバに転送されます。

RADIUS サーバはクライアントの ID を確認し、クライアントに対して access challenge back を送ります。

RADIUS サーバからの EAP パケットには Challenge 及び認証モードが含まれます。クライアントソフト及び RADIUS サーバの設定によっては、クライアントは認証モードを拒否し、他の認証モードを要求することができます。認証モードには、MD5、TLS (Transport Layer Security)、TTLS (Tunneled Transport Layer Security) 等があります。

クライアントは、パスワードや証明書などと共に、適切な方法により応答します。

RADIUS サーバはクライアントの証明書を確認し、許可または不許可のパケットを返します。認証が成功した場合、クライアントに対してネットワークへのアクセスを許可します。そうでない場合は、アクセスは否定され、ポートはブロックされます。

IEEE802.1x 認証を使用するには本機に以下の設定を行います。

- スイッチの IP アドレスの設定を行います。
- RADIUS 認証を有効にし、RADIUS サーバの IP アドレスを設定します。
- 認証を行う各ポートで dot1x"Auto" モードに設定します。
- 接続されるクライアント側に dot1x クライアントソフトがインストールされ、適切な設定を行います。
- RADIUS サーバ及び IEEE802.1x クライアントは EAP をサポートする必要があります（本機では EAP パケットをサーバからクライアントにパスするための EAPOL のみをサポートしています）
- RADIUS サーバとクライアントは MD5、TLS、TTLS、PEAP 等の同じ EAP 認証タイプをサポートしている必要があります（一部は Windows でサポートされていますが、それ以外に関しては IEEE802.1x クライアントによりサポートされている必要があります）

802.1x グローバル設定

Security > Port Authentication (Configure Global) ページを使用し、IEEE 802.1X ポート認証の設定を行います。ポート設定をアクティブにする前に、802.1X プロトコルをスイッチシステム全体で有効にする必要があります。

設定・表示項目

Port Authentication Status

802.1X のグローバル設定（初期設定：無効）

EAPOL Pass Through

dot1x がグローバルで無効時に、STP フォワーディング状態の全てのポートへ EAPOL フレームを通過させます。（初期設定：無効）

Identity Profile User Name

Dot1x サブリカントユーザ名（範囲：1-8 文字）

Set Password

dot1x サブリカントパスワードを入力

Identity Profile Password

認証者から MD5 challenge へ返答をした際、dot1x サブリカントパスワードは、このスイッチをサブリカントとして識別する為に使用されます。

Confirm Profile Password

dot1x サブリカントパスワードの確認

設定方法

- (1) [Security] → [Port Authentication] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 各種設定を行い、< Apply >をクリックします。

Security > Port Authentication

Step: 1. Configure Global ▼

Port Authentication Status

☐ Enabled

EAPOL Pass Through

☐ Enabled

Identity Profile User Name

admin

☒ Set Password

Identity Profile Password

●●●●●●

Confirm Profile Password

●●●●●●

Apply

Revert

802.1X 認証ポート設定

802.1X を有効にした場合、クライアントとスイッチ間及びスイッチと認証サーバ間のクライアント認証プロセスに関するパラメータを設定する必要があります。これらのパラメータについて解説します。

機能解説

- スイッチが、スイッチに取り付けられたサブリカンとデバイスと認証サーバ間のローカルオーセンティケーターとして機能する時、" Authenticator configuration" ページで、オーセンティケーターとクライアント間の EAP メッセージ交換をするためにパラメータを設定してください。
- ポートに取り付けられたデバイスがネットワークの他のオーセンティケーターへリクエストを出さなくてはならない時、「Configure Global page」(P232 「802.1x グローバル設定」) ページで "Identity Profile parameters" の設定を行い、リモート認証を通してクライアントを認証する必要がある、それらのポートの為のサブリカントパラメータも設定してください (P236 「802.1X ポートサブリカント設定」を参照)。
- 本機は、この設定ページで「Control Mode」を「Auto」にすることで、選択されたポートのオーセンティケーターの役として設定することが可能です。また、このページで「Control Mode」を「Force Authorized」にし、「Supplicant configuration」ページで PAE サブリカントを有効にすることで、他のポートのサブリカントとなることが可能です。

設定・表示項目

Port

ポート番号

Status

ポートの認証の有効 / 無効

Authorized

- Yes — 接続されたクライアントは認証されています。
- No — 接続されたクライアントは認証されていません。

Supplicant

接続されたクライアントの MAC アドレス

Control Mode

認証モードを以下のオプションの中から設定します。

- Auto — dot1x 対応クライアントに対して RADIUS サーバによる認証を要求します。dot1x 非対応クライアントからのアクセスは許可しません。
- Force-Authorized — dot1x 対応クライアントを含めたすべてのクライアントのアクセスを許可します。
- Force-Unauthorized — dot1x 対応クライアントを含めたすべてのクライアントのアクセスを禁止します。

Operation Mode

802.1X 認証ポートへ接続する 1 つまたは複数のホスト（クライアント）を許可します。

- Single-Host — 1 ホストのみこのポートへの接続を許可
- Multi-Host — 複数のホストのこのポートへの接続を許可
- MAC-Based — 複数のホストのこのポートへの接続を許可。それぞれのホストは認証が必要。このモードでは、ポートに接続されたそれぞれのホストは認証を通る必要があります。このモードでポートオペレーティングへアクセスを許可されるホストの数はセキュアアドレステーブルの利用可能なスペースにのみ制限されます。

Max Mac Count

Multi-Host 設定時の最大接続可能クライアント数（設定範囲：1-1024、初期設定：5）

Max-Request

認証セッションがタイムアウトになる前に、EAP リクエストパケットをスイッチポートからクライアントへ再送信する場合の最大回数（範囲：1-10 回、初期設定：2 回）

TX Period

認証時に EAP パケットの再送信を行う間隔（範囲：1-65535 秒、初期設定：30 秒）

Supplicant Timeout

スイッチポートが EAP パケットの再送信までに、クライアントからの EAP リクエストを待つ時間を設定（範囲：1-65535 初期設定：30 秒）

Server Timeout

スイッチポートが EAP パケットの再送信までに、認証サーバからの EAP リクエストを待つ時間を設定（固定設定：10 秒）

Re-authentication Status

Re-authentication Period で設定した期間経過後にクライアントを再認証するかどうか。再認証により、新たな機器がスイッチポートに接続されていないかを検出できます（初期設定：無効）

Re-authentication Period

接続済みのクライアントの再認証を行う間隔（範囲：1-65535 秒、初期設定：3600 秒）

Intrusion Action

- － Block Traffic － 全ての非 EAP トラフィックをブロックします（初期設定）
- － Guest VLAN － ポートの全トラフィックはゲスト VLAN にアサインされます。
（P83 「VLAN グループの設定」、P188 「ポートのネットワークアクセス設定」を参照してください）

Authenticator PAE State Machine

State

現在の状態（initialize、disconnected、connecting、authenticating、authenticated、aborting、held、force_authorized、force_unauthorized）

Reauth Count

再度接続状態に入った回数

Current Identifier

認証サーバによって、それぞれの EAP 成功・失敗、リクエストパケットに送られた識別子

Backend State Machine

State

現在の状態（request、response、success、fail、timeout、idle、initialize）

Request Count

応答を受け取らずにサブリカントへ送信する EAP リクエストパケットの数

Identifier (Server)

認証サーバによって、それぞれの EAP 成功・失敗、リクエストパケットに送られた識別子

Reauthentication State Machine

State

現在の状態（初期化、再認証）

設定方法

- (1) [Security] → [Port Authentication] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 各種設定を行い、< Apply >をクリックします。

Security > Port Authentication

Step: 2. Configure Interface

Type
☒ Authenticator
☐ Supplicant

Port
1

Status
Disabled

Authorized
Yes

Supplicant
00-00-00-00-00-00

Control Mode
Auto

Operation Mode
Single-Host

Max MAC Count (1-1024)
5

Max Request (1-10)
2

Quiet Period (1-65535)
60 sec

Tx Period (1-65535)
30 sec

Supplicant Timeout (1-65535)
30 sec

Server Timeout
10 sec

Re-authentication Status
☐ Enabled

Re-authentication Period (1-65535)
3600 sec

Intrusion Action
Block Traffic

Authenticator PAE State Machine

State
Initialize

Reauth Count
0

Current Identifier
0

Backend State Machine

State
Initialize

Request Count
0

Identifier (Server)
0

Reauthentication State Machine

State
Initialize

Apply

802.1X ポートサブリカント設定

Security > Port Authentication (Configure Interface - Supplicant) ページを使用し、ポートから他のデバイスのオーセンティケータへ発行される、サブリカントリクエストの 802.1X ポート設定を行います。802.1X が有効であり、コントロールモードが「Force-Authorized」に設定されている際、(P233 「802.1X 認証ポート設定」を参照) クライアントがネットワークの他のデバイスを通して認証される場合には、クライアントサブリカントプロセスのためにパラメータの設定を行う必要があります。

機能解説

- ・ ポートに取り付けられたデバイスがネットワークの他のオーセンティケータへリクエストを出さなくてはならない時、「Configure Global page」(P232 「802.1x グローバル設定」を参照) ページで "Identity Profile parameters" の設定を行い、リモート認証を通してクライアントを認証する必要がある、それらのポートの為のサブリカントパラメータも設定してください (P236 「802.1X ポートサブリカント設定」を参照)。
- ・ 本機は、このオーセンティケータ設定ページで「Control Mode」を「Auto」にすることで、選択されたポートのオーセンティケータの役として設定することが可能です。また、このページで「Control Mode」を「Force Authorized」にし、「Supplicant configuration」 ページで PAE サブリカントを有効にすることで、他のポートのサブリカントとなることが可能です。

設定・表示項目

Port

ポート番号

PAE Supplicant

EAP サブリカントモードの有効化 (初期設定: 無効)

接続されているクライアントが、ネットワークの他のデバイスを通して認証される必要がある場合、サブリカントステータスを有効にしてください。

サブリカントステータスは、このポートで PAE コントロールモードが "Force-Authorized" になっている場合のみ有効にできます (P233 「802.1X 認証ポート設定」を参照)。

ポートがトランクメンバーであるか、このポートで LACP が有効の時、PAR サブリカントステータスを有効にすることはできません。

Authentication Period

サブリカントポートがオーセンティケータからの返答を待つ時間

(範囲: 1-65535 秒 初期設定: 30 秒)

Hold Period

サブリカントポートが新しいオーセンティケータへ証明書を再送するまでの待ち時間

(範囲: 1-65535 秒 初期設定: 30 秒)

Start Period

サブリカントポートが EAPOL スタートフレームをオーセンティケータへ再送するまでの待ち時間 (範囲: 1-65535 秒 初期設定: 30 秒)

Maximum Start

ポートサブリカントがクライアントへ EAP スタートフレームを送信する最大数

(範囲: 1-65535 秒 初期設定: 3)

Authenticated

サブリカントが認証されたか否かを表示。

設定方法

- (1) [Security] → [Port Authentication] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Supplicant」 をクリックします。
- (4) 各種設定を行い、< Apply >をクリックします。

Security > Port Authentication

Step: 2. Configure Interface

Type
☐ Authenticator
☒ Supplicant

Port
2

PAE Supplicant
☒ Enabled

Authentication Period (1-65535)
30

Hold Period (1-65535)
60

Start Period (1-65535)
30

Maximum Start (1-65535)
3

Authenticated
No

Apply
Revert

IEEE802.1x 統計情報の表示

dot1x プロトコルの各ポートの統計情報を表示します。

機能解説

パラメータ	解説
<i>Authenticator</i>	
Rx EXPOL Start	EAPOL スタートフレームの受信数
Rx EAPOL Logoff	EAPOL ログオフフレームの受信数
Rx EAPOL Invalid	全 EAPOL フレームの受信数
Rx EAPOL Total	有効な EAPOL フレームの受信数
Rx Last EAPOLVer	直近の受信 EAPOL フレームのプロトコルバージョン
Rx Last EAPOLSrc	直近の受信 EAPOL フレームのソース MAC アドレス
Rx EAP Resp/Id	EAP Resp/Id フレームの受信数
Rx EAP Resp/Oth	Resp/Id frames 以外の有効な EAP 応答フレームの受信数
Rx EAP LenError	パケット長が不正な無効 EAPOL フレームの受信数
Tx EAP Req/Id	EAP Resp/Id フレームの送信数
Tx EAP Req/Oth	Resp/Id frames 以外の有効な EAP 応答フレームの送信数
Tx EAPOL Total	全 EAPOL フレームの送信数
<i>Supplicant</i>	
Rx EAPOL Invalid	フレームタイプが認識されないサブリカントによって受信された EAPOL フレーム数
Rx EAPOL Total	有効な EAPOL フレームの受信数
Rx Last EAPOLVer	直近の受信 EAPOL フレームのプロトコルバージョン
Rx Last EAPOLSrc	直近の受信 EAPOL フレームのソース MAC アドレス
Rx EAP Resp/Id	EAP Resp/Id フレームの受信数
Rx EAP Resp/Oth	Resp/Id frames 以外の有効な EAP 応答フレームの受信数
Rx EAP LenError	パケット長が不正な無効 EAPOL フレームの受信数
Tx EAPOL Total	全 EAPOL フレームの送信数
Tx EAPOL Start	EAPOL スタートフレームの受信数
Tx EAPOL Logoff	EAPOL スタートフレームの受信数
Tx EAP Req/Id	EAP Resp/Id フレームの送信数
Tx EAP Req/Oth	Resp/Id frames 以外の有効な EAP 応答フレームの送信数

設定方法

802.1X ポート認証統計を表示

- (1) [Security] → [Port Authentication] をクリックします。
- (2) 「Step」 リストから「Show Statistics」を選択します。
- (3) 「Authentication」 をクリックします。

Security > Port Authentication

Step: 3. Show Statistics

Type ☒ Authenticator ☐ Supplicant

Port 1

Port Authentication Authenticator Statistics

Rx EAPOL Start	0	Rx EAP Resp/Id	0
Rx EAPOL Logoff	0	Rx EAP Resp/Oth	0
Rx EAPOL Invalid	0	Rx EAP LenError	0
Rx EAPOL Total	0	Tx EAP Req/Id	0
Rx Last EAPOLVer	0	Tx EAP Req/Oth	0
Rx Last EAPOLSrc	00-00-00-00-00-00	Tx EAPOL Total	0

Refresh

802.1X ポートサブリカント統計を表示

- (1) [Security] → [Port Authentication] をクリックします。
- (2) 「Step」 リストから「Show Statistics」を選択します。
- (3) 「Supplicant」 をクリックします。

Security > Port Authentication

Step: 3. Show Statistics

Type ☐ Authenticator ☒ Supplicant

Port 1

Port Authentication Supplicant Statistics

Rx EAPOL Invalid	0	Rx EAP LenError	0
Rx EAPOL Total	0	Tx EAPOL Total	1
Rx Last EAPOLVer	0	Tx EAPOL Start	1
Rx Last EAPOLSrc	00-00-00-00-00-00	Tx EAPOL Logoff	0
Rx EAP Resp/Id	0	Tx EAP Req/Id	0
Rx EAP Resp/Oth	0	Tx EAP Req/Oth	0

Refresh

3.12.12 IP ソースガード

IP ソースガードは、IP ソースガードテーブルに手動で構成されたエントリか、DHCP スヌーピングを有効にしたときの固定・動的エントリを基にして、ネットワークインタフェース上の IP トラフィックをフィルタするセキュリティ機能です。IP ソースガードはあるホストがネットワークにアクセスしてネットワーク内の IP アドレスを使用しようという試みがあつたとき、引き起こされる攻撃から守るために使用されます。この項は IP ソースガードで使用するコマンドについて解説します。

IP ソースガードポート設定

IP ソースガードはネットワークやファイアウォールの外側からメッセージを受信した、保護されていないポート上のトラフィックをフィルタするために使用されます。

[注意] マルチキャストアドレスは IP ソースガードで使うことができません。

機能解説

- 有効にしたとき、トラフィックは DHCP スヌーピングを通して学習したダイナミックエントリや IP ソースガードのバインドテーブルで構成された固定アドレスを基にフィルタが行われます。フィルタはスイッチのインバウンドパケットに対して行われ、IP アドレスのみ (SIP)、もしくは IP アドレスと MAC アドレスの両方 (SIP-MAC) がバインドテーブル上のエントリと比較されます。パケットがバインドテーブル上のエントリと違う場合、パケットは破棄されます。
- この機能は選択したポートで、ソースガードモードを SIP (Source IP) または SIP-MAC (Source IP と MAC) の有効にします。バインディングテーブルの全てのエントリにたいし、VLAN ID、ソース IP アドレス、ポート番号のチェックを行うには SIP オプションを使用してください。これらと同じパラメータに加え、ソース MAC アドレスのチェックを行うには、SIP-MAC オプションを使用して下さい。もしマッチするエントリが見つからない場合、パケットは破棄されます。
- IP ソースガードが有効の場合、上りのパケットの IP アドレス (SIP オプション) またはその IP アドレスと対応する MAC アドレスの両方 (SIP-MAC オプション) はバインディングテーブルに照らし合わされます。もしマッチするエントリが見つからない時、パケットは破棄されます。
- フィルタリングルールは以下のように実行されます。
 - DHCP スヌーピングが無効の際 (P245 参照)、IP ソースガードは VLAN ID、ソース IP アドレス、ポート番号、ソース MAC アドレス (SIP-MAC オプション) をチェックします。もしバインディングテーブルにマッチするエントリが見つからない時、パケットは破棄されます。
 - DHCP スヌーピングが有効の際、IP ソースガードは VLAN ID、ソース IP アドレス、ポート番号、ソース MAC アドレス (SIP-MAC オプション) をチェックします。もしバインディングテーブルまたは見つからず、エントリタイプが静的 IP ソースガードバインディングまたは動的 DHCP スヌーピングバインディングである場合、パケットは転送されます。
 - IP ソースガードが IP ソースバインディングが未設定のインタフェース (IP ソースガードバインディングテーブルの静的設定と DHCP スヌーピングからの動的学習のいずれか) で有効の際、スイッチはポートの DHCP パケット以外全ての IP トラフィックを破棄します。

設定・表示項目

Filter Type

送信元 IP アドレスまたは対応する MAC アドレスを元にした入力トラフィックのフィルタリングを設定

- None — ポートで IP ソースガードフィルタリングを無効
- SIP — バインディングテーブルに保存された IP アドレスによるトラフィックフィルタリングを有効
- SIP-MAC — バインディングテーブルに保存された IP アドレスおよび対応する MAC アドレスによるトラフィックフィルタリングを有効

SIP-MAC

送信元 IP アドレスまたは対応する MAC アドレスを元にした入力トラフィックのフィルタリングを有効化

設定方法

- (1) [Security] → [IP Source Guard] → [Port Configuration] をクリックします。
- (2) それぞれのポートで必要とされるフィルタリングタイプを設定します。
- (3) < Apply > をクリックします。

Security > IP Source Guard > Port Configuration		
Port Configuration List Max: 26 Total: 26		
Port	Filter Type	
1	None	▼
2	None	▼
3	None	▼
4	None	▼
5	SIP	▼

IP ソースガード静的バインディング設定

IP ソースガードのバインドテーブルに固定アドレスを追加します。エントリは MAC アドレス、IP アドレス、リースタイム、エントリの種類 (Static、Dynamic)、VLAN ID、Port ID を含んでいます。すべての固定エントリはリースタイムが無限で構成されます。リースタイムはテーブル上では 0 で表示されます。

機能解説

- ・ ソースガードバインディングテーブルの静的アドレスエントリは、無限のリース時間で自動的に設定されます。DHCP スヌーピングで学習された動的エントリは DHCP サーバ自身で設定されます。
- ・ 静的バインディングは以下のように処理されます。
 - － 同一の VLAN ID と MAC アドレスに項目が無い場合、新しいエントリは静的 IP ソースガードバインディングタイプを使用し、バインディングテーブルに追加されます。
 - － 同一の VLAN ID と MAC アドレスに項目が無く、エントリのタイプが静的 IP ソースガードバインディングである場合、新しいエントリが古い物を置き換えます。
 - － 同一の VLAN ID と MAC アドレスに項目が無く、エントリのタイプが動的 DHCP スヌーピングバインディングである場合、新しいエントリが古い物を置き換え、エントリタイプは静的 IP ソースガードバインディングに変更されます。

設定・表示項目

Port

静的項目がバウンドされているポート

VLAN

設定を行う VLAN ID (範囲：1-4093)

MAC Address

有効なユニキャスト MAC アドレス

IP Address

有効なユニキャスト IP アドレス

設定方法

IP ソースガードの静的バインディングを設定

- (1) [Security] → [IP Source Guard] → [Static Binding] をクリックします。
- (2) 「Action」 リストから「Add」を選択します。
- (3) それぞれのポートで必要とされるバインディングを入力します。
- (4) < Apply > をクリックします。

Security > IP Source Guard > Static Binding

Action: Add ▼

Port 1 ▼

VLAN 1 ▼

MAC Address 00-10-B5-F3-00-01

IP Address 192.168.0.23

Apply Revert

IP ソースガードの静的バインディングを表示

- (1) [Security] → [IP Source Guard] → [Static Binding] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

Security > IP Source Guard > Static Binding

Action: Show ▼

Static Binding List Max: 50 Total: 1

	VLAN	MAC Address	Interface	IP Address	Type	Lease Time (sec)
☐	1	00-10-B5-F3-00-01	Unit 1 / Port 1	192.168.0.23	IPv4	0

Apply Revert

動的 IP ソースガードバインディング情報の表示

選択したインタフェースの IP ソースガードの動的に取得した分のバインドテーブルを表示します。

設定・表示項目

Query by

- Port —スイッチ上のポート
- VLAN —設定された VLAN（範囲：1-4093）
- MAC Address —有効なユニキャスト MAC アドレス
- IP Address —有効なユニキャスト IP アドレス（クラスタイプ A、B、C を含む）

Dynamic Binding List

- VLAN —この項目にバウンドされている VLAN
- MAC Address —エントリと関連付けられる物理アドレス
- Interface —この項目にバウンドされているポート
- IP Address —クライアントに対応している IP アドレス
- Type —静的または動的バインディング
- Lease Time —この IP アドレスがクライアントにリースされる時間

設定方法

- (1) [Security] → [IP Source Guard] → [Dynamic Binding] をクリックします。
- (2) 検索条件をチェックし、必要な値を入力します。
- (3) それぞれのポートで必要とされるバインディングを入力します。
- (4) < Query > をクリックします。

Security > IP Source Guard > Dynamic Binding

Query by:
☐ Port
☐ VLAN
☐ MAC Address
☐ IP Address

Dynamic Binding List Max: 50 Total: 3

VLAN	MAC Address	Interface	IP Address	Type	Lease Time (sec)
1	00-10-B5-F4-00-01	Unit 1 / Port 2	10.2.44.96	IPv4	5
1	00-10-B5-F4-00-02	Unit 1 / Port 4	10.2.44.97	IPv4	25
2	00-10-B5-F4-00-03	Unit 1 / Port 7	10.2.44.98	IPv4	47

3.12.13 DHCP スヌーピング

DHCP Snooping は悪意のある DHCP サーバーや DHCP サーバーに関連のある情報を送信する他のデバイスからネットワークを守ります。この情報は物理ポートへ IP アドレスを戻す際の追跡に役立つ場合があります。

機能解説

- ネットワークの外側から悪意のある DHCP メッセージが受信されたとき、ネットワークトラフィックが混乱する可能性があります。DHCP Snooping はネットワークやファイアウォールの外側からの安全でないインタフェースで受信した DHCP メッセージをフィルタするために使用されます。DHCP Snooping を有効にして VLAN インタフェースに設定したとき、DHCP Snooping テーブル上に載っていないデバイスから untrust のインタフェースで DHCP メッセージを受信するとそれを破棄します。
- テーブルエントリは Trusted インタフェースのためにのみ学習されます。クライアントが DHCP サーバから IP アドレスを受信またはリリースした時、エントリを DHCP スヌーピングテーブルへ動的に追加または削除します。それぞれのエントリは MAC アドレス、IP アドレス、リースタイム、VLAN 識別情報、ポート識別情報を含みます。
- スイッチによって処理が可能な DHCP メッセージのレートリミットは毎秒 100 パケットです。この制限を越えた DHCP パケットはドロップされます。
- 有効にしたとき、untrust のインタフェースに入った DHCP メッセージには、DHCP Snooping で学習したダイナミックエントリをベースにしたフィルタが行われます。

フィルタのルールは下記の通りです。

- DHCP Snooping が無効の場合、DHCP パケットは転送される。
- DHCP Snooping が有効で DHCP パケットを受信する VLAN 上でも有効の場合、すべての DHCP パケットは trust 状態のポートに向けて転送されます。受信したパケットが DHCP ACK メッセージの場合、このエントリはバインドテーブルに追加されます。
- DHCP Snooping が有効で DHCP パケットを受信する VLAN 上でも有効だが、ポートが trust でない場合は下記の動作を行います。
 - DHCP パケットが DHCP サーバーからの返答パケット (OFFER, ACK, NAK メッセージを含む) の場合、そのパケットは破棄されます。
 - DHCP パケットがクライアントからのものである場合、DECLINE や RELEASE メッセージのようなパケットは、一致するエントリがバインドテーブルで見つかった場合のみ、スイッチはパケットを転送します。
 - DHCP パケットがクライアントからのものである場合、DISCOVER、REQUEST、INFORM、DECLINE、RELEASE メッセージのようなパケットは、MAC アドレスによる照合が無効である場合にはパケットは転送されます。しかし、MAC アドレスの照合が有効の場合、DHCP パケットに記録されているクライアントのハードウェアアドレスが Ethernet ヘッダの Source MAC アドレスと同じ場合にパケットは転送されます。
 - DHCP パケットが認識できないタイプの場合は破棄されます。
- クライアントからの DHCP パケットが上記のフィルタ基準を通過した場合、同じ VLAN の trust ポートに転送されます。

- サーバーからの DHCP パケットが trust ポートで受信された場合、同じ VLAN の trust ポートと untrust ポートに転送されます。
- DHCP Snooping が無効の場合、すべてのダイナミックエントリはバインドテーブルから取り除かれます。
- スイッチ自身が DHCP クライアントの場合の動作
スイッチが DHCP サーバーにクライアントの Request パケットを送信するポートは trust として設定しなくてはなりません。スイッチは DHCP サーバーから ACK メッセージを受信したとき、自身の情報をバインドテーブルのダイナミックエントリとして追加しません。また、スイッチが DHCP クライアントのパケットを自身に送信したとき、フィルタの動作は発生しません。しかし、スイッチが DHCP サーバーからメッセージを受信したとき、untrust ポートで受信したパケットはすべて破棄されます。

DHCP Snooping Option 82

- DHCP はスイッチと DHCP クライアントについての情報を DHCP サーバーに送信するリレーメカニズムを提供します。これは DHCP Option 82 として知られており、IP アドレスを割り当てたときの情報を使うため、もしくはクライアントに他のサービスやポリシーを設定するために DHCP サーバーに互換性を提供します。
- オプション 82 情報をリクエストパケットに挿入することが出来るように、DHCP スヌーピングを有効にする必要があります。
- DHCP スヌーピング情報オプション 82 をスイッチで有効にした際、VLAN (DHCP スヌーピングフィルタリングルールに依存) 上で受信された DHCP リクエストパケットに情報が挿入されます。情報は、ゲートウェイインターネットアドレスと同様にサーキット ID、リモート ID を含む、中継されたパケットに挿入されます。
- すでに DHCP オプション 82 情報を含むクライアントから DHCP パケットを受信した時、スイッチはこれらのパケットのためにアクションポリシーを設定することが可能です。スイッチは DHCP パケットをドロップするか、既存の情報を維持するか、スイッチのリレー情報で置き替える事が出来ます。

DHCP スヌーピング設定

IP Service > DHCP > Snooping (Configure Global) を使用し、DHCP スヌーピングをグローバルで有効 / 無効、または MAC アドレス検証の設定を行います。

設定・表示項目

DHCP Snooping Status

スイッチで DHCP スヌーピングを有効 / 無効にします。

DHCP Snooping MAC-Address Verification

MAC address 検証の有効 / 無効。

もしパケットの Ethernet ヘッダー で送信元 MAC アドレスが DHCP パケットでクライアントのハードウェアアドレスと同じではないなら、DHCP パケットは破棄されます。

(初期設定：有効)

DHCP Snooping Information Option Status

DHCP Option 82 Information Relay 有効 / 無効 (初期設定：無効)

DHCP Snooping Information Option Policy

Option 82 を含む DHCP クライアントからのパケットのため、DHCP Snooping Information オプションを設定します。

- Drop – 既にリレー情報があった場合そのメッセージを破棄し、全ての VLAN にフラットニングします。
- Keep – 既存のリレー情報をそのまま保持します。
- Replace – スイッチのリレー情報で、DHCP クライアントパケットのインフォメーションを上書きします。

設定方法

- (1) [IP Service] → [DHCP Snooping] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 必要な項目の設定を行い、< Apply >をクリックします。

IP Service > DHCP > Snooping

Step: 1. Configure Global

General

DHCP Snooping Status ☒ Enabled

DHCP Snooping MAC-Address Verification ☒ Enabled

Information

DHCP Snooping Information Option Status ☒ Enabled

DHCP Snooping Information Option Policy Replace

Apply Revert

DHCP スヌーピング VLAN 設定

IP Service > DHCP > Snooping (Configure VLAN) ページを使用し、特定の VLAN 上で DHCP Snooping を有効にします。

機能解説

- DHCP スヌーピングがスイッチのグローバルかつ指定された VLAN で有効の時、DHCP パケットフィルタリングは、VLAN に属する全ての Untrust ポートで実行されます。
- DHCP スヌーピングがグローバルで無効時、DHCP スヌーピングは依然指定された VLAN での設定が可能です。DHCP スヌーピングがグローバルで再度有効になるまで効果は反映されません。
- DHCP スヌーピングがグローバルで有効であり、VLAN で無効になった場合、この VLAN での全ての動的バインディング学習はバインディングテーブルから取り除かれます。

設定・表示項目

VLAN ID

設定を行う VLAN (範囲：1-4093)

DHCP Snooping Status

選択した VLAN での DHCP スヌーピングの有効 / 無効 (初期設定：無効)

設定方法

- (1) [IP Service] → [DHCP Snooping] をクリックします。
- (2) 「Step」 リストから「Configure VLAN」を選択します。
- (3) 既存のいずれかの VLAN で DHCP Snooping を有効にします。
- (4) < Apply > をクリックします。

IP Service > DHCP > Snooping

Step: 2. Configure VLAN

VLAN 1

DHCP Snooping Status ☒ Enabled

Apply Revert

DHCP スヌーピングポート設定

IP Service > DHCP > Snooping (Configure Interface) ページを使用し、スイッチのポートを trust か untrust に設定することができます。

機能解説

- untrust に設定したインタフェースはネットワークやファイアウォールの外側からメッセージを受信するように構成されます。trust に設定したインタフェースはネットワーク内部からのメッセージのみ受信するよう構成されます。
- DHCP スヌーピングがグローバルと VLAN 両方で有効時、DHCP パケットフィルタリングは VLAN 中の untrusted ポート上でも実行されます。
- untrusted ポートが trusted ポートに変更された時、このポートに関連付けられている全ての動的 DHCP スヌーピングバインディングは削除されます。
- ローカルネットワークまたはファイアウォール内の DHCP サーバに接続される全てのポートは trusted に設定してください。ローカルネットワークまたはファイアウォールの外にあるその他全てのポートは untrusted に設定します。

設定・表示項目

Trust Status

ポートを Trust ポートとして有効 / 無効に設定します。（初期設定：無効）

設定方法

- (1) [IP Service] → [DHCP Snooping] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) ポートの "Trusted Status" の "Enabled" にチェックを入れます。
- (4) < Apply > をクリックします。

IP Service > DHCP > Snooping

Step: 3. Configure Interface

Interface ☒ Port ☐ Trunk

DHCP Snooping Port List Max: 26 Total: 26

Port	Trust Status
1	☐ Enabled
2	☐ Enabled
3	☒ Enabled
4	☐ Enabled
5	☐ Enabled

DHCP スヌーピングバインディング情報

IP Service > DHCP > Snooping (Show Information) ページを使用し、DHCP スヌーピングバインディング情報を表示します。

設定・表示項目

MAC Address

エントリに関連する MAC アドレス

IP Address

クライアントに対応する IP アドレス

Lease Time (Seconds)

この IP アドレスがクライアントにリースされる時間

Type

- DHCP-Snooping —動的に詮索
- Static-DHCPSNP —静的に設定

VLAN

このエントリがバウンドされる VLAN

Interface

このエントリがバウンドされるポートまたはトランク

Store

動的に学習された全てのスヌーピングエントリをフラッシュメモリへ書き込みます。

Clear

動的に学習された全てのスヌーピングエントリをフラッシュメモリから取り除きます。

設定方法

- (1) [IP Service] → [DHCP Snooping] をクリックします。
- (2) 「Step」 リストから「Show Information」を選択します。
- (3) 必要に応じ、「Store」または「Clear」機能を使用してください。

IP Service > DHCP > Snooping

Step: 4. Show Information

DHCP Snooping Binding List Max: 75 Total: 6

MAC Address	IP Address	Lease Time (seconds)	Type	VLAN	Interface
00-10-B5-F4-00-01	10.2.44.96	5	DHCP-Snooping	1	Trunk 1
00-10-B5-F4-00-02	10.3.44.96	15	Static-DHCPSNP	1	Unit 1 / Port 2
00-10-B5-F4-00-03	10.4.44.96	25	DHCP-Snooping	1	Unit 1 / Port 3
00-10-B5-F4-00-04	10.5.44.96	10	Static-DHCPSNP	1	Trunk 4
00-10-B5-F4-00-05	10.6.44.96	10	DHCP-Snooping	1	Unit 1 / Port 5
00-10-B5-F4-00-06	10.7.44.96	5	Static-DHCPSNP	1	Unit 1 / Port 6

Store

Click the button to Store DHCP Snooping binding entries to flash.

Clear

Click the button to Clear DHCP Snooping binding entries from flash.

3.13 基本管理プロトコル

3.13.1 Event Logging の設定

エラーメッセージのログに関する設定を行うことができます。スイッチ本体へ保存するイベントメッセージの種類、syslog サーバへのログの保存、及び最新のイベントメッセージの一覧表示などが可能です。

syslog の設定

本機は、イベントメッセージの保存 / 非保存、RAM/ フラッシュメモリに保存するメッセージレベルの指定が可能です。

フラッシュメモリのメッセージは本機に永久的に保存され、ネットワークで障害が起こった際のトラブル解決に役立ちます。フラッシュメモリには 4096 件まで保存することができ、保存可能なログメモリ (256KB) を超えた場合は最も古いエントリから上書きされます。

System Logs 画面では、フラッシュメモリ / RAM に保存するシステムメッセージの制限を設定できます。初期設定では、フラッシュメモリには 0-3 のレベル、又 RAM には 0-6 のレベルのイベントに関してそれぞれ保存されます。

設定・表示項目

System Log Status

デバッグ又はエラーメッセージのログ保存の有効 / 無効（初期設定：有効）

Flash Level

スイッチ本体のフラッシュメモリに永久的に保存するログメッセージ。指定したレベルより上のレベルのメッセージをすべて保存します。例えば "3" を指定すると、0-3 のレベルのメッセージがすべてフラッシュメモリに保存されます（範囲：0-7、初期設定：3）

レベル	名前	解説
7	Debug	デバッグメッセージ
6	Informational	情報メッセージ
5	Notice	重要なメッセージ
4	Warning	警告メッセージ
3	Error	エラー状態を示すメッセージ
2	Critical	重大な状態を示すエラーメッセージ
1	Alert	迅速な対応が必要なメッセージ
0	Emergency	システム不安定状態を示すメッセージ

※現在のファームウェアではレベル 2、5、6 のエラーメッセージのみサポート

RAM Level

スイッチ本体の RAM に一時的に保存するログメッセージ。指定したレベルより上のレベルのメッセージをすべて保存します。例えば "7" を指定すると、0-7 のレベルのメッセージがすべてフラッシュメモリに保存されます（範囲：0-7、初期設定：7）

[注意] フラッシュメモリのレベルは RAM レベルと同じか、これより下のレベルにして下さい。

設定方法

システムメモリログの設定

- (1) [Administration] → [Log] → [System] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) システムロギングを有効/無効にし、フラッシュメモリと RAM に記録されるイベントメッセージのレベルを設定します。
- (4) < Apply > をクリックします。

Administration > Log > System

Step: 1. Configure Global ▼

System Log Status ☒ Enabled

Flash Level 3 - Error ▼

RAM Level 7 - Debugging ▼

Note: The Flash Level must be equal to or less than the RAM Level.

Apply Revert

システムメモリに記録されたエラーメッセージの表示

- (1) [Administration] → [Log] → [System] をクリックします。
- (2) 「Step」 リストから「Show System Logs」を選択します。

Administration > Log > System

Step: 2. Show System Logs ▼

System Logs

```
[10] 16:12:10 2010-03-29
"User(admin/Web) (::FFFF:192.168.1.20), login successful"
level: 6, module: 5, function: 1, and event no: 1
-----
[9] 16:07:58 2010-03-29
"User(admin/Console), login successful."
level: 6, module: 5, function: 1, and event no: 1
-----
[8] 16:07:51 2010-03-29
"Reject WEB 192.168.1.20."
level: 6, module: 5, function: 1, and event no: 1
-----
[7] 16:07:30 2010-03-29
"Reject WEB 192.168.1.20."
level: 6, module: 5, function: 1, and event no: 1
-----
[6] 16:07:25 2010-03-29
"Reject WEB 192.168.1.20."
```

リモートログの設定

Administration > Log > Remote ページでは、他の管理ステーションから syslog サーバへ送信するイベントメッセージのログに関する設定を行います。指定したレベルより下のエラーメッセージだけ送信するよう制限することができます。

設定・表示項目

Remote Log Status

デバッグ又はエラーメッセージのリモートログ保存の有効 / 無効（初期設定：無効）

Logging Facility

送信する syslog メッセージのファシリティタイプ。8 つのファシリティタイプを 16-23 の値で指定します。syslog サーバはイベントメッセージを適切なサービスへ送信するためにファシリティタイプを使用します。

本属性では syslog メッセージとして送信するファシリティタイプタグを指定します（詳細：RFC3164）。タイプの設定は、本機により報告するメッセージの種類に影響しません。syslog サーバにおいてソートやデータベースへの保存の際に使用されます（範囲：16-23、初期設定：23）

Logging Trap Level

syslog サーバに送信するメッセージの種類。指定したレベルより上のレベルのメッセージをすべて保存します。例えば "3" を指定すると、0-3 のレベルのメッセージがすべてリモートサーバに保存されます（範囲：0-7、初期設定：7）

Server IP Address

syslog メッセージを送られるリモートサーバの IP アドレス

設定方法

- (1) [Administration] → [Log] → [Remote] をクリックします。
- (2) リモートロギングを有効にし、syslog メッセージに使用する "facility" タイプを指定します。リモートサーバの IP アドレスを入力します。
- (3) < Apply > をクリックします。

Administration > Log > Remote

Remote Log Status	☒ Enabled
Logging Facility	17 - Local use 1
Logging Trap Level	7 - Debugging messages
Server IP Address 1	10.1.1.1
Server IP Address 2	10.2.2.2
Server IP Address 3	10.3.3.3
Server IP Address 4	
Server IP Address 5	

Apply Revert

SMTP (Simple Mail Transfer Protocol)

Administration > Log > SMTP ページを使用し、SMTP (Simple Mail Transfer Protocol) の設定を行うことができます。

指定したレベルのイベントが発生した際、システム管理者にトラブルの発生を知らせるために、本機は SMTP を使用したメール送信を行うことができます。メールはネットワークに接続している指定した SMTP サーバに送信され、POP 又は IMAP クライアントから受信できます。

設定・表示項目

SMTP Status

SMTP 機能の有効 / 無効（初期設定：有効）

Severity

アラートメッセージのしきい値。指定したレベルより上のレベルのイベント発生時には、設定したメール受信者あてに送信されます。例えば "7" を指定すると、0-7 のレベルのメッセージがすべて通知されます。レベルについては P251 を参照してください。（初期設定：7）

Email Source Address

アラートメッセージの "From" に入力されるメール送信者名を設定します。本機を識別するためのアドレス（文字列）や本機の管理者のアドレスなどを使用します。

Email Destination Address

アラートメッセージを受信するアドレス。アドレスをフィールドに入力し、[Add] をクリックすることでリストへの追加、[Remove] をクリックすることでリストからの削除をおこなえます。

Server IP Address

本機からのアラートメッセージを受信する最大 3 つの SMTP サーバを指定。

設定方法

- (1) [Administration] → [Log] → [SMTP] をクリックします。
- (2) SMTP を有効にし、source/Destination E メールアドレスを指定します。
1 つまたはそれ以上の SMTP サーバを指定します。
- (3) < Apply > をクリックします。

Administration > Log > SMTP

SMTP Status	☒ Enabled
Severity	3 - Error ▼
E-mail Source Address	aaa@fxc.jp
E-mail Destination Address 1	bbb@fxc.jp
E-mail Destination Address 2	
E-mail Destination Address 3	
E-mail Destination Address 4	
E-mail Destination Address 5	
Server IP Address 1	192.168.1.5
Server IP Address 2	
Server IP Address 3	

Apply Revert

3.13.2 LLDP

Link Layer Discovery Protocol (LLDP) はローカルブロードキャストドメインの中の接続デバイスについての基本的な情報を発見するために使用します。LLDP はレイヤ 2 のプロトコルであり、デバイスについての情報を周期的なブロードキャストで伝達します。伝達された情報は IEEE802.1ab に従って Type Length Value (TLV) で表され、そこにはデバイス自身の識別情報、能力、設定情報の詳細が含まれています。また LLDP は発見した近隣のネットワークノードについて集められた情報の保存方法と管理方法を定義します。

3.13.3 LLDP タイム属性の設定

LLDP の有効化、メッセージのエージアウトタイム、通常の情報伝達をブロードキャストする間隔、LLDP MIB の変更についての伝達といった、一般的な設定は LLDP 設定画面で行います。

設定・表示項目

LLDP

LLDP をスイッチグローバルで有効 / 無効にします。(初期設定：有効)

Transmission Interval

LLDP の情報伝達のため周期的に送信する間隔を設定します

(範囲：5 - 32768 秒 初期設定：30 秒)

この値は下の数式に従って計算します。

$(\text{Transmission Interval} \times \text{Hold Time Multiplier}) \leq 65536$

$\text{Transmission Interval} \geq (4 \times \text{Delay Interval})$

Hold Time Multiplier

下の式で示されているように、LLDP のアドバタイズメントで送信された Time-To-Live (TTL) 値を設定します (範囲：2 - 10 初期設定：4)

TTL は、タイムリーな方法でアップデートが送信されない場合、送信した LLDP エージェントに関係のあるすべての情報をどのくらいの期間維持するかを受信した LLDP エージェントに伝達します。TTL は秒で表され、下の数式で計算します。

$\text{Transmission Interval} \times \text{Hold Time Multiplier} \leq 65536$

つまり上の式からデフォルトの TTL は下のようになります。

$4 \times 30 = 120$

Delay Interval

ローカル LLDP MIB の変数に変化が起こった後に引き続き、アドバタイズメントを送信するまでの時間を設定します (範囲：1 ~ 8192 秒 初期設定：2 秒)

この値は下の数式に従って計算します。

$(4 \times \text{Delay Interval}) \leq \text{Transmission Interval}$

Reinitialization Delay

LLDP ポートが無効になるかリンクダウンした後、再初期化を試みるまでの時間を設定します (範囲：1 - 10 秒 初期設定：2 秒)

Notification Interval

LLDP MIB の変更を行い、SNMP 通知が送信されるまでの時間を設定します

(範囲：5 - 3600 秒 初期設定：5 秒)

設定方法

- (1) [Administration] → [LLDP] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) LLDP を有効にし、各パラメータを編集します。
- (4) < Apply > をクリックします。

Administration > LLDP

Step: 1. Configure Global ▼

LLDP	☒ Enabled
Transmission Interval (5-32768)	30 sec
Hold Time Multiplier (2-10)	4
Delay Interval (1-8192)	2 sec
Reinitialization Delay (1-10)	2 sec
Notification Interval (5-3600)	5 sec

Note: The Transmission Interval must be greater than or equal to 4 times the Delay Interval.

3.13.4 LLDP インタフェースの設定

個別のインターフェースに対し、メッセージの内容を指定するために LLDP ポート・トランクの設定を行います。

設定・表示項目

Admin Status

LLDP メッセージの送信・受信のモードを有効にします

(設定項目: Tx only, Rx only, TxRx, Disabled 初期設定: TxRx)

SNMP Notification

LLDP と LLDP-MED の変更について SNMP トラップ通知の送信を有効にします

(初期設定: 有効)

Basic Optional TLVs

アドバタイズするメッセージの TLV フィールドの情報について設定します。

- Management Address — スイッチの IPv4 アドレスが含まれます。スイッチに管理用のアドレスがない場合、アドレスはスイッチの CPU の MAC アドレスが、このアドバタイズメントを送信するポートの MAC アドレスになります。
- Port Description — RFC2863 の ifDescr オブジェクトで規定されています。これには製造者、スイッチの製品名、インターフェースのハードウェアとソフトウェアのバージョンが含まれます。
- System Capabilities — システムの主な機能が含まれます。この情報には機能自体が有効かどうかは関係ありません。この TLV によってアドバタイズされる情報は IEEE802.1AB 規格に記述されています。
- System Description — RFC3418 の sysDescr オブジェクトで規定されています。システムのハードウェア、オペレーティングソフト、ネットワーキングソフトのフルネームとバージョンが含まれています。
- System Name — RFC3418 の sysName オブジェクトで規定されています。システムの管理用に割り当てられた名前が含まれます。

802.1 Organizationally Specific TLVs

アドバタイズドメッセージの TLV フィールドに含まれる 802.1 情報を設定。

- Protocol Identity— このインタフェースを通してアクセス可能なプロトコル (P98 「プロトコル VLAN」 参照)
- VLAN ID — ポートのデフォルト VLAN 識別子 (PVID) は VLAN がタグ無しであるか、関連付けられたプライオリティタグ付きフレームであることを示します (P80 「IEEE802.1Q VLAN」 参照)
- VLAN Name—このインタフェースがアサインされる全ての VLAN の名前 (P80 「IEEE802.1Q VLAN」、P98 「プロトコル VLAN」 参照)
- Port And Protocol VLAN ID—このインタフェースに設定されたポートベースとプロトコルベース VLAN(P80 「IEEE802.1Q VLAN」、P98 「プロトコル VLAN」 参照)

802.3 Organizationally Specific TLVs

アドバタイズドメッセージの TLV フィールドに含まれる IEEE802.3 情報

- － Link Aggregation－ リンクアグリゲーション機能、リンクのアグリゲーションステータス、このインタフェースが現在リンクアグリゲーションメンバーである場合は IEEE802.3 アグリゲーションポート識別子
- － Max Frame Size－ 最大フレームサイズ（P25 「Jumbo フレームの有効化」を参照）
- － MAC/PHY Configuration/Status－ オートネゴシエーションサポート/性能の情報を含む、MAC/PHY 設定とステータスと、操作可能な Multistation Access Unit（MAU）タイプ

設定方法

- (1) [Administration] → [LLDP] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) LLDP 送信 / 受信モードを設定し、SNMP トラップメッセージを送信するか否かを指定します。LLDP メッセージでアダプタイズする情報を選択します。
- (4) < Apply > をクリックします。

Administration > LLDP

Step: 2. Configure Interface

Interface ☒ Port 2 ☐ Trunk

Admin Status Tx Rx

SNMP Notification ☒ Enabled

Basic Optional TLVs:

☒ Management Address ☒ Port Description ☒ System Capabilities ☒ System Description ☒ System Name

802.1 Organizationally Specific TLVs:

☒ Protocol Identity ☒ VLAN ID ☒ VLAN Name ☒ Port And Protocol VLAN ID

802.3 Organizationally Specific TLVs:

☒ Link Aggregation ☒ Max Frame Size ☒ MAC/PHY Configuration/Status

Apply Revert

3.13.5 LLDP ローカルデバイス情報の表示

Administration > LLDP (Show Local Device Information) を使用し、MAC アドレス、シャーシ ID、管理 IP アドレス、ポート等、本機の情報を表示します。

設定・表示項目

グローバル設定

Chassis Type

送信 LLDP エージェントと関連付けられる IEEE802 LAN エンティティを含むシャーシを識別します。シャーシを識別し、コンポーネントのタイプを示すために使用されるシャーシ ID サブタイプが、シャーシ ID フィールドに参照されるためにはいくつかの方法があります。

シャーシ ID サブタイプ

ID Basis	Reference
Chassis component	entPhysClass が "chassis(3)" の値を持つ時は EntPhysicalAlias (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	entPhysicalClass が "port(10)" または "backplane(4)" の値を持つ時は EntPhysicalAlias (IETF RFC 2737)
MAC address	MAC アドレス (IEEE Std 802-2001)
Network address	ネットワークアドレス
Interface name	ifName (IETF RFC 2863)
Locally assigned	ローカルに割り当てられる

Chassis ID

このシステムの特定のシャーシの指定された識別子を示す、8 進数ストリング。

System Name

システムの管理上に割り当てられた名前を示すストリング (P23 「システム情報の表示」を参照)

System Description

ネットワークエンティティの記述。このフィールドは "show system" コマンドでも表示されます。

System Capabilities Supported

システムのプライマリファンクションを定義するケイパビリティ

システム性能

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 および IETF RFC 2670
End Station Only	IETF RFC 2011

System Capabilities Enabled

現在有効になっているシステムのプライマリファンクション。前のテーブルを参照してください。

Management Address

ローカルシステムに関連付けられる管理アドレス。

インタフェース設定

下のリストされた属性はポートとトランクインタフェースタイプ両方に適用可能です。

トランクがリストされた時、説明はトランクの最初のポートに適用されます。

Port/Trunk Description

ポートまたはトランクの説明。RFC 2863 が実装されている場合、ifDescr オブジェクトがこのフィールドに使用されます。

Port/Trunk ID

ポートまたはトランクの識別子

設定方法

LLDP のローカルデバイス情報を表示 (General)

- (1) [Administration] → [LLDP] をクリックします。
- (2) 「Step」 リストから「Show Local Device Information」を選択します。
- (3) "General"、"Port"、"Trunk" からいずれかを選択します。

Administration > LLDP

Step: 3. Show Local Device Information

☒ General
☐ Port
☐ Trunk

LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-1A-7E-AB-FD-12
System Name	
System Description	FXC3326
System Capabilities Supported	Bridge
System Capabilities Enabled	Bridge
Management Address	192.168.1.1 (IPv4)

LLDP のローカルデバイス情報を表示 (Port)

Administration > LLDP

Step: 3. Show Local Device Information

☐ General ☒ Port ☐ Trunk

LLDP Local Device Port List Max: 26 Total: 26

Port	Port Description	Port ID
1	Ethernet Port on unit 1, port 1	00-1A-7E-AB-FD-13
2	Ethernet Port on unit 1, port 2	00-1A-7E-AB-FD-14
3	Ethernet Port on unit 1, port 3	00-1A-7E-AB-FD-15
4	Ethernet Port on unit 1, port 4	00-1A-7E-AB-FD-16
5	Ethernet Port on unit 1, port 5	00-1A-7E-AB-FD-17

3.13.6 LLDP リモートポート情報の表示

LLDP Remote Port/Trunk Information 画面は、スイッチのポートに直接接続されたデバイスについての情報を表示します。これらの情報は LLDP を通してアドバタイズされています。

設定・表示項目

ポート

Local Port

リモート LLDP 対応の装置が取り付けられているローカルポート
attached.

Chassis ID

このシステムの特定のシャーシの指定された識別子を示す、8 進数ストリング

Port ID

ポート識別子

System Name

システムの管理上に割り当てられた名前を示すストリング

ポート詳細

Local Port

リモート LLDP 対応の装置が取り付けられているローカルポート

Chassis Type

送信 LLDP エージェントと関連付けられる IEEE802 LAN エンティティを含むシャーシを識別します。シャーシを識別し、コンポーネントのタイプを示すために使用されるシャーシ ID サブタイプが、シャーシ ID フィールドに参照されるためにはいくつかの方法があります。(P260 「シャーシ ID サブタイプ」を参照)

Chassis ID

このシステムの特定のシャーシの指定された識別子を示す、8 進数ストリング。

System Name

システムの管理上に割り当てられた名前を示すストリング。

System Description

ネットワークエンティティの記述。

Port Type

ポート ID フィールドでリストされる識別子を基礎に示します。

ポート ID サブタイプ

ID Basis	Reference
Interface alias	IfAlias (IETF RFC 2863)
Chassis component	entPhysClass が 'chassis(3)' の値を持つ時に EntPhysicalAlias (IETF RFC 2737)
Port alias	entPhysicalClass が 'port(10)' または 'backplane(4)' を持つ時は EntPhysicalAlias(IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	ネットワークアドレス
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	エージェントサーキット (IETF RFC 3046)
Locally assigned	ローカルに割り当てられる

Port Description

ポートの説明。RFC 2863 が実装されている場合、ifDescr オブジェクトがこのフィールドに使用されます。

Port ID

ポート識別子。

System Capabilities Supported

システムのプライマリファンクションを定義するケイパビリティ (P260 「システム性能」を参照)

System Capabilities Enabled

現在有効になっているシステムのプライマリファンクション。(P260 「システム性能」を参照)

Management Address List

このデバイスの管理アドレス。一般的には、レイヤ 3 デバイスに結び付けられる多くの異なるアドレスが存在するため、個々の LLDP PDU は 1 つ以上の管理アドレス TLV を含みます。
マネージメントアドレスが利用可能でない場合、アドレスは CPU またはポートのためにこのアドバタイズメントを送信します。

ポート詳細 (802.1 拡張情報)

Remote Port VID

ポートのデフォルト VLAN 識別子 (PVID) は VLAN がタグ無しまたはプライオリティタグフレームが割り当てられているかを示します。

Remote Port-Protocol VLAN List

このインタフェースに設定されているポートベースおよびプロトコルベース VLAN。

Remote VLAN Name List

ポートに関連付けられる VLAN 名。

Remote Protocol Identity List

ポートを通過してアクセス可能な特定のプロトコルの情報。

ポート詳細 (802.3 拡張情報)

Remote Port Auto-Neg Supported

所定のポート（リモートシステムに関連付けられた）がオートネゴシエーションをサポートするか否かを示します。

Remote Port Auto-Neg Adv-Capability

リモートシステムのポートに関連付けられた IfMauAutoNegCapAdvertisedBits オブジェクトの値（ビットマップ）（IETF RFC 3636 で定義）

リモートポートオートネゴシエーションアドバタイズドキャパビリティ

Bit	Reference
0	その他または未知
1	10BASE-T half duplex mode
2	10BASE-T full duplex mode
3	100BASE-T4
4	100BASE-TX half duplex mode
5	100BASE-TX full duplex mode
6	100BASE-T2 half duplex mode
7	100BASE-T2 full duplex mode
8	PAUSE for full-duplex links
9	Asymmetric PAUSE for full-duplex links
10	Symmetric PAUSE for full-duplex links
11	Asymmetric and Symmetric PAUSE for full-duplex links
12	1000BASE-X, -LX, -SX, -CX half duplex mode
13	1000BASE-X, -LX, -SX, -CX full duplex mode
14	1000BASE-T half duplex mode
15	1000BASE-T full duplex mode

Remote Port Auto-Neg Status

リモートシステムに関連付けられたポートでオートネゴシエーションが有効か否かを表示。

Remote Port MAU Type

送信デバイスの稼動している MAU タイプを示す整数値。このオブジェクトは IETF RFC 3636 にリストされた dot3MauType に対応するリストポジションから得られる整数値を含み、それぞれの dot3MauType OID の最後の数と等しいです。

ポート詳細 (802.3 拡張パワー情報)

Remote Power Class

リモートシステムに関連付けられる所定のポートのポートクラス (PSE - Power Sourcing Equipment または PD - Powered Device)

Remote Power MDI Status

リモートシステムに関連付けられる所定のポートで MDI パワーが有効か否かを表示

Remote Power Pairs

"Signal" は信号ペアのみ使用されていることを意味します。"Spare" は予備のペアのみしようされていることを意味します。

Remote Power MDI Supported

リモートシステムに関連付けられた所定のポートに、MDI パワーがサポートされているか否かを表示します。

Remote Power Pair Controlable

ペアセレクションがリモートシステムに関連付けられた所定のポートの sourcing power でコントロール可能か否かを示します。

Remote Power Classification

LAN ネットワーク上の異なるパワーターミナルを電力消費量に従いタグを使用することで分類します。IP 電話のようなデバイス、WLAN アクセスポイント、その他はそれらの必要電力条件によって分類されます。

ポート詳細 (802.3 拡張トランク情報)

Remote Link Aggregation Capable

リモートポートがリンクアグリゲーション状態にあるか否か、またはリンクアグリゲーションをサポートしているかいないかを表示。

Remote Link Aggregation Enable

リンクの現在のアグリゲーション状態。

Remote Link Aggregation Port ID

リモートシステムに関連付けられたポートコンポーネントの ifIndex の ifNumber から得られた IEEE 802.3 aggregated port identifier、aAggPortID (IEEE 802.3-2002, 30.7.2.1.1) を含みます。リモートポートがリンクアグリゲーション状態に無いかサポートしていない場合、この値は 0 になります。

設定方法

LLDP のリモートデバイス情報を表示 (Port)

- (1) [Administration] → [LLDP] をクリックします。
- (2) 「Step」 リストから「Remote Device Information」を選択します。
- (3) 「Port」、「Port Details」、「Trunk」、「Trunk Details」からいずれかを選択します。
- (4) < Apply > をクリックします。

Administration > LLDP

Step: 4. Show Remote Device Information

☒ Port
 ☐ Port Details
 ☐ Trunk
 ☐ Trunk Details

LLDP Remote Device Port List Max: 10 Total: 2

Local Port	Chassis ID	Port ID	System Name
3	00-0D-54-FC-8C-74	00-0D-54-FC-8C-74	ES3510MA
4	00-0D-54-FC-8C-74	00-0D-54-FC-8C-77	ES3510MA

LLDP のリモートデバイス情報を表示 (Port 詳細)

Administration > LLDP

Step: 4. Show Remote Device Information

☐ Port
 ☒ Port Details
 ☐ Trunk
 ☐ Trunk Details

Port 2

LLDP Remote Device Port Information

Local Port	2	Port Type	MAC Address
Chassis Type	MAC Address	Port Description	Ethernet Port on unit 1, port 1
Chassis ID	00-E0-0C-00-00-FE	Port ID	00-E0-0C-00-00-FF
System Name		System Capabilities Supported	Bridge
System Description		System Capabilities Enabled	Bridge

Management Address List Total: 1

Address	Address Type
192.168.0.3	IPv4 Address

802.3 Extension Port Information

Remote Port Auto-Neg Supported	Yes	Remote Port Auto-Neg Status	Enabled
Remote Port Auto-Neg Adv-Capability	0000	Remote Port MAU Type	6

802.3 Extension Power Information

Remote Power Class	PSE	Remote Power MDI Supported	Yes
Remote Power MDI Status	Enabled	Remote Power Pair Controlable	No
Remote Power Pairs	Spare	Remote Power Classification	Class1

802.3 Extension Trunk Information

Remote Link Aggregation Capable	Yes	Remote Link Aggregation Status	Disabled
Remote Link Port ID	0		

802.3 Extension Frame Information

Remote Max Frame Size	1518		

3.13.7 デバイス統計値の表示

LAdministration > LLDP (Show Device Statistics) ページを使用し、このスイッチに接続されている LLDP が有効なすべてのデバイスの統計を表示します。

設定・表示項目

リモートデバイスの概要統計値

Neighbor Entries List Last Updated

LLDP 隣接エントリリストが最後に更新された時。

New Neighbor Entries Count

リモート TTL の期限が切れていない LLDP 隣接の数。

Neighbor Entries Deleted Count

なんらかの理由で、LLDP リモートシステム MIB から取り除かれた LLDP 隣接の数。

Neighbor Entries Dropped Count

リソース不足のために、スイッチ上のリモートデータベースが LLDP DU をドロップした時間数

Neighbor Entries Age-out Count

TTL タイマーの期限切れが原因で、近隣の情報が LLDP リモートシステム MIB から削除された時間数。

ポート / トランク

Frames Discarded

特定の TLV に定義された指定の使用ルールに加え、通常の承認規則に準じずに破棄されたフレーム数。

Frames Invalid

全ての LLDPDU の 1 つまたはそれ以上で探知可能なエラーの数。

Frames Received

受信された LLDP PDU。

Frames Sent

送信された LLDP PDU。

TLVs Unrecognized

受信された LLDP ローカルエージェントによって認識されない全ての TLV の数。

TLVs Discarded

受信され、メモリ不足、アウトオブシーケンスまたはその他の理由で破棄された全ての LLDPDU の数

Neighbor Ageouts

TTL タイマの期限切れが理由で、近隣情報が LLDP リモートシステム MIB から削除された時間。

設定方法

LLDP デバイス統計値の表示（General）

- (1) [Administration] → [LLDP] をクリックします。
- (2) 「Step」 リストから「Show Device Statistics」を選択します。
- (3) “General”、“Port”、“Trunk” からいずれかを選択します。

Administration > LLDP

Step: 5. Show Device Statistics ▼

☒ General
 ☐ Port
 ☐ Trunk

LLDP Device Statistics

Neighbor Entries List Last Updated 0 sec

New Neighbor Entries Count 0
 Neighbor Entries Deleted Count 0
 Neighbor Entries Dropped Count 0
 Neighbor Entries Age-out Count 0

LLDP デバイス統計値の表示（Port）

Administration > LLDP

Step: 5. Show Device Statistics ▼

☐ General
 ☒ Port
 ☐ Trunk

Port 3 ▼

LLDP Device Port Statistics

Frames Discarded	0	TLVs Unrecognized	0
Frames Invalid	0	TLVs Discarded	0
Frames Received	0	Neighbor Ageouts	0
Frames Sent	0		

Refresh

3.13.8 SNMP

Simple Network Management Protocol (SNMP) はネットワーク上の機器の管理用の通信プロトコルです。SNMP は一般的にネットワーク機器やコンピュータなどの監視や設定をネットワーク経由で行う際に使用されます。

本機は SNMP エージェントを搭載し、ポートの通信やハードウェアの状態を監視することができます。SNMP 対応のネットワーク管理ソフトウェアを使用することで、これらの情報にアクセスすることが可能です。本機の内蔵エージェントへのアクセス権はコミュニティ名 (Community Strings) により設定されます。そのため、本機にアクセスするためには、事前に管理ソフトウェアのコミュニティ名を適切な値に設定する必要があります。

本機は、SNMP バージョン 1,2c,3 をサポートするエージェントを搭載し、ポートの通信やハードウェアの状態を監視することができます。ネットワーク上のマネージメントステーションは、ネットワーク管理ソフトウェアを使用し、これらの情報にアクセスすることが可能です。

SNMPv1,v2c を使用時のアクセス認証はコミュニティ名によってのみ行われますが、SNMPv3 ではマネージャとエージェント間が交換するメッセージを認証、暗号化することによって、機器へのセキュアなアクセスを提供しています。

SNMPv3 では、セキュリティモデルおよびセキュリティレベルが定義されます。セキュリティモデルは、ユーザーおよび、ユーザーが属するグループを設定するプロセスです。セキュリティレベルは、セキュリティモデルで許可されるセキュリティのレベルです。セキュリティモデルとセキュリティレベルの組み合わせによって、SNMP パケットの取り扱いに際して使用されるプロセスが決定されます。セキュリティモデルには SNMPv1、SNMPv2c および SNMPv3 の 3 種類が定義されています。

SNMPv3 セキュリティモデルとレベル

Model	Level	Group	Read View	Write View	Notify View	security
v1	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v1	noAuthNoPriv	user defined	user defined	user defined	user defined	Community string only
v2c	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v2c	noAuthNoPriv	user defined	user defined	user defined	user defined	Community string only
v3	noAuthNoPriv	user defined	user defined	user defined	user defined	A user name match only
v3	AuthNoPriv	user defined	user defined	user defined	user defined	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	user defined	user defined	user defined	user defined	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

[注意] 既定値のデフォルトグループとビューはシステムから削除可能です。その後にアクセスに必要な、カスタマイズグループとビューを定義することができます。

機能解説

SNMPv1/2c 管理アクセスの設定

スイッチに SNMPv1 または v2c 管理アクセスを設定するには、以下のステップを行ってください。

- (1) Administration > SNMP (Configure Global) ページを使用し、スイッチ上の SNMP とトラップマネージャを有効にします。
- (2) Use the Administration > SNMP (Configure User - Add Community) ページを使用し、管理アクセスのために認可されたコミュニティストリングを設定します。
- (3) Administration > SNMP (Configure Trap) ページを使用し、このスイッチによってキーイベントが管理ステーションにレポートを行うように、トラップマネージャを指定します。

SNMPv3 管理アクセスの設定

- (1) Administration > SNMP (Configure Global) ページを使用し、スイッチ上の SNMP とトラップマネージャを有効にします。
- (2) Administration > SNMP (Configure Trap) ページを使用し、このスイッチによってキーイベントが管理ステーションにレポートを行うように、トラップマネージャを指定します。
- (3) Administration > SNMP (Configure Engine) ページを使用し、ローカルエンジン ID を変更します。デフォルトエンジン ID を変更したい場合、他のパラメータの設定前に行ってください。
- (4) Administration > SNMP (Configure View) ページを使用し、スイッチ MIB ツリーの read、write アクセスビューを指定します。
- (5) Administration > SNMP (Configure User) ページを使用し、要求されるセキュリティモデル (SNMP v1、v2c、v3) とセキュリティレベル (authentication および privacy) と共に SNMP ユーザーグループを設定します。
- (6) Administration > SNMP (Configure Group) ページを使用し、特定の認証とプライバシーパスワードと共に、SNMP ユーザをグループに割り当てます。

3.13.9 SNMP グローバル設定

Administration > SNMP (Configure Global) ページを使用し、全ての管理クライアントの SNMPv3 サービスとトラップマネージャを有効にします。

設定・表示項目

Agent Status

チェックを入れることで、SNMP エージェントが有効になります

Authentication Traps*

認証時に不正なパスワードが送信された場合にトラップが発行されます
(初期設定：有効)

Link-up and Link-down Traps*

Link-up 又は Link-down 時にトラップが発行されます (初期設定：有効)

* これらは旧式の通知であり、SNMPv3 ホスト使用時、通知ビュー (P276) の対応する項目に関連して有効になります。

設定方法

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) SNMP と必要なトラップ対応を有効にします。
- (4) < Apply > をクリックします。

Administration > SNMP

Step: 1. Configure Global ▼

Agent Status	☒ Enabled
Authentication Traps	☒ Enabled
Link-up and Link-down Traps	☒ Enabled

Apply Revert

ローカルエンジン ID の設定

SNMPv3 エンジンとは、スイッチ上の独立した SNMP エージェントです。このエンジンはメッセージの再送、遅延およびリダイレクションを防止します。エンジン ID は、ユーザーパスワードと組み合わせて、SNMPv3 パケットの認証と暗号化を行うためのセキュリティキーを生成します。

機能解説

ローカルエンジン ID はスイッチにたいして固有になるように自動的に生成されます。これをデフォルトエンジン ID とよびます。

ローカルエンジン ID が削除または変更された場合、全ての SNMP ユーザーはクリアされます。そのため既存のユーザーの再構成を行う必要があります。

設定・表示項目

Engine ID

新しいエンジン ID は 9 から 64 の 16 進数（16 進形式の 5 から 32 の 8 オクテット）で指定することが可能です。

もし半端な番号が指定された時、後置 0 が最後のオクテットを埋めるために追加されます。

例えば、"123456789" の値は "1234567890" と同等です。 .

設定方法

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure Engine」を選択します。
- (3) 「Action」 リストから「Set Engine ID」を選択します。
- (4) エンジン ID を入力し、< Save >をクリックします。

Administration > SNMP

Step: 2. Configure Engine Action: Set Engine ID

Engine ID 800063e6030012cff3de460000

Default Save

リモートエンジン ID の設定

リモートデバイス上の SNMPv3 ユーザーヘインフォームメッセージを送る場合、最初にリモートエンジン ID を設定します。リモートエンジン ID は、リモートホストで認証と暗号化パケットのセキュリティダイジェストを計算するために使用されます。

機能解説

SNMP パスワードは、信頼できるエージェントのエンジン ID を使用してローカライズされます。インフォームの信頼できる SNMP エージェントはリモートエージェントです。そのため、プロキシリクエストまたはインフォームを送信する前にリモートエージェントの SNMP エンジン ID を設定する必要があります。(詳しくは P287 「トラップマネージャの指定」 および P285 「SNMPv3 リモートユーザーの設定」を参照してください)

設定・表示項目

Remote Engine ID

新しいエンジン ID は 9 から 64 の 16 進数 (16 進形式の 5 から 32 の 8 オクテット) で指定することが可能です。
もし半端な番号が指定された時、後置 0 が最後のオクテットを埋めるために追加されます。
例えば、"123456789" の値は "1234567890" と同等です。

Remote IP Host

指定されたエンジン ID を使用する、リモート管理ステーションの IP アドレス。

設定方法

リモート SNMP エンジン ID の設定

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure Engine」を選択します。
- (3) 「Action」 リストから「Add Remote Engine」を選択します。
- (4) エンジン ID を入力し、< Save >をクリックします。

Administration > SNMP

Step: 2. Configure Engine ▼ Action: Add Remote Engine ▼

Remote Engine ID: 5432100000

Remote IP Host: 192.168.1.19

Apply Revert

リモート SNMP エンジン ID の表示

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure Engine」を選択します。
- (3) 「Action」 リストから「Show Remote Engine」を選択します。

Administration > SNMP

Step: 2. Configure Engine ▼ Action: Show Remote Engine ▼

SNMPv3 Remote Engine List Max: 5 Total: 1

	Remote Engine ID	Remote IP Host
☐	5432100000	192.168.1.19

Delete Revert

SNMPv3 ビューの設定

SNMP ビューとは、SNMP オブジェクトと、それらのオブジェクトについて使用可能なアクセス権限と対応関係を示した物です。

事前に定義されているビュー（デフォルトビュー）には全体の MIB ツリーへのアクセスが含まれます。

設定・表示項目

Add View

View Name

SNMP ビュー名（1-64 文字）

OID Subtrees

ビューの内容が表示されます

Type

[OID Subtrees] で指定した OID を、参照可能な範囲に含む（included）か含まない（excluded）かを選択します

Add OID Subtree

View Name

「Add View」 ページで設定された SNMP ビューリスト

OID Subtrees

ビューの内容が表示されます

Type

[OID Subtrees] で指定した OID を、参照可能な範囲に含む（included）か含まない（excluded）かを選択します

設定方法

スイッチの MIB データベースの SNMP ビューを設定

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure View」を選択します。
- (3) 「Action」 リストから「Add View」を選択します。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Administration > SNMP

Step: 3. Configure View Action: Add View

View Name: EntryA

OID Subtree: 1.3.6.1.2.1.2.2.1.1

Type: Included

Apply Revert

SNMPv3 ビューを表示

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure View」を選択します。
- (3) 「Action」 リストから「Show View」を選択します。

Administration > SNMP

Step: 3. Configure View Action: Show View

SNMPv3 View List Max: 32 Total: 2

	View Name
☐	EntryA
☐	defaultview

Delete Revert

OID サブツリーを SNMPv3 ビューへ追加

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure View」を選択します。
- (3) 「Action」 リストから「Add OID Subtree」を選択します。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Administration > SNMP

Step: 3. Configure View Action: Add OID Subtree

View Name: EntryA

OID Subtree: 1.3.6.1.2.1.2.2.1.2

Type: Included

Apply Revert

SNMPv3 ビューに設定された OID サブツリーを表示

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure View」を選択します。
- (3) 「Action」 リストから「Show OID Subtree」を選択します。
- (4) 既存のリストからビュー名を選択してください。

Administration > SNMP

Step: 3. Configure View Action: Show OID Subtree

View Name: EntryA

SNMPv3 View OID Subtree List Max: 32 Total: 2

	OID Subtree	Type
☐	1.3.6.1.2.1.2.2.1.1	Included
☐	1.3.6.1.2.1.2.2.1.2	Included

Delete Revert

SNMPv3 グループの設定

SNMPv3 グループは、特定のセキュリティモデルに属するユーザーの集合です。グループはそのグループに属する全ユーザーのアクセスポリシーを定義します。アクセスポリシーによって、読み取り、書き込み、または受信できるトラップ通知の制限が行われます。

設定・表示項目

Group Name

グループ名 (1-32 文字)

Security Model

セキュリティモデル (1,v2c,v3)

Security Label

- noAuthNoPriv — 認証も暗号化も行いません
- AuthNoPriv — 認証を行いますが暗号化は行いません (v3 セキュリティモデルでのみ設定可)
- AuthPriv — 認証と暗号化を行います (v3 セキュリティモデルでのみ設定可)

Read View

Read アクセスのビューを設定します (範囲: 1-64 文字)

Write View

Write アクセスのビューを設定します (範囲: 1-64 文字)

Notify View

通知ビューを設定します。下表にてサポートする通知メッセージを示します。(範囲: 1-64 文字)

Object Label	Object ID
<i>RFC1493Traps</i>	
newRoot	1.3.6.1.2.1.17.0.1
topologyChange	1.3.6.1.2.1.17.0.2
<i>SNMPv2 Traps</i>	
coldStart	1.3.6.1.6.3.1.1.5.1
warmStart	1.3.6.1.6.3.1.1.5.2
linkDown*	1.3.6.1.6.3.1.1.5.3
linkUp*	1.3.6.1.6.3.1.1.5.4
authentication Failure*	1.3.6.1.6.3.1.1.5.5
<i>RMON Events(V2)</i>	
risingAlarm	1.3.6.1.2.1.16.0.1
fallingAlarm	1.3.6.1.2.1.16.0.2
<i>Private Traps</i>	
swPowerStatus Change Trap	1.3.6.1.4.1.202.20.56.63.2.1.0.1
swPortSecurityTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.36
swIpFilter RejectTrap	1.3.6.1.4.1.202.20.56.63.2.1.0.40
swAuthenticationFailure	1.3.6.1.4.1.25574.10.1.11.2.1.0.66
swAuthenticationSuccess	1.3.6.1.4.1.25574.10.1.11.2.1.0.67
swAtcBcastStormAlarmFireTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.70

Web インタフェース

基本管理プロトコル

swAtcBcastStormAlarmClearTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.71
swAtcBcastStormTcApplyTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.72
swAtcBcastStormTcReleaseTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.73
swAtcMcastStormAlarmFireTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.74
swAtcMcastStormAlarmClearTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.75
swAtcMcastStormTcApplyTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.76
swAtcMcastStormTcReleaseTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.77
swLoopbackDetectionTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.92
networkAccessPortLinkDetectionTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.96
autoUpgradeTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.104
swCpuUtiRisingNotification	1.3.6.1.4.1.25574.10.1.11.2.1.0.107
swCpuUtiFallingNotification	1.3.6.1.4.1.25574.10.1.11.2.1.0.108
swMemoryUtiRisingThresholdNotification	1.3.6.1.4.1.25574.10.1.11.2.1.0.109
swMemoryUtiFallingThresholdNotification	1.3.6.1.4.1.25574.10.1.11.2.1.0.110
dhcpRougeServerAttackTrap	1.3.6.1.4.1.25574.10.1.11.2.1.0.114

* これらは旧式の通知であり、SNMP 設定メニュー上の対応するトラップと関連して有効になります。

設定方法

SNMP グループの設定

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure Group」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Administration > SNMP

Step: 4. Configure Group Action: Add

Group Name:

Security Model: v3

Security Level: authPriv

Read View: ☒ EntryA ☐

Write View: ☒ EntryA ☐

Notify View: ☒ EntryA ☐

Apply Revert

SNMP グループの表示

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure Group」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Administration > SNMP

Step: 4. Configure Group Action: Show

SNMPv3 Group List Max: 26 Total: 5

☐	Group Name	Model	Level	Read View	Write View	Notify View
☐	public	v1	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
☐	public	v2c	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
☐	private	v1	noAuthNoPriv	defaultview	defaultview	No notifyview specified
☐	private	v2c	noAuthNoPriv	defaultview	defaultview	No notifyview specified
☐	secure-users	v3	authPriv	EntryA	EntryA	EntryA

Delete Revert

3.13.10 コミュニティ名の設定

管理アクセスの認証のためのコミュニティ名を最大 5 つ設定することができます。IP トラップマネージャで使用されるコミュニティ名もすべてここにリストされています。

セキュリティのため、初期設定のコミュニティ名を削除することを推奨します。

設定・表示項目

Community String

SNMP でのアクセスを行う際にパスワードの役割を果たすコミュニティ名
(初期設定: "public" (Read-Only アクセス), "private" (Read/Write アクセス)、設定範囲: 1-32 文字, 大文字小文字は区別されます)

Access Mode

コミュニティ名へのアクセス権を設定します:

- Read-Only — 読み取り専用アクセスとなります。管理ソフトウェアからは MIB オブジェクトの取得のみができます。
- Read/Write — 読み書き可能なアクセスとなります。認可された管理ステーションは MIB オブジェクトの取得と変更の両方が可能です。

設定方法

コミュニティ名の設定

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure User」を選択します。
- (3) 「Action」 リストから「Add Community」を選択します。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Administration > SNMP

Step: 5. Configure User Action: Add Community

Community String: spiderman

Access Mode: Read/Write

Apply Revert

コミュニティ名の表示

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure User」を選択します。
- (3) 「Action」 リストから「Show Community」を選択します。

Administration > SNMP

Step: 5. Configure User Action: Show Community

SNMP Community String List Max: 5 Total: 3

	Community String	Access Mode
☐	public	Read-Only
☐	private	Read/Write
☐	spiderman	Read/Write

Delete Revert

SNMPv3 ローカルユーザーの設定

それぞれの SNMPv3 ユーザーは固有の名前を持ちます。
ここでは、各ユーザーの所属グループ、セキュリティレベル等を設定します。SNMP v3 では、ユーザーが所属するグループによってアクセス制限が定義されます。

設定・表示項目

User Name

SNMPv3 ユーザー名 (1-32 文字)

Group Name

既存のグループから選択または新規グループを作成します (1-32 文字)

Security Model

セキュリティモデルを選択します (v1,v2c,v3)

Security Level

セキュリティレベル

- noAuthNoPriv — 認証も暗号化も行いません (初期設定)
- AuthNoPriv — 認証を行いますが暗号化は行いません
- AuthPriv — 認証と暗号化を行います

Authentication Protocol

認証用プロトコルの選択。MD5 または SHA (初期設定: MD5)

Authentication Password

認証用パスワード (最小 8 文字)

Privacy Protocol

暗号化プロトコル。DES56bit のみ使用可。

Privacy Password

プライバシーパスワード (最小 8 文字)

設定方法

SNMPv3 ローカルユーザの設定

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure User」を選択します。
- (3) 「Action」 リストから「Add SNMPv3 Local User」を選択します。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Administration > SNMP

Step: 5. Configure User Action: Add SNMPv3 Local User

SNMPv3 User

User Name:

Group Name: ☐ public ☒ R&D

Security Model: v3

Security Level: authPriv

User Authentication

Authentication Protocol: MD5

Authentication Password:

Data Privacy

Privacy Protocol: DES56

Privacy Password:

Apply Revert

SNMPv3 ローカルユーザの表示

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure User」を選択します。
- (3) 「Action」 リストから「Show SNMPv3 Local User」を選択します。

Administration > SNMP

Step: 5. Configure User Action: Show SNMPv3 Local User

SNMPv3 Local User List Max: 16 Total: 1

☐	User Name	Group Name	Model	Level	Authentication	Privacy
☐	chris	R&D	v3	authPriv	MD5	DES56

Delete Revert

SNMPv3 リモートユーザーの設定

Administration > SNMP (Configure User - Add SNMPv3 Remote User) ページを使用し、ローカルスイッチから送信される SNMPv3 通知メッセージのソースを識別します。

それぞれの SNMPv3 ユーザーは固有の名前を持ちます。

機能解説

- SNMP v3 では、ユーザーが所属するグループによってアクセス制限が定義されます。リモートデバイス上の SNMP ユーザーヘインフォームメッセージを送るために、最初に、ユーザーが属するリモートデバイス上の SNMP エージェントへ ID を設定します。リモートエンジン ID は、リモートホストで認証と暗号化パケットのセキュリティダイジェストを計算するために使用されます。(詳細は P287 「トラップマネージャの指定」および P274 「リモートエンジン ID の設定」を参照してください)

設定・表示項目

User Name

SNMPv3 ユーザー名 (1-32 文字)

Group Name

グループ名を選択します (1-32 文字)

Remote IP

ユーザーが属するリモートデバイスのインターネットアドレス

Security Model

セキュリティモデル (v1,v2c,v3 初期設定: v3)

Security Label

セキュリティレベル

- noAuthNoPriv — 認証も暗号化も行いません (初期設定)
- AuthNoPriv — 認証を行いますが暗号化は行いません
- AuthPriv — 認証と暗号化を行います

Authentication Protocol

認証用プロトコルの選択。MD5 または SHA (初期設定: MD5)

Authentication Password

認証用パスワード (最小 8 文字)

Privacy Protocol

暗号化プロトコル。DES56bit のみ使用可。

Privacy Password

プライバシーパスワード (最小 8 文字)

設定方法

SNMPv3 リモートユーザの設定

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure User」を選択します。
- (3) 「Action」 リストから「Add SNMPv3 Remote User」を選択します。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Administration > SNMP

Step: 5. Configure User Action: Add SNMPv3 Remote User

SNMPv3 User

User Name: mark

Group Name: ☐ public ☒ R&D

Remote IP: 192.168.1.19

Security Model: v3

Security Level: authPriv

User Authentication

Authentication Protocol: MD5

Authentication Password: greenpeace

Data Privacy

Privacy Protocol: DES56

Privacy Password: greenpeace

Apply Revert

SNMPv3 リモートユーザの表示

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure User」を選択します。
- (3) 「Action」 リストから「Show SNMPv3 Remote User」を選択します。

Administration > SNMP

Step: 5. Configure User Action: Show SNMPv3 Remote User

SNMPv3 Remote User List Max: 5 Total: 1

	User Name	Group Name	Engine ID	Model	Level	Authentication	Privacy
☐	mark	R&D	5432100000	v3	authPriv	MD5	DES56

Delete Revert

トラップマネージャの指定

本機の状態に変更があった場合に本機からトラップマネージャに対してトラップが出されます。トラップを有効にするためにはトラップを受け取るトラップマネージャを指定する必要があります。

認証失敗メッセージ及び他のトラップメッセージを受信する管理端末を最大 5 つまで指定することができます。

機能解説

- ・ スイッチは、初期設定でトラップメッセージの通知を行いますが、トラップメッセージの受け取り側はスイッチへ応答を送りません。その為十分な信頼性は確保できません。インフォームを使用することにより、重要情報がホストに受け取られるのを保証することが可能です。
インフォームを使用した場合、スイッチは応答を受け取るまでの間、情報をメモリ内に保持しなくてはならないため多くのシステムリソースを使用します。またインフォームはネットワークトラフィックにも影響を与えます。これらの影響を考慮した上でトラップまたはインフォームの使用を決定してください。

SNMPv2 ホストヘインフォームを送信するには、以下のステップを完了させてください。

- (1) SNMP エージェントを有効にします。(P272)
- (2) 必要とされる通知メッセージでビューを作成します。(P276)
- (3) 必要とされる通知ビューを含む、グループ（「Configure Trap - Add page」ページ (P279) で指定されたコミュニティストリングマッチする）を設定します。
- (4) トラップ通知を有効にします。

SNMPv3 ホストヘインフォームを送信するには、以下のステップを完了させてください。

- (1) SNMP エージェントを有効にします。(P272)
- (2) メッセージ交換プロセスで使用される、ローカル SNMPv3 ユーザを作成します。(P283)
- (3) 必要とされる通知メッセージでビューを作成します。(P276)
- (4) 必要とされる通知ビューを含む、グループを作成します。(P279)
- (5) トラップ通知を有効にします。

設定・表示項目

SNMP Version1

IP Address

通知メッセージを受け取る新しい管理ステーションの IP アドレス

Version

通知を送るトラップを SNMPv1、v2c または v3 から選択します。(初期設定：1)

Community String

新しいトラップマネージャエントリの有効なコミュニティストリングを指定。

(1-32 文字。大文字小文字を区別します。)

この項目は Configure Trap - Add ページでも設定できますが、Configure User - Add Community ページで定義することを推奨します。

UDP Port

トラップマネージャで使用する UDP ポート番号 (初期設定: 162)

SNMP Version2c

IP Address

通知メッセージを受け取る新しい管理ステーションの IP アドレス

Version

通知を送るトラップを SNMPv1、v2c または v3 から選択します。

Notification Type

- Traps — 通知はトラップメッセージとして送信されます。
- Inform — 通知は通知メッセージとして送信されます。(初期設定: トラップ)
- Timeout — 通知メッセージを再送する前に、承認を待つ秒数
(範囲: 0-2147483647 センチセカンド 初期設定: 1500 センチセカンド)
- Retry times — レシピエントが受け取ったことを知らせない場合に、通知メッセージを再送する最大数 (範囲: 0-255 初期設定: 3)

Community String

新しいトラップマネージャエントリの有効なコミュニティストリングを指定 (1-32 文字。大文字小文字を区別します。)

この項目は Configure Trap - Add ページでも設定できますが、Configure User - Add Community ページで定義することを推奨します。

UDP Port

トラップマネージャで使用する UDP ポート番号 (初期設定: 162)

SNMP Version3

IP Address

通知メッセージを受け取る新しい管理ステーションの IP アドレス

Version

通知を送るトラップを SNMPv1、v2c または v3 から選択します。

Notification Type

- Traps — 通知はトラップメッセージとして送信されます。
- Inform — 通知は通知メッセージとして送信されます。(初期設定: トラップ)
- Timeout — 通知メッセージを再送する前に、承認を待つ秒数
(範囲: 0-2147483647 センチセカンド 初期設定: 1500 センチセカンド)
- Retry times — レシピエントが受け取ったことを知らせない場合に、通知メッセージを再送する最大数 (範囲: 0-255 初期設定: 3)

Local User Name

ローカルスイッチから送信される SNMPv3 トラップメッセージのソースを識別するために使用されるローカルユーザ名（範囲：1-32 文字）

指定されたユーザのアカウントが作成されていない場合際には (P383)、1 つが自動で生成されます。

Remote User Name

ローカルスイッチから送信される SNMPv3 通知メッセージのソースを識別するために使用されるローカルユーザ名（範囲：1-32 文字）

指定されたユーザのアカウントが作成されていない場合際には (P383)、1 つが自動で生成されます。

UDP Port

トラップマネージャで使用する UDP ポート番号（初期設定：162）

Security Level

セキュリティレベル（初期設定：noAuthNoPriv）

- － noAuthNoPriv － 認証も暗号化も行いません（初期設定）
- － AuthNoPriv － 認証を行いますが暗号化は行いません
- － AuthPriv － 認証と暗号化を行います

設定方法

トラップマネージャの設定 (SNMPv1)

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure Trap」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) 必要な項目を入力し、< Apply >をクリックします。

Administration > SNMP

Step: 6. Configure Trap ▼ Action: Add ▼

IP Address	192.168.0.3
Version	v1 ▼
Community String	private
UDP Port (1-65535)	162

Apply Revert

トラップマネージャの設定 (SNMPv2c)

Administration > SNMP

Step: 6. Configure Trap ▼ Action: Add ▼

IP Address	192.168.2.9
Version	v2c ▼
Notification Type	Inform ▼
Timeout (0-2147483647)	1600 centiseconds
Retry Times (0-255)	5
Community String	venus
UDP Port (1-65535)	162

Apply Revert

トラップマネージャの設定 (SNMPv3)

Administration > SNMP

Step: 6. Configure Trap Action: Add

IP Address: 192.168.3.6

Version: v3

Notification Type: Inform

Timeout (0-2147483647): 1600 centiseconds

Retry Times (0-255): 5

Remote User Name: margaret

UDP Port (1-65535): 162

Security Level: authPriv

Apply Revert

トラップマネージャ設定の表示

- (1) [Administration] → [SNMP] をクリックします。
- (2) 「Step」 リストから「Configure Trap」を選択します。
- (3) 「Action」 リストから「show」を選択します。

Administration > SNMP

Step: 6. Configure Trap Action: Show

SNMP Trap Manager List Max: 5 Total: 3

	IP Address	Version	Community String/User Name	UDP Port	Security Level	Timeout	Retry Times
☐	192.168.0.3	v1	private	162			
☐	192.168.2.9	v2c	venus	162		1500	3
☐	192.168.2.10	v3	manager	162	authPriv	1500	3

Delete Revert

3.13.11 リモートモニタリング

リモートモニタリングは、リモート装置が非依存を基礎に、指定されたイベントの情報を収集または対処することを可能にします。

本機は、独立して広範囲のタスクを実行することが可能な RMON に対応しており、ネットワーク管理トラフィックを大幅に低減することが出来ます。

この機能により、連続的な診断とログ情報収集を行えます。

本機は統計、履歴、イベント、アラームグループから成る、mini-RMON をサポートしています。

RMON 有効時、システムは次第にその物理的インタフェースに関する情報を増強し、この情報に適切な RMON データベースグループへ保存します。

管理エージェントは SNMP プロトコルを使用し、周期的にスイッチとコミュニケーションを行います。

もしスイッチが致命的なイベントに遭遇した場合、それは管理エージェントへ自動でトラップメッセージを送信します。

RMON アラームの設定

Administration > RMON (Configure Global - Add - Alarm) ページを使用し、応答イベントを生成するための、特定の基準を定義します。

アラームは指定された時間間隔に渡ってテストを行うよう設定することが可能で、無制限または変化値を監視することが出来ます。(特定の値に達する統計カウンタまたは、設定した間隔を超える量で変化した統計量)

また、上昇または降下しきい値への対処を設定することが可能です(アラームが引き起こされた後、統計上の値が反対の境界を成すしきい値を越え、トリガとなるしきい値の先へ後退するまで、それが再び引き起こされないことに注意してください。)

機能解説

- ・ インデックスにて既にアラームが定義されている場合、変更を行う前にエントリを削除してください。

設定・表示項目

Index

このエントリのインデックス (範囲: 1-65535)

Variable

サンプルされる MIB 変数のオブジェクト識別子。

"etherStatsEntry.n.n" タイプのみがサンプルされます。

"etherStatsEntry.n" は一意的に MIB 変数を定義し、"etherStatsEntry.n.n" は MIB 変数と "etherStatsIndex" を定義します。

(例: 1.3.6.1.2.1.16.1.1.1.6.1 は "etherStatsBroadcastPkts" そして 1 の "etherStatsIndex" を示します)

Interval

ポーリング間隔 (範囲: 1-31622400 秒)

Sample Type

指定された変数の絶対的または相対的变化のテストを実行

- ・ Absolute – 変数はサンプリングピリオドの終わりのしきい値と直接比較されます。
- ・ Delta – 最終サンプルは現在の値から引かれ、相違がしきい値と比較されます。

Rising Threshold

上方閾値の値を指定します。(範囲：1-65535)

Rising Event Index

モニタされる変数が上方閾値に達するか越えたことによってアラームが引き起こされた際に使用されるイベントのインデックス。(範囲：1-65535)

Falling Threshold

下方閾値の値を指定します。(範囲：1-65535)

Falling Event Index

モニタされる変数が下方閾値に達するか下回ったことによってアラームが引き起こされた際に使用されるイベントのインデックス。(範囲：1-65535)

Owner

このエントリを作成した人の名前 (範囲：1-127 文字)

設定方法

RMON アラームの設定

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) 「Alarm」 をクリックします。
- (5) 必要な項目を入力し、[Apply] をクリックします。

Administration > RMON

Step: 1. Configure Global Action: Add

☒ Alarm ☐ Event

Index (1-65535)

Variable

Interval (1-31622400) sec

Sample Type

Rising Threshold (0-2147483647)

Rising Event Index (0-65535)

Falling Threshold (0-2147483647)

Falling Event Index (0-65535)

Owner

Apply Revert

RMON アラーム設定の表示

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Show」を選択します。
- (4) 「Alarm」 をクリックします。

Administration > RMON

Step: 1. Configure Global Action: Show

☒ Alarm ☐ Event

RMON Alarm List Max: 64 Total: 26

	Index	Status	Variable	Interval	Type	Last Value	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner
☐	1	Valid	1.3.6.1.2.1.16.1.1.1.6.1	30	Delta	0	892800	0	446400	0	
☐	2	Valid	1.3.6.1.2.1.16.1.1.1.6.2	30	Delta	0	892800	0	446400	0	
☐	3	Valid	1.3.6.1.2.1.16.1.1.1.6.3	30	Delta	0	892800	0	446400	0	
☐	4	Valid	1.3.6.1.2.1.16.1.1.1.6.4	30	Delta	0	892800	0	446400	0	
☐	5	Valid	1.3.6.1.2.1.16.1.1.1.6.5	30	Delta	0	892800	0	446400	0	

RMON イベントの設定

Administration > RMON (Configure Global - Add - Event) を使用し、アラームが引き起こされた時に行う行動を設定します。

応答にはアラームのロギングまたはトラップマネージャへのメッセージの送信を含むことが可能です。アラームと対応するイベントは、重要なネットワークプログラムに即座に応答する方法を提供します。

機能解説

- インデックスで既にアラームが定義されている場合、変更を行う前にエントリを削除してください。
- 以下の 1 つの初期イベントが設定されています。
event Index = 1
Description: RMON_TRAP_LOG
Event type: log & trap
Event community name is public
Owner is RMON_SNMP

設定・表示項目

Index

このエントリのインデックス（範囲：1-65535）

Type

開始イベントのタイプを指定

- None – イベントは生成されません。
- Log – イベントが引き起こされた時、RMON ログエントリが生成されます。ログメッセージはイベントロギングの最新の設定に基づいて処理されます。（251 ページの「Event Logging の設定」を参照）
- Trap – 設定された全てのトラップマネージャへトラップメッセージを送信します。（287 ページの「トラップマネージャの指定」を参照）
- Log and Trap – イベントのログとトラップメッセージの送信。

Community

トラップオペレーションで SNMPv1,v2c ホストに送信された、パスワードのようなコミュニティストリング。この設定ページでコミュニティストリングの設定を行うことも出来ますが、ここで設定を行う前に SNMP trap configuration ページ（P287）で定義することを推奨します。（範囲：1-32 文字）

Description

このイベントを説明するコメント（範囲：1-127 文字）

Owner

このエントリを作成した人の名前（範囲：1-127 文字）

設定方法

RMON イベントの設定

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) 「Event」 をクリックします。
- (5) 必要な項目を入力し、[Apply] をクリックします。

Administration > RMON

Step: 1. Configure Global ▼ Action: Add ▼

☐ Alarm ☒ Event

Index (1-65535)

Type

Community

Description

Owner

RMON アラーム設定の表示

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Show」を選択します。
- (4) 「Event」 をクリックします。

Administration > RMON

Step: 1. Configure Global ▼ Action: Show ▼

☐ Alarm ☒ Event

RMON Event List Max: 32 Total: 1

☐	Index	Status	Type	Community	Description	Owner	Last Fired
☐	2	Valid	Log and Trap	private	for the software group	david	00:00:00

RMON 履歴サンプルの設定

Administration > RMON (Configure Interface - Add - History) を使用し、ネットワーク使用率、パケットタイプ、エラーを監視するために、物理インタフェース上の統計値を収集します。

活動の履歴の記録は断続的な問題を追跡するために使用できます。

記録は通常のベースライン活動を確立するために使用することが出来ます。

これらはハイトラフィックレベル、ブロードキャストストーム、その他普通ではないイベントと関係づけられる問題を明らかにします。

また、ネットワーク成長を予測し、負荷が大きくなる前に拡張のプランを立てるためにも使用出来ます。

機能解説

- それぞれのインデックス番号はスイッチのポートと同等です。
- history collection が既にインタフェースで有効になっている場合、変更を行う前にエントリを削除してください。
- それぞれのサンプルで収集される情報には以下が含まれます。
input octets、packets、broadcast packets、multicast packets、undersize packets、oversize packets、fragments、jabbers、CRC alignment errors、collisions、drop events、network utilization
「Show Details」ページで表示される統計値の説明は 58 ページの「ポート・トランク統計情報表示」を参照してください。

設定・表示項目

Port

スイッチのポート番号

Index

このエントリのインデックス（範囲：1-65535）

Interval

ポーリングインターバル（範囲：1-3600 秒 初期設定：1800 秒）

Buckets

このエントリでリクエストされるバケットの番号（範囲：1-65535 初期設定：50）
生成されたバケットの番号は「Show」ページで表示されます。

Owner

このエントリを作成した人の名前（範囲：1-127 文字）

設定方法

ポートの統計値を周期的に収集

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) 「History」 をクリックします。
- (5) ポートを選択します。
- (6) 必要な項目を入力し、[Apply] をクリックします。

Administration > RMON

Step: 2. Configure Interface Action: Add

☒ History ☐ Statistics

Port
2

Index (1-65535) 100

Interval (1-3600) 60 sec

Buckets (1-65535) 10

Owner david

Apply Revert

設定された RMON 履歴サンプルの表示

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Show」を選択します。
- (4) リストからポートを選択します。
- (5) 「History」 をクリックします。

Administration > RMON

Step: 2. Configure Interface Action: Show

☒ History ☐ Statistics

Port
2

RMON History Port List Max: 96 Total: 3

☐	Index	Status	Interval	Requested Buckets	Granted Buckets	Owner
☐	3	Valid	1800	8	8	
☐	4	Valid	30	8	8	
☐	100	Valid	60	10	8	david

Delete Revert

収集された RMON 履歴サンプルを表示

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Show Details」を選択します。
- (4) リストからポートを選択します。
- (5) 「History」をクリックします。

Administration > RMON

Step: 2. Configure Interface Action: Show Details

☒ History ☐ Statistics

Port

2

RMON History Deatils Port List Max: 24 Total: 16

History Index	Sample Index	Interval Start	Octets	Packets	Broadcast Packets	Multicast Packets	Undersize Packets	Oversize Packets	Fragments	Jabbers	CRC Align Errors	Collisions	Drop Events	Network Utilization
3	2	00:30:01	0	0	0	0	0	0	0	0	0	0	0	0
3	3	01:00:01	0	0	0	0	0	0	0	0	0	0	0	0
3	4	01:30:01	0	0	0	0	0	0	0	0	0	0	0	0
3	5	02:00:01	0	0	0	0	0	0	0	0	0	0	0	0
3	6	02:30:01	0	0	0	0	0	0	0	0	0	0	0	0
3	7	03:00:01	0	0	0	0	0	0	0	0	0	0	0	0
3	8	03:30:01	0	0	0	0	0	0	0	0	0	0	0	0
3	9	04:00:01	0	0	0	0	0	0	0	0	0	0	0	0
4	570	04:44:34	0	0	0	0	0	0	0	0	0	0	0	0

RMON 統計サンプルの設定

Administration > RMON (Configure Interface - Add - Statistics) ページを使用し、ポートの統計値を収集して、エラーと全体のトラフィックレートのためにネットワークを監視することが出来ます。

機能解説

- 既にインタフェースで統計値の収集が有効になっている場合、変更を行う前にエントリを削除してください。
- それぞれのサンプルで収集される情報には以下が含まれます。
input octets、packets、broadcast packets、multicast packets、undersize packets、oversize packets、fragments、jabbers、CRC alignment errors、collisions、drop events、network utilization
「Show Details」ページで表示される統計値の説明は 58 ページの「ポート・トランク統計情報表示」を参照してください。

設定・表示項目

Port

スイッチのポート番号

Index

このエントリのインデックス（範囲：1-65535）

Owner

このエントリを作成した人の名前（範囲：1-127 文字）

設定方法

ポートで通常の統計値サンプルを有効にします。

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) 「Statistics」 をクリックします。
- (5) リストからポートを選択します。
- (6) 必要な項目を入力し、[Apply] をクリックします。

Administration > RMON

Step: 2. Configure Interface Action: Add

☐ History ☒ Statistics

Port
2

Index (1-65535) 100

Owner mary

Apply Revert

設定された RMON 履歴サンプルの表示

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) 「Action」 リストから「Show」を選択します。
- (4) リストからポートを選択します。
- (5) 「Statistics」 をクリックします。

Administration > RMON

Step: 2. Configure Interface Action: Show

☐ History ☒ Statistics

Port
2

RMON Statistics Port List Max: 10 Total: 1

	Index	Status	Owner
☐	2	Valid	

Delete Revert

収集された RMON 履歴サンプルを表示

- (1) [Administration] → [RMON] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 「Action」 リストから「Show Details」を選択します。
- (4) リストからポートを選択します。
- (5) 「Statistics」 をクリックします。

Administration > RMON

Step: 2. Configure Interface ▼ Action: Show Details ▼

☐ History ☒ Statistics

Port
1 ▼

RMON Statistics Port Details

Received Octets	6718661	Collisions	0
Received Packets	16243	Drop Events	0
Broadcast Packets	18	Frames of 64 Octets	8877
Multicast Packets	2	Frames of 65 to 127 Octets	1482
Undersize Packets	0	Frames of 128 to 255 Octets	804
Oversize Packets	0	Frames of 256 to 511 Octets	159
CRC Align Errors	0	Frames of 512 to 1023 Octets	1302
Jabbers	0	Frames of 1024 to 1518 Octets	3619
Fragments	0		

Refresh

3.13.12 スイッチクラスタリング

スイッチクラスタリングは 1 つのスイッチを通した中央管理を有効にするため、スイッチをグループ化する機能です。クラスタリングをサポートするスイッチは、それらが同じローカルネットワーク内に接続されている限り、物理的な場所やスイッチの種類に関係なくグループ化することができます。

機能解説

- スイッチクラスタは、クラスタの他のすべてのメンバーを管理するために使用するコマンドユニットを持ちます。管理端末は IP アドレスを通してコマンドと直接通信するために Telnet と Web インタフェースの両方を使用することができます。またコマンドはクラスタの内部 IP アドレスを使用してメンバースイッチを管理します。
- スイッチをクラスタのコマンダーとして構成した直後、コマンダーはネットワーク上のクラスタを有効にしたスイッチを自動的に発見します。発見されたスイッチは Candidate（候補）と呼ばれ、管理端末を通して手動でクラスタのメンバーに設定することができます。
- 1 つのクラスタに最大 100 の候補と 36 個のメンバーを追加することができます。
- スイッチは 1 つのクラスタのメンバーにのみなれます。
- コマンダーとメンバーを構成した後、Web エージェントのメニューからクラスタの ID を選択することで、クラスタに参加したスイッチの管理を行うことができます。

クラスタ設定

Administration > Cluster (Configure Global) ページを使用し、スイッチクラスタを作成します。

機能解説

- 最初に、スイッチ上でクラスタリングが有効（初期設定は無効）になっていることを確認し、その後にスイッチをクラスタコマンドとして設定します。ネットワーク IP サブネットと矛盾しないクラスタ IP プールを設定してください。それらがメンバーになった時、クラスタ IP アドレスはスイッチに割り当てられ、そしてメンバースイッチとコマンド間のコミュニケーションで使用されます。

設定・表示項目

Cluster Status

スイッチクラスタリングの有効 / 無効（初期設定：無効）

Commander Status

スイッチをクラスタコマンダーとして有効 / 無効（初期設定：無効）

IP Pool

クラスタ内のメンバースイッチへの IP アドレス割り当てに使用される “internal” IP アドレスプール。IP アドレスプールの設定がメンバースイッチに割り当てられる IP アドレスとして内部的に使用されます。クラスタの IP アドレスの形式は「10.x.x. メンバースイッチの ID」という構成になります。メンバーに設定する必要がある IP アドレスの数は 1 個から 32 個です。（初期設定：10.254.254.1）

Role

クラスタスイッチの現在の役割を表示

(Commander、Member、Candidate 初期設定：Candidate)

Number of Members

現在のクラスタメンバー数

Number of Candidates

現在、ネットワーク内で検索された候補スイッチ

設定方法

- (1) [Administration] → [Cluster] をクリックします。
- (2) 「Step」 リストから「Configure Global」を選択します。
- (3) 必要な項目を入力し < Apply > をクリックします。

Administration > Cluster

Step: 1. Configure Global ▼

Cluster Status	☒ Enabled
Commander Status	☒ Enabled
IP Pool	10.254.254.1
Role	Candidate
Number of Members	0
Number of Candidates	0

クラスタメンバー設定

候補スイッチをクラスタのメンバースイッチとして追加します。

設定・表示項目

Member ID

選択した候補スイッチにメンバー ID を設定します。(範囲：1-36)

MAC Address

候補テーブルから、スイッチの MAC アドレスを選択します。あるいは、既知のスイッチ MAC アドレスを指定します。

設定方法

クラスタメンバーの設定

- (1) [Administration] → [Cluster] をクリックします。
- (2) 「Step」 リストから「Configure Member」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) 必要な項目を入力し「Apply」をクリックします。

Administration > Cluster

Step: 2. Configure Member Action: Add

Member ID (1-36)

MAC Address ☒ Candidate 11-22-33-44-55-11

☐

Apply Revert

クラスタメンバーの表示

- (1) [Administration] → [Cluster] をクリックします。
- (2) 「Step」 リストから「Configure Member」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Administration > Cluster

Step: 2. Configure Member Action: Show

Cluster Member List Max: 36 Total: 2

☐	Member ID	Role	IP Address	MAC Address	Description
☐	1	Active Member	10.254.254.2	11-22-33-44-55-33	ES3510MA
☐	2	Candidate	10.254.254.3	11-22-33-44-55-77	ES3510MA

Delete Revert

クラスタ候補の表示

- (1) [Administration] → [Cluster] をクリックします。
- (2) 「Step」 リストから「Configure Member」を選択します。
- (3) 「Action」 リストから「Show Candidate」を選択します。

Administration > Cluster

Step: 2. Configure Member Action: Show Candidate

Cluster Candidate List Max: 100 Total: 1

Role	MAC Address	Description
Member To Be	11-22-33-44-55-66	

Clear

クラスタメンバーの管理

Administration > Cluster (Show Member) ページを使用し、クラスタの他スイッチを管理します。

設定・表示項目

Member ID

メンバースイッチの ID 番号（範囲：1-36）

Role

現在のスイッチクラスタステータス

IP Address

メンバースイッチに割り当てられた、内部クラスタ IP アドレス

MAC Address

メンバースイッチの MAC アドレス

Description

メンバースイッチの説明

Operate

クラスタメンバーをリモートで管理

設定方法

クラスタメンバーの管理

- (1) [Administration] → [Cluster] をクリックします。
- (2) 「Step」 リストから「Show Member」を選択します。
- (3) クラスタメンバーリストから表示するメンバーを選択します。
- (4) 「Operate」をクリックします。

Administration > Cluster

Step: 3. Show Member

Cluster Member List Max: 36 Total: 1

	Member ID	Role	IP Address	MAC Address	Description
	1	Member To Be	10.254.254.2	11-22-33-44-55-66	

Operate

3.14 IP 設定

ネットワーク上のスイッチへの管理アクセス用 IP インタフェースの設定について解説します。
本機は IP バージョン 4 および 6 をサポートしており、これらのアドレスタイプのいずれかを通して同時に管理が可能です。

IPv4 または IPv6 アドレスを手動で設定するか、起動時に IPv4 アドレスを BOOTP または DHCP サーバーからダイレクトに取得することが可能です。IPv6 アドレスは手動で設定または動的に生成されることが可能です。

3.14.1 PING

IP > General > Ping ページを使用して、ネットワーク内の他のノードへ ICMP echo リクエストパケットを送信することが出来ます。

設定・表示項目

Type

ターゲットを IP アドレスまたはホスト名で指定

- IP Address —ホストの IP アドレス
- Host —ホストの名前またはエイリアス。host name-to-IP address 変換を適切に機能させるためには、host name lookup (329 ページの「DNS サービスの一般設定」を参照) および、指定された 1 つ以上の DNS サーバ (P331 「ネームサーバリストの設定」または P332 「静的 DNS ホストのアドレスエントリ」を参照) 有効にしてください。

Probe Count

送信するパケットの数 (範囲: 1-16)

Packet Size

パケットのサイズ (範囲: 32-512bytes)

設定方法

- (1) [IP] → [General] → [Ping] をクリックします。
- (2) ターゲットデバイスと PING パラメータを指定します。
- (3) < Apply > をクリックします。

IP > General > Ping

Type: Host (dropdown)

Host Name: 192.168.1.99

Probe Count (1-16): 16

Packet Size (32-512): 512 bytes

Apply Revert

Result

```
PING to 192.168.1.99, by 16 of 512-byte payload ICMP packets, timeout is 3 seconds
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 10 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
```

3.14.2 ARP

Address Resolution Protocol (ARP) は IP アドレスを物理レイヤ (例: MAC) アドレスへマッピングするために使用します。

装置が IP ヘッダを持つパケットを送信または受信した時、最初に MAC アドレスへのディスティネーション IP アドレスを解決する必要があります。

IP フレームがスイッチで受信された時、それは最初に ARP キャッシュのディスティネーション IP アドレスに対応している MAC アドレスを検索します。アドレスが見つかった場合、スイッチはフレームヘッダの適切なフィールドに MAC アドレスを書き込み、ディスティネーション上のフレームに転送します。

IP アドレスが ARP キャッシュに見つからない場合、スイッチは ARP リクエストパケットをネットワーク上の全てのデバイスへブロードキャストします。

ARP リクエストは以下の例のようなフィールドを含みます。

Address Resolution Protocol

destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

装置がリクエストを受信した時、それらのアドレスがメッセージのディスティネーション IP アドレスに一致しない場合は破棄します。しかしながら、もしそれが一致しない場合それらは自身のハードウェアアドレスをディスティネーション MAC アドレスフィールドに書き込みメッセージはソースハードウェアアドレスに戻ります。

ソース装置が返答を受け取った時、それはディスティネーション IP アドレスと関連する MAC アドレスをキャッシュに書き込み、ディスティネーション上に IP トラフィックを転送します。この項目がタイムアウトしない限り、スイッチはこのディスティネーションへ他の ARP リクエストをブロードキャストすることなく、直接トラフィックの転送を行うことが可能です。

同じく、スイッチがそれ自身の IP アドレスのリクエストを受信した場合返答を返し、またソース装置の IP アドレスの MAC をキャッシュします。

ARP タイムアウトの設定

IP > ARP (Configure General) ページを使用し、ARP キャッシュエントリのタイムアウトを指定します。

設定・表示項目

Timeout

ARP キャッシュの動的エントリのエージングタイムを設定（範囲：300-86400 秒）

初期設定：1200 秒）

ARP エージングタイムは全ての VLAN でグローバルにのみ設定可能です。

設定方法

- (1) [IP] → [ARP] をクリックします。
- (2) 「Step」 リストから「Configure General」を選択します。
- (3) タイムアウト値を入力し、< Apply >をクリックします。

IP > ARP

Step: 1. Configure General ▼

Timeout (300-86400) sec

Apply Revert

ARP エントリの表示

IP > ARP (Show Information) ページを使用し、ARP キャッシュの動的またはローカルエントリを表示します。

設定方法

- (1) [IP] → [ARP] をクリックします。
- (2) 「Step」 リストから「Show Information」を選択します。

IP > ARP

Step: 2. Show Information ▼

Dynamic Address List Max: 2304 Total: 1

IP Address	MAC Address	Interface
192.168.1.99	00-0A-E4-33-CD-26	VLAN 1

Clear

3.14.3 IP アドレスの設定 (IP Version4)

ネットワーク経由での管理アクセスを行うために IP アドレスが必要となります。初期設定では、IP アドレスは設定されていません。

手動で IP アドレスの設定を行う際は、使用するネットワークで利用可能な IP アドレスを設定して下さい。(手動設定時の初期設定は、IP アドレス :192.168.1.1、サブネットマスク 255.0.0.0) また、他のネットワークセグメント上の管理用 PC からアクセスする場合にはデフォルトゲートウェイの設定を行う必要があります。

本機では、手動での IP アドレスの設定及び BOOTP 又は DHCP サーバを用いて IP アドレスの取得を行うことができます。

設定・表示項目

Management VLAN

VLAN の ID(1-4093)。初期設定ではすべてのポートが VLAN 1 に所属しています。しかし、IP アドレスを割り当てる VLAN を設定することにより、管理端末を IP アドレスを割り当てた任意のポートに接続することができます。

IP Address Mode

IP アドレスを設定する方法を Static (手動設定)、DHCP、BOOTP から選択します。DHCP 又は BOOTP を選択した場合、サーバからの応答があるまで IP アドレスの取得ができません。IP アドレスを取得するためのサーバへのリクエストは周期的に送信されます (DHCP 又は BOOTP から取得する情報には IP アドレス、サブネットマスク及びデフォルトゲートウェイの情報を含みます)

IP Address

管理アクセスを行うことができる VLAN インタフェースの IP アドレスを設定します。有効な IP アドレスは、0-255 までの十進数 4 桁によって表現され、それぞれピリオドで区切られます (初期設定 : 192.168.1.10)

Subnet Mask

サブネットマスクを設定します。ルーティングに使用されるホストアドレスのビット数の識別に利用されます (初期設定 : 255.255.255.0)

Gateway IP Address

管理端末へのゲートウェイの IP アドレスを設定します。
管理端末が異なったセグメントにある場合には、設定が必要となります
(初期設定 : 0.0.0.0)

MAC Address

本機の MAC アドレスを表示しています。

Restart DHCP

DHCP サーバへ新しい IP アドレスを要求します。

設定方法

IPv4 アドレスを手動で設定

- (1) [System] → [IP] をクリックします。
- (2) 管理 VLAN、IP アドレス、サブネットマスク、ゲートウェイアドレスを入力します。
- (3) < Apply > をクリックします。

The screenshot shows the 'System > IP' configuration page. The 'Management VLAN' is set to 1. The 'IP Address Mode' is set to 'Static'. The 'IP Address' field contains '192.168.1.1', the 'Subnet Mask' is '255.255.255.0', and the 'Gateway IP Address' is '192.168.1.255'. The 'MAC Address' is '00-1A-7E-AB-FD-12'. At the bottom right, there are 'Apply' and 'Revert' buttons.

アドレスを DHCP/BOOTP から自動で取得

- (1) [System] → [IP] をクリックします。
- (2) 管理 VLAN を入力し、IP アドレスモードを "DHCP" または "BOOTP" にします。
- (3) < Apply > をクリックし、設定を保存します。
- (4) 新しいアドレスを要求するため、< Restart DHCP > をクリックします。

The screenshot shows the 'System > IP' configuration page with 'IP Address Mode' set to 'DHCP'. The 'Management VLAN' is 1, 'IP Address' is '192.168.1.1', 'Subnet Mask' is '255.255.255.0', and 'Gateway IP Address' is '192.168.1.255'. The 'MAC Address' remains '00-1A-7E-AB-FD-12'. A 'Restart DHCP' button is visible with a tooltip that says 'Click the button to restart DHCP service.' At the bottom right, there are 'Apply' and 'Revert' buttons.

[注意] 毎電源リセット時、スイッチは IP 設定のリクエストをブロードキャストします。

[注意] 管理接続を失ってしまった場合、スイッチへコンソール接続を行い "show ip interface" で新しいスイッチアドレスを確認してください。

DHCP の更新

DHCP は、永久又は一定期間クライアントに IP アドレスを貸し出します。指定された期間が過ぎた場合や、本機を他のネットワークセグメントへ移動した場合、本機への管理アクセスが行えなくなります。その場合には、本機の再起動を行うか、コンソール経由で IP アドレスの再取得を行うリクエストを送信して下さい。

3.14.4 IP アドレスの設定 (IP Version6)

このセクションでは、ネットワーク経由の管理アクセスのために IPv6 インタフェースの設定を行う方法について解説します。本機は IPv4 と IPv6 の両方をサポートしており、これらのアドレスタイプいずれかで管理されることが可能です。

IPv4 アドレスの設定に関する情報は、P311 「IP アドレスの設定 (IP Version4)」を参照してください。

機能解説

IPv6 は 2 つのアドレスタイプ—リンクローカルユニキャストとグローバルユニキャストを含みます。

リンクローカルアドレスは、同じローカルサブネットに取り付けられた全てのデバイスに、スイッチへの IPv6 のアクセスを可能にします。この種類のアドレスを使用した管理トラフィックはサブネットの外側でルータによって受け渡しされることが出来ません。

リンクローカルアドレスは設定が容易であり、シンプルネットワークや基本的なトラブルシューティングには役立ちますが、複数セグメントから成るより大規模なネットワークに接続するためには、グローバルなユニキャストアドレスを設定する必要があります。

リンクローカルとグローバルユニキャストアドレスタイプの両方は同様に、動的アサインまたは手動で設定することが可能です。

IPv6 デフォルトゲートウェイの設定

Use the IP > IPv6 Configuration (Configure Global) ページを使用し、スイッチの IPv6 デフォルトゲートウェイを設定します。

設定・表示項目

Default Gateway

デフォルトネクストホップルータの IPv6 アドレスを設定します。

- ・管理ステーションが異なる IPv6 セグメントにある場合、IPv6 デフォルトゲートウェイの設定が必要です。
- ・直接ゲートウェイに接続する ネットワークインタフェース がスイッチの上に構成を設定された時のみ IPv6 デフォルトゲートウェイの設定は成功します。

設定方法

- (1) [IP] → [IPv6] をクリックします。
- (2) 「Action」 リストから「Configure Global」を選択します。
- (3) IPv6 デフォルトゲートウェイを入力します。
- (4) [Apply] をクリックします。

IP > IPv6 Configuration

Action: Configure Global

Default Gateway 2001:DB8:2222:7272::254

Apply Revert

IPv6 インタフェース設定

IP > IPv6 Configuration (Configure Interface) ページを使用し、IPv6 一般設定を行うことが出来ます。

機能解説

- スイッチは常にリンクローカルアドレスで設定されなくてはなりません。ルータアドバタイズメントがローカルインタフェースで発見された場合、スイッチのアドレス自動設定機能は、IPv6 グローバルアドレスと同様に自動的にリンクローカルアドレスを作成します。
- IPv6 の明示的有効化を選択することでリンクローカルアドレスも作成されますが、自動設定が有効でない場合、グローバル IPv6 アドレスは生成しません。このケースではアドレスを手動で設定してください。(P317 「IPv6 アドレスの設定」を参照)
- IPv6 近隣探索プロトコルは、IPv6 ネットワークの v4 アドレス解決プロトコルに取って代わります。同じネットワークセグメントの IPv6 ノードは近隣探索をお互いの存在を発見する、お互いのリンクレイヤアドレスを決定する、ルータを発見する為に使います。

設定・表示項目

VLAN

管理アクセス使用に設定された VLAN の ID。デフォルトでは、全てのポートは VLAN1 メンバーですが、管理ステーションは VLAN が IP アドレスにアサインされている限り、どの VLAN に属しているポートにも加入することが可能です。(範囲：1-4093)

Address Autoconfig

インタフェースで IPv6 アドレスの自動設定を有効化、およびインタフェース上で IPv6 機能を有効化します。アドレスのネットワーク部は IPv6 ルータアドバタイズメントメッセージで受け取られたプレフィックスを基にし、ホスト部はインタフェース識別子（スイッチの MAC アドレス）のモディファイド EUI-64 フォームを使用して自動的に生成されます。

- ルータアドバタイズメントが "other stateful configuration" フラグセットを持つ場合、スイッチは他のノンアドレス設定情報を獲得しようと試みます。(デフォルトゲートウェイ等)
- 自動設定が選択されない場合、アドレスは "Add Interface" ページを使用し、手動で設定します。

Enable IPv6 Explicitly

インタフェースで IPv6 を有効にします。インタフェースに明示的なアドレスが割り当てられる時、IPv6 は自動的に有効になり、全ての割り当てられたアドレスが取り除かれるまで無効に出来ません。(初期設定：無効)
このパラメータを無効にしても、IPv6 アドレスで明示的に設定されたインタフェースの IPv6 は無効になりません。

MTU

インタフェースに送られる IPv6 パケットの、Maximum Transmission Unit (MTU) のサイズを設定します。(範囲：1280-65535 bytes 初期設定：1500 bytes)

- IPv6 ルータは他のルータから転送された IPv6 パケットをフラグメントしませんが、IPv6 ルータへ接続されたエンドステーションから源を発するトラフィックはフラグメントします。
- 同じ物理媒体上の全てのデバイスは、正確に稼動するため、同じ MTU を使用しなくてはなりません。
- MTU が設定可能になる前に、IPv6 はインタフェースで有効にしなくてはなりません。IPv6 アドレスがスイッチにアサインされていない場合、MTU フィールドに "N/A" が表示されます。

ND DAD Attempts

重複アドレス検出の間にインタフェースで送られる、連続したネイバー要請メッセージの数
(範囲：0-600 初期設定：1)

- 0 の値を設定することは重複アドレス検出を無効にします。
- サスペンド状態になっているインタフェースでは重複アドレス検出は停止します。(83 ページの「VLAN グループの設定」を参照) インタフェースがサスペンド中、インタフェースに割り当てられた全ての IPv6 ユニキャストアドレスは "pending" になります。インタフェースが管理上再度アクティブになった時、重複アドレス検出は自動的に再開します。
- 再アクティブ化したインタフェースは、全てのユニキャスト IPv6 アドレスで重複アドレス検出を再開します。重複アドレス検出がインタフェースのリンクローカルアドレスで実行されている間、その他の IPv6 アドレスは "tentative" 状態で残っています。もし、重複したリンクローカルアドレスが見つからない場合、重複アドレス検出は残りの IPv6 アドレスに対し実行されます。
- 重複したアドレスが見つかった場合、これは "duplicant (重複)" ステータスにセットされ、コンソールへ警告メッセージが送られます。もし、重複したリンクローカルアドレスが検出された場合、IPv6 プロセスはインタフェースで無効になります。重複したグローバルユニキャストアドレスが検出された場合、それは使用されません。
- インタフェースのリンクローカルアドレスが変更された場合、重複アドレス検出は新しいリンクローカルアドレスで実行されますが、既にインタフェースと関連付けられた IPv6 ユニキャストアドレスには実行しません。

ND NS Interval

インタフェース上での IPv6 近隣要請メッセージ送信間隔

(範囲：1000-3600000 ミリ秒 初期設定：近隣検出オペレーション=1000 ミリ秒

ルータアドバタイズメントのアドバタイズ=0 ミリ秒)

この属性は、アドレス解決または近隣の到達可能性を探る時に、近隣要請メッセージを送信する間隔を指定します。通常の IPv6 オペレーションのために、非常に短い間隔を使用するのは避けてください。

Restart DHCPv6

IP アドレスプレフィックスの DHCPv6 設定は現在のソフトウェアではサポートされていません。ルータアドバタイズメントが "other stateful configuration" フラグセットを持つ場合、スイッチは DHCPv6 サーバから、他のノンアドレス設定情報（デフォルトゲートウェイ等）を獲得しようと試みます。

設定方法

- (1) [IP] → [IPv6 Configuration] をクリックします。
- (2) 「Action」 リストから「Configure Interface」を選択します。
- (3) 必要な項目の設定を行い、[Apply] をクリックします。

IP > IPv6 Configuration

Action: Configure Interface

VLAN

1

Address Autoconfig

☐ Enabled

Enable IPv6 Explicitly

☒ Enabled

MTU (1280-65535)

1280

bytes

ND DAD Attempts (0-600)

3

ND NS Interval (1000-3600000)

1000

ms

Restart DHCPv6

Click the button to restart DHCPv6 service.

Apply

Revert

IPv6 アドレスの設定

IP > IPv6 Configuration (Add IPv6 Address) ページを使用し、ネットワーク上の管理アクセス用 IPv6 インタフェースを設定できます。

機能解説

- 全ての IPv6 アドレスは、RFC2373"IPv6 Addressing Architecture" に従ってフォーマットされなくてはなりません。8 つの 16 ビット 16 進数をコロンで区切った値を使用します。アドレス内の不適格なフィールドを満たす為に必要とされるゼロの適切な数を示すため 1 つのダブルコロンが使用されます。
- スイッチは常にリンクローカルアドレスで設定されます。そのため、IPv6 機能を可能にする設定プロセス、またはグローバルユニキャストアドレスのスイッチへの割り当て、アドレス自動設定または明示的 IPv6 有効化 (P314 「IPv6 インタフェース設定」を参照) は自動的にリンクローカルユニキャストアドレスを生成します。リンクローカルアドレスのプレフィックスの長さは 64 ビットに固定されており、デフォルトアドレスのホスト部はインタフェース識別子 (物理的な MAC アドレス) のモディファイド EUI-64(Extended Universal Identifier) フォームを基にします。代わりにネットワークプレフィックス FE80 でフルアドレスを入力し、リンクローカルアドレスを手動で設定することが可能です。
- 多数のサブネットが存在する大規模なネットワークへ接続するには、グローバルユニキャストアドレスを設定する必要があります。このアドレスタイプの設定にはいくつかの選択肢があります。
 - グローバルユニキャストアドレスは、ローカルなインタフェース上のルータアドレスバタイズメントからネットワークプレフィックスを取ることによって自動的に設定されることが可能です。そして、インタフェース識別子のモディファイド EUI-64 フォームを使用し、アドレスのホスト部を自動的に作成します。(314 ページの「IPv6 インタフェース設定」を参照)
 - 全てのネットワークプレフィックスとプレフィックスの長さを指定することによって、手動で設定することが可能です。そして、インタフェース識別子のモディファイド EUI-64 フォームを使用し、自動でアドレスのホスト部のローオーダー 64 ビットを作成します。
 - フルアドレスとプレフィックスを入力することによって、手動でグローバルユニキャストアドレスを設定することも可能です。
- インタフェースごとに、複数の IPv6 グローバルユニキャストアドレスを設定することが可能ですが、1 つのインタフェースにリンクローカルアドレスは 1 つです。
- ローカルセグメントで、重複するリンクローカルアドレスが検出された場合、インタフェースは無効になり、コンソールに警告メッセージが表示されます。ネットワークで重複グローバルユニキャストアドレスが検出された場合、アドレスはこのインタフェースで無効になり、コンソールに警告メッセージが表示されます。
- 明示的アドレスがインタフェースに割り当てられる時、IPv6 は自動的に有効になり、割り当てられたアドレスが取り除かれるまで無効には出来ません。

設定・表示項目

VLAN

管理アクセス使用に設定された VLAN の ID。デフォルトでは全てのポートは VLAN1 メンバーですが、管理ステーションは VLAN が IP アドレスにアサインされている限り、どの VLAN に属しているポートにも加入することが可能です。(範囲：1-4093)

Address Type

インタフェースで設定されるアドレスタイプを定義。

- Global – フル IPv6 アドレスで IPv6 グローバルユニキャストアドレスを設定
- EUI-64 (Extended Universal Identifier) – ローオーダー 64 ビットの EUI-64 インタフェース ID を使用して、インタフェースの IPv6 アドレスを設定
 - アドレスのホスト部でローオーダー 64 ビットのために EUI-64 フォーマットを使用した時、IPv6 アドレスフィールドに入力された値はアドレスのネットワーク部を含み、プレフィックス長はいくつの連続的なアドレスのビット (左から) がプレフィックスから構成されるかを示します。(アドレスのネットワーク部) 指定されたプレフィックス長が 64 ビットよりも短い場合、IPv6 アドレスフィールドで指定された値がハイオーダーホストビットの若干を含みます。指定されたプレフィックスが 64 ビットを超えている場合、アドレスのネットワーク部で使われたビットはインタフェース識別子より優先されます。
 - IPv6 アドレスの長さは 16 バイトで、最下位 8 バイトが一般に装置の MAC アドレスに基づいてユニークなホスト識別子を形成します。EUI-64 仕様は拡張された 8 バイト MAC アドレスを使用するデバイスのために設計されています。依然 6 バイト MAC アドレス (同じく EUI-48 フォーマットとして知られる) を使用するデバイスのため、それはアドレスのユニバーサル / ローカルビットを反転し、上下の MAC アドレスの 3 バイトの間に 16 進数 FFFE を挿入することによって、EUI-64 フォーマットに変換されなくてはなりません。例えば、もしデバイスが 28-9F-18-1C-82-35 の EUI-48 アドレスを持つ場合、グローバル / ローカルビットは 28 を 2A に変えている EUI-64 必要条件を満たす為、最初に反転されなくてはなりません。そして、2 バイト FFFE が OUI (Organizationally Unique Identifier または Company Identifier) の間に挿入され、残りのアドレスが、2A-9F-18-FF-FE-1C-82-35 のモディファイド EUI-64 インタフェース識別子を結果としてもたらしめます。
 - インタフェースが異なるサブネットに付属する限り、このホストアドレッシングメソッドは、同じインタフェース識別子が 1 つのデバイスの複数の IP インタフェースに使用されることを可能にします。
- Link Local – IPv6 リンクローカルアドレスを設定
 - アドレスプレフィックスは FE80 になります。
 - インタフェースごとに 1 つのリンクローカルアドレスのみ設定できます。
 - 指定されたアドレスをインタフェースで自動的に生成されたリンクローカルアドレスに置き換えられます。

IPv6 Address

このインタフェースに割り当てられた IPv6 アドレス

設定方法

- (1) [IP] → [IPv6 Configuration] をクリックします。
- (2) 「Action」 リストから「Add IPv6 Address」を選択します。
- (3) 設定を行う VLAN を指定し、アドレスタイプを選択します。IPv6 アドレスとプレフィックス長を入力します。
- (4) < Apply >をクリックします。

IP > IPv6 Configuration

Action: Add IPv6 Address ▼

VLAN 1 ▼

Address Type Global ▼

IPv6 Address 2001:DB8:2222:7272:72/96

Apply Revert

IPv6 アドレスの表示

Use the IP > IPv6 Configuration (Show IPv6 Address) ページを使用し、インタフェースに割り当てられた IPv6 アドレスを表示します。

設定・表示項目

VLAN

管理アクセス使用に設定された VLAN の ID。デフォルトでは、全てのポートは VLAN1 メンバーですが、管理ステーションは、VLAN が IP アドレスにアサインされている限り、どの VLAN に属しているポートにも加入することが可能です。(範囲：1-4093)

IP Address Type

IP アドレスタイプ (グローバル、EUI-64、リンクローカル)
インタフェースに割り当てられたユニキャストアドレスに加え、ホストは同じく all-nodes マルチキャストアドレス FF01::1 (interface-local scope) と FF02::1 (link-local scope) を聴取することを要求します。

FF01::1/16 は、IPv6 ノードに付加された全ての非常駐インタフェースローカルマルチキャストアドレスで、FF02::1/16 は、IPv6 ノードに付加された全てのリンクローカルマルチキャストアドレスです。

インタフェースローカルマルチキャストアドレスはマルチキャストトラフィックのループバック転送にのみ使用されます。リンクローカルマルチキャストアドレスはリンクローカルユニキャストアドレスによって使用されるタイプと同じタイプをカバーします。

IPv6 は IPv4 のアドレス解決プロトコルで使用するブロードキャストメソッドをサポートしないため、近隣ノードの MAC アドレスを解決するために solicited-node マルチキャストアドレス (link-local scope FF02) が使用されます。

Configuration Mode

このアドレスが手動設定で、自動的に生成されたか否かを示します。

設定方法

- (1) [IP] → [IPv6 Configuration] をクリックします。
- (2) 「Action」 リストから「Show IPv6 Address」を選択します。
- (3) リストから VLAN を選択します。

IP > IPv6 Configuration

Action: Show IPv6 Address

VLAN 1

IPv6 Address List Max: 10 Total: 2

☐	IP Address Type	IP Address	Configuration Mode
☐	Global	2001:DB8:2222:7272::96	Manual
☐	Link Local	FE80::212:CFFF:FEF3:DE46%1/64	Auto

Apply Revert

IPv6 近隣キャッシュの表示

IP > IPv6 Configuration (Show IPv6 Neighbor Cache) を使用し、ネイバーデバイスに発見された IPv6 アドレスを表示します。

設定・表示項目

IPv6 近隣の表示

フィールド	解説
IPv6 Address	近隣の IPv6 アドレス
Age	アドレスが到達可能として実証されてからの時間（秒）静的エントリは "Permanent" と示されます。
Link-layer Addr	物理層 MAC アドレス
State	近隣のキャッシュエントリの状態を指定します。IPv6 近隣検出キャッシュ内の動的エントリの状態は、以下のとおりです。 ♦INCMP (Incomplete) — エントリ上でアドレス解決が実行中です。近隣要請メッセージが、ターゲットの要請されたマルチキャストアドレスに送信されましたが、対応する近隣アドバタイズメントメッセージがまだ受信されていません。 ♦REACH (到達可能) — 近隣への転送パスが正常に機能していることを示す確認メッセージ（正常）が、最後の Reachable Time（到達可能な時間）（ミリ秒）内に受信されました。REACH（到達）状態の間は、デバイスはパケットの送信中に特別な動作をしません。 ♦STALE — 転送パスが正常に機能していることを示す最後の確認メッセージ（正常）が受信されてから、ReachableTime（到達可能な時間）（ミリ秒）を超える時間が経過しました。STALE（期限切れ）状態の間は、デバイスはパケットが送信されるまで特別な動作をしません ♦DELAY — 転送パスが正常に機能していることを示す最後の確認メッセージ（正常）が受信されてから、ReachableTime（到達可能な時間）（ミリ秒）を超える時間が経過しました。前回の DELAY_FIRST_PROBE_TIME 秒内にパケットが送信されました。DELAY（遅延）状態に入ってから DELAY_FIRST_PROBE_TIME 秒内に到達可能性確認が受信されない場合は、近隣要求メッセージを送信し、状態を PROBE（調査）に変えます。 ♦PROBE — 到達可能性確認が受信されるまで、近隣要請メッセージを RetransTimer ミリ秒間隔で再送信することで、到達可能性確認がアクティブに求められます。 ♦UNKNO — 未知の状態 以下の状態は静的エントリに使用されます。 ♦INCMP (Incomplete) ♦REACH (Reachable)
VLAN	到達したアドレスの VLAN インタフェース

設定方法

- (1) [IP] → [IPv6 Configuration] をクリックします。
- (2) 「Action」 リストから「Show IPv6 Neighbor Cache」を選択します。

IP > IPv6

Action: Show IPv6 Neighbor Cache

Current Neighbor Cache Table Max: 10 Total: 2

IPv6 Address	Age	Link-layer Address	State	VLAN
2001::2001	0	00-00-00-00-00-01	Stale	2
2001::2001	0	00-00-00-00-00-02	Stale	2

Clear

IPv6 統計の表示

IP > IPv6 Configuration (Show Statistics) を使用し、このスイッチを経過している IPv6 トラフィックの統計を表示することが出来ます。

機能解説

- **IPv6** –バージョン 6 アドレスのインターネットプロトコルは、ソースからディスタネーションへのデータの送信ブロックメカニズムを提供します。そして、そこでこれらのネットワーク装置は固定長アドレスによって識別されます。インターネットプロトコルはまた、必要な場合に "small packet" ネットワークを通しての伝送のため、ロングパケットのフラグメントと再アセンブリを提供します。
- **ICMPv6** –バージョン 6 の Internet Control Message Protocol は、IPv6 パケット処理エラーをレポートするためのメッセージパケットを転送するネットワークレイヤプロトコルです。ICMP はインターネットプロトコルにとって、不可欠な部分です。ICMP メッセージは、データグラム未到達、ゲートウェイがデータグラム転送を行うバッファリング容量を持たない時など、様々な状態のレポートに使用されます。ICMP はまた、特定の目的地に使うより適切なルート（ネクストホップルータ）についての情報をフィードバックするためにも使用されます。
- **UDP** – User Datagram Protocol はパケット交換通信のデータグラムモードを提供します。基礎をなすトランスポートメカニズムとして IP を使用し、IP のようなサービスへのアクセスを提供します。UDP パケットは IP パケットと全く同じように届けられます。TCP が複雑すぎる、遅すぎる、または不要の場合、UDP は有要です。

設定・表示項目

IPv6 統計の表示

フィールド	解説
IPv6 統計	
IPv6 受信	
Total	エラーで受信したものも含め、インタフェースで受信した入力データグラムの総数。
Header Errors	IPv6 ヘッダのエラーが原因で破棄された入力データグラムの数。バージョン番号の不一致、その他のフォーマットエラー、ホップ数の許容値超過、IPv6 オプションの処理で検出されたエラーなどが含まれます。
Too Big Errors	サイズが送信インタフェースのリンク MTU を超えたために転送できなかった受信データグラムの数。
No Routes	送信先に送信するためのルートが検出されなかったために破棄された入力データグラムの数。
Address Errors	IPv6 ヘッダの送信先フィールド内の IPv6 アドレスがこのエンティティで受信できる有効なアドレスでなかったために破棄された入力データグラムの数。このカウントには、無効なアドレス (::0 など) およびサポートされていないアドレス（未割り当てのプレフィックスを持つアドレスなど）も含まれます。IPv6 ルーターではなく、そのためにデータグラムを転送しないエンティティについては、このカウンタの値には破棄されたデータグラムの数も含まれます。送信先アドレスがローカルアドレスではなかったからです。

IPv6 統計の表示

Unknown Protocols	正常に受信したものの、プロトコルが不明であるか、サポートされていないことが原因で破棄されたローカルアドレス指定のデータグラムの数。このカウンタは、これらのデータグラムの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のデータグラムにとっては必ずしも入力インタフェースではない場合もあります。
Truncated Packets	データグラムフレームのデータ量が足りなかったために破棄された入力データグラムの数。
Discards	処理の継続を妨げるような問題が発生していないにもかかわらず（バッファ領域の不足などの理由で）破棄された入力 IPv6 データグラムの数。このカウンタの値には、再構成の待機中に破棄されたデータグラムの数は含まれません。
Delivers	IPv6 ユーザープロトコルに正常に送信されたデータグラムの総数（ICMP を含む）。このカウンタは、これらのデータグラムの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のデータグラムにとっては必ずしも入力インタフェースではない場合もあります。
Reassembly Request Datagrams	このインタフェースで再構成される必要がある、受信した IPv6 フラグメントの数。このカウンタは、これらのフラグメントの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のフラグメントにとっては必ずしも入力インタフェースではない場合もあります。
Reassembled Succeeded	正常に再構成された IPv6 データグラムの数。このカウンタは、これらのデータグラムの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のフラグメントにとっては必ずしも入力インタフェースではない場合もあります。
Reassembled Failed	IPv6 再構成アルゴリズムによって検出されたエラーの数（タイムアウトなど、エラーの種類は問いません）。アルゴリズムによっては（特に RFC 815 内のアルゴリズム）フラグメントを受信時に結合してしまい、その数を追跡できないため、この値は必ずしも破棄された IPv6 フラグメントの数であるとは限りません。このカウンタは、これらのフラグメントの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のフラグメントにとっては必ずしも入力インタフェースではない場合もあります。
IPv6 送信	
Forwards Datagrams	このエンティティが受信し、最終送信先に転送した出力データグラムの数。IPv6 ルーターとして動作しないエンティティでは、このカウンタの値には、このエンティティを介して Source-Route（送信元ルート指定）され、Source-Route が適切に処理されたパケットの数のみが含まれます。正常に転送されたデータグラムの場合は、出力インタフェースのカウンタがインクリメントされます。
Requests	ローカル IPv6 ユーザープロトコル（ICMP を含む）がトランスミッションの要請で IPv6 に供給した pv6 データグラムの総数 "ipv6IfStatsOutForwDatagrams" でカウントされるデータグラムはこのカウンタに含まれません。
Discards	処理の継続を妨げるような問題が発生していないにもかかわらず（バッファ領域の不足などの理由で）破棄された入力 IPv6 データグラムの数。
No Routes	送信先に送信するためのルートが検出されなかったために破棄された入力データグラムの数。
Generated Fragments	この出力インタフェースで行われたフラグメント化によって生成された出力データグラムフラグメントの数。
Fragment Succeeded	この出力インタフェースで正常にフラグメント化された IPv6 データグラムの数。
Fragment Failed	このインタフェースでフラグメント化できなかった出力データグラムの数。
ICMPv6 統計	

IPv6 統計の表示

ICMPv6 受信	
Input	インタフェースで受信した ICMP メッセージの総数。ipv6IcmpInErrors によってカウントされたメッセージがすべて含まれます。このインタフェースは、ICMP メッセージの宛先とされたインタフェースであり、必ずしもメッセージにとっての入力インタフェースではない可能性があります。
Errors	インタフェースで受信したものの ICMP 特有のエラー（無効な ICMP チェックサム、無効なメッセージ長など）があると判断された ICMP メッセージの総数。
Destination Unreachable Messages	インタフェースで受信した ICMP 送信先到達不能メッセージの数。
Packet Too Big Messages	インタフェースで受信した "ICMP Packet Too Big"（ICMP パケットが大きすぎます）メッセージの数。
Time Exceeded Messages	インタフェースで受信した ICMP 時間超過メッセージの数。
Parameter Problem Messages	インタフェースで受信した ICMP パラメータ問題メッセージの数。
Echo Request Messages	インタフェースで受信した ICMP エコー（要求）メッセージの数。
Echo Reply Messages	インタフェースで受信した ICMP エコー応答メッセージの数。
Redirect Messages	インタフェースで受信したリダイレクトメッセージの数。
Group Membership Query Messages	インタフェースで受信した ICMPv6 グループメンバーシップクエリーメッセージの数。
Group Membership Response Messages	インタフェースで受信した ICMPv6 グループメンバーシップ応答メッセージの数。
Group Membership Reduction Messages	インタフェースで受信した ICMPv6 グループメンバーシップ取り消しメッセージの数。
Router Solicit Messages	インタフェースで受信した ICMP ルーター要請メッセージの数。
Router Advertisement Messages	インタフェースで受信した ICMP ルーターアドバタイズメントメッセージの数。
Neighbor Solicit Messages	インタフェースで受信した ICMP 近隣要請メッセージの数。
Neighbor Advertisement Messages	インタフェースで受信した ICMP 近隣アドバタイズメントメッセージの数。
Redirect Messages	インタフェースで受信した ICMPv6 リダイレクトメッセージの数。
ICMPv6 送信	
Output	このインタフェースが送信を試みた ICMP メッセージの総数。このカウンタ値には、icmpOutErrors によってカウントされる数が含まれます。
Destination Unreachable Messages	インタフェースで送信された ICMP 送信先到達不能メッセージの数。

IPv6 統計の表示

Packet Too Big Messages	インタフェースで送信された "ICMP Packet Too Big" (ICMP パケットが大きすぎます) メッセージの数。
Time Exceeded Messages	インタフェースで送信された ICMP 時間超過メッセージの数。
Parameter Problem Message	インタフェースで送信された ICMP パラメータ問題メッセージの数。
Echo Reply Messages	インタフェースで送信された ICMP エコー応答メッセージの数。
Router Solicit Messages	インタフェースで送信された ICMP ルーター要請メッセージの数。
Neighbor Advertisement Messages	インタフェースで送信された ICMP 近隣アドバタイズメントメッセージの数。
Redirect Messages	送信されたリダイレクトメッセージの数。
Group Membership Response Messages	送信された ICMPv6 グループメンバーシップ応答メッセージの数。
Group Membership Reduction Messages	送信された ICMPv6 グループメンバーシップ取り消しメッセージの数。
UDP 統計	
Input	UDP ユーザに送信された UDP データグラムの総数。
No Port Errors	受信された目的地ポートにアプリケーションが無かったデータグラムの総数。
Other Errors	目的地ポートで、アプリケーションの欠如以外の理由で送信されることが出来なかった受信 UDP データグラムの数。
Output	このエンティティから送信された UDP データグラムの総数。

設定方法

- (1) [IP] → [IPv6 Configuration] をクリックします。
- (2) 「Action」 リストから「Show Statistics」を選択します。
- (3) 「IPv6」、「ICMPv6」、「UDP」 をクリックします。

(IPv6)

IP > IPv6 Configuration

Action: Show Statistics

Type ☒ IPv6 ☐ ICMPv6 ☐ UDP

IPv6 Statistics

Total Received	0	Received Reassembled Succeeded	0
Received Header Errors	0	Received Reassembled Failed	0
Received Too Big Errors	0	Transmitted Forwards Datagrams	0
Received No Routes	0	Transmitted Requests	7
Received Address Errors	0	Transmitted Discards	0
Received Unknown Protocols	0	Transmitted No Routes	0
Received Truncated Packets	0	Transmitted Generated Fragments	0
Received Discards	0	Transmitted Fragment Succeeded	0
Received Delivers	0	Transmitted Fragment Failed	0
Received Reassembly Request Datarams	0		

Clear

(ICMPv6)

IP > IPv6 Configuration

Action: Show Statistics

Type ☐ IPv6 ☒ ICMPv6 ☐ UDP

ICMPv6 Statistics

Received Input	0	Received Neighbor Advertisement Messages	0
Received Errors	0	Received Redirect Messages	0
Received Destination Unreachable Messages	0	Transmitted Output	7
Received Packet Too Big Messages	0	Transmitted Destination Unreachable Messages	0
Received Time Exceeded Messages	0	Transmitted Packet Too Big Messages	0
Received Parameter Problem Messages	0	Transmitted Time Exceeded Messages	0
Received Echo Request Messages	0	Transmitted Parameter Problem Message	0
Received Echo Reply Messages	0	Transmitted Echo Reply Messages	0
Received Redirect Messages	0	Transmitted Router Solicit Messages	3
Received Group Membership Query Messages	0	Transmitted Neighbor Solicit Messages	4
Received Group Membership Response Messages	0	Transmitted Neighbor Advertisement Messages	0
Received Group Membership Reduction			

(UDP)

IP > IPv6 Configuration

Action: Show Statistics

Type

☐ IPv6

☐ ICMPv6

☒ UDP

UDP Statistics

Input

0

No Port Errors

0

Other Errors

0

Output

0

Clear

応答側ディスティネーションの MTU を表示

IP > IPv6 Configuration (Show MTU) ページを使用し、maximum transmission unit (MTU) キャッシュを表示します。

設定・表示項目

MTU の表示

フィールド	解説
MTU	この目的地から返させる ICMP "packet-too-big" メッセージに含まれる、調整された MTU
Since	ICMP "packet-too-big" メッセージがこの目的地から受信されてからの時間
Destination Address	ICMP "packet-too-big" メッセージが送られたアドレス

設定方法

- (1) [IP] → [IPv6 Configuration] をクリックします。
- (2) 「Action」 リストから「Show MTU」を選択します。

IP > IPv6 Configuration

Action: Show MTU

MTU Table Max: 10 Total: 1

MTU	Since	Destination Address
1280	1181116:13:22	2001:DB8:2222:7272:72::

3.15 IP サービス

本機の Domain Name Service (DNS) の設定について解説します。

このフォルダに含まれる DHCP スヌーピングに関する情報は 245 ページの「DHCP スヌーピング」を参照してください。

本機の DNS サービスは、静的なテーブルエントリを使用するか、ネットワーク上のその他のネームサーバーへのリダイレクションによって、ホスト名を IP アドレスにマップすることを可能にします。

クライアント装置が本機を DNS サーバーとして指名した時、クライアントはスイッチに DNS クエリを転送し、返答を待つことによって、IP アドレスの中にホスト名解決を試みます。

ドメイン名の IP アドレスへのマッピングを使用し、ドメイン名からアドレスへの変換に使用される初期ドメイン名または 1 つ以上のネームサーバーを指定することによって、DNS テーブル内の項目は手動で設定することが可能です。

3.15.1 DNS (Domain Name Service)

本機の DNS(Domain Naming System) サービスは、ドメイン名と IP アドレスのマッピングを行なう DNS テーブルの手動での設定を行なえる他、デフォルトドメイン名の設定又はアドレス変換を行なうための複数のネームサーバの指定を行なうことができます。

DNS サービスの一般設定

IP Service > DNS - General (Configure Global) ページを使用し、ドメインルックアップの有効化およびデフォルトドメイン名の設定を行います。

機能解説

- ・ スイッチで DNS サービスを有効にするため、まず最初に一つ以上のネームサーバーを設定後、ドメインルックアップステータスを有効にします。

設定・表示項目

Domain Lookup

DNS ホスト名・アドレス変換を有効にします。(初期設定：無効)

Default Domain Name

不完全なホスト名に付加するデフォルトドメイン名を指定します。(範囲：1-127 文字)

設定方法

- (1) [IP Service] → [DNS] をクリックします。
- (2) 「Action」 リストから「Configure Global」を選択します。
- (3) ドメインルックアップを有効にし、デフォルトドメイン名を設定します。
- (4) < Apply > をクリックします。

IP Service > DNS > General

Action: Configure Global

Domain Lookup ☒ Enabled

Default Domain Name

Apply Revert

ドメインネームリストの設定

IP Service > DNS - General (Add Domain Name) ページを使用し、ドメインネームのリストを設定できます。

機能解説

- DNS クライアントから受信した不完全なホスト名に付加するデフォルトドメイン名またはドメインネームリストを指定することが可能です。
- ドメインリストが存在しない場合、デフォルトドメイン名が使われます。ドメインリストが存在する場合はデフォルトドメイン名は使用されません。
- 本機の DNS サーバが不完全なホスト名を受信し、ドメイン名リストが指定された場合、本機は追加するリスト内の各ドメイン名をホスト名に加え、一致する特定のネームサーバを確認して、ドメインリストにより動作します。

設定・表示項目

Domain Name

ホスト名。(範囲：1-68 文字)

設定方法

ドメインネームリストの作成

- (1) [IP Service] → [DNS] をクリックします。
- (2) 「Action」 リストから「Add Domain Name」を選択します。
- (3) 1 度に 1 つのドメインネームを入力してください。
- (4) < Apply > をクリックします。

IP Service > DNS > General

Action: Add Domain Name

Domain Name: sample.com.jp

Apply Revert

ドメインネームリストの表示

- (1) [IP Service] → [DNS] をクリックします。
- (2) 「Action」 リストから「Show Domain Names」を選択します。

IP Service > DNS > General

Action: Show Domain Names

Domain Name List Max: 3 Total: 2

	Domain Name
☐	sample.com.uk
☐	sample.com.jp

Delete Revert

ネームサーバリストの設定

IP Service > DNS - General (Add Name Server) ページを使用し、ネームサーバのリストを設定出来ます。

機能解説

- スイッチで DNS サービスを有効にするため、まず最初に一つ以上のネームサーバを設定後、ドメインルックアップステータスを有効にします。
- 一つ以上のサーバが指定されている時、サーバは応答を受信するまで、又はリストの最後に到達するまで、にリクエストを送信し続けます。
- ネームサーバが削除された場合、DNS 機能は自動で無効になります。

設定・表示項目

Name Server IP Address

name-to-address 解決の為に使用される、ドメインネームサーバのアドレスを指定します。ネームサーバリストには、最大 6 つの IP アドレスを追加することが出来ます。

設定方法

ネームサーバリストの作成

- (1) [IP Service] → [DNS] をクリックします。
- (2) 「Action」 リストから「Add Name Server」を選択します。
- (3) 1 度に 1 つのネームサーバを入力してください。
- (4) < Apply > をクリックします。

IP Service > DNS > General

Action: Add Name Server

Name Server IP Address: 192.168.1.10

Apply Revert

ネームサーバリストの表示

- (1) [IP Service] → [DNS] をクリックします。
- (2) 「Action」 リストから「Show Name Servers」を選択します。

IP Service > DNS > General

Action: Show Name Servers

Name Server IP Address List Max: 6 Total: 1

	Name Server IP Address
☐	192.168.1.10

Delete Revert

静的 DNS ホストのアドレスエントリ

DNS テーブルのホスト名と IP アドレスのマッピングの静的設定を行ないます。

機能解説

- サーバや他のネットワーク機器は複数の IP アドレスによる複数接続をサポートしています。2 つ以上の IP アドレスを静的テーブルやネームサーバからの応答によりホスト名と関連付けする場合、DNS クライアントは接続が確立するまで各アドレスに接続を試みます。

設定・表示項目

Host Name

ホスト名（設定範囲：1-127 文字）

IP Address

ホスト名に関連付けられるインターネットアドレス

設定方法

DNS テーブルの静的エントリを設定

- [IP Service] → [DNS] → [Static Host Table] をクリックします。
- 「Action」 リストから「Add」を選択します。
- ホスト名と対応するアドレスを入力します。
- < Apply >をクリックします。

IP Service > DNS > Static Host Table

Action: Add

Host Name: yahoo.com

IP Address: 10.2.7.3

Apply Revert

DNS テーブルの静的エントリを表示

- [IP Service] → [DNS] → [Static Host Table] をクリックします。
- 「Action」 リストから「Show」を選択します。

IP Service > DNS > Static Host Table

Action: Show

IP Address List Max: 16 Total: 1

	Host Name	IP Address
☐	sample.com	10.2.7.3

Delete Revert

DNS キャッシュの表示

DNS キャッシュの内容を表示します。

機能解説

- ・ サーバーまたはその他のネットワーク装置は、一つ以上の複数 IP アドレス経由の接続をサポートしています。
1 つ以上の IP アドレスが、ネームサーバーから戻ってきた情報によってホスト名に関連付けられている場合、DNS クライントは、ターゲット装置との接続が確立するまで、それぞれのアドレスを連続して試みる事が可能です。

設定・表示項目

No

各リソースレコードのエントリ番号

Flag

キャッシュエントリのフラグは常に "4"

Type

標準的又はプライマリ名が指定された「CNAME」、既存のエントリと同じ IP アドレスをマッピングされている多数のドメイン名が指定された「ALIAS」

IP

レコードに関連した IP アドレス

TTL

ネームサーバにより報告された生存可能時間

Domain

レコードに関連するドメイン名

設定方法

(1) [IP Service] → [DNS] → [Cache] をクリックします。

IP Service > DNS > Cache					
Cache Information Max: 2560 Total: 3					
No.	Flag	Type	IP	TTL	Domain
1	4	CNAME	192.168.110.2	360	www.sina.com.cn
2	4	CNAME	10.2.44.3	892	www.yahoo.akadns.new
3	4	ALIAS	pointer to: 2	298	www.yahoo.com
Clear					

3.16 マルチキャストフィルタリング

マルチキャストはビデオカンファレンスやストリーミングなどのリアルタイムアプリケーションの動作をサポートします。マルチキャストサーバは各クライアントに対し異なるコネクションを確立することができません。ネットワークにブロードキャストを行うサービスとなり、マルチキャストを必要とするホストは接続されているマルチキャストサーバ / ルータと共に登録されます。また、この方法はマルチキャストサーバによりネットワークのオーバーヘッドを削減します。ブロードキャストトラフィックは各マルチキャストスイッチ / ルータによって本サービスに加入しているホストにのみ転送されるよう処理されます。

本機では接続されるホストがマルチキャストサービスを必要とするか IGMP (Internet Group Management Protocol) のクエリを使用します。サービスに参加を要求しているホストを含むポートを特定し、そのポートにのみデータを送ります。また、マルチキャストサービスを受信しつづけるためにサービスリクエストを隣接するマルチキャストスイッチ / ルータに広めます。この機能をマルチキャストフィルタリングと呼びます。

IP マルチキャストフィルタリングの目的は、スイッチのネットワークパフォーマンスを最適化し、マルチキャストパケットをマルチキャストグループホスト又はマルチキャストルータ / スwitchに接続されたポートのみに転送し、サブネット内の全てのポートにフラディングするのを防ぎます。

3.16.1 レイヤ 2 IGMP (Snooping and Query)

IGMP Snooping and Query – マルチキャストルーティングがネットワーク上の他の機器でサポートされていない場合、IGMP Snooping 及び Query を利用し、マルチキャストクライアントとサーバ間での IGMP サービスリクエストの通過を監視し、動的にマルチキャストトラフィックを転送するポートの設定を行なうことができます。

IGMPv3 スヌーピングを使用時、IGMP バージョン 1,2,3 ホストからのサービスリクエストは全て IGMPv3 レポートとして、上流のルータへ転送されます。

IGMPv3 スヌーピングによって提供される主な拡張は、下流の IGMPv3 ホストが要求または拒絶した特定のマルチキャストソースに関する情報の記録・追跡です。IGMPv3 ホストのみ特定のマルチキャストソースからサービスを要求出来ます。下流のホストが特定のマルチキャストサービスのソースからサービスを要求した時、これらのソースは全て Include リストに置かれ、トラフィックはこれらのソースのそれぞれからホストへ転送されます。

IGMPv3 ホストはまた、指定以外の全てのソースからのサービス転送の要求も行います。この場合、トラフィックは Exclude リストのソースからフィルタされ、その他全ての使用可能なソースから転送されます。

[注意] スイッチが IGMPv3 スヌーピングを使用するよう設定されている時、それぞれの VLAN で検索された IGMP クエリパケットのバージョンに依存し、スヌーピングバージョンはバージョン 2 または 1 にダウングレードされます。

[注意] スイッチ上のマルチキャストルータポートが有効にならない限り、IGMP スヌーピングは機能しません。これは 2 つの内 1 つで達成が可能です。静的ルータポートは手動で設定が可能です。(338 ページの「マルチキャストルータの静的インタフェースを設定」を参照) このメソッドを使用し、ルータポートはタイムアウトをせず、明示的に削除されるまで機能し続けます。

スイッチに頼るもう 1 つのメソッドは、マルチキャストルーティングプロトコルパケットまたは IGMP クエリパケットがポートで検出された時、マルチキャストルーティングポートを動的に作成します。

静的 IGMP ルータインタフェース— IGMP Snooping が IGMP クエリアを検索できない場合、手動で IGMP クエリア（マルチキャストルータ / スイッチ）に接続された本機のインタフェースの指定を行なうことができます。その後、指定したインタフェースは接続されたルータ / スイッチのすべてのマルチキャストグループに参加し、マルチキャストトラフィックは本機内の適切なインタフェースに転送されます。

静的 IGMP ホストインタフェース— 確実にコントロールする必要のあるマルチキャストアプリケーションに対しては、特定のポートに対して手動でマルチキャストサービスを指定することができます。（P340 参照）

IGMP スヌーピングとプロキシレポーティング— 本機は Last Leave クエリサプレッション（DSL Forum TR-101, April 2006 で定義されている）をサポートしています。

◆ Last Leave : IGMP ホストから来る IGMP Leave をインターセプト・併合し、要約します。IGMP Leave は必要な時だけ（最後のユーザがマルチキャストグループから去る時）アップストリームに中継されます。

◆ Query Suppression : IGMP に指定されたクエリが、クライアントポートへ送信されない方法で IGMP クエリをインターセプトし、処理します。

IGMP Snooping とクエリパラメータの設定

マルチキャストトラフィックの転送設定を行います。
IGMP クエリ及びリポートメッセージに基づき、マルチキャストトラフィックを必要とするポートにのみ通信します。すべてのポートに通信をブロードキャストし、ネットワークパフォーマンスの低下を招くことを防ぎます。

機能解説

- IGMP Snooping — 本機は、IGMP クエリの snoop を受け、リポートパケットを IP マルチキャストルータ / スイッチ間で転送し、IP マルチキャストホストグループを IP マルチキャストグループメンバーに設定します。IGMP パケットの通過を監視し、グループ登録情報を検知し、それに従ってマルチキャストフィルタの設定を行います。

[注意] 最初に受信が行われる際、数秒の間未知のマルチキャストトラフィックが VLAN 内の全てのポートにフラッディングされます。
マルチキャストルータポートが VLAN に存在している場合、IGMP スヌーピングを受けさせることで、トラフィックはフィルタされます。
ルータポートが VLAN に存在しない、またはマルチキャストフィルタリングテーブルが既に一杯の場合、スイッチは、トラフィックを VLAN 内へフラッディングし続けます。

- IGMP Querier — ルータ又はマルチキャスト対応スイッチは、定期的にホストに対しマルチキャストトラフィックが必要かどうかを質問します。もしその LAN 上に 2 つ以上の IP マルチキャストルータ / スイッチが存在した場合、1 つのデバイスが "クエリア" となります。その後、マルチキャストサービスを受け続けるために接続されたマルチキャストスイッチ / ルータに対しサービスリクエストを広げます。

[注意] マルチキャストルータはこれらの情報を、DVMRP や PIM などのマルチキャストルーティングプロトコルと共に、インターネットの IP マルチキャストをサポートするために使用します。

設定・表示項目

IGMP Snooping Status

有効時、スイッチはネットワークトラフィックをモニタし、どのホストがマルチキャストトラフィックを望んでいるかを決定します。(初期設定：無効)

IGMP スヌーピングがグローバルで有効の時、IGMP スヌーピングの VLAN インタフェースごとの設定が優先されます。(P342 「インタフェース毎の IGMP Snooping 設定」を参照)

IGMP スヌーピングがグローバルで無効の時、VLAN ごとのスヌーピングの設定は依然行えますが、インタフェース設定はスヌーピングがグローバルで再度有効になるまで効力を発しません。

Proxy Reporting Status

プロキシレポーティングを有効にします。(初期設定：無効)

このコマンドでプロキシレポーティングが有効になっている時、スイッチは Last Leave、Query Suppression を含む、"IGMP Snooping with Proxy Reporting" (DSL Forum TR-101, April 2006 で定義) を実行します。

TCN Flood

スパニングツリートポロジ変更通知 (TCN) が生じた際、マルチキャストトラフィックのフラディングを有効にします。(初期設定：無効)

TCN Query Solicit

スパニングツリートポロジ変更通知 (TCN) が生じた際、GMP 通常クエリ要請を送信します。(初期設定：無効)

Router Alert Option

ルータアラートオプションを含まない、全ての IGMPv2/v3 パケットを破棄します。(初期設定：無効)

Unregistered Data Flooding

付属した VLAN へ未登録のマルチキャストトラフィックをフラッドします。(初期設定：無効)

Version Exclusive

IGMP バージョン属性によって設定された現在のバージョンと異なるバージョンを使用している、受信した IGMP メッセージを破棄します。

IGMP Unsolicited Report Interval

アップストリームインタフェースが、プロキシレポーティング有効時に非要請 IGMP レポートを送信する間隔を指定 (範囲：1-65535 秒 初期設定：400 秒)

Router Port Expire Time

期限が切れる前にクエリアが止まった後、スイッチが待つ時間 (範囲：1-65535、推奨範囲：30-500 秒、初期設定：300)

IGMP Snooping Version

ネットワーク上の他のデバイスと互換するため、プロトコルバージョンを設定します。これはスイッチがスヌーピングレポートを送信するために使用する IGMP バージョンです。(範囲：1-3 初期設定：2)

Querier Status

有効時、スイッチはホストにマルチキャストトラフィックを受け取ることを望むか訪ねる責任を持つクエリアとして動作します。この機能は IGMPv3 snooping ではサポートされていません (初期設定：無効)

設定方法

DNS テーブルの静的エントリを設定

- (1) [Multicast] → [IGMP Snooping] → [General] をクリックします。
- (2) 必要に応じ、IGMP 設定の調整を行います。
- (3) < Apply > をクリックします。

Multicast > IGMP Snooping > General

IGMP Snooping Status	☒ Enabled
Proxy Reporting Status	☒ Enabled
TCN Flood	☐ Enabled
TCN Query Solicit	☐ Enabled
Router Alert Option	☐ Enabled
Unregistered Data Flooding	☐ Enabled
Version Exclusive	☐ Enabled
IGMP Unsolicited Report Interval (1-65535)	400 seconds
Router Port Expire Time (1-65535)	300 seconds
IGMP Snooping Version (1-3)	2
Querier Status	☐ Enabled

マルチキャストルータの静的インタフェースを設定

ネットワーク接続状況により、IGMP snooping による IGMP クエリアが配置されない場合があります。IGMP クエリアとなるマルチキャストルータ / スイッチが接続されているインタフェース（ポート又はトランク）が判明している場合、ルータがサポートするマルチキャストグループへのインタフェース（及び VLAN）の参加設定を手動で行えます。これにより、本機のすべての適切なインタフェースへマルチキャストトラフィックが渡すことができます。

設定・表示項目

VLAN

マルチキャストルータ / スイッチから送られるマルチキャストトラフィックを受信し、転送する VLAN を選択します。(1-4093)

Interface

ポートまたはトランクをスクロールダウンリストから選択します。

Port/Trunk

マルチキャストルータに接続されたインタフェースを指定します。

設定方法

マルチキャストルータの静的インタフェースを設定

- (1) [Multicast] → [IGMP Snooping] → [Multicast Router] をクリックします。
- (2) 「Action」 リストから「Add Static Multicast Router」を選択します。
- (3) 必要な項目を設定し、< Apply >をクリックします。

Multicast > IGMP Snooping > Multicast Router

Action: Add Static Multicast Router ▼

VLAN: 1 ▼

Interface: ☒ Port 1 ▼ ☐ Trunk ▼

Apply Revert

マルチキャストルータに接続された静的インタフェースを表示

- (1) [Multicast] → [IGMP Snooping] → [Multicast Router] をクリックします。
- (2) 「Action」 リストから「Show Static Multicast Router」を選択します。
- (3) 情報を表示する VLAN を選択します。

Multicast > IGMP Snooping > Multicast Router

Action: Show Static Multicast Router ▼

VLAN: 1 ▼

Static Multicast Router Interface List Max: 32 Total: 1

	Interface
☐	Unit 1 / Port 1

Delete Revert

マルチキャストルータに接続された全てのインタフェースを表示

- (1) [Multicast] → [IGMP Snooping] → [Multicast Router] をクリックします。
- (2) 「Action」 リストから「Current Multicast Router」を選択します。
- (3) 情報を表示する VLAN を選択します。

Multicast > IGMP Snooping > Multicast Router

Action: Show Current Multicast Router ▼

VLAN: 1 ▼

Multicast Router Interface Information Max: 32 Total: 1

Interface	Type
Unit 1 / Port 1	Static

マルチキャストサービスヘインタフェースをアサイン

マルチキャストフィルタリングは、P335 「IGMP Snooping とクエリパラメータの設定」の通り、IGMP snooping と IGMP クエリメッセージを使用し、動的に設定することができます。一部のアプリケーションではさらに細かい設定が必要なため、静的にマルチキャストサービスの設定を行う必要があります。同じ VLAN に参加するホストの接続されたすべてのポートを加え、その後 VLAN グループにマルチキャストサービスの設定を行います。

機能解説

- 静的マルチキャストアドレスはタイムアウトを起こしません。
- マルチキャストアドレスが特定の VLAN に設定された場合、関連するトラフィックは VLAN 内のポートにのみ転送されます。

設定・表示項目

VLAN

マルチキャストルータ / スイッチからのマルチキャストトラフィックを受信し、転送する VLAN を選択します。(範囲：1-4093)

Interface

ポートまたはトランクをスクロールダウンリストで選択します。

Port/Trunk

マルチキャストルータに接続されたインタフェースの番号を指定します。

Multicast IP

マルチキャストサービスを行う IP アドレスを入力します。

設定方法

インタフェースをマルチキャストサービスへ静的に追加

- (1) [Multicast] → [IGMP Snooping] → [IGMP Member] をクリックします。
- (2) 「Action」 リストから「Add Static Member」を選択します。
- (3) 必要な項目を設定し、< Apply >をクリックします。

Multicast > IGMP Snooping > IGMP Member

Action: Add Static Member

VLAN: 1

Interface: ☒ Port 1 ☐ Trunk

Multicast IP: 224.1.1.1

Apply Revert

マルチキャストサービスにアサインされた静的インタフェースの表示

- (1) [Multicast] → [IGMP Snooping] → [IGMP Member] をクリックします。
- (2) 「Action」 リストから「Show Static Member」を選択します。
- (3) 情報を表示する VLAN を選択します。

Multicast > IGMP Snooping > IGMP Member

Action: Show Static Member

VLAN: 1

IGMP Member Interface List Max: 255 Total: 1

	Interface	Multicast IP
☐	Unit 1 / Port 1	224.1.1.1

Delete Revert

マルチキャストサービスにアサインされた静的・動的全てのインタフェースを表示

- (1) [Multicast] → [IGMP Snooping] → [IGMP Member] をクリックします。
- (2) 「Action」 リストから「Current Member」を選択します。
- (3) 情報を表示する VLAN を選択します。

Multicast > IGMP Snooping > IGMP Member

Action: Show Current Member

VLAN: 1

IGMP Member Interface List Max: 16 Total: 6

Interface	Multicast IP	Type
Unit 1 / Port 1	224.1.1.1	Dynamic
Unit 1 / Port 2	224.1.2.2	Static
Unit 1 / Port 3	230.1.1.1	Static
Trunk 2	230.1.2.2	Static
Trunk 5	239.1.1.1	Dynamic
Unit 1 / Port 4	239.2.2.2	Dynamic

インタフェース毎の IGMP Snooping 設定

Multicast > IGMP Snooping > Interface (Configure) ページを使用し、VLAN インタフェースの IGMP スヌーピング属性を設定します。スヌーピングをグローバルで設定するには、P335 「IGMP Snooping とクエリパラメータの設定」を参照してください。

機能解説

マルチキャストスルータディスカバリ

マルチキャストルータを識別するために使われるメカニズムには多くの物がありました。これはマルチキャストルータと異なるベンダのスヌーピングスイッチ間で互換性の問題を引き起こしました。

この問題の解決策として、IGMP スヌーピングとマルチキャストルーティングデバイスのために Multicast Router Discovery (MRD) プロトコルが開発されました。

MRD はマルチキャストルータに付随しているインタフェースで使用され、IGMP 使用可能装置が、マルチキャストソースとグループメンバーシップメッセージがどこへ送信するかを決定することを可能にします。

マルチキャストソースデータとグループメンバーシップレポートは、セグメント内の全てのマルチキャストルータで受信される必要があります。グループメンバーシッププロトコルクエリメッセージを使用して、マルチキャストルータを発見することは、クエリサプレッションの理由で不十分です。従って、MRD は特定のマルチキャストルーティングプロトコルに頼らずマルチキャストルータを識別する、標準化された方法を提供します。

[注意] MRD ドラフトの推奨された初期値はスイッチに実装されます。

マルチキャストルータディスカバリーは、マルチキャストルータを発見するために、以下の 3 つのメッセージタイプを使用します。

- Multicast Router Advertisement – アドバタイズメントはルータによって、IP マルチキャスト転送が有効化され、アドバタイズされます。これらのメッセージは、マルチキャスト転送が有効時、全てのルータインタフェース上で周期的に非要請を送信します。以下のイベントの発生上で送信されます。
 - 周期的（ランダム）タイマーの失効
 - ルータのスタートアップ手順の一部として
 - マルチキャストフォワーディングインタフェースの再起動中
 - 要請メッセージの受領時
- Multicast Router Solicitation – デバイスは、マルチキャストルータからの要請アドバタイズドメントメッセージに従って要請メッセージを送信します。これらのメッセージはダイレクトに付随したリンクにマルチキャストルータを発見するために使用されます。要請メッセージはまた、マルチキャストフォワーディングインタフェースが初期化または最初期化される時に送られます。IP マルチキャストフォワーディングと MRD 有効のインタフェースで要請メッセージを受信するとすぐに、ルータはアドバタイズメントを返答します。
- Multicast Router Termination – これらのメッセージは、ルータがインタフェースで IP マルチキャストルーティング機能を停止した時に送信されます。ターミネーションメッセージは以下の状態で、マルチキャストルータによって送信されます。
 - インタフェースでマルチキャストフォワーディングが無効
 - インタフェースが無効
 - ルータがグローバルでシャットダウン

アドバタイズメントおよびターミネーションメッセージは全てのスヌーパーズマルチキャストアドレスへ送られます。要請メッセージは全てのルータのマルチキャストアドレスへ送られます。

[注意] MRD メッセージはIGMP スヌーピングまたはルーティングが有効な VLAN の全てのポートにフラッドされます。MRD をサポートしない古いスイッチが同じくマルチキャストルータポートを学習できることを保証するために、スイッチは VLAN に付属する全てのポートへ空白 (0.0.0.0) のソースアドレスを持たない IGMP の一般的なクエリパケットをフラッドします。空白のソースアドレスを持つ IGMP パケットは、システムがマルチキャストフラッディングモードで動作している時のみ VLAN の全てのポートへフラッドされます。(新しい VLAN または新しいルータポートが確立された、またはスパニングツリートポロジに変化が起こった時等) さもないければ、この種類のパケットは周知のマルチキャストルーティングポートのみへ転送されます。

設定・表示項目

VLAN

設定を行う VLAN の ID (範囲: 1-4093)

IGMP Snooping Status

ホストはマルチキャストトラフィックの受信を求めます。これは IGMP スヌーピングとして参照されます。(初期設定: 無効) IGMP スヌーピングがグローバルで有効の時、(P335) IGMP の VLAN ごとのインタフェース設定が優先されます。IGMP スヌーピングがグローバルで無効の時、スヌーピングは依然 VLAN インタフェースごとに設定されることが可能ですが、スヌーピングがグローバルで再度有効になるまで、効力を発しません。

Version Exclusive

受信された、IGMP バージョン属性によって現在の設定と異なるバージョンを使用する全ての IGMP メッセージを破棄します (マルチキャストプロトコルパケットを除く) (初期設定: 無効) version exclusive が VLAN で無効の場合、この設定は Multicast>IGMP Snooping>General ページで行われたグローバル設定が基になります。VLAN で有効の場合、この設定はグローバル設定よりも優先となります。

Immediate Leave Status

親 VLAN で Immediate Leave が有効であり、ポートで Leave パケットが受信された際、マルチキャストサービスのメンバーポートを即座に削除します。(初期設定: 無効) Immediate Leave が使用されない場合、IGMP v2 グループ Leave メッセージが受信された時にマルチキャストルータ (またはクエリア) が group-specific query メッセージを送信します。指定したタイムアウト期間の内にホストがクエリへ返答しない場合に限り、ルータ / クエリアはトラフィックの転送を停止します。

Multicast Router Discovery

MRD はどのインタフェースがマルチキャストルータに付属しているかを発見するために使用されます。

General Query Suppression

下流マルチキャストホストに属しているポート以外の、通常のクエリを抑制します。(初期設定: 無効) デフォルトで、通常のクエリメッセージは、それらが受信されるマルチキャストルータを除く全てのポートへフラッドされます。通常クエリサプレッションが有効の場合、これらのメッセージはマルチキャストサービスに加入している下流ポートへのみ転送されます。

Proxy Reporting

プロキシレポーティングを有効にします (初期設定: グローバル設定に基づく) 本コマンドにてプロキシレポーティングを有効にすると、スイッチは last leave とクエリサプレッションを含む、"IGMP Snooping with Proxy Reporting" を行います。(DSL Forum TR-101, April 2006 で定義) 最後のメンバーがマルチキャストグループを去った時、last leave はプロキシクエリを送ります。

クエリサプレッションは特定のクエリと通常のクエリのいずれも、アップストリームマルチキャストルータからホストへの転送を行われないことを意味します。

Interface Version

ネットワーク上の他デバイスとの互換性の為、プロトコルバージョンを設定します。
これは、スイッチがスヌーピングレポートを送信するために使用する IGMP バージョンです。
(範囲：1-3 初期設定：2)

この属性は、IGMP スヌーピングで使用される IGMP レポート / クエリのバージョンを設定します。バージョン 1-3 の全てがサポートされ、バージョン 2 と 3 には下位互換性があるので、スイッチは使用しているスヌーピングバージョンに関わらず、他のデバイスと動作することが可能です。

Proxy Query Interval

IGMP プロキシ通常クエリの送信間隔 (範囲：2-31744 秒 初期設定：125 秒)

Proxy Query Response Interval

システムがプロキシ通常クエリへの返答を待つ最大時間 (範囲：10-31744 秒 初期設定：10 秒)

Last Member Query Interval

group-specific または group-and-source-specific クエリメッセージへの返答を待つ間隔 (範囲：1-31744 秒 初期設定：1 秒)

マルチキャストホストがグループを去る時、IGMP leave メッセージを送信します。

Leave メッセージがスイッチで受信された際、それは IGMP groupspecific または group-and-source-specific クエリメッセージを送信することで、このホストがグループを去る最後のメンバーであるかどうかを調べます。

Last Member Query Count

システムがこれ以上のローカルメンバーが存在しないことを仮定する前に送信される。IGMP proxy groupspecific または group-and-source-specific クエリメッセージの数。(範囲：1-255 初期設定：2) この属性は IGMP スヌーピングプロキシレポーティングまたは IGMP クエリアが有効の場合のみ効力を発します。

Proxy Query Address

IGMP プロキシレポーティングを使用し、ローカルで生成されたクエリとレポートメッセージの静的ソースアドレス (初期設定：0.0.0.0)

設定方法

VLAN で IGMP snooping を設定。

- (1) [Multicast] → [IGMP Snooping] → [Interface] をクリックします。
- (2) 「Action」 リストから「Configure」を選択します。
- (3) 設定を行う VLAN を選択し、必要なパラメータを更新します。
- (4) < Apply > をクリックします。

Multicast > IGMP Snooping > Interface

Action: Configure

VLAN 1

IGMP Snooping Status ☒ Enabled

Version Exclusive ☐ Enabled

Immediate Leave Status ☐ Enabled

Multicast Router Discovery ☒ Enabled

General Query Suppression ☐ Enabled

Proxy Reporting Disabled

Interface Version (1-3) 2

Proxy Query Interval (2-31744) 125 seconds

Proxy Query Response Interval (10-31740) 100 (1/10 seconds, multiple of 10)

Last Member Query Interval (1-31744) 10 (1/10 seconds, multiple of 10)

Last Member Query Count (1-255) 2

Proxy (Query) Address 0.0.0.0

Apply Revert

IGMP snooping のインタフェース設定を表示

- (1) [Multicast] → [IGMP Snooping] → [Interface] をクリックします。
- (2) 「Action」 リストから「Show」を選択します。

Multicast > IGMP Snooping > Interface												
Action: Show												
IGMP Snooping VLAN List Max: 256 Total: 2												
VLAN	IGMP Snooping Status	Immediate Leave Status	Proxy Query Interval	Proxy Query Response Interval	Last Member Query Interval	Last Member Query Count	Proxy (Query) Address	Proxy Reporting	Multicast Router Discovery	General Query Suppression	Version Exclusive	Interface Version
1	Enabled	Disabled	125	100	10	2	0.0.0.0	Disabled	Enabled	Disabled	Disabled	2
4093	Enabled	Disabled	125	100	10	2	0.0.0.0	Disabled	Enabled	Disabled	Disabled	2

IGMP Snooping で発見されたマルチキャストグループを表示

Multicast > IGMP Snooping > Forwarding Entry ページを使用し、IGMP Snooping で学習された転送エントリを表示します。

機能解説

- マルチキャストグループの情報を表示するには、最初にスイッチ上で IGMP Snooping を有効にしてください。

設定・表示項目

VLAN

VLAN ID (範囲: 1-4093)

Source Address

指定されたグループへの、マルチキャストサーバー送信トラフィックの内の 1 つのアドレス

Interface

ポートまたはトランク

設定方法

IGMP Snooping で発見されたマルチキャストグループを表示

- [Multicast] → [IGMP Snooping] → [Forwarding Entry] をクリックします。
- 情報を表示する VLAN を選択します。

Multicast > IGMP Snooping > Forwarding Entry

VLAN

IGMP Snooping Forwarding Entry List Max: 255 Total: 9

Group Address	Source Address	Interface
224.1.1.1	10.1.1.1	Unit 1 / Port 4
224.1.1.1	10.1.1.1	Unit 1 / Port 5
224.1.1.1	10.1.1.1	Trunk 3
224.1.1.1	10.1.1.1	Trunk 8
224.1.1.2	10.1.1.1	Unit 1 / Port 3
224.1.2.1	10.1.1.1	Unit 1 / Port 5
224.1.2.1	10.1.1.1	Unit 1 / Port 7
224.3.1.1	10.1.1.1	Trunk 2
224.3.1.2	10.1.1.1	Trunk 5

3.16.2 IGMP フィルタリング / スロットリング

特定の定期購読契約に基づいた IP/TV サービス等の環境において、管理者が、エンドユーザーの入手できるマルチキャストサービスの制御を希望する場合があります。IGMP フィルタリングは、指定されたスイッチポート上のマルチキャストサービスへのアクセス制限したり、同時にアクセスできるマルチキャストグループの数を調整することによって、この条件を満たすことが可能です。

IGMP フィルタリング機能を使用することにより、プロファイルを特定のマルチキャストグループのスイッチポートに割り当て、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP フィルタプロファイルは、一つまたは複数のアドレスを含む範囲を指定することが可能です。ただし、ポートに割り当てられるプロファイルは1つのみです。アクセスを拒否する IGMP プロファイルがスイッチポートに適用された場合、IP マルチキャストトラフィックのストリームを要求する IGMP Join レポートは廃棄され、ポートはそのグループからの IP マルチキャストトラフィックを受信できなくなります。マルチキャストグループへのアクセスが許可されている場合は、ポートからのレポート転送はされ、通常の処理が行われます。

IGMP スロットリングは、同時に加入が可能なマルチキャストグループポートの最大値を設定します。グループ数が、設定した最大値に達した時、スイッチは「どちらも拒否する」「置き換え」の内どちらかの処理を行うことができます。「拒否する」設定になっている場合、全ての新規 IGMPjoin レポートは破棄されます。「置き換え」設定になっている場合、スイッチはランダムに既存のグループを取り去り、新しいマルチキャストグループに置き換えます。

IGMP フィルタリング / スロットリングの有効

IGMP フィルタリングおよび IGMP スロットリングをスイッチ上で実行するため、まず最初に、設定を有効にし、IGMP プロファイル番号を作成します。

設定・表示項目

IGMP Filter Status

IGMP フィルタリングおよびスロットリングを、スイッチ上で有効にします。(初期設定：無効)

設定方法

- (1) [Multicast] → [IGMP Snooping] → [Filter] をクリックします。
- (2) 「Action」 リストから「Configure General」を選択します。
- (3) IGMP フィルタステータスを有効 / 無効にします。
- (4) < Apply > をクリックします。

Multicast > IGMP Snooping > Filter

Step: 1. Configure General

IGMP Filter Status ☒ Enabled

Apply Revert

IGMP フィルタプロファイルの設定

IGMP プロファイル番号を作成後、マルチキャストグループのフィルタへの設定、およびアクセスモードの設定を行うことができます。

設定・表示項目

Add

Profile ID

IGMP プロファイルを作成。(範囲：1-4294967295)

Access Mode

プロファイルのアクセスモードを設定します。Permit (許可) または deny (拒否) を指定してください。(初期設定：Deny (拒否))

Add Multicast Group Range

Profile ID

IGMP プロファイル設定を選択。

Start Multicast IP Address

マルチキャストグループ範囲の最初のアドレス

End Multicast IP Address

マルチキャストグループ範囲の最後のアドレス

設定方法

IGMP フィルタプロファイルの作成とアクセスモードの設定

- (1) [Multicast] → [IGMP Snooping] → [Filter] をクリックします。
- (2) 「Step」 リストから「Configure Profile」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) プロファイル番号を入力し、アクセスモードを設定します。
- (5) < Apply > をクリックします。

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile ▼ Action: Add ▼

Profile ID (1-4294967295)

Access Mode

IGMP フィルタプロファイルの表示

- (1) [Multicast] → [IGMP Snooping] → [Filter] をクリックします。
- (2) 「Step」 リストから「Configure Profile」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile ▼ Action: Show ▼

IGMP Snooping Filter Profile List Max: 15 Total: 1

☐	Profile ID	Action Mode
☐	19	Permit

Web インタフェース

マルチキャストフィルタリング

IGMP フィルタプロファイルにマルチキャストグループの範囲を追加

- (1) [Multicast] → [IGMP Snooping] → [Filter] をクリックします。
- (2) 「Step」 リストから「Configure Profile」を選択します。
- (3) 「Action」 リストから「Add Multicast Group Range」を選択します。
- (4) 設定を行うプロファイルを選択し、マルチキャストグループアドレスまたは範囲を追加します。
- (5) < Apply > をクリックします。

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Add Multicast Group Range

Profile ID: 19

Start Multicast IP Address: 239.2.3.1

End Multicast IP Address: 239.2.3.200

Apply Revert

IGMP フィルタプロファイルに設定されたマルチキャストグループの表示

- (1) [Multicast] → [IGMP Snooping] → [Filter] をクリックします。
- (2) 「Step」 リストから「Configure Profile」を選択します。
- (3) 「Action」 リストから「Show Multicast Group Range」を選択します。
- (4) 情報を表示するプロファイルを選択します。

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Show Multicast Group Range

Profile ID: 19

Multicast IP Address Range List Max: 255 Total: 1

	Start Multicast IP Address	End Multicast IP Address
☐	239.2.3.1	239.2.3.200

Delete Revert

IGMP フィルタリング / スロットリングの設定 (ポート)

IGMP プロファイルの設定を行うと、それらをインタフェースに適用することができます。また、IGMP スロットリングの設定を行うことで、インターフェイスが加入できる IGMP グループの最大数を設定することもできます。

機能解説

- IGMP スロットリングは、同時に加入が可能なマルチキャストグループポートの最大値を設定します。グループ数が、設定した最大値に達した時、スイッチは「どちら拒否する」「置き換え」の内どちらかの処理を行うことができます。「拒否する」設定になっている場合、全ての新規 IGMP join レポートは破棄されます。「置き換え」設定になっている場合、スイッチはランダムに既存のグループを取り去り、新しいマルチキャストグループに置き換えます。

設定・表示項目

Interface

ポートまたはトランク識別子。

Profile ID

既存のプロファイル、インタフェースに適用するプロファイル番号を選択します。

Max Multicast Groups

同時に加入が可能なマルチキャストグループの最大値を設定します。
(範囲：0-1024 初期設定：256)

Current Multicast Groups

現在加入しているマルチキャストグループを表示します。

Throttling Action Mode

グループ数が、設定した最大値に達した時の処理を選択。(初期設定：deny)

- deny
新規のレポートは破棄されます。
- replace
既存のマルチキャストグループは、新しいグループへ置き換えられます。

Throttling Status

インタフェース上で、スロットリングの動作が実行されたかどうかを表示します。(オプション：true または False)

設定方法

- (1) [Multicast] → [IGMP Snooping] → [Filter] をクリックします。
- (2) 「Step」 リストから「Configure Interface」を選択します。
- (3) インタフェースへアサインするプロファイルを選択し、マルチキャストグループに許可する最大数とスロットリングアクションモードを設定します。
- (4) < Apply > をクリックします。

Multicast > IGMP Snooping > Filter

Step: 3. Configure Interface ▼

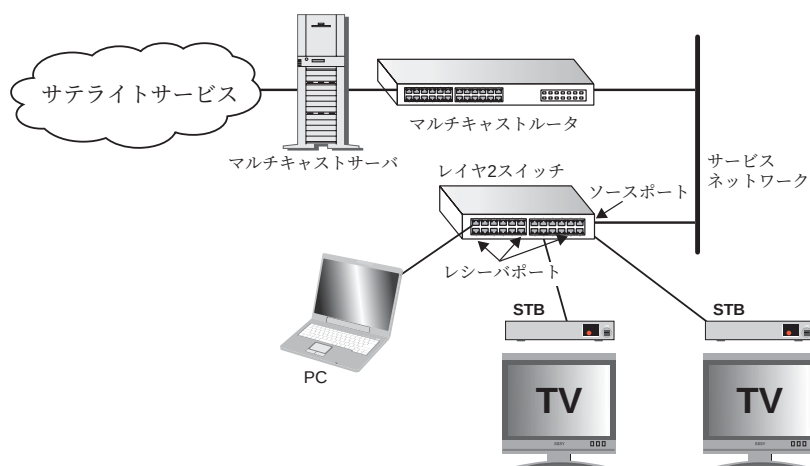
Interface ☒ Port ☐ Trunk

IGMP Filter and Throttling Port List Max: 26 Total: 26 1 2 3

Port	Profile ID	Max Multicast Groups (0-255)	Current Multicast Groups	Throttling Action Mode	Throttling Status
1	19 ▼	64	0	Deny ▼	False
2	(none) ▼	255	0	Deny ▼	False
3	(none) ▼	255	0	Deny ▼	False
4	(none) ▼	255	0	Deny ▼	False
5	(none) ▼	255	0	Deny ▼	False

3.17 MVR (Multicast VLAN Registration)

Multicast VLAN Registration(MVR) はサービスプロバイダのネットワーク上の、VLAN にマルチキャストのトラフィック（例：テレビチャンネル、ビデオ・オン・デマンド）を送信するために使用されるシングルネットワークへの通信を管理するプロトコルです。MVR ネットワークに入るどのマルチキャストトラフィックも、接続されたすべての Subscribers に送信されます。このプロトコルは動的な監視に必要なオーバーヘッドのプロセスを著しく減少させ、正常なマルチキャスト VLAN のため配送ツリーを設立することができます。これはマルチキャストルーティングプロトコルを使用せずに、広大なネットワークの上に共通のマルチキャストサービスのサポートを可能にします。



機能解説

MVR の一般的な設定手順

- (1) スイッチ全体に MVR を有効にして、MVR に使用する VLAN ID を選択します。次にトラフィックを流すマルチキャストグループを追加します。
- (2) ソースポート、レシーバポートとして MVR に参加するインタフェースを設定します。
- (3) 長時間送信し、安定してホストに関連付けられるマルチキャストストリームのため、マルチキャストグループを参加するインタフェースに固定的に結びつけることができます。(357 ページの「静的マルチキャストグループをインタフェースへ追加」を参照)

グローバル MVR 設定

MVR(Multicast VLAN Registration) のグローバル設定は、スイッチ全体での MVR の有効 / 無効、サービスプロバイダによってサポートされた通常マルチキャストストリームの単独チャンネルの役をする VLAN の選択、マルチキャストグループアドレスをそれぞれのサービスのため MVR VLAN への割り当てを含みます。

機能解説

- IGMP スヌーピングと MVR は最大 256 グループを共有します。
この限界を超過して受信されたマルチキャストストリームは関連付けられた VLAN の全てのポートへフラディングされます。

設定・表示項目

MVR Status

スイッチの MVR 機能の有効・無効（初期設定：無効）

MVR VLAN

ストリーミングのチャンネルとして動作する VLAN ID を指定。

MVR Running Status

MVR 環境において、全ての必要条件が満たされているか否かを表示します。

MVR Group IP

MVR マルチキャストグループの IP アドレス。

（範囲：224.0.1.0 - 239.255.255.255 初期設定：MVR VLAN にグループはありません）

Count

連続する MVR グループアドレスの数。（範囲：1-255 初期設定：0）

設定方法

- [Multicast] → [MVR] をクリックします。
- 「Step」リストから「Configure General」を選択します。
- 必要な項目の設定を行い、< Apply >をクリックします。

Multicast > MVR

Step: 1. Configure General

MVR Status

☒ Enabled

MVR VLAN

1

MVR Running Status

Inactive

MVR Group IP

224.1.1.1

Count (1-255)

10

Apply

Revert

MVR インタフェースの設定

MVR に参加したそれぞれのインタフェースは、MVR のソースポートかレシーバーポートとして設定しなくてはなりません。マルチキャストを受信している、インタフェースに接続されているサブスクリバが 1 つだけの場合、即時脱退機能を有効にすることができます。

機能解説

- 1 つもしくはそれ以上のインタフェースを MVR ソースポートとして設定することができます。
- MVR レシーバーポートはトランクのメンバーにすることができない。レシーバーポートは複数の VLAN に属することができるが、MVR のメンバーにとして設定すべきではありません。
- IGMP Snooping は、マルチキャストフィルタリングの標準ルールを使用して MVR のマルチキャストグループに動的に参加、離脱するソースポートやレシーバーポートを割り当てることができます。マルチキャストグループはソースポートやレシーバーポートに固定的に割り当てることができます。
- Immediate Leave 機能はレシーバーポートのみに適用されます。有効にしたとき、レシーバーポートは離脱メッセージに記録されたマルチキャストグループから即座に取り除かれます。Immediate Leave を無効にしたとき、スイッチはグループリストからポートを取り除く前にマルチキャストグループのサブスクリバが残っている場合、レシーバーポートに特定のグループのクエリを送信し決定するための返事を待つという、標準のルールに従います。Immediate Leave 機能で離脱するまでの時間を短くすることができますが、同じインタフェースに接続されているグループメンバーへのサービスを混乱させることを避けるため、1 つのマルチキャストのサブスクリバがポートに接続されている場合のみ有効にしてください。Immediate Leave 機能はポートに固定的に割り当てられたマルチキャストグループには適用されません。

設定・表示項目

Port

ポート識別子。

Type

本機では以下にインタフェースタイプをサポートしています。

- Source — MVR VLAN にアサインされたグループへマルチキャストデータを送受信できるアップリンクポート
- Receiver — MVR VLAN を通して送信されるマルチキャストデータを受信できる加入者ポート
- Non-MVR — MVR VLAN に参加しないインタフェース（初期設定）

Oper. Status

リンクステータスを表示。

MVR Status

MVR ステータスを表示。

Immediate Leave

即時脱退処理。Leave メッセージを受け取るとすぐにインタフェースを転送テーブルから削除できるようにします。

設定方法

- (1) [Multicast] → [MVR] をクリックします。
- (2) 「Action」 リストから「Configure Interface」を選択します。
- (3) 必要な項目の設定を行い、< Apply >をクリックします。

Multicast > MVR

Step: 2. Configure Interface

Port Configuration List Max: 26 Total: 26

Port	Type	Oper. Status	MVR Status	Immediate Leave
1	Receiver	Up	Inactive	☒ Enabled
2	Source	Down	Inactive	☐ Enabled
3	Non-MVR	Down	Inactive	☐ Enabled
4	Non-MVR	Down	Inactive	☐ Enabled
5	Non-MVR	Down	Inactive	☐ Enabled

静的マルチキャストグループをインタフェースへ追加

長時間送信し、安定してホストに関連付けられるマルチキャストストリームのため、マルチキャストグループに参加するインタフェースに固定的に結びつけることができます。

設定・表示項目

Port

ポート識別子。

VLAN

VLAN 識別子。

Group IP Address

選択されたポートへ送信するマルチキャストサービスを定義します。

設定方法

静的 MVR をポートへアサイン。

- (1) [Multicast] → [MVR] をクリックします。
- (2) 「Step」 リストから「Configure Static Group」を選択します。
- (3) 「Action」 リストから「Add」を選択します。
- (4) 必要な項目の設定を行い、< Apply >をクリックします。

Multicast > MVR

Step: 3. Configure Static Group Member Action: Add

Port 1

VLAN 1

Group IP Address 224.1.1.1

Apply Revert

ポートにアサインされた静的 MVR グループを表示。

- (1) [Multicast] → [MVR] をクリックします。
- (2) 「Step」 リストから「Configure Static Group」を選択します。
- (3) 「Action」 リストから「Show」を選択します。

Multicast > MVR

Step: 3. Configure Static Group Member Action: Show

Port 2

MVR Static Group Member List Max: 16 Total: 3

	VLAN	Group IP Address
☐	2	224.1.1.1
☐	2	224.1.1.2
☐	3	224.1.1.3

Delete Revert

4. コマンドラインインタフェース

4.1 コマンドラインインタフェースの利用

4.1.1 コマンドラインインタフェースへのアクセス

コンソールポート、又はネットワークから Telnet 経由で管理インタフェースにアクセスする場合、Unix のコマンドに似たコマンドキーとパラメータのプロンプト（コマンドラインインタフェース /CLI）により本機の設定を行います。

4.1.2 コンソール接続

コンソールポートへの接続は以下の手順で行います。

- (1) コンソールプロンプトでユーザ名とパスワードを入力します。初期設定のユーザ名は "admin" と "guest"、パスワードも同じく "admin" と "guest" となっています。管理者ユーザ名とパスワード（初期設定ではどちらも "admin"）を入力した場合、CLI には "Console#" と表示され Privileged Exec モードとなります。一方ゲストユーザ名とパスワード（初期設定ではどちらも "guest"）を入力した場合、CLI には "Console>" と表示され Normal Exec モードとなります。
- (2) ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。
- (3) 終了時には "quit" 又は "exit" コマンドを使用しセッションを終了します。

コンソールポートからシステムに接続すると以下のログイン画面が表示されます。

```
Username: admin
Password:

      CLI session with the FXC3326 is opened.
      To end the CLI session, enter [Exit].

Console#
```

4.1.3 Telnet 接続

Telnet を利用するとネットワーク経由での管理が可能となります。Telnet を行うには管理端末側と本機側のどちらにも IP アドレスを事前に設定する必要があります。また、異なるサブネットからアクセスする場合にはデフォルトゲートウェイもあわせて設定する必要があります。

[注意] 工場出荷時には、本機は DHCP サーバ経由で IP アドレスが割り振られる設定になっています。

IP アドレスとデフォルトゲートウェイの設定例は以下の通りです。

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

本機を外部と接続されたネットワークに接続する場合には、登録された IP アドレスを設定する必要があります。独立したネットワークの場合には内部で自由に IP アドレスを割り当てることができます。

本機の IP アドレスを設定した後、以下の手順で Telnet セッションを開始することができます。

- (1) リモートホストから Telnet コマンドと本機の IP アドレスを入力します。
- (2) プロンプト上でユーザ名とパスワードを入力します。Privileged Exec モードの場合には "Vty-0#" と表示されます。Normal Exec モードの場合には "Vty-0>" と表示されます。
- (3) ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。
- (4) 終了時には "quit" 又は "exit" コマンドを使用しセッションを終了します。

```
Username: admin
Password:

      CLI session with the FXC3326 is opened.
      To end the CLI session, enter [Exit].

Console#
```

[注意] 同時に最大 4 セッションまでの Telnet 接続が可能です。

4.2 コマンド入力

4.2.1 キーワードと引数

CLI コマンドはキーワードと引数のグループから構成されます。キーワードによりコマンドを決定し、引数により設定パラメータを入力します。

例えば、"show interfaces status ethernet 1/5" というコマンドの場合、"show interfaces" と "status" というキーワードがコマンドなり、"ethernet" と "1/5" がそれぞれインタフェースとユニット / ポートを指定する引数となります。

以下の手順でコマンドの入力を行います。

- 簡単なコマンドを入力する場合は、コマンドキーワードを入力します。
- 複数のコマンドを入力する場合は、各コマンドを必要とされる順番で入力します。例えば Privileged Exec コマンドモードを有効にして、起動設定を表示するためには、以下のようにコマンドを入力します。

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

- パラメータを必要とするコマンドを入力する場合は、コマンドキーワードの後に必要なパラメータを入力します。例えば、管理者パスワードを設定する場合には、以下のようにコマンドを入力します。

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

4.2.2 コマンドの省略

CLI ではコマンドの省略を行うことができます。例えば "configuration" というコマンドを "con" と入力するだけでもコマンドとして認識されます。但し、省略したものが複数のコマンドとなり得る場合には、システムから再度コマンドの入力を要求されます。

4.2.3 コマンド上でのヘルプの表示

コマンド上で "help" コマンドを入力することで、簡単なヘルプが表示されます。また "?" と入力するとキーワードやパラメータのコマンド文法が表示されます。

コマンドの表示

コマンド上で "?" と入力すると、現在のコマンドクラスの第一階層にあるすべてのキーワードが表示されます。また特定のコマンドのキーワードを表示することもできます。例えば "show ?" と入力すると、"show" コマンド内で使用できるコマンド一覧が表示されます。

```

Console#show ?
access-group      Access groups
access-list       Access lists
accounting        Uses the specified accounting list
arp               Information of ARP cache
authorization      Enables EXEC accounting
auto-traffic-control Auto traffic control information
bridge-ext        Bridge extension information
cable-diagnostics Shows the information of cable diagnostics
calendar          Date and time information
class-map          Displays class maps
cluster           Display cluster
dns               DNS information
dot1q-tunnel       dot1q-tunnel
dot1x             802.1X content
garp              GARP properties
gvrp              GVRP interface information
history           Shows history information
hosts             Host information
interfaces        Shows interface information
ip                IP information
ipv6              IPv6 information
lacp              LACP statistics
line              TTY line information
lldp              LLDP
log               Log records
logging           Logging setting
mac               MAC access list
mac-address-table Configuration of the address table
mac-vlan          MAC-based VLAN information
management        Shows management information
mvr               multicast vlan registration
network-access    Shows the entries of the secure port.
nlm               Show notification log
policy-map        Displays policy maps
port              Port characteristics
power             Shows power
power-save        Shows the power saving information
process           Device process
protocol-vlan      Protocol-VLAN information
public-key        Public key information
qos               Quality of Service
queue             Priority queue information
radius-server      RADIUS server information
reload            Shows the reload settings
rmon              Remote monitoring information
rspan             Display status of the current RSPAN configuration

```

(続く)

コマンドラインインタフェース

コマンド入力

(続き)

running-config	Information on the running configuration
snmp	Simple Network Management Protocol configuration and statistics
sntp	Simple Network Time Protocol configuration
spanning-tree	Spanning-tree configuration
ssh	Secure shell server connections
startup-config	Startup system configuration
subnet-vlan	IP subnet-based VLAN information
system	System information
tacacs-server	TACACS server information
time-range	Time range
traffic-segmentation	Traffic segmentation information
upgrade	Shows upgrade information
users	Information about users logged in
version	System hardware and software versions
vlan	Shows virtual LAN settings
voice	Shows the voice VLAN information
web-auth	Shows web authentication configuration

"show interfaces ?" と入力した場合には、以下のような情報が表示されます。

```
Console#show interfaces ?
brief          Shows brief interface description
counters       Interface counters information
protocol-vlan  Protocol-VLAN information
status         Shows interface status
switchport     Shows interface switchport information
Console#show interfaces
```

4.2.4 キーワードの検索

キーワードの一部と共に "?" を入力すると、入力した文字列から始まるすべてのキーワードが表示されます（入力する際に文字列と "?" の間にスペースを空けないで下さい）例えば、"s?" と入力すると、以下のように "s" から始まるすべてのキーワードが表示されます。

```
Console#show s?
snmp          snmp          spanning-tree  ssh          startup-config
subnet-vlan   system
```

4.2.5 コマンドのキャンセル

多くのコマンドにおいて、コマンドの前に "no" と入力することでコマンド実行の取り消し、又は初期設定へのリセットを行うことができます。例えば、"logging" コマンドではホストサーバにシステムメッセージを保存します。"no logging" コマンドを使用するとシステムメッセージの保存が無効となります。

本マニュアルでは、各コマンドの解説で "no" を利用してコマンドのキャンセルができる場合にはその旨の記載がしてあります。

4.2.6 コマンド入力履歴の利用

CLI では入力されたコマンドの履歴が保存されています。「↑」キーを押すことで、以前入力した履歴が表示されます。表示された履歴は、再びコマンドとして利用することができる他、履歴に表示されたコマンドの一部を修正して利用することもできます。

また、"show history" コマンドを使用すると最近利用したコマンドの一覧が表示されます。

4.2.7 コマンドモード

コマンドセットは Exec と Configuration クラスによって分割されます。Exec コマンドは情報の表示と統計情報のリセットを主に行います。一方の Configuration コマンドでは、設定パラメータの変更や、スイッチの各種機能の有効化などを行えます。

これらのクラスは複数のモードに分けられ、使用できるコマンドはそれぞれのモード毎に異なります。"? " コマンドを入力すると、現在のモードで使用できるすべてのコマンドの一覧が表示されます。コマンドのクラスとモードは以下の表の通りです。

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

※ Global Configuration モードへは、Privileged Exec モードの場合のみアクセス可能です。他の Configuration モードを使用する場合は、Global Configuration モードになる必要があります。

4.2.8 Exec コマンド

コンソールへの接続にユーザ名 "guest" でログインした場合、Normal Exec モード（ゲストモード）となります。この場合、一部のコマンドしか使用できず、コマンドの使用に制限があります。すべてのコマンドを使用するためには、再度ユーザ名 "admin" でセッションを開始するか、"enable" コマンドを使用して Privileged Exec モード（管理者モード）へ移行します（管理者モード用のパスワードを設定している場合には別途パスワードの入力が必要です）

Normal Exec モードの場合にはコマンドプロンプトの表示が "Console>" と表示されます。

Privileged Exec モードの場合には "Console#" と表示されます。

Privileged Exec モードにアクセスするためには、以下のコマンドとパスワードを入力します。

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

      CLI session with the FXC3326 is opened.
      To end the CLI session, enter [Exit].

Console#
```

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

      CLI session with the FXC3326 is opened.
      To end the CLI session, enter [Exit].

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

4.2.9 Configuration コマンド

Configuration コマンドは Privileged Exec（管理者）モード内のコマンドで、本機の設定変更を行う際に使用します。これらのコマンドはランニングコンフィグレーションのみが変更され、再起動時には保存されません。

電源を切った時にもランニングコンフィグレーションを保存するためには、"copy running-config startup-config" コマンドを使用します。

Configuration コマンドは複数の異なるモードがあります。

- **Global Configuration** — "hostname"、"snmp-server community" コマンドなどシステム関連の設定変更を行うためのモードです。
- **Access Control List Configuration** — パケットフィルタリングを行なうためのモードです。
- **Class Map Configuration** — DiffServe クラスマップを作成するためのモードです。
- **IGMP Profile** — DiffServe クラスマップを作成するためのモードです。
- **Interface Configuration** — プロファイルグループを設定し、IGMP フィルタプロファイル設定ページへ入ります。
- **Line Configuration** — "parity" や "databits" などコンソールポート関連の設定を行うためのモードです。
- **Multiple Spanning Tree Configuration** — MST インスタンス関連の設定を行なうためのモードです。
- **Policy Map Configuration** — パケットフィルタリングを行なうためのモードです。
- **Time Range** — ACL 等の機能で使用するタイムレンジを設定します。
- **VLAN Configuration** — VLAN グループを設定するためのモードです。

Global Configuration モードにアクセスするためには、Privileged Exec モードで "configure" コマンドを入力します。画面上のプロンプトが "Console(config)#" と変更になり、Global Configuration のすべてのコマンドを使用することができるようになります。

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

他のモードへは、以下の表のコマンドを入力することにより入ることができます。又、それぞれのモードからは "exit" 又は "end" コマンドを使用して Privileged Exec モードに戻ることもできます。

モード	コマンド	プロンプト	ページ
Line	Line {console vty}	Console(config-line)#	P398
Access Control List	access-list ip standard access-list ip extended access-list ip mac	Console(config-std-acl) Console(config-ext-acl) Console(config-mac-acl)	P586 P588 P592
Class Map	class map	Console(config-cmap)	P764
Interface	interface {ethernet <i>port</i> port-channel <i>id</i> vlan <i>id</i> }	Console(config-if)#	P601

MSTP	spanning-tree mst-configuration	Console(config-mstp)#	P677
Policy Map	policy map	Console(config-pmap)	P768
Time Range	time-range	Console(config-time-range)	P434
VLAN	vlan database	Console(config-vlan)	P703

以下の例では、Interface Configuration モードにアクセスし、その後 Privileged Exec モードに戻る動作を行っています。

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

4.2.10 コマンドラインプロセス

CLI のコマンドでは大文字と小文字の区別はありません。他のコマンドとパラメータの区別ができればコマンドとパラメータの省略をすることができます。また、コマンドの補完をするためにタブ・キーを使用することや、コマンドの一部と "?" コマンドを利用して関連するコマンドを表示させることもできます。

その他に、以下の表のキー入力を使用することもできます。

キー操作	機能
Ctrl-A	カーソルをコマンドラインの一番前に移動します。
Ctrl-B	カーソルを 1 文字左に移動します。
Ctrl-C	現在のタスクを終了し、コマンドプロンプトを表示します。
Ctrl-E	カーソルをコマンドラインの最後に移動します。
Ctrl-F	カーソルを 1 文字右に移動します。
Ctrl-K	カーソルから行の最後まで文字を削除します。
Ctrl-L	現在のコマンド行を新しい行で繰り返します。
Ctrl-N	コマンド入力履歴の次のコマンドを表示します。
Ctrl-P	最後に入力したコマンドを表示します。
Ctrl-R	現在のコマンド行を新しい行で繰り返します。
Ctrl-U	入力した行を削除します。
Ctrl-W	入力した最後のワードを削除します。
Esc-B	カーソルを 1 文字戻します。
Esc-D	カーソルから文字の最後までを削除します。
Esc-F	文字カーソルを進めます。
Delete 又は backspace	コマンド入力を間違えた際に削除します。

4.3 コマンドグループ

システムコマンドは機能別に以下の表の通り分類されます：

コマンドグループ	内容	ページ
General	Privileged Exec モードへのアクセスやシステムの再起動、CLI からのログアウトなど基本的なコマンド	P368
System Management	システムログ、システムパスワード、ユーザ名、ジャンボフレームサポート、Web 管理オプション、HTTPS、SSH などシステム情報に関連したコマンド	P376
SNMP	認証エラートラップ：コミュニティ名及びトラップマネージャの設定	P445
Remote Monitoring	統計、履歴、アラーム、イベントグループをサポート	
User Authentication	ユーザ名・パスワード、ローカルまたはリモート認証（AAA セキュリティを含む）Web サーバの管理アクセス、Telnet サーバ、SSH 等の設定	P471
General Security Measures	設定された静的または動的アドレス、Web 認証、MAC アドレス認証、DHCP リクエストとリプライのフィルタリング、無効な ARP レスポンスの廃棄によるデータポートに接続されたクライアントのトラフィックを分離および無効なアクセス防止。	P533
Access Control List	IP アドレス、プロトコル、TCP/UDP ポート番号、TCP コントロールコード、MAC アドレス及びイーサネットタイプによるフィルタリングの提供	P585
Interface	Trunk、LACP や VLAN など各ポートの設定	P601
Link Aggregation	複数ポートをグループ化するポートトランク及び Link Aggregation Control Protocol (LACP) の設定	P623
Mirror Port	通信監視のため、ポートを通るデータを他のポートにミラーリングを行う設定	P634
Rate Limit	通信の最大送受信帯域のコントロール	P644
Automatic Traffic Control	自動トラフィック制御の設定	P645
Address Table	アドレスフィルタの設定やアドレステーブル情報の表示とクリア、エージングタイムの設定	P664
Spanning Tree	STA 設定	P669
VLAN	各ポートの VLAN グループの設定及びプライベート VLAN、プロトコル VLAN の設定	P703
Class of Service	タグなしフレームの各ポートのプライオリティの設定。各プライオリティキューのウェイトの確認。IP precedence、DSCP、TCP トラフィックタイプのプライオリティの設定	P747
Quality of Service	Diff Serv の設定	P762
Multicast Filtering	IGMP マルチキャストフィルタ、クエリア、クエリ及び、各ポートに関連するマルチキャストルータの設定	P782
LLDP	LLDP 設定	P826
DNS	DNS サーバの設定	P843
DHCP	DNS サーバの設定	P843
IP Interface	DHCP クライアント機能を設定	P858

本章内の表で用いられるコマンドモードは以下の括弧内のモードを省略したものです。

ACL (Access Control List Configuration)	MST (Multiple Spanning Tree)
CM (Class Map Configuration)	NE (Normal Exec)
GC (Global Configuration)	PE (Privileged Exec)
IC (Interface Configuration)	PM (Policy Map Configuration)
IPC (IGMP Profile Configuration)	VC (VLAN Database Configuration)
LC (Line Configuration)	

コマンドラインインタフェース

General（一般コマンド）

4.4 General（一般コマンド）

コマンド	機能	モード	ページ
prompt	CLI プロンプトのカスタマイズ	GC	P368
reload	システムリセットの時間を設定	GC	P369
enable	Privileged モードの有効化	NE	P370
quit	CLI セッションを終了	NE,PE	P371
show history	コマンド履歴バッファの表示	NE,PE	P372
configure	Global Configuration モードの有効化	PE	P373
disable	Privileged モードから Normal モードへの変更	PE	P373
reload	本機の再起動	PE	P369
show reload	現在のリロード設定を表示	PE	P374
end	Privileged Exec モードへの変更	GC,IC,LC,VC	P375
exit	前の設定モードに戻る。 又は CLI セッションを終了	すべて	P375

prompt

CLI プロンプトのカスタマイズを行なうことができます。"no" を前に置くことで初期設定に戻ります。

文法

prompt *string*

no prompt

- *string* — CLI プロンプトに表示される名称（最大 255 文字）

初期設定

Console

コマンドモード

Global Configuration

例

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

reload (Global Configuration)

指定した経過時間または周期的な時間経過後にシステムの再起動を行います。
"cancel" オプションを使用することで設定を削除します。

文法

```
reload { at hour minute { month day | day month } { year } |  
in hour hour minute minute  
regularity hour minute { period < daily | weekly day-of-week | monthly day } > }  
cancel { at | in | regularity } }
```

- **reload at** — 指定した日時にスイッチの再起動をおこないます。
 - *hour* - 再起動する時間を指定 (時) (範囲: 0-23)
 - *minute* - 再起動する時間を指定 (分) (範囲: 0-59)
 - *month* - 再起動する時間を指定 (月) (範囲: january-december)
 - *day* - 再起動する時間を指定 (日) (範囲: 1-31)
 - *year* - 再起動する時間を指定 (年) (範囲: 2001-2050)
- **reload in** — 指定した日時にスイッチの再起動をおこないます。
 - *hour* - 経過時間を指定 (時) (0-576)
 - *minute* - 経過時間を指定 (分) (Range: 0-59)
- **reload regularity** — 周期的な間隔でスイッチの再起動をおこないます。
 - *hour* - 再起動する時間 (時) (範囲: 0-23)
 - *minute* - 再起動する時間 (分) (範囲: 0-59)
 - *month* - 再起動する曜日 (範囲: Monday-saturday)
 - *day* - 再起動する日付 (範囲: 1-31)
- **reload cancel** — 指定した再起動オプションをキャンセル。

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 本コマンドは全システムの再起動を行います。
- 再起動オプションはどのような組み合わせでも指定できます。再指定時、前回の設定は上書きされます。
- システム再起動時、Power-On セルフテストが行われます。"copy running-config startup-config" (P389) コマンドで保存された全ての設定情報は保持されます。

例

30 分後にスイッチを再起動する設定です。

```
Console(config)#reload in minute 30  
***  
*** --- Rebooting at January 1 03:38:34 2001 ---  
Are you sure to reboot the system at the specified time? <y/n>
```

コマンドラインインタフェース

General (一般コマンド)

enable

Privileged Exec モードを有効にする際に使用します。Privileged Exec モードでは他のコマンドを使用することができ、スイッチの情報を表示することができます。詳しくは P363 「コマンドモード」を参照して下さい。

文法

enable { *level* }

- *level* — Privilege Level の設定

本機では 2 つの異なるモードが存在します。

0: Normal Exec、15: Privileged Exec

Privileged Exec モードにアクセスするためには level 「15」を入力して下さい。

初期設定

Level 15

コマンドモード

Normal Exec

コマンド解説

- "super" が Normal Exec から Privileged Exec モードに変更するための初期設定パスワードになります (パスワードの設定・変更を行う場合は、P472 「enable password」を参照して下さい)
- プロンプトの最後に "#" が表示されている場合は、Privileged Exec モードを表します。

例

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

関連するコマンド

disable (P373)

enable password (P472)

quit

CLIを終了する際に利用します。

初期設定

なし

コマンドモード

Normal Exec

Privileged Exec

例

本例は、CLIセッションの終了を示しています。

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

コマンドラインインタフェース

General（一般コマンド）

show history

保存されているコマンドの履歴を表示する際に利用します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

本機に保存できるコマンド履歴は Execution コマンドと Configuration コマンドがそれぞれ最大 10 コマンドです。

例

本例では、コマンド履歴として保存されているコマンドを表示しています。

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

4 interface vlan 1
3 exit
2 interface vlan 1
1 end

Console#
```

"!" コマンドを用いると、履歴のコマンドを実行することが可能です。Normal 又は Privileged Exec モード時には Execution コマンドを、Configuration モード時には Configuration コマンドの実行が行えます。

本例では、"!2" コマンドを入力することで、Execution コマンド履歴内の 2 番目のコマンド ("config" コマンド) を実行しています。

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

configure

Global Configuration モードを有効にする場合に使用します。スイッチの設定を行うためには Global Configuration モードにする必要があります。さらに Interface Configuration, Line Configuration, VLAN Database Configuration などを行うためには、その先のモードにアクセスします。詳細は P363 「コマンドモード」を参照して下さい。

初期設定

なし

コマンドモード

Privileged Exec

例

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

関連するコマンド

end (P375)

disable

Privileged Exec から Normal Exec へ移行する際に使用します。

Normal Exec モードでは、本機の設定及び統計情報の基本的な情報の表示しか行えません。すべてのコマンドを使用するためには Privileged Exec モードにする必要があります。

詳細は P363 「コマンドモード」を参照して下さい。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

プロンプトの最後に ">" が表示されている場合は Normal Exec モードを表します。

例

```
Console#disable
Console>
```

関連するコマンド

enable (P370)

コマンドラインインタフェース

General (一般コマンド)

reload (Privileged Exec)

システムの再起動を行う際に利用します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 本コマンドは直ちに全てのシステムを再起動します。
- Power-On セルフテストが行われます。"copy running-config startup-config" (P389) コマンドで保存された全ての設定情報は保持されます。

例

本機の再起動方法を示しています。

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

show reload

現在の再起動設定と、次回予定されている再起動を表示します。

コマンドモード

Privileged Exec

例

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

The switch will be rebooted at January 1 02:11:50 2001.
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

end

Privileged モードに戻る際に利用します。

初期設定

なし

コマンドモード

Global Configuration

Interface Configuration

Line Configuration

VLAN Database Configuration

MSTP Configuration

例

本例は、Interface Configuration から Privileged Exec モードへの変更を示しています。

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

exit

Privileged Exec モードに戻る場合や、CLI を終了する場合に使用します。

初期設定

なし

コマンドモード

すべて

例

Global Configuration モードから Privileged Exec モードへの変更と、CLI の終了を示しています。

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

Press ENTER to start session

User Access Verification

Username:
```

4.5 システム管理

このコマンドはシステムログ、ユーザ名、パスワード、Web インタフェースの設定に使用されます。また、他のシステム情報の表示や設定を行えます。

コマンド	機能	ページ
Device Designation	本機を特定する情報設定	P377
System Status	管理者やシステムバージョン、システム情報の表示	P378
Frame Size	ジャンボフレームサポートの有効化	P386
File Manangement	コードイメージまたはスイッチ設定ファイルの管理	P387
Line	シリアルポートの接続パラメータを設定	P398
Event Logging	エラーメッセージログ設定	P412
SMTP Alerts	SMTP E メールアラートを設定	P421
Time (System Clock)	NTP/SNTP サーバによる自動時刻設定及び手動時刻設定	P426
Time Range	ACL 等で使用するタイムレンジの設定	P434
Switch Clustering	複数デバイスを 1 つの IP アドレスで管理する設定	P438

4.5.1 Device Designation コマンド

コマンド	機能	モード	ページ
hostname	ホスト名の設定	GC	P377
snmp-server contact	システムコンタクト者の設定	GC	P448
snmp-server location	システムロケーションの設定	GC	P448

hostname

本機のホスト名の設定及び変更を行うことができます。"no" を前に置くことで設定を削除します。

文法

hostname *name*

no hostname

- *name* — ホスト名（最大 255 文字）

初期設定

なし

コマンドモード

Global Configuration

例

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

4.5.2 システム情報の表示

システム情報を表示する為に使用するコマンドを解説します。

コマンド	機能	モード	ページ
show access-list tcamutilization	TCAM 利用率パラメータを表示	PE	P378
show memory	メモリ使用率パラメータを表示	NE,PE	P379
show process cpu	CPU 使用率パラメータを表示	NE,PE	P379
show running-config	実行中の設定ファイルの表示	PE	P380
show startup-config	フラッシュメモリ内のスタートアップ設定ファイルの内容の表示	PE	P382
show system	システム情報の表示	NE,PE	P383
show users	現在コンソール及び Telnet で接続されているユーザのユーザ名、接続時間、及び Telnet クライアントの IP アドレスの表示	NE,PE	P384
show version	システムバージョン情報の表示	NE,PE	P385

show access-list tcam-utilization

使用中のポリシーコントロールエントリ、フリーエントリ、TCAM の全体的なパーセンテージを含む、TCAM (Ternary Content Addressable Memory) の利用パラメータを表示します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Policy control entires (PCEs) は、Access Control Lists (ACLs)、IP ソースガードフィルタルール、Quality of Service(QoS) 処理、トラップ等、ルールベースの検索に頼る様々なシステム機能で使われます。例えば、ACL をポートへバインディングする時、ACL のそれぞれのルールは 2 つの PCEs を使用します。また、ポートに IP ソースガードフィルタルールを設定を行う時、システムは同じく 2 つの PCEs を使用します。

例

```
Console#show access-list tcam-utilization
Total Policy Control Entries      : 512
Free Policy Control Entries      : 352
Entries Used by System           : 160
Entries Used by User             : 0
TCAM Utilization                 : 31.25%
Console#
```

show memory

メモリ使用率のパラメータを表示します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

現在使用されていなメモリの容量と、アクティブな処理に割り当てられたメモリの容量を表示します。.

例

```
Console#show memory
Status Bytes
-----
Free 50917376
Used 83300352
Total 134217728
Console#
```

show process cpu

CPU 使用率のパラメータを表示します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show process cpu
CPU Utilization in the past 5 seconds : 3.98%
Console#
```

show running-config

現在実行中の設定ファイルを表示するためのコマンドです。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 起動用ファイルと、実行中の設定ファイルの内容を比較する場合には "show startup-config" コマンドと一緒に使用して下さい。
- キーコマンドモードの設定が表示されます。各モードのグループは "!" によって分けられて configuration モードと対応するモードが表示されます。このコマンドでは以下の情報が表示されます。

- －本機の MAC アドレス
- － SNMP サーバの設定
- － SNMP コミュニティ名
- － ユーザ（ユーザ名及びアクセスレベル）
- － VLAN データベース（VLAN ID, VLAN 名及び状態）
- － 各インタフェースの VLAN 設定状態
- － MST インスタンス（名前とインタフェース）
- － 本機の IP アドレス設定
- － レイヤ 4 Precedence 設定
- － スパニングツリー設定
- － インタフェース設定
- － コンソール及び Telnet に関する設定

例

```

Console#show running-config
Building running configuration. Please wait...
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-12-cf-f3-de-46_00</stackingMac>
!
snmp-server community public ro
snmp-server community private rw
!
snmp-server enable traps authentication
!!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca!

!
vlan database
  VLAN 1 name DefaultVlan media ethernet state active
  VLAN 4093 media ethernet state active
!
spanning-tree mst configuration
!
interface ethernet 1/1
  switchport allowed vlan add 1 untagged
  switchport native vlan 1
  switchport allowed vlan add 4093 tagged
.
(省略)
.
!
interface ethernet 1/26
  switchport allowed vlan add 1 untagged
  switchport native vlan 1
  switchport allowed vlan add 4093 tagged
!
interface vlan 1
  ip address 192.168.1.1 255.255.255.0
!
queue mode strict-wrr 0 0 0 1
!
interface vlan 1
!
line console
!
line vty
!
end
!Console#

```

関連するコマンド

show startup-config (P382)

show startup-config

システム起動用に保存されている設定ファイルを表示するためのコマンドです。

コマンドモード

Privileged Exec

コマンド解説

- 実行中の設定ファイルと、起動用ファイルの内容を比較する場合には "show running-config" コマンドと一緒に使用して下さい。
- キーコマンドモードの設定が表示されます。各モードのグループは "!" によって分けられて configuration モードと対応するモードが表示されます。このコマンドでは以下の情報が表示されます：

- － 本機の MAC アドレス
- － SNMP コミュニティ名
- － SNMP トラップ認証
- － RMON アラーム設定
- － ユーザ（ユーザ名及びアクセスレベル）
- － VLAN データベース（VLAN ID, VLAN 名及び状態）
- － MST インスタンス（名前とインタフェース）
- － 各インタフェースの VLAN 設定状態
- － 本機の IP アドレス設定
- － コンソール及び Telnet に関する設定

例

「show running-config」の内容を参照してください。

関連するコマンド

show running-config (P380)

show system

システム情報を表示するためのコマンドです。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- コマンドを使用して表示された内容に関するの詳細は P23 「システム情報の表示」を参照して下さい。
- "POST result" は正常時にはすべて "PASS" と表示されます。"POST result" に "FAIL" があった場合には販売店、またはサポートまで連絡して下さい。

例

```
Console#show system
System Description : FXC3326
System OID String  : 1.3.6.1.4.1.25574.11
System Information
  System Up Time      : 0 days, 0 hours, 2 minutes, and 28.65
seconds
  System Name         :
  System Location     :
  System Contact      :
  MAC Address (Unit 1) : 00-1A-7E-AB-FD-12
  Web Server          : Enabled
  Web Server Port     : 80
  Web Secure Server   : Disabled
  Web Secure Server Port : 443
  Telnet Server       : Enabled
  Telnet Server Port  : 23
  Jumbo Frame         : Disabled
Console#
```

show users

コンソール及び Telnet で接続されているユーザの情報を表示するためのコマンドです。
ユーザ名、接続時間及び Telnet 接続時の IP アドレスを表示します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

コマンドを実行したユーザは行の先頭に "*" が表示されています。

例

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

Online Users:
  Line    User Name                               Idle time (h:m:s) Remote IP addr
  -----
* Console admin                               0:00:00

Web Online Users:
  Line    User Name                               Idle time (h:m:s) Remote IP Addr
  -----
  HTTP    admin                               0:00:04           192.168.1.20

Console#
```

show version

ハードウェアとソフトウェアのバージョン情報を表示するためのコマンドです。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

表示される情報に関する詳細は P24 「ハードウェア及びソフトウェアバージョンの表示」を参照して下さい。

[注意] ご購入いただきました製品につきましては、製品底面に添付された serialnumber をご参照下さい。

例

```
Console#show version
Unit 1
  Serial Number       : LN10220064
  Hardware Version    : R01A
  EPLD Version        : 0.00
  Number of Ports     : 26
  Main Power Status   : Up
  Redundant Power Status : Not present
  Role                : Master
  Loader Version      : 1.0.1.5R01
  Linux Kernel Version : 2.6.22.18
  Boot ROM Version    : 0.0.0.1
  Operation Code Version : 1.1.0.1
Console#
```

4.5.3 フレームサイズコマンド

コマンド	機能	モード	ページ
jumbo frame	ジャンボフレームの利用	GC	P386

jumbo frame

ジャンボフレームの使用を有効にします。"no" を前に置くことで無効となります。

文法

jumbo frame

no jumbo frame

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 本機で最大 10240byte までのジャンボフレームに対応することで効率的なデータ転送を実現します。通常 1.5KB までのイーサネットフレームに比べジャンボフレームを使用することで各パケットのオーバーヘッドが縮小されます。
- ジャンボフレームを使用する場合は、送信側及び受信側（サーバや PC 等）がどちらも本機能をサポートしている必要があります。また Full-Duplex 時には 2 つのエンドノード間のスイッチのすべてが本機能に対応している必要があります。Half-Duplex 時にはコリジョンドメイン内の全てのデバイスが本機能に対応している必要があります。
- ジャンボフレームの現在の設定内容は "show system" コマンド (P383) で確認ができます。

例

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


4.5.4 ファイル管理（Flash/File）

ファームウェアの管理

FTP/TFTP サーバから、ファームウェアのアップロードおよびダウンロードが可能です。
FTP/TFTP サーバで、ファイルヘランタイムコードをセーブすることによって、そのファイルを後にスイッチへダウンロードすることでオペレーションを復活することが可能です。
本機はまた、以前のバージョンを上書きせずに新しいファームウェアを使用するように設定することが可能です。
ランタイムコードをダウンロードする際、現在のイメージを置き換えるか最初のファイルとは別のファイル名を使用してダウンロードをすることが出来ますので、ダウンロード後に新しいファイルを起動ファイルとして設定してください。

設定のセーブまたはリストア

FTP/TFTP サーバから、設定ファイルのアップロードおよびダウンロードが可能です。
設定ファイルは後にスイッチの設定をリストアするために使用できます。
設定ファイルは新しいファイル名でダウンロードし起動ファイルとして設定するか、現在の起動ファイルをディスティネーションファイルとして指定されたファイル名でダイレクトに置き換えることができます。

"Factory_Default_Config.cfg" は FTP/TFTP サーバにコピーすることは可能ですが、ディスティネーションとして使用することは出来ません。

コマンド	機能	モード	ページ
boot system	システム起動ファイル、イメージの設定	GC	P388
copy	コードイメージや設定ファイルのフラッシュメモリへのコピーや TFTP サーバ間のコピー	PE	P389
delete	ファイルやコードイメージの削除	PE	P392
dir	フラッシュメモリ内のファイルの一覧の表示	PE	P393
whichboot	ブートファイルの表示	PE	P394
自動コードアップグレードコマンド			
upgrade opcode auto	指定したサーバに新しいバージョンが見つかった時、現在のイメージを自動アップグレード。	GC	P395
upgrade opcode path	FTP/TFTP サーバの指定と新しいオペレーションコードが保存されるディレクトリを指定	GC	P397

boot system

システム起動に使用するファイル又はイメージを指定する際に利用します。

文法

boot system < boot-rom | config | opcode > : *filename*

設定するファイルタイプは以下の通りです。

- boot-rom — ブート ROM
- config — 設定ファイル
- opcode — ランタイムオペレーションコード
- *filename* — ファイルまたはイメージ名

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- ファイルタイプの指定の後にはコロン (:) が必要です。
- ファイルにエラーがある場合には、起動ファイルに設定できません。

例

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

関連するコマンド

dir (P393)

whichboot (P394)

copy

コードイメージのアップロード、ダウンロードや設定ファイルの本機、FTP/TFTP サーバ間のアップロード、ダウンロードを行います。

コードイメージや設定ファイルを FTP/TFTP サーバに置いてある場合には、それらのファイルを本機にダウンロードしシステム設定等を置き換えることができます。ファイル転送は TFTP サーバの設定やネットワーク環境によっては失敗する場合があります。

文法

copy *file* < file | ftp | running-config | startup-config | tftp >

copy running-config < file | ftp | startup-config | tftp >

copy startup-config < file | ftp | running-config | tftp >

copy tftp < file | running-config | startup-config |https-certificate | public-key >

- *file* — ファイルのコピーを可能にするキーワード
- ftp — FTP サーバから（または FTP サーバーへ）のコピーを行うキーワード
- https-certificate — TFTP サーバ間の HTTPS 認証をコピー
- public-key — TFTP サーバから SSH キーをコピー（詳細は、500 ページの「Secure Shell コマンド」を参照）
- running-config — 実行中の設定をコピーするキーワード
- startup-config — システムの起動に使用する設定
- tftp — TFTP サーバから（または TFTP サーバーへ）のコピーを行うキーワード

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- データをコピーするために完全なコマンドの入力が必要です。
- ファイル名は大文字と小文字が区別されます。ファイル名にはスラッシュ及びバックスラッシュは使用できません。ファイル名の最初の文字にピリオド(.)は使用できません。ファイル名の長さは FTP/TFTP サーバ上では 124 文字以下、本機上は 31 文字以下となります（ファイル名に使用できる文字は A-Z, a-z, 0-9, ".", "-", "_" です）
- フラッシュメモリ容量の制限により、オペレーションコードは 2 つのみ保存可能です。
- ユーザ設定ファイル数はフラッシュメモリの容量に依存します。

- "Factory_Default_Config.cfg" を使用し、工場出荷時設定をコピー元にすることはできますが、" Factory_Default_Config.cfg" をコピー先に指定することはできません。
- 起動時の設定を変更するためには "startup-config" をコピー先にする必要があります。
- ブート ROM とローダは FTP/TFTP サーバからダウンロードができますが、スイッチからファイルサーバへのアップロードはできません。
- "http-certificate" の設定については、195 ページの「サイト証明書の置き換え」を参照して下さい。HTTPS を使い、高セキュリティを確保した接続を行うための本機の設定については、495 ページの「ip http secure-server」を参照して下さい。

例

本例では、TFTP サーバからの新しいファームウェアのダウンロードを示しています。

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

本例では、TFTP サーバを利用した設定ファイルのアップロードを示しています。

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

Console#
```

本例では実行ファイルのスタートアップファイルへのコピーを示しています。

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

Console#
```

本例では、設定ファイルのダウンロード方法を示しています。

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

\Write to FLASH finish.
Success.

Console#
```

本例では、TFTP サーバのセキュアサイト承認を示しています。承認を完了するため、再起動を行っています。

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

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

本例では、TFTP サーバから SSH で使用するための公開キーをコピーしています。SSH による公開キー認証は、本機に対して設定済みのユーザに対してのみ可能であることに注意して下さい。

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

以下はファイルを FTP サーバにコピーする方法を示しています。

```
Console#copy ftp file
FTP server IP address: 169.254.1.11
User[anonymous]: admin
Password[]: *****
Choose file type:
  1. config: 2. opcode: 4. diag: 5. loader: <1,2,4,5>: 2
Source file name: BLANC.BIX
Destination file name: BLANC.BIX
Console#
```

delete

ファイルやイメージを削除する際に利用します。

文法

delete *filename*

- *filename* — 設定ファイルまたはイメージファイル名

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 起動ファイルは削除することができません。
- "Factory_Default_Config.cfg" は削除することができません。

例

本例ではフラッシュメモリからの設定ファイル "test2.cfg" の削除を示しています。

```
Console#delete test2.cfg
Console#
```

関連するコマンド

dir (P393)

delete public-key (P507)

dir

フラッシュメモリ内のファイルの一覧を表示させる際に利用します。

文法

`dir { boot-rom | config | opcode : filename }`

表示するファイル、イメージタイプは以下のとおりです：

- boot-rom — ブート ROM 又は、診断イメージファイル
- config — 設定ファイル
- opcode — Run-time operation code イメージファイル
- filename — ファイル又はイメージ名。ファイルが存在してもファイル内にエラーがある場合には表示できません。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- パラメータを入力せずに "dir" コマンドのみを入力した場合にはすべてのファイルが表示されます。
- 表示されるファイルの情報は以下の表の通りです

項目	解説
file name	ファイル名
file type	ファイルタイプ：Boot-Rom、Operation Code、Config file
startup	起動時に使用されているかどうか
Create Time	ファイルが作成された日時
size	ファイルサイズ (byte)

例

本例は、すべてのファイル情報の表示を示しています。

Console#dir						
	File Name	Type	Startup	Modify	Time	
Size (bytes)						

Unit 1:						
es3526ma-7lf-xc_v1.1.0.1.bix	OpCode	Y	1970-01-01	00:00:00		11474116
Factory_Default_Config.cfg	Config	N	2010-08-10	12:03:29		509
mannual_1	Config	Y	2010-08-10	12:04:53		4586
startup1.cfg	Config	N	2010-08-10	12:03:46		4587

	Free space for compressed user config files:					638976
Console#						

whichboot

現在、本機がどのファイルから起動されているかを表示します。

文法

whichboot

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#whichboot
      File Name           Type  Startup  Modify Time      Size(bytes)
-----
Unit 1:
es3526ma-71f-xc_v1.1.0.1.bix  OpCode   Y  1970-01-01 00:00:00  11351388
startup2                     Config    Y  2010-03-29 16:09:10    2323
Console#
```


upgrade opcode auto

"upgrade opcode path" コマンドで指定されたサーバに、新しいバージョンが検出された時、現在のオペレーションコードを自動でアップグレードします。"no" を使用することで設定を初期値に戻します。

文法

upgrade opcode auto

no upgrade opcode auto

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- このコマンドは、オペレーションコードの自動アップグレードを有効または無効にします。本コマンドにより自動イメージアップグレードを有効にした場合、スイッチは起動時に以下のプロセスを行います。
 - (1) "upgrade opcode path" コマンド (P397) で指定された場所でイメージの新しいバージョンを検索します。FTP/TFTP サーバに保存される新しいイメージの名前は "FXC3326.bix" にしてください。
スイッチが現在使用しているよりも新しいコードバージョン検出した場合、新しいイメージをダウンロードします。もし既に 2 つのイメージがスイッチに保存されている場合、起動ファイルに設定されていないイメージが新しいバージョンで上書きされます。
 - (2) イメージのダウンロード後、スイッチはログへアップグレードオペレーションが成功したか否かのトラップメッセージを送信します。
 - (3) 新しいバージョンをスタートアップイメージとして設定します。
 - (4) 新しいイメージを使用するためにシステムの再起動を行います。
- 初期設定に対して行われた変更は "show running-config" (P380) または "show startup-config" (P382) コマンドで表示されます。

例

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

指定された場所に新しいイメージが見つかった場合、システム起動時に以下のタイプのメッセージが表示されます。

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

upgrade opcode path

新しいオペレーションコードが保存される FTP/TFTP サーバおよびディレクトリを指定します。"no" を前に置くことで現在の設定を削除します。

文法

upgrade opcode path *opcode-dir-url*

no upgrade opcode path

- *opcode-dir-url* — 新しいコードの場所

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- このコマンドで指定する場所に保存された新しいオペレーションコードの自動アップグレードを行います。
- FTP/TFTP サーバに保存された新しいイメージの名前は "FXC3326.bix" にしてください。ファイル名はこのコマンドに含まれません。
- TFTP サーバを指定した時、filedir が新しいイメージが含まれるディレクトリへのパスを示すには以下の文法が使われます。
tftp://192.168.0.1[filedir]
- FTP サーバを指定した時、filedir が新しいイメージが含まれるディレクトリへのパスを示すには以下の文法が使われます。
ftp://[username[:password@]]192.168.0.1[filedir]/
ユーザ名が省略された場合、"Anonymous" が接続に使用されます。パスワードが省略された場合、空白 "" が接続に使用されます。

例

TFTP サーバで新しいコードが保存されている場所を指定しています。

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

例

FTP サーバで新しいコードが保存されている場所を指定しています。

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

4.5.5 Line（ラインコマンド）

VT100 互換のデバイスを使用し、シリアルポート経由で本機の管理プログラムにアクセスすることができます。本コマンドはシリアルポート接続及び Telnet 端末との接続の設定を行うために使用されます。

コマンド	機能	モード	ページ
line	コンソール接続の設定及び line configuration モードの開始	GC	P399
accounting exec	認可メソッドをローカルコンソール、Telnet、SSH 接続に適用	LC	P490
authorization exec	認証メソッドをローカルコンソール、Telnet、SSH 接続に適用	LC	P491
databits*	各文字あたりのデータビットの設定	LC	P403
exec-timeout	接続時のタイムアウトまでのインターバル時間の設定	LC	P401
login	コンソール接続時のパスワードの有効化	LC	P402
parity*	パリティビット生成の設定	LC	P400
password	コンソール接続時のパスワードの設定	LC	P404
password-thresh	パスワード入力時のリトライ数の設定	LC	P405
silent-time*	ログインに失敗した後のコンソール無効時間の設定	LC	P406
speed*	ボーレートの設定	LC	P407
stopbits*	1byte あたりのストップビット値の設定	LC	P408
timeout login response	CLI のログイン入力待ち時間の設定	LC	P409
disconnect	Line 接続を終了	PE	P408
show line	ターミナル接続の設定情報を表示	NE,PE	P411

* これらの設定はシリアルポートにのみ適用されます。

Line

Line の設定を行うために使用します。また、本コマンドを使用した後、詳細な設定が行えます。

文法

line <console | vty >

- console — コンソール接続
- vty — 仮想ターミナルのためのリモートコンソール接続

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

Telnet は仮想ターミナルの一部となり "show users" コマンドを使用した場合などは "vty" と表示されます。但し、"databits" などのシリアル接続のパラメータは Telnet 接続に影響しません。

例

本例ではコンソールラインモードに入るための例を示しています。

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

関連するコマンド

show line (P411)
show users (P384)

databits

コンソールポートで生成される各文字あたりのデータビットの値を設定するためのコマンドです。"no" を前に置くことで初期設定に戻します。

文法

databits < 7 | 8 >

no databits

- 7 – 7 データビット
- 8 – 8 データビット

初期設定

8 データビット

コマンドモード

Line Configuration

コマンド解説

パリティが生成されている場合は 7 データビットを、パリティが生成されていない場合 (no parity) は 8 データビットを指定して下さい。

例

本例では 7 データビットに設定しています。

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

関連するコマンド

parity (P400)

exec-timeout

ユーザ入力のタイムアウト時間の設定を行います。"no" を前に置くことでタイムアウト時間の設定を削除します。

文法

exec-timeout *seconds*

no exec-timeout

- *seconds* — タイムアウト時間（秒）（0 - 65535（秒）、0：タイムアウト設定なし）

初期設定

10 分

コマンドモード

Line Configuration

コマンド解説

- 設定時間内に入力が行なわれた場合、接続は維持されます。設定時間内に入力がない場合には接続は切断され、ターミナルは待機状態となります。
- 本コマンドはコンソール接続と Telnet 接続の両方に有効となります。
- Telnet のタイムアウトを無効にすることはできません。

例

本例ではタイムアウト時間を 120 秒（2 分）に設定しています。

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

関連するコマンド

silent-time (P406)

timeout login response (P409)

login

ログイン時のパスワードを有効にします。"no" を前に置くことでパスワードの確認を無効にし、パスワードなしでアクセスすることが可能になります。

文法

login { local }

no login

- local — ローカル接続時のパスワードが有効となっています。認証は "username" コマンドで設定したユーザ名を元に行います。

初期設定

login local

コマンドモード

Line Configuration

コマンド解説

- 本機へのログインには 3 種類の認証モードがあります。
 - login を選択した場合、コンソール接続用のコマンドは 1 つだけになります。この場合管理インタフェースは Normal Exec (NE) モードとなります。
 - login local を選択した場合、"username" コマンドを使用して指定したユーザ名とパスワードを使用してユーザ認証が行なわれます。この場合、管理インタフェースは入力したユーザのユーザレベルに応じて Normal Exec (NE) モード又は Privileged Exec (PE) モードのどちらかになります。
 - no login を選択すると認証はなくなります。この場合、管理インタフェースは Normal Exec(NE) モードとなります。
- 本コマンドはユーザ認証を本体で行う場合のものです。認証サーバを使用してユーザ名とパスワードの設定を行う場合には RADIUS 又は TACACS+ ソフトウェアをサーバにインストールする必要があります。

例

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

関連するコマンド

username (P473)

password (P404)

parity

パリティビットの設定のためのコマンドです。"no" を前に置くことで初期設定に戻します。

文法

parity < none | even | odd >

no parity

- none — パリティ無し
- even — 偶数パリティ
- odd — 奇数パリティ

初期設定

パリティ無し

コマンドモード

Line Configuration

コマンド解説

接続するターミナルやモデムなどの機器によっては個々のパリティビットの設定を要求する場合があります。

例

本例では no parity を設定しています。

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

password

コンソール接続のためのパスワードの設定を行います。"no" を前に置くことでパスワードを削除します。

文法

`password < 0 | 7> password`

`no password`

- {0 | 7} — "0" は平文パスワードを、"7" は暗号化されたパスワードとなります。
- *password* — コンソール接続用のパスワード（最大 8 文字（平文時）、32 文字（暗号化時）。大文字と小文字は区別されます）。

初期設定

パスワードは設定されていません

コマンドモード

Line Configuration

コマンド解説

- パスワードの設定を行うと、接続時にパスワードを要求するプロンプトが表示されます。正しいパスワードを入力するとログインできます。"password-thresh" コマンドを使用し、パスワード入力時のリトライ数を設定することができます。
- 暗号化されたパスワードはシステム起動時に設定ファイルを読み込む場合や TFTP サーバにダウンロードする場合のためにテキスト（平文）パスワードとの互換性があります。暗号化されたパスワードを手動で生成する必要はありません。

例

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

関連するコマンド

`login` (P402)

`password-thresh` (P405)

password-thresh

ログイン時のパスワード入力のリトライ回数の設定に使用するコマンドです。"no" を前に置くことで指定したリトライ回数は削除されます。

文法

password-thresh *threshold*

no password-thresh

- *threshold* – リトライ可能なパスワード入力回数（設定範囲：1-120、0：回数の制限をなくします）

初期設定

3 回

コマンドモード

Line Configuration

コマンド解説

- リトライ数が設定値を超えた場合、本機は一定時間、ログインのリクエストに応答しなくなります（応答をしなくなる時間に関しては "silent-time" コマンドでその長さを指定できます）。Telnet 時にリトライ数が制限値を超えた場合には Telnet インタフェースが終了となります。

例

本例ではパスワードのリトライ回数を 5 回に設定しています。

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

関連するコマンド

silent-time (P406)

silent-time

ログインに失敗し、"password-thresh" コマンドで指定したパスワード入力のリトライ数を超えた場合にログイン要求に反応をしない時間を設定するためのコマンドです。"no" を前に置くことで設定されている値を削除します。

文法

silent-time *seconds*

no silent-time

- *seconds* – コンソールの無効時間（秒）（設定範囲：0-65535、0：コンソールを無効にしない）

初期設定

コンソールの応答無効時間は設定されていません。

コマンドモード

Line Configuration

例

本例ではコンソール無効時間を 60 秒に設定しています。

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

関連するコマンド

password-thresh (P405)

speed

ターミナル接続のボーレートを指定するためのコマンドです。本設定では送受信両方の値を指定します。"no" を前に置くことで初期設定に戻します。

文法

speed *bps*

no speed

- *bps* – ボーレートを bps で指定
(オプション：9600、19200、38400、57600、115200 bps)

初期設定

9600bps

コマンドモード

Line Configuration

コマンド解説

シリアルポートに接続された機器でサポートされているボーレートを指定してください。一部のボーレートは本機ではサポートしていない場合があります。サポートされていない値を指定した場合にはメッセージが表示されます。

例

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

stopbits

送信するストップビットの値を指定します。"no" を前に置くことで初期設定に戻します。

文法

stopbits < 1 | 2 >

no stopbits

- 1 – ストップビット "1"
- 2 – ストップビット "2"

初期設定

ストップビット 1

コマンドモード

Line Configuration

例

本例ではストップビット "2" に設定しています。

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

timeout login response

CLI からのログイン入力のタイムアウト時間を設定します。"no" を前に置くことで初期設定に戻します。

文法

timeout login response { *seconds* }

no timeout login response

- *seconds* — タイムアウト時間（秒）（範囲：0-300 秒、0：タイムアウト設定なし）

初期設定

- CLI：無効（0 秒）
- Telnet：300 秒

コマンドモード

Line Configuration

コマンド解説

- 設定時間内にログインが検知されなかった場合、接続は切断されます。
- 本コマンドはコンソール接続と Telnet 接続の両方に有効となります。
- Telnet のタイムアウトを無効にすることはできません。
- タイムアウトを指定せずコマンドを実行した場合、初期設定に戻します。

例

本例ではタイムアウト時間を 120 秒（2 分）に設定しています。

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

disconnect

本コマンドを使用し SSH、Telnet、コンソール接続を終了することができます。

文法

disconnect *session-id*

- *session-id* — SSH、Telnet、コンソール接続のセッション ID (範囲 :0-4)

コマンドモード

Privileged Exec

コマンド解説

セッション ID "0" を指定するとコンソール接続を終了させます。その他のセッション ID を指定した場合には SSH 又は Telnet 接続を終了させます。

例

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

関連するコマンド

show ssh (P512)

show users (P384)

show line

ターミナル接続の設定を表示します。

文法

show line { console | vty }

- console – コンソール接続設定
- vty – リモート接続用の仮想ターミナル設定

初期設定

すべてを表示

コマンドモード

Normal Exec, Privileged Exec

例

本例ではすべての接続の設定を表示しています。

```
Console#show line
Console Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : Disabled
  Login Timeout      : Disabled
  Silent Time        : Disabled
  Baud Rate          : 115200
  Data Bits          : 8
  Parity             : None
  Stop Bits          : 1

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

4.5.6 Event Logging コマンド

コマンド	機能	モード	ページ
logging facility	リモートで syslog を保存する際のファシリティタイプの競って尾	GC	P412
logging history	重要度に基づいた SNMP 管理端末に送信する syslog の設定	GC	P413
logging host	syslog を送信するホストの IP アドレスの設定	GC	P414
logging on	エラーメッセージログの設定	GC	P415
logging trap	リモートサーバへの重要度にもとづいてた syslog メッセージの保存	GC	P416
clear log	ログバッファのクリア	PE	P416
show log	ログメッセージの表示	PE	P418
show logging	ログ関連情報の表示	PE	P419

logging facility

syslog メッセージを送る際の facility タイプを設定します。"no" を前に置くことで初期設定に戻します。

文法

logging facility *type*

no logging facility

type — syslog サーバで使用する facility タイプの値を指定します。(16-23)

初期設定

23

コマンドモード

Global Configuration

コマンド解説

syslog メッセージとして送信するファシリティタイプタグの設定を行ないます (詳細: RFC3164)。タイプの設定は、本機により報告するメッセージの種類に影響しません。syslog サーバにおいてソートやデータベースへの保存の際に使用されます。

例

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

logging history

本体のメモリに保存するメッセージの種類を指定することができます。"no" を前に置くことで初期設定に戻します。

文法

logging history < flash | ram > *level*

no logging history < flash | ram >

- flash – フラッシュメモリに保存されたイベント履歴
- ram – RAM に保存されたイベント履歴
- *level* – レベルは以下の表の通りです。選択した Level から Level0 までのメッセージが保存されます（範囲：0-7）

レベル引数	レベル	解説	syslog 定義
debugging	7	デバッグメッセージ	LOG_DEBUG
Informational	6	情報メッセージ	LOG_INFO
notifications	5	重要なメッセージ	LOG_NOTICE
warnings	4	警告メッセージ	LOG_WARNING
Errors	3	エラー状態を示すメッセージ	LOG_ERR
Critical	2	重大な状態を示すエラーメッセージ	LOG_CRIT
alerts	1	迅速な対応が必要なメッセージ	LOG_ALERT
emergencies	0	システム不安定状態を示すメッセージ	LOG_EMERG

初期設定

Flash: errors (level 3 - 0)

RAM: debugging (level 7 - 0)

コマンドモード

Global Configuration

コマンド解説

フラッシュメモリには、RAM に設定する Level より高い Level を設定して下さい。

例

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

logging host

ログメッセージを受け取る syslog サーバの IP アドレスを設定します。"no" を前に置くことで syslog サーバを削除します。

文法

logging host *host_ip_address*

no logging host *host_ip_address*

- *host_ip_address* — syslog サーバの IP アドレス

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 異なる IP アドレスのホストを指定したコマンドを入力し、最大 5 つの syslog サーバを設定できます。

例

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

logging on

エラーメッセージのログを取るためのコマンドです。デバッグ又はエラーメッセージをログとして保存します。"no" を前に置くことで設定を無効にします。

文法

logging on

no logging on

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

ログとして保存されるエラーメッセージは本体のメモリ又はリモートの syslog サーバに保存されます。"logging history" コマンドを使用してメモリに保存するログの種類を選択することができます。

例

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

関連するコマンド

logging history (P413)

logging trap (P416)

clear logging (P416)

logging trap

syslog サーバに送信するメッセージの種類を指定することができます。"no" を前に置くことで初期設定に戻します。

文法

logging trap *level*

no logging trap

level – レベルは以下の表の通りです。選択した Level から Level0 までのメッセージが送信されます（P413 の表を参照）

初期設定

無効（level 7）

コマンドモード

Global Configuration

コマンド解説

- レベルを指定しない場合、syslog サーバへの送信を有効に設定し、保存されるメッセージレベルを初期設定に戻します。

例

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

clear log

ログをバッファから削除するコマンドです。

文法

clear log < flash | ram >

- flash — フラッシュメモリに保存されたイベント履歴
- ram — RAM に保存されたイベント履歴

初期設定

Flash and RAM

コマンドモード

Privileged Exec

例

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

関連するコマンド

show logging (P419)

show log

スイッチのメモリに送信された、システム / イベントメッセージを表示します。

文法

show log < flash | ram >

- flash — フラッシュメモリ (恒久的) に保存されたイベント履歴
- ram — RAM (電源投入時に消去される) に保存されたイベント履歴

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

メモリに保存されたシステム / イベントメッセージを表示します。タイムスタンプ、メッセージレベル、プログラムモジュール、機能、及びイベント番号を表示します。

例

本例では、RAM に保存しているサンプルメッセージを表示しています。

```
Console#show log ram
[5] 00:01:06 2001-01-01
    "STA root change notification."
    level: 6, module: 6, function: 1, and event no.: 1
[4] 00:01:00 2001-01-01
    "STA root change notification."
    level: 6, module: 6, function: 1, and event no.: 1
[3] 00:00:54 2001-01-01
    "STA root change notification."
    level: 6, module: 6, function: 1, and event no.: 1
[2] 00:00:50 2001-01-01
    "STA topology change notification."
    level: 6, module: 6, function: 1, and event no.: 1
[1] 00:00:48 2001-01-01
    "VLAN 1 link-up notification."
    level: 6, module: 6, function: 1, and event no.: 1
Console#
```


show logging

システム、イベントメッセージに関するログを表示します。

文法

show logging < flash | ram | sendmail | trap >

- flash — フラッシュメモリに保存されたイベント履歴
- ram — RAM に保存されたイベント履歴
- sendmail — SMTP イベントハンドラの設定を表示 (P421)
- trap — トラップ機能設定の表示

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show logging flash
Syslog logging:      Enable
History logging in FLASH: level errors
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
Console#
```

項目	解説
Syslog logging	logging on コマンドによりシステムログが有効化されているかを表示
History logging in FLASH	logging history コマンドによるリポートされるメッセージレベル
History logging in RAM	logging history コマンドによるリポートされるメッセージレベル

```
Console#show logging trap
Syslog logging:      Enable
REMOTELOG Status: disable
REMOTELOG Facility Type: Local use 7
REMOTELOG Level Type:      Debugging messages
REMOTELOG server IP Address: 1.2.3.4
REMOTELOG server IP Address: 0.0.0.0
REMOTELOG server IP Address: 0.0.0.0
REMOTELOG server IP Address: 0.0.0.0
REMOTELOG server IP Address: 0.0.0.0
Console#
```

項目	解説
Syslog logging	logging on コマンドによりシステムログが有効化されているかを表示
REMOTELOG status	logging trap コマンドによってリモートロギングが有効化されているかを表示
REMOTELOG facility type	logging facility コマンドによって指定されたシスログメッセージのリモートロギングのファシリティタイプ
REMOTELOG level type	logging trap コマンドによって指定されたリモートサーバに送られるシスログメッセージの重大なしきい値
REMOTELOG server IP address	logging host コマンドによって指定されたシスログサーバのアドレス

関連するコマンド

show logging sendmail (P425)

4.5.7 SMTP アラートコマンド

SMTP イベントハンドル及びアラートメッセージの SMTP サーバ及びメール受信者への送信の設定を行います。

コマンド	機能	モード	ページ
logging sendmail	SMTP イベントハンドリングの有効化	GC	P421
logging sendmail host	アラートメッセージを受信する SMTP サーバ	GC	P422
logging sendmail level	アラートメッセージのしきい値設定	GC	P423
logging sendmail destination-email	メール受信者の設定	GC	P424
logging sendmail source-email	メールの "From" 行に入力されるアドレスの設定	GC	P425
show logging sendmail	SMTP イベントハンドラ設定の表示	NE,PE	P425

logging sendmail

SMTP イベントハンドラを有効にします。"no" を前に置くことで機能を無効にします。

文法

logging sendmail

no logging sendmail

初期設定

無効

コマンドモード

Global Configuration

例

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

logging sendmail host

アラートメッセージを送信する SMTP サーバを指定します。

"no" を前に置くことで SMTP サーバの設定を削除します。

文法

logging sendmail host *ip_address*

no logging sendmail host *ip_address*

- *ip_address* – アラートが送られる SMTP サーバの IP アドレス

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 最大 3 つの SMTP サーバを指定できます。複数のサーバを指定する場合は、サーバ毎にコマンドを入力して下さい。
- e-mail アラートを送信する場合、本機はまず接続を行ない、すべての e-mail アラートを順番に 1 通ずつ送信した後、接続を閉じます。
- 接続を行なう場合、本機は前回の接続時にメールの送信が成功したサーバへの接続を試みます。そのサーバでの接続に失敗した場合、本機はリストの次のサーバでのメールの送信を試みます。その接続も失敗した場合には、本機は周期的に接続を試みます (接続が行なえなかった場合には、トラップが発行されます)

例

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

logging sendmail level

アラートメッセージのしきい値の設定を行ないます。

文法

logging sendmail level *level*

- *level* — システムメッセージレベル (P416)。設定した値からレベル 0 までのメッセージが送信されます（設定範囲：0-7、初期設定：7）

初期設定

Level 7

コマンドモード

Global Configuration

コマンド解説

イベントしきい値のレベルを指定します。設定したレベルとそれ以上のレベルのイベントが指定したメール受信者に送信されます（例：レベル 7 にした場合はレベル 7 から 0 のイベントが送信されます）

例

本例ではレベル 3 からレベル 0 のシステムエラーがメールで送信されます。

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

logging sendmail destination-email

アラートメッセージのメール受信者を指定します。"no" を前に置くことで受信者を削除します。

文法

logging sendmail destination-email *email-address*

no logging sendmail destination-email *email-address*

- *email-address* — アラートメッセージの送信先アドレス（設定範囲：1-41 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

最大 5 つのアドレスを指定することができます。複数のアドレスを設定する際はアドレス毎にコマンドを入力して下さい。

例

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

logging sendmail source-email

メールの "From" 行に入力されるメール送信者名を設定します。"no" を前に置くことで初期設定に戻します。

文法

logging sendmail source-email *email-address*

no logging sendmail source-email

- *email-address* — アラートメッセージの送信元アドレス（設定範囲：1-41 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

本機を識別するためのアドレス（文字列）や本機の管理者のアドレスなどを使用します。

例

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

show logging sendmail

SMTP イベントハンドラの設定を表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show logging sendmail
SMTP servers
-----
192.168.1.19
SMTP minimum severity level: 4

SMTP destination email addresses
-----
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enable

Console#
```

4.5.8 Time コマンド

NTP 又は SNTP タイムサーバを指定することによりシステム時刻の動的な設定を行なうことができます。

コマンド	機能	モード	ページ
SNTP コマンド			
sntp client	特定のタイムサーバからの時刻の取得	GC	P427
sntp poll	リクエスト送信間隔の設定	GC	P428
sntp server	タイムサーバの指定	GC	P429
show sntp	SNTP 設定の表示	NE,PE	P430
手動設定コマンド			
clock timezone	本機内部時刻のタイムゾーンの設定	GC	P431
calendar set	システム日時の設定	PE	P432
show calendar	現在の時刻及び設定の表示	NE,PE	P433

sntp client

"sntp client" コマンドにより指定した NTP 又は SNTP タイムサーバへの SNTP クライアントリクエストを有効にします。"no" を前に置くことで SNTP クライアントリクエストを無効にします。

文法

sntp client

no sntp client

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 本機の内部時刻の設定を正確に保つことにより、システムログの保存の際に日時を正確に記録することができます。時刻の設定がされていない場合、起動時の時刻 (00:00:00, Jan. 1, 2001) が初期設定の時刻となり、そこからの時間経過となります。
- 本コマンドによりクライアント時刻リクエストが有効となり "sntp poll" コマンドにより設定した間隔で、"sntp servers" コマンドにより指定されたサーバにリクエストを行います。

例

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time: Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
SNTP status:Enabled
SNTP server:10.1.0.19.0.0.0.0.0.0.0.0.0
Current server:10.1.0.19
Console#
```

関連するコマンド

sntp server (P429)

sntp poll (P428)

show sntp (P430)

sntp poll

SNTP クライアントモード時に時刻同期要求の送信間隔を設定します。"no" を前に置くことで初期設定に戻します。

文法

sntp poll *seconds*

no sntp poll

- *seconds* — リクエスト間隔（設定範囲：6-16384 秒）

初期設定

16 秒

コマンドモード

Global Configuration

例

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

関連するコマンド

sntp client (P427)

sntp server

SNTP タイムリクエストを受け付ける IP アドレスを指定します。"no" を前に置くことで、すべてのタイムサーバを削除します。

文法

sntp server { ip } { ip2 } { ip3 }

- ip – NTP/SNTP タイムサーバの IP アドレス（設定可能数：1-3）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

SNTP クライアントモード時の時刻同期リクエストを送信するタイムサーバの指定を行いません。本機はタイムサーバに対して応答を受信するまで要求を送信します。"sntp poll" コマンドに基づいた間隔でリクエストを送信します。

例

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

関連するコマンド

sntp client (P427)

sntp poll (P428)

show sntp (P430)

show sntp

SNTP クライアントの設定及び現在の時間を表示し、現地時間が適切に更新されているか確認します。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

現在時刻、SNTP クライアントモード時の時刻更新リクエスト送信間隔、現在の SNTP モードを表示します。

例

```
Console#show sntp
Current time: Dec 23 05:13:28 2002
Poll interval: 16
Current mode: unicast
SNTP status:Enabled
SNTP server:137.92.140.80.0.0.0.0.0.0.0
Current server:137.92.140.80
Console#
```

clock timezone

本機内部時刻のタイムゾーンの設定を行ないます。

文法

clock timezone *name* *hour* *hours* *minute* *minutes* < before-utc | after-utc >

- *name* — タイムゾーン名（範囲：1-30 文字）
- *hours* — UTC との時間差（時間）（範囲：0-12 時間）
- *minutes* — UTC との時間差（分）（範囲：0-59 分）
- *before-utc* — UTC からのタイムゾーンの時差がマイナス（東）の場合
- *after-utc* — UTC からのタイムゾーンの時差がプラス（西）の場合

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

SNTP では UTC(Coordinated Universal Time: 協定世界時間。別名：GMT/Greenwich Mean Time) を使用します。

本機を設置している現地時間に対応させて表示するために UTC からの時差（タイムゾーン）の設定を行う必要があります。

例

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

関連するコマンド

show sntp （P430）

calendar set

システム時刻の設定を行ないます。

文法

calendar set *hour min sec* < *day month year* | *month day year* >

- *hour* — 時間（範囲：0 - 23）
- *min* — 分（範囲 0 - 59）
- *sec* — 秒（範囲 0 - 59）
- *day* — 日付（範囲：1-31）
- *month* — 月：<january | february | march | april | may | june | july | august | september | october | november | december>
- *year* — 年（西暦 4 桁、設定範囲：2001-2100）

初期設定

なし

コマンドモード

Privileged Exec

例

本例ではシステム時刻を 2010 年 2 月 1 日 15 時 12 分 34 秒に設定しています。

```
Console#calendar set 15 12 34 february 1 2010
Console#
```

show calendar

システム時刻を表示します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show calendar
15:12:34 February 1 2010
Console#
```

4.5.9 タイムレンジ

この項では、ACL 等で使用されるタイムレンジの設定を行うために使用するコマンドについて記述します。

コマンド	機能	モード	ページ
time-range	Specifies the name of a time range, and enters time range configuration mode	GC	P434
absolute	Sets the time range for the execution of a command	TR	P435
periodic	Sets the time range for the periodic execution of a command	TR	P436
show time-range	Shows configured time ranges.	PE	P437

time-range

タイムレンジの名前を設定し、タイムレンジ設定モードへ入ります。"no" を前に置くことで現在指定されているタイムレンジを削除します。

文法

time-range *name*
no time-range *name*

- *name* – タイムレンジ名（範囲：1-30 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- このコマンドは、ACL 等の機能で使用されるタイムレンジを設定します。

例

```
Console(config)#time-range r&d  
Console(config-time-range)#
```

関連するコマンド

Access Control Lists (P585)

absolute

コマンドの実行に使用するタイムレンジを設定します。"no" を前に置くことで現在指定されている時間を削除します。

文法

absolute start *hour minute day month year* [end *hour minutes day month year*]

absolute end *hour minutes day month year*

no absolute

- *hour* — 24 時間形式で時刻を指定（範囲：0-23）
- *minutes* — 分（範囲 0-59）
- *day* — 月の内の日（範囲：1-31 文字）
- *month* — january | february | march | april | may | june | july | august | september | october | november | december
- *year* — 年（範囲：2009-2109 4 桁）

初期設定

なし

コマンドモード

Time Range Configuration

コマンド解説

- タイムレンジが既に設定されている場合、このコマンドの "no" フォームを使用し新しいタイムレンジを設定する前に現在のエントリを削除します。

例

```
Console(config)#time-range r&d
Console(config-time-range)#absolute start 1 1 1 april 2010 end 2 1 1 april 2011
Console(config-time-range)#
```

periodic

コマンドの周期的実行に使用するタイムレンジを設定します。"no" を前に置くことで現在指定されている時間を削除します。

文法

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

- daily — 毎日
- friday — 金曜日
- monday — 月曜日
- saturday — 土曜日
- sunday — 日曜日
- thursday — 木曜日
- tuesday — 火曜日
- wednesday — 水曜日
- weekdays — 週日
- weekend — 週末
- *hour* — 24 時間形式で時刻を指定（範囲：0-23）
- *minutes* — 分（範囲 0-59）

初期設定

なし

コマンドモード

Time Range Configuration

例

```
Console(config)#time-range r&d
Console(config-time-range)#periodic daily 1 1 to 2 1
Console(config-time-range)#
```

show time-range

設定されたタイムレンジを表示します。

文法

show time-range { *name* }

- *name*— タイムレンジ名（範囲：1-30 文字）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show time-range r&d
Time-range r&d:
  absolute start 01:01 01 April 2010 end 02:01 01 April 2010
  periodic      Daily 01:01 to      Daily 02:01
Console#
```

4.5.10 スイッチクラスタ

スイッチクラスタリングは1つのスイッチを通した中央管理を有効にするため、スイッチをグループ化する機能です。スイッチクラスタは、クラスタの他のすべてのメンバーを管理するために使用するコマンドユニットを持ちます。管理端末はIPアドレスを通してコマンドと直接通信するためにTelnetとWebインターフェースの両方を使用することができます。またコマンドはクラスタの内部IPアドレスを使用してメンバースイッチを管理します。1つのクラスタに36個のメンバーを追加することができます。クラスタのスイッチは1つのIPサブネット内に制限されます。

コマンド	機能	モード	ページ
cluster	スイッチクラスタの設定	GC	P439
cluster commander	スイッチをクラスタコマンドに設定	GC	P440
cluster ip-pool	クラスタIPアドレスプールを設定	GC	P441
cluster member	候補スイッチをクラスタメンバーに設定	GC	P442
rcommand	メンバースイッチへのコンフィギュレーションアクセスを提供	GC	P443
show cluster	スイッチクラスタリング設定を表示	PE	P443
show cluster members	現在のクラスタメンバーを表示	PE	P444
show cluster candidates	ネットワーク上の、クラスタ候補スイッチを表示	PE	P444

スイッチクラスタリングの使用

- スイッチクラスタは"コマンドと呼ばれるプライマリユニットを持ちます。これは、クラスタ内のその他全ての"Member"スイッチを管理するために使用されます。管理ステーションはTelnetとWebインターフェースの両方を使用し、そのIPアドレスを通るコマンドと直接通信します。
- 一旦スイッチがクラスタコマンドに設定されると、自動的にネットワーク内の他のクラスタ有効スイッチを検索します。管理ステーションからアドミニストレータに手動で選択された際、"Candidate"スイッチはクラスタメンバにのみなれます。

[注意] クラスタメンバスイッチはコマンドへのTelnet接続またはコマンドへのWeb管理接続によって管理されることが可能です。コンソール接続使用時、メンバスイッチへの接続にはコマンドCLIプロンプトから"rcommand"コマンド(P443)を使います。

cluster

このコマンドはスイッチのクラスタリングを有効にします。no を付けるとクラスタリングを無効にします。

文法

cluster

no cluster

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- スwitchのクラスタを作成するためには、最初にスイッチ上でクラスタリングが有効であることを確認し（出荷時設定で有効）、次にクラスタのコマンドとしてスイッチを設定します。ネットワークの他の IP サブネットと干渉しないようにクラスタの IP プールを設定します。クラスタ用の IP アドレスは、スイッチがメンバーになりメンバースイッチとコマンドの間の通信で使用されるときにスイッチに割り当てられます。
- スwitchクラスタは 1 つのサブネットに制限されます。
- スwitchは 1 つのクラスタのメンバーにだけ所属することができます。
- 構成されたスイッチクラスタはリセット、ネットワークの変更を行っても維持されます。

例

```
Console(config)#cluster
Console(config)#
```

cluster commander

このコマンドはクラスタのコマンダとしてスイッチを設定します。no を付けるとスイッチのコマンダ設定が無効になります。

文法

cluster commander

no cluster commander

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- スwitchをコマンドとして設定した直後に、スイッチは自動的にネットワーク上のクラスタ機能が有効になっているスイッチを発見しようとします。これらの候補状態のスイッチは、管理端末を通して管理者が手動で選択したときクラスタのメンバーになることができます。
- クラスタのメンバーは Telnet でコマンドに接続することで管理することができます。コマンドから CLI でメンバースイッチに接続するには rcommand id コマンドを使います。

例

```
Console(config)#cluster commander
Console(config)#
```

cluster ip-pool

このコマンドはクラスタの IP アドレスプールを設定します。no を付けるとアドレスを初期状態に戻すことができます。

文法

cluster ip-pool [*ip-address*]

no cluster ip-pool

- *ip-address* — クラスタメンバーにアサインされた IP アドレス (10.x.x.x.)

初期設定

10.254.254.1

コマンドモード

Global Configuration

コマンド解説

- IP アドレスプールの設定が Member スイッチに割り当てられる IP アドレスとして内部的に使用されます。クラスタの IP アドレスの形式は「10.x.x.Member スイッチの id」という構成になります。Member に設定する必要のある IP アドレスの数は 1 個から 36 個です。
- ネットワークの IP サブネットと矛盾しないようクラスタの IP プールを設定してください。クラスタの IP アドレスはスイッチが Member になり、Member スイッチと Commander スイッチが相互に通信するときにスイッチに割り当てられます。
- スイッチが現在 Commander モードの場合、クラスタの IP プールの変更ができません。最初に Commander モードを無効にしてください。

例

```
Console(config)#cluster ip-pool 10.2.3.4
Console(config)#
```

cluster member

このコマンドは候補スイッチをクラスタメンバーとして設定します。.

文法

cluster member mac-address *mac-address* id *member-id*

no cluster member id *member-id*

- *mac-address* — 候補スイッチの MAC アドレス
- *member-id* — メンバースイッチに割り振られた ID 番号（範囲：1-36）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- クラスタメンバーの最大数は 36 です。
- 候補スイッチの最大数は 100 です。

例

```
Console(config)#cluster member mac-address 00-12-34-56-78-9a id 5
Console(config)#
```

rcommand

このコマンドを使用するとクラスタのメンバーに CLI でアクセスできます。

文法

rcommand id *member-id*

- *member-id* — メンバースイッチの ID (範囲：1-36)

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- このコマンドはコマンドスイッチへの Telnet 接続を通してのみ実行できます。コマンド上にローカルコンソール接続をした上でのクラスタのメンバーの管理はサポートしていません。
- メンバースイッチの CLI にアクセスするためにユーザーネームとパスワードを入力する必要はありません。

例

```
Vty-0#rcommand id 1
      CLI session with the FXC3326 is opened.
      To end the CLI session, enter [Exit].
Vty-0#
```

show cluster

スイッチクラスターリング設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show cluster
Role                : commander
Interval heartbeat  : 30
Heartbeat loss count: 3
Number of Members   : 1
Number of Candidates: 2
Console#
```

show cluster members

現在のスイッチクラスタメンバーを表示します。

コマンドモード

Privileged Exec

例

```
Console#show cluster members
Cluster Members:
ID           : 1
Role         : Active member
IP Address   : 10.254.254.2
MAC Address  : 00-12-cf-23-49-c0
Description  : FXC3326 Managed GE Switch
Console#
```

show cluster candidates

ネットワーク上の候補スイッチを検索します。

コマンドモード

Privileged Exec

例

```
Console#show cluster candidates
Cluster Candidates:
Role           Mac           Description
-----
ACTIVE MEMBER  00-12-cf-23-49-c0  FXC3326 Managed GE Switch
CANDIDATE      00-12-cf-0b-47-a0  FXC3326 Managed GE Switch
Console#
```

4.6 SNMP

トラップマネージャで送信するエラータイプなどの SNMP 管理端末を使用した本機へのアクセスに関する設定を行います。

コマンド	機能	モード	ページ
通常 SNMP コマンド			
snmp-server	SNMP サーバーを有効化	GC	P446
snmp-server community	SNMP コマンドでアクセスするためのコミュニティ名の設定	GC	P447
snmp-server contact	システムコンタクト情報の設定	GC	P448
snmp-server location	システム設置情報の設定	GC	P448
show snmp	SNMP の設定情報を表示	NE,PE	P449
SNMP ターゲットホストコマンド			
snmp-server enable traps	SNMP メッセージを受信するホストの有効化	GC	P450
snmp-server host	SNMP メッセージを受信するホストの設定	GC	P451
SNMPv3 エンジンコマンド			
snmp-server engine-id	エンジン ID の設定	GC	P453
snmp-server group	グループの追加と、ユーザーをビューへマッピング	GC	P454
snmp-server user	SNMP v3 グループへユーザーの追加	GC	P460
snmp-server view	ビューの設定	GC	P456
show snmp engine-id	エンジン ID の表示	PE	P457
show snmp group	グループの表示	PE	P458
show snmp user	SNMP v3 ユーザーの表示	PE	P460
show snmp view	ビューの表示	PE	P460
ログ通知コマンド			
nlm	指定された通知ログを有効化	GC	P462
snmp-server notify-filter	通知ログの作成とターゲットホストの指定	GC	P463
show nlm oper-status	設定された通知ログの動作ステータスを表示	PE	P464
show snmp notify-filter	設定された通知ログを表示	PE	P464
ATC トラップコマンド			
snmp-server enable port-traps atc broadcast-alarm-clear	ストームコントロールレスポンスが発生した後、ブロードキャストトラフィックが下限値を下回った特にトラップを送信	IC (Port)	P655
snmp-server enable port-traps atc broadcast-alarm-fired	ブロードキャストトラフィックが自動ストームコントロールの上限値を超えた時にトラップを送信	IC (Port)	P656
snmp-server enable port-traps atc broadcast-control-apply	ブロードキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信	IC (Port)	P657

コマンドラインインタフェース

SNMP

snmp-server enable port-traps atc broadcast- control-release	ブロードキャストトラフィックが自動ストーム コントロールの上限値を越え、アプライタイマ が失効した時にトラップを送信	IC (Port)	P658
snmp-server enable port-traps atc multicast- alarm-clear	ストームコントロールレスポンスが発生した 後、マルチキャストトラフィックが下限値を下 回った特にトラップを送信	IC (Port)	P659
snmp-server enable port-traps atc multicast- alarm-fire	マルチキャストトラフィックが自動ストームコ ントロールの上限値を超えた時にトラップを送 信	IC (Port)	P660
snmp-server enable port-traps atc multicast- control-apply	マルチキャストトラフィックが自動ストームコ ントロールの上限値を越え、アプライタイマが 失効した時にトラップを送信	IC (Port)	P661
snmp-server enable port-traps atc multicast- control-release	マルチキャストトラフィックが自動ストームコ ントロールの上限値を越え、アプライタイマが 失効した時にトラップを送信	IC (Port)	P662

snmp-server

SNMPv3 エンジンおよび、その他全ての管理クライアントサービスを有効にします。

"no" を前に置くことでサービスを無効にします。

文法

snmp-server

no snmp-server

初期設定

有効

コマンドモード

Global Configuration

例

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

snmp-server community

SNMP 使用時のコミュニティ名を設定します。"no" を前に置くことで個々のコミュニティ名の削除を行います。

文法

snmp-server community *string* { ro | rw }

no snmp-server community *string*

- *string* — SNMP プロトコルにアクセスするためのパスワードとなるコミュニティ名（最大 32 文字、大文字小文字は区別されます。最大 5 つのコミュニティ名を設定できます）
- ro — 読み取りのみ可能なアクセス。ro に指定された管理端末は MIB オブジェクトの取得のみが行えます
- rw — 読み書きが可能なアクセス。rw に指定された管理端末は MIB オブジェクトの取得及び変更が行えます

初期設定

- public — 読み取り専用アクセス (ro)。MIB オブジェクトの取得のみが行えます
- private — 読み書き可能なアクセス (rw)。管理端末は MIB オブジェクトの取得及び変更が行えます

コマンドモード

Global Configuration

例

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

snmp-server contact

システムコンタクト情報の設定を行います。"no" を前に置くことでシステムコンタクト情報を削除します。

文法

snmp-server contact *text*

no snmp-server contact

- *text* — システムコンタクト情報の解説（最大 255 文字）

初期設定

なし

コマンドモード

Global Configuration

例

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

関連するコマンド

snmp-server location (P448)

snmp-server location

システム設置場所情報の設定を行います。"no" を前に置くことでシステム設置場所情報を削除します。

文法

snmp-server location *text*

no snmp-server location

- *text* — システム設置場所の解説（最大 255 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server location Room 23
Console(config)#
```

関連するコマンド

snmp-server contact (P448)

show snmp

SNMP のステータスを表示します。

文法

show snmp

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

本コマンドを使用することで、コミュニティ名に関する情報、及び SNMP の入出力データの数が "snmp-server enable traps" コマンドが有効になっていなくても表示されます。

例

```
Console#show snmp

SNMP Agent : Enabled

SNMP Traps :
  Authentication : Enabled
  Link-up-down   : Enabled

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

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

SNMP Logging: Disabled
Console#
```

snmp-server enable traps

SNMP のトラップメッセージの送信を有効化します。"no" を前に置くことで機能を無効にします。

文法

[no] snmp-server enable traps { authentication | link-up-down }

- authentication — 認証時に不正なパスワードが送信された場合にトラップが発行されます
- link-up-down — Link-up 又は Link-down 時にトラップが発行されます

初期設定

authentication 及び link-up-down トラップを通知

コマンドモード

Global Configuration

コマンド解説

- snmp-server enable traps" コマンドを使用しない場合、一切のメッセージは送信されません。SNMP メッセージを送信するためには最低 1 つの "snmp-server enable traps" コマンドを入力する必要があります。キーワードを入力せずにコマンドを入力した場合にはすべてのメッセージが有効となります。キーワードを入力した場合には、キーワードに関連するメッセージのみが有効となります。
- "snmp-server host" コマンドは "snmp-server enable traps" コマンドとともに使用されます。"snmp-server host" コマンドでは SNMP メッセージを受け取るホストを指定します。ホストが SNMP メッセージを受信するためには最低 1 つ以上の "snmp-server host" コマンドが指定されホストが有効になっている必要があります。

例

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

関連するコマンド

snmp-server host (P451)

snmp-server host

SNMP メッセージを受け取るホストの指定を行います。"no" を前に置くことでホストを削除します。

文法

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

```
no snmp-server host host-addr
```

- *host-addr* — SNMP メッセージを受け取るホストのアドレス（最大 5 つのホストを設定できます）
- *inform* — インフォームを使用（version2c と 3 でのみ使用可）
 - *retry retries* — 再送を行う最大回数（0-255 回 初期設定：3 回）
 - *timeout seconds* — 再送までの待ち時間（0-2147483647 センチセカンド 初期設定：1500 センチセカンド）
- *community-string* — メッセージとともに送られるコミュニティ名。本コマンドでもコミュニティ名の設定が行えますが、"snmp-server community" コマンドを利用して設定することを推奨します（最大 32 文字）
- *version* — トラップバージョンを指定します（範囲：v1,v2c,v3）
 - *auth | noauth | priv* — v3 使用時に設定します。これらの認証\暗号化オプションの詳細については P270 「SNMP」を参照してください。
- *port* — トラップマネージャが使用する UDP ポートを指定（1-65535 初期設定：162）

初期設定

Host Address：なし

通知：トラップ

SNMP Version：1

UDP ポート：162

コマンドモード

Global Configuration

コマンド解説

- "snmp-server host" コマンドを使用しない場合は、SNMP メッセージは送信されません。SNMP メッセージの送信を行うためには必ず "snmp-server host" コマンドを使用し最低 1 つのホストを指定して下さい。複数のホストを設定する場合にはそれぞれに "snmp-server host" コマンドを使用してホストの設定を行って下さい。
- "snmp-server host" コマンドは "snmp-server enable traps" コマンドとともに使用されます。"snmp-server enable traps" コマンドではどのような SNMP メッセージを送信するか指定します。ホストが SNMP メッセージを受信するためには最低 1 つ以上の

"snmp-server enable traps" コマンドと "snmp-server host" コマンドが指定されホストが有効になっている必要があります。

- 一部のメッセージタイプは "snmp-server enable traps" コマンドで指定することができず、メッセージは常に有効になります。
- スイッチは初期設定でトラップメッセージの通知を行いますが、トラップメッセージの受け取り側はスイッチへ応答を送りません。その為、十分な信頼性は確保できません。インフォームを使用することにより、重要情報がホストに受け取られるのを保証することが可能です。

インフォームを SNMPv2c ホストへ送信するには、以下のステップを行ってください。

- (1) SNMP エージェントを有効にする。(P446)
- (2) 必要な通知メッセージでビューを作成。(P456)
- (3) 必要な通知ビューを含むグループを作成。(P454)
- (4) スイッチに SNMP トラップ（通知）送信を許可する。(P450)
- (5) 本項で解説する "snmp-server host" コマンドを使用し、インフォームメッセージを受信するターゲットホストを指定。

- インフォームを SNMPv3 ホストへ送信するには、以下のステップを行ってください。

- (1) SNMP エージェントを有効にする。(P446)
- (2) メッセージ交換プロセスで使用するローカル SNMPv3 ユーザを作成。
- (3) 必要な通知メッセージでビューを作成。(P456)
- (4) 必要な通知ビューを含むグループを作成 (P454)
- (5) スイッチに SNMP トラップ（通知）送信を許可する。(P450)
- (6) 本項で解説する "snmp-server host" コマンドを使用し、インフォームメッセージを受信するターゲットホストを指定。

- スイッチは SNMPv1,2c,3 通知を管理ステーションがサポートする SNMP バージョンに基づいて、ホスト IP アドレスに送信出来ます。

"snmp-server host" コマンドが SNMP バージョンを指定しない場合、初期設定では SNMP バージョン 1 の通知を送信します。

- SNMPv3 ホストを指定している場合、トラップマネージャのコミュニティ名は、SNMP ユーザー名として解釈されます。SNMPv3 認証または暗号化オプションを使用している際には (authNoPriv または authPriv)、最初に P460 「show snmp user」でユーザー名を定義してください。ユーザー名が定義されていない場合、認証パスワードおよびプライバシーパスワードが存在せず、スイッチはホストからのアクセスを許可しません。
尚、SNMPv3 ホストを no authentication (noAuth) として設定している場合には、SNMP ユーザーアカウントは自動的に生成されますので、スイッチはホストからのアクセスを許可します。

例

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

関連するコマンド

snmp-server enable traps (P450)

snmp-server engine-id

エンジン ID の設定を行います。エンジン ID はデバイス内のエージェントを固有に識別するためのものです。"no" を前に置くことでエンジン ID を初期設定値に戻します。

文法

snmp-server engine-id < local | remote *ip address* > *engine-id*

no snmp-server engine-id < local | remote *ip address* >

- local — スイッチ上の SNMP エンジン指定
- remote — リモートデバイス上の SNMP エンジン指定
- *ip address* — リモートデバイスの IP アドレス
- *engine-id* — エンジン ID

初期設定

スイッチの MAC アドレスを基に自動的に生成されます

コマンドモード

Global Configuration

コマンド解説

- SNMP エンジンにはメッセージ再送、遅延およびダイレクションを防止します。
エンジン ID はユーザパスワードと組み合わせて、SNMPv3 パケットの認証と暗号化を行うためのセキュリティキーを生成します。
- リモートエンジン ID は SNMPv3 インフォームを使用する際に必要です。(詳しくは P451 「snmp-server host」を参照してください) リモートエンジン ID は、リモートホストでユーザに送られた認証と暗号化パケットのセキュリティダイジェストを計算するために使用されます。SNMP パスワードは信頼できるエージェントのエンジン ID を使用してローカライズされます。インフォームの信頼できるエージェントはリモートエージェントです。したがってプロキシリクエストまたはインフォームを送信する前に、リモートエージェントの SNMP エンジン ID を変更を行う必要があります。
- ローカルエンジン ID はスイッチにたいして固有になるように自動的に生成されます。これをデフォルトエンジン ID とよびます。ローカルエンジン ID が削除または変更された場合、全ての SNMP ユーザーはクリアされます。そのため既存のユーザーの再構成を行う必要があります。

例

```
Console(config)#snmp-server engine-id local 123456789
Console(config)#snmp-server engine-id remote 192.168.1.19
9876543210
Console(config)#
```

関連するコマンド

snmp-server host (P451)

snmp-server group

SNMP グループ追加と、SNMP ユーザーのビューへのマッピングを行います。
"no" を前に置くことでグループを削除します。

文法

[no] snmp-server group *groupname* < v1 | v2c | v3 < auth | noauth | priv> >
{read *readview* | write *writeview* | notify *notify view* }

- *groupname* — SNMP グループ名 (1-32 文字)
- v1 | v2c | v3 — 使用する SNMP バージョンを選択します
 - auth | noauth | priv — v3 使用時に設定します。これらの認証 \ 暗号化オプションの詳細については P270 「SNMP」を参照してください。
- *readview* — Read アクセスのビューを設定します (1-64 文字)
- *writeview* — write アクセスのビューを設定します (1-64 文字)
- *notify view* — 通知ビューを設定します (1-64 文字)

初期設定

Default groups : public (read only)、private (read/write)

readview - 全てのオブジェクトは Internet OID space (1) に属します

writeview - なし

notifyview - なし

コマンドモード

Global Configuration

コマンド解説

- SNMP グループは、所属するユーザーのアクセスポリシーを定義します。
- authentication が有効時は、「show snmp user」で、MD5 または SHA どちらかの認証方式を選択してください。
- privacy が有効時は、DES56bit 暗号化方式が使用されます。
- 本機がサポートする通知メッセージの詳細な情報については P286 「必要な項目を入力し、< Apply >をクリックします。」を参照してください。また、authentication, link-up および link-down のレガシートラップについては P450 「snmp-server enable traps」を参照してください。

例

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

snmp-server user

SNMP ユーザーをグループへ追加します。"no" を前に置くことでユーザーをグループから除きます。

文法

```
snmp-server user username groupname
{ remote ip-address } < v1 | v2c | v3 { encrypted } { auth < md5 | sha > auth-password }
{ priv des56 priv-password } >
```

```
no snmp-server user username { v1 | v2c | v3 | remote IP Address }
```

- *username* — ユーザー名 (1-32 文字)
- *groupname* — グループ名 (1-32 文字)
- *remote* — リモートデバイス上の SNMP エンジンを選択します
- *ip-address* — リモートデバイスの IP アドレス
- *v1 | v2c | v3* — SNMP バージョンの選択します
- *encrypted* — 暗号化パスワード
- *auth* — 認証を使用します
- *md5 | sha* — MD5 または SHA 認証を選択します
- *auth-password* — 認証パスワード (8 文字以上)
- *priv des56* — プライバシーと DES56 暗号化 SNMP V3 を使用
- *priv-password* — プライバシーパスワード

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- リモートユーザーの設定を行う前に、「snmp-server engine-id」コマンドで、リモートエンジン ID の設定を行ってください。その後「show snmp user」を使用しユーザーと、ユーザーが所属するリモートデバイスの IP アドレスを設定してください。リモートエージェントのエンジン ID はユーザーのパスワードから認証 / プライバシーのダイジェストを計算するのに使用されます。
- SNMP パスワードは、信頼できるエージェントのエンジン ID を使用してローカライズされます。トラップ通知の信頼できる SNMP エージェントはリモートエージェントです。そのため、プロキシリクエストまたはトラップ通知を送信する前にリモートエージェントの SNMP エンジン ID を設定する必要があります。(詳しくは P287 「トラップマネージャの指定」および P285 「SNMPv3 リモートユーザーの設定」を参照してください)

例

```
Console(config)#snmp-server user steve r&d v3 auth md5 greenpeace
priv des56 einstien
Console(config)#snmp-server user mark r&d remote 192.168.1.19 v3
auth md5 greenpeace priv des56 einstien
Console(config)#
```

snmp-server view

このコマンドでは、ビューの追加を行います。"no" を前に置くことでビューを削除します。

文法

snmp-server view *view-name* {*oid-tree*} <include | exclude>

no snmp-server view *view-name*

- *view-name* — ビューの名前（1-32 文字）
- *oid-tree* — 参照可能にする MIB ツリーの OID。ストリングの特定の部分に、ワイルドカードを使用してマスクをかけることができます
- include — include ビューを指定
- exclude — exclude ビューを指定

初期設定

デフォルトビュー（全ての MIB ツリーへのアクセスを含む）

コマンドモード

Global Configuration

コマンド解説

- 作成されたビューは、MIB ツリーの指定された範囲へのユーザアクセスを制限するために使用されます。
- デフォルトビューは全体の MIB ツリーへのアクセスを含みます。

例

MIB-2 を含む View を設定

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

MIB-2 インタフェーステーブル、ifDescr を含む View を設定。ワイルドカードは、このテーブル内のすべてのインデックス値を選択するのに使用されます。

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2
included
Console(config)#
```

MIB-2 インタフェーステーブルを含む View を設定。マスクはすべてのインデックスエントリを選択します。

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
included
Console(config)#
```

show snmp engine-id

設定中の SNMP エンジン ID を表示します

文法

show snmp engine-id

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

項目	解説
Local SNMP engineID	ローカルエンジン ID を表示
Local SNMP engineBoots	前回エンジン ID の設定が行われてから、エンジンの（再）初期化が行われた回数を表示
Remote SNMP engineID	リモートデバイスのエンジン ID を表示
IP address	リモートエンジンの IP アドレスを表示

例

```

Console#show snmp engine-id
Local SNMP engineID: 8000002a80000000000e8666672
Local SNMP engineBoots: 1
Remote SNMP engineID                               IP address
800000000030004e2b316c54321                        192.168.1.19
Console#

```

show snmp group

4 つのデフォルトグループが提供されます。
SNMPv1 の read-only および read/ write アクセス。
SNMPv2 の read-only および read/write アクセス。

文法

show snmp group

コマンドモード

Privileged Exec

コマンド解説

項目	解説
groupname	グループ名
security model	セキュリティモデル
read view	read ビュー
write view	write ビュー
notify view	通知ビュー
storage-type	このエントリーのストレージタイプ
Row Status	ビューの状態

例

```
Console#show snmp group
Group Name: fxc
Security Model: v3
Read View: defaultview
Write View: none
Notify View: none
Storage Type: nonvolatile
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#
```

show snmp user

SNMP ユーザー情報を表示します。

文法

show snmp user

コマンドモード

Privileged Exec

コマンド解説

項目	解説
EngineId	エンジン ID
User Name	ユーザー名
Authentication Protocol	認証プロトコル
Privacy Protocol	暗号化方式
storage type	このエントリーのストレージタイプ
Row Status	ビューの状態
SNMP remote user	リモートデバイス上の SNMP エンジンに所属するユーザー

例

```
Console#show snmp user
EngineId: 01000000000000000000000000000000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

show snmp view

ビューを表示します。

文法

show snmp view

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

項目	解説
View Name	ビュー名
Subtree OID	参照可能な MIB ツリーの OID
View Type	OID で表示される MIB ノードがビューに含まれてるか (included)、含まれていないか (excluded)
Storage Type	このエントリーのストレージタイプ
Row Status	ビューの状態

例

```

Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active

Console#

```

nlm

指定した通知ログのを有効または無効にします。

文法

nlm *filter-name*
no nlm

- *filter-name* — 通知ログ名（範囲：1-32 文字）

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- 通知ロギングは初期設定で有効ですが、"snmp-server notify-filter" コマンドで指定されたロギングプロファイルが "nlm" コマンドで有効になるまで、情報の記録を開始しません。
- このコマンドによるロギングの無効は、通知ログに保存されているエントリを削除しません。

例

```
Console(config)#nlm A1
Console(config)#nlm A2
Console(config)#
```

snmp-server notify-filter

SNMP 通知ログを作成します。前に "no" を置くことで、このログを削除します。

文法

[no] snmp-server notify-filter *profile-name* remote *ip-address*

- *profile-name* — 通知ログプロファイル名（範囲：1-32 文字）
- *ip-address* — リモートデバイスのインターネットアドレス。

[注意] 通知ログはローカルに保存され、リモートデバイスへは送信されません。このリモートホストパラメータは SNMP 通知 MIB の管理フィールドを完了することだけを必要とされます。

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- SNMP をサポートするシステムはしばしば通知の消失に対する予防として通知情報を記録するメカニズムを必要とします。通知ログ MIB (Notification Log MIB NLM, RFC 3014) は MIB 情報の基礎構造を提供します。
- 通知ロギングが有効に設定されていない時にスイッチが再起動を行った場合、いくつかの SNMP トラップ (warm start など) は記録されません。
この問題を回避するため、通知ロギングの設定を行い、" snmp-server notify-filter" コマンドで有効にしてください。また、これらのコマンドは起動設定ファイルに保存されています。スイッチ再起動時、SNMP トラップ (warm start など) は保存されます。
- このコマンドの実行時、通知ログが作成されます。(RFC3014 で定義されたデフォルトパラメータ) 通知ロギングは初期設定で有効 (P462 「nlm」 参照) になっていますが、このコマンドで指定されたロギングプロファイルが "nlm" コマンドで有効になるまで、情報の記録を開始しません
- RFC3014 で使用される初期設定に基づいて、通知ログは最大 256 エントリを含むことが可能であり、エントリのエージングタイムは 1440 分です。
通知ログに記録された情報、エントリエージングタイムはネットワーク管理ステーションから SNMP を使用してのみ設定が可能です。

例

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server notify-filter A1 remote 10.1.19.23
Console#
```

show nlm oper-status

設定された通知ログの稼動状況を表示します。

文法

show nlm oper-status

コマンドモード

Privileged Exec

例

```
Console#sh nlm oper-status
Filter Name: A1
Oper-Status: Operational
Filter Name: A2
Oper-Status: Operational
Console#
```

show snmp notify-filter

設定された通知ログを表示します。

文法

show snmp notify-filter

コマンドモード

Privileged Exec

例

```
Console#show snmp notify-filter
Filter profile name      IP address
-----
A1                      10.1.19.23
A2                      10.1.19.22
traphost.1.1.1.1.private 1.1.1.1
Console#
```

4.7 リモートモニタリング

リモートモニタリングは、リモート装置が非依存を基礎に指定されたイベントの情報を、収集または対処することを可能にします。

本機は、独立して広範囲のタスクを実行することが可能な RMON に対応しており、ネットワーク管理トラフィックを大幅に低減することが出来ます。この機能により連続的な診断とログ情報収集を行えます。

本機は統計、履歴、イベント、アラームグループから成る、mini-RMON をサポートしています。RMON 有効時、システムは次第にその物理的インタフェースに関する情報を増強し、この情報に適切な RMON データベースグループへ保存します。

管理エージェントは SNMP プロトコルを使用し、周期的にスイッチとコミュニケーションを行います。もしスイッチが致命的なイベントに遭遇した場合、それは管理エージェントへ自動でトラップメッセージを送信します。

コマンド	機能	モード	ページ
rmon alarm	監視される変数のための閾値の限界を設定	GC	P466
rmon event	アラームの返答イベントを作成	GC	P467
rmon collection history	周期的に統計のサンプルを採取	IC	P468
show rmon alarm	全てのアラームの設定を表示	PE	P469
show rmon event	全てのイベントの設定を表示	PE	P469
show rmon history	それぞれのエントリのサンプリングパラメータを表示	PE	P470
show rmon statistics	収集された統計を表示	PE	P470

rmon alarm

監視される変数のしきい値の限界を設定します。"no" を前に置くことでアラームを削除します。

文法

rmon alarm *index variable interval seconds* < absolute | delta > rising-threshold *threshold*
event-index falling-threshold *threshold* { *event-index* } { *owner name* }

no rmon event *index*

- *index* — このエントリのインデックス（範囲：1-65535）
- *variable* — サンプルされる MIB 変数のオブジェクト識別子。
タイプ etherStatsEntry.n.n の変数のみがサンプルされます。etherStatsEntry.n は一意的に MIB 変数を定義し、etherStatsEntry.n.n は MIB 変数に加えて etherStatsIndex を定義することにご注意下さい。例えば、1.3.6.1.2.1.16.1.1.1.6.1 は etherStatsBroadcastPkts に加えて 1 の etherStatsIndex を示します。
- *seconds* — ポーリング間隔（範囲：1-31622400 秒）
- absolute — 変数はサンプリングピリオドの終わりに直接しきい値と比較されます。
- delta — 最後のサンプルは現在の値から引かれ、相違がしきい値と比較されます。
- *threshold* — サンプルされた変数のアラームしきい値（範囲：1-65535）
- *event-index* — アラームが引き起こされた時に使用されるイベントのインデックス。
もし対応するエントリがイベントコントロールテーブルにない場合、イベントは生成されません（範囲：1-65535）
- *name* — このエントリの作成者の名前（範囲：1-127 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 既にイベントがインデックスに定義されている場合、このコマンドで変更を行う前にエントリを削除してください。

例

```
Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta rising-  
threshold 100 falling-threshold 30  
Console(config)#
```


rmon event

アラームの返答イベント作成します。"no" を前に置くことでイベントを削除します。

文法

rmon event *index* { *log* } | { *trap community* } | { *description string* } | { *owner name* }

no rmon event *index*

- *index* — このエントリのインデックス（範囲：1-65535）
- *log* — イベント発生時、RMON ログエントリを生成。
- ログメッセージはイベントロギングの現在の設定を基に処理されます。
("Event Logging" (P412) 参照)
- *trap* — 設定されたトラップマネージャにトラップメッセージを送信。("snmp-server host" (P451) 参照)
- *community* — トラップオペレーションと共に SNMPv1 および v2c ホストへ送信される、パスワードのようなコミュニティストリング。このストリングがそれ自身によって "rmon event" コマンド (P467) を使用して設定されることが可能ですが、ストリングは "rmon event" コマンドを使用するよりも、"snmp-server community" コマンド (P447) を使用して定義することを推奨します。（範囲：1-32）
- *string* — このイベントを説明するコメント（範囲：1-127 文字）
- *name* — このエントリの作成者の名前（範囲：1-127 文字）

初期設定

1 つの初期イベントが以下のように設定されています。

event Index = 1

Description: RMON_TRAP_LOG

Event type: log & trap

Event community name is public

Owner is RMON_SNMP

コマンドモード

Global Configuration

コマンド解説

- 既にイベントがインデックスに定義されている場合、このコマンドで変更を行う前にエントリを削除してください。
- 指定されたイベントは、このイベントでアラームが起こった時取るアクションを決定します。アラームへの返答はアラームのロギングまたはトラップマネージャへのメッセージ送信を含みます。

例

```
Console(config)#rmon event 2 log description urgent owner mike
Console(config)#
```

rmon collection history

物理インタフェース上の統計値を周期的にサンプルします。"no" を前に置くことで周期的サンプリングを無効にします。

文法

rmon collection history controlEntry *index* { *buckets number* } | { *interval seconds* } |
{ *owner name* }

no rmon collection history *index*

- *index* — このエントリのインデックス（範囲：1-65535）
- *number* — このエントリで要求されるバケットの数（範囲：1-65536）
- *seconds* — ポーリングインターバル（範囲：1-3600 秒）
- *name* — このエントリの作成者の名前（範囲：1-127 文字）

初期設定

有効

バケット：50

インターバル：1800 秒

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 初期設定では、それぞれのインデックス番号はスイッチのポートと同等ですが、現在使用していないどんな数にも変更することが可能です。
- インタフェースで周期的サンプルが既に有効になっている場合、このコマンドで変更を行う前にエントリを削除してください。
- それぞれのサンプルで収集される情報：
インプットオクテット、パケットブロードキャストパケット、マルチキャストパケット、アンダーサイズパケット、オーバーサイズパケット、フラグメント、ジャバー、CRC アライメントエラー、ドロップイベント、ネットワーク使用率。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection history controlEntry 24 interval 60
Console(config-if)#
```

show rmon alarm

全ての設定されたアラームを表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon alarm
alarm Index = 1
    alarm Interval = 30
    alarm Type is Delta
    alarm Value = 0
    alarm Rising Threshold = 892800
    alarm Rising Event = 0
    alarm Falling Threshold = 446400
    alarm Falling Event = 0
    alarm Owner is RMON_SNMP
.
.
.
```

show rmon event

全ての設定されたイベントを表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon event
event Index = 1
    Description: RMON_TRAP_LOG
    Event type: log & trap
    Event community name is public
    Last Time Sent = 0
    Owner is RMON_SNMP
Console#
```

show rmon history

ヒストリグループのそれぞれのエントリに設定されたサンプリングパラメータを表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon history
  history index = 1
    data source ifindex = 1
    buckets requested = 8
    buckets granted = 8
    Interval = 1800
    Owner RMON_SNMP

  history index = 2
    data source ifindex = 1
    buckets requested = 8
    buckets granted = 8
    Interval = 30
    Owner RMON_SNMP
.
.
.
```

show rmon statistics

統計グループで、設定された全てのエントリで収集された情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon statistics
  rmon collection index 1
  stats->ifindex = 1
  input packets 00, bytes 00, dropped 00, multicast packets 00
  output packets 00, bytes 05, multicast packets 00 broadcast packets 00
  rmon collection index 2
  stats->ifindex = 2
  input packets 00, bytes 00, dropped 00, multicast packets 00
  output packets 00, bytes 05, multicast packets 00 broadcast packets 00
.
.
.
```

4.8 認証コマンド

本機へ、ローカルまたはリモート認証メソッドを使用した管理アクセスへのユーザのログイン認証を設定することが可能です。
同じく、アップリンクポートへの管理アクセス、またはデータポートへのクライアントアクセスへ IEEE802.1X を使用したポートベース認証を設定することが可能です。

コマンドグループ	機能	ページ
User Accounts	管理アクセスの基本ユーザ名、パスワードを設定	P471
Authentication Sequence	ログイン認証方式と優先順位の設定	P474
RADIUS Client	RADIUS サーバ認証の設定	P476
TACACS+ Client	TACACS+ サーバ認証の設定	P481
AAA	認証, 認可, アカウンティング (AAA) の設定	P484
Web Server	Web ブラウザからの管理アクセスを有効化	P493
Telnet Server	Telnet サーバからの管理アクセスを有効化	P497
Secure Shell	Telnet に安全なリプレースを提供	P500
802.1X Port Authentication	IEEE802.1X によるポート認証の設定	P513
Management IP Filter	管理アクセスを許可される IP アドレスを設定	P531

4.8.1 ユーザーアカウント

管理アクセスのための基本的なコマンドです。管理アクセスに関するその他の設定に関しては、P404 「password」や P474 「認証シーケンス」、P513 「802.1x ポート認証コマンド」があります。

コマンド	機能	モード	ページ
enable password	各アクセスレベルのパスワードの設定	GC	P472
username	ログインするためのユーザ名の設定	GC	P473

enable password

Normal Exec レベルから Privileged Exec レベルに移行する際に使用します。"no" を前に置くことで初期設定に戻ります。

安全のためパスワードは初期設定から変更してください。変更したパスワードは忘れないようにして下さい。

文法

enable password [level *level* | 0 | 7] *password*

no enable password [level | *level*]

- level *level* — Privileged Exec へは Level 15 を入力します。
(Level 0-14 は使用しません)
- 0 | 7 — "0" は平文パスワードを、"7" は暗号化されたパスワードとなります。
- *password* — privileged Exec レベルへのパスワード
(最大 32 文字、大文字小文字は区別されます)

初期設定

初期設定レベル 15

初期設定パスワード "super"

コマンドモード

Global Configuration

コマンド解説

- パスワードを空欄にすることはできません。P370 「enable」コマンドを使用し Normal Exec から Privileged Exec へのコマンドモードの変更パスワードを入力して下さい。
- 暗号化されたパスワードはシステム起動時に設定ファイルを読み込む場合や TFTP サーバにダウンロードする場合のためにテキスト（平文）パスワードとの互換性があります。暗号化されたパスワードを手動で生成する必要はありません。

例

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

関連するコマンド

enable (P370)

authentication enabled (P474)

username

ログインする際のユーザ名及びパスワードの設定を行います。"no" を前に置くことでユーザ名を削除します。

文法

username *name* [access-level *level* | nopassword | password <0 | 7> *password*]

no username *name*

- *name* — ユーザ名（最大 8 文字。大文字と小文字は区別されます）。最大ユーザ数：16 ユーザ
- access-level *level* — ユーザレベルの設定
本機には 2 種類のアクセスレベルがあります：0: Normal Exec、15: Privileged Exec
- nopassword — ログインパスワードが必要ない場合
- <0 | 7> — "0" は平文パスワードを、"7" は暗号化されたパスワードとなります。
- password *password* — ユーザ用のパスワード（最大 32 文字。大文字と小文字は区別されます）

初期設定

- 初期設定のアクセスレベルは Normal Exec レベルです。
- 初期設定のユーザ名とパスワードは以下の通りです。

ユーザ名	アクセスレベル	パスワード
guest	0	guest
admin	15	admin

コマンドモード

Global Configuration

コマンド解説

暗号化されたパスワードはシステム起動時に設定ファイルを読み込む場合や TFTP サーバにダウンロードする場合のためにテキスト（平文）パスワードとの互換性があります。暗号化されたパスワードを手動で生成する必要はありません。

例

本例は、ユーザへのアクセスレベルとパスワードの設定を示しています。

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

4.8.2 認証シーケンス

管理アクセス用システムへのユーザログイン認証を行うため、3つの認証メソッドを指定することが可能です。ここで解説するコマンドは認証メソッドとシーケンスを定義するために使用します。

コマンド	機能	モード	ページ
authentication enable	コマンドモード変更時の認証方式と優先順位の設定	GC	P475
Authentication login	認証方法と優先順位の設定	GC	P475

authentication enable

"enable" コマンド (P370) で Exec モードから Privileged Exec モードへ変更する場合の、ログイン認証方法及び優先順位を設定します。"no" を前に置くことで初期設定に戻します。

文法

authentication enable <local | radius | tacacs >

no authentication enable

- local — ローカル認証を使用します
- radius — RADIUS サーバ認証を使用します
- tacacs — TACACS+ サーバ認証を使用します

初期設定

Local

コマンドモード

Global Configuration

コマンド解説

- RADIUS では UDP、TACACS+ では TCP を使用します。UDP はベストエフォート型の接続ですが、TCP は接続確立型の接続となります。また、RADIUS 暗号化はクライアントからサーバへのアクセス要求パケットのパスワードのみが暗号化されます。
- RADIUS 及び TACACS+ ログイン認証は各ユーザ名とパスワードに対しアクセスレベルを設定することができます。ユーザ名とパスワード、アクセスレベルは認証サーバ側で設定することができます。
- 3つの認証方式を1つのコマンドで設定することができます。例えば、"authentication enable radius tacacs local" とした場合、ユーザ名とパスワードを RADIUS サーバに対し最初に確認します。RADIUS サーバが利用できない場合、TACACS+ サーバにアクセスします。TACACS+ サーバが利用できない場合はローカルのユーザ名とパスワードを利用します。

例

```
Console(config)#authentication enable radius
Console(config)#
```

関連するコマンド

enable password (P370) — コマンドモード変更のためのパスワードの設定

Authentication login

ログイン認証方法及び優先順位を設定します。"no" を前に置くことで初期設定に戻します。

文法

authentication login <local | radius | tacacs>

no authentication login

- local — ローカル認証を使用します
- radius — RADIUS サーバ認証を使用します
- tacacs — TACACS+ サーバ認証を使用します

初期設定

Local のみ

コマンドモード

Global Configuration

コマンド解説

- RADIUS では UDP、TACACS+ では TCP を使用します。UDP はベストエフォート型の接続ですが、TCP は接続確立型の接続となります。また、RADIUS 暗号化はクライアントからサーバへのアクセス要求パケットのパスワードのみが暗号化されます。
- RADIUS 及び TACACS+ ログイン認証は各ユーザ名とパスワードに対しアクセスレベルを設定することができます。ユーザ名とパスワード、アクセスレベルは認証サーバ側で設定することができます。
- 3 つの認証方式を 1 つのコマンドで設定することができます。例えば、"authentication login radius tacacs local" とした場合、ユーザ名とパスワードを RADIUS サーバに対し最初に確認します。RADIUS サーバが利用できない場合、TACACS+ サーバにアクセスします。TACACS+ サーバが利用できない場合はローカルのユーザ名とパスワードを利用します。

例

```
Console(config)#authentication login radius
Console(config)#
```

関連するコマンド

username (P473) — ローカルユーザ名とパスワードの設定

4.8.3 Radius クライアントコマンド

RADIUS(Remote Authentication Dial-in User Service) は、ネットワーク上の RADIUS 対応デバイスのアクセスコントロールを認証サーバにより集中的に管理することができます。認証サーバは複数のユーザ名 / パスワードと各ユーザの本機へのアクセスレベルを管理するデータベースを保有しています。

コマンド	機能	モード	ページ
radius-server acct-port	RADIUS サーバネットワークポートの設定	GC	P476
radius-server auth-port	RADIUS サーバネットワークポートの設定	GC	P477
radius-server host	RADIUS サーバの設定	GC	P476
radius-server key	RADIUS 暗号キーの設定	GC	P479
radius-server retransmit	リトライ回数の設定	GC	P479
radius-server timeout	認証リクエストの間隔の設定	GC	P480
show radius-server	RADIUS 関連設定情報の表示	PE	P480

radius-server acct-port

アカウントメッセージに使用する、RADIUS サーバネットワークポートの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

radius-server port acct-port *port_number*

no radius-server acct-port

- port_number* — アカウンティングメッセージに使用される、RADIUS サーバ認証用 UDP ポート番号 (範囲 : 1-65535)

初期設定

1813

コマンドモード

Global Configuration

例

```
Console(config)#radius-server acct-port 181
Console(config)#
```

radius-server auth-port

アカウントメッセージに使用する、RADIUS サーバネットワークポートの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

radius-server port auth-port *port_number*

no radius-server auth-port

- *port_number* — 認証メッセージに使用される、RADIUS サーバ認証用 UDP ポート番号 (範囲：1-65535)

初期設定

1812

コマンドモード

Global Configuration

例

```
Console(config)#radius-server auth-port 181
Console(config)#
```

radius-server host

プライマリ / バックアップ RADIUS サーバ、及び各サーバの認証パラメータの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

radius-server *index* **host** { *host_ip_address* } { *auth-port* *auth-port* } { *acct-port* *acct-port* } { *Timeout* *Timeout* } { *retransmit* *retransmit* } { *key* *key* }

no radius-server *index*

- *index* — サーバを 5 つまで設定できます。指定したサーバの順に、サーバが応答するかタイムアウトがくるまでリクエストを送信します。
- *host_ip_address* — RADIUS サーバの IP アドレス
- *auth-port* — 認証メッセージに使用される UDP ポート（範囲：1-65535）
- *acct-port* — アカウンティングメッセージに使用される UDP ポート（範囲：1-65535）
- *key* — クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入られません（最大 48 文字）

初期設定

- *auth-port* : 1812
- *acct-port* : 1813
- *timeout* : 5 秒
- *retransmit* : 2

コマンドモード

Global Configuration

例

```
Console(config)#radius-server 1 host 192.168.1.20 auth-port 181 timeout  
10 retransmit 5 key green  
Console(config)#
```

radius-server key

RADIUS 暗号キーを設定します。"no" を前に置くことで初期設定に戻します。

文法

radius-server key *key_string*

no radius-server key

- *key_string* — クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入れられません（最大 48 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

リトライ数を設定します。"no" を前に置くことで初期設定に戻します。

文法

radius-server retransmit *number-of-retries*

no radius-server retransmit

- *number-of-retries* — スイッチが RADIUS サーバ経由で、認証ログオンを試みる回数（範囲：1-30）

初期設定

2

コマンドモード

Global Configuration

例

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

RADIUS サーバへの認証要求を送信する間隔を設定します。"no" を前に置くことで初期設定に戻します。

文法

radius-server timeout *number_of_seconds*

no radius-server timeout

- *number_of_seconds* — サーバからの応答を待ち、再送信を行うまでの時間（秒）
（範囲：1-65535）

初期設定

5

コマンドモード

Global Configuration

例

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

現在の RADIUS サーバ関連の設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
  Authentication Port Number : 1812
  Accounting Port Number    : 1813
  Retransmit Times          : 2
  Request Timeout           : 10
Server 1:
  Server IP Address         : 192.168.1.25
  Authentication Port Number : 10
  Accounting Port Number    : 11
  Retransmit Times          : 2
  Request Timeout           : 10
Radius Server Group:
Group Name      Member Index
-----
radius          1
Console#
```

4.8.4 TACACS+ クライアントコマンド

TACACS+(Terminal Access Controller Access Control System) は、ネットワーク上の TACACS+ 対応のデバイスのアクセスコントロールを認証サーバにより集中的に行うことができます。認証サーバは複数のユーザ名 / パスワードと各ユーザの本機へのアクセスレベルを管理するデータベースを保有しています。

コマンド	機能	モード	ページ
tacacs-server	TACACS+ サーバとオプションパラメータの指定	GC	P481
tacacs-server host	TACACS+ サーバの設定	GC	P482
tacacs-server key	TACACS+ 暗号キーの設定	GC	P482
tacacs-server port	TACACS+ サーバのポートの設定	GC	P483
show tacacs-server	TACACS+ 関連設定情報の表示	GC	P483

tacacs-server

TACACS+ サーバとその他のオプションパラメータを指定します。"no" を前に置くことでサーバを削除するか、設定を初期値に戻します。

文法

tacacs-server *index* host *host_ip_address* { port *port_number* } { key *key* }

no tacacs-server *index*

- *index* —サーバのインデックス番号を指定（範囲：1）
- *host_ip_address* — TACACS+ サーバの IP アドレス
- *port_number* — 認証メッセージに使用される TCP ポート（範囲：1-65535）
- *key* — クライアントへの認証ログインアクセスのための暗号キー。スペースは入れられません。（範囲：48 文字）

初期設定

10.11.12.13

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server 1 host 192.168.1.25
Console(config)#
```

tacacs-server host

TACACS+ サーバの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

tacacs-server *index* **host** *host_ip_address*

no tacacs-server *index*

- *host_ip_address* — TACACS+ サーバの IP アドレス

初期設定

10.11.12.13

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server 1 host 192.168.1.25
Console(config)#
```

tacacs-server key

TACACS+ 暗号キーを設定します。"no" を前に置くことで初期設定に戻します。

文法

tacacs-server **key** *key_string*

no tacacs-server **key**

- *key_string* — クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入れられません（最大 48 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server key green
Console(config)#
```


tacacs-server port

TACACS+ サーバのポートの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

tacacs-server port *port_number*
no tacacs-server port

- *port_number* — TACACS+ サーバの認証用 TCP ポート番号 (範囲：1-65535)

初期設定

49

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server port 181
Console(config)#
```

show tacacs-server

現在の TACACS+ サーバ関連の設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show tacacs-server

Remote TACACS+ Server Configuration:

Global Settings:
  Server Port Number : 49

Server 1:
  Server IP Address   : 192.168.1.3
  Server Port Number : 49

Tacacs Server Group:
Group Name            Member Index
-----
tacacs+               1
Console#
```

4.8.5 AAA（認証・許可・アカウントティング）コマンド

オーセンティケーション、オーソライゼーション、アカウントティング（AAA）機能はスイッチ上でアクセス制御を行うための主要なフレームワークを規定します。AAA 機能を使用するにはネットワーク上で RADIUS サーバー、もしくは TACACS+ サーバーを構成することが必要です。

コマンド	機能	モード	ページ
aaa accounting dot1x	802.1X サービスのアカウントティングを有効	GC	P486
aaa accounting exec	Exec モードコマンドのアカウントティングを有効	GC	P486
aaa accounting update	定期的なアップデートをアカウントティングサーバへ送信	GC	P487
aaa authorization exec	Exec セッションの許可を有効	GC	P487
aaa group server	グループサーバ名の設定	GC	P488
server	グループリスト内サーバの IP アドレスを設定	SG	P488
accounting dot1x	アカウントティングメソッドをインタフェースへ適用	IC	P489
accounting exec	アカウントティングメソッドをローカルコンソール、Telnet、SSH 接続へ適用	Line	P490
authorization exec	許可メソッドをローカルコンソール、Telnet、SSH 接続へ適用	Line	P491
show accounting	アカウントティング情報の表示	PE	P492

aaa accounting dot1x

ネットワークアクセスのために要求された 802.1X アカウンティングサービスを有効にします。"no" を前に置くことで、機能を無効にします。

文法

aaa accounting dot1x < default | *method-name* > start-stop group
<radius | tacacs+ |*server-group*>

no aaa accounting dot1x <default | *method-name*>

- default — サービスリクエストの、デフォルトアカウンティングメソッドを指定します
- *method-name* — サービスリクエストのアカウンティングメソッドを指定します。
(範囲：1-255 文字)
- start-stop — 開始から停止時までのアカウンティングを記録します。
- group — 使用するサーバグループを指定します
 - radius — 設定された全ての RADIUS+ ホストを指定 (P481 参照)
 - tacacs+ — 設定された全ての TACACS+ ホストを指定 (P481 参照)
 - *server-group* — aaa グループサーバに設定されたサーバグループの名前を指定 (P488 参照) (範囲：1-255 文字)

初期設定

アカウンティング：無効

サーバ：未指定

コマンドモード

Global Configuration

コマンド解説

- default および *method-name* フィールドは、指定された RADIUS または TACACS+ サーバに設定されたアカウンティングメソッドを記述するためだけに使用され、実際には、使用するメソッドについての情報をサーバへ送りません。

例

```
Console(config)#aaa accounting dot1x default start-stop group radius
Console(config)#
```

aaa accounting exec

ネットワークアクセスのために要求された Exec サービスのアカウントリングを有効にします。"no" を前に置くことで、機能を無効にします。

文法

aaa accounting exec < default | method-name > start-stop group
<radius | tacacs+ |server-group>

no aaa accounting exec <default | method-name>

- default — サービスリクエストの、デフォルトアカウントリングメソッドを指定します
- method-name — サービスリクエストのアカウントリングメソッドを指定します。
(範囲：1-255 文字)
- start-stop — 開始から停止時までのアカウントリングを記録します。
- group — 使用するサーバグループを指定します
 - radius — RADIUS サーバに設定された全ての RADIUS ホスト (P476 参照)
 - tacacs+ — TACACS+ サーバに設定された全ての TACACS+ ホスト
(P481 参照)
 - server-group — aaa グループサーバに設定されたサーバグループの名前を指定
(P488 参照)

初期設定

アカウントリング：無効

サーバ：未指定

コマンドモード

Global Configuration

例

```
Console(config)#aaa accounting exec default start-stop group  
tacacs+  
Console(config)#
```

aaa accounting update

アカウントिंगサーバへの定期的な更新を有効にします。"no" を前に置くことで、機能を無効にします。

文法

aaa accounting update { *periodic interval* }
no aaa accounting update

- *interval* — サーバへアカウントングレコードを送信する間隔を指定します
(範囲：1-2147483647 分)

初期設定

1 分

コマンドモード

Global Configuration

例

```
Console(config)#aaa accounting update periodic 30  
Console(config)#
```

aaa authorization exec

Exec アクセスの認可を有効にします。no" を前に置くことで、機能を無効にします。

文法

aaa authorization exec <default | *method-name*> group <tacacs+ | *server-group*>
no aaa authorization exec < default | *method-name* >

- default — Exec アクセスの、デフォルト認可メソッドを指定します
- *method-name* — メソッド名を指定します (範囲：1-255 文字)
- group — 使用するサーバグループを指定します
 - tacacs+ — TACACS+ サーバに設定された全ての TACACS+ ホスト (P481 参照)
 - *server-group* — aaa グループサーバに設定されたサーバグループの名前を指定 (P488 参照) (範囲：1-255 文字)

初期設定

認証：無効

サーバ：未指定

コマンドモード

Global Configuration

例

```
Console(config)#aaa authorization exec default group tacacs+  
Console(config)#
```

aaa group server

セキュリティサーバホストのグループ名を設定します。"no" を前に置くことで初期設定に戻します。

文法

aaa group server < radius | tacacs+ > *group-name*

no aaa group server < radius | tacacs+ > *group-name*

- radius — RADIUS サーバグループ
- tacacs+ — TACACS+ サーバグループ
- *group-name* — セキュリティサーバグループ名（範囲：1-7 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

server

セキュリティサーバを AAA サーバグループに追加します。"no" を前に置くことで、グループからサーバを削除します。

文法

server < *index* | *ip-address* >

no server < *index* | *ip-address* >

- *index* — サーバインデックスを指定します（範囲：RADIUS 1-5 TACACS+ 1）
- *ip-address* —サーバ IP アドレスを指定します

初期設定

なし

コマンドモード

Server Group Configuration

例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

accounting dot1x

インタフェースに、802.1x サービスリクエストのアカウントिंगメソッドを適用します。
no" を前に置くことで、機能を無効にします。

文法

accounting dot1x < default | *list-name* >

no accounting dot1x

- **default** — "aaa accounting dot1x" コマンドで作成された、デフォルトメソッドリストを指定します (P486 参照)
- ***list-name*** — "aaa accounting dot1x" コマンドで作成された、メソッドリストを指定します。 (P485 参照)

初期設定

なし

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

accounting exec

ローカルコンソールまたは Telnet 接続にアカウントिंगメソッドを適用します。no" を前に置くことで、機能を無効にします。

文法

accounting exec < default | *list-name* >

no accounting exec

- *default*— "aaa accounting dot1x" コマンドで作成された、デフォルトメソッドリストを指定します (P486 参照)
- *list-name*— "aaa accounting dot1x" コマンドで作成された、メソッドリストを指定します。

初期設定

なし

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#
```


authorization exec

ローカルコンソールまたは Telnet 接続に認可メソッドを適用します。no" を前に置くことで、機能を無効にします。

文法

authorization exec < default | *list-name* >

no authorization exec

- default — "aaa authorization exec" で作成されたデフォルトメソッドリスト (P487 参照)
- *list-name* — "aaa accounting dot1x" コマンドで作成された、メソッドリストを指定します。

初期設定

なし

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#
```

show accounting

機能ごと、またはポートごとに、現在のアカウンティング設定情報を表示します。

文法

show accounting {commands { *level* } | dot1x {statistics { username *user-name* | interface *interface* } } | exec { statistics } } | statistics }

- **commands** — 特権レベルコマンドアカウンティング情報の表示
- **level** — 指定されたコマンドレベルのコマンドアカウンティング情報を表示
- **dot1x** — dot1x アカウンティング情報の表示
- **exec** — exec アカウンティング情報の表示
- **statistics** — アカウンティング記録の表示
- **user-name** — 指定したユーザーのアカウンティング記録の表示
- **interface**
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show accounting
Accounting Type : dot1x
  Method List   : default
  Group List    : radius
  Interface     :

Accounting Type : EXEC
  Method List   : default
  Group List    : tacacs+
  Interface     :

Console#
```

4.8.6 Web サーバーコマンド

コマンド	機能	モード	ページ
ip http port	Web インタフェースに使用するポートの設定	GC	P493
ip http server	管理用 Web インタフェースの使用	GC	P494
ip http secure-server	セキュア HTTP (HTTPS) サーバの使用	GC	P495
ip http secure-port	HTTPS 接続に使用するポートの設定	GC	P495

ip http port

Web インタフェースでアクセスする場合の TCP ポート番号を指定します。"no" を前に置くことで初期設定に戻ります。

文法

ip http port *port-number*

no ip http port

- *port-number* — Web インタフェースに使用する TCP ポート (1-65535)

初期設定

80

コマンドモード

Global Configuration

例

```
Console(config)#ip http port 769
Console(config)#
```

関連するコマンド

ip http server (P494)

show system (P383)

コマンドラインインタフェース

認証コマンド

ip http server

Web ブラウザから本機の設定、及び設定情報の閲覧を可能にします。
"no" を前に置くことで本機能は無効となります。

文法

ip http server
no ip http server

初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#ip http server  
Console(config)#
```

関連するコマンド

ip http port (P493)
show system (P383)

ip http secure-server

Web インタフェースを使用し本機への暗号化された安全な接続を行うために、Secure Socket Layer (SSL) を使用した Secure hypertext transfer protocol (HTTPS) を使用するためのコマンドです。"no" を前に置くことで本機能を無効にします。

文法

ip http secure-server

no ip http secure-server

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- HTTP 及び HTTPS サービスはそれぞれのサービスを個別に有効にすることが可能です。
- HTTPS を有効にした場合は Web ブラウザのアドレスバーに https://device[: ポート番号] と入力します。
- HTTPS を有効にした場合、以下の手順で接続が確立されます：
 - クライアントはサーバのデジタル証明書を使用し、サーバを確認します。
 - クライアントおよびサーバは、接続のために使用する 1 セットのセキュリティ・プロトコルを協定します。
 - クライアントおよびサーバは、データを暗号化し解読するためのセッション・キーを生成します。
- クライアントとサーバ間の暗号化されたアクセスが確立した場合、Internet Explorer 5.x 以上及び Netscape Navigator 6.2 以上、Mozilla Firefox 2.0.0.0 以上のステータスバーに鍵マークが表示されます。

※セキュアサイト証明の詳細は P195 「サイト証明書の置き換え」を参照して下さい。

例

```
Console(config)#ip http secure-server
Console(config)#
```

関連するコマンド

ip http secure-port (P495)

copy tftp https-certificate (P387)

show system (P383)

ip http secure-port

コマンドラインインタフェース

認証コマンド

Web インタフェースからの HTTPS/SSL 接続で使用する UDP ポートを設定することができます。"no" を前に置くことで初期設定に戻ります。

文法

ip http secure-port *port_number*

no ip http secure-port

- *port_number* — HTTPS/SSL に使用する UDP ポート番号 (1-65535)

初期設定

443

コマンドモード

Global Configuration

コマンド解説

- HTTP と HTTPS で同じポートは設定できません。
- HTTPS ポート番号を設定した場合、HTTPS サーバにアクセスするためには URL にポート番号を指定する必要があります。(https://device:[ポート番号])

例

```
Console(config)#ip http secure-port 1000
Console(config)#
```

関連するコマンド

ip http secure-server (P495)

show system (P383)

4.8.7 Telnet サーバコマンド

コマンド	機能	モード	ページ
ip telnet max-sessions	同時にシステムへ接続可能な Telnet セッションの最大数を設定	GC	P497
ip telnet port	Telnet インタフェースが使用するポート番号を指定	GC	P498
ip telnet server	管理用 Telnet インタフェースの使用を許可	GC	P498
show ip telnet	Telnet サーバ設定を表示	GC	P499

ip telnet max-sessions

同時にシステムへ接続可能な Telnet セッションの最大数を設定します。"no" を前に置くことで設定を初期状態へ戻します。

文法

ip telnet max-sessions *session-count*

no ip telnet max-sessions

- *session-count* — 許可される Telnet の最大セッション数（範囲：0-4）

初期設定

4 セッション

コマンドモード

Global Configuration

例

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

ip telnet port

Telnet インタフェースが使用する TCP ポート番号を指定します。"no" を前に置くことで設定を初期状態へ戻します。

文法

ip telnet port *port* *port-number*

no ip telnet port

- *port* — Telnet インタフェースが使用する TCP ポート（範囲：1-65535）

初期設定

23

コマンドモード

Global Configuration

例

```
Console(config)#ip telnet port 123
Console(config)#
```

ip telnet server

Telnet から本機の設定、及び設定情報の閲覧を可能にします。"no" を前に置くことで本機能は無効となります。

文法

ip telnet server

no ip telnet server

初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#ip telnet server
Console(config)#
```

show ip telnet

Telnet サーバの設定情報を表示します。

文法

show ip telnet

コマンドモード

Normal Exec、Privileged Exec

例

```
Console#show ip telnet
IP Telnet Configuration:

Telnet Status: Enabled
Telnet Service Port: 123
Telnet Max Session: 1
Console#
```

4.8.8 Secure Shell コマンド

ここでは、SSH サーバを設定するためのコマンドを解説します。

なお、SSH 経由での管理アクセスを行なうためには、クライアントに SSH クライアントをインストールする必要があります。

[注意] 本機では SSH Version1.5 と 2.0 をサポートしています。

コマンド	機能	モード	ページ
ip ssh authentication-retries	クライアントに許可するリトライ数の設定	GC	P503
ip ssh server	SSH サーバの使用	GC	P504
ip ssh server-key size	SSH サーバキーサイズの設定	GC	P505
ip ssh timeout	SSH サーバの認証タイムアウト設定	GC	P506
copy tftp public-key	ユーザ公開キーの TFTP サーバから本機へコピー	PE	P387
delete public-key	特定ユーザの公開キーの削除	PE	P507
disconnect	ライン接続の終了	PE	P408
ip ssh crypto host-key generate	ホストキーの生成	PE	P508
ip ssh crypto zeroize	RAM からのホストキーの削除	PE	P509
ip ssh save host-key	RAM からフラッシュメモリへのホストキーの保存	PE	P509
show ip ssh	SSH サーバの状態の表示及び SSH 認証タイムアウト時間とリトライ回数の設定	PE	P510
show public-key	特定のユーザ又はホストの公開キーの表示	PE	P511
show ssh	SSH セッション状態の表示	PE	P512
show users	SSH ユーザ、アクセスレベル、公開キータイプの表示	PE	P384

設定ガイドライン

本機の SSH サーバはパスワード及びパブリックキー認証をサポートしています。SSH クライアントによりパスワード認証を選択した場合、認証設定ページで設定したパスワードにより本機内、RADIUS、TACACS+ のいずれかの認証方式を用います。クライアントがパブリックキー認証を選択した場合には、クライアント及び本機に対して認証キーの設定を行う必要があります。公開暗号キー又はパスワード認証のどちらかを使用するに関わらず、本機上の認証キー（SSH ホストキー）を生成し、SSH サーバを有効にする必要があります。

SSH サーバを使用するには以下の手順で設定を行ないます。

- (1) **ホストキーペアの生成** — "ip ssh crypto host-key generate" コマンドによりホストパブリック / プライベートキーのペアを生成します。
- (2) **ホスト公開キーのクライアントへの提供** — 多くの SSH クライアントは、本機との自動的に初期接続設定中に自動的にホストキーを受け取ります。そうでない場合には、手動で管理端末のホストファイルを作成し、ホスト公開キーを置く必要があります。ホストファイル中の公開暗号キーは以下の例のように表示されます。


```
10.1.0.54 1024 35
15684995401867669259333946775054617325313674890836547254150202455931998685443583
61651999923329781766065830956
1082591321289023376546801726272571413428762941301196195566782
59566410486957427888146206519417467729848654686157177393901647793559423035774130
9802273708779454524083971752646358058176716709574804776117
```
- (3) **クライアント公開キーの本機への取り込み** — P389 「copy」 コマンドを使用し、SSH クライアントの本機の管理アクセスに提供される公開キーを含むファイルをコピーします。クライアントへはこれらのキーを使用し、認証が行なわれます。現在のファームウェアでは以下のような UNIX 標準フォーマットのファイルのみ受け入れることが可能です。


```
1024 35
13410816856098939210409449201554253476316419218729589211431738800555361616310517
75940838686311092912322268285192543746031009371877211996963178136627741416898513
20491172048303392543241016379975923714490119380060902539484084827178194372288402
533115952134861022902978982721353267131629432532818915045306393916643
steve@192.168.1.19
```
- (4) **オプションパラメータの設定** — SSH 設定ページで、認証タイムアウト、リトライ回数、サーバキーサイズなどの設定を行なってください。
- (5) **SSH の有効化** — "ip ssh server" コマンドを使用し、本機の SSH サーバを有効にして下さい。
- (6) **Challenge/Response 認証** — SSH クライアントが本機と接続しようとした場合、SSH サーバはセッションキーと暗号化方式を調整するためにホストキーペアを使用します。本機上に保存された公開キーに対応するプライベートキーを持つクライアントのみアクセスすることができます。

以下のような手順で認証プロセスが行なわれます。

- a. クライアントが公開キーを本機に送ります。
- b. 本機はクライアントの公開キーとメモリに保存されている情報を比較します。
- c. 一致した場合、公開キーを利用し本機はバイトの任意のシーケンスを暗号化し、その値をクライアントに送信します。
- d. クライアントはプライベートキーを使用してバイトを解読し、解読したバイトを本機に送信します。

コマンドラインインタフェース

認証コマンド

- e. 本機は、元のバイトと解読されたバイトを比較します。2つのバイトが一致した場合、クライアントのプライベートキーが許可された公開キーに対応していることを意味し、クライアントが認証されます。

[注意] パスワード認証と共に SSH を使用する場合にも、ホスト公開キーは初期接続時又は手動によりクライアントのホストファイルに与えられます。但し、クライアントキーの設定を行なう必要はありません。

ip ssh authentication-retries

SSH サーバがユーザの再認証を行なう回数を設定します。"no" を前に置くことで初期設定に戻ります。

文法

ip ssh authentication-retries *count*

no ip ssh authentication-retries

- *count* — インタフェースがリセット後、認証を行なうことができる回数
(設定範囲：1-5)

初期設定

3

コマンドモード

Global Configuration

例

```
Console(config)#ip ssh authentication-retries 2
Console(config)#
```

関連するコマンド

show ip ssh (P510)

ip ssh server

SSH サーバの使用を有効にします。"no" を前に置くことで設定を無効にします。

文法

ip ssh server

no ip ssh server

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 最大 4 セッションの同時接続をサポートします。最大セッション数は Telnet 及び SSH の合計数です。
- SSH サーバはクライアントとの接続を確立する際に DAS 又は RAS を使ったキー交換を行います。その後、DES (56-bit) または 3DES (168-bit) を用いてデータの暗号化を行います。
- SSH サーバを有効にする前に、ホストキーを生成する必要があります。

例

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

関連するコマンド

ip ssh crypto host-key generate (P508)

show ssh (P512)

ip ssh server-key size

SSH サーバキーサイズを設定します。"no" を前に置くことで初期設定に戻ります。

文法

ip ssh server-key size *key-size*

no ip ssh server-key size

- *key-size* — サーバキーのサイズ（設定範囲：512-896bits）

初期設定

768 bits

コマンドモード

Global Configuration

コマンド解説

- サーバキーはプライベートキーとなり本機以外との共有はしません。
- SSH クライアントと共有するホストキーサイズは 1024bit に固定されています。

例

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

ip ssh timeout

SSH サーバのタイムアウト時間を設定します。"no" を前に置くことで初期設定に戻ります。

文法

ip ssh timeout *seconds*

no ip ssh timeout

- *seconds* — SSH 接続調整時のクライアント応答のタイムアウト時間（設定範囲：1-120）

初期設定

10 秒

コマンドモード

Global Configuration

コマンド解説

タイムアウトは SSH 情報交換時のクライアントからの応答を本機が待つ時間の指定を行います。SSH セッションが確立した後のユーザ入力のタイムアウトは vty セッションへの "exec-timeout" コマンドを使用します。

例

```
Console(config)#ip ssh timeout 60
Console(config)#
```

関連するコマンド

exec-timeout (P401)

show ip ssh (P510)

delete public-key

特定のユーザパブリックキーを削除します。

文法

delete public-key *username* { dsa | rsa }

- *username* — SSH サーバ名（設定範囲：1-8 文字）
- dsa — DSA 公開キータイプ
- rsa — RSA 公開キータイプ

初期設定

DSA 及び RSA キーの両方の削除

コマンドモード

Privileged Exec

例

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

パブリック及びプライベートのホストキーペアの生成を行ないます。

文法

ip ssh crypto host-key generate < dsa | rsa >

- dsa — DSA (Version2) キータイプ
- rsa — RSA (Version1) キータイプ

初期設定

DSA 及び RSA キーペア両方の生成

コマンドモード

Privileged Exec

コマンド解説

- 本コマンドはホストキーペアをメモリ (RAM) に保存します。" ip ssh save host-key" コマンドを使用してホストキーペアをフラッシュメモリに保存できます。
- 多くの SSH クライアントは接続設定時に自動的にパブリックキーをホストファイルとして保存します。そうでない場合には、手動で管理端末のホストファイルを作成し、ホスト公開キーを置く必要があります。
- SSH サーバは、接続しようとするクライアントとセッションキー及び暗号化方法を取り決めるためにホストキーを使用します。

例

```
Console#ip ssh crypto host-key generate dsa
Console#
```

関連するコマンド

ip ssh crypto zeroize (P509)

ip ssh save host-key (P509)

ip ssh crypto zeroize

ホストキーをメモリ (RAM) から削除します。

文法

ip ssh crypto zeroize < dsa | rsa >

- dsa — DSA キータイプ
- rsa — RSA キータイプ

初期設定

DSA 及び RSA キーの両方を削除

コマンドモード

Privileged Exec

コマンド解説

- RAM からホストキーを削除します。" no ip ssh save host-key" コマンドを使用することでフラッシュメモリからホストキーを削除できます。
- 本コマンドを使用する際は事前に SSH サーバを無効にして下さい。

例

```
Console#ip ssh crypto zeroize dsa
Console#
```

ip ssh save host-key

ホストキーを RAM からフラッシュメモリに保存します。

文法

ip ssh save host-key

初期設定

DSA と RSA キーの両方を保存

コマンドモード

Privileged Exec

例

```
Console#ip ssh save host-key
Console#
```

関連するコマンド

ip ssh crypto host-key generate (P508)

コマンドラインインタフェース

認証コマンド

show ip ssh

このコマンドを使用することで SSH サーバの設定状況を閲覧することができます。

コマンドモード

Privileged Exec

例

```
Console#show ip ssh
SSH Enabled - version 1.99
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

show public-key

特定のユーザ又はホストの公開キーを表示します。

文法

show public-key { user { *username* } | host }

- *username* — SSH ユーザ名（範囲：1-8 文字）

初期設定

すべての公開キーの表示

コマンドモード

Privileged Exec

コマンド解説

- パラメータを設定しない場合には、すべてのキーが表示されます。キーワードを入力し、ユーザ名を指定しない場合、すべてのユーザの公開キーが表示されます。
- RSA キーが表示された場合、最初のフィールドはホストキーサイズ (1024) となり、次のフィールドはエンコードされた公開指数 (35)、その後の値がエンコードされたモジュールとなります。DSA キーが表示された場合、最初のフィールドは SSH で使用される暗号化方式の DSS となり、その後の値がエンコードされたモジュールとなります。

例

```
Console#show public-key host
Host:
RSA:
1024 35
156849954018676692593339467750546173253136748908365472541502024559319986
854435836165199992332978176606583095861082591321289023376546801726272571
413428762941301196195566782595664104869574278881462065194174677298486546
861571773939016477935594230357741309802273708779454524083971752646358058
176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/
Dg0h2HxcYV44sXZ2JXhamLK6P8bvuiyacWbUW/
a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfvJlPdOkFgzLGMInvSNYQwiQXbKTbH0
Z4mUZpE85PWxDZMacNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEAsy5YWDC9
9ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR2G395Nly5Qd7ZDxfA9mCOFT/
yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/
Kjw6BmiFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/
ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOyDbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcF
Ru41bS2KV5LAWecsigF/+DjKGWtPNIQqabKgYCW2 o/
dVzX4Gg+yqdTlYmGA7fHGm8ARGeig4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
w0W
Console#
```

コマンドラインインタフェース

認証コマンド

show ssh

現在の SSH サーバへの接続状況を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ssh
Connection Version  State           Username  Encryption
0           2.0      Session-Started admin      ctos aes128-cbc-hmac-md5
                                stoc aes128-cbc-hmac-md5
Console#
```

項目	解説
Session	セッション番号 (0-3)
Version	SSH バージョン番号
State	認証接続状態 (値: Negotiation-Started, Authentication-Started, Session-Started)
Username	クライアントのユーザ名

4.8.9 802.1x ポート認証コマンド

本機では IEEE802.1X (dot1x) のポートベースアクセスコントロールをサポートし、ID とパスワードによる認証により許可されないネットワークへのアクセスを防ぐことができます。クライアントの認証は RADIUS サーバにより EAP(Extensible Authentication Protocol) を用いて行われます。

コマンド	機能	モード	ページ
通常コマンド			
dot1x default	dot1x の設定値をすべて初期設定に戻します。	GC	P516
dot1x eapol-pass-through	dot1x がグローバルで有効時、EAPOL フレームを STP 転送状態の全てのポートへパス	GC	P514
dot1x system-auth-control	dot1x をスイッチ全体に有効に設定	GC	P514
認証コマンド			
dot1x intrusion-action	認証失敗時の、侵入にたいするポート返答	IC	P515
dot1x max-req	認証プロセスを初めからやり直す前に認証プロセスを繰り返す最大回数	GC	P514
dot1x operation-mode	dot1x ポートへの接続可能ホスト数の設定	IC	P517
dot1x port-control	ポートへの dot1x モードの設定	IC	P518
dot1x re-authentication	全ポートへの再認証の強制	GC	P519
dot1x timeout quiet-period	max-req を超えた後、クライアントの応答を待つ時間	GC	P520
dot1x timeout re-authperiod	接続済みクライアントの再認証間隔の設定	GC	P520
dot1x timeout supp-timeout	スイッチが EAP パケットの再認証待機中の認証セッションの間の期間を設定	IC	P521
dot1x timeout tx-period	認証中の EAP パケットの再送信間隔の設定	GC	P522
dot1x re-authenticate	特定ポートへの再認証の強制	PE	P522
サブリカントコマンド			
dot1x identity profile	dot1x サブリカントユーザとパスワードの設定	GC	P523
dot1x max-start	ポートサブリカントが EAP スタートフレームをクライアントへ送信する最大時間数を設定	IC	P524
dot1x pae supplicant	インタフェースで dot1x サブリカントモードを有効化	IC	P525
dot1x timeout auth-period	サブリカントポートがオーセンティケータからの返答を待つ時間を設定	IC	P526
dot1x timeout held-period	最大スタートカウントが超えられた後、ポートがもう 1 つのオーセンティケータを探そうと試みる前に待つ時間を設定	IC	P527
情報表示コマンド			
show dot1x	dot1x 関連情報の表示	PE	P528

dot1x default

すべての dot1x の設定を初期設定に戻します。

文法

dot1x default

コマンドモード

Global Configuration

例

```
Console(config)#dot1x default
Console(config)#
```

dot1x eapol-pass-through

dot1x がグローバルで無効時、STP フォワーディング状態の全てのポートへ EAPOL フレームを渡します。"no" を前に置くことで初期設定に戻します。

文法

dot1x eapol-pass-through

no dot1x eapol-pass-through

初期設定

dot1x がグローバルで無効時、全ての EAPOL フレームを破棄。

コマンドモード

Global Configuration

コマンド解説

- この装置がネットワークの中間接点として機能し、dot1x 認証を行う必要が無い時、"dot1x eapol pass-through" コマンドは、認証サーバ上の他のスイッチからの EAPOL フレーム転送を行うために使用することが出来ます。それによって、認証プロセスがネットワークのエッジにあるスイッチによって依然実行されることを可能にします。
- この装置がエッジスイッチとして機能していて、接続されているクライアントが認証を必要としない場合、"no dot1x eapol-pass-through" コマンドを不必要な EAPOL トラフィックを破棄するために使用することが出来ます。

例

```
Console(config)#dot1x eapol-pass-through
Console(config)#
```


dot1x system-auth-control

スイッチが、802.1X ポート認証を使用できるよう設定します。"no" を前に置くことで初期設定に戻します。

文法

dot1x system-auth-control

no dot1x system-auth-control

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#dot1x system-auth-control
Console(config)#
```

dot1x intrusion-action

認証失敗時、全てのトラフィックをブロックするか、ポートのトラフィックをゲスト VLAN に割り当てるかを設定します。"no" を前に置くことで初期設定に戻します。

文法

dot1x intrusion-action < block-traffic | guest-vlan >

no dot1x intrusion-action

初期設定

block-traffic

コマンドモード

Interface Configuration

コマンド解説

- ・ ゲスト VLAN 割り当てを行うには、あらかじめ VLAN の設定を行い、"Active" にしてください。(P703 「VLAN」を参照) またゲスト VLAN として割り当てを行ってください。(P539 「network-access dynamic-qos」を参照)

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```

dot1x max-req

ユーザ認証のタイムアウトまでのクライアントへの EAP リクエストパケットの最大送信回数の設定を行います。"no" を前に置くことで初期設定に戻します。

文法

dot1x max-req *count*

no dot1x max-req

- *count* — 最大送信回数（範囲：1-10）

初期設定

2

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x operation-mode

IEEE802.1x 認証ポートに対して 1 台もしくは複数のホスト（クライアント）の接続を許可する設定を行います。キーワードなしで "no" を前に置くことで初期設定に戻ります。"multi-host max-count" キーワードと共に "no" を前に置くことで複数ホスト時の初期値 5 となります。

文法

dot1x operation-mode [single-host | multi-host {max-count *count* } | mac-based-auth]

no dot1x operation-mode { multi-host max-count }

- single-host — ポートへの 1 台のホストの接続のみを許可
- multi-host — ポートへの複数のホストの接続を許可
- max-count — 最大ホスト数
 - *count* — ポートに接続可能な最大ホスト数（設定範囲：1-1024、初期設定：5）
- mac-based-auth — このポートへの複数のホストのアクセスを許可（それぞれのホストが認証される必要があります）

初期設定

Single-host

コマンドモード

Interface Configuration

コマンド解説

- "max-count" パラメータは P518 「dot1x port-control」で "auto" に設定されている場合にのみ有効です。
- "multi-host" を設定すると、ポートに接続するホストのうちの 1 台のみが認証の許可を得られれば、他の複数のホストもネットワークへのアクセスが可能になります。逆に、接続するホスト再認証に失敗したり、EAPOL ログオフメッセージを送信した場合、他のホストも認証に失敗したことになります。
- "mac-based-auth" モードでは、ポートに接続されているそれぞれのホストが認証のを通る必要があります。このモードで稼動してるポートへのアクセスを許可されるホストの数は、セキュアアドレステーブルの使用可能なスペースによってのみ制限されます。

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x port-control

ポートに対して dot1x モードの設定を行います。

文法

dot1x port-control < auto | force-authorized | force-unauthorized >

no dot1x port-control

- auto — dot1x 対応クライアントに対して RADIUS サーバによる認証を要求します。
dot1x 非対応クライアントからのアクセスは許可しません。
- force-authorized — dot1x 対応クライアントを含めたすべてのクライアントのアクセスを許可します。
- force-unauthorized — dot1x 対応クライアントを含めたすべてのクライアントのアクセスを禁止します。

初期設定

force-authorized

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x re-authentication

全ポートでの周期的な再認証を有効にします。"no" を前に置くことで再認証を無効にします。

文法

dot1x re-authentication

no dot1x re-authentication

コマンドモード

Interface Configuration

コマンド解説

- 再認証プロセスは、接続されたクライアントのユーザ ID とパスワードを RADIUS サーバで照合します。再認証の間、クライアントはネットワークへの接続を維持し、プロセスは dot1x クライアントソフトウェアによって、透過的に処理されます。
もし再認証が失敗した場合のみ、ポートはブロックされるか、ユーザはゲスト VLAN に割り当てられます。(515 ページの「dot1x intrusion-action」を参照)
- 接続されたクライアントは、" dot1x timeout re-authperiod" コマンド (P520) で設定したインターバルの後、再認証されます。初期設定は 3600 秒です。

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

dot1x timeout quiet-period

EAP リクエストパケットの最大送信回数を過ぎた後、新しいクライアントの接続待機状態に移行するまでの時間を設定します。"no" を前に置くことで初期設定に戻します。

文法

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

- seconds* — 秒数 (範囲: 1-65535 秒)

初期設定

60 秒

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod

接続されたクライアントに再認証を要求する間隔を設定します。

文法

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

- *seconds* — 秒数（範囲：1-65535 秒）

初期設定

3600 秒

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

dot1x timeout supp-timeout

スイッチのインタフェースが EAP パケットを再送信する前に、クライアントから EAP リクエストへの返答待つ時間を設定します。"no" を前に置くことで設定を初期値に戻します。

文法

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

- *seconds* — 秒数（範囲：1-65535 秒）

初期設定

30 秒

コマンドモード

Interface Configuration

コマンド解説

- このコマンドは、EAP リクエスト /EAP identity フレーム以外のリクエストフレームのタイムアウトを設定します。dot1x 認証がポートで有効の場合、スイッチは、ポートリンクステータスが来た時に認証を開始します。それはクライアントへアイデンティティを要求するためと、その後に認証情報の 1 つ以上の要請を求めるため、EAP リクエスト /EAP identity フレームをクライアントへ送信します。また、要求された再認証のアクティブな接続の間、その他の EAP リクエストフレームをクライアントへ送ります

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout supp-timeout 300
Console(config-if)#
```

dot1x timeout tx-period

認証時に EAP パケットの再送信を行う間隔を設定します。"no" を前に置くことで初期設定に戻します。

文法

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

- *seconds* — 秒数（範囲：1-65535 秒）

初期設定

30 秒

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

dot1x re-authenticate

全ポート又は特定のポートでの再認証を強制的に行います。

文法

dot1x re-authenticate { *interface* }

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号（範囲：1-26）

コマンドモード

Privileged Exec

コマンド解説

- 再認証プロセスは、接続されたクライアントのユーザ ID とパスワードを RADIUS サーバで照合します。再認証の間、クライアントはネットワークへの接続を維持し、プロセスは dot1x クライアントソフトウェアによって、透過的に処理されます。
もし再認証が失敗した場合のみ、ポートはブロックされるか、ユーザはゲスト VLAN に割り当てられます。(515 ページの「dot1x intrusion-action」を参照)

例

```
Console#dot1x re-authenticate
Console#
```


dot1x identity profile

dot1x サプリカントユーザとパスワードを設定します。"no" を前に置くことで識別設定を削除します。

文法

dot1x identity profile [username *username* | password *password*]

no dot1x identity profile [username | password]

- *username* — サプリカントユーザ名を指定（範囲：1-8 文字）
- *password* — サプリカントパスワードを指定（範囲：1-8 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- グローバルサプリカント名とパスワードは、オーセンティケータから MD5 challenge への返答時、本機をサプリカントとして識別するために使用します。本機がネットワークの他のオーセンティケータヘクライアント認証リクエストを渡す時に、これらのパラメータを設定します。("dot1x pae supplicant" コマンド（P525）を参照）

例

```
Console(config)#dot1x identity profile username steve
Console(config)#dot1x identity profile password excess
Console(config)#
```

dot1x max-start

クライアントが 802.1X を認知しないクライアントを想定する前に、ポートサブリカントが EAP スタートフレームをクライアントへ送る最大数を設定します。"no" を前に置くことで初期設定に戻します。

文法

dot1x max-start *count*

no dot1x max-start

- *count* – EAP スタートフレームの最大数（範囲 1-65535）

初期設定

3

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-start 10
Console(config-if)#
```

dot1x pae supplicant

ポートの dot1x サプリカントモードを有効にします。"no" を前に置くことで、dot1x サプリカントモードをポートで無効にします。

文法

dot1x pae supplicant
no dot1x pae supplicant

初期設定

無効

コマンドモード

Interface Configuration

コマンド解説

- コントロールモードを "auto" ("dot1x port-control" コマンド (P518) を参照) に設定することで、本機は選択されたポートのオーセンティケータとして設定でき、コントロールモードを "force-authorized" に設定し、このコマンドで dot1x サプリカントモードを有効にすることで、他のポートのサブリカンとして設定できます。
- トランクのメンバーであるか、ポートで LACP が有効の場合、ポートを dot1x サプリカントとして設定することはできません。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x pae supplicant
Console(config-if)#
```

dot1x timeout auth-period

サブリカントポートがオーセンティケータからの返答を待つ時間を設定します。"no" を前に置くことで初期設定に戻します。

文法

dot1x timeout auth-period *seconds*
no dot1x timeout auth-period

- *seconds* — 秒数（範囲：1-65535）

初期設定

30 秒

コマンドモード

Interface Configuration

コマンド解説

- このコマンドはサブリカントが EAPOL-Start. 以外のパケットのオーセンティケータから返答を待つ時間を設定します。

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout auth-period 60
Console(config-if)#
```

dot1x timeout held-period

サブリカントポートがその証明書を再送の前に、新しいオーセンティケータを見つけるのを待つ時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

dot1x timeout held-period *seconds*

no dot1x timeout held-period

- *seconds* — 秒数（範囲：1-65535）

初期設定

60 秒

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout held-period 120
Console(config-if)#
```

dot1x timeout start-period

サブリカントポートがオーセンティケータへの EAPOL start フレームの再送を待つ時間。"no" を前に置くことで設定を初期状態に戻します。

文法

dot1x timeout start-period *seconds*

no dot1x timeout start-period

- *seconds* — 秒数（範囲：1-65535）

初期設定

30 秒

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout start-period 60
Console(config-if)#
```

show dot1x

本機または特定のインタフェースのポート認証に関連した設定状態の表示を行います。

文法

show dot1x { statistics | interface *interface* }

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 “1”
 - port* — ポート番号 (範囲: 1-26)

コマンドモード

Privileged Exec

コマンド解説

本コマンドで表示されるのは以下の情報です。

コマンド解説

本コマンドで表示されるのは以下の情報です。

- *Global 802.1X Parameters* — 本機全体に対する、802.1X ポート認証の有効 / 無効
- *Authenticator Parameters* — EAPOL pass-through の有効 / 無効を表示 (P514)
- *Supplicant Parameters* — スイッチがオーセンティケータから MD5 challenge へ返答する時に使用する、サブリカントユーザ名を表示 (P523)
- *802.1X Port Summary* — 各インタフェースのアクセスコントロールの設定値
 - Type — ポートアクセスコントロールの管理状態
 - Operation Mode — P517 「dot1x operation-mode」 の設定値
 - Mode — dot1x port-control で設定する dot1x モード (P518)
 - Authorized — 認証状態 (yes 又は n/a - not authorized)
- *802.1X Port Details* — 各インタフェースでのポートアクセスコントロール設定の詳細を表示します。以下の値が表示されます。
 - reauthentication - 周期的な再認証 (P519)
 - reauth-period - 接続されたクライアントに再認証を要求する間隔 (P520)
 - quiet-period - 最大送信回数超過後、新しいクライアントの接続待機状態に移行するまでの時間 (P520)
 - tx-period - 認証時に EAP パケットの再送信を行う間隔 (P522)
 - supplicant-timeout - クライアントのタイムアウト
 - server-timeout - サーバのタイムアウト
 - reauth max retries - 再認証の最大回数

- max request - ユーザ認証のタイムアウトまでの、ポートからクライアントへの EAP リクエストパケットの最大送信回数 (P516)
- Operation Mode - 802.1X 認証ポートに 1 台もしくは複数のホスト (クライアント) の接続が許可されているか
- Port-control - ポートの dot1x モードが "auto"、"force-authorized" 又は "force-unauthorized" のいずれになっているか (P518)
- Intrusion action- 認証失敗時、スイッチが全ての非 EAP トラックをブロックするか、ゲスト VLAN へのポートにトラフィックをアサインするかを設定 (P515)
- Supplicant - 認証されたクライアントの MAC アドレス
- *Authenticator State Machine* —
 - State — **現在の状態** (initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized)
 - Reauth Count — **再認証回数**
 - Current Identifier— 認証機能により、現行の認証接続を識別するために使用される整数値 (0-255)
- *Backend State Machine* —
 - State — **現在の状態**
(request、response、success、fail、timeout、idle、initialize)
 - Request Count — クライアントからの応答がない場合に送信される EAP リクエストパケットの送信回数
 - Identifier(Server) — 直近の EAP の成功 / 失敗又は認証サーバから受信したパケット
- *Reauthentication State Machine* —
 - State — **現在の状態** (initialize、reauthenticate)

例

```
Console#show dot1x
Global 802.1X Parameters
system-auth-control: enable

802.1X Port Summary

Port Name Status Operation Mode Mode Authorized
1/1 disabled Single-Host ForceAuthorized n/a
1/2 enabled Single-Host auto yes ...
1/26 disabled Single-Host ForceAuthorized n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
reauth-enabled: Enable
reauth-period: 1800
quiet-period: 30
tx-period: 40
supplicant-timeout: 30
server-timeout: 10
reauth-max: 2
max-req: 5
Status Authorized
Operation mode Single-Host
Max count 5
Port-control Auto
Supplicant 00-12-cf-49-5e-dc
Current Identifier 3
Intrusion action Guest VLAN

Authenticator State Machine
State Authenticated
Reauth Count 0

Backend State Machine
State Idle
Request Count 0
Identifier(Server) 2

Reauthentication State Machine
State Initialize
.
.
.
```


4.8.10 管理 IP フィルターコマンド

コマンド	機能	モード	ページ
management	管理アクセスを許可する IP アドレスを設定	GC	P531
show management	本機の管理アクセスに接続されているクライアントの表示	PE	P532

management

本機では管理アクセスに接続を許可するクライアントの IP アドレスの設定を行なうことができます。"no" を前に置くことで設定を削除します。

文法

management [all-client | http-client | snmp-client | telnet-client] *start-address* { *end-address* }

no management [all-client | http-client | snmp-client | telnet-client] *start-address* { *end-address* }

- all-client — SNMP/Web ブラウザ /Telnet クライアントの IP アドレス
- http-client — Web ブラウザクライアントの IP アドレス
- snmp-client — SNMP クライアントの IP アドレス
- telnet-client — Telnet クライアントの IP アドレス
- *start-address* — IP アドレス又は IP アドレスグループの最初の IP アドレス
- *end-address* — IP アドレスグループの最後の IP アドレス

初期設定

全てのアドレス

コマンドモード

Global Configuration

コマンド解説

- 設定以外の無効な IP アドレスから管理アクセスに接続された場合、本機は接続を拒否し、イベントメッセージをシステムログに保存し、トラップメッセージの送信を行ないます。
- SNMP、Web ブラウザ、Telnet アクセスへの IP アドレス又は IP アドレス範囲の設定は合計で最大 5 つまで設定可能です。
- SNMP、Web ブラウザ、Telnet の同一グループに対して IP アドレス範囲を重複して設定することはできません。異なるグループの場合には IP アドレス範囲を重複して設定することは可能です。
- 設定した IP アドレス範囲から特定の IP アドレスのみを削除することはできません。IP アドレス範囲をすべて削除し、その後設定をし直して下さい。
- IP アドレス範囲の削除は IP アドレス範囲の最初のアドレスだけを入力しても削除することができます。また、最初のアドレスと最後のアドレスの両方を入力して削除することも可能です。

例

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

管理アクセスへの接続が許可されている IP アドレスを表示します。

文法

show management < all-client | http-client | snmp-client | telnet-client >

- all-client — SNMP/Web ブラウザ /Telnet クライアントの IP アドレス
- http-client — Web ブラウザクライアントの IP アドレス
- snmp-client — SNMP クライアントの IP アドレス .
- telnet-client — Telnet クライアントの IP アドレス

コマンドモード

Privileged Exec

例

```
Console#show management all-client
Management Ip Filter
Http-Client:
Start ip address End ip address
-----
1. 192.168.1.19 192.168.1.19
2. 192.168.1.25 192.168.1.30

Snmp-Client:
Start ip address End ip address
-----
1. 192.168.1.19 192.168.1.19
2. 192.168.1.25 192.168.1.30

Telnet-Client:
Start ip address End ip address
-----
1. 192.168.1.19 192.168.1.19
2. 192.168.1.25 192.168.1.30

Console#
```

4.9 セキュリティ

本機はそれぞれのデータポートに接続されたクライアントのためにトラフィックを分離、または認証されたクライアントのみネットワークへのアクセスを可能にするため様々なメソッドをサポートしています。プライベート VLAN と IEEE 802.1X を使用したポートベース認証は通常これらの目的のために使用されます。
この節では、これらのメソッドに加え、クライアントセキュリティを提供するためのその他の多数のオプションについて説明します。

コマンド	機能	ページ
Port Security*	ポートのセキュアアドレスを設定	P533
802.1X Port Authentication*	802.1X を利用した、指定したポートでのホスト認証を設定	P513
Network Access*	MAC 認証及び動的 VLAN 割り当ての設定	P535
Web Authentication*	Web 認証の設定	P552
Access Control Lists*	IP フレーム（アドレス、プロトコル、レイヤ 4 プロトコルポート番号、TCP コントロールコードを基にする）、IP フレーム以外（MAC アドレスまたはイーサネットタイプを基にする）のフィルタリングを提供	P585
DHCP Snooping*	DHCP スヌーピングバインディングテーブルによる、アントラスト DHCP メッセージのフィルタ	P560
IP Source Guard*	DHCP スヌーピングテーブル上の動的エントリを基にし、ネットワークインタフェース上の IP トラフィックをフィルタ	P570
ARP Inspection	ARP パケットで MAC-to-IP アドレスバインディングの妥当性を検査	P575

* これらフィルタリングコマンド実行のプライオリティは、Port Security、Port Authentication、Network Access、Web Authentication、Access Control Lists、DHCP Snooping、IP Source Guard になります。

4.9.1 ポートセキュリティコマンド

ポートへのポートセキュリティ機能を使用できるようにします。ポートセキュリティ機能を使用すると、ポートにおける最大学習数に達した際に MAC アドレスの学習を止めます。そして、そのポートの動的 / 静的なアドレステーブルに既に登録されているソース MAC アドレスの受信フレームのみネットワークへのアクセスを許可します。そのポートでも他のポートからも学習されていない不明なソース MAC アドレスの受信フレームは破棄します。学習されていない MAC アドレスを送信するデバイスがあった場合、この動作はスイッチで検知され、自動的にそのポートを無効にし、SNMP トラップメッセージを送信します。

コマンド	機能	モード	ページ
mac-address-table static	VLAN 内のポートへの静的アドレスのマッピング	GC	P665
port security	ポートセキュリティの設定	IC	P534
show mac-address-table	フォワーディングデータベースのエントリ表示	PE	P667

port security

ポートへのポートセキュリティを有効に設定します。キーワードを使用せず "no" を前に置くことでポートセキュリティを無効にします。キーワードと共に "no" を前に置くことで侵入動作及び最大 MAC アドレス登録数を初期設定に戻します。

文法

port security { action < shutdown | trap | trap-and-shutdown >
| max-mac-count *address-count* }

no port security {action | *max-mac-count* }

- action — ポートセキュリティが破られた場合のアクション
 - shutdown — ポートを無効
 - trap — SNMP トラップメッセージの発行
 - trap-and-shutdown — SNMP トラップメッセージを発行しポートを無効
- max-mac-count
 - *address-count* — ポートにおいて学習する MAC アドレスの最大値
(範囲：0-1024 0は無効)

初期設定

- Status：無効
- Action：なし
- Maximum Addresses：0

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- ポートセキュリティを有効にした場合、本機は設定した最大学習数に達すると、有効にしたポートで MAC アドレスの学習を行わなくなります。すでにアドレステーブルに登録済みの MAC アドレスのデータのみがアクセスすることができます。
- まず "port security max-mac-count" コマンドを使用して学習するアドレス数を設定し、"port security" コマンドでポートのセキュリティを有効に設定します。
- 新しい VLAN メンバーを追加する場合には、MAC アドレスを "mac-address-table static" コマンドを使用します。
- セキュアポートには以下の制限があります：
 - ネットワークを相互接続するデバイスには接続できません。
 - トランクグループに加えることはできません。
- ポートセキュリティが機能しポートを無効にした場合、"no shutdown" コマンドを使用し、手動で再度有効にする必要があります。

例

本例では、5 番ポートにポートセキュリティとポートセキュリティ動作を設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

4.9.2 ネットワークアクセス (MAC アドレス認証)

スイッチポートに接続するいくつかのデバイスは、ハードウェアやソフトウェアの制限により 802.1x 認証をサポートできないことがあります。これはネットワークプリンタ、IP 電話、ワイヤレスアクセスポイントのようなデバイスでしばしば遭遇します。スイッチは、RADIUS サーバーでデバイスの MAC アドレスを認証し管理することで、これらのデバイスからのネットワークアクセスを可能にします。

コマンド	機能	モード	ページ
network-access aging	MAC アドレスエージングの有効化	GC	P536
network-access mac-filter	MAC アドレスをフィルタテーブルへ追加	GC	P537
mac-authentication reauth-time	認証された MAC アドレスが再認証を行うまでの時間を設定	GC	P547
network-access dynamic-qos	動的 QoS 機能を有効	IC	P539
network-access dynamic-vlan	認証ポートの、動的 VLAN 割り当てを有効	IC	P539
network-access guest-vlan	ネットワークアクセス (Mac 認証) あるいは 802.1x 認証が拒否時、全てのトラフィックをゲスト VLAN ポートへ割り当て	IC	P539
network-access link-detection	リンク検出機能を有効化	IC	P539
network-access link-detection link-down	リンクダウンイベントを検出し作用するよう、リンク検出機能を有効化	IC	P542
network-access link-detection link-up	リンクアップイベントを検出し作用するよう、リンク検出機能を有効化	IC	P543
network-access link-detection link-up-down	リンクアップ / ダウンイベントを検出し作用するよう、リンク検出機能を有効化	IC	P544
network-access max-mac-count	インタフェースの認証 MAC アドレス最大数を設定	IC	P545
network-access mode mac-authentication	インタフェースで MAC 認証を有効	IC	P546
network-access port-mac-filter	指定した MAC アドレスフィルタを有効化	IC	P547
mac-authentication intrusion-action	ポートで認証可能な MAC アドレスの最大数を設定	IC	P547
mac-authentication max-mac-count	802.1X 認証あるいは Mac 認証によって、ポートに認証可能な MAC アドレスの最大数を設定	IC	P539
show network-access	ポートインタフェースの MAC 認証設定を表示	PE	P549
show network-access macaddress-table	セキュア MAC アドレステーブルのエントリ情報を表示	PE	P550
show network-access mac-filter	MAC フィルタテーブルのエントリ情報を表示	PE	P551

network-access aging

安全な MAC アドレステーブルに保存されている認証 MAC アドレスのエージングを有効にします。 "no" を前に置くことで無効に設定します。

文法

network-access aging

no network-access aging

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- ・ 認証された MAC アドレスは、スイッチのセキュア MAC アドレステーブルに動的エントリとして保存されており、エージングタイムが経過すると削除されます。
アドレスエージングタイムについては " mac-address-table aging-time " (P664) を参照してください。
- ・ 本機でサポートされている、セキュア MAC アドレスの最大数は 1024 です。

例

```
Console(config)#network-access aging
Console(config)#
```

network-access mac-filter

フィルタテーブルに MAC アドレスを追加します。"no" を前に置くことで指定した MAC アドレスを取り除きます。

文法

network-access mac-filter < *filter-id* > mac-address *mac-address* mask *mask*

no network-access mac-filter < *filter-id* > mac-address *mac-address* mask *mask*

- *filter-id* — MAC アドレスフィルタテーブルを指定 (範囲: 1-64)
- *mac-address* — MAC アドレスエントリを指定 (フォーマット: xx-xx-xx-xx-xx-xx)
- *mask* — MAC アドレスビットマスクで範囲を指定

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 指定されたアドレスはネットワーク認証を免除されます。
- このコマンドは、マスクを使用しアドレスの範囲を設定する点と、"network-access port-mac-filter" を使用し、これらのアドレスを 1 つ以上のポートにアサインする点で "mac-address-table static" コマンド (P665) を使用する静的アドレスの設定とは異なります。
- 最大 64 のフィルタテーブルを定義することができます。
- フィルタテーブルに入れるエントリ数に制限はありません。

例

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66  
Console(config)#
```

mac-authentication reauth-time

接続された MAC アドレスが再認証された後の期間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

mac-authentication reauth-time *seconds*

no mac-authentication reauth-time

- *seconds* — 再認証間隔 （範囲：120-1000000 秒）

初期設定

1800

コマンドモード

Global Configuration

コマンド解説

- 再認証時間はグローバル設定と、全てのポートに適用されます。
- セキュア MAC アドレスの再認証時間の期限が切れると、RADIUS サーバーで再び認証がおこなわれます。再認証プロセスの間、ポートを通るトラフィックは影響を受けません。

例

```
Console(config)#mac-authentication reauth-time 300
Console(config)#
```


network-access dynamic-qos

認証ポートの、動的 QoS 機能を有効にします。"no" を前に置くことで無効に設定します。

文法

network-access dynamic-qos

no network-access dynamic-qos

初期設定

無効

コマンドモード

Interface Configuration

コマンド解説

- RADIUS サーバはオプションとして、認証されたユーザのスイッチポートへ適用される、ダイナミック QoS 割り当てを返します。"Filter-ID" 属性（属性 11）は以下の QoS 情報を渡す RADIUS サーバで設定されます。

ダイナミック QoS プロファイル

プロファイル	属性構文	例
DiffServ	service-policy-in=policy-map-name	service-policy-in=p1
Rate Limit	rate-limit-input=rate	rate-limit-input=100 (in units of Kbps)
802.1p	switchport-priority-default=value	switchport-priority-default=2

- 最後のユーザが QoS 割り当てを持つポートをログオフする時、スイッチはポートをオリジナル QoS 設定へリストアします。
- ユーザが、既に同じポートへログオンしたユーザと違う動的 QoS プロファイルと共にネットワークへのログインを試みた場合、アクセスは拒否されます。
- ポートが動的プロファイルされている間、全ての手動 QoS 設定変更は、全てのユーザがポートからログオフした後にのみ効果が適用されます。

[注意] 動的 QoS の設定変更はスイッチ設定ファイルに保存されません。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

network-access dynamic-vlan

認証ポートへの動的 VLAN の割り当てを有効にします。"no" を前に置くことで設定を無効にします。

文法

network-access dynamic-vlan

no network-access dynamic-vlan

初期設定

有効

コマンドモード

Interface Configuration

コマンド解説

- 有効時、スイッチに既に VLAN が作成されているならば、RADIUS サーバから返された VLAN 識別子がポートへ適用されます。VLAN を作成する為に GVRP は使用されません。
- 最初に認証された MAC アドレスによって指定された VLAN 設定がポートに導入されます。その他のポートで認証された MAC アドレスは同じ VLAN 設定を持つか、認証失敗として取り扱われます。
- もし動的 VLAN 割り当てがポートで使用可能であり、RADIUS サーバが VLAN 設定を返さないなら、認証は依然成功として取り扱われます。
- ポートで、動的 VLAN 割り当てステータスが変更された場合、全ての認証されたアドレスはセキュア MAC アドレステーブルからクリアされます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```

network-access guest-vlan

ネットワークアクセス (Mac 認証) あるいは 802.1x 認証が拒否時、全てのトラフィックをゲスト VLAN ポートへ割り当てます。"no" を前に置くことでゲスト VLAN アサイメントを無効にします。

文法

network-access guest-vlan *vlan-id*

no network-access guest-vlan

- *vlan-id* — VLAN ID を指定 (範囲: 1-4093)

初期設定

無効

コマンドモード

Interface Configuration

コマンド解説

- ゲスト VLAN として使用される VLAN は先に定義しアクティブに設定してください (710 ページの「vlan database」を参照)
- 802.1X 認証で使用される際には、"intrusion-action" は "guest-vlan" に対し効果があるよう設定する必要があります。(P515)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

network-access link-detection

選択したポートでのリンク検出を有効にします。"no" を前に置くことで設定を初期状態に戻します。

文法

network-access link-detection

no network-access link-detection

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection
Console(config-if)#
```

network-access link-detection link-down

リンクダウンイベントの検出を行います。検出時、スイッチはポートをシャットダウンするか、SNMP トラップを送信します。またはその両方を行います。
"no" を前に置くことで機能を無効します。

文法

network-access link-detection link-down action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

- shutdown — ポートを無効
- trap — SNMP トラップメッセージを発行
- trap-and-shutdown — SNMP トラップメッセージの発行とポートの無効

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-down action trap
Console(config-if)#
```

network-access link-detection link-up

リンクアップイベントの検出を行います。検出時、スイッチはポートをシャットダウンするか、SNMP トラップを送信します。またはその両方を行います。"no" を前に置くことで機能を無効します。

文法

network-access link-detection link-up action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

- shutdown — ポートを無効
- trap — SNMP トラップメッセージを発行
- trap-and-shutdown — SNMP トラップメッセージの発行とポートの無効

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up action trap
Console(config-if)#
```

network-access link-detection link-up-down

リンクアップとリンクダウンイベントの検出を行います。いずれかのイベントを検出時、スイッチはポートをシャットダウンするか、SNMP トラップを送信します。またはその両方を行います。"no" を前に置くことで機能を無効します。

文法

network-access link-detection link-up-down action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

- shutdown — ポートを無効
- trap — SNMP トラップメッセージを発行
- trap-and-shutdown — SNMP トラップメッセージの発行とポートの無効

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up-down action trap
Console(config-if)#
```

network-access max-mac-count

全ての認証フォームによって、ポートインタフェースで認証できる MAC アドレスの最大数を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

network-access max-mac-count *count*

no network-access max-mac-count

- *count* — 許可される認証 MAC アドレスの最大数（範囲：1-2048 0 は制限無し）

初期設定

1024

コマンドモード

Interface Configuration

コマンド解説

- ポートごとの MAC アドレスの最大数は 1024 であり、本機でサポートされているセキュア MAC アドレスの最大数は 1024 です。制限に達すると、全ての新しい MAC アドレスは認証失敗として取り扱われます。

例

```
Console(config-if)#network-access max-mac-count 5
Console(config-if)#
```

network-access mode mac-authentication

ネットワークアクセス認証をポートで有効にします。"no" を前に置くことで無効に設定します。

文法

network-access mode mac-authentication
no network-access mode mac-authentication

初期設定

無効

コマンドモード

Interface Configuration

コマンド解説

- ポートで有効の場合、認証プロセスは、設定された RADIUS サーバへパスワード認証プロトコル（PAP）リクエストを送信します。
- RADIUS サーバ上では、PAP ユーザ名とパスワードは MAC アドレスフォーマットで設定されます。
- 認証された MAC アドレスは、スイッチのセキュアアドレステーブルに動的エントリとして保存され、エイジングタイムの期限が切れると削除されます。
本機でサポートされているセキュア MAC アドレスの最大数は 1024 です。
- スイッチポートで見られた静的 MAC アドレスはセキュアアドレステーブルに追加されます。静的アドレスは RADIUS サーバへリクエストを送らずに、認証されたアドレスとして取り扱われます。
- MAC 認証、802.1X、ポートセキュリティは同時に同じポートに設定することはできません。1 つのセキュリティメカニズムのみが適用できます。
- MAC 認証はトランクポートに設定できません。
- ポートステータスがダウンへ変わると、全ての MAC アドレスはセキュアアドレステーブルから削除されます。静的 VLAN 割り当てはリストアされません。
- RADIUS サーバはオプションとして、VLAN 識別のリストを返します。VLAN 識別リストは "Tunnel-Private-Group-ID" 属性に載せられます。VLAN リストは、"1u,2t," フォーマットを使用して、複数の VLAN 識別を含むことが出来ます。"u" はタグ無し VLAN を示し、"t" はタグ付き VLAN を示します。"Tunnel-Type" 属性は "VLAN," と "Tunnel-Medium-Type" 属性を "802" にセットします。

例

```
Console(config-if)#network-access mode mac-authentication  
Console(config-if)#
```

network-access port-mac-filter

指定した MAC アドレスフィルタを有効にします。"no" を前に置くことで無効にします。

文法

network-access port-mac-filter *filter-id*

no network-access port-mac-filter

- *filter-id* — MAC アドレスフィルタテーブルを指定 (範囲: 1-64)

初期設定

なし

コマンドモード

Interface Configuration

コマンド解説

- ポートに割り当てられるフィルタテーブルは 1 つだけです。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access port-mac-filter 1
Console(config-if)#
```

mac-authentication intrusion-action

MAC 認証失敗時に、ポートがホストへ行う行動を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

mac-authentication intrusion-action < block traffic | pass traffic >

no mac-authentication intrusion-action

初期設定

Block Traffic

コマンドモード

Interface Configuration

例

```
Console(config-if)#mac-authentication intrusion-action block-traffic
Console(config-if)#
```

mac-authentication max-mac-count

802.1X 認証あるいは Mac 認証によって、ポートに認証可能な MAC アドレスの最大数を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

mac-authentication max-mac-count *count*

no mac-authentication max-mac-count

- *count* — 認証できる MAC アドレスの最大数を設定します。(範囲：1-1024)

初期設定

1024

コマンドモード

Interface Configuration

例

```
Console(config-if)#mac-authentication max-mac-count 32
Console(config-if)#
```

show network-access

ポートインタフェースの、MAC 認証設定を表示します。

文法

show network-access { interface *interface* }

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)

初期設定

全てのインタフェースを表示

コマンドモード

Privileged Exec

例

```
Console#show network-access interface ethernet 1/1
Global secure port information
Reauthentication Time                : 1800
-----
Port : 1/1
MAC Authentication                   : Disabled
MAC Authentication Intrusion action  : Block traffic
MAC Authentication Maximum MAC Counts : 1024
Maximum MAC Counts                   : 2048
Dynamic VLAN Assignment              : Enabled
Guest VLAN                           : Disabled
Console#
```

show network-access mac-address-table

セキュア MAC アドレステーブルエントリを表示します。

文法

show network-access mac-address-table { static | dynamic |
address *mac-address mask* | interface *interface* | sort < address | interface> }

- static — 静的アドレスエントリを指定
- dynamic — 動的アドレスエントリを指定
- *mac-address* — MAC アドレスエントリを指定（フォーマット：xx-xx-xx-xx-xx-xx）
- *mask* — MAC アドレスビットマスクを指定
- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号（範囲：1-26）
- sort — 表示されたエントリを MAC アドレスまたはインタフェースでソートします。

初期設定

全てのフィルタを表示

コマンドモード

Privileged Exec

例

```
Console#show network-access mac-address-table
-----
Port  MAC-Address      RADIUS-Server  Attribute  Time
-----
1/1   00-00-01-02-03-04 172.155.120.17 Static     00d06h32m50s
1/1   00-00-01-02-03-05 172.155.120.17 Dynamic    00d06h33m20s
1/1   00-00-01-02-03-06 172.155.120.17 Static     00d06h35m10s
1/3   00-00-01-02-03-07 172.155.120.17 Dynamic    00d06h34m20s
Console#
```

show network-access mac-filter

MAC フィルタテーブルの項目に関する情報を表示します。

文法

show network-access mac-filter { *filter-id* }

- *filter-id* — MAC アドレスフィルタテーブルを表示（範囲：1-64）

初期設定

全てのフィルタを表示

コマンドモード

Privileged Exec

例

```
Console#show network-access mac-filter
Filter ID MAC Address MAC Mask
-----
1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF
Console#
```

4.9.3 Web 認証

Web 認証は、802.1x やネットワークアクセス認証が実行不可能または実用的でない状況で、ネットワークへの認証とアクセスを行うことを端末に許可します。Web 認証機能は IP アドレスを割り当てる DHCP のリクエストと受信、DNS クエリの実行を、認証されていないホストに許可します。HTTP を除いたほかのすべてのトラフィックはブロックされます。スイッチは HTTP トラフィックを傍受し、RADIUS を通してユーザーネームとパスワードを入力する、スイッチが生成した Web ページにリダイレクトします。一度認証に成功すると、Web ブラウザは元のリクエストされた Web ページに転送されます。認証が成功したポートに接続されたすべてのホストについて、認証が有効になります。

[注意] 適切に機能させるために RADIUS 認証をアクティベートし、Web 認証用に適切に構成してください。

[注意] Web 認証はトランクポートに設定することはできません。

コマンド	機能	モード	ページ
web-auth login-attempts	Web 認証ログイン失敗時の再認証回数を設定	GC	P553
web-auth quiet-period	Web 認証ログインの最大回数を過ぎた後、接続待機状態に移行するまでの時間を設定	GC	P554
web-auth session-timeout	セッションタイムアウト時間を設定	GC	P554
web-auth system-auth-control	Web 認証をグローバルで有効	GC	P555
web-auth	Web 認証をインタフェースで有効	IC	P555
web-auth re-authenticate(Port)	ポートに確立されている全ての Web 認証セッションを終了	PE	P556
web-auth re-authenticate (IP)	ートに確立されている全ての Web 認証セッションを終了	PE	P556
show web-auth	グローバル Web 認証パラメータを表示	PE	P557
show web-auth interface	指定したインタフェースの Web 認証パラメータおよび統計値を表示	PE	P558
show web-auth summary	指定した IP アドレスで確立されている Web 認証セッションを終了	PE	P559

web-auth login-attempts

認証ログイン失敗時に、再認証を行う制限を設定します。設定した最大回数を過ぎた後は、"web-authquiet-period" を設定した期限が切れるまで、スイッチはそれ以上のログインを拒否します。"no" を前に置くことで設定を初期値に戻します。

文法

web-auth login-attempts *count*

no web-auth login-attempts

- *count* — ログインの試行回数の上限を設定します（範囲：1-3 回）

初期設定

3

コマンドモード

Global Configuration

例

```
Console(config)#web-auth login-attempts 2
Console(config)#
```

web-auth quiet-period

Web 認証ログインの、最大試行回数を過ぎた後、ログイン待機状態に移行するまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

web-auth quiet-period *time*

no web-auth quiet-period

- *time*— ホストがログインの試行回数の上限を超えた後、再び認証ができるまでに待機する時間を設定します（範囲：1 – 180 秒）

初期設定

60 秒

コマンドモード

Global Configuration

例

```
Console(config)#web-auth quiet-period 120
Console(config)#
```

web-auth session-timeout

セッションタイムアウト時間を設定します。設定したタイムアウト時間に達した時、ホストは強制的にログオフされ、再度認証を行う必要があります。"no" を前に置くことで設定を初期状態に戻します。

文法

web-auth session-timeout *timeout*

no web-auth session-timeout

- *timeout*— ホストの再認証をする前に認証セッションをどのくらいの時間維持するかを設定します。"(範囲：0、300 ～ 3600 秒)

初期設定

3600 秒

コマンドモード

Global Configuration

例

```
Console(config)#web-auth session-timeout 1800
Console(config)#
```


web-auth system-auth-control

Web 認証をグローバルで有効にします。"no" を前に置くことで設定を初期状態に戻します。

文法

web-auth system-auth-control

no web-auth system-auth-control

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#web-auth system-auth-control  
Console(config)#
```

web-auth

Web 認証をインタフェースで有効にします。"no" を前に置くことで設定を初期状態に戻します。

文法

web-auth

no web-auth

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config-if)#web-auth  
Console(config-if)#
```

web-auth re-authenticate (Port)

ポートに確立されている全ての Web 認証セッションを終了します。ユーザは再認証を行う必要があります。

文法

web-auth re-authenticate interface *interface*

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#web-auth re-authenticate interface ethernet 1/2
Failed to reauth .
Console#
```

web-auth re-authenticate (IP)

指定した IP アドレスで確立されている Web 認証セッションを終了します。ユーザは再認証を行う必要があります。

文法

web-auth re-authenticate interface *interface* *IP Address*

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
- *IP Address* — IPv4 フォーマット IP アドレス

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Console#
```

show web-auth

グローバル Web 認証パラメータを表示します。

文法

show web-auth

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show web-auth

Global Web-Auth Parameters

  System Auth Control      : Disabled
  Session Timeout          : 3600
  Quiet Period             : 60
  Max Login Attempts       : 3
Console#
```

show web-auth interface

指定したインタフェースの Web 認証パラメータおよび統計値を表示します。

文法

show web-auth interface *interface*

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Web Auth Status      : Disabled

Host Summary

IP address           Web-Auth-State Remaining-Session-Time
-----
1.1.1.1              Authenticated      295
1.1.1.2              Authenticated      111
Console#
```

show web-auth summary

Web 認証ポートパラメータおよび統計値の概要を表示します。

文法

show web-auth summary

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show web-auth summary
Global Web-Auth Parameters:
  System Auth Control : Disabled

Port      Status      Authenticated Host Count
-----
1/ 1      Enabled      0
.
. 省略
.
1/25      Disabled     0
1/26      Disabled     0
Console#
```

4.9.4 DHCP スヌーピング

DHCP スヌーピングは、悪意のある DHCP サーバーや DHCP サーバーに関連のある情報を送信する他のデバイスからネットワークを守ります。この情報は物理ポートへ IP アドレスを戻す際の追跡に役立つ場合があります。この項では DHCP スヌーピング機能を構成するために使用するコマンドについて記載しています。

コマンド	機能	モード	ページ
ip dhcp snooping	DHCP スヌーピングをスイッチで有効化	GC	P561
ip dhcp snooping database flash	全ての動的学習スヌーピングエントリをフラッシュメモリに書き込み	GC	P562
ip dhcp snooping information option	DHCP Option 82 情報リレーを有効 / 無効化	GC	P563
ip dhcp snooping information policy	DHCP Option 82 情報を含む、DHCP クライアントパケット Information option policy を設定	GC	P564
ip dhcp snooping verify mac-address	イーサネットヘッダ中の MAC アドレスに対して DHCP パケットにストアされたクライアントのハードウェアアドレスを確認	GC	P565
ip dhcp snooping vlan	DHCP スヌーピングを指定の VLAN で有効化	GC	P566
ip dhcp snooping trust	指定したインタフェースを trusted ポートに設定	IC	P567
clear ip dhcp snooping database flash	動的に学習されている全てのスヌーピングエントリをフラッシュメモリから削除	PE	P568
show ip dhcp snooping	DHCP スヌーピング設定を表示	PE	P568
show ip dhcp snooping binding	DHCP スヌーピングバインディングテーブルエントリを表示	PE	P569

ip dhcp snooping

このコマンドは DHCP スヌーピング機能を有効にします。no を付けると設定を初期状態に戻します。

文法

ip dhcp snooping

no ip dhcp snooping

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- ネットワークの外側から悪意のある DHCP メッセージが受信されたとき、ネットワークトラフィックが混乱する可能性があります。DHCP スヌーピングはネットワークやファイアウォールの外側からの安全でないインターフェースで受信した DHCP メッセージをフィルタするために使用されます。DHCP スヌーピングをこのコマンドで有効にして ip dhcp snooping vlan コマンドで VLAN インターフェース上の DHCP スヌーピングを有効にしたとき、DHCP スヌーピングテーブルのリストに載っていないデバイスから、スイッチの untrust インターフェースで DHCP メッセージを受信すると、それを破棄します。
 - 有効にしたとき、untrust のインターフェースに入った DHCP メッセージには、DHCP スヌーピングで学習したダイナミックエントリをベースにしたフィルタが行われます。
 - DHCP スヌーピングテーブルのエントリは、untrust インターフェースからのパケットのみ学習されます。それぞれのエントリには MAC アドレス、IP アドレス、リースタイム、エントリタイプ (Dynamic DHCP Binding、Static DHCP Binding)、VLAN ID、Port ID が含まれています。
 - DHCP スヌーピングを有効にしたとき、スイッチが処理することのできる DHCP メッセージの数の制限が設定され、1 秒当たり 100 パケットとなります。この制限を越える DHCP パケットは破棄されます。
 - フィルタのルールは下記の通りです。
 - DHCP スヌーピングが無効の場合、DHCP パケットは転送される。
 - DHCP スヌーピングが有効で DHCP パケットを受信する VLAN 上でも有効の場合、すべての DHCP パケットは trust 状態のポートに向けて転送されます。受信したパケットが DHCP ACK メッセージの場合、このエントリはバインドテーブルに追加されます。
 - DHCP スヌーピングが有効で DHCP パケットを受信する VLAN 上でも有効だが、ポートが trust でない場合は下記の動作を行います。
- DHCP パケットが DHCP サーバーからの返答パケット (OFFER,ACK,NAK メッセージを含む) の場合、そのパケットは破棄されます。
 - DHCP パケットがクライアントからのものである場合、DECLINE や RELEASE メッセージのようなパケットは、一致するエントリがバインドテーブルで見つかった場合のみ、スイッチはパケットを転送します。

- (3) DHCP パケットがクライアントからのものである場合、DISCOVER、REQUEST、INFORM、DECLINE、RELEASE メッセージのようなパケットは、MAC アドレスによる照合が無効である場合にはパケットは転送されます。しかし、MAC アドレスの照合が有効の場合、DHCP パケットに記録されているクライアントのハードウェアアドレスが Ethernet ヘッダの Source MAC アドレスと同じ場合にパケットは転送されます。
- (4) DHCP パケットが認識できないタイプの場合は破棄されます。
 - クライアントからの DHCP パケットが上記のフィルタ基準を通過した場合、同じ VLAN の trust ポートに転送されます。
 - サーバーからの DHCP パケットが trust ポートで受信された場合、同じ VLAN の trust ポートと untrust ポートに転送されます。
- DHCP スヌーピングが無効の場合、すべてのダイナミックエントリはバインドテーブルから取り除かれます。
- スイッチ自身が DHCP クライアントの場合の動作：スイッチが DHCP サーバーにクライアントの Request パケットを送信するポートは trust として設定しなくてはなりません。スイッチは DHCP サーバーから ACK メッセージを受信したとき、自身の情報をバインドテーブルのダイナミックエントリとして追加しません。また、スイッチが DHCP クライアントのパケットを自身に送信したとき、フィルタの動作は発生しません。しかし、スイッチが DHCP サーバーからメッセージを受信したとき、untrust ポートで受信したパケットはすべて破棄されます。

例

```
Console(config)#ip dhcp snooping
Console(config)#
```

関連するコマンド

ip dhcp snooping vlan (P566)

ip dhcp snooping trust (P567)

ip dhcp snooping database flash

全ての動的学習スヌーピングエントリをフラッシュメモリに書き込みます。

コマンドモード

Privileged Exec

例

```
Console(config)#ip dhcp snooping database flash
Console(config)#
```


ip dhcp snooping information option

このコマンドはスイッチの DHCP Option 82 Information Relay 機能を有効にします。no を付けるとこの機能は無効になります。

文法

ip dhcp snooping information option

no ip dhcp snooping information option

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- DHCP 機能はスイッチと DHCP クライアントについての情報を DHCP サーバーに送信するため、リレー機能を装備しています。DHCP Option 82 として知られる機能で、IP アドレスを割り当てるときの情報を使用するため、もしくはクライアントに他のサービスやポリシーを設定するために DHCP サーバーを共用できる状態にします。
- DHCP Snooping Information Option が有効のとき、クライアントは MAC アドレスよりむしろクライアントが接続されているスイッチのポートによって同一のものであると識別されます。それにより、DHCP クライアントとサーバー間のメッセージ交換は、VLAN 全体にメッセージをフラッディングすることなしでクライアントとサーバー間を直接転送します。
- スイッチ上で DHCP Option 82 の情報をパケットの中に入れるためには DHCP Snooping 機能を有効にしてください。

例

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

ip dhcp snooping information policy

このコマンドは Option 82 を含む DHCP クライアントからのパケットのため、DHCP スヌーピング Information Option を設定します。

文法

ip dhcp snooping information policy <drop | keep | replace>

- drop — パケット中の Option82 情報を破棄し、全ての VLAN にフラットニングします。
- keep — DHCP クライアント情報を残します。
- replace — DHCP クライアントパケット情報をスイッチ自身のリレー情報で置き換えます。

初期設定

replace

コマンドモード

Global Configuration

コマンド解説

スイッチが DHCP Option 82 を既に含んでいるクライアントから DHCP パケットを受信したとき、スイッチはこれらのパケットのためアクションポリシーの設定を構成します。DHCP パケットを破棄するかどうか、Option 82 の情報をそのままにするか、Option 82 をスイッチ自身のリレー情報に置き換えるかを選択することができます。

例

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

ip dhcp snooping verify mac-address

DHCP パケットにストアされたクライアントハードウェアアドレスに対し、イーサネットヘッダの送信元 MAC アドレスを検査します、

文法

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- MAC アドレス検査が有効であり、パケットのイーサネットヘッダ内の送信元 MAC アドレスが、クライアントの DHCP パケットのハードウェアアドレスと一致しない場合、パケットは破棄されます。 .

例

```
Console(config)#ip dhcp snooping verify mac-address  
Console(config)#
```

関連するコマンド

ip dhcp snooping (P561)

ip dhcp snooping vlan (P566)

ip dhcp snooping trust (P567)

ip dhcp snooping vlan

このコマンドは指定した VLAN 上で DHCP スヌーピング機能を有効にします。no を付けると設定を初期状態に戻します。

文法

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping vlan *vlan-id*

- *vlan-id* — 設定を行う VLAN ID（範囲：1-4093）

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- ip dhcp snooping コマンドを使用して DHCP スヌーピングを有効にした後にこのコマンドで DHCP Snooping を VLAN 上で有効にしたとき、ip dhcp snooping trust コマンドで指定した VLAN 内の untrust ポートで DHCP パケットのフィルタが実行されます。
- DHCP スヌーピングの全体の設定を無効にした（no ip dhcp snooping を実行）とき、VLAN 上での DHCP スヌーピング設定はまだ可能ですが、この変更は DHCP Snooping 全体の設定が再度有効になるまで反映されません。
- DHCP スヌーピングが有効のとき、VLAN の DHCP スヌーピング設定を変更すると下のような結果になります。
 - VLAN 上で DHCP スヌーピング設定を無効にした場合、この VLAN で学習したすべてのダイナミックエントリはバインドテーブルから削除されます。

例

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

関連するコマンド

ip dhcp snooping （P561）

ip dhcp snooping trust （P567）

ip dhcp snooping trust

このコマンドは特定のインターフェースを **trust** として設定します。no を付けると設定を初期状態に戻します。

文法

ip dhcp snooping trust

no ip dhcp snooping trust

初期設定

全てのインターフェースは **Untrust** に設定

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **untrust** インターフェースはネットワークやファイアウォールの外側からメッセージを受信するよう設定されたインターフェースです。**trust** インターフェースはネットワークの内側からメッセージのみ受信するよう設定されたインターフェースです。
- **ip dhcp snooping** を使用して DHCP スヌーピング機能を有効にし、次に VLAN 上で DHCP スヌーピングを有効にしたとき、DHCP パケットのフィルタリングが VLAN 内の **untrust** ポートで実行されます。
- **untrust** ポートが **trust** ポートに変更されたとき、このポートに関連付けられたすべての DHCP スヌーピングのダイナミックエントリは削除されます。
- スイッチ自身が DHCP クライアントの場合の動作：DHCP クライアントとしてのリクエストを DHCP サーバーに出力するポートを **trust** に設定してください。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

関連するコマンド

ip dhcp snooping (P561)

ip dhcp snooping vlan (P566)

clear ip dhcp snooping database flash

全ての動的学習スヌーピングエントリをフラッシュメモリに書き込みます。

コマンドモード

Privileged Exec

例

```
Console#clear ip dhcp snooping database flash
Console#
```

show ip dhcp snooping

DHCP スヌーピング設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp snooping
Global DHCP Snooping status: disable
DHCP Snooping is configured on the following VLANs:
1
Verify Source Mac-Address: enable
Interface          Trusted
-----
Eth 1/1            No
Eth 1/2            No
Eth 1/3            No
Eth 1/4            No
Eth 1/5            Yes
.
.
.
```

show ip dhcp snooping binding

DHCP スヌーピング・バインディングテーブルのエントリを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
11-22-33-44-55-66  192.168.0.99    0           Static         1     Eth 1/5
Console#
```

4.9.5 IP ソースガード

IP ソースガードは、IP ソースガードテーブル上の手動で設定されたエントリ、もしくは DHCP スヌーピング機能を有効にしたときに DHCP スヌーピングテーブル上のダイナミックエントリを基にしたネットワークインターフェース上の IP トラフィックをフィルタするセキュリティ機能です。IP ソースガードは、あるホストがネットワークにアクセスする別のホストの IP アドレスを使用する試みがあったとき、そのホストが行う攻撃からネットワークを守るために使用されます。

この項は IP ソースガードの設定を行うために使用するコマンドを記載しています。

コマンド	機能	モード	ページ
ip source-guard binding	IP Source Guard のバインドテーブルに固定 IP アドレスを追加します。	GC	P570
ip source-guard	送信元 IP アドレス、もしくは送信元 IP アドレスと対応する MAC アドレスを基に入カトラフィックをフィルタするようスイッチを設定します。	IC	P572
show ip source-guard	それぞれのインターフェースで IP Source Guard 機能が有効か無効かどうかを表示します。	PE	P573
show ip source-guard binding	IP Source Guard のバインドテーブルを表示します。	PE	P570

ip source-guard binding

このコマンドはソースガードのバインドテーブルにスタティックアドレスを追加します。
no を付けるとスタティックエントリを削除します。

文法

ip source-guard binding *mac-address* *vlan* *vlan-id* *ip-address*

interface ethernet *unit/port*

no ip source-guard binding *mac-address* *vlan* *vlan-id*

- *mac-address* — 有効なユニキャスト MAC アドレス
- *vlan-id* — 設定を行う VLAN ID (範囲 1-4093)
- *ip-address* — 有効なユニキャスト IP アドレス
- *unit* — スタックユニット (常に 1)
- *port* — ポート番号 (範囲 1-26)

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- テーブルエントリには MAC アドレス、IP アドレス、リースタイム、エントリの種類 (Static IP SG Binding、Dynamic DHCP Binding、Static DHCP Binding)、VLAN ID、ポート ID が含まれます。
- すべてのスタティックエントリはリースタイムが無限で設定されます。show ip source-guard コマンドを実行すると、そのスタティックエントリのリースタイムには 0 が表示されます。
- ソースガードを有効にしたとき、DHCP スヌーピングを通して学習されたダイナミックエントリ、DHCP スヌーピングを通して設定されたスタティックエントリ、このコマンドで設定されたスタティックアドレスに基づいてトラフィックのフィルタが行われます。
- スタティックバインドテーブルは下のような処理を行います。
 - 同じ VLAN ID と MAC アドレスのエントリがない場合、新しいエントリが Static IP Source Guard Binding としてバインドテーブルに追加されます。
 - 同じ VLAN ID と MAC アドレスのエントリがありエントリの種類が Static IP Source Guard Binding である場合、新しいエントリは古いエントリを上書きします。
 - 同じ VLAN ID と MAC アドレスのエントリがありエントリの種類が Dynamic DHCP Snooping Binding である場合、新しいエントリは古いエントリを上書きし、エントリの種類は Static IP Source Guard Binding に変更されます。

例

```
Console(config)#ip source-guard binding 00-11-22-33-44-55-66 vlan 1  
192.168.0.99 interface ethernet 1/5  
Console(config-if)#
```

関連するコマンド

ip source-guard (P572)
ip dhcp snooping (P561)
ip dhcp snooping vlan (P566)

ip source-guard

このコマンドは送信元 IP アドレス、もしくは送信元 IP アドレスと対応する MAC アドレスを基に入力トラフィックをフィルタするようスイッチを設定します。no を付けると設定を無効にすることができます。

文法

ip source-guard < sip | sip-mac >

no ip source-guard

- sip — バインディングテーブルにストアされた IP アドレスによる、トラフィックのフィルタリング
- sip-mac — バインディングテーブルにストアされた IP アドレスおよび、関連した MAC アドレスによる、トラフィックのフィルタリング

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- IP ソースガードはネットワークやファイアウォールの外側からメッセージを受信した、保護されていないポート上のトラフィックをフィルタするために使用されます。
- "sip" や "sip-mac" にソースガードのモードを設定することにより、選択したポート上でこの機能を有効にします。バインドテーブルのすべてのエントリに対して VLAN ID、送信元 IP アドレスポート番号をチェックするには "sip" オプションを使用してください。"sip-mac" オプションを使用すると、上に加えて送信元 MAC アドレスもチェックします。選択したポートでこの機能を無効にするには no source guard コマンドを使用します。
- 有効にしたとき、トラフィックは DHCP スヌーピングを通して学習したダイナミックエントリや IP ソースガードのバインドテーブルで構成された固定アドレスを基にフィルタが行われます。
- テーブルエントリには MAC アドレス、IP アドレス、リースタイム、エントリの種類 (Static IP SG Binding、Dynamic DHCP Binding、Static DHCP Binding)、VLAN ID、ポート ID が含まれます。
- ip source-guard binding コマンドを実行して表示されるソースガードバインドテーブル上に入力された静的アドレスは、リースタイムが無限として自動的に設定されます。DHCP スヌーピングを通して学習されたダイナミックエントリは DHCP サーバー自身によって構成されます。スタティックエントリには手動で設定されたリースタイムが含まれます。
- IP ソースガードを有効にした場合、入力パケットの IP アドレス (sip オプションが有効の場合)、もしくは入力パケットの IP アドレスと MAC アドレス (sip-mac オプションが有効の場合) はバインドテーブルと比較されます。エントリが合致していないことが分かった場合、パケットは破棄されます。

- フィルタのルールは下のように実行されます。
 - DHCP スヌーピングが無効の場合、IP ソースガードは VLAN ID、送信元 IP アドレス、ポート番号、送信元 MAC アドレス (sip-mac オプションが有効の場合) をチェックします。バインドテーブルに合致するエントリがありエントリの種類が Static (IP ソースガードバインドテーブルに記載) の場合、パケットは転送されます。
 - DHCP スヌーピングが有効の場合、IP ソースガードは VLAN ID、送信元 IP アドレス、ポート番号、送信元 MAC アドレス (sip-mac オプションが有効の場合) をチェックします。バインドテーブルに合致するエントリがありエントリの種類が Static (IP ソースガードバインドテーブルに記載)、Static (DHCP スヌーピングバインドテーブルに記載)、Dynamic (DHCP スヌーピングバインドテーブルに記載) のいずれかの場合にパケットは転送されます。
 - IP ソースガードが Static、Dynamic のエントリのどちらもまだ存在しない状態においてインターフェース上で有効になった場合、スイッチはそのポート上のすべての IP トラフィックを破棄します。ただし DHCP パケットは除きます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

関連するコマンド

ip source-guard binding (P574)
ip dhcp snooping (P561)
ip dhcp snooping vlan (P566)

show ip source-guard

このコマンドは、それぞれのインタフェースでソースガードが有効か無効かを表示します。

文法

show ip source-guard

コマンドモード

Privileged Exec

例

```
Console#show ip source-guard
Interface Filter-type
-----
Eth 1/1  DISABLED
Eth 1/2  DISABLED
Eth 1/3  DISABLED
Eth 1/4  DISABLED
Eth 1/5  SIP
Eth 1/6  DISABLED
```

show ip source-guard binding

ソースガードバインディングテーブルを表示します。

文法

show ip source-guard binding { dhcp-snooping | static }

- dhcp-snooping — DHCP スヌーピングコマンド（P560）で設定された動的エントリを表示
- static — ip source-guard binding コマンド（P570）で設定された静的エントリを表示

コマンドモード

Privileged Exec

例

```
Console#show ip source-guard binding
MacAddress      IPAddress      Lease(sec)  Type   VLAN  Interface
-----
11-22-33-44-55-66 192.168.0.99      0    Static    1     Eth 1/5
Console#
```

4.9.6 ARP インспекション

ARP インспекションは、Address Resolution packet (ARP) プロトコルのための、MAC アドレスバインディングの妥当性の検査を行うセキュリティ機能です。

この機能によりある種の man-in-the-middle 攻撃等からネットワークを保護できます。

この機能は、ローカル ARP キャッシュがアップデートされるか、またはパケットが適切な目的地に転送される前に全ての ARP リクエストを途中で捕らえ、これらのパケットのそれぞれを照合することによって達成されます。無効な ARP パケットは破棄されます。

ARP インспекションは、信頼できるデータベース (DHCP スヌーピングバインディングデータベース) に保存された、正当な IP-to-MAC アドレスバインディングに基づいて、ARP パケットの正当性を決定します。このデータベースは機能がスイッチと VLAN で有効になっている時に、DHCP スヌーピングによって構築されます。

また、ARP インспекションは、ユーザで設定された ARP アクセスコントロールリスト (ACL) に対して、ARP パケットの妥当性を確認することも可能です。

コマンド	機能	モード	ページ
ip arp inspection	ARP インспекションをグローバルで有効化	GC	P576
ip arp inspection filter	1 つまたは 1 つ以上の VLAN へ適用する ARP ACL を指定	GC	P577
ip arp inspection log-buffer logs	ログメッセージに保存されるエントリの最大数およびこれらのメッセージが送信されるレイトを設定	GC	P578
ip arp inspection validate	ARP パケットアドレスコンポーネントの追加妥当性検査を指定	GC	P579
ip arp inspection vlan	指定した VLAN または範囲で ARP インспекションを有効化	GC	P580
ip arp inspection limit	ポートで受信される ARP パケットのレートリミットを設定	IC	P581
ip arp inspection trust	ポートを "trust" に設定し、ARP インспекションから免除	IC	P582
show ip arp inspection configuration	ARP インспекションのグローバル設定を表示	PE	P582
show ip arp inspection interface	ポートの trust ステータスとインспекションレートリミットを表示	PE	P583
show ip arp inspection log	関連付けられる VLAN、ポート、アドレスコンポーネントを含む、ログに保存されているエントリの情報を表示	PE	P583
show ip arp inspection statistics	処理された ARP パケット数に関する統計、または破棄された様々な理由の表示	PE	P584
show ip arp inspection vlan	ARP インспекションステータス、ARP ACL 名および ACL 妥当性検査終了後に DHCP スヌーピングデータベースが使用されているかを含む、VLAN 設定を表示	PE	P584

ip arp inspection

ARP インспекションを、スイッチでグローバルに有効にします。"no" を前に置くことでこの機能を無効にします。

文法

ip arp inspection

no ip arp inspection

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- このコマンドを利用しグローバルで ARP インспекションを有効にすると、"ip arp inspection vlan" コマンドで有効にされた VLAN でのみアクティブになります。(P580 を参照)
- ARP インспекションがグローバルで有効であり、選択した VLAN でも有効である場合、これらの VLAN の全ての ARP リクエスト / リプライパケットは CPU へリダイレクトされ、スイッチングは ARP インспекションエンジンによって処理されます。
- ARP インспекションがグローバルで無効の際、ARP インспекションが有効である物も含めて、全ての VLAN で非アクティブになります。
- ARP インспекションが無効の際、全ての ARP リクエストとリプライパケットは ARP インспекションエンジンを回避し、スイッチング方法はその他全てのパケットと同等になります。
- ARP インспекションをグローバルで無効にすることと、その後に再度有効にすることは、VLAN の ARP インспекション設定に影響を与えません。
- ARP インспекションがグローバルで無効の際、それぞれの VLAN で、ARP インспекションの設定は依然可能です。これらの設定変更は ARP インспекションが再度グローバルで有効になった時のみアクティブになります。

例

```
Console(config)#ip arp inspection
Console(config)#
```

ip arp inspection filter

ARP ACL を VLAN に適用します。"no" を前に置くことで ACL バインディングを削除します。

文法

ip arp inspection filter *arp-acl-name* vlan < *vlan-id* | *vlan-range* > { static }

no ip arp inspection filter *arp-acl-name* vlan *vlan-id*

- *arp-acl-name* — ACL 名 (最大 16 文字)
- *vlan-id* — VLAN ID (範囲 : 1-4093)
- *vlan-range* — ハイフンを使用し VLAN の連続する範囲を指定、またはカンマでそれぞれのエントリを区切り、VLAN のランダムグループを指定
- static — ARP パケットは指定された ACL のみにたいして妥当性検査を実行し、DHCP スヌーピングデータベースのアドレスバインディングはチェックされません。

初期設定

ARP ACL は VLAN にバウンドされていません。

Static mode : 無効

コマンドモード

Global Configuration

コマンド解説

- ARP ACL は P597 「ARP ACL」 で設定をおこないます。
- Static モードが有効の場合、スイッチは ARP パケットと指定された ARP ACL を比較します。許可 / 拒否ルールで IP-to-MAC address へのバインディングと一致しているパケットがそれに応じて処理されます。ACL ルールのいずれとも一致しないパケットは破棄されます。DHCP スヌーピングのアドレスバインディングはチェックされません。
- Static モードが無効の場合、パケットは最初に指定した ARP ACL パケットにたいして妥当性検査が行われます。拒否ルールに一致したパケットは破棄されます。全ての残ったパケットは DHCP スヌーピングデータベースのアドレスバインディングにたいして妥当性検査が行われます。

例

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

ip arp inspection log-buffer logs

ログメッセージに保存されるエントリの最大数および、それらメッセージ送信のレートを設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

ip arp inspection log-buffer logs *message-number* *interval seconds*

no ip arp inspection log-buffer logs

- *message-number* — ログメッセージに保存されるエントリの最大数
(範囲：0-256、0 はセーブ無効)
- *seconds* — ログメッセージが送信される間隔 (範囲：0-86400)

初期設定

メッセージ数：5

間隔：1 秒

コマンドモード

Global Configuration

コマンド解説

- このコマンドをスイッチに適用する前に、ARP インспекションを " ip arp inspection" で有効にしてください。(P576 参照)
- 初期設定ではロギングは ARP インспекションで有効であり、無効には出来ません。
- スイッチはパケットをドロップした際、エントリをログバッファに起きます。それぞれのエントリは、受信した VLAN、ポート番号、ソースおよびディスティネーション IP アドレス、ソースおよびディスティネーション MAC アドレスの情報を含みます。
- もし複数の同一な無効 ARP パケットが同じ VLAN で連続して受信される場合、ロギングファシリティはログバッファに 1 つのエントリと、対応する 1 つのシステムメッセージのみ生成します。
- ログバッファに保存可能なエントリの最大数はメッセージ番号パラメータで決定されます。もしログバッファがメッセージ送信前に一杯になった場合、一番古いエントリは最新のものに置き換えられます。
- スイッチは "seconds" 値によって決定されるレートコントロールを基にシステムメッセージを生成します。システムメッセージが生成された後、全てのエントリはログバッファからクリアされます。

例

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```


ip arp inspection validate

ARP パケットのアドレスコンポーネントに対し、追加検証を指定します。"no" を前に置くことで ACL バインディングを初期状態に戻します。

文法

ip arp inspection validate < dst-mac { ip } {src-mac } | ip { src-mac } | src-mac >

no ip arp inspection validate

- dst-mac — ARP ボディ内のターゲット MAC アドレスに対し、イーサネットヘッダのディスティネーション MAC アドレスの妥当性検査をおこないます。この検査は ARP レスポンスにたいして実行されます。有効時、異なる MAC アドレスのパケットは無効なパケットとして分類、破棄されます。
- ip — 不正および予期せぬ IP アドレスの ARP ボディをチェックします。アドレスは 0.0.0.0, 255.255.255.255 と、全ての IP マルチキャストアドレスを含みます。センサー IP アドレスは全ての ARP リクエストとレスポンスをチェックされます。ターゲット IP アドレスは ARP レスポンスのみチェックされます。
- src-mac — ハイフンを使用し VLAN の連続する範囲を指定、またはカンマでそれぞれのエントリを区切り、VLAN のランダムグループを指定

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 初期設定では、ARP インスペクションは ARP ACL または DHCP スヌーピングデータベースで指定された IP-to-MAC アドレスバインディングのみチェックを行います。

例

```
Console(config)#ip arp inspection validate dst-mac  
Console(config)#
```

ip arp inspection vlan

指定した VLAN で ARP インспекションを有効にします。"no" を前に置くことでこの機能を無効にします。

文法

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan < *vlan-id* | *vlan-range* >

- *vlan-id* — VLAN ID. (Range: 1-4093)
- *vlan-range* — ハイフンを使用し VLAN の連続する範囲を指定、またはカンマでそれぞれのエントリを区切り、VLAN のランダムグループを指定

初期設定

全ての VLAN で無効

コマンドモード

Global Configuration

コマンド解説

- ARP インспекションがグローバルで有効であり、選択した VLAN でも有効である場合、これらの VLAN の全ての ARP リクエスト / リプライパケットは CPU ヘリダイレクトされ、スイッチングは ARP インспекションエンジンによって処理されます。
- ARP インспекションがグローバルで無効の際、それは ARP インспекションが有効である物も含めて、全ての VLAN で非アクティブになります。
- ARP インспекションが無効の際、全ての ARP リクエストとリプライパケットは ARP インспекションエンジンを回避し、スイッチング方法はその他全てのパケットと同等になります。
- ARP インспекションをグローバルで無効にすることと、その後に再度有効にすることは、VLAN の ARP インспекション設定に影響を与えません。
- ARP インспекションがグローバルで無効の際、それぞれの VLAN で、ARP インспекションの設定は依然可能です。これらの設定変更は ARP インспекションが再度グローバルで有効になった時のみアクティブになります。

例

```
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

ip arp inspection limit

ポートを "trusted" として設定し、ARP インспекションから免除します。"no" を前に置くことで ACL バインディングを初期状態に戻します。

文法

ip arp inspection limit < rate *pps* | none >

no ip arp inspection limit

- *pps* — CPU で 1 秒ごとに処理可能な ARP パケットの最大数
(範囲：0-2048, 0 は ARP パケット転送無効)
- none — CPU で処理可能な ARP パケット数に制限は無し

初期設定

15

コマンドモード

Interface Configuration (Port)

コマンド解説

- このコマンドは Untrusted ポートにのみ適用されます。
- 入力 ARP パケットのレートが設定した制限を越えた場合、スイッチは、制限を超えた全てのパケットを破棄します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit rate 150
Console(config-if)#
```

ip arp inspection trust

ポートを "trusted" として設定し、ARP インспекションから免除します。"no" を前に置くことで ACL バインディングを初期状態に戻します。

文法

ip arp inspection trust
no ip arp inspection trust

初期設定

Untrusted

コマンドモード

Interface Configuration (Port)

コマンド解説

- Untrusted ポートに到着したパケットは設定された ARP インспекションと追加妥当性検査を受けます。trusted ポートに到着したパケットはそれら全てのテストを免除され、通常のスイッチルールに従って転送されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

show ip arp inspection configuration

ARP インспекションのグローバル設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection configuration

ARP inspection global information:

Global IP ARP Inspection status : disabled
Log Message Interval             : 1 s
Log Message Number               : 5
Need Additional Validation(s)    : No
Additional Validation Type       :
Console#
```

show ip arp inspection interface

ポートの trust ステータスおよび ARP インスペクションレートリミットを表示します。

文法

show ip arp inspection interface { interface }

- Interface
 - ethernet unit/port
 - unit — ユニット番号 "1"
 - port — ポート番号 (範囲: 1-26)

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection interface ethernet 1/5
```

Port Number	Trust Status	Limit Rate (pps)
Eth 1/1	trusted	150

```
Console#
```

show ip arp inspection log

関連付けられた VLAN、ポート、アドレスコンポーネントを含む、ログに保存されているエントリの情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection log
```

Total log entries number is 1

Num	VLAN	Port	Src IP Address	Dst IP Address	Src MAC Address	Dst MAC Address
1	1	11	192.168.2.2	192.168.2.1	00-04-E2-A0-E2-7C	FF-FF-FF-FF-FF-FF

```
Console#
```

show ip arp inspection statistics

処理された ARP パケット数に関する統計、または破棄された様々な理由の表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection statistics

ARP packets received before rate limit           : 0
ARP packets dropped due to rate limit             : 0
Total ARP packets processed by ARP Inspection    : 0
ARP packets dropped by additional validation (source MAC address) : 0
ARP packets dropped by additional validation (destination MAC address) : 0
ARP packets dropped by additional validation (IP address) : 0
ARP packets dropped by ARP ACLs                   : 0
ARP packets dropped by DHCP snooping              : 0

Console#
```

show ip arp inspection vlan

ARP インспекションステータス、ARP ACL 名および ACL 妥当性検査終了後に DHCP スヌーピングデータベースが使用されているかを含む、VLAN 設定を表示します。

文法

show ip arp inspection vlan { *vlan-id* | *vlan-range* }

- *vlan-id* — VLAN ID. (範囲 : 1-4093)
- *vlan-range* — ハイフンを使用し VLAN の連続する範囲を指定、またはカンマでそれぞれのエントリを区切り、VLAN のランダムグループを指定

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection vlan 1

VLAN ID      DAI Status      ACL Name      ACL Status
-----
1            disable        sales         static
Console#
```

4.10 ACL (Access Control Lists)

Access Control Lists (ACL) は IPv4 フレーム（アドレス、プロトコル、レイヤ 4 プロトコルポート番号または TCP コントロールコード）またはその他のフレーム（MAC アドレス、イーサネットタイプ）による IP パケットへのパケットフィルタリングを提供します。

入力されるパケットのフィルタリングを行うには、初めにアクセスリストを作成し、必要なルールを追加します。その後、リストに特定のポートをバインドします。

コマンド	機能	ページ
IPv4 ACLs	IP アドレス、TCP/UDP ポート番号、TCP コントロールコードに基づく ACL の設定	P585
MAC ACLs	ハードウェアアドレス、パケットフォーマット、イーサネットタイプに基づく ACL の設定	P592
ARP ACLs	ARP メッセージアドレスに基づく ACL の設定	P597
ACL Information	ACL 及び関連するルールの表示。各ポートの ACL の表示	P600

4.10.1 IPv4 ACL

IP アドレス、TCP/UDP ポート番号、プロトコルタイプ、TCP コントロールコードに基づく ACL の設定をおこないます。

IP ACL の設定を行うには、初めにアクセスリストを作成し、必要なルールを追加します。その後、リストに特定のポートをバインドします。

コマンド	機能	モード	ページ
access-list IP	IPv4 ACL の作成と configuration mode への移行	GC	P586
permit,deny	ソース IPv4 アドレスが一致するパケットのフィルタリング	IPv4-STD-ACL	P587
permit,deny	ソース又はディスティネーション IPv4 アドレス、TCP/UDP ポート番号、プロトコルタイプ、TCP コントロールコードに基づくフィルタリング	IPv4-EXT-ACL	P588
ip access-group	IPv4 ACL へのポートの追加	IC	P590
show ip access-group	IPv4 ACL にアサインされたポートの表示	PE	P591
show ip access-list	設定済み IPv4 ACL のルールの表示	PE	P591

コマンドラインインタフェース

ACL (Access Control Lists)

access-list ip

IP ACL を追加し、スタンダード又は拡張 IPv4 ACL の設定モードに移行します。"no" を前に置くことで特定の ACL を削除します。

文法

access-list ip < standard | extended > *acl_name*

no access-list ip < standard | extended > *acl_name*

- standard —ソース IP アドレスに基づくフィルタリングを行う ACL
- extended —ソース又はディステーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号に基づくフィルタリングを行う ACL
- *acl_name* — ACL 名 (最大 16 文字)

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 新しい ACL を作成した場合や、既存の ACL の設定モードに移行した場合、"permit" 又は "deny" コマンドを使用し、新しいルールを追加します。ACL を作成するには、最低 1 つのルールを設定する必要があります。
- ルールを削除するには "no permit" 又は "no deny" コマンドに続けて設定済みのルールを入力します。
- 1 つの ACL には最大 128 個のルールが設定可能です。

例

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

関連するコマンド

permit, deny (P587)

ip access-group (P590)

show ip access-list (P591)

permit,deny (Standard IP ACL)

スタンダード IPv4 ACL ルールを追加します。本ルールでは特定のソース IP アドレスからのパケットへのフィルタリングが行えます。"no" を前に置くことでルールを削除します。

文法

[permit | deny] [any | source bitmask | host source] { time-range time-range-name }

no [permit | deny] [any | source bitmask | host source]

- any — すべての IP アドレス
- source — ソース IP アドレス
- bitmask — 一致するアドレスビットを表す 10 進数値
- host — 特定の IP アドレスを指定
- time-range-name — タイムレンジ名（範囲：1-30 文字）

初期設定

なし

コマンドモード

Standard ipv4 ACL

コマンド解説

- 新しいルールはリストの最後に追加されます。
- アドレスビットマスクはサブネットマスクと似ており、4 つの 0-255 の値で表示され、それぞれがピリオド (.) により分割されています。2 進数のビットが "1" の場合、一致するビットであり、"0" の場合、拒否するビットとなります。ビットマスクはビット毎に特定の IP アドレスと共に使用し、ACL が指定した入力 IP パケットのアドレスと比較されます。

例

本例では、10.1.1.21 のソースアドレスへの許可 (permit) ルールとビットマスクを使用した 168.92.16.x-168.92.31.x までのソースアドレスへの許可 (permit) ルールを設定しています。

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

関連するコマンド

access-list ip (P586)

time range (P434)

permit,deny (Extended IPv4 ACL)

拡張 IPv4 ACL へのルールの追加を行います。ソース又はディスティネーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号、TCP コントロールコードに基づくフィルタリングを行います。"no" を前に置くことでルールの削除を行います。

文法

```
[no] {permit | deny} [ protocol-number | udp ]  
    { any | source address-bitmask | host source }  
    { any | destination address-bitmask | host destination }  
    [ precedence precedence ] [ tos tos ] [ dscp dscp ]  
    [ source-port sport [ bitmask ] ] [ destination-port dport [ port-bitmask ] ]  
    { time-range time-range-name }
```

```
[no] {permit | deny} tcp  
    { any | source address-bitmask | host source }  
    { any | destination address-bitmask | host destination }  
    [ precedence precedence ] [ tos tos ] [ dscp dscp ]  
    [ source-port sport [ bitmask ] ] [ destination-port dport [ port-bitmask ] ]  
    [ control-flag control-flags flag-bitmask ]
```

- *protocol-number* — 特定のプロトコル番号 (範囲: 0-255)
- *source* — ソース IP アドレス
- *destination* — ディスティネーション IP アドレス
- *address-bitmask* — アドレスビットマスク
- *host* — 特定の IP アドレスの指定
- *precedence* — IP precedence レベル (範囲: 0-7)
- *tos* — ToS レベル (範囲: 0-15)
- *dscp* — DSCP プライオリティレベル (範囲: 0-63)
- *sport* — プロトコル * ソースポート番号 (範囲: 0-65535)
- *dport* — プロトコル * ディスティネーションポート番号 (範囲: 0-65535)
- *port-bitmask* — マッチするポートビットを表す 10 進数 (範囲: 0-65535)
- *control-flags* — TCP ヘッダのバイト 14 でフラッグビットを指定する 10 進数 (ビットストリングを表す) (範囲: 0-63)
- *flag-bitmask* — マッチするコードビットを表す 10 進数
- *time-range-name* — タイムレンジ名 (範囲: 1-30 文字)

初期設定

なし

コマンドモード

Extended IPv4 ACL

コマンド解説

- 新しいルールはリストの最後に追加されます。
- アドレスビットマスクはサブネットマスクと似ており、4 つの 0-255 の値で表示され、それぞれがピリオド (.) により分割されています。2 進数のビットが "1" の場合、一致するビットであり、"0" の場合、無視するビットとなります。ビットマスクはビット毎に特定の IP アドレスと共に使用し、ACL が指定した入力 IP パケットのアドレスと比較されます。
- 同じルール内で Precedence 及び ToS の両方を指定することができます。しかし、DSCP を使用した場合、Precedence 及び ToS は指定することができません。
- コントロールビットマスクは、コントロールコードに使用される 10 進数の値です。10 進数の値を入力し、等価な 2 進数のビットが "1" の場合、一致するビットであり、"0" の場合、無視するビットとなります。以下のビットが指定されます。
 - 1 (fin) — Finish
 - 2 (syn) — Synchronize
 - 4 (rst) — Reset
 - 8 (psh) — Push
 - 16 (ack) — Acknowledgement
 - 32 (urg) — Urgent pointer
- 例えば、コード値及びコードマスクを利用し、パケットをつかむには以下のフラグをセットします。
 - 有効な SYN flag — "control-code 2 2"
 - 有効な SYN 及び ACK — "control-code 18 18"
 - 有効な SYN 及び無効な ACK — "control-code 2 18"

例

本例では、ソースアドレスがサブネット 10.7.1.x 内の場合、すべての入力パケットを許可します。

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

本例では、ディスティネーション TCP ポート番号 80 のクラス C アドレス 192.168.1.0 からすべてのディスティネーションアドレスへの TCP パケットを許可します。

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
destination-port 80
Console(config-ext-acl)##
```

関連するコマンド

access-list ip (P586)

time range (P434)

コマンドラインインタフェース

ACL (Access Control Lists)

ip access-group

IPv4 ACL へのポートのバインドを行います。"no" を前に置くことでポートを外します。

文法

ip access-group *acl_name* in { time-range *time-range-name* }

no ip access-group *acl_name* in

- *acl_name* — (最大 16 文字)
- in — 入力パケットへのリスト
- *time-range-name* — タイムレンジ名 (範囲：1-30 文字)

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- ポートにた 1 つの ACL のみ設定可能です。
- ポートがすでに ACL を設定済みで、他の ACL をバインドした場合、新しくバインドした ACL が有効となります。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

関連するコマンド

show ip access-list (P591)

time range (P434)

show ip access-group

IP ACL のポートの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip access-group
Interface ethernet 1/2
  IP access-list david in
Console#
```

関連するコマンド

ip access-group (P590)

show ip access-list

設定済みの IPv4 ACL のルールを表示します。

文法

show ip access-list < standard | extended > *acl_name*

- standard —スタンダード IP ACL
- extended —拡張 IP ACL
- *acl_name* — ACL 名 (最大 16 文字)

コマンドモード

Privileged Exec

例

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.16.0 255.255.240.0
Console#
```

関連するコマンド

permit, deny (P587)

ip access-group (P590)

コマンドラインインタフェース

ACL (Access Control Lists)

4.10.2 MAC ACL

コマンド	機能	モード	ページ
access-list mac	MAC ACL の作成と configuration mode への移行	GC	P592
permit,deny	ソース又はディスティネーションアドレス、パケットフォーマット、イーサネットタイプに基づくフィルタリング	MAC-ACL	P593
mac access-group	MAC ACL へのポートの追加	IC	P595
show mac access-group	MAC ACL に指定したポートの表示	PE	P595
show mac access-list	設定済み MAC ACL のルールの表示	PE	P596

access-list mac

MAC アドレスリストを追加し、MAC ACL 設定モードに移行します。"no" を前に置くことで指定した ACL を削除します。

文法

access-list mac *acl_name*

no access-list mac *acl_name*

- *acl_name* — ACL 名（最大 16 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 新しい ACL を作成した場合や、既存の ACL の設定モードに移行した場合、"permit" 又は "deny" コマンドを使用し、新しいルールを追加します。ACL を作成するには、最低 1 つのルールを設定する必要があります。
- ルールを削除するには "no permit" 又は "no deny" コマンドに続けて設定済みのルールを入力します。
- 1 つの ACL には最大 128 個のルールが設定可能です。

例

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

関連するコマンド

permit, deny (MAC ACL) (P587)

mac access-group (P590)

show mac access-list (P591)

permit,deny (MAC ACL)

MAC ACL へのルールの追加を行います。MAC ソース / ディスティネーションアドレス、イーサネットプロトコルタイプによりフィルタリングを行います。"no" を前に置くことでルールを削除します。

文法

[no] {permit | deny}

{any | host source|source address-bitmask}

{any | host destination | destination address-bitmask}

[vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]

{ time-range time-range-name }

※初期設定は Ethernet2 パケットです。

[no] {permit | deny} tagged-eth2

{any | host source|source address-bitmask}

{any | host destination | destination address-bitmask}

[vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]

[no] {permit | deny} untagged-eth2

{any | host source|source address-bitmask}

{any | host destination | destination address-bitmask}

[ethertype protocol [protocol-bitmask]]

{ time-range time-range-name }

[no] {permit | deny} tagged-802.3

{any | host source|source address-bitmask}

{any | host destination | destination address-bitmask}

[vid vid vid-bitmask]

[no] {permit | deny} untagged-802.3

{any | host source|source address-bitmask}

{any | host destination | destination address-bitmask}

{ time-range time-range-name }

- *protocol-number* — 特定のプロトコル番号 (範囲: 0-255)
- tagged-eth2 — タグ付きイーサネット 2 パケット
- untagged-eth2 — タグ無しイーサネット 2 パケット定
- tagged-802.3 — タグ付きイーサネット 802.3 パケット
- untagged-802.3 — タグ無しイーサネット 802.3 パケット
- any — すべての MAC ソース / ディスティネーションアドレス
- host — 特定の MAC アドレス
- source — ソース MAC アドレス
- destination — ビットマスクを含むディスティネーション MAC アドレス範囲

コマンドラインインタフェース

ACL (Access Control Lists)

- *address-bitmask* — MAC アドレスのビットマスク (16 進数)
- *vid* — VLAN ID (範囲: 1-4094)
- *vid bitmask* — VLAN ビットマスク (範囲: 1-4095)
- *protocol* — イーサネットプロトコル番号 (範囲: 600-fff 16 進数)
- *protocol -bitmask* — プロトコルビットマスク (範囲: 600-fff 16 進数)
- *time-range-name* — タイムレンジ名 (範囲: 1-30 文字)

初期設定

なし

コマンドモード

MAC ACL

コマンド解説

- 新しいルールはリストの最後に追加されます。
- イーサネットタイプオプションは Ethernet II のフィルタにのみ使用します。
- イーサネットプロトコルタイプのリストは RFC 1060 で定義されていますが、一般的なタイプは以下の通りです。
 - 0800(IP)
 - 0806(ARP)
 - 8137(IPX)

例

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

関連するコマンド

access-list mac (P592)

time range (P434)

mac access-group

MAC ACL へのポートのバインドを行います。"no" を前に置くことでポートを外します。

文法

mac access-group *acl_name* in { time-range *time-range-name* }

no mac access-group *acl_name* < in | out >

- *acl_name* — ACL 名 (最大 16 文字)
- in — 入力パケットへのリスト
- *time-range-name* — タイムレンジ名 (範囲: 1-30 文字)

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

関連するコマンド

show mac access-list (P596)

time range (P434)

show mac access-group

MAC ACL に指定されたポートを表示します。

コマンドモード

Privileged Exec

例

```
Console#show mac access-group
Interface ethernet 1/5
  MAC access-list M5 in
Console#
```

関連するコマンド

mac access-group (P595)

コマンドラインインタフェース

ACL (Access Control Lists)

show mac access-list

MAC ACL のルールを表示します。

文法

show mac access-list { *acl_name* }

- *acl_name* — ACL 名 (最大 16 文字)

コマンドモード

Privileged Exec

例

```
Console#show mac access-list
MAC access-list jerry:
    permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

関連するコマンド

permit, deny (P593)

mac access-group (P595)

4.10.3 ARP ACL

ARP リクエスト・リプライメッセージを含む、IP または MAC アドレスに基づく ACL の設定を行います。ARP ACL の設定を行うには、初めにアクセスリストを作成し必要な ルールを追加します。その後、" ip arp inspection vlan" コマンド（P580）を使用し、アクセスリストを 1 つまたは 1 つ以上の VLAN ヘバインドします。

コマンド	機能	モード	ページ
access-list larp	ARP ACL を作成し、設定モードへ移行します	GC	P597
permit,deny	ARP メッセージのソースまたはディスティネーションアドレスが一致するパケットのフィルタリング	ARP-ACL	P598
show arp access-list	ARP ACL に設定されたルールを表示	PE	P599

access-list arp

ARP アクセスリストを追加し、ARP ACL の設定モードに移行します。"no" を前に置くことで特定の ACL を削除します。

文法

access-list arp *acl-name*

no access-list arp *acl-name*

- *acl-name* — ACL 名（最大 16 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 新しい ACL を作成や、既存の ACL の設定モードに移行した時、"permit" 又は "deny" コマンドを使用し、新しいルールを追加します。ACL を作成するには、最低 1 つのルールを設定する必要があります。
- ルールを削除するには "no permit" 又は "no deny" コマンドに続けて設定済みのルールを入力します。
- 1 つの ACL には最大 128 個のルールが設定可能です。

例

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

関連するコマンド

permit, deny (P598)

show arp access-list (P599)

permit,deny (ARP ACL)

ARP ACL ヘルールを追加します。このルールは、ARP メッセージで指定されたソースまたはディスティネーションアドレスと一致しているパケットをフィルタします。"no" を前に置くことでルールを削除します。

文法

[no] { permit | deny }

ip { any | host *source-ip* | *source-ip* *ip-address-bitmask* }

mac { any | host *source-ip* | *source-ip* *ip-address-bitmask* } [log]

注意：この形式はリクエストまたはレスポンスパケットを示します。

[no] { permit | deny } request

ip { any | host *source-ip* | *source-ip* *ip-address-bitmask* }

mac { any | host *source-mac* | *source-mac* *mac-address-bitmask* } [log]

[no] { permit | deny } response

ip { any | host *source-ip* | *source-ip* *ip-address-bitmask* }

{ any | host *destination-ip* | *destination-ip* *ip-address-bitmask* }

mac { any | host *source-mac* | *source-mac* *mac-address-bitmask* }

[any | host *destination-mac* | *destination-mac* *mac-address-bitmask*] [log]

- *source-ip* — ソース IP アドレス
- *destination-ip* — ディスティネーション IP アドレス
- *ip-address-bitmask* — マッチするアドレスビットを示す IPv4 番号
- *source-mac* — ソース MAC アドレス
- *destination-mac* — ディスティネーション MAC アドレス範囲
- *mac-address-bitmask* — MAC アドレスビットマスク
- log — アクセスコントロール縁撮るにマッチしたパケットのログ

初期設定

なし

コマンドモード

ARP ACL

コマンド解説

- 新しいルールはリストの最後に追加されます。

例

```
Console(config-arp-acl)#permit response ip any 192.168.0.0 255.255.0.0
mac any any
Console(config-mac-acl)#
```

関連するコマンド

access-list arp (P597)

show arp access-list

設定済みの ARP ACL のルールを表示します。

文法

show arp access-list { *acl-name* }

- *acl-name* — ACL 名 (最大 16 文字)

コマンドモード

Privileged Exec

例

```
Console#show arp access-list
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

関連するコマンド

permit, deny (P598)

コマンドラインインタフェース

ACL (Access Control Lists)

4.10.4 ACL 情報の表示

コマンド	機能	モード	ページ
show access-group	それぞれのポートに割り当てられた ACL の表示	PE	P600
show access-list	全ての ACL と関連するルールの表示	PE	P600

show access-group

ACL のポートの指定を表示します。

コマンドモード

Privileged Executive

例

```
Console#show access-group
Interface ethernet 1/2
  IP access-list david
  MAC access-list jerry
Console#
```

show access-list

すべての ACL とユーザ定義マスクを含む関連するルールを表示します。

コマンドモード

Privileged Exec

例

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.16.0 255.255.240.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
IP access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  permit any any
Console#
```

4.11 インタフェース

コマンド	機能	モード	ページ
インタフェース設定			
interface	本機の DHCP クライアント ID の指定	GC	P602
alias	インタフェースのエイリアス名を設定	IC	
capabilities	オートネゴシエーション無効時の通信速度、通信方式の設定	IC	P603
description	インタフェースタイプの設定及び interface configuration モードへの変更	IC	P605
flowcontrol	インタフェースへのフローコントロール設定	IC	P606
media-type	コンボポートの固定ポートタイプを選択	IC	P607
negotiation	インタフェースへのオートネゴシエーションの設定	IC	P608
shutdown	インタフェースの無効	IC	P609
speed-duplex	インタフェースの解説	IC	P610
switchport packet-rate*	ストームコントロールの閾値を設定	IC	P611
clear counters	インタフェースの統計情報のクリア	PE	P612
show interfaces brief	操作上のステータス、VLAN ID、デフォルトプライオリティ、speed/duplex、ポートタイプを含む、キー情報のサマリを表示	PE	P613
show interfaces counters	インタフェースの統計情報の表示	NE,P E	P614
show interfaces status	インタフェースの設定状況を表示	NE,P E	P616
show interfaces switchport	インタフェースの管理、運用状況の表示	NE,P E	P617
ケーブル診断			
test cable-diagnostics	ケーブル診断の実行	PE	P619
show cable-diagnostics	ケーブル診断結果の表示	PE	P620
パワーセービング			
power-save	指定のポートでパワーセービングモードを有効化	IC	P621
show power-save	パワーセービングの設定情報を表示	PE	P622

* このコマンドでポートのハードウェアレベルストームコントロールを有効にした時、同じポートで "auto-traffic-control" コマンド (P650) によりソフトウェアレベル自動ストームコントロールが設定されている場合は無効になります。

interface

インタフェースの設定及び interface configuration モードへの移行が行えます。"no" を前に置くことでトランクを解除することができます。

文法

interface *interface*

no interface

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* — Channel ID (1-12)
 - vlan *vlan-id* — VLAN ID (1-4093)

初期設定

なし

コマンドモード

Global Configuration

例

本例では 3 番ポートの指定を行っています。

```
Console(config)#interface ethernet 1/3
Console(config-if)#
```


alias

インタフェースのエイリアス名を設定します。"no" を前に置くことでエイリアス名を削除します。

文法

alias *string*

no alias

- *string* — インタフェースに名前を設定します。(範囲：1-64 文字)

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

本例は、3 番ポートに名前を付けています。

```
Console(config)#interface ethernet 1/3
Console(config-if)#alias finance
Console(config-if)#
```

capabilities

オートネゴシエーション時のポートの通信方式を設定します。

"no" を前に置きパラメータを設定することで指定したパラメータの値を削除します。パラメータを設定せず "no" を前に置いた場合には初期設定に戻ります。

文法

capabilities <1000full | 100full | 100half | 10full | 10half | flowcontrol | symmetric>

no capabilities <1000full | 100full | 100half | 10full | 10half | flowcontrol | symmetric>

- 1000full — 1000Mbps full-duplex 通信
- 100full — 100Mbps full-duplex 通信
- 100half — 100Mbps half-duplex 通信
- 10full — 10Mbps full-duplex 通信
- 10half — 10Mbps half-duplex 通信
- flowcontrol — flow control サポート
- symmetric — フローコントロールからポーズフレームを送受信(本機ではsymmetric ポーズフレームのみがサポートされています)。(ギガビット環境のみ)

初期設定

- 100BASE-TX : 10half, 10full, 100half, 100full
- 1000BASE-T : 10half, 10full, 100half, 100full, 1000full
- SFP : 1000full

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

"negotiation" コマンドを使用しオートネゴシエーションが有効になっている場合、"capabilities" コマンドで指定された内容に基づき最適な通信方式でリンクを行います。オートネゴシエーションが無効の場合には "speed-duplex" コマンドと "flowcontrol" コマンドを使用して手動で通信方式を設定する必要があります。

例

本例では 5 番ポートに 100half, 100full 及びフローコントロールを設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

関連するコマンド

speed-duplex (P610)

negotiation (P608)

flow control (P606)

description

各インタフェースの解説を行います。"no" を前に置くことで解説を削除します。

文法

description *string*

no description

- *string* — 設定や監視作業を行いやすくするための各ポートの接続先などのコメントや解説（範囲：1-64 文字）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

本例は、3 番ポートに解説を加えている設定です。

```
Console(config)#interface ethernet 1/3
Console(config-if)#description RD-SW#3
Console(config-if)#
```

flow control

フローコントロールを有効にします。"no" を前に置くことでフローコントロールを無効にします。

文法

flowcontrol

no flowcontrol

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ・ フローコントロールを使用するとスイッチのバッファ容量がいっぱいになった場合に通信のロスが発生するのを防ぐことができます。フローコントロールを有効にした場合、full-duplex では IEEE802.3x 準拠、half-duplex ではバックプレッシャを用いてフローコントロールを行います。"negotiation" コマンドを使用しオートネゴシエーションを有効にした場合、"capabilities" コマンドによりフローコントロールを使用するか決定されます。オートネゴシエーション時にフローコントロールを有効にするためには各ポートの機能 (Capabilities) に "flowcontrol" を含める必要があります。
- ・ flowcontrol" コマンド又は "no flowcontrol" コマンドを使用してフローコントロールを固定設定する場合には、"no negotiation" コマンドを使用してオートネゴシエーションを無効にする必要があります。
- ・ HUB と接続されたポートではフローコントロールを使用することは避けて下さい。使用した場合にはバックプレッシャのジャム信号が全体のネットワークパフォーマンスを低下させる可能性があります。

例

本例では 5 番ポートでフローコントロールを有効にしています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

関連するコマンド

negotiation (P608)

capabilities (flowcontrol, symmetric) (P603)

media-type

コンビネーションポート 25-26 に、選択されたポートタイプを固定設定します。
"no" を前に置くことで設定を初期値に戻します。

文法

media-type *mode*

no media-type

- *mode* — モードを選択
 - copper-forced — 常に組み込まれた RJ-45 ポートを使用
 - sfp-forced — 常に SFP ポート (モジュールが未装着でも) を使用
 - sfp-preferred-auto — 両方のコンビネーションタイプが作用し、SFP ポートが有効なリンクを保持している時、SFP ポートを使用

初期設定

sfp-preferred-auto

コマンドモード

Interface Configuration (Ethernet- ポート 25-26)

例

```
Console(config)#interface ethernet 1/25
Console(config-if)#media-type copper-forced
Console(config-if)#
```

negotiation

各ポートのオートネゴシエーションを有効にします。"no" を前に置くことでオートネゴシエーションを無効にします。

文法

negotiation
no negotiation

初期設定

有効 (Enabled)

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- オートネゴシエーションが有効になっている場合、"capabilities" コマンドに指定された内容に基づき、最適な通信方法を選択します。オートネゴシエーションが無効の場合には "speed-duplex" コマンドと "flowcontrol" コマンドを使用して手動で通信方式を設定する必要があります。
- オートネゴシエーションが無効の場合には RJ-45 ポートの MDI-MDI-X 自動認識機能も無効となります。

例

本例では 10 番ポートをオートネゴシエーションの設定にしています。

```
Console(config)#interface ethernet 1/10
Console(config-if)#negotiation
Console(config-if)#
```

関連するコマンド

capabilities (P603)
speed-duplex (P610)

shutdown

インタフェースを無効にします。"no" を前に置くことでインタフェースを有効にします。

文法

shutdown
no shutdown

初期設定

すべてのインタフェースが有効になっています。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

コリジョンの発生などによる異常な動作を回避するなどの目的や、セキュリティの目的でポートを無効にすることができます。問題が解決した場合や、ポートを使用する場合には再度ポートを有効にすることができます。

例

本例では 5 番ポートを無効にしています。

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

speed-duplex

オートネゴシエーションを無効にした場合の通信速度及び通信方式の設定が行えます。"no"を前に置くことで初期設定に戻します。

文法

speed-duplex < 100full | 100half | 10full | 10half >

no speed-duplex

- 100full — 100 Mbps full-duplex **固定**
- 100half — 100 Mbps half-duplex **固定**
- 10full — 10 Mbps full-duplex **固定**
- 10half — 10 Mbps half-duplex **固定**

初期設定

- 初期設定ではオートネゴシエーションが有効になっています。
- オートネゴシエーションが無効時、初期設定値は 100BASE-TX、ギガビットイーサネット共に 100full です。

コマンドモード

Interface Configuration (Ethernet、Port Channel)

コマンド解説

- 通信速度と Duplex を固定設定にするためには "speed-duplex" コマンドを使用します。又、"no negotiation" コマンドを使用しオートネゴシエーションを無効にしてください。
- "negotiation" コマンドを使用しオートネゴシエーションが有効になっている場合は "capabilities" コマンドを使用することで最適な接続を行うことができます。オートネゴシエーション時の通信速度、通信方式の設定を行うためには "capabilities" コマンドを使用する必要があります。

例

本例では 5 番ポートに 100Mbps half-duplex 固定の設定を行っています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

関連するコマンド

negotiation (P608)

capabilities (P603)

switchport packet-rate

ブロードキャスト、マルチキャスト、未知のユニキャストストームコントロールの設定をします。"no" を前に置くことでブロードキャストストームコントロールを無効にします。

文法

switchport [broadcast | multicast | unicast] **packet-rate** *rate*

no switchport [broadcast | multicast | unicast]

- broadcast — ブロードキャストトラフィックのストームコントロールを指定
- multicast — マルチキャストトラフィックのストームコントロールを指定
- unicast — ユニキャストトラフィックのストームコントロールを指定
- *rate* — レートの閾値（範囲：500-262143packets/ 秒）

初期設定

ブロードキャストストームコントロール：有効、パケットレートリミット =64Kbps

マルチキャストストームコントロール：無効

未知のユニキャストストームコントロール：無効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- トラフィックが、ブロードキャスト、マルチキャスト、未知のユニキャストトラフィックが指定した閾値を超えた場合、超えたパケットは破棄されます。
- 同じインタフェース上で帯域制御とストームコントロールの両方を使用することは、予期せぬ結果を導く可能性があります。
例えば、ファーストイーサネットポートで "switchport broadcast packet-rate 500," コマンドでブロードキャストストームコントロールを 500kbps に設定し、"rate-limit input 20000" コマンドで帯域制御を 20000Kbps に設定した場合、2000kbps はラインスピードの 1/5 (100Mbps) ですから、受信レートは実際 100Kbps またはストームコントロールコマンドで設定されたリミット、500Kbps の 1/5 になります。同じインタフェース上にこれら両方のコマンドを使用することは賢明ではありません。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

コマンドラインインタフェース インタフェース

clear counters

インタフェースの統計情報をクリアします。

文法

clear counters *interface*

- *Interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

統計情報は電源をリセットした場合のみ初期化されます。本機能を使用した場合、現在の管理セッションで表示されている統計情報はリセットされます。但し、一度ログアウトし再度管理画面にログインした場合には統計情報は最後に電源をリセットした時からの値となります。

例

本例では 5 番ポートの統計情報をクリアしています。

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces brief

オペレーショナルステータス、ネイティブ VLAN ID、デフォルトプライオリティ、スピード / デュプレックスモード、全てのポートのポートタイプを含む、キー情報のサマリを表示します。

文法

show interfaces status brief

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show interfaces brief
Interface Name      Status  PVID Pri Speed/Duplex  Type
Trunk
-----
Eth 1/ 1           Down    1   0 Auto          100TX
None
Eth 1/ 2           Down    1   0 Auto          100TX
None
Eth 1/ 3           Down    1   0 Auto          100TX
None
Eth 1/ 4           Down    1   0 Auto          100TX
None
Eth 1/ 5           Down    1   0 Auto          100TX
None
Eth 1/ 6           Down    1   0 Auto          100TX
None
.
.
.
```

show interfaces counters

インタフェースの統計情報を表示します。

文法

show interfaces counters { *interface* }

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲：1-26)
 - port-channel *channel-id* (範囲：1-12)

初期設定

すべてのポートのカウンタを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- ポートを指定しない場合は、すべてのポートの状況が表示されます。
- 本コマンドを使用した際に表示される情報の詳細は 58 ページの「ポート・トランク統計情報表示」を参照して下さい。

例

```

Console#show interfaces counters ethernet 1/7
Ethernet 1/ 7
===== IF table Stats =====
0 Octets Input
0 Octets Output
0 Unicast Input
0 Unicast Output
0 Discard Input
0 Discard Output
0 Error Input
0 Error Output
0 Unknown Protos Input
0 QLen Output
===== Extended Iftable Stats =====
0 Multi-cast Input
0 Multi-cast Output
0 Broadcast Input
0 Broadcast Output
===== Ether-like Stats =====
0 Alignment Errors
0 FCS Errors
0 Single Collision Frames
0 Multiple Collision Frames
0 SQE Test Errors
0 Deferred Transmissions
0 Late Collisions
0 Excessive Collisions
0 Internal Mac Transmit Errors
0 Internal Mac Receive Errors
0 Frames Too Long
0 Carrier Sense Errors
0 Symbol Errors
===== RMON Stats =====
0 Drop Events
0 Octets
0 Packets
0 Broadcast PKTS
0 Multi-cast PKTS
0 Undersize PKTS
0 Oversize PKTS
0 Fragments
0 Jabbers
0 CRC Align Errors
0 Collisions
0 Packet Size <= 64 Octets
0 Packet Size 65 to 127 Octets
0 Packet Size 128 to 255 Octets
0 Packet Size 256 to 511 Octets
0 Packet Size 512 to 1023 Octets
0 Packet Size 1024 to 1518 Octets
Console#

```

show interfaces status

インタフェースの状態を表示します。

文法

show interfaces status *interface*

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)
 - vlan *vlan-id* — VLAN ID (1-4093)

初期設定

すべてのインタフェースの状況が表示されます。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- ポートを指定しない場合は、すべてのポートの状況が表示されます。
- 本コマンドを使用した際に表示される情報の詳細は P51 「接続状況の表示」を参照して下さい。

例

```
Console#show interfaces status ethernet 1/7
Information of Eth 1/7
Basic Information:
  Port Type           : 100TX
  Mac Address         : 00-1A-7E-AB-FD-19
Configuration:
  Name                :
  Port Admin          : Up
  Speed-duplex        : Auto
  Capabilities        : 10half, 10full, 100half, 100full
  Broadcast Storm     : Enabled
  Broadcast Storm Limit : 64 Kbits/second
  Multicast Storm     : Disabled
  Multicast Storm Limit : 64 Kbits/second
  Unknown Unicast Storm : Disabled
  Unknown Unicast Storm Limit : 64 Kbits/second
  Flow Control        : Disabled
  LACP                : Disabled
  Port Security       : Disabled
  Max MAC Count       : 0
  Port Security Action : None
  Media Type          : Copper forced
Current Status:
  Link Status         : Down
  Operation Speed-duplex : 100full
  Flow Control Type   : None
Console#
```

show interfaces switchport

指定したポートの管理、運用状況を表示します。

文法

show interfaces switchport { *interface* }

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

初期設定

すべてのインタフェースを表示

コマンドモード

Normal Exec, Privileged Exec

例

本例は 7 番ポートの情報を表示しています。

```
Console#show interfaces switchport ethernet 1/7
Information of Eth 1/7
Broadcast Threshold           : Enabled, 64 Kbits/second
Multicast Threshold           : Disabled
Unknown Unicast Threshold     : Disabled
LACP Status                   : Disabled
Ingress Rate Limit            : Disabled, 64 Kbits per second
Egress Rate Limit             : Disabled, 100000 Kbits per second
VLAN Membership Mode          : Hybrid
Ingress Rule                  : Disabled
Acceptable Frame Type         : All frames
Native VLAN                   : 1
Priority for Untagged Traffic  : 0
GVRP Status                   : Disabled
Allowed VLAN                   : 1(u), 4093(t)
Forbidden VLAN                :
802.1Q-tunnel Status          : Disable
802.1Q-tunnel Mode            : NORMAL
802.1Q-tunnel TPID            : 8100(Hex)
Console#
```

コマンド解説

項目	解説
Broadcast threshold	ブロードキャストストーム制御機能の有効 / 無効の表示。有効時にはしきい値を表示 (P611 参照)
Multicast Threshold	マルチキャストストーム制御機能の有効 / 無効の表示。有効時にはしきい値を表示 (P611 参照)
Unknown-unicast Threshold	未知のユニキャストストーム制御機能の有効 / 無効の表示。有効時にはしきい値を表示 (P611 参照)
Lacp status	LACP の有効 / 無効 (P625 参照)
Ingress/ Egress rate limit	入力 / 出力帯域制御の有効 / 無効。現在の設定 (P644 参照)
VLAN membership mode	トランク又は Hybrid のメンバーモードを表示 (P717 参照)
Ingress rule	イングレスフィルタの有効 / 無効の表示 (P716 参照)
Acceptable frame type	VLAN フレームは、全てのフレームタイプか、タグフレームのみ受け取り可能か (P714 参照)
Native VLAN	デフォルトポート VLAN ID の表示 (P718 参照)
Priority for untagged traffic	タグなしフレームへの初期設定のプライオリティの表示 (P747 参照)
Gvrp status	GVRP の有効 / 無効 (P704 参照)
Allowed Vlan	参加している VLAN の表示。"(u)" はタグなし、"(t)" はタグ (P715 参照)
Forbidden Vlan	GVRP によって動的に参加できない VLAN の表示 (P706 参照)
802.1Q-tunnel Status	このインタフェースで 802.1Q トンネルが有効時に表示 (P723 参照)
802.1Q-tunnel Mode	802.1Q トンネルまたは 802.1Q トンネルアップリンクのトンネルモードを表示 (P724 参照)
802.1Q-tunnel TPID	学習とパケットのスイッチングに使用される、タグプロトコル識別を表示 (P725 参照)

test cable-diagnostics

ケーブル障害（ショート、オープン、その他）を診断するため、指定したポートでケーブル診断を実行します。

文法

test cable-diagnostics interface *interface*

- *Interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号（範囲：1-26）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- ケーブル診断はデジタル信号処理 (DSP) テストメソッドを使用して実行されます。
- このケーブルテストは 7 ～ 140m のケーブルのみ正確に診断可能です。
- テストには約 5 秒かかります。テストが完了後、スイッチはただちにそれぞれのケーブルペアのおよその長さや状態、共通エラーを含む、診断結果を表示します。
- 診断で検出される可能性のある状態
 - OK：正確に終結したペア
 - Open：オープンペア、リンクパートナー無し
 - Short：ショートしたペア
 - Not Supported：リンクアップしているイーサネットポート、または 1000Mbps 下のスピードでリンクアップしているギガビットイーサネットポートについて表示されます。
 - Impedance mismatch：終端接続のインピーダンスが基準範囲外です。
- ケーブル診断実行中、ポートはリンクダウンします。

例

```
Console#test cable-diagnostics interface ethernet 1/25
Console#show cable-diagnostics interface ethernet 1/25
Port      Type Link Status Pair A (meters)  Pair B (meters)  Last Update
-----
Eth 1/25  GE   Up      OK (21)          OK (21)          2009-11-13 09:44:19
Console#
```

コマンドラインインタフェース インタフェース

show cable-diagnostics

ケーブル診断テストの結果を表示します。

文法

show cable-diagnostics interface *interface*

- *Interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)

コマンドモード

Privileged Exec

例

```
Console#show cable-diagnostics interface ethernet 1/25
Port      Type  Link Status Pair A (meters) Pair B (meters)  Last Update
-----
Eth 1/25  GE    Up      OK (21)      OK (21)  2009-11-13 09:44:19
Console#
```

power-save

指定されたポートで、パワーセービングモードを有効にします。

文法

power-save
no power-save

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- IEEE 802.3 はイーサネット 100m で稼動しているケーブル接続に基づいた標準およびサブシーケンス電源条件を定義しています。パワーセービングモードを有効にすることで、60m 以下のケーブル（20m 以下ではより顕著に）で使用電力を低減することが可能であり、信号安全性を保証し続けます。
- パワーセービングモードは銅メディアを使用しているギガビットイーサネットポートにのみ適用されます。
- パワーセービングはギガビット RJ-45 ポートでのみ有効に出来ます。
- 本機で提供されるパワーセービングメソッド
 - ・ リンクパートナー不在時のパワーセービング
通常稼動時、スイッチはリンクパートナーを見つけるために継続してオートネゴシエーションをし、たとえリンク接続が存在しないとしても、MAC インタフェースはパワーアップ状態を維持しています。
パワーセービングモードを使用時、スイッチはリンクパートナーの有無を決定するため、サーキットのエネルギーをチェックします。もし何も検出されない場合、スイッチはトランスミッタと受信電気回路の大部分を自動的にターンオフします。（スリープモードへ入ります）このモードでは、low-power energy-detection サーキットが連続的にケーブルのエネルギーをチェックします。エネルギー検出されない場合、スイッチは直ちにトランスミッタとレシーバ機能をターンオフし、MAC インタフェースをパワーアップします。
 - ・ リンクパートナーがいる時のパワーセービング
従来のイーサネット接続は、平均のネットワークケーブル長が短くても、最低 100m をサポートするために十分なパワーで機能しています。ケーブル長がより短い場合、信号衰弱はケーブル長に比例しているためパワー消費は低減出来ます。パワーセービングモード有効時、スイッチは特定のリンク上で使用された信号出力レベルを低減できるかどうかを決定するため、ケーブル長を分析します。

[注意] パワーセービングはツイストペアケーブルを使用した、ギガビットイーサネットポートでのみ実行可能です。アクティブリンクのパワーセービングモードは接続スピード 1Gbps でライン長が 60m 以下の時のみ稼動します。

例

```
Console(config)#interface ethernet 1/26
Console(config-if)#power-save
Console(config-if)#
```

show power-save

パワーセービングの設定を表示します。

文法

show power-save interface *interface*

- *Interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 25-26)

コマンドモード

Privileged Exec

例

```
Console#show power-save interface ethernet 1/26
Power Saving Status:
 Ethernet 1/26 : Enabled
Console#
```

4.12 リンクアグリゲーション

バンド幅拡張と、又ネットワーク障害時の回避のため、ポートを束ねた静的グループを設定することができます。また、IEEE802.1ad 準拠の Link Aggregation Control Protocol (LACP) を使用し、本機と他のデバイス間のトランクを自動的に行うこともできます。静的トランクでは、本機は Cisco EtherChannel 標準との互換性があります。動的トランクに関しては IEEE802.1ad 準拠の LACP となります。

2 つの 1000Mbps ポートをトランクした場合、full duplex 時には最大 4Gbps のバンド幅となります。

コマンド	機能	モード	ページ
手動設定コマンド			
interface port-channel	interface configuration モードへの移動とトランク設定	GC	P602
channel-group	トランクへのポートの追加	IC	P624
動的設定コマンド			
lacp	現在のインタフェースでの LACP の設定	IC	P625
lacp admin-key	ポートアドミンキーの設定	IC (Ethernet)	P627
lacp port-priority	LACP ポートプライオリティの設定	IC (Ethernet)	P628
lacp system-priority	ポート LACP システムプライオリティの設定	IC (Ethernet)	P629
lacp admin-key	ポートチャンネルアドミンキーの設定	IC(Port Channel)	P630
トランクステータス表示コマンド			
show interfaces status port-channel	トランク情報の表示	NE,PE	P616
show lacp	LACP 関連情報の表示	PE	P631

トランク設定ガイドライン

- ループを防ぐため、ネットワークケーブルを接続する前にトランクの設定を完了させて下さい。
- 各トランクは最大 8 ポートまでトランク可能です。
- トランクの両端のポートはトランクポートとして設定される必要があります。
- トランクに参加するすべてのポートは、通信速度、duplex モード、フローコントロール、VLAN、CoS などすべて同一の設定である必要があります。
- port-channel を使用し VLAN からの移動、追加、削除する場合、トランクされたすべてのポートは1つのものとして扱われます。
- STP、VLAN および IGMP の設定は、指定したポートチャンネルを使用しすべてのトランクに設定することができます。

LACP 設定ガイドライン

ポートを同一ポートチャンネルに設定するには以下の条件に一致する必要があります。

- ポートは同一の LACP システムプライオリティの必要があります
- ポートは同一のポートアドミンキーの必要があります (Ethernet Interface)
- チャンネルグループが形成される場合に、ポートチャンネルアドミンキーをセットしなければ、このキーは、グループのインタフェースのポートアドミンキーと同一の値に設定されます。
- ポートチャンネルアドミンキーを設定する場合には、ポートアドミンキーはチャンネルグループへの参加が可能な同じ値を設定する必要があります。
- リンクが落ちた場合、LACP ポートプライオリティはバックアップリンクを選択します。

channel-group

トランクにポートを追加します。"no" を前に置くことでポートをトランクからはずします。

文法

channel-group *channel-id*

no channel-group

- *channel-id* — トランク ID (範囲: 1-12)

初期設定

現在のポートが、指定したトランクに追加されます。

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 静的トランクの設定を行う場合、対向のスイッチは Cisco EtherChannel 標準と互換性がなくてはなりません。
- "no channel-group" コマンドを使うことでポートグループをトランクからはずします。
- "no interfaces port-channel" コマンドを使うことでスイッチからトランクを削除します。

例

本例では、trunk 1 を生成し、11 番ポートをメンバーに加えています。

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

IEEE802.3ad 準拠の LACP を現在のインタフェースに対して設定します。"no" を前に置くことで本機能を無効にします。

文法

lacp

no lacp

初期設定

無効 (Disabled)

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- LACP トランクの両端は固定設定もしくはオートネゴシエーションにより full duplex に設定されている必要があります。
- LACP を使用したトランクは自動的に使用可能なポートチャンネル ID を割り当てられます。
- 対向のスイッチも接続するポートで LACP を有効にしている場合、トランクは自動的に有効になります。
- 8 つ以上のポートが同じ対向のスイッチに接続されて、LACP が有効になっている場合、追加されるポートはスタンバイモードとなり、他のアクティブなリンクが落ちた場合にのみ有効となります。

例

本例では、1 から 3 番ポートの LACP を有効にしています。"show interfaces status port-channel 1" コマンドを使用し、Trunk1 が対向の機器と確立されていることを確認することができます。

```
Console(config)#interface ethernet 1/1
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
Port type:                100TX
Mac address:               00-00-e8-00-00-0b
Configuration:
Name:
Port admin:               Up
Speed-duplex:             Auto
Capabilities:             10half, 10full, 100half, 100full,
Flow control status:      Disabled
Port security:            Disabled
Max MAC count:            0
Current status:
Created by:               LACP
Link status:              Up
Operation speed-duplex: 100full
Flow control type:        None
Member Ports: Eth1/11, Eth1/12, Eth1/13,
Console#
```


lacp admin-key (Ethernet Interface)

ポートの LACP アドミニストレーションキーの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

lacp {actor | partner} **admin-key** *key*

no lacp {actor | partner} **admin-key**

- actor — リンクアグリゲーションのローカル側
- partner — リンクアグリゲーションのリモート側
- *key* — ポートアドミンキーは同じ LAG のポートが同一の値を設定する必要があります (範囲：0-65535)

初期設定

0

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 同じ LAG に参加するには、LACP システムプライオリティが一致し、LACP ポートアドミンキーが一致し、LACP ポートチャンネルキーが一致した場合となります。
- ポートチャンネルアドミンキーを設定する場合には、ポートアドミンキーはチャンネルグループへの参加が可能な同じ値を設定する必要があります。
- リモート側のリンクが確立されると、LACP 運用設定は使用されている状態です。パートナーの LACP 設定は運用状態ではなく管理状態を表し、今後 LACP がパートナーと確立される際に使用されます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp port-priority

LACP ポートプライオリティの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

lacp { actor | partner } **port-priority** *priority*

no lacp { actor | partner } **port-priority**

- actor — リンクアグリゲーションのローカル側
- partner — リンクアグリゲーションのリモート側
- *priority* — バックアップリンクに使用する LACP ポートプライオリティ (範囲：0-65535)

初期設定

32768

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 低い値が高いプライオリティを示します。
- アクティブなポートがダウンした場合、高いプライオリティを持ったポートがバックアップとなります。複数のポートが同じプライオリティの場合には低いポート番号のポートがバックアップリンクとなります。
- リモート側のリンクが確立されると、LACP 運用設定は使用されている状態です。パートナーの LACP 設定は運用状態ではなく管理状態を表し、今後 LACP がパートナーと確立される際に使用されます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

lacp system-priority

ポートの LACP システムプライオリティの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

lacp {actor | partner} **system-priority** *priority*

no lacp {actor | partner} **system-priority**

- actor — リンクアグリゲーションのローカル側
- partner — リンクアグリゲーションのリモート側
- *priority* — プライオリティは、リンクアグリゲーショングループ (LAG) メンバーシップを決定し、又 LAG 接続時に他のスイッチが本機を識別するために使用します（範囲：0-65535）

初期設定

32768

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 同一 LAG に参加するポートは同一システムプライオリティに設定する必要があります。
- システムプライオリティは本機の MAC アドレスと結合し LAG ID となります。ID は他のシステムとの LACP 接続時の特定の LAG を表すために使用されます。
- リモート側のリンクが確立されると、LACP 運用設定は使用されている状態です。パートナーの LACP 設定は運用状態ではなく管理状態を表し、今後 LACP がパートナーと確立される際に使用されます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key (Port Channel)

ポートチャンネル LACP アドミネストレーションキーの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

lacp admin-key *key*

no lacp admin-key

- *key* — ポートアドミンキーは同じ LAG のポートが同一の値を設定する必要があります (範囲：0-65535)

初期設定

0

コマンドモード

Interface Configuration (Port Channel)

コマンド解説

- 同じ LAG に参加するには、LACP システムプライオリティが一致し、LACP ポートアドミンキーが一致し、LACP ポートチャンネルアドミンキーが一致した場合となります。
- チャンネルグループが形成され、ポートチャンネルアドミンキーが設定されていない場合、ポートアドミンキーと同一の値に設定されます。LAG がポートチャンネルアドミンキーを使用しない場合には 0 にリセットされます。

例

```
Console(config)#interface port-channel 1
Console(config-if)#lacp actor admin-key 3
Console(config-if)#
```

show lacp

LACP 情報の表示を行います。

文法

show lacp [*port-channel* | counters | internal | neighbors | sys-id]

- *port-channel* — リンクアグリゲーショングループ ID (範囲：1-12)
- counters — LACP プロトコルメッセージの統計情報
- internal — ローカルサイドの運用状況と設定情報
- neighbors — リモートサイドの運用状況と設定情報
- sys-id — すべてのチャンネルグループの MAC アドレスとシステムプライオリティのサマリ

初期設定

Port Channel：すべて

コマンドモード

Privileged Exec

例

```
Console#show lacp 1 counters
Port channel : 1
-----
Eth 1/ 2
-----
LACPDUs Sent      : 21
LACPDUs Received  : 21
Marker Sent       : 0
Marker Received   : 0
LACPDUs Unknown Pkts : 0
LACPDUs Illegal Pkts : 0
```

項目	解説
LACPDUs Sent	チャンネルグループから送信された有効な LACPDU の数
LACPDUs Received	チャンネルグループが受信した有効な LACPDU の数
Marker Sent	本チャンネルグループから送信された有効な Marker PDU の数
Marker Received	本チャンネルグループが受信した有効な Marker PDU の数
LACPDUs Unknown Pkts	以下のフレームの受信数 (1) スロープロトコル・イーサネット・タイプ値を運び、未知の PDU を含んでいるフレーム (2) スロープロトコルグループ MAC アドレスに属し、スロープロトコル・イーサネット・タイプ値を運んでいないフレーム
LACPDUs Illegal Pkts	不正な PDU 又はプロトコルサブタイプが不正な値を含むスロープロトコルイーサネットパケットを運ぶフレーム数

コマンドラインインタフェース リンクアグリゲーション

例

```

Console#show lacp 1 internal
Port channel : 1
-----
-
Oper Key      : 4
Admin Key     : 0
Eth 1/1
-----
-
LACPDU Internal      : 30 sec
LACP System Priority : 32768
LACP Port Priority   : 32768
Admin Key            : 4
Oper Key             : 4
Admin State          : defaulted,aggregation,long timeout,
                      LACP-activity
Oper State           : distributing, collecting, synchronization,
                      aggregation, long timeout, LACP-activity

```

項目	解説
Oper Key	現在のアグリゲーションポートのキーの運用値
Admin Key	現在のアグリゲーションポートのキーの管理値
LACPDU Internal	受信した LACPDU 情報を無効にするまでの秒数
LACP System Priority	本ポートチャンネルに割り当てられた LACP システムプライオリティ
LACP Port Priority	本ポートチャンネルグループに割り当てられた LACP ポートプライオリティ
Admin State, Oper State	Actor の管理値又は運用値の状態のパラメータ。 Expired — Actor の受信機器は失効状態です Defaulted — Actor の受信機器は初期設定の運用 partner の情報を使用しています Distributing — 誤りの場合、このリンク上の出力フレームの配信は無効になります。配信は現在無効状態で、受信プロトコル情報の管理上の変更、又は変更がない状態で有効にはなりません。 Collecting — このリンク上の入力フレームの収集は可能な状態です。収集は現在可能な状態で、受信プロトコル情報の管理上の変化、又は変化がない状態で無効にはなりません。 Synchronization — システムはリンクを IN_SYNC と認識します。それにより正しいリンクアグリゲーショングループに属することができます。グループは互換性のある Aggregator に関係します。リンクアグリゲーショングループの ID はシステム ID と送信されたオペレーショナルキー情報から形成されます。 Aggregation — システムは、アグリゲーション可能なリンクと認識しています。アグリゲーションの存在的な候補です。 Long timeout — LACPDU の周期的な送信にスロー転送レートを使用します。 LACP-Activity — 本リンクに関するアクティブコントロール値 (0 : Passive、1 : Active)

例

```

Console#show lacp 1 neighbors
Port channel : 1 neighbors
-----
Eth 1/1
-----
Partner Admin System ID   : 32768, 00-00-00-00-00-00
Partner Oper System ID   : 32768, 00-00-00-00-00-01
Partner Admin Port Number : 1
Partner Oper Port Number  : 1
Port Admin Priority       : 32768
Port Oper Priority        : 32768
Admin Key                 : 0
Oper Key                  : 4
Admin State               : defaulted, distributing, collecting,
                           synchronization, long timeout,
Oper State                : distributing, collecting, synchronization,
                           aggregation, long timeout, LACP-activity

```

項目	解説
Partner Admin System ID	ユーザにより指定された LAG partner のシステム ID
Partner Oper System ID	LACP プロトコルにより指定された LAG partner のシステム ID
Partner Admin Port Number	プロトコル partner のポート番号の現在の管理値
Partner Oper Port Number	ポートのプロトコル partner によりアグリゲーションポートに指定された運用ポート番号
Port Admin Priority	プロトコル partner のポートプライオリティの現在の管理値
Port Oper Priority	partner により指定された本アグリゲーションポートのプライオリティ
Admin Key	プロトコル partner のキーの現在の管理値
Oper Key	プロトコル partner のキーの現在の運用値
Admin State	partner のパラメータの管理値（前の表を参照）
Oper State	partner のパラメータの運用値（前の表を参照）

例

```

Console#show lacp sysid
Port Channel      System Priority      System MAC Address
-----
                1                32768      00-30-F1-D3-26-00
                2                32768      00-30-F1-D3-26-00
                3                32768      00-30-F1-D3-26-00
Console#

```

項目	解説
Channel group	本機のリンクアグリゲーショングループ設定
System Priority*	本チャンネルグループの LACP システムプライオリティ
System MAC Address*	システム MAC アドレス

*LACP system priority 及び system MAC address は LAG システム ID から形成します。

4.13 ポートミラーリング

ソフトウェアモニタリングツールまたはハードウェア測定を使用し、解析の為に同じスイッチのローカルポートまたは他のスイッチのリモートポートからデータのミラーを行うことが可能です。本機は以下のミラーリングモードをサポートしています。

コマンド	機能	ページ
Local Port Mirroring	通過するデータまたは被モニタポートのパフォーマンスに影響を与えずに、分析のためにもう 1 つのポートへデータをコピーします。	P634
RSPAN Mirroring	専用 VLAN 上にリモートスイッチからデータをミラーします	P637

4.13.1 ローカルポートミラーリング

ミラーセッションの設定方法を解説しています。

コマンド	機能	モード	ページ
port monitor	ミラーセッションの設定	IC	P635
show port monitor	ミラーポートの設定の表示	PE	P636

port monitor

ミラーセッションの設定を行います。"no" を前に置くことでミラーセッションをクリアします。

文法

port monitor [*interface* { rx | tx | both } | *vlan* *vlan-id* | *mac-address* *mac-address*]
no port monitor *interface*

- *interface* — ethernet *unit/port* (source port)
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
- rx — 受信パケットのミラー
- tx — 送信パケットのミラー
- both — 送受信両パケットのミラー
- *vlan-id* — VLAN ID (範囲: 1-4093)
- *mac-address* — MAC アドレス (フォーマット: xx-xx-xx-xx-xx-xx または xxxxxxxxxxxx)

初期設定

- ミラーセッション: 未定義
- インタフェースで有効時: ミラーリングは受信 / 送信パケット両方
- VLAN または MAC アドレスで有効時: ミラーリングは受信パケットのみ

コマンドモード

Interface Configuration (Ethernet, destination port)

コマンド解説

- ソースポートからディスティネーションポートに通信をミラーし、リアルタイムでの通信分析を行えます。ディスティネーションポートにネットワーク解析装置 (Sniffer 等) 又は RMON プロブを接続し、通信に影響を与えずにソースポートのトラフィックを解析することができます。
- ディスティネーションポートは Ethernet インタフェースに設定します。
- ソース及びディスティネーションポートの通信速度は同じ必要があります。同じ通信速度でない場合には通信がソースポートから落とされます。
- VLAN ミラーとポートミラーの両方が有効である時、ターゲットポートは 2 倍のミラーパケットを受信します。一度目はソースミラーポートから受信し、その後再びソースミラー VLAN からになります。
- MAC アドレスのミラー時、スイッチのターゲットポート以外の全てのポートに入る、指定されたソースアドレスの入力トラフィックはディスティネーションポートにミラーされます。
- スパニングツリー BPDU パケットはターゲットポートへミラーされません。
- 複数のミラーセッションを作成することが可能ですが、全てのセッションは単一のディスティネーションポートを共有します。

例

本例では 6 番から 5 番ポートへのミラーを行います。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

ミラー情報の表示を行います。

文法

show port monitor { *interface* | *vlan vlan id* | *mac-address mac-address* }

- *interface*
 - *ethernet unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)

初期設定

すべてのセッションを表示

コマンドモード

Privileged Exec

コマンド解説

ソースがポートである時、コマンドはディスティネーションポート、ソースポートおよびミラーモード (RX、TX、RX/TX) を表示します。ソースが VLAN である時、ディスティネーションポートとソースポートのみが表示されます。ソースが MAC アドレスである時、ディスティネーションポートと MAC アドレスのみが表示されます。

例

本例では 6 番から 5 番ポートへのミラーの設定が表示されています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination port(listen port) :Eth1/5
Source port(monitored port)   :Eth1/6
Mode                          :RX/TX
Console#
```

4.13.2 RSPAN ミラーリング

Remote Switched Port Analyzer (RSPAN) により、分析の為にローカルディスティネーションポートでリモートスイッチからのトラフィックのミラーが出来ます。

コマンド	機能	モード	ページ
vlan rspan	RSPAN トラフィックを運ぶ為に専有される VLAN を作成	VC	P711
rspan source	ミラーを行うソースポートとトラフィックタイプを指定	GC	P639
rspan destination	被ミラートラフィックをモニタするディスティネーションポートを指定	GC	P640
rspan remote vlan	RSPAN VLAN、スイッチロール（ソース、中間、ディスティネーション）、アップリンクポートを指定	GC	P641
no rspan session	設定された RSPAN セッションを削除	GC	P642
show rspan	RSPAN セッションの設定を表示	PE	P643

設定ガイドライン

RSPAN セッションを設定するには以下の手順を行ってください。

- (1) “vlan rspan” コマンド (P639) を使用し、RSPAN に使用する VLAN を設定します。
(デフォルト VLAN1 とスイッチクラスタ VLAN4093 は禁止されています)
- (2) “rspan source” コマンド (P639) を使用し、インタフェースとモニタを行うトラフィックタイプ (Rx、Tx、Both) を指定します。
- (3) “rspan destination” コマンド (P640) を使用し、RSPAN セッションによる被モニタトラフィックのディスティネーションポートを指定します。
- (4) “rspan remote vlan” コマンド (P641) を使用し、RSPAN セッションで使用される VLAN、スイッチのロール、中間リレー、被ミラートラフィックのディスティネーション、アップリンクポートを指定します。

RSPAN 制限

本機の RSPAN 機能には以下の制限があります。

- RSPAN ポートポートのみが RSPAN ソース、ディスティネーションまたはアップリンクに設定できます。静的または動的トランクは許可されません。また、ソースポートとディスティネーションは同じスイッチ上で設定することは出来ません。
- Local/Remote Mirror – ローカルモニタセッションのディスティネーション (port monitor コマンドで作成された) は RSPAN トラフィックのディスティネーションには使用できません。
- Spanning Tree – スパニングツリー無効時、BPDU は RSPAN VLAN 上にはフラッドされません。
RSPAN がスイッチで有効時、MAC アドレス学習は RSPAN アップリンクポートではサポートされません。そのため、たとえ RSPAN が設定された後にスパニングツリーが有効になっても MAC アドレス学習は RSPAN アップリンクポート上で再開されません。
- IEEE 802.1X – RSPAN と 802.1X は相互に排他的な機能です。802.1X がグローバルで有効時、RSPAN ソースおよびディスティネーションポートは設定可能ですが、RSPAN

コマンドラインインタフェース

ポートミラーリング

アップリンクポートは設定できません。

RSPAN アップリンクポートがスイッチで有効時、802.1X はグローバルで有効に出来ません。

- Port Security –ポートでポートセキュリティが有効時、RSPAN ソースまたはディスティネーションポートとして設定は出来ませんが、RSPAN アップリンクポートとして設定できません。また、ポートがRSPAN アップリンクポートとして設定されている時、このポートでポートセキュリティは有効にできません。

rspan source

リモートでミラーを行うソースポートとトラフィックタイプを指定します。"no" を前に置くことで指定したポートの RSPAN を無効にするか、指定されたタイプのミラーリングを無効にします。

文法

[no] **rspan session** *session-id* **source interface** *interface-list* { rx | tx | both }

- *session-id* — RSPAN セッションの識別番号を指定（範囲：1-2）ローカルとリモートモニタリング両方を含む、2 つのミラーセッションのみが許可されます。
"port monitor" コマンド（P635）でローカルミラーリングが有効時、RSPAN で使用可能な 1 つのセッションのみがあります。
- *interface-list* — 1 つ以上のソースポート。連即したリストを指定するにはハイフンを使用してください。連続していないリストにはコンマを使用してください。
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号（範囲：1-26）
- rx — 受信パケットをミラー
- tx — 送信パケットをミラー
- both — 受信、送信両方のパケットをミラー

初期設定

Tx、Rx 両方のトラフィックをミラー

コマンドモード

Global Configuration

コマンド解説

- 1 つ以上のソースポートを同じスイッチまたは異なるスイッチのいずれか同じ RSPAN セッションにアサインできます。
- ポートのみを RSPAN ソースとして設定できます。静的・動的トランクは許可されません。
- ソースポートとディスティネーションポートを同じスイッチに設定することはできません。

例

```
Console(config)#rspan session 1 source interface ethernet 1/2
Console(config)#rspan session 1 source interface ethernet 1/3
Console(config)#
```

rspan destination

ミラートラフィックのモニタを行うディスティネーションポートを指定します。前に "no" を置くことで、指定したポートの RSPAN を無効にします。

文法

rspan session *session-id* **destination** interface *interface* { tagged | untagged }

- *session-id* — RSPAN セッションの識別番号を指定（範囲：1-2）ローカルとリモートモニタリング両方を含む、2つのミラーセッションのみが許可されます。
"port monitor" コマンド（P635）でローカルミラーリングが有効時、RSPAN で使用可能な1つのセッションのみがあります。
- *interface-list* — 1つ以上のソースポート。連即したリストを指定するにはハイフンを使用してください。連続していないリストにはコンマを使用してください。
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号（範囲：1-26）
- tagged — ディスティネーションポートを出るトラフィックに RSPAN VLAN タグを付加します。
- untagged — ディスティネーションポートを出るトラフィックをタグ無しにします。

初期設定

タグ無し

コマンドモード

Global Configuration

コマンド解説

- 同じスイッチのセッション毎に、1つのディスティネーションポートのみ設定が可能ですが、同じセッションの1つ以上のスイッチに設定することは可能です。
- ポートのみを RSPAN ソースとして設定できます。静的・動的トランクは許可されません。
- ソースポートとディスティネーションポートを同じスイッチに設定することはできません。
- ディスティネーションポートは、これ以降もトラフィックの送受信とアサインされたレイヤ2プロトコルに参加が可能です。

例

```
Console(config)#rspan session 1 destination interface ethernet 1/2
Console(config)#
```

rspan remote vlan

RSPAN VLAN とスイッチロール、アップリンクポートを指定します。"no" を前に置くことで、指定した VLAN の RSPAN を無効にします。

文法

[no] **rspan session session-id remote vlan vlan-id** < source | intermediate | destination >
uplink interface

- *session-id* — RSPAN セッションの識別番号を指定（範囲：1-2）ローカルとリモートモニタリング両方を含む、2 つのミラーセッションのみが許可されます。
"port monitor" コマンド（P635）でローカルミラーリングが有効時、RSPAN で使用可能な 1 つのセッションのみがあります。
- *vlan-id* — RSPAN VLAN を設定する ID（範囲：2-4092、4094）
RSPAN を有効にする前に、"vlan rspan" コマンドを使用し、RSPAN ミラーリングを行う VLAN を確保します。
- *source* — 本機をリモートミラーのソースに指定
- *intermediate* — 本機を中間スイッチに指定
- *destination* — 本機をディスティネーションポートに指定
- *uplink* — 本機をアップリンクに指定
- *interface* — ethernet unit/port
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号（範囲：1-26）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 802.1Q トランクまたはハイブリッドポートを RSPAN アップリンクポートとして設定できます。アクセスポートは許可されていません（"switchport mode"（P717）を参照）
- ソーススイッチの 1 つのアップリンクポートのみ設定が可能ですが、中間またはディスティネーションスイッチ上のアップリンクポートの数に制限はありません。
- ディスティネーションとアップリンクポートのみがこの VLAN のメンバーとしてスイッチにアサインされます。"switchport allowed vlan" コマンド（P715）を使用し、ポートを RSPAN VLAN へ手動でアサインすることはできません。同様に、GVRP によって RSPAN VLAN に動的にポートメンバーを追加することもできません。
また、"show vlan" コマンド（P715）を使用しても、RSPAN VLAN のメンバーを表示しませんが、設定された RSPAN VLAN 識別子のみ表示します。

例

```
Console(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3
Console(config)#
```

no rspan session

設定された RSPAN セッションを削除します。

文法

no rspan session *session-id*

- *session-id* – RSPAN セッションの識別番号を指定（範囲：1-2）ローカルとリモートモニタリング両方を含む、2つのミラーセッションのみが許可されます。
"port monitor" コマンド（P635）でローカルミラーリングが有効時、RSPAN で使用可能な1つのセッションのみがあります。

コマンドモード

Global Configuration

コマンド解説

- "no rspan session" コマンドは、VLAN データベースから削除される前に、RSPAN VLAN を無効にするために使用します。("vlan" コマンド（P711）を参照）

例

```
Console(config)#no rspan session 1
Console(config)#
```


show rspan

RSPAN セッションの設定を表示します。

文法

show rspan session { *session-id* }

- *session-id* – RSPAN セッションの識別番号を指定（範囲：1-2）ローカルとリモートモニタリング両方を含む、2つのミラーセッションのみが許可されます。

"port monitor" コマンド（P635）でローカルミラーリングが有効時、RSPAN で使用可能な1つのセッションのみがあります。

コマンドモード

Privileged Exec

例

```
Console#show rspan session
RSPAN Session ID           : 2
Source Ports (mirrored ports)
  RX Only                   : None
  TX Only                   : None
  BOTH                      : Eth 1/5
Destination Port (monitor port) : None
Destination Tagged Mode     : None
Switch Role                 : None
RSPAN VLAN                  : None
RSPAN Uplink Ports          : None
Operation Status            : Down
Console#
```

4.14 帯域制御

帯域制御機能では各インタフェースの送信及び受信の最大速度を設定することができます。帯域制御は各ポート / トランク毎に設定可能です。帯域制御を有効にすると、通信はハードウェアにより監視され、設定を超える通信は破棄されます。設定範囲内の通信はそのまま転送されます。

コマンド	機能	モード	ページ
rate-limit	ポートの入出力の最大帯域の設定	IC	P644

rate-limit

特定のインタフェースの帯域制御レベルを設定します。帯域を設定せずに本コマンドを使用すると初期値が適用されます。"no" を前に置くことで本機能を無効とします。

文法

rate-limit < input | output > { *rate* }

no rate-limit <input | output>

- input — 入力帯域（レート）
- output — 出力帯域（レート）
- *rate* — トラフィックレートリミットレベル
（範囲：64kbps — 100Mbps（Fast Ethernet） 64kbps — 1000Mbps（Gigabit Ethernet））

初期設定

無効

コマンドモード

Interface Configuration（Ethernet, Port Channel）

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64
Console(config-if)#
```

関連するコマンド

show interfaces switchport（P617）

4.15 自動トラフィック制御

Automatic Traffic Control (ATC) は、設定されたレートリミットまたはポートのシャットダウンのトリガに使用できる、ブロードキャスト、マルチキャストストームのしきい値の境界を設定します。

コマンド	機能	モード	ページ
しきい値コマンド			
auto-traffic-control apply-timer	入力トラフィックが上限値を超えた後、コントロールレスポンスを適用する時間を設定	GC	P648
auto-traffic-control release-timer	入力トラフィックが下限値を下まわった後、コントロールレスポンスをリリースする時間を設定	GC	P649
auto-traffic-control*	ブロードキャストまたはマルチキャストストームの自動トラフィックコントロールを有効化	IC (Port)	P650
auto-traffic-control action	入力トラフィックのリミットまたは攻撃的ポートのシャットダウンのコントロールアクションを設定	IC (Port)	P651
auto-traffic-control alarm-clear-threshold	クリアされたストームコントロールトラップが送られる入力フィルタの下限値を設定	IC (Port)	P652
auto-traffic-control alarm-fire-threshold	イングレストラフィックの上限値を越えて、ストームコントロールレスポンスがアプライタイマ失効の後に引き起こされる立入りトラフィックに設定	IC (Port)	P653
auto-traffic-control control-release	手動でコントロールレスポンスをリリース	IC (Port)	P654
auto-traffic-control auto-control-release	自動でコントロールレスポンスをリリース	PE	P654
SNMP トラップコマンド			
snmp-server enable port-traps atc broadcast-alarm-clear	ストームコントロールレスポンスが発生した後、ブロードキャストトラフィックが下限値を下回った特にトラップを送信	IC (Port)	P655
snmp-server enable port-traps atc broadcast-alarm-fire	ブロードキャストトラフィックが自動ストームコントロールの上限値を超えた時にトラップを送信	IC (Port)	P656
snmp-server enable port-traps atc broadcast-control-apply	ブロードキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信	IC (Port)	P657
snmp-server enable port-traps atc broadcast-control-release	ブロードキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信	IC (Port)	P658
snmp-server enable port-traps atc multicast-alarm-clear	ストームコントロールレスポンスが発生した後、マルチキャストトラフィックが下限値を下回った特にトラップを送信	IC (Port)	P659
snmp-server enable port-traps atc multicast-alarm-fire	マルチキャストトラフィックが自動ストームコントロールの上限値を超えた時にトラップを送信	IC (Port)	P660
snmp-server enable port-traps atc multicast-control-apply	マルチキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信	IC (Port)	P661
snmp-server enable port-traps atc multicast-control-release	マルチキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信	IC (Port)	P662
ATC 表示コマンド			
show auto-traffic-control	自動ストームコントロールのグローバル設定を表示	PE	P663
show auto-traffic-control interface	指定したポートの、インタフェース設定およびストームコントロールステータスを表示	PE	P663

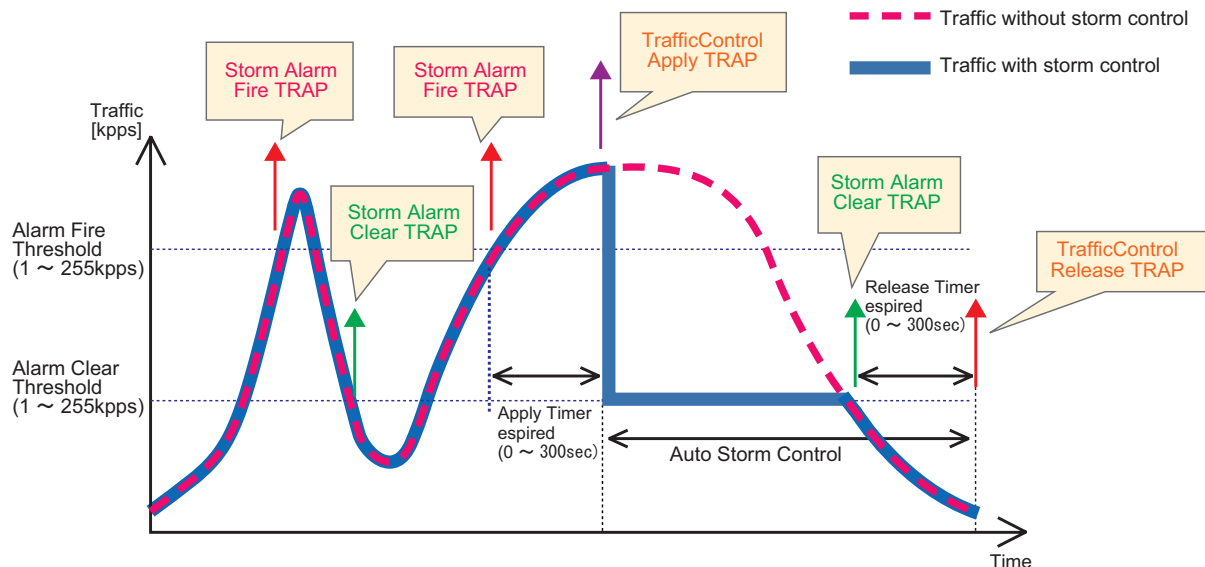
コマンドラインインタフェース

自動トラフィック制御

* ポートでの自動ストーム制御の有効は、もし "switchport packet-rate" コマンド (P611) で設定されている場合、同じポートのハードウェアレベルストームコントロールを無効にします。

ユーザガイドライン

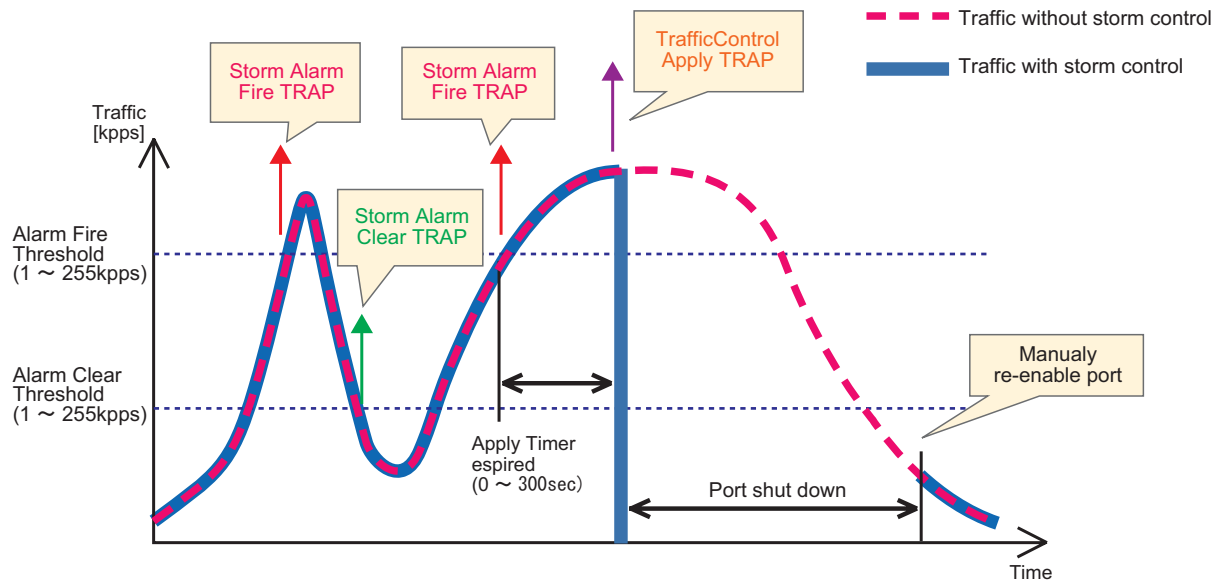
ATC はブロードキャストまたはマルチキャストトラフィックのストームコントロールを含みます。以下の図で示すように、これらトラフィックタイプとコントロールレスポンスは同様です。



この図のキーエレメントは以下です。

- Alarm Fire Threshold – 受容可能な最大トラフィックレート。入力トラフィックがしきい値を越えた時、ATC は "Storm Alarm Fire Trap" の送信とログを行います。
- トラフィックが "alarm fire threshold" を越え、アプライタイマが失効した時、トラフィックコントロールレスポンスが適用され、"Traffic Control Apply" トラップ送信とログを行います。
- Alarm Clear Threshold – リリースタイマ期限が切れた後、下限値を下回るコントロールレスポンスは自動的に終了させることができます。入力トラフィックがしきい値以下に下がる時、ATC は "Storm Alarm Clear Trap" トラップの送信とログを行います。
- リリースタイマ失効後、トラフィックがアラームクリアしきい値を下まわる時、トラフィックコントロールは停止し、"Traffic Control Release Trap" の送信とログをおこないます。
- レートリミットのトラフィックコントロールレスポンスは自動または手動でリリースが可能です。ポートのシャットダウンのコントロールレスポンスは手動でのみリリースが可能です。

ポートシャットダウンによるストームコントロール



この図のキーエレメントは、コントロールレスポンスの自動リリースが提供されないこと以外は、前の図で説明したのと同様です。
トラフィックコントロールが適用される時、ポートの再有効化は使用で行わなければなりません。

機能の制限

自動ストームコントロールはソフトウェアレベルコントロール機能です。

トラフィックストームは "switchport packet-rate" コマンド (P611) を使用して、ハードウェアレベルでもコントロールが可能です。これらのコントロールタイプの内 1 つだけがポートへ適用可能です。ポートで自動ストームコントロールが有効にされると、ハードウェアレベルストームコントロールは無効になります。

auto-traffic-control apply-timer

入力トラフィックが上限値を越えた後、コントロールレスポンスを適用する時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

auto-traffic-control < broadcast | multicast > **apply-timer** *seconds*

no auto-traffic-control < broadcast | multicast > **apply-timer**

- broadcast — ブロードキャストトラフィックの自動ストームコントロールを指定
- multicast — マルチキャストトラフィックの自動ストームコントロールを指定
- *seconds* — コントロールレスポンスを適用する上限値を超えた後のインターバル (範囲: 1-300 秒)

初期設定

300 秒

コマンドモード

Global Configuration

コマンド解説

- アプライタイマが失効した後、"auto-traffic-control action" コマンド (P651) で指定されたコントロールアクションが発生し、"snmp-server enable port-traps atc broadcast-control-apply" (P657) または "snmp-server enable port-traps atc multicast-control-apply" コマンド (P661) で指定されたトラップメッセージが送信されます。

例

```
Console(config)#auto-traffic-control broadcast apply-timer 200
Console(config)#
```

auto-traffic-control release-timer

入力トラフィックが下限値を下まわった後に、コントロールレスポンスのリリース時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

auto-traffic-control < broadcast | multicast > **release-timer** *seconds*

no auto-traffic-control < broadcast | multicast > **release-timer**

- broadcast — ブロードキャストトラフィックの自動ストームコントロールを指定
- multicast — マルチキャストトラフィックの自動ストームコントロールを指定
- *seconds* — 入力トラフィックが下限値を下まわった後に、コントロールレスポンスをリリースする時間 (範囲：1-900 秒)

初期設定

900 秒

コマンドモード

Global Configuration

コマンド解説

- このコマンドは コントロールレスポンスが終了された後の遅延を設定します。"auto-traffic-control auto-control-release" コマンド (P654) が自動リリースの有効 / 無効を設定するために使用されます。

例

```
Console(config)#auto-traffic-control broadcast release-timer 800
Console(config)#
```

auto-traffic-control

ブロードキャストまたはマルチキャストストームの自動トラフィックコントロールを有効にします。"no" を前に置くことで設定を無効にします。

文法

auto-traffic-control < broadcast | multicast >

no auto-traffic-control < broadcast | multicast >

- broadcast — ブロードキャストトラフィックの自動ストームコントロールを指定
- multicast — マルチキャストトラフィックの自動ストームコントロールを指定

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 自動ストームコントロールはブロードキャストあるいはマルチキャストトラフィックにたいし有効に出来ます。これら両方のトラフィックにたいし、同時に有効にすることは出来ません。
- 自動ストームコントロールはソフトウェアレベルコントロール機能です。トラフィックストームは "switchport packet-rate" コマンド (P611) を使用して、ハードウェアレベルでもコントロールが可能です。これらのコントロールタイプの内 1 つだけがポートへ適用可能です。ポートで自動ストームコントロールが有効にされると、ハードウェアレベルストームコントロールは無効になります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast
Console(config-if)#
```


auto-traffic-control action

入力トラフィックの制限または違反のあったポートのシャットダウンを行う為のコントロールアクションを設定します。"no" を前に置くことで設定を初期値に戻します。

文法

auto-traffic-control < broadcast | multicast > **action** < rate-control | shutdown >

no auto-traffic-control < broadcast | multicast > **action**

- broadcast — ブロードキャストトラフィックの自動ストームコントロールを指定
- multicast — マルチキャストトラフィックの自動ストームコントロールを指定
- rate-control — コントロール反応が引き起こされた際、入力トラフィックのレートは "auto-traffic-control alarm-clear-threshold" コマンド（P652）で設定されたしきい値に基づいて制限されます。
- shutdown — コントロール反応が引き起こされた際、ポートは無効になります。自動トラフィックコントロールによって無効になったポートは手動でのみ再有効化が可能です。

初期設定

rate-control

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 上限のしきい値が超えられ、アプライタイマが期限切れになった時、このコマンドを基にコントロール反応が発生します。
- コントロール反応が、このコマンドによってレート制限に設定されている際、レートリミットは "auto-traffic-control alarm-clear-threshold" コマンド（P652）で決定されます。
- ポートがコントロール反応によってシャットダウンされた時、自動トラフィックコントロールでは再度有効にすることは出来ません。"auto-traffic-control control-release" コマンド（P654）により手動でのみ再有効化が可能です。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

auto-traffic-control alarm-clear-threshold

ストームコントロールクリアトラップを送信する、入力トラフィックの下限值を設定します。"no" を前に置くことで設定を初期値に戻します。

文法

auto-traffic-control < broadcast | multicast > **alarm-clear-threshold** *threshold*

no auto-traffic-control < broadcast | multicast > **alarm-clear-threshold**

- broadcast — ブロードキャストトラフィックの自動ストームコントロールを指定
- multicast — マルチキャストトラフィックの自動ストームコントロールを指定
- *threshold* — アプライタイマ失効後、ストームコントロールレスポンスが引き起こされる入力トラフィックの上限値（範囲：1-255Kpacket/ 秒）

初期設定

128Kpacket/ 秒

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 一度下限値を下回ると " snmp-server enable port-traps atc broadcast-alarm-clear" コマンド（P655）または " snmp-server enable port-traps atc multicast-alarm-clear" コマンド（P659）で設定されたトラップメッセージが送信されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-clear-threshold 155
Console(config-if)#
```

auto-traffic-control alarm-fire-threshold

アプライタイマ失効後、ストームコントロールレスポンスが引き起こされる入力トラフィックの上限値を設定します。"no" を前に置くことで設定を初期値に戻します。

文法

auto-traffic-control < broadcast | multicast > **alarm-fire-threshold** *threshold*

no auto-traffic-control < broadcast | multicast > **alarm-fire-threshold**

- broadcast — ブロードキャストトラフィックの自動ストームコントロールを指定
- multicast — マルチキャストトラフィックの自動ストームコントロールを指定
- *threshold* — アプライタイマ失効後、ストームコントロールレスポンスが引き起こされる入力トラフィックの上限値（範囲：1-255Kpacket/ 秒）

初期設定

128Kpacket/ 秒

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- "snmp-server enable port-traps atc broadcast-alarm-fire" (P656) または "snmp-server enable port-traps atc multicast-alarm-fire" (P660) コマンドで設定がおこなわれている場合、一度上限値を越えると、トラップメッセージが送信されます。上限値を越えた後、コントロールタイマは、"auto-traffic-control action" (P651) によって設定される場合、コントロールレスポンスが引き起こされるより前に "auto-traffic-control apply-timer" (P648) コマンドの設定に準じ失効します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255
Console(config-if)#
```

auto-traffic-control control-release

コントロールレスポンスを手動でリリースします。

文法

auto-traffic-control < broadcast | multicast > **control-release**

- broadcast — ブロードキャストトラフィックの自動ストームコントロールを指定
- multicast — マルチキャストトラフィックの自動ストームコントロールを指定

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- このコマンドは、指定されたアクションが引き起こされた後、コントロールレスポンスを手動で停止するために使用します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast control-release
Console(config-if)#
```

auto-traffic-control auto-control-release

"auto-traffic-control release-timer" コマンド (P649) で指定された期限が切れた後、コントロールレスポンスを自動でリリースします。

文法

auto-traffic-control < broadcast | multicast > **auto-control-release**

- broadcast — ブロードキャストトラフィックの自動ストームコントロールを指定
- multicast — マルチキャストトラフィックの自動ストームコントロールを指定

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- このコマンドは、指定されたアクションが引き起こされ、リリースタイマの期限が切れた後に、コントロールレスポンスを自動で停止するために使用します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-release
Console(config-if)#
```

snmp-server enable port-traps atc broadcast-alarm-clear

ストームコントロールレスポンスが引き起こされた後、ブロードキャストトラフィックが下限のしきい値を下回った時にトラップを送信します。"no" を前に置くことでトラップを無効にします。

文法

snmp-server enable port-traps atc broadcast-alarm-clear

no snmp-server enable port-traps atc broadcast-alarm-clear

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear
Console(config-if)##
```

関連するコマンド

auto-traffic-control action (P651)

auto-traffic-control alarm-clear-threshold (P652)

snmp-server enable port-traps atc broadcast-alarm-fire

ブロードキャストトラフィックが、自動ストームコントロールのしきい値の上限を超えた時にトラップを送ります。"no" を前に置くことでトラップを無効にします。

文法

snmp-server enable port-traps atc broadcast-alarm-fire

no snmp-server enable port-traps atc broadcast-alarm-fire

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold (P653)

snmp-server enable port-traps atc broadcast-control-apply

ブロードキャストトラフィックが自動ストームコントロールの上限のしきい値を超え、アラタイマが期限切れになった時にトラップを送信します。"no" を前に置くことでトラップを無効にします。

文法

snmp-server enable port-traps atc broadcast-control-apply

no snmp-server enable port-traps atc broadcast-control-apply

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc
broadcast-control-apply
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold (P653)

auto-traffic-control apply-timer (P648)

snmp-server enable port-traps atc broadcast-control-release

ストームコントロールレスポンスが引き起こされ、リリースタイマの期限が切れた後に、ブロードキャストトラフィックが下限のしきい値を下回った時トラップを送信します。"no"を前に置くことでトラップを無効にします。

文法

snmp-server enable port-traps atc broadcast-control-release

no snmp-server enable port-traps atc broadcast-control-release

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc
broadcast-control-release
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-clear-threshold (P652)

auto-traffic-control action (P651)

auto-traffic-control release-timer (P649)

snmp-server enable port-traps atc multicast-alarm-clear

ストームコントロールレスポンスが引き起こされた後、マルチキャストトラフィックが下限のしきい値を下回った時にトラップを送信します。"no" を前に置くことでトラップを無効にします。

文法

snmp-server enable port-traps atc multicast-alarm-clear
no snmp-server enable port-traps atc multicast-alarm-clear

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-clear
Console(config-if)#
```

関連するコマンド

auto-traffic-control action (P651)
auto-traffic-control alarm-clear-threshold (P652)

snmp-server enable port-traps atc multicast-alarm-fire

マルチキャストトラフィックが、自動ストームコントロールのしきい値の上限を超えた時にトラップを送ります。"no" を前に置くことでトラップを無効にします。

文法

snmp-server enable port-traps atc multicast-alarm-fire

no snmp-server enable port-traps atc multicast-alarm-fire

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-fire
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold (P653)

snmp-server enable port-traps atc multicast-control-apply

マルチキャストトラフィックが自動ストームコントロールの上限のしきい値を超え、アライタイマが期限切れになった時にトラップを送信します。"no" を前に置くことでトラップを無効にします。

文法

snmp-server enable port-traps atc multicast-control-apply

no snmp-server enable port-traps atc multicast-control-apply

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc
multicast-control-apply
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold (P653)

snmp-server enable port-traps atc multicast-control-release

ストームコントロールレスポンスが引き起こされ、リリースタイマの期限が切れた後に、マルチキャストトラフィックが下限のしきい値を下回った時トラップを送信します。"no" を前に置くことでトラップを無効にします。

文法

snmp-server enable port-traps atc multicast-control-release

no snmp-server enable port-traps atc multicast-control-release

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc
multicast-control-release
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-clear-threshold (P652)

auto-traffic-control action (P651)

auto-traffic-control release-timer (P649)

show auto-traffic-control

自動ストームコントロールのグローバル設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show auto-traffic-control

Storm-control: Broadcast
  Apply-timer (sec)      : 300
  release-timer (sec)    : 900

Storm-control: Multicast
  Apply-timer(sec)       : 300
  release-timer(sec)     : 900
Console#
```

show auto-traffic-control interface

指定されたポートのインタフェース設定とストームコントロールステータスを表示します。

文法

show auto-traffic-control interface *interface*

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)

コマンドモード

Privileged Exec

例

```
Console#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
-----
Storm Control:           Broadcast           Multicast
State:                   Disabled            Disabled
Action:                  rate-control        rate-control
Auto Release Control:    Disabled            Disabled
Alarm Fire Threshold(Kpps): 128              128
Alarm Clear Threshold(Kpps):128              128
Trap Storm Fire:         Disabled            Disabled
Trap Storm Clear:        Disabled            Disabled
Trap Traffic Apply:      Disabled            Disabled
Trap Traffic Release:    Disabled            Disabled
-----
Console#
```

4.16 アドレステーブル

MAC アドレステーブルに対するアドレスフィルタリング、現在エントリーされているアドレスの表示、テーブルのクリア、エージングタイムの設定を行います。

コマンド	機能	モード	ページ
mac-address-table aging-time	アドレステーブルのエージングタイムの設定	GC	P664
mac-address-table static	VLAN ポートへの MAC アドレスの静的なマッピング	GC	P665
clear mac-address-table dynamic	転送データベースに学習された情報の削除	PE	P666
show mac-address-table	転送データベースに登録された情報の表示	PE	P667
show mac-address-table aging-time	アドレステーブルのエージングタイムの表示	PE	P668

mac-address-table aging-time

アドレステーブルのエージングタイムを設定します。"no" を前に置くことで初期設定に戻します。

文法

mac-address-table aging-time *seconds*

no mac-address-table aging-time

- *seconds* - 秒数を設定します
(10-844 の値。0 に設定した場合はエージングを無効にします)

初期設定

300 (秒)

コマンドモード

Global Configuration

コマンド解説

エージングタイムは動的転送情報を本機に保持する時間を表します。

例

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

mac-address-table static

VLAN のポートに静的に MAC アドレスをマッピングします。"no" を前に置くことで MAC アドレスを削除します。

文法

mac-address-table static *mac-address* interface *interface* vlan *vlan-id* [*action*]

no mac-address-table static *mac-address* vlan *vlan-id*

- *mac-address* — MAC アドレス
- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)
- vlan *vlan-id* — VLAN ID (1-4093)
- *action*
 - delete-on-reset — 本機が再起動されるまで登録されます。
 - permanent — 永久に登録されます。

初期設定

mac-address: なし

action: permanent

コマンドモード

Global Configuration

コマンド解説

静的アドレスは特定の VLAN の特定のポートに割り当てることができます。本コマンドを使用して静的アドレスを MAC アドレステーブルに追加することができます。静的アドレスは以下の特性を持っています。

- インタフェースのリンクがダウンしても、静的アドレスはアドレステーブルから削除されません。
- 静的アドレスは指定したインタフェースに固定され、他のインタフェースに移動することはありません。静的アドレスが他のインタフェースに現れた場合、アドレスは拒否されアドレステーブルに記録されません。
- 静的アドレスは "no" コマンドを使って削除するまで、他のポートで学習されません。

例

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
interface ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

コマンドラインインタフェース アドレステーブル

clear mac-address-table dynamic

転送データベースから、学習されたエントリを削除します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#clear mac-address-table dynamic
Console#
```


show mac-address-table

ブリッジ転送データベースに登録されている情報を表示します。

文法

```
show mac-address-table {address mac-address { mask } } { interface interface }
{ vlan vlan-id } { sort <address | vlan | interface> }
```

- *mac-address* — MAC アドレス
- *mask* — アドレス内の一致するビット
- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
- port-channel *channel-id* (範囲: 1-12)
- *vlan-id* — VLAN ID (1-4093)
- *sort* — アドレス、VLAN、インタフェースによる並び替え

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- MAC アドレステーブルはそれぞれのインタフェースに関連付けられた MAC アドレスを含みます。タイプフィールドには以下のタイプがあります。
 - Learn - 動的アドレスエントリ
 - Config - 静的エントリ
- アドレスエントリの最大数は 16K です。

例

```
Console#show mac-address-table
Interface      Mac Address          Vlan  Type
-----
Eth 1/1        00-00-E8-49-5E-DC    1     Delete-on-reset
Trunk 2        00-E0-29-8F-AA-1B    1     Learned
Console#
```

コマンドラインインタフェース アドレステーブル

show mac-address-table aging-time

アドレステーブルのエージングタイムを表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show mac-address-table aging-time
Aging Status : Enabled
Aging Time: 300 sec.
Console#
```

4.17 スパニングツリー

本機へのスパニングツリーアルゴリズム (Spanning Tree Algorithm/STA) の設定と、選択したインタフェースへの STA の設定を行うコマンドです。

コマンド	機能	モード	ページ
spanning-tree	スパニングツリープロトコルの有効化	GC	P671
spanning-tree forward-time	スパニングツリーブリッジ転送時間の設定	GC	P672
spanning-tree hello-time	スパニングツリーブリッジハロー時間の設定	GC	P673
spanning-tree max-age	スパニングツリーブリッジ最長時間の設定	GC	P674
spanning-tree mode	STP/RSTP/MSTP モードの選択	GC	P675
spanning-tree path cost method	RSTP/MSTP のパスコスト方法の設定	GC	P676
spanning-tree priority	スパニングツリーブリッジプライオリティの設定	GC	P677
spanning-tree mst-configuration	MSTP 設定モードの変更	GC	P677
spanning-tree transmission-limit	RSTP/MSTP の送信リミットの設定	GC	P678
max-hops	BPDU が破棄される前最大ホップ数の設定	MST	P679
mst priority	スパニングツリーインスタンスのプライオリティの設定	MST	P680
mst vlan	スパニングツリーインスタンスへの VLAN の追加	MST	P681
name	MST 名の設定	MST	P682
revision	MST リビジョンナンバーの設定	MST	P683
spanning-tree bpdu-filter	エッジポートの BPDU フィルタ	IC	P684
spanning-tree bpdu-guard	BPDU 受信時にエッジポートをシャットダウン	IC	P685
spanning-tree cost	各インタフェースのスパニングツリーのパスコスト設定	IC	P686
spanning-tree edge-port	エッジポートへのポートファストの有効化	IC	P687
spanning-tree link-type	RSTP/MSTP のリンクタイプを設定	IC	P688
spanning-tree loopback-detection	ポートで BPDU ループバック検出を有効化	IC	P689
spanning-tree loopback-detection release-mode	ポートでループバックリリースモードを設定	IC	P690
spanning-tree loopback-detection trap	ポートの BPDU ループバック SNMP トラップ通知を有効化	IC	P691

コマンドラインインタフェース スパニングツリー

spanning-tree mst cost	MST インスタンスのパスコストの設定	IC	P692
spanning-tree mst port-priority	MST インスタンスプライオリティの設定	IC	P694
spanning-tree port-priority	各インタフェースのスパニングツリーのプライオリティ設定	IC	P695
spanning-tree root-guard	指定されたポートが上位の BPDU 通過を阻止	IC	P696
spanning-tree spanning-disabled	インタフェースのスパニングツリーの無効化	IC	P697
spanning-tree loopbackdetection release	ループバック検索によって、Discarding 状態おかれているポートを手動で開放します。	PE	P698
spanning-tree protocol-migration	適切な BPDU フォーマットの再確認	PE	P699
show spanning-tree	スパニングツリーの設定を表示	PE	P700
show spanning-tree mst configuration	MST 設定の表示	PE	P702

spanning-tree

本機に対して spanning-tree (STA) を有効に設定します。"no" を前に置くことで機能を無効にします。

文法

spanning-tree

no spanning-tree

初期設定

STA 有効

コマンドモード

Global Configuration

コマンド解説

STA はネットワークのループを防ぎつつブリッジ、スイッチ及びルータ間のバックアップリンクを提供します。STA 機能を有するスイッチ、ブリッジ及びルータ間で互いに連携し、各機器間のリンクで 1 つのルートがアクティブになるようにします。また、別途バックアップ用のリンクを提供し、メインのリンクがダウンした場合には自動的にバックアップを行います。

例

本例では STA を有効にしています。

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree forward-time

スパニングツリー転送遅延時間を本機すべてのインタフェースに設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree forward-time *seconds*

no spanning-tree forward-time

- *seconds* — 秒数（範囲：4-30 秒）
最小値は 4 又は $[(\text{max-age} / 2) + 1]$ のどちらか小さい方となります。

初期設定

15（秒）

コマンドモード

Global Configuration

コマンド解説

ルートデバイスがステータスを変更するまでの最大時間を設定することができます。各デバイスがフレームの転送をはじめる前にトポロジー変更を受け取るために遅延時間が必要です。また、各ポートの競合する情報を受信し、廃棄するためにも時間が必要となります。そうしなければ一時的にでも、データのループが発生します。

例

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

スパニングツリー Hello タイムを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree hello-time *time*

no spanning-tree hello-time

- *time* — 秒数（範囲：1-26 秒）
最大値は 10 または $[(\text{max-age} / 2) - 1]$ の小さい方となります。

初期設定

2（秒）

コマンドモード

Global Configuration

コマンド解説

設定情報の送信を行う間隔を設定するためのコマンドです。

例

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

関連するコマンド

spanning-tree forward-time (P672)

spanning-tree max-age (P674)

spanning-tree max-age

スパニングツリーの最大エージングタイムを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree max-age *seconds*

no spanning-tree max-age

- *seconds* — 秒（範囲：6-40 秒）
最小値は 6 又は $[2 \times (\text{hello-time} + 1)]$ のどちらか大きい値です。
最大値は 40 又は $[2 \times (\text{forward-time} - 1)]$ のどちらか小さい値です。

初期設定

20（秒）

コマンドモード

Global Configuration

コマンド解説

設定変更を行う前に設定情報を受け取るまでの最大待ち時間（秒）。
指定ポートを除くすべてのポートが設定情報を一定の間隔で受け取ります。タイムアウトした STP ポートは付属する LAN のための指定ポートになります。そのポートがルートポートの場合、ネットワークに接続された他のポートがルートポートとして選択されます。

例

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

関連するコマンド

spanning-tree forward-time（P672）

spanning-tree hello-time（P673）

spanning-tree mode

STP のモードを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree mode < stp | rstp | mstp >

no spanning-tree mode

- stp — Spanning Tree Protocol (IEEE 802.1D 準拠)
- rstp — Rapid Spanning Tree Protocol (IEEE 802.1w 準拠)
- mstp — mstp - Multiple Spanning Tree (IEEE 802.1s 準拠)

初期設定

rstp

コマンドモード

Global Configuration

コマンド解説

- Spanning Tree Protocol(STP)
スイッチ内部では RSTP を用いますが、外部へは IEEE802.1D 準拠の BPDU の送信のみを行います。
- Rapid Spanning Tree Protocol(RSTP)
RSTP は以下の入ってくるメッセージの種類を判断し STP 及び RSTP のいずれにも自動的に対応することができます。
 - STP Mode — ポートの移行遅延タイマーが切れた後に IEEE802.1D BPDU を受け取ると、本機は IEEE802.1D ブリッジと接続していると判断し、IEEE802.1D BPDU のみを使用します。
 - RSTP Mode — IEEE802.1D BPDU を使用し、ポートの移行遅延タイマーが切れた後に RSTP BPDU を受け取ると、RSTP は移行遅延タイマーを再スタートさせ、そのポートに対し RSTP BPDU を使用します。
- Multiple Spanning Tree Protocol(MSTP)
 - ネットワーク上で MSTP を有効にするには、接続された関連するブリッジにおいても同様の MSTP の設定を行ない、スパニングツリーインスタンスに参加することを許可する必要があります。
 - スパニングツリーインスタンスは、互換性を持つ VLAN インスタンスを持つブリッジにのみ設定可能です。
 - スパニングツリーモードを変更する場合、変更前のモードのスパニングツリーインスタンスをすべて止め、その後新しいモードにおいて通信を再開します。スパニングツリーのモード変更時には通信が一時的に遮断されるので注意して下さい。

例

本例では RSTP を使用する設定をしています。

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree pathcost method

RSTP のパスコストを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree pathcost method < long | short >

no spanning-tree pathcost method

- long — 0-200,000,000 までの 32 ビットの値
- short — 0-65535 までの 16 ビットの値

初期設定

long

コマンドモード

Global Configuration

コマンド解説

パスコストはデバイス間の最適なパスを決定するために使用されます。速度の速いポートに対し小さい値を設定し、速度の遅いポートに対し大きな値を設定します。path cost (P686) は port priority (P695) よりも優先されます。

例

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree priority

本機全体に対してスパニングツリーのプライオリティの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree priority *priority*

no spanning-tree priority

- *priority* — ブリッジの優先順位
(0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

初期設定

32768

コマンドモード

Global Configuration

コマンド解説

プライオリティはルートデバイス、ルートポート、指定ポートを決定する際に使用されます。一番高いプライオリティを持ったデバイスが STA ルートデバイスとなります。すべてのデバイスが同じプライオリティの場合、MAC アドレスが一番小さいデバイスがルートデバイスとなります。

例

```
Console(config)#spanning-tree priority 40960
Console(config)#
```

spanning-tree mst configuration

MST 設定モードに移行します。

初期設定

- MST インスタンスに VLAN がマッピングされていません
- リジョン名は本機の MAC アドレスです

コマンドモード

Global Configuration

例

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

spanning-tree transmission-limit

RSTP BPDU の最小送信間隔を設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

- *count* — 転送リミットの秒数（範囲：1-10 秒）

初期設定

3

コマンドモード

Global Configuration

コマンド解説

本コマンドでは BPDU の最大転送レートを制限します。

例

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

max-hops

BPDU が破棄される前の MST 内での最大ホップ数を設定します。"no" を前に置くことで初期設定に戻ります。

文法

max-hops *hop-number*

- *hop-number* — MST の最大ホップ数（設定範囲：1-40）

初期設定

20

コマンドモード

MST Configuration

コマンド解説

MSTI リジンは STP と RSTP プロトコルでは単一のノードとして扱われます。従って MSTI リジョン内の BPDU のメッセージエイジは変更されません。しかし、リジョン内の各スパニングツリーインスタンス及びインスタンスを接続する内部スパニングツリー (IST) は、BPDU を広げるためブリッジの最大数を指定するために hop カウントを使用します。各ブリッジは BPDU を渡す前に hop カウントを 1 つ減らします。hop カウントが 0 になった場合にはメッセージは破棄されます。

例

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

mst priority

スパニングツリーインスタンスのプライオリティを設定します。"no" を前に置くことで初期設定に戻します。

文法

mst *instance_id* **priority** *priority*

no mst *instance_id* **priority**

- *instance_id* — MST インスタンス ID (範囲：0-4094)
- *priority* — MST インスタンスのプライオリティ
(0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

初期設定

32768

コマンドモード

MST Configuration

コマンド解説

- MST プライオリティはルートデバイス、特定のインスタンスの代理ブリッジの決定に使用されます。一番高いプライオリティを持ったデバイスが MSTI ルートデバイスとなります。すべてのデバイスが同じプライオリティの場合、MAC アドレスが一番小さいデバイスがルートデバイスとなります。
- プライオリティを 0 に設定することにより本機を MSTI のルートデバイスに、16384 に設定することにより代理デバイスに設定できます。

例

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

mst vlan

スパニングツリーインスタンスに VLAN を追加します。"no" を前に置くことで特定の VLAN を削除します。VLAN を指定しない場合にはすべての VLAN を削除します。

文法

mst *instance_id* **vlan** *vlan-range*

no mst *instance_id* **vlan** *vlan-range*

- *instance_id* — MST インスタンス ID (範囲：0-4094)
- *vlan-range* — VLAN 範囲 (範囲：1-4093)

初期設定

なし

コマンドモード

MST Configuration

コマンド解説

- 本コマンドによりスパニングツリーに VLAN をグループ化します。MSTP は各インスタンスに対し特定のスパニングツリーを生成します。これによりネットワーク上に複数のパスを構築し、通信のロードバランスを行い、単一のインスタンスに不具合が発生した場合に大規模なネットワークの障害が発生することを回避すると共に、不具合の発生したインスタンスの新しいトポロジーへの変更を迅速に行ないます。
- 初期設定では、MST リジョン内のすべてのブリッジと LAN に接続されたすべての VLAN が内部スパニングツリー (MSTI 0) に割り当てられています。本機では最大 58 のインスタンスをサポートしています。但し、同一インスタンスのセットにより同一 MSTI 内のすべてのブリッジ、及び同一 VLAN のセットにより同一インスタンスを形成する必要があります。RSTP は単一ノードとして各 MSTI を扱い、すべての MSTI を Common Spanning Tree として接続する点に注意して下さい。

例

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

コマンドラインインタフェース

スパニングツリー

name

本機の設置されている MST リジョン名の設定を行ないます。"no" を前に置くことで名前を削除します。

文法

name *name*

- *name* — スパニングツリー名

初期設定

本機の MAC アドレス

コマンドモード

MST Configuration

コマンド解説

MST リジョン名とリビジョンナンバーは唯一の MST リジョンを指定するために使用されます。(本機のようなスパニングツリー対応機器である)ブリッジは1つのMST リジョンにのみ属することができます。同じリジョン内のすべてのブリッジはすべて同じMST インスタンスの設定をする必要があります。

例

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

関連するコマンド

revision (P683)

revision

本機の MST 設定のリビジョンナンバーの設定を行ないます。"no" を前に置くことで初期設定に戻ります。

文法

revision number

- *number* — スパニングツリーのリビジョンナンバー（範囲：0-65535）

コマンドモード

MST Configuration

コマンド解説

MST リジョン名とリビジョンナンバーは唯一の MST リジョンを指定するために使用されます。（本機のようなスパニングツリー対応機器である）ブリッジは 1 つの MST リジョンにのみ属することができます。同じリジョン内のすべてのブリッジはすべて同じ MST インスタンスの設定をする必要があります。

例

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

関連するコマンド

name (P682)

spanning-tree bpdud-filter

エッジポートで受信された全ての BUDU をフィルタします。"no" を使用することで機能を無効にします。

文法

spanning-tree bpdud-filter
no spanning-tree bpdud-filter

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdud-filter
Console(config-if)#
```

関連するコマンド

spanning-tree edge-port (P687)

spanning-tree bpduguard

BPDU が受信された際、エッジポートをシャットダウンします。"no" を前に置くことで設定を初期値へ戻します。

文法

spanning-tree bpduguard

no spanning-tree bpduguard

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- エッジポートは BPDU を生成しないエンドノードへのみ接続されます。
もし BPDU がエッジポートで受信された場合、不正なネットワーク設定またはスイッチがハッカーによる攻撃を受けていることを示します。
インタフェースが BPDU ガードによってシャットダウンされた場合、"no spanning-tree spanning-disable" コマンド (P697) を使用し、手動で再有効化する必要があります。
- BPDU ガードを有効にする前に、"spanning-tree edge-port" コマンド (P687) を使用し、インタフェースをエッジポートとして設定してください。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpduguard
Console(config-if)#
```

関連するコマンド

spanning-tree edge-port (P687)

spanning-tree spanning-disabled (P697)

spanning-tree cost

各ポートの STA パスコストを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree cost *cost*

no spanning-tree cost

- *cost* — インタフェースへのパスコストの値（範囲：1-200,000,000）

STA パスコスト推奨範囲

ポートタイプ	IEEE 802.1D-1998	IEEE 802.1w-2001
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

STA パスコスト推奨値

ポートタイプ	リンクタイプ	IEEE 802.1D-1998	IEEE 802.1w-2001
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

初期設定

初期値

ポートタイプ	リンクタイプ	IEEE 802.1w-2001
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 本コマンドはデバイス間の STA のパスを最適に決定するためのコマンドです。従って、速度の速いポートに対し小さい値を設定し、速度の遅いポートに対し大きな値を設定します。
- パスコストはポートプライオリティより優先されます。
- STP パスコストが "short" に設定されている場合には最大値が 65,535 となります。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree edge-port

エッジに対するポートを指定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree edge-port

no spanning-tree edge-port

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 本コマンドは選択したポートに対しファストスパニングツリーモードの設定を行います。このモードでは、ポートは学習ステートをパスして、フォワーディングを行います。エンドノードではループを発生しないため、スパニングツリーステートの変更を通常よりも早く行うことができます。ファストフォワーディングは、エンドノードのサーバ、ワークステーションに対し STP によるタイムアウトを軽減します。(ファストフォワーディングは LAN のエンドノードのデバイス又は LAN のエンドのブリッジに接続されたポートにのみ有効にして下さい。)

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

spanning-tree link-type

RSTP のリンクタイプを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree link-type < auto | point-to-point | shared >

no spanning-tree link-type

- auto — duplex モードの設定から自動的に設定
- point-to-point — point to point リンク
- shared — シェアードメディアム

初期設定

auto

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ポートが対向のブリッジにのみ接続されている場合は point-to-point リンクを、複数のブリッジに接続されている場合には shared を選択します。
- 自動検知が選択されている場合、リンクタイプは duplex モードから選択されます。Full-duplex のポートでは point-to-point リンクが、half-duplex ポートでは、shared リンクが自動的に選択されます。
- RSTP は 2 つのブリッジ間の point-to-point リンクでのみ機能します。指定されたポートが shared リンクの場合には RSTP は許可されません。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree loopback-detection

このコマンドは、ポートで検出とスパニングツリーループバックパケットへの返答を有効にします。"no" を前に置くことでこの機能を無効にします。

文法

spanning-tree loopback-detection

no spanning-tree loopback-detection

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ループバック検出が有効であり、ポートがそれ自身の BPDU を受信した場合、ポートは IEEE Standard 802.1W-2001 9.3.4 に従って、ループバック BPDU を破棄します。.
- スイッチでスパニングツリーが無効の場合、ポートループバック検出はアクティブになりません。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

spanning-tree loopback-detection release-mode

BPDU ループバックが受信された為にディスカードイングステーツに置かれているポートのリリースモードを設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

spanning-tree loopback-detection release-mode < auto | manual >

no spanning-tree loopback-detection

- auto — ループバックステーツ終了時、ディスカードイングステーツから自動でリリースさせます。
- manual — ポートは手動でのみリリースされます。

初期設定

auto

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ポートが自動ループバックリリースに設定されている場合、以下の条件の内一つが満たされたとき、ポートはフォワーディングステーツへ戻ります。
 - ポートが自身以外の BPDU を受信
 - ポートリンクステータスがリンクダウンへ変更後再リンクアップ
 - フォワード遅延間隔の間にポートが自身の BPDU の受信を中止した場合
- ループバック検出が無効である、ポートが自身の BPDU を受信した場合、IEEE Standard 802.1W-2001 9.3.4 に従いループバック BPDU を破棄します。
- スイッチでスパニングツリーが無効の場合、ポートループバック検出はアクティブになりません。
- 手動リリースモードに設定されている時、リンクダウン / アップイベントはポートをディスカードイングステーツからリリースしません。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
```


spanning-tree loopback-detection trap

スパニングツリーループバック BPDU 検出の SNMP トラップ通知を有効にします。
"no" を前に置くことで設定を初期状態に戻します。

文法

spanning-tree loopback-detection trap

no spanning-tree loopback-detection trap

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

spanning-tree mst cost

MST のインスタンスのパスコストの設定を行ないます。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree mst *instance_id* **cost** *cost*

no spanning-tree mst *instance_id* **cost**

- *instance_id* — MST インスタンス ID (範囲：0-4094)
- *cost* — インタフェースへのパスコストの値 (1-200,000,000)
パスコスト推奨範囲は P686 「STA パスコスト推奨範囲」、パスコスト推奨値は P686 「STA パスコスト推奨値」を参照してください。

初期設定

パスコスト初期値は P686 「初期値」の表を参照してください。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 各スパニングツリーインスタンスは VLAN ID に関連付けられます。
- 本コマンドはデバイス間の MSTA のパスを最適に決定するためのコマンドです。従って、速度の速いポートに対し小さい値を設定し、速度の遅いポートに対し大きな値を設定します。
- パスコストはインタフェースプライオリティより優先されます。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

関連するコマンド

spanning-tree mst port-priority (P694)

spanning-tree mst port-priority

MST インスタンスのインタフェースプライオリティの設定を行いません。"no" を前に置くことで初期設定に戻ります。

文法

spanning-tree mst *instance_id* **port-priority** *priority*

no spanning-tree mst *instance_id* **port-priority**

- *instance_id* — MST インスタンス ID (範囲：0-4094)
- *priority* — ポートの優先順位 (0-240 の間で 16 間隔の値)

初期設定

128

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- MST に使用するインタフェースの優先順位を指定するためのコマンドです。もし、すべてのポートのパスコストが同じ場合には、高い優先順位（低い設定値）のポートが STP のアクティブリンクとなります。
- 複数のポートに最優先順位が割り当てられる場合、ポート番号の低いポートが有効となります。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

関連するコマンド

spanning-tree mst cost (P692)

spanning-tree port-priority

指定ポートのプライオリティを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree port-priority *priority*

no spanning-tree port-priority

- *priority* — ポートの優先順位（0-240 の間で 16 間隔の値）

初期設定

128

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- STP に使用するポートの優先順位を指定するためのコマンドです。もし、すべてのポートのパスコストが同じ場合には、高い優先順位（低い設定値）のポートが STP のアクティブリンクとなります。
- 1 つ以上のポートに最優先順位が割り当てられる場合、ポート番号の低いポートが有効となります。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

関連するコマンド

spanning-tree cost (P686)

spanning-tree root-guard

このコマンドは、指定されたポートが上位の BPDU を考慮に入れ、新しい STP ルートポートを選択されることを阻止するように設定します。
"no" を前に置くことで機能を無効にします。

文法

spanning-tree root-guard

no spanning-tree root-guard

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 低いブリッジ識別子（または同じ識別子と低い MAC アドレス）を持つブリッジはいつでもルートブリッジを引き継ぐことが可能です。
- スパニングツリーがスイッチまたはインタフェースでグローバルに初期化された時、スイッチはルートガードを有効にする前に、スパニングツリーが一点に集まったことが保証されるまで、20 秒間待ちます。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

spanning-tree spanning-disabled

特定のポートの STA を無効にします。"no" を前に置くことで再び STA を有効にします。

文法

spanning-tree spanning-disabled

no spanning-tree spanning-disabled

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

5 番ポートの STA を無効にしています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree loopback-detection release

ループバック検索によって、ディスカードイング状態に置かれているポートを開放します。

文法

spanning-tree loopback-detection release *interface*

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

コマンド解説

- このコマンドは "spanning-tree loopback-detection release-mode" コマンド (P690) によって、" loopback detection release mode" が " manual" に設定されており、BPDU ループバックが発生した時に、ディスカードイング状態からインタフェースを解放します。

例

```
Console#spanning-tree loopback-detection release ethernet 1/1
Console#
```


spanning-tree protocol-migration

選択したポートに送信する適切な BPDU フォーマットを再確認します。

文法

spanning-tree protocol-migration *interface*

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

コマンド解説

本機が設定、トポロジーチェンジ BPDU を含む STP BPDU を検知した場合、該当するポートは自動的に STP 互換モードにセットされます。"spanning-tree protocol-migration" コマンドを使用し、手動で選択したポートに対して最適な BPDU フォーマット (RSTP 又は STP 互換) の再確認を行うことができます。

例

```
Console#spanning-tree protocol-migration ethernet 1/5
Console#
```

show spanning-tree

STP の設定内容を表示します。

文法

show spanning-tree { *interface* | mst *instance-id* }

- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲：1-26)
 - port-channel *channel-id* (範囲：1-12)
- *instance-id* — MST インスタンス ID (範囲：0-4094)

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- パラメータを使わず "show spanning-tree" コマンドを使用した場合、ツリー内の各インタフェースのための本機のスパニングツリー設定が表示されます。
- "show spanning-tree interface" コマンドを使用した場合、指定したインタフェースのスパニングツリー設定のみ表示されます。
- 「Spanning-tree information」で表示される情報の詳細は P118 「グローバル設定」を参照して下さい。各インタフェースで表示される内容は P126 「インタフェース設定の表示」を参照して下さい。

例

```

Console#show spanning-tree
Spanning Tree Information
-----
Spanning Tree Mode           : RSTP
Spanning Tree Enabled/Disabled : Enabled
Instance                     : 0
VLANs Configuration         : 1-4093
Priority                     : 32768
Bridge Hello Time (sec.)    : 2
Bridge Max. Age (sec.)      : 20
Bridge Forward Delay (sec.) : 15
Root Hello Time (sec.)      : 2
Root Max. Age (sec.)        : 20
Root Forward Delay (sec.)   : 15
Max. Hops                    : 20
Remaining Hops               : 20
Designated Root              : 32768.001A7EABFD12
Current Root Port            : 0
Current Root Cost             : 0
Number of Topology Changes   : 0
Last Topology Change Time (sec.): 27778
Transmission Limit           : 3
Path Cost Method              : Long
-----

Eth 1/ 1 Information
-----
Admin Status                 : Enabled
Role                         : Disabled
State                        : Discarding
Admin Path Cost               : 0
Oper Path Cost                : 100000
Priority                      : 128
Designated Cost               : 0
Designated Port               : 128.1
Designated Root               : 32768.001A7EABFD12
Designated Bridge             : 32768.001A7EABFD12
Forward Transitions           : 0
Admin Edge Port               : Disabled
Oper Edge Port                : Disabled
Admin Link Type               : Auto
Oper Link Type                 : Point-to-point
Spanning-Tree Status          : Enabled
Loopback Detection Status     : Enabled
Loopback Detection Release Mode : Auto
Loopback Detection Trap       : Disabled
Root Guard Status             : Disabled
BPDU Guard Status             : Disabled
BPDU Filter Status            : Disabled
.
. 省略
.
Console#

```

show spanning-tree mst configuration

MST の設定を表示します。

文法

show spanning-tree mst configuration

コマンドモード

Privileged Exec

例

```
Console#show spanning-tree mst configuration
MSTP Configuration Information
-----
Configuration Name : 00 1a 7e ab fd 12
Revision Level      : 0

Instance VLANs
-----
      0      1-4093
Console#
```

4.18 VLAN

VLAN はネットワーク上のどこにでも位置することができますが、あたかもそれらが物理的な同一セグメントに属するかのように動作し、通信を行うポートのグループです。

ここでは VLAN 関連コマンドを使用し、指定するポートの VLAN グループの生成、メンバーポートの追加、VLAN タグ使用法の設定、自動 VLAN 登録の有効化を行います。

コマンドグループ	機能	ページ
GVRP and Bridge Extension	GVRP の設定	P703
Editing VLAN Groups	VLAN 名、VID、状態を含む VLAN の設定	P710
Configuring VLAN Interfaces	入力フィルタ、入力 / 出力タグモード、PVID、GVRP を含む VLAN インタフェースパラメータの設定	P712
Displaying VLAN Information	状態、ポートメンバー、MAC アドレスを含む VLAN グループの表示	P721
Configuring 802.1Q Tunneling	802.1Q トンネリング (QinQ トンネリング) の設定	P722
Configuring Port-based Traffic Segmentation	指定したダウンリンク / アップリンクポートに基づく、異なるクライアントセッションのトラフィックセグメンテーション設定	P727
Configuring Protocol VLANs	フレームタイプおよびプロトコルを基にしたプロトコルベース VLAN の設定	P730
Configuring IP Subnet VLANs	IP サブネット VLAN の設定	P734
Configuring MAC Based VLANs	MAC ベース VLAN の設定	P737
Configuring Voice VLANs	VoIP トラフィック検出とボイス VLAN の有効化	P740

4.18.1 GVRP の設定

GARP VLAN Registration Protocol(GVRP) はスイッチが自動的にネットワークを介してインタフェースを VLAN メンバーとして登録するために VLAN 情報を交換する方法を定義します。各インタフェース又は本機全体への GVRP の有効化の方法と、Bridge Extension MIB の設定の表示方法を説明しています。

コマンド	機能	モード	ページ
bridge-ext gvrp	本機全体に対し GVRP を有効化	GC	P704
garp timer	選択した機能への GARP タイマーの設定	IC	P705
switchport forbidden vlan	インタフェースへの登録禁止 VLAN の設定	IC	P706
switchport gvrp	インタフェースへの GVRP の有効化	IC	P707
show bridge-ext	bridge extension 情報の表示	PE	P707
show garp timer	選択した機能への GARP タイマーの表示	NE,PE	P708
show gvrp configuration	選択したインタフェースへの GVRP の設定の表示	NE,PE	P709

bridge-ext gvrp

GVRP を有効に設定します。"no" を前に置くことで機能を無効にします。

文法

bridge-ext gvrp

no bridge-ext gvrp

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

GVRP は、スイッチがネットワークを介してポートを VLAN メンバーとして登録するために VLAN 情報を交換する方法を定義します。この機能によって自動的に VLAN 登録を行うことができ、ローカルのスイッチを越えた VLAN の設定をサポートします。

例

```
Console(config)#bridge-ext gvrp
Console(config)#
```

garp timer

leave、leaveall、join タイマーに値を設定します。"no" を前に置くことで初期設定の値に戻します。

文法

garp timer < join | leave | leaveall > *timer_value*

no garp timer < join | leave | leaveall >

- < join | leave | leaveall > — 設定するタイマーの種類
- *timer_value* — タイマーの値

範囲：

join：20-1000 センチセカンド

leave：60-3000 センチセカンド

leaveall：500-18000 センチセカンド

初期設定

- join：20 センチセカンド
- leave：60 センチセカンド
- leaveall：1000 センチセカンド

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ブリッジされた LAN 内でのクライアントサービスのクライアント属性の登録、削除を行うために、Group Address Registration Protocol(GARP) は GVRP 及び GMRP で使用されます。GARP タイマーの初期設定の値は、メディアアクセス方法又はデータレートと独立しています。GMRP 又は GVRP 登録 / 削除に関する問題がない場合には、これらの値は変更しないで下さい。
- タイマーの値はすべての VLAN の GVRP に設定されます。
- タイマーの値は以下の式に適応した値である必要があります：
leave $\geq$ (2 x join)
leaveall > leave

[注意] GVRP タイマーの値は同一ネットワーク内のすべての L2 スイッチで同じに設定して下さい。同じ値に設定されない場合は GVRP が正常に機能しません。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

関連するコマンド

show garp timer (P708)

switchport forbidden vlan

禁止 VLAN の設定を行います。"no" を前に置くことで禁止 VLAN リストから削除します。

文法

switchport forbidden vlan [add *vlan-list* | remove *vlan-list*]

no switchport forbidden vlan

- add *vlan-list* — 追加する VLAN の ID のリスト
- remove *vlan-list* — 解除する VLAN の ID のリスト
- *vlan-list* — 連続しない VLAN ID をカンマで分けて入力（スペースは入れない）。
連続する ID はハイフンで範囲を指定（範囲：1-4093）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- GVRP で自動的に VLAN に加えられることを防ぐためのコマンドです。
- インタフェース上で VLAN が許可 VLAN にセットされている場合、同じインタフェースの禁止 VLAN リストに加えることはできません。

例

本例では 1 番ポートを VLAN 3 に加えることを防いでいます。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```


switchport gvrp

ポートの GVRP を有効に設定します。"no" を前に置くことで機能を無効にします。

文法

switchport gvrp

no switchport gvrp

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/6
Console(config-if)#switchport gvrp
Console(config-if)#
```

show bridge-ext

ブリッジ拡張コマンドの設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

表示される内容は P26 「ブリッジ拡張機能の表示」を参照して下さい。

例

```
Console#show bridge-ext
Maximum Supported VLAN Numbers      : 26
Maximum Supported VLAN ID           : 4093
Extended Multicast Filtering Services : No
Static Entry Individual Port         : Yes
VLAN Learning                       : IVL
Configurable PVID Tagging            : Yes
Local VLAN Capable                   : No
Traffic Classes                      : Enabled
Global GVRP Status                   : Disabled
GMRP                                 : Disabled
Console#
```

show garp timer

選択したポートの GARP タイマーを表示します。

文法

show garp timer { *interface* }

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-5)

初期設定

すべての GARP タイマーを表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP Timer Status:
Join Timer      : 20 centiseconds
Leave Timer      : 60 centiseconds
Leave All Timer  : 1000 centiseconds
Console#
```

関連するコマンド

garp timer (P705)

show gvrp configuration

GVRP が有効か無効かを表示します。

文法

show gvrp configuration { interface }

- *interface*
 - *ethernet unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

初期設定

全体と各インタフェース両方の設定を表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show gvrp configuration ethernet 1/6
Eth 1/ 6:
  Gvrp configuration: Enabled
Console#
```

4.18.2 VLAN グループの設定

コマンド	機能	モード	ページ
vlan database	VLAN database モードに入り、VLAN の設定を行う	GC	P710
VLAN	VID,VLAN 名、ステートなど VLAN の設定	VC	P711

vlan database

VLAN データベースモードに入ります。このモードのコマンドは設定後直ちに有効となります。

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- VLAN データベースコマンドを使用し VLAN の追加、変更、削除が行えます。VLAN の設定終了後は "show vlan" コマンドを使用しエントリー毎に VLAN 設定を表示することができます。
- "interface vlan" コマンドモードを使用し、ポートメンバーの指定や、VLAN からのポートの追加、削除が行えます。コマンドを使用した結果は、実行中の設定ファイルに書き込まれ "show running-config" コマンドを使用することでファイルの内容を表示させることができます。

例

```
Console(config)#vlan database
Console(config-vlan)#
```

関連するコマンド

show vlan (P721)

vlan

VLAN を設定します。"no" を前に置くことで VLAN の削除、もしくは初期設定に戻します。

文法

vlan *vlan-id* [name *vlan-name*] [media ethernet { state < active | suspend > }] { rspan }

no vlan *vlan-id* { name | state }

- *vlan-id* — 設定する VLAN ID (範囲：1-4093)
- name — 識別するための VLAN 名
- *vlan-name* — 1-32 文字
- media ethernet — イーサネットメディアの種類
- state — VLAN のステートの識別
 - active — VLAN の実行
 - suspend — VLAN の中断。中断中の VLAN はパケットの転送を行いません。
 - rspan — リモートスイッチからのトラフィックミラーリングに使用される VLAN を作成します。RSPAN で使用される VLAN は VLAN1 (スイッチのデフォルト VLAN) と VLAN4093 (スイッチクラスタリングで使用) を含むことが出来ません。CLI からの RSPAN 設定については 637 ページの「RSPAN ミラーリング」を参照してください。

初期設定

初期設定では VLAN 1 が存在し、active 状態です。

コマンドモード

VLAN Database Configuration

コマンド解説

- "no vlan *vlan-id*" を使用した場合、VLAN が削除されます。
- "no vlan *vlan-id* name" を使用した場合、VLAN 名が削除されます。
- "no vlan *vlan-id* state" を使用した場合、VLAN は初期設定の状態 (active) に戻ります。
- 最大 4093VLAN の設定が可能です。

[注意] 本機は最大 255 個のユーザ管理可能な VLAN を作成することが出来ます。

例

VLAN ID：105、VLAN name：RD5 で新しい VLAN を追加しています。VLAN は初期設定で active になっています。

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

関連するコマンド

show vlan (P721)

4.18.3 VLAN インタフェースの設定

コマンド	機能	モード	ページ
interface vlan	VLAN を設定するための Interface 設定モードへの参加	IC	P713
switchport acceptable frame types	インタフェースで受け入れ可能なフレームタイプの設定	IC	P714
switchport allowed vlan	インタフェースに関連した VLAN の設定	IC	P715
switchport forbidden vlan	インタフェースの登録を禁止する VLAN の設定	IC	P706
switchport gvrp	インタフェースへの GVRP の有効化	IC	P707
switchport ingress-filtering	インタフェースへの入力フィルタの有効化	IC	P716
switchport mode	インタフェースの VLAN メンバーモードの設定	IC	P717
switchport native vlan	インタフェースの PVID(native VLAN) の設定	IC	P718
switchport priority default	タグなし受信フレームのポートプライオリティの設定	IC	P750
vlan-trunking	スイッチを通る未知の VLAN を許可	IC	P719

interface vlan

VLAN の設定のために interface 設定モードに入り、各インタフェースの設定を行います。
"no" を前に置くことで設定を削除します。

文法

interface vlan *vlan-id*
no interface vlan

- *vlan-id* — 設定する VLAN ID（範囲：1-4093）

初期設定

なし

コマンドモード

Global Configuration

例

本例では、VLAN 1 の interface configuration モードに参加し、VLAN に対し IP アドレスを設定しています。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

関連するコマンド

show vlan (P721)
interface vlan (P713)

switchport acceptable-frame-types

ポートの受け入れ可能なフレームの種類を指定します。"no" を前に置くことで初期設定に戻します。

文法

`switchport acceptable-frame-types < all | tagged >`

`no switchport acceptable-frame-types`

- all — タグ付、タグなしのすべてのフレームを受け入れます。
- tagged — タグ付フレームのみを受け入れます。

初期設定

すべてのフレームタイプ

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

すべてのフレームを許可する設定にした場合、タグなし受信フレームはデフォルト VLAN に指定されます。

例

本例では 1 番ポートにタグ付フレームのみを許可する設定にしています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

関連するコマンド

`switchport mode` (P717)

switchport allowed vlan

選択したインタフェースの VLAN グループの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

switchport allowed vlan [add *vlan-list* { tagged | untagged } | remove *vlan-list*]

no switchport allowed vlan

- add *vlan-list* — 追加する VLAN の ID のリスト
- remove *vlan-list* — 解除する VLAN の ID のリスト
- *vlan-list* — 連続しない VLAN ID をカンマで分けて入力（スペースは入れない）。連続する ID はハイフンで範囲を指定（範囲：1-4093）

初期設定

すべてのポートが VLAN 1 に参加。
フレームタイプはタグなし。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- switchport モードが "trunk" に設定されている場合、インタフェースをタグ付メンバーとしてしか VLAN に設定できません。
- インタフェースの switchport mode が "hybrid" に設定されている場合、インタフェースを最低 1 つの VLAN にタグなしメンバーとして設定する必要があります。
- スイッチ内では常にフレームはタグ付となっています。タグ付及びタグなしパラメータはインタフェースへ VLAN を加えるとき使われ、出力ポートでフレームのタグをはずすか保持するかを決定します。
- ネットワークの途中や対向のデバイスが VLAN をサポートしていない場合、インタフェースはこれらの VLAN をタグなしメンバーとして加えます。1 つの VLAN にタグなしとして加え、その VLAN がネイティブ VLAN となります。
- インタフェースの禁止リスト上の VLAN が手動でインタフェースに加えられた場合、VLAN は自動的にインタフェースの禁止リストから削除されます。

例

本例では、1 番ポートのタグ付 VLAN 許可リストに VLAN1,2,5,6 を加えています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport ingress-filtering

ポートに対してイングレスフィルタリングを有効にします。"no" を前に置くことで初期設定に戻します。

文法

switch port ingress-filtering

no switchport ingress-filtering

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ・ イングレスフィルタリングはタグ付フレームにのみ有効です。
- ・ イングレスフィルタリングが有効の場合、メンバーでない VLAN へのタグがついたフレームを受信すると、そのフレームは捨てられます。
- ・ イングレスフィルタリングは GVRP や STP などの VLAN と関連のない BPDU フレームには影響を与えません。但し、VLAN に関連した GMRP などの BPDU フレームには影響を与えます。

例

本例では、1 番ポートを指定し、イングレスフィルタリングを有効にしています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport mode

ポートの VLAN メンバーシップモードの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

switchport mode < access | hybrid | trunk >

no switchport mode

- access — アクセス VLAN インタフェースを指定。このポートはタグ無しフレームのみ受信 / 転送を行います。
- hybrid — ハイブリッド VLAN インタフェースを指定。ポートはタグ付及びタグなしフレームを送信します。
- trunk — VLAN トランクに使用されるポートを指定します。トランクは 2 つのスイッチ間の直接接続で、ポートはソース VLAN を示すタグ付フレームを送信します。デフォルト VLAN に所属するフレームもタグ付フレームを送信します。

初期設定

すべてのポートは hybrid に指定され、VLAN 1 が PVID に設定されています。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

アクセスモードと VLAN トランキング (719 ページの「vlan-trunking」を参照) は相互に排他的です。もし VLAN トランキングがインタフェースで有効の場合、インタフェースはアクセスモードに設定できず、その逆もまた同様です。

例

本例では、1 番ポートの configuration モードに入り、switchport モードを hybrid に指定しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

関連するコマンド

switchport acceptable-frame-types (P714)

switchport native vlan

ポートへのデフォルト VLAN ID である PVID の設定を行います。"no" を前に置くことで初期設定に戻します。

文法

switchport native vlan *vlan-id*

no switchport native vlan

- *vlan-id* — ポートへのデフォルト VLAN ID（範囲：1-4093）

初期設定

VLAN 1

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- PVID を設定するためには、対象のポートが指定する PVID と同じ VLAN に所属しており、またその VLAN がタグなしである必要があります。
- 受け入れ可能なフレームタイプを "all" にしている場合か、switchport モードを "hybrid" にしている場合、入力ポートに入るすべてのタグなしフレームには PVID が挿入されます。

例

本例では PVID を VLAN3 として 1 番ポートに設定しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

vlan-trunking

未知の VLAN グループが指定されたインタフェースを通過することを許可します。
"no" を前に置くことで、この機能を無効にします。

文法

vlan-trunking
no vlan-trunking

初期設定

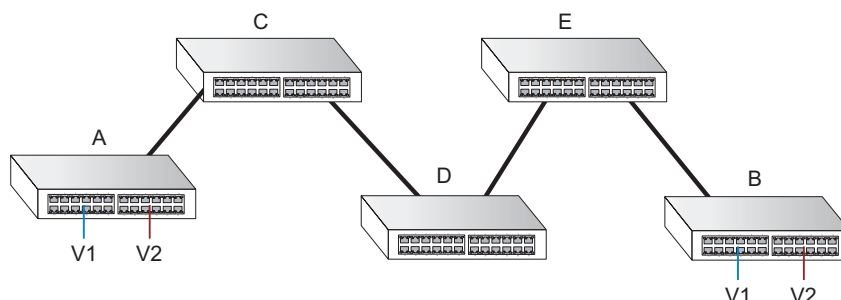
無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 本コマンドは、それらが属さない VLAN グループのトラフィックを渡す 1 つ以上の中
間スイッチを横切るトンネルを設定します。
以下の図は VLAN1 と 2 をスイッチ A と B へ VLAN トランキングと共に設定し、ス
イッチ C,D および E を横断するこれらの VLAN グループがトラフィックを渡すために
使用されます。



VLAN トランキングが無い場合、全ての中間スイッチへ VLAN1 と 2 を設定する必要があります。さもなければこれらのスイッチは未知の VLAN グループタグのついたフ
レームを破棄します。VLAN トランキングを有効にすれば、スイッチ A と B へのみ、
これらの VLAN グループを作成するだけで中間スイッチポートは経路に沿って VLAN1
と VLAN2 の接続が行えます。

D と E は、VLAN グループタグ 1 と 2 が付いたフレームを自動的に許可し、VLAN ト
ランキングポートを通過することが可能になります。

- この機能には以下の制限が適用されます。
 - VLAN トランキングは "access" スイッチポートモード（717 ページの「switchport mode」を参照）と相互に排他的です。もし VLAN トランキングがインタフェースで有効の場合、このインタフェースはアクセスモードには設定することが出来ません。その逆もまた同様です。
 - スパニングツリー構成からのループを防ぐ為、全ての未知の VLAN は一つのインスタンス（STP/RSTP または MSTP インスタンス、選択された STA モードに依存）へバインドされます。

コマンドラインインタフェース

VLAN

- ポートで、VLAN トランキングとイングレスフィルタリングの両方が無効の場合、未知のタグが付いたパケットはこのインタフェースへ入ることを許可され、VLAN トランキングが有効であるその他全てのポートへフラッドされます。(VLAN トランキングの効果は未知の VLAN で依然有効です。)

例

```
Console(config)#interface ethernet 1/25
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/26
Console(config-if)#vlan-trunking
Console(config-if)#
```

4.18.4 VLAN 情報の表示

コマンド	機能	モード	ページ
show interfaces status vlan	特定 VLAN インタフェースの状態の表示	NE,PE	P616
show interfaces switchport	インタフェースの管理、運用状態の表示	NE,PE	P617
show vlan	VLAN 情報の表示	NE,PE	P721

show vlan

VLAN 情報の表示を行います。

文法

show vlan { id *vlan-id* | name *vlan-name* }

- *vlan-id* — VLAN ID（範囲：1-4093）
- *vlan-name* — VLAN 名（範囲：1-32 文字）

初期設定

すべての VLAN を表示

コマンドモード

Normal Exec, Privileged Exec

例

本例では VLAN 1 の情報を表示しています。

```

Console#show vlan id 1

VLAN ID          : 1
Type              : Static
Name              : DefaultVlan
Status            : Active
Ports/Port Channels : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                   Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                   Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                   Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                   Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                   Eth1/26(S)

Console#

```

4.18.5 IEEE802.1Q トンネリングの設定

IEEE 802.1Q トンネリング (QinQ) 機能を使用することにより、サービス プロバイダは複数の VLAN を設定しているカスタマを、1 つの VLAN を使用してサポートできます。カスタマの VID は保持されるため、さまざまなカスタマからのトラフィックは、同じ VLAN 上に存在するように見える場合でも、サービスプロバイダのインフラストラクチャ内では分離されています。QinQ トンネリングでは、VLAN 内 VLAN 階層を使用して、タグ付きパケットに再度タグ付けを行うこと (ダブルタギングとも呼ばれます) によって、VLAN スペースを拡張します。

この節では、QinQ トンネリングの設定に使用されるコマンドについて説明します。

コマンド	機能	モード	ページ
dot1q-tunnel system-tunnel-control	スイッチをノーマルモードまたは QinQ モードに設定	GC	P723
switchport dot1q-tunnel mode	インタフェースを QinQ トンネルポートに設定	IC	P724
switchport dot1q-tunnel tpid	トンネルポートの TPID (Tag Protocol Identifier) 値を設定	IC	P725
show dot1q-tunnel	QinQ トンネルポートの設定を表示	PE	P726
show interfaces switchport	QinQ ポートステータスを表示	PE	P617

QinQ の一般的な設定ガイド

- (1) スwitchを QinQ モードに設定 (dot1q-tunnel system-tunnel-control P723)
- (2) SPVLAN を作成 (vlan P711)
- (3) QinQ トンネルアクセスポートを dot1Q トンネルアクセスモードに設定 (switchport dot1q-tunnel mode P724)
- (4) トンネルアクセスポートの Tag Protocol Identifier (TPID) 値を設定。このステップは、接続されているクライアントが、802.1Q タグ付きフレームの識別に非標準 2-byte イーサタイプを使用している場合に必要です。 (switchport dot1q-tunnel tpid P725)
- (5) QinQ トンネルアクセスポートをタグ無しメンバーとして SPVLAN に追加 (switchport allowed vlan P715)
- (6) QinQ トンネルアクセスポートの SPVLAN ID をネイティブ VID として設定 (switchport native vlan P718)
- (7) QinQ トンネルアップリンクポートを dot1Q トンネルアップリンクモードに設定 (switchport dot1q-tunnel mode P724)
- (8) QinQ トンネルアップリンクポートをタグ付きメンバーとして SPVLAN に追加 (switchport allowed vlan P715)

QinQ の制限事項

- トンネルアップリンクポートのネイティブ VLAN とトンネルアクセスポートは同一には出来ませんが、同じサービス VLAN を両方のトンネルポートタイプに設定することは可能です。
- トンネルポートでは IGMP スヌーピングを有効に出来ません。
- スパニングツリープロトコルが有効時に、スパニングツリー構造がツリーの中断を克服するために自動で再配置された場合、トンネルアクセスまたはトンネルアップリンクポートは無効になります。これらのポートではスパニングツリーを無効にすることが賢明です。

dot1q-tunnel system-tunnel-control

スイッチが QinQ モードで動作するよう設定を行います。"no" を前に置くと QinQ オペレーティングモードを無効にします。

文法

dot1q-tunnel system-tunnel-control

no dot1q-tunnel system-tunnel-control

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

QinQ インタフェース設定が機能するために、QinQ トンネルモードをスイッチで有効にしてください。

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

関連するコマンド

show dot1q-tunnel (P726)

show interfaces switchport (P617)

switchport dot1q-tunnel mode

インタフェースを QinQ トンネルポートとして設定します。"no" を前に置くことでインタフェースの QinQ を無効にします。

文法

switchport dot1q-tunnel mode < access | uplink >

no switchport dot1q-tunnel mode

- access — ポートを 802.1Q トンネルアクセスポートに設定
- uplink — ポートを 802.1Q トンネルアップリンクポートに設定

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- switchport dot1q-tunnel mode インタフェースコマンドを使用する前に、dot1q-tunnel system-tunnel-control コマンド (P723) を使用して QinQ トンネリングを有効にする必要があります。
- トンネルアップリンクポートがカスタマからのパケットを受信した際、カスタマタグ (1 つ以上のタグレイヤがあるか否かにかかわらず) は内側に保持され、サービスプロバイダのタグが外側のタグに付加されます。
- トンネルアップリンクポートがサービスプロバイダからのパケットを受信した際、外側のサービスプロバイダタグは取り除かれ、パケットは内側のタグが示す VLAN へ渡されます。内側のタグが見つからない場合、パケットはアップリンクポートに定義されたネイティブ VLAN へ渡されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

関連するコマンド

show dot1q-tunnel (P726)

show interfaces switchport (P617)

switchport dot1q-tunnel tpid

トンネルポートの Tag Protocol Identifier (TPID) 値を設定します。"no" を前に置くことで設定を初期値へ戻します。

文法

switchport dot1q-tunnel tpid *tpid*

no switchport dot1q-tunnel tpid

- *tpid* — 802.1Q カプセル化のイーサタイプ値を設定。この識別子は 802.1Q タグ付きフレームの識別に非標準 2-byte を選択するために使用します。標準イーサタイプ値は 0x8100 (範囲: 0800-FFFF16 進数)

初期設定

0x8100

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- "switchport dot1q-tunnel tpid" コマンドは選択されたインタフェースのカスタム 802.1Q イーサタイプ値を設定します。
この機能は本機へ、802.1Q タグ付きフレームの識別に標準 0x8100 イーサタイプを使用しないサードパーティ製スイッチとインタオペレートすることを許可します。
例えば、0x1234 はトランクポートのカスタム 802.1Q イーサタイプとして設定され、このイーサタイプを含む入力フレームは、イーサタイプフィールドに続くタグに含まれる VLAN へ、標準的 802.1Q トランクとして割り当てられます。
その他のイーサタイプを持つポートへ到着したフレームはタグ無しフレームとして見られ、このポートのネイティブ VLAN へ割り当てられます。
- スwitchの全てのポートは同じイーサタイプに設定されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

関連するコマンド

show interfaces switchport (P617)

show dot1q-tunnel

QinQ トンネルポート情報を表示します。

コマンドモード

Privileged Exec

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel

Current double-tagged status of the system is Enabled

The dot1q-tunnel mode of the set interface 1/1 is Access mode,
TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/2 is Uplink mode,
TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/3 is Normal mode,
TPID is 0x8100.
.
.
.
```

関連するコマンド

switchport dot1q-tunnel mode (P724)

4.18.6 ポートベーストラフィックセグメンテーション

ローカルネットワークおよびサービスプロバイダへのアップリンクポート上で、異なるクライアントからダウンリンクポートを通過するトラフィックに、より厳しいセキュリティが必要とされる際、個々のクライアントセッションのトラフィックを隔離するためにポートベーストラフィックセグメンテーションを使用できます。

コマンド	機能	モード	ページ
traffic-segmentation	トラフィックセグメンテーションの有効化と設定	GC	P728
show traffic-segmentation	トラフィックセグメンテーション設定の表示	PE	P729

traffic-segmentation

トラフィックセグメンテーションをグローバルで有効にします。また、ポートのセグメンテーショングループのアップリンクおよびダウンリンクポートの設定を行います。"no" を前に置くことで、トラフィックセグメンテーションをグローバルで無効にします。

文法

[no] traffic-segmentation { uplink interface-list downlink interface-list }

- uplink— アップリンクインタフェースを指定
- downlink— ダウンリンクインタフェースを指定

初期設定

グローバルで無効

セグメンテーションポートグループは未定義

コマンドモード

Global Configuration

コマンド解説

- トラフィックセグメンテーションは、ポートベースセキュリティと VLAN 内のポート間の隔離を提供します。
ダウンリンクポートのデータトラフィックはディスティネーションアップリンクポートとのみ送受信が可能です。データは、同じセグメントされたグループ内のダウンリンクポート間または同じグループに属さないポート間でやり取りされません。
- ポートはアップリンクポートまたはダウンリンクポートとして定義することが可能ですが、両方の役割で動作するよう設定は出来ません。
- トラフィックセグメンテーションおよび通常 VLAN は同じスイッチの中に同時に存在することが出来ます。トラフィックはセグメントされたグループのアップリンクポート間と通常 VLAN のポートを自由に通ることが出来ます。
- パラメータ無しで "traffic-segmentation" コマンドでトラフィックセグメンテーションを有効にし、セグメントされたグループのインタフェースメンバーを設定します。
- "no" を前に付けると、トラフィックセグメンテーションを無効にし、セグメントされたグループの設定をクリアします。

例

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/10
downlink ethernet 1/5-8
Console(config)#
```

show traffic-segmentation

トラフィックセグメンテーションの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show traffic-segmentation
Private VLAN status: Disabled
Up-link Port:
  Ethernet 1/12
Down-link Port:
  Ethernet 1/5
  Ethernet 1/6
  Ethernet 1/7
  Ethernet 1/8
Console#
```

4.18.7 プロトコル VLAN の設定

通常の VLAN では、プロトコル毎の VLAN グループの形成を容易に行なうことはできません。そのため、特定のプロトコルに関連するすべての機器が通信を行えるよう、特殊なネットワーク機器を使用して異なる VLAN 間の通信をサポートする必要があります。しかし、このような方法では、セキュリティと容易な設定が可能な VLAN のメリットを失ってしまいます。

そのような問題を回避するため、本機では物理的なネットワークの構成を、プロトコルを基にした論理的 VLAN のネットワーク構成とすることが可能なプロトコルベース VLAN 機能を提供します。ポートがフレームを受信した際、受信フレームのプロトコルタイプに応じて VLAN メンバーシップが決定されます。

コマンド	機能	モード	ページ
protocol-vlan protocol-group	プロトコルグループの作成及びサポートプロトコルの指定	GC	P731
protocol-vlan protocol-group	プロトコルグループの VLAN へのマッピング	IC	P732
show protocol-vlan protocol-group	プロトコルグループの設定の表示	PE	P733
show interfaces protocolvlan protocol-group	VLAN へのプロトコルグループマッピングの表示	PE	P733

プロトコル VLAN の設定は以下の手順で行ないます。

- (1) 使用するプロトコルのための VLAN グループを作成します。主要なプロトコル毎に VLAN の作成を行なうこと推奨します。また、この時点ではポートメンバーの追加を行なわないで下さい。
- (2) VLAN に設定するプロトコル毎のグループを "protocol-vlan protocol-group" コマンド (Global Configuration mode) を利用して生成します。
- (3) 適切な VLAN に各インタフェースのプロトコルを "protocol-vlan protocol-group" コマンド (Interface Configuration mode) を利用してマッピングします。

protocol-vlan protocol-group (Configuring Groups)

プロトコルグループの作成及び特定のプロトコルのグループへの追加を行ないます。"no" を前に置くことでプロトコルグループを削除します。

文法

protocol-vlan protocol-group *group-id* [< add | remove > frame-type *frame*
protocol-type *protocol*]

no protocol-vlan protocol-group *group-id*

- *group-id* — プロトコルグループ ID (設定範囲: 1-2147483647)
- *frame* — プロトコルで使用するフレームタイプ (オプション: ethernet、rfc_1042、llc_other)
- *protocol* — プロトコルタイプ。iic_other フレームタイプは ipx_raw のみ選択できます。その他全てのフレームタイプのオプションは ip、arp、rarp、ipv6 です。

初期設定

プロトコルグループ未設定

コマンドモード

Global Configuration

例

プロトコルグループ "1" を作成し、フレームタイプを "Ethernet"、プロトコルタイプを "ARP" に設定しています。

```
Console(config)#protocol-vlan protocol-group 2 add frame-type ethernet
protocol-type arp
Console(config)#
```

protocol-vlan protocol-group (Configuring Interface)

インタフェースにおいてプロトコルグループを VLAN にマッピングします。"no" を前におくことでインタフェースのプロトコルのマッピングを解除します。

文法

protocol-vlan protocol-group *group-id* **vlan** *vlan-id*

no protocol-vlan protocol-group *group-id* **vlan**

- *group-id* — プロトコルグループ ID (設定範囲：1-2147483647)
- *vlan-id* — 致したプロトコルの通信が転送される VLAN (設定範囲：1-4093)

初期設定

プロトコルグループはインタフェースにマップされていません。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- フレームがプロトコル VLAN に割り当てられたポートに入力する場合、以下の方法で処理されます。
 - －フレームにタグ付フレームの場合、タグの情報に基づき処理されます。
 - －フレームがタグなしフレームで、プロトコルタイプが一致した場合、フレームは適切な VLAN に転送されます。
 - －フレームがタグなしフレームで、プロトコルタイプが一致しない場合、フレームはインタフェースのデフォルト VLAN に転送されます。

例

本例では、1 番ポートに入ってきた通信でプロトコルグループ 1 と一致する通信が VLAN2 にマッピングしています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

プロトコルグループに関連したフレーム及びプロトコルタイプの表示

文法

show protocol-vlan protocol-group { *group-id* }

- *group-id* — プロトコルグループ ID（設定範囲：1-2147483647）

初期設定

すべてのプロトコルグループを表示

コマンドモード

Privileged Exec

例

```
Console#show protocol-vlan protocol-group
ProtocolGroup ID Frame Type Protocol Type
-----
                2   RFC 1042         08 00
Console#
```

show interfaces protocol-vlan protocol-group

プロトコルグループから VLAN へのマッピングを表示します。

文法

show interfaces protocol-vlan protocol-group { *interface* }

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号（範囲：1-26）
 - port-channel *channel-id*（範囲：1-12）

初期設定

マッピングされた全てのプロトコルグループを表示

コマンドモード

Privileged Exec

例

```
Console#show interfaces protocol-vlan protocol-group

Port          ProtocolGroup ID   VLAN ID
-----
Eth 1/1              1         vlan2
Console#
```

4.18.8 IP サブネット VLAN

ポートベースの分類を使用する時、ポートによって受け取られた全てのタグ無しフレームは、ポートと関連付けられた VID (PVID) の VLAN に属しているとして分類されます。

IP サブネット VLAN 分類が有効時、タグ無し入力フレームのソースアドレスは IP subnet-to-VLAN マッピングテーブルにたいしてチェックが行われます。

エントリがサブネットに見つかった場合、これらのフレームはエントリが示し VLAN へ割り当てられます。

IP サブネットが一致しない場合、タグ無しフレームは受信ポートの VLAN ID (PVID) に属しているとして分類されます。

コマンド	機能	モード	ページ
subnet-vlan	IP サブネット VLAN を定義	GC	P735
show subnet-vlan	IP サブネット VLAN 設定を表示	PE	P736

subnet-vlan

IP サブネット VLAN 割り当てを設定します。"no" を前に置くことで、IP サブネットから VLAN への割り当てを削除します。

文法

subnet-vlan subnet *ip-address mask* *vlan* *vlan-id* { *priority* *priority* }

no subnet-vlan < *ip-address mask* | all >

- *ip-address* — *ip-address* - サブネットを定義する IP アドレス。有効な IP アドレスはピリオドで区切られた 0-255 の 4 つの 10 進数で成り立ちます。
- *mask* — IP サブネットのホストアドレスビットを識別します。
- *vlan-id* — VLAN ID(範囲：1-4093)
- *priority* — タグ無し入カトラフィックにアサインされるプライオリティ（範囲：0-7 7 が最高プライオリティ）

初期設定

プライオリティ：0

コマンドモード

Global Configuration

コマンド解説

- それぞれの IP サブネットは 1 つの VLAN ID へのみマップが可能です。IP サブネットは IP アドレスとマスクから構成されます。
- ポートでタグ無しフレームが受信された際、ソース IP アドレスは IP subnet-to-VLAN マッピングテーブルに対してチェックが行われ、もしエントリが見つかった場合、対応する VLAN ID がフレームに割り当てられます。
もしマッピングが見つからない場合、受信ポートの PVID がフレームへ割り当てられます。
- IP サブネットはブロードキャストまたはマルチキャスト IP アドレスになることはできません。
- MAC ベース、IP サブネットベース、プロトコルベース VLAN が同時にサポートされる時、プライオリティはこの順番で適用され、ポートベース VLAN は最後になります。

例

VLAN4 にサブネット 192.168.12.192、マスク 255.255.255.224 のトラフィックを割り当てます。

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```

show subnet-vlan

IP サブネット VLAN 割り当てを表示します。

コマンドモード

Privileged Exec

コマンド解説

・本コマンドは subnet-to-VLAN マッピングを表示するために使用します。

例

全ての設定された IP サブネットベース VLAN を表示しています。

```
Console#show subnet-vlan
IP Address      Mask              VLAN ID  Priority
-----
192.168.1.1     255.255.255.0    1        0
Console#
```

4.18.9 MAC ベース VLAN

802.1Q ポートベース VLAN 分類を使用する時、ポートで受信される全てのタグ無しフレームは、VID (PVID) がそのポートと関連付けられた VLAN に所属するように分類されます。MAC ベース VLAN 有効時、タグ無し入力フレームのソースアドレスは、MAC address-to-VLAN テーブルに対して照合が行われます。

このアドレスのエントリが見つかった場合、これらのフレームはエントリが示す VLAN へ割り当てられます。

MAC アドレスが一致しない場合、タグ無しフレームは受信ポートの VLAN ID (PVID) に属しているとして分類されます。

コマンド	機能	モード	ページ
mac-vlan	MAC address-to-VLAN マッピングを設定	GC	P738
show mac-vlan	MAC ベース VLAN 設定の表示	PE	P739

mac-vlan

MAC address-to-VLAN マッピングの設定を行います。"no" を前に置くことで割り当てを削除します。

文法

mac-vlan mac-address *mac-address* vlan *vlan-id* { *priority priority* }

no mac-vlan mac-address < *mac-address* | all >

- *mac-address* — マッチするソース MAC アドレス。設定された MAC アドレスはユニキャストアドレスにのみなれます。MAC アドレスは "xx-xx-xx-xx-xx-xx" または "xxxxxxxxxxxx" のフォーマットで指定してください。
- *vlan-id* — ソース MAC アドレスとマッチする VLAN（設定範囲：1-4093）
- *priority* — タグ無し入力トラフィックにアサインされるプライオリティ（範囲：0-7 7 が最高プライオリティ）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- MAC-to-VLAN マッピングは本機の全てのポートへ適用されます。
- ソース MAC アドレスは 1 つの VLAN ID へのみマップされることが可能です。
- 設定された MAC アドレスはブロードキャストまたはマルチキャストアドレスにはなりません。
- MAC ベース、IP サブネットベース、プロトコル VLAN が同時にサポートされる時、このシーケンスではプライオリティが適用され、最後にポートベース VLAN になります。

例

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10
Console(config)#
```


show mac-vlan

MAC address-to-VLAN 割り当てを表示します。

コマンドモード

Privileged Exec

コマンド解説

- このコマンドは MAC Address-to-VLAN マッピングを表示するために使用します。

例

```
Console#show mac-vlan
      MAC address      VLAN ID
-----
  00-00-00-11-22-33    10
Console#
```

4.18.10 Voice VLAN

IP 電話がエンタープライズネットワークに配置される場合、他のデータトラフィックから VoIP ネットワークを分離することを推奨します。トラフィックの分離は極端なパケット到達遅延、パケットロス、ジッターを防ぎ、より高い音声品質を得ることにつながります。これは 1 つの Voice VLAN にすべての VoIP トラフィックを割り当てることで実現できます。

Voice VLAN を使用することにはいくつかの利点があります。他のデータトラフィックから VoIP トラフィックを分離することでセキュリティが保たれます。エンドツーエンドの QoS ポリシーと高い優先度の設定により、ネットワークを横断して VoIP VLAN トラフィックに必要な帯域幅を保証することができます。また、VLAN 分割は音声品質に重大な影響を及ぼすブロードキャストやマルチキャストからトラフィックを保護することができます。

スイッチはネットワーク間で Voice VLAN を設定し、VoIP トラフィックに CoS 値を設定することができます。VoIP トラフィックはパケットの送信先 MAC アドレス、もしくは接続された VoIP デバイスを発見するために LLDP (IEEE802.1AB) を使うことで、スイッチポート上において検出されます。VoIP トラフィックが設定されたポート上で検出されたとき、スイッチは自動的に Voice VLAN のタグメンバーとしてポートを割り当てます。スイッチポートを手動で設定することもできます。

コマンド	機能	モード	ページ
voice vlan	Voice VLAN ID を設定	GC	P741
voice vlan aging	Voice VLAN ポートのエイジングタイムを設定	GC	P741
voice vlan mac-address	VoIP デバイスの MAC アドレスを設定	GC	P742
switchport voice vlan	Voice VLAN ポートモードを設定	IC	P743
switchport voice vlan priority	ポートの VoIP トラフィックプライオリティを設定	IC	P743
switchport voice vlan rule	自動 VoIP トラフィック検出メソッドをポートに設定	IC	P744
switchport voice vlan security	ポートの Voice VLAN セキュリティを有効	IC	P745
show voice vlan	Voice VLAN 設定を表示	PE	P746

voice vlan

VoIP トラフィックの検出を有効にし、Voice VLAN ID を定義します。"no" を前に置くことで機能を無効にします。

文法

voice vlan *voice-vlan-id*

no voice vlan

- *voice-vlan-id* — Voice VLAN ID を指定します（範囲：1-4093）

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#voice vlan 1234
Console(config)#
```

voice vlan aging

Voice VLAN ID タイムアウトを設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

voice vlan aging *minutes*

no voice vlan

- *minutes* — タイムアウトを指定します（範囲：5-43200 分）

初期設定

1440 分

コマンドモード

Global Configuration

例

```
Console(config)#voice vlan aging 3000
Console(config)#
```

voice vlan mac-address

OUI テレフォニーリストに追加する MAC アドレスの範囲を指定します。"no" を前に置くことでリストからエントリを削除します。

文法

voice vlan mac-address *mac-address* mask *mask-address* { *description* *description* }

no voice vlan mac-address *mac-address* mask *mask-address*

- *mac-address* — ネットワーク上の VoIP デバイスを識別する MAC アドレス OUI を指定します。(例：01-23-45-00-00-00)
- *mask-address* — VoIP デバイスの MAC アドレスの範囲を確定します。
(範囲：80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF 初期設定：FF-FF-FF-00-00-00)
- *description* — VoIP デバイスを識別するためのユーザー定義テキスト (範囲：1-32 文字)

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- Mask の設定 — 「FF-FF-FF-00-00-00」を設定すると同じ OUI 番号（最初の 3 オクテットが同一）であるすべてのデバイスを VoIP デバイスとして認識します。他の値を指定することで MAC アドレスの範囲を制限することができます。ここで「FF-FF-FF-FF-FF-FF」を選択すると 1 つの MAC アドレスのみ VoIP デバイスとして設定します

例

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask  
ff-ff-ff-00-00-00 description A new phone  
Console(config)#
```

switchport voice vlan

ポートの Voice VLAN モードを指定します。"no" を前に置くことで、ポートの Voice VLAN 機能を無効にします。

文法

switchport voice vlan < manual | auto >
no switchport voice vlan

- manual — Voice VLAN 機能はポート上で有効になりますが、ポートは手動で Voice VLAN に追加されます。
- auto — ポートが VoIP トラフィックを検出したとき、ポートは Voice VLAN のタグメンバーとして追加されます。VoIP トラフィックを検出する方法を、OUI か 802.1AB のどちらから選択しなくてははいけません。OUI を選択した場合、Telephony OUI List で MAC アドレスの範囲を確認してください。

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

switchport voice vlan priority

ポートの VoIP トラフィックに、CoS プライオリティを指定します。"no" を前に置くことで、設定を初期状態に戻します。

文法

switchport voice vlan priority *priority-value*
no switchport voice vlan priority

priority-value — CoS プライオリティ値（範囲：0-6）

初期設定

6

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

switchport voice vlan rule

ポートで VoIP トラフィックを検出する方法を選択します。"no" を前に置くことで、選択した検出メソッドを無効にします。

文法

switchport voice vlan rule < oui | lldp >

no switchport voice vlan rule < oui | lldp >

- oui — VoIP デバイスからのトラフィックは送信元 MAC アドレスの Organizationally Unique Identifier (OUI) によって検出されます。OUI 番号は製造者によって割り当てられ、デバイスの MAC アドレスの最初の 3 オクテットを構成します。スイッチが VoIP デバイスからのトラフィックを認識するには、MAC アドレスの OUI 番号を Telephony OUI List で構成しなくてはなりません。
- lldp — ポートに接続された VoIP デバイス発見するために LLDP を使用します。LLDP は System Capability TLV の中の Telephone Bit が有効であるかどうかをチェックします。LLDP (Link Layer Discovery Protocol) については 826 ページの「LLDP コマンド」を参照してください。

初期設定

OUI：有効

LLDP：無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

switchport voice vlan security

ポートの、VoIP トラフィックのセキュリティフィルタリングを有効にします。"no" を前に置くことで、フィルタリングを無効にします。

文法

switchport voice vlan security

no switchport voice vlan security

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

show voice vlan

Voice VLAN 設定情報および OUI テレフォニーリストを表示します。

文法

show voice vlan <oui | status>

oui — OUI テレフォニーリストの表示します。

status — グローバルおよびポートの Voice VLAN 設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status      : Disabled
Voice VLAN aging time  : 1440 minutes

Voice VLAN Port Summary
Port      Mode      Security Rule      Priority Remaining Age
                                   (minutes)
-----
Eth 1/ 1 Disabled Disabled OUI                6
Eth 1/ 2 Disabled Disabled OUI                6
Eth 1/ 3 Disabled Disabled OUI                5
Eth 1/ 4 Disabled Disabled OUI                6
Eth 1/ 5 Disabled Disabled OUI                6
Eth 1/ 6 Disabled Disabled OUI                6
Eth 1/ 7 Disabled Disabled OUI                6
Eth 1/ 8 Disabled Disabled OUI                6
Eth 1/ 9 Disabled Disabled OUI                6
Eth 1/10 Disabled Disabled OUI                6
.
.
.
Console#
Console#show voice vlan oui
OUI Address      Mask      Description
-----
00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#
```


4.19 Class Of Service

通信の過密によりパケットがスイッチにバッファされた場合、通信の優先権を持つデータパケットを明確にすることができます。本機は各ポートに4段階のプライオリティキューを持つ CoS をサポートします。

ポートの最高プライオリティキューの付いたデータパケットは、より低いプライオリティのキューのパケットよりも先に送信されます。各ポートに対しデフォルトプライオリティ、各キューの重みの関連、フレームプライオリティタグのマッピングをスイッチのキューに付けることができます。

コマンドグループ	機能	ページ
Priority (Layer 2)	タグなしフレームへのデフォルトプライオリティの設定、キューウエイトの設定、CoS タグのハードウェアキューへのマッピング	P747
Priority (Layer 3 and 4)	TCP ポート、IP DSCP タグの CoS 値への設定	P752

4.19.1 プライオリティコマンド (Layer 2)

コマンド	機能	モード	ページ
queue mode	キューモードを "strict" 又は "Weighted Round-Robin (WRR)" に設定	GC	P748
queue weight	Assigns round-robin weights to the priority queues	GC	
switchport priority default	入力タグなしフレームにポートプライオリティを設定	IC	P750
show interfaces switchport	インタフェースの管理、運用ステータスの表示	PE	P617
show queue mode	現在のキューモードを表示	PE	P751
show queue weight	重み付けされたキューに割り当てられたウェイトを表示	PE	P751

queue mode

キューモードの設定を行います。CoS のプライオリティキューを strict 又は Weighted Round-Robin (WRR) のどちらのモードで行うかを設定します。"no" を前に置くことで初期設定に戻します。

文法

queue mode < strict | wrr | strict-wrr [queue-type-list] >

no queue mode

- strict — 出力キューの高いプライオリティのキューが優先され、低いプライオリティのキューは高いプライオリティのキューがすべてなくなった後に送信されます。
- wrr — WRR はキュー 0-3 にそれぞれスケジューリングウエイト 1、2、4、6 を設定し、その値に応じて帯域を共有します。
- strict-wrr — Strict プライオリティは高プライオリティキューと残りのキューの SDWRR に使用されます。
- queue-type-list — キューがノーマルまたは Strict どちらのタイプであるかを示します。(オプション: 0 はノーマルキュー、1 は Strict キュー)

初期設定

Strict and WRR, with Queue 3 using strict mode

コマンドモード

Global Configuration

コマンド解説

- プライオリティモードを "strict" に設定した場合、出力キューの高いプライオリティのキューが優先され、低いプライオリティのキューは高いプライオリティのキューがすべてなくなった後に送信されます。
プライオリティモードを "wrr" に設定した場合、WRR はキュー 0-3 にそれぞれスケジューリングウエイト 1、2、4、6 を設定し、その値に応じて各キューの使用時間の割合を設定し帯域を共有します。これにより "strict" モード時に発生する HOL Blocking を回避することが可能となります。
- スイッチは Strict プライオリティ、SDWRR、Strict と Weighted の組合せをに基づいて、ポートキューにサービスを提供することが可能です。
- Strict プライオリティは、低プライオリティキューにサービスが提供される前に、高プライオリティキューの全てのトラフィックが処理されることを必要とします。

例

本例ではキューモードを Strict に設定しています。

```
Console(config)#queue mode strict
Console(config)#
```

関連するコマンド

queue weight (P749)

show queue mode (P751)

queue weight

加重されたキューイングを使用する時に、ウェイトを 4 つの Class of Service (CoS) プライオリティキューに割り当めます。"no" を前に置くことで設定を初期状態に戻します。

文法

queue weight [*weight0...weight3*]

no queue weight

- *weight0...weight3* — 0-3 キューのウェイトの比率は SWDRR スケジューラによって使用されるウェイトを決定します。(範囲：1-15)

初期設定

Weights 1, 2, 4, 6 はそれぞれキュー 0-3 に割り当てられます。

コマンドモード

Global Configuration

コマンド解説

- 帯域は、それぞれのラウンドについての毎秒バイトの正確な数を計算することによって、それぞれのキューに割り当てられます。

例

```
Console(config)#queue weight 1 2 3 4
Console(config)#
```

関連するコマンド

queue mode (P751)

show queue weight (P751)

switchport priority default

入力されるタグなしフレームに対してプライオリティを設定します。"no" を前に置くことで初期設定に戻します。

文法

switchport priority default *default-priority-id*

no switchport priority default

- *default-priority-id* — 入力されるタグなしフレームへのプライオリティ番号 (0-7、7 が最高のプライオリティ)

初期設定

プライオリティ未設定。タグなしフレームへの初期設定値は 0。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- プライオリティマッピングの優先順位は IP DSCP、デフォルトプライオリティの順番です。
- デフォルトプライオリティは、タグなしフレームを受信した際に設定されます。入力されたフレームが IEEE8021Q タグ付フレームの場合、IEEE802.1p のプライオリティ bit が使用されます。このプライオリティは IEEE802.1Q VLAN tagging フレームには適用されません。
- 本機では 4 段階のプライオリティキューを各ポートに提供します。それらは重み付けラウンドロビンを使用し、"show queue bandwidth" コマンドを使用し確認することが可能です。タグ VLAN ではない入力フレームは入力ポートでタグによりデフォルトプライオリティを付けられ、適切なプライオリティキューにより出力ポートに送られます。すべてのポートのデフォルトプライオリティは "0" に設定されています。したがって、初期設定ではプライオリティタグを持たないすべての入力フレームは出力ポートの "0" キューとなります (出力ポートがタグなしに設定されている場合、送信されるフレームは送信前にタグが取り外されます)

例

本例では 3 番ポートのデフォルトプライオリティを 5 に設定しています。

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

関連するコマンド

show interface switchport (P617)

show queue mode

現在のキューモードを表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show queue mode

Queue Mode : Weighted Round Robin Mode
Console#
```

show queue weight

キューの重み付けに使用されるウェイトを表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show queue weight

Queue ID  Weight
-----  -
          0          1
          1          2
          2          4
          3          6
Console#
```

4.19.2 プライオリティコマンド (Layer 3 and 4)

この項ではスイッチの、レイヤ 3、4 トラフィックマッピングの設定に使用するコマンドについて解説します。

コマンド	機能	モード	ページ
qos map cos-dscp	内部優先順位処理のため、入力パケットの CoS/CFI 値を per-hop behavior および drop precedence 値へマップ	IC	P753
qos map dscp-mutation	内部優先順位処理のため、入力パケットの DSCP 値を per-hop behavior および drop precedence 値へマップ	IC	P755
qos map phb-queue	内部 per-hop behavior 値をハードウェアキューへマップ	IC	P756
qos map trust-mode	QoS マッピングを DSCP または CoS へ設定	IC	P757
show qos map dscp-mutation	入力 DSCO から内部 DSCP へのマップを表示	PE	P758
show qos map phb-queue	ハードウェアキューマップへの内部 per-hop behavior を表示	PE	P758
show qos map cos-dscp	内部 DSCP マップへの入力 CoS を表示	PE	P760
show qos map trust-mode	QoS マッピングモードを表示	PE	P761

* マッピングプライオリティ値から内部 DSCP 値とハードウェアキューへのマッピングに使用される初期設定は大多数のネットワークアプリケーションのプライオリティサービスを最適化します。特定のアプリケーションでキューイングの問題が起こらない限り、初期設定の修正を行う必要はありません。

qos map cos-dscp

優先順位処理の為、入力パケットの CoS/CFI 値を per-hop behavior および drop precedence 値へマップします。"no" を前に置くことで初期設定に戻します。

文法

qos map cos-dscp *phb drop-precedence* from *cos0 cfi0...cos7 cfi7*

no qos map cos-dscp *cos0 cfi0...cos7 cfi7*

- *phb*— このルータホップで使用する Per-hop behavior またはプライオリティ (範囲：0-7)
- *drop-precedence* — トラフィック輻輳コントロールの Random Early Detection に使用される Drop precedence (範囲：0- 緑、3- 黄、1- 赤)
- *cos* — 入力パケットの CoS 値 (範囲：0-7)
- *cfi* — 標準フォーマット識別子 (Canonical Format Indicator)。このパラメータを "0" に設定することは、MAC アドレス情報は標準フォーマット内のフレームで運ばれることを示します。(範囲：0-1)

初期設定

内部 PHB/Drop Precedence への Cos/CFI のデフォルトマッピング

	CFI 0	1
Cos		
0	(0,0)	(0,0)
1	(1,0)	(1,0)
2	(2,0)	(2,0)
3	(3,0)	(3,0)
4	(4,0)	(4,0)
5	(5,0)	(5,0)
6	(6,0)	(6,0)
7	(7,0)	(7,0)

コマンドモード

Interface Configuration (Port, Static Aggregation)

コマンド解説

- P753 「内部 PHB/Drop Precedence への Cos/CFI のデフォルトマッピング」に表示される CoS から PHB 値への初期マッピングは、CoS 値の出力キューへのマッピングの IEEE 802.1p で推奨される設定を基にしています。
- 802.1Q ヘッダを付加されている IP パケット以外のパケットが到着した場合、CoS/CFI-to-PHB/Drop Precedence マッピングテーブルはプライオリティおよび内部処理の drop precedence 値を生成します。オリジナルパケットのプライオリティタグはこのコマンドでは編集されません。

コマンドラインインタフェース

Class Of Service

- 内部 DSCP はパケットが送られるキューを決定する per-hop behavior (PHB) の 3 ビットと、トラフィック輻輳をコントロールする Random Early Detection (RED) で使用される 2 ビットの drop precedence から成ります。
- バッファが 1-26 ポートで最大 16 パケット、25-26 ポートで最大 72 パケットが一杯になった時、RED は黄のドロップを開始します。また、バッファが 1-26 ポートで最大 58 パケット、25-26 ポートで最大 80 パケットが一杯になった時、色に関係なく全てのパケットをドロップします。
- 指定したマッピングは全てのインタフェースに適用されます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map cos-dscp 0 0 from 0 1
Console(config-if)#
```


qos map dscp-mutation

優先順位処理の為、入力パケットの DSCP 値を per-hop behavior および drop precedence 値にマップします。"no" を前に置くことで初期設定に戻します。

文法

qos map dscp-mutation *phb drop-precedence from dscp0 ... dscp7*

no qos map dscp-mutation *dscp0 ... dscp7*

- *phb*— このルータホップで使用する Per-hop behavior またはプライオリティ (範囲：0-7)
- *drop-precedence* — トラフィック輻輳コントロールの Random Early Detection に使用される Drop precedence (範囲：0- 緑、3- 黄、1- 赤)
- *dscp* — 入力パケットの DSCP 値 (範囲：0-63)

初期設定

内部 PHB/Drop Precedence への DSCP 値のデフォルトマッピング

ingress dscp1	0	1	2	3	4	5	6	7	8	9
ingress dscp10										
0	(0,0)	(0,1)	(0,0)	(0,3)	(0,0)	(0,1)	(0,0)	(0,3)	(1,0)	(1,1)
1	(1,0)	(1,3)	(1,0)	(1,1)	(1,0)	(1,3)	(2,0)	(2,1)	(2,0)	(2,3)
2	(2,0)	(2,1)	(2,0)	(2,3)	(3,0)	(3,1)	(3,0)	(3,3)	(3,0)	(3,1)
3	(3,0)	(3,3)	(4,0)	(4,1)	(4,0)	(4,3)	(4,0)	(4,1)	(4,0)	(4,3)
4	(5,0)	(5,1)	(5,0)	(5,3)	(5,0)	(5,1)	(6,0)	(5,3)	(6,0)	(6,1)
5	(6,0)	(6,3)	(6,0)	(6,1)	(6,0)	(6,3)	(7,0)	(7,1)	(7,0)	(7,3)
6	(7,0)	(7,1)	(7,0)	(7,3)						

* 入力 DSCP は ingress-dscp10 (左コラムの最も重要な列) と ingress-dscp1 (最も重要度の低い一番上の行) で構成されています。(ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1) 対応する内部 DSCP はテーブルの重なるセルに示されます。入力 DSCP はビットワイズが drop precedence を決定するために 2 進法の値 11 で AND をとられます。もし結果として乗じる値が 2 進の 10 であるなら、drop precedence は 0 にセットされます。

コマンドモード

Interface Configuration (Port, Static Aggregation)

コマンド解説

- このマップは "qos map trust-mode" コマンド (P757) で QoS マッピングモードが "DSCP" に設定されていて、入力パケットタイプが IPv4 の時のみ使用されます。
- バッファが最大 0x60 パケットが一杯になった時、Random Early Detection は黄と赤のドロップを開始します。また、バッファが 0x 80 パケットが一杯になった時、色に関係なく全てのパケットをドロップします。
- 指定したマッピングは全てのインタフェースに適用されます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map dscp-mutation 3 1 from 1
Console(config-if)#
```

qos map phb-queue

内部 per-hop behavior 値に基づいて使用されるハードウェアアウトプットキューを決定します。"no" を前に置くことで初期設定に戻します。

文法

qos map phb-queue *queue-id* from *phb0* ... *phb7*
no qos map phb-queue *phb0* ... *phb7*

- *phb* — このルータホップで使用される Per-hop behavior またはプライオリティ (範囲：0-7)
- *queue-id* — プライオリティキューの ID (範囲：0-7 7 が最高プライオリティキュー)

初期設定

内部 Per-hop Behavior からへのハードウェアキューへのマッピング

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	1	0	0	1	2	2	3	3

コマンドモード

Interface Configuration (Port, Static Aggregation)

コマンド解説

- キーワード "from" に続いてキュー識別子を、そして最大 8 つのスペースで分割された内部 per-hop behavior 値を入力してください。
- 出力パケットはこのコマンドで定義されたマッピングに従い、ハードウェアキューに置かれます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map phb-queue 0 from 1 2 3
Console(config-if)#
```

qos map trust-mode

QoS マッピングを DSCP または CoS にセットします。"no" を前に置くことで初期設定に戻します。

文法

qos map trust-mode < dscp | cos >
no qos map trust-mode

- dscp — QoS マッピングモードを DSCP に設定
- cos — QoS マッピングモードを CoS に設定

初期設定

DSCP

コマンドモード

Interface Configuration (Port, Static Aggregation)

コマンド解説

- このコマンドで QoS マッピングモードを DSCP に設定し、入力パケットが IPv4 である場合、プライオリティ処理は入力パケットの DSCP 値を基にします。
- QoS マッピングモードを DSCP に設定し、IP パケット以外を受信した際、パケットがタグ付きであるならパケットの CoS と CF 値 I（標準フォーマット識別子）がプライオリティ処理に使用されます。タグ無しパケットの場合、プライオリティ処理にはデフォルトポートプライオリティ（750 ページの「switchport priority default」を参照）が使用されます。
- このコマンドで QoS マッピングモードを CoS に設定し、入力パケットが IPv4 である場合、プライオリティ処理は入力パケットの CoS および CFI 値を基にします。タグ無しパケットの場合、プライオリティ処理にはデフォルトポートプライオリティ（750 ページの「switchport priority default」を参照）が使用されます。

例

```
Console(config)#int et 1/1
Console(config-if)#qos map trust-mode cos
Console(config-if)#
```

show qos map dscp-mutation

内部 DSCP マップへの入力 DSCP を表示します。

文法

show qos map dscp-mutation interface *interface*

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

コマンド解説

- このマップは、"qos map trust-mode" コマンド (P757) によって QoS マッピングモードが "DSCP" に設定されており、入力パケットタイプが IPv4 の時にのみ使用されます。

例

```
Console#show qos map dscp-mutation interface ethernet 1/5
dscp mutation map.(x,y),x: phb,y: drop precedence:
d1: d2 0      1      2      3      4      5      6      7      8      9
-----
0 :      (0,0) (0,1) (0,0) (0,3) (0,0) (0,1) (0,0) (0,3) (1,0) (1,1)
1 :      (1,0) (1,3) (1,0) (1,1) (1,0) (1,3) (2,0) (2,1) (2,0) (2,3)
2 :      (2,0) (2,1) (2,0) (2,3) (3,0) (3,1) (3,0) (3,3) (3,0) (3,1)
3 :      (3,0) (3,3) (4,0) (4,1) (4,0) (4,3) (4,0) (4,1) (4,0) (4,3)
4 :      (5,0) (5,1) (5,0) (5,3) (5,0) (5,1) (5,0) (5,3) (6,0) (6,1)
5 :      (6,0) (6,3) (6,0) (6,1) (6,0) (6,3) (7,0) (7,1) (7,0) (7,3)
6 :      (7,0) (7,1) (7,0) (7,3)
Console#
```

show qos map phb-queue

ハードウェアキューマップへの内部 per-hop behavior を表示します。

文法

show qos map phb-queue interface *interface*

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

例

```
Console#show qos map phb-queue interface ethernet 1/5
Information of Eth 1/5
phb-queue map:
phb:          0      1      2      3      4      5      6      7
-----
queue:        1      0      0      1      2      2      3      3
Console#
```

show qos map cos-dscp

内部 DSCP マップへの入力 CoS/CFI を表示します。

文法

show qos map cos-dscp interface *interface*

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

例

```
Console#show qos map cos-dscp interface ethernet 1/5
COS Information of Eth 1/5
cos-dscp map.(x,y),x: phb,y: drop precedence:
cos  : cfi  0          1
-----
0          (0,0)      (0,0)
1          (1,0)      (1,0)
2          (2,0)      (2,0)
3          (3,0)      (3,0)
4          (4,0)      (4,0)
5          (5,0)      (5,0)
6          (6,0)      (6,0)
7          (7,0)      (7,0)
Console#
```

show qos map trust-mode

QoS マッピングモードを表示します。

文法

show qos map trust-mode interface *interface*

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

例

```
Console#show qos map trust-mode interface ethernet 1/5
Information of Eth 1/5
  COS Map mode:          cos mode
Console#
```

4.20 Quality of Service

この章で記載されているコマンドは QoS(Quality of Service) 機能の基準とサービスポリシーを構成するために使用されます。DiffServ(Differentiated Services) 機能は、ネットワーク上を流れるフレームの 1 つの単位を特定のトラフィックの要件に合致させるため、ネットワークリソースを優先する管理機能を提供します。それぞれのパケットはアクセスリスト、IP Precedence、DSCP、VLAN リストをベースにしたネットワークの中のエントリによって分類されます。アクセスリストを使用することにより、それぞれのパケットが含んでいるレイヤ 2 ～ 4 の情報を元にトラフィックの選別を許可します。設定されたネットワークポリシーをベースにして、異なる種類のトラフィックに対し、異なる種類の転送のために印を付けることができます。

コマンド	機能	モード	ページ
class-map	クラスマップを作成	GC	P764
description	クラスマップの説明を指定	CM	P765
match	クラス分類のためトラフィックに使う条件を定義	CM	P766
rename	クラスマップの名前を再定義	CM	P767
policy-map	ポリシーマップを作成	GC	P768
description	クラスマップの記述を指定	PM	P765
class	ポリシー上で実行するクラスを設定	PM	P769
rename	クラスマップの名前を再定義	PM	P767
police flow	メータされたフローレートに基づいて、分類されたトラフィックのエンフォースを定義	PM-C	P770
police srctcm-color	Single rate three color meter に基づいて、分類されたトラフィックのエンフォースを定義	PM-C	P771
police trtcm-color	two rate three color meter に基づいて、分類されたトラフィックのエンフォースを定義	PM-C	P773
set cos	内部処理のためにマッチするパケットにたいして CoS 値で設定された IP トラフィックをサービス	PM-C	P775
set ip dscp	内部処理のためにマッチするパケットにたいして DSCP 値で設定された IP トラフィックをサービス	PM-C	P776
set phb	内部処理のためにマッチするパケットにたいして per-hop behavior 値で設定された IP トラフィックをサービス	PM-C	P777
service-policy	ポリシーマップをインターフェースに適用	IC	P778
show class-map	クラスマップの情報を表示	PE	P779
show policy-map	ポリシーマップの情報を表示	PE	P780
show policy-map interface	インターフェースに設定されたポリシーマップの情報を表示	PE	P781

指定された入力トラフィックのカテゴリのサービスポリシーを作成するには、以下の手順に従ってください。

- (1) "Class-map" コマンドを使用して、指定したトラフィックのカテゴリにクラス名を指定し、クラスマップ設定モードへ移行します。
- (2) "match" コマンドを使用し、アクセスリスト・DSCP・IP Precedence 値または VLAN をベースに、指定したトラフィックのタイプを選択します。
- (3) ACL を "match" コマンドで指定された基準のフィルタリングを有効にするように設定します。
- (4) "Policy-map" コマンドを使用して、入力トラフィックが処理される指定したマナーのポリシー名を指名し、ポリシーマップ設定モードへ移行します。
- (5) "class" コマンドを使用し、クラスマップを識別してポリシーマップクラス設定モードへ移行します。ポリシーマップは複数のクラスステートメントを含むことが出来ます。
- (6) "set phb" または "set cos" を使用し、マッチするトラフィッククラスの per-hop behavior または CoS の編集を行います。また、"police" コマンドのいずれかを使用し、平均フローおよびバーストレートのようなパラメータをモニタし、指定したレートを超えたトラフィックをドロップするか、指定したレートを超えたトラフィックの DSCP サービス値を減少します。
- (7) "service-policy" コマンドを使用して、ポリシーマップを指定のインタフェースへ割り当てます。

[注意] ポリシーマップ(P768)を作成する前に、クラスマップ (P764)を作成してください。

class-map

このコマンドはクラスマップを作成し、クラスマップコンフィグレーションモードに移行します。no を付けるとクラスマップを削除し、グローバルコンフィグレーションモードに戻ります。

文法

class-map *class-map-name* { match-any }

no class-map *class-map-name*

- match-any — クラスマップの条件のうちいずれか 1 つに一致するトラフィックを対象
- *class-map-name* — クラスマップ名 (1-16 文字)

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 最初にこのコマンドを実行してクラスマップを作成し、クラスマップコンフィグレーションモードに入ります。次に入力トラフィックの分類条件を match コマンドで指定します。
- 1 つ以上のクラスマップをポリシーマップ (P768) に割り当てることが可能です。ポリシーマップはそれから、サービスポリシーによってインタフェースにバウンドされます (P778)。サービスポリシーはパケット分類、サービスタギング、帯域ポリッシングを定義します。ポリシーマップがインタフェースにバウンドされると、追加クラスマップはポリシーマップに加えられず、"match" または "set" コマンドで割り当てられたクラスマップに変更は行われません。

例

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

関連するコマンド

show class map (P779)

description

クラスマップまたはポリシーマップの説明を入力します。

文法

description *string*

string — クラスマップまたはポリシーマップの説明（範囲：1-64 文字）

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description matches packets marked for DSCP service
value 3
Console(config-cmap)#
```

match

このコマンドはトラフィックを分類するために使用する条件を設定します。
no を付けると基準を削除します。

文法

match { access-list *acl-name* | ip dscp *dscp* | ip precedence *ip-precedence* | vlan *vlan* }

no match access-list *acl-name*

- *acl-name* — アクセスコントロールリスト名 (1-16 文字)
- *dscp* — DSCP 値 (範囲: 0-63)
- *ip-precedence* — IP Precedence 値 (範囲: 0-7)
- *vlan* — VLAN (範囲: 1-4093)

初期設定

なし

コマンドモード

Class Map Configuration

コマンド解説

- 最初に class-map コマンドを実行してクラスマップを作成し、クラスマップコンフィグレーションモードに入ります。次にこのクラスマップ上で合致させたい入力パケット中の値を match コマンドで指定します。
- 入力パケットが、このコマンドで指定された ACL にマッチした場合、ACL に含まれる拒否ルールは無視されます。
- マッチ基準が IP ACL または IP プライオリティルールを含む場合、VLAN ルールは同じクラスマップに含まれることが出来ません。
- マッチ基準が MAC ACL または VLAN ルールを含む場合、IP ACL と IP プライオリティルールのいずれも同じクラスマップに含まれることが出来ません。
- 最大 16 マッチエントリがクラスマップに含まれることが可能です。

例

```
Console(config)#class-map rd_class#1_ match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

rename

クラスマップまたはポリシーマップの名前を再定義します。

文法

rename *map-name*

map-name — クラスマップまたはポリシーマップの名前（範囲：1-16 文字）

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

policy-map

このコマンドはポリシーマップを作成し、ポリシーマップコンフィグレーションモードに入ります。no を付けるとポリシーマップは削除され、グローバルコンフィグレーションモードに戻ります。

文法

policy-map *policy-map-name*

no policy-map *policy-map-name*

- *policy-map-name* — ポリシーマップ名 (1-16 文字)

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- ポリシーマップの名前を設定するために policy-map コマンドを使用します。次にクラスマップで指定された条件に合致するトラフィックにポリシーを設定するため、class コマンドを使用します。
- ポリシーマップは複数の、" service-policy" コマンドで同じインタフェースに適用されるクラスステートメントを含むことができます。
- ポリシーマップを作成する前にクラスマップを作成する必要があります。

例

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 0
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

class

このコマンドはポリシーマップが実行するクラスマップを指定し、ポリシーマップ・クラスコンフィグレーションモードに入ります。no を付けるとクラスマップを削除し、ポリシーマップコンフィグレーションモードに戻ります。

文法

class *class-map-name*

no class *class-map-name*

- *class-map-name* — クラスマップ名 (1-16 文字)

初期設定

なし

コマンドモード

Policy Map Configuration

コマンド解説

- ポリシーマップの設定を行うために policy-map コマンドを使用し、ポリシーマップコンフィグレーションモードに入ります。次にポリシーマップ・クラスコンフィグレーションモードに入るために class コマンドを使用します。そして最後に、set コマンドと police コマンドを使用して設定を行います。
 - set phb — マッチするパケットに per-hop behavior 値を設定
(内部処理のためのみパケットプライオリティを修正)
 - set cos — マッチするパケットに CoS 値を設定
(VLAN タグのパケットプライオリティを修正)
 - police — コマンドは最大スループット、バーストレート等、規則に従わないトラフィックに対する対応を定義します。
- 1 つのクラスマップあたり最大 16 個のルールを設定できます。また、ポリシーマップには複数のクラスを所属させることができます。

例

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

police flow

metered flow rate を基に、分類されたトラフィックのエンフォーサを定義します。"no" を前に置くことでポリサを削除します。

文法

[no] **police flow** *committed-rate committed-burst* conform-action transmit
violate-action { drop | *new-dscp* }

- *committed-rate* — レートを指定。(範囲：64kbps の精度または最大ポートスピードで 64-10000000 kbps) レートは設定されたインタフェーススピードを越えられません。
- *committed-burst* — バーストサイズを指定。(範囲：4k バイトの精度で 4000-16000000) バーストサイズは 16Mbytes を越えられません。
- conform-action — パケットが CIR と BC 内である時のアクション。
- violate-action — パケットが CIR と BC を超えた時のアクション。
- transmit — アクションをせずに送信。
- drop — 違反アクションによってパケットをドロップします。
- *new-dscp* — DSCP 値を定義 (範囲：0-63)

初期設定

なし

コマンドモード

Policy Map Configuration

コマンド解説

- 入力ポートに最大 16 のポリサ (クラスマップ) を設定できます。
- *committed-rate* はインタフェーススピードを越えることはできず、*committed-burst* は 16 Mbytes を越えることができません。
- ポリシングはトークンバケツを基にし、バケツの深さ (最大バーストになる前のオーバーフロー) は *committed-burst* フィールドで指定され、バケツに加えられるトークンの平均レートは *committed-rate* オプションで指定されます。
- メータのふるまいは、1 つのバケツ (C)、トークンが増加するレート (CIR — Committed Information Rate)、トークンバケツの最大サイズ (BC — Committed Burst サイズ) に関して算定されます。トークンバケツ C は初期状態で満杯で、トークンカウントは $Tc(0) = BC$ になります。その後は以下のように毎秒 CIR 回ずつ更新されます。
 - Tc が BC より小さければひとつだけ増加される。
 - Tc は増加しない。

時刻 t に B バイトのパケットが到着したら、以下のように動作します。

- $Tc(t) - B \leq 0$ の場合、パケットは緑に色づけされ、 Tc が B だけ減少する。 $(Tc$ の最低値は 0)
- パケットは赤色にされ、 Tc も Te も減少しない

例

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 100000 4000 conform-action
transmit
    violate-action drop
Console(config-pmap-c)#
```

police srtcm-color

single rate three color meter (srTCM) を基に、分類されたトラフィックのエンフォーサを定義します。"no" を前に置くことでポリサを削除します。

文法

[no] police {srtcm-color-blind | srtcm-color-aware} committed-rate committed-burst
excess-burst conform-action transmit exceed-action {drop | new-dscp}
violate action {drop | new-dscp}

- **srtcm-color-blind** — カラーバインドモードの Single rate three color meter
- **srtcm-color-aware** — カラーアウェアモードの Single rate three color meter
- *committed-rate* — コミットされた information rate (CIR)
- *committed-burst* — バーストサイズを指定。
(範囲：4k バイトの精度で 4000-16000000)
- *excess-burst* — 超過バーストサイズ (範囲：4k バイトの精度で 4000-16000000)
- conform-action — パケットが CIR と BC 内である時のアクション
- exceed-action — レートが CIR および BC を超過したけれど、BE 内である時のアクション
- violate action — パケットが BE を超過した時のアクション
- transmit — アクションをせずに送信
- drop — 違反アクションによってパケットをドロップします。
- *new-dscp* — DSCP 値を定義 (範囲：0-63)

初期設定

なし

コマンドモード

Policy Map Class Configuration

コマンド解説

- 入力ポートに最大 16 のポリサ（クラスマップ）を設定できます。
- committed-rate はインタフェーススピードを越えることはできず、committed-burst は 16 Mbytes を越えることができません。
- SrTCM は RFC2697 で定義されるように、トラフィックストリームを測り、3 つのトラフィックパラメータに従ってパケットを処理します。— Committed Information Rate (CIR), Committed Burst Size (BC), and Excess Burst Size (BE)
- PHB ラベルは、3 ビットの per-hop behavior、2 ビットのキュー輻輳のコントロールに使用されるカラスキームの 5 ビットで構成されます。CIR と BC を超過しない場合、パケットは緑にマークされ、CIR と BC を超過し、BE はしていない場合は黄にマークされ、その他は赤となります。
- メータは次の二つのモードのうちどちらかで動作します。
カラーバインドモードではパケットにマーキング（色付け）がされていないとみなし、カラーアウェアモードではあらかじめ何らかの前段の存在がパケットにマーキング（色付け）をしているとみなします。（パケットは既に緑・黄色・赤のいずれか）。
IP パケットの色付けはメータの結果に従ってします。色はパケットの DS フィールド (RFC2474) でコード化されます。
- メータのふるまいは、モードの基準と、共通のレートサークルを共有する C と E のふたつのトークンバケツで指定されます。C の最大値は BC、E の最大値は BE です。C と E は時刻 0 では満杯です ($T_c(0) = BC$ 、 $T_e(0) = BE$)。その後は以下のように毎秒 CIR 回ずつ更新されます。
 - T_c が BC より小さければひとつだけ増加される。
 - T_e が BE より小さければひとつだけ増加される。
 - T_c も T_e も増やされない。

時刻 t に B バイトのパケットが到着したら、srTCM がカラーバインドモードで機能している時、以下のように動作します

- $T_c(t) - B \leq 0$ の時、パケットは緑になり T_c は 0 の最小値まで B 減少する。
- $T_e(t) - B \leq 0$ の時、パケットは黄になり、 T_c は 0 の最小値まで B 減少する。
- その他はパケットは赤になり、 T_c も T_e も減少しない。

時刻 t に B バイトのパケットが到着したら、srTCM がカラーアウェアモードで機能している時、以下のように動作します

- パケットが前もって緑に塗られ、 $T_c(t) - B \leq 0$ の時、パケットは緑になり、 T_c は 0 の最小値まで B 減少する。
- パケットが前もって黄に塗られ、 $T_e(t) - B \leq 0$ の時、パケットは黄になり、 T_e は 0 の最小値まで B 減少する。
- その他はパケットは赤になり、 T_c も T_e も減少しない。

例

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police srtcm-color-blind 100000 4000 6000
conform-action
transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

police trtcm-color

two rate three color meter (trTCM) を基に、分類されたトラフィックのエンフォーサを定義します。"no" を前に置くことでポリサを削除します。

文法

[no] police {trtcm-color-blind | trtcm-color-aware} committed-rate committed-burst peak-rate peak-burst conform-action transmit exceed-action {drop | new-dscp}

violate action {drop | new-dscp}

- **trtcm-color-blind** — カラーバインドモードの Two rate three color meter
- **trtcm-color-aware** — カラーアウェアモードの Two rate three color meter
- *committed-rate* — レートを指定。(範囲：64kbps の精度または最大ポートスピードで 64-10000000 kbps) レートは設定されたインタフェーススピードを越えられません。
- *committed-burst* — バーストサイズを指定。(範囲：4k バイトの精度で 4000-16000000) バーストサイズは 16Mbytes を越えられません。
- *peak-rate* (PIR) — レートを指定 (範囲：64kbps の精度または最大ポートスピードで 64-10000000)
- *peak-burst* — バーストサイズを指定 (範囲：4kbps の精度で 4000-16000000) バーストサイズは 16Mbytes を越えられません。
- *conform-action* — パケットが CIR と BP 内である時のアクション
- *violate action* — パケットが CIR と BC を超えた時のアクション
- *drop* — 違反アクションによってパケットをドロップします。
- *transmit* — アクションをせずに送信。
- *new-dscp* — DSCP 値を定義 (範囲：0-63)

初期設定

なし

コマンドモード

Policy Map Class Configuration

コマンド解説

- 入力ポートに最大 16 のポリサ（クラスマップ）を設定できます。
- committed-rate はインタフェーススピードを越えることはできず、committed-burst は 16 Mbytes を越えることができません。
- SrTCM は RFC2698 で定義されるように、トラフィックストリームを測り、2 つのトラフィックレートに従ってパケットを処理します。－ Committed Information Rate (CIR), Peak Information Rate (PIR) またはそれらが関連するバーストサイズ (BC)、ピークバーストサイズ (BP)
- PHB ラベルは、3 ビットの per-hop behavior、2 ビットのキュー輻輳のコントロールに使用されるカラースキームの 5 ビットで構成されます。RIP を超過した場合パケットは赤になり、CIR を超過するかしないかで黄または緑のいずれかになります。TrTCM はサービスの入力ポリッシングに役立ちます。ピークレートはコミットされたレートから区別されて実施する必要があります。
- トークンバケツ P と C は初期状態で満杯で、トークンカウントは $Tp(0) = BP$ 、 $Tc(0) = BC$ になります。その後は以下のように毎秒 CIR 回ずつ更新されます。

時刻 t に B バイトのパケットが到着したら、trTCM がカラーバインドモードで機能している時、以下のように動作します

- $Tp(t)-B < 0$ の時、パケットは赤になる。
- $Tc(t)-B < 0$ のとき、パケットは黄になり、TP は B 減少する。
- パケットは緑になり、 Tp と Tc の両方共が B 減少する。

時刻 t に B バイトのパケットが到着したら、trTCM がカラーアウェアモードで機能している時、以下のように動作します：

- パケットが前もって赤に塗られるか、 $Tp(t)-B < 0$ の時、パケットは赤になる。
- パケットが前もって黄に塗られるか、 $Tc(t)-B < 0$ の時、パケットは黄になり、 Tp は B 現象する。
- パケットが緑で、 Tp と Tc が B 減少する。

例

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police trtcm-color-blind 100000 4000 100000 6000
    conform-action transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

set cos

パケットの VLAN タグで、マッチするパケット ("match" コマンドで指定された) の CoS 値の変更を行います。"no" を前に置くことで設定を削除します。

文法

set cos *cos-value*

no set cos *cos-value*

- *cos-value* — CoS の値 (0-7)

初期設定

なし

コマンドモード

Policy Map Class Configuration

コマンド解説

- "set cos" コマンドはマッチするパケットの VLAN タグ内の CoS 値の設定に使用されます。
- "set cos" および "set php" コマンドはプライオリティの同じレベルで機能します。そのため、これらのコマンドのいずれかの設定は、他のコマンドによってすでに設定されているアクションを上書きします。

例

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

set ip dscp

パケットの VLAN タグで、マッチするパケット ("match" コマンドで指定された) の DSCP 値の変更を行います。"no" を前に置くことで設定を削除します。

文法

set dscp *dscp-value*

no set dscp *dscp-value*

- *dscp-value* — DSCP の値 (0-63)

初期設定

なし

コマンドモード

Policy Map Class Configuration

例

```
ES-3026(config)#policy-map rd-policy
ES-3026(config-pmap)#class rd-class
ES-3026(config-pmap-c)#set ip dscp 3
ES-3026(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
ES-3026(config-pmap-c)#
```

set php

内部処理で、マッチするパケット ("match" コマンドによって指定された) の per-hop behavior 値を設定することによって、IP トラフィックをサービスします。"no" を前に置くことでこの設定を削除します。

文法

set phb *phb-value*

no set phb *phb-value*

- *phb-value* — PHB の値 (0-7)

初期設定

なし

コマンドモード

Policy Map Class Configuration

コマンド解説

- "set cos" および "set php" コマンドはプライオリティの同じレベルで機能します。そのため、これらのコマンドのいずれかの設定は、他のコマンドによってすでに設定されているアクションを上書きします。
- "set phb" コマンドはマッチするパケット (P755 「内部 PHB/Drop Precedence への DSCP 値のデフォルトマッピング」を参照) のハードウェアの内部 QoS 値を設定するために使用します。QoS ラベルは 3 ビットの per-hop behavior、2 ビットのキュー輻輳のコントロールを行うカラースキームの 5 ビットから構成されます。

例

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

service-policy

"policy-map" コマンドで定義されたポリシーマップを特定のインタフェースの入力サイドに適用します。"no" を前に置くことでこのマッピングを削除します。

文法

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

- input — 入力トラフィックにインタフェースを適用
- *policy-map-name* — ポリシーマップ名 (1-32 文字)

初期設定

インタフェースにポリシーマップは未適用

コマンドモード

Interface Configuration (Ethernet、Port Channel)

コマンド解説

- インターフェースには 1 つのポリシーマップのみ割り当てることができます。
- 最初にクラスマップを定義し、次にポリシーマップを設定し、最後に service-policy コマンドを使用して必要なインターフェースにポリシーマップを関連付けてください。
- 本機では、ポリシーマップを出力トラフィックのインタフェースにバウンドすることは出来ません。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd_policy
Console(config-if)#
```


show class-map

このコマンドは match コマンドで設定した QoS のクラスマップを表示します。

文法

show class-map { *class-map-name* }

- *class-map-name* — クラスマップ名 (1-32 文字)

初期設定

全てのクラスマップを表示

コマンドモード

Privileged Exec

例

```
Console#show class-map
Class Map match-any rd-class#1
Description:
  Match ip dscp 10
  Match access-list rd-access
  Match ip dscp 0

Class Map match-any rd-class#2
  Match ip precedence 5

Class Map match-any rd-class#3
  Match vlan 1

Console#
```

show policy-map

このコマンドは QoS のポリシーマップを表示します。

文法

show policy-map { *policy-map-name* class *class-map-name* }

- *policy-map-name* — ポリシーマップ名 (1-16 文字)
- *class-map-name* — クラスマップ名 (1-16 文字)

初期設定

全てのポリシーマップおよびクラスマップを表示

コマンドモード

Privileged Exec

例

```
Console#show policy-map
Policy Map rd_policy
Description:
  class rd-class
  set phb 3
Console#show policy-map rd-policy class rd-class
Policy Map rd-policy
  class rd-class
  set phb 3
Console#
```

show policy-map interface

このコマンドはインターフェースに割り当てられたサービスポリシーを表示します。.

文法

show policy-map interface *interface* input

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

例

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#
```

4.21 マルチキャストフィルタリング

IGMP (Internet Group Management Protocol) を使用し、特定のマルチキャストサービスを受けたいホストに対してクエリを実行します。リクエストしているホストが所属するポートを特定し、それらのポートにのみデータを送ります。マルチキャストサービスを受け取り続けるために、隣接するマルチキャストスイッチ / ルータにサービスリクエストを伝搬します。

コマンドグループ	機能	ページ
IGMP Snooping	IGMP snooping 又は静的設定によるマルチキャストグループの設定。IGMP バージョンの設定、設定状態、マルチキャストサービスグループやメンバーの表示	P782
Static Multicast Routing	静的マルチキャストルータポートの設定	P806
IGMP Filtering and Throttling	IGMP フィルタリングおよびスロットリングの設定	P808
Multicast VLAN Registration	MVR の設定	P819

4.21.1 IGMP Snooping コマンド

コマンド	機能	モード	ページ
ip igmp snooping	IGMP snooping の有効化	GC	P784
ip igmp snooping proxy-reporting	プロキシレポーティングで IGMP スヌーピングを有効化	GC	P785
ip igmp snooping querier	この装置を IGMP スヌーピングのクエリアにします。	GC	P786
ip igmp snooping router-alert-option-check	ルータアラートオプションを含まない IGMPv2/v3 パケットを破棄	GC	P787
ip igmp snooping router-port- expire-time	クエリアタイムアウトを設定	GC	P788
ip igmp snooping tcn-flood	スパニングツリートポロジに変更があった時、マルチキャストトラフィックをフラッド	GC	P789
ip igmp snooping tcn-query-solicit	スパニングツリートポロジに変更があった時、IGMP クエリア要請を送信	GC	P790
ip igmp snooping unregistered-data-flood	未登録のマルチキャストトラフィックを付属する VLAN にフラッド	GC	P791
ip igmp snooping unsolicited-report-interval	アップストリームインタフェースが非要請 IGMP レポートを送信する間隔を指定（プロキシレポーティングが有効時）	GC	P792
ip igmp snooping version	スヌーピングの IGMP バージョンを設定	GC	P793

ip igmp snooping version-exclusive	現在の設定と異なるバージョンを使用する受信された IGMP メッセージを破棄	GC	P794
ip igmp snooping vlan general-query-suppression	ダウンストリームマルチキャストホストに属するポート以外の通常クエリを抑制	GC	P795
ip igmp snooping vlan immediate-leave	ポートで Leave パケットが受信され、親 VLAN で immediate-leave が有効の場合、マルチキャストサービスのメンバーポートを直ちに削除	GC	P796
ip igmp snooping vlan last-memb-query-count	システムがローカルなメンバーがいないと想定する前に送られる IGMP プロキシクエリメッセージの数を設定	GC	P797
ip igmp snooping vlan last-memb-query-intvl	last-member-query 間隔を設定	GC	P798
ip igmp snooping vlan mrd	マルチキャストルータ要請メッセージを送信	GC	P799
ip igmp snooping vlan proxy-address	プロキシ IGMP クエリとレポートの静的アドレスを設定	GC	P800
ip igmp snooping vlan proxy-query-interval	IGMP プロキシ通常クエリの送信間隔を設定	GC	P801
ip igmp snooping vlan proxy-query-resp-intvl	システムがプロキシ通常クエリの返答を待つ最大時間を設定	GC	P802
ip igmp snooping vlan proxy-reporting	プロキシレポートの IGMP スヌーピングを有効化	GC	P785
ip igmp snooping vlan static	インタフェースをマルチキャストグループのメンバーとして追加	GC	P803
ip igmp snooping vlan version	スヌーピングの IGMP バージョンを設定	GC	P793
ip igmp snooping vlan version-exclusive	現在の設定と異なるバージョンを使用する受信された IGMP メッセージを破棄	GC	P794
show ip igmp snooping	IGMP スヌーピング、プロキシ、クエリ設定を表示	PE	P804
show ip igmp snooping group	既知のマルチキャストグループ、ソース、ホストポートマッピングを表示	PE	P805

ip igmp snooping

IGMP snooping を有効にします。"no" を前に置くことで機能を無効にします。

文法

ip igmp snooping { vlan *vlan-id* }

no ip igmp snooping

- *vlan-id* — VLAN ID (範囲：1-4093)

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- IGMP スヌーピングがグローバルで有効時、IGMP スヌーピングの VLAN インタフェース毎の設定が優先されます。
- IGMP スヌーピングがグローバルで無効時、スヌーピングは依然 VLAN インタフェース毎の設定を行えますが、インタフェース設定はスヌーピングがグローバルで再度有効化されるまで効果は発しません。

例

本例では IGMP snooping を有効にしています。

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping proxy-reporting

プロキシレポーティングの IGMP スヌーピングを有効にします。"no" を前に置くことで初期設定に戻します。

文法

[no] ip igmp snooping proxy-reporting

ip igmp snooping vlan *vlan-id* proxy-reporting < enable | disable >

no ip igmp snooping vlan *vlan-id* proxy-reporting

- *vlan-id* — VLAN ID（範囲：1-4093）
- enable — 指定した VLAN で有効
- disable — 指定した VLAN で無効

初期設定

グローバル：有効

VLAN：グローバル設定に準じる

コマンドモード

Global Configuration

コマンド解説

- プロキシレポーティングがこのコマンドで有効時、スイッチは last leave、query suppression を含む "IGMP Snooping with Proxy Reporting"（DSL Forum TR-101, April 2006 で定義）を実行します。
- IGMP プロキシレポーティングが VLAN で設定されている場合、この設定はグローバル設定よりも優先されます。

例

```
Console(config)#ip igmp snooping proxy-reporting
Console(config)#
```

ip igmp snooping querier

スイッチを IGMP クエリアとして有効にします。"no" を前に置くことで無効にします。

文法

ip igmp snooping querier
no ip igmp snooping querier

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- IGMPv3 スヌーピング（793 ページの「ip igmp snooping version」を参照）では IGMP スヌーピングクエリアはサポートされていません。
- 有効にした場合、選出されるとスイッチはクエリアとして動作します。クエリアはホストにマルチキャストトラフィックの受信の要求を尋ねる責任を持ちます。

例

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping router-alert-option-check

ルータアラートオプションに含まない IGMPv2/v3 パケットを破棄します。
"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping router-alert-option-check
no ip igmp snooping router-alert-option-check

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- ルータアラートオプションは DOS 攻撃から保護するために仕様できます。攻撃の 1 つの方法は、クエリアの役割を引き継ぐ侵入者によって始動され、多数の group-and-source-specific クエリアを送りマルチキャストホストへ加重負荷をかけることを開始し、それぞれの大きなソースリストと最大返答時間を大きな値に設定します。この種類の攻撃から保護するため、(1) ルータは質問を転送しない。クエリがルータアラートオプションを伴う場合、これは容易です。(2) また、スイッチがマルチキャストとして行動している時（プロキシルーティング使用時のように）ルータアラートオプションに含まないバージョン 2 または 3 クエリアを無視します。

例

```
Console(config)#ip igmp snooping router-alert-option-check
Console(config)#
```

ip igmp snooping router-port- expire-time

クエリアタイムアウトを設定します。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

- *seconds* — 期限が切れたことを考慮する前に、前のクエリアが停止停止した後にスイッチが待つ時間（範囲：1-65535 推奨範囲：300-500）

初期設定

300 秒

コマンドモード

Global Configuration

例

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

ip igmp snooping tcn-flood

スパニングツリートポロジ変更通知 (TCN) が発生した時、マルチキャストトラフィックのフラッディングを有効にします。"no" を前に置くことでフラッディングを無効にします。

文法

ip igmp snooping tcn-flood
no ip igmp snooping tcn-flood

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- ・ スパニングツリートポロジチェンジ発生時、スイッチによって学習されているマルチキャストメンバーシップ情報は古くなります。例えば、トポロジチェンジ (TC) 前に 1 つのポートへリンクされているホストが他のポートへ移動した時などです。初期設定では、トポロジが安定し、全てのマルチキャストレシーバの新しい場所が学習されるまで、ブリッジプロトコルデータ (BPDU) と TC ビットセット (ルートブリッジによって) を受け取る VLAN のスイッチ (IGMP が有効になっている) は "multicast flooding mode" に入ります。
- ・ トポロジ変更通知 (TCN) が受け取られると、全てのアップリンクポートが続いて削除され、タイムアウトメカニズムは現在学習されている全てのマルチキャストチャンネルの削除に使用されます。
- ・ 新しいアップリンクポートがスタートアップした時、スイッチは全ての現在学習されている、新しいアップリンクポートを通して外へ出るチャンネルの非要請レポートを送信します。
- ・ 初期設定ではスパニングツリートポロジ変更が発生時、スイッチは直ちに "multicast flooding mode" へ入ります。このモードでは、マルチキャストトラフィックは全ての VLAN ポートへフラッドされます。もし多くのポートが異なるマルチキャストグループを予約している場合、フラッディングはスイッチとエンドホスト間のリンク上で過度のローディングを起こす可能性があります。
- ・ スパニングツリートポロジが変更された時、ルートブリッジはマルチキャストチャンネルに関連するホストメンバーシップとポートを早急に再学習するために、プロキシクエリを送信します。ルートブリッジはまた、この VLAN のマルチキャストルータの位置を定める為、早急に非要請 Multicast Router Discover (MRD) リクエストを送信します。プロキシクエリと非要請 MRD リクエストはスイッチがそのようなパケットを受け取った時に、受信ポートを除く全ての VLAN ポートにフラッドされます。

例

```
Console(config)#ip igmp snooping tcn-flood  
Console(config)#
```

ip igmp snooping tcn-query-solicit

スパニングツリーポロジ変更通知（TCN）が起きる時に、スイッチが IGMP 通常クエリ要請を送信します。

"no" を前に置くことでこの機能を無効にします。

文法

ip igmp snooping tcn-query-solicit
no ip igmp snooping tcn-query-solicit

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- スパニングツリーのルートブリッジが IGMP スヌーピングが有効になっている VLAN のトポロジ変更通知を受信した時、グローバルの IGMP leave message を発行します（クエリ要請）。スイッチがこの要請を受信した時、それはスパニングツリー変更が発生した VLAN の全てのポートにフラッドされます。アップストリームマルチキャストルータがこの要請を受信した時、それはまた直ちに IGMP 通常クエリを発行します。
- この "ip igmp snooping tcn query-solicit" コマンドは、たとえスパニングツリーがルートブリッジでないとしても、トポロジチェンジに気がついた時いつでもクエリ要請を送信するために使用されます。

例

```
Console(config)#ip igmp snooping tcn-query-solicit  
Console(config)#
```

ip igmp snooping unregistered-data-flood

登録されていないマルチキャストトラフィックを付属する VLAN へフラッドします。"no" を前に置くことで登録されていないマルチキャストトラフィックを破棄します。

文法

ip igmp snooping unregistered-data-flood
no ip igmp snooping unregistered-data-flood

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- IGMP スヌーピングとマルチキャストルーティングのマルチキャストエントリ保存に使用されるテーブルが一杯になると、新しいエントリは学習されません。付属する VLAN にルータポートが設定されておらず、未登録のフラッディングが無効の場合、テーブルで見つからない次のマルチキャストトラフィックはドロップされます。

例

```
Console(config)#ip igmp snooping unregistered-data-flood
Console(config)#
```

ip igmp snooping unsolicited-report-interval

プロキシレポーティング有効時、アップストリームインタフェースが unsolicited IGMP レポートを送信する間隔を指定します。"no" を前に置くことで初期設定に戻します。

文法

ip ip igmp snooping unsolicited-report-interval *seconds*
no ip igmp snooping unsolicited-report-interval

- *seconds* — unsolicited レポートを発行する間隔（範囲：1-65535 秒）

初期設定

400 秒

コマンドモード

Global Configuration

コマンド解説

- 新しいアップストリームインタフェース（アップリンクポート）の開始時、スイッチは現在学習されている新しいアップストリームインタフェースを通して出る、全てのマルチキャストチャンネルへ非要請レポートを送信します。
- このコマンドはプロキシレポーティング（P785）が有効時のみ適用されます。

例

```
Console(config)#ip igmp snooping unsolicited-report-interval 5
Console(config)#
```

ip igmp snooping version

IGMP スヌーピングバージョンを設定します。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping [vlan *vlan-id*] version <1 | 2 | 3 >
no ip igmp snooping version

- *vlan-id* — VLAN ID（範囲：1-4093）
- 1 — IGMP Version 1
- 2 — IGMP Version 2
- 3 — IGMP Version 3

初期設定

グローバル；IGMP バージョン 2

VLAN：未設定、グローバル設定に準じる

コマンドモード

Global Configuration

コマンド解説

- IGMP スヌーピングで使用される、IGMP レポート / クエリバージョンを設定します。バージョン 1-3 は全てサポートされ、バージョン 2 と 3 は下位互換性があるので、スイッチは使用されているスヌーピングバージョンに関係なく、他のデバイスと稼動することが可能です。
- VLAN で IGMP スヌーピングバージョンが設定されている場合、設定はグローバルコンフィグレーション設定に優先されます。

例

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping version-exclusive

受信された、"ip igmp snooping version" で設定された現在のバージョンと異なるバージョンを使用する IGMP メッセージ（マルチキャストプロトコルパケットを除く）を削除します。
"no" を前に置くことでこの機能を無効にします。

文法

ip igmp snooping [vlan *vlan-id*] version-exclusive
no ip igmp snooping version-exclusive

- *vlan-id* — VLAN ID（範囲：1-4093）

初期設定

グローバル：無効

VLAN：無効

コマンドモード

Global Configuration

コマンド解説

- もし version-exclusive が VLAN で無効の場合、この設定はグローバル設定を基にします。VLAN で有効の場合、この設定はグローバル設定に優先されます。
- この機能の無効の場合、現在選択されているバージョンは下位互換性があります。("igmp snooping version" コマンド（P793）を参照）

例

```
Console(config)#ip igmp snooping version-exclusive
Console(config)#
```


ip igmp snooping vlan general-query-suppression

ダウンストリームマルチキャストホストに付属するポート以外の通常クエリを押さえます。
"no" を前に置くことで、通常クエリをマルチキャストルータポートを除く全てのポートへフラッドします。

文法

[no] ip igmp snooping vlan *vlan-id* general-query-suppression

- *vlan-id* — VLAN ID（範囲：1-4093）

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 初期設定では、通常クエリメッセージは受信されるマルチキャストルータを除く全てのポートへフラッドされます。
- 通常クエリサプレッションが有効の場合、メッセージはマルチキャストサービスに加わっているダウンストリームポートへのみ転送されます。

例

```
Console(config)#ip igmp snooping vlan 1 general-query-suppression
Console(config)#
```

ip igmp snooping vlan immediate-leave

ポートで leave packet が受信され、immediate-leave が親 VLAN で有効になっている時、マルチキャストサービスのメンバーポートをただちに削除します。"no" を前に置くことで初期設定に戻します。

文法

[no] ip igmp snooping vlan *vlan-id* immediate-leave

- *vlan-id* — VLAN ID (範囲：1-4093)

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- immediate-leave が使用されない場合、IGMPv2/v3 グループが leave メッセージを受信した時、マルチキャストルータ（またはクエリア）はグループ指定クエリメッセージを送信します。タイムアウト期間の内にホストがクエリに返答しない場合に限り、ルータ / クエリはグループのトラフィック転送を停止します。（このリリースのタイムアウトは現在 Last Member Query Interval によって定義されています（1 秒に固定）
*RFC2236 で定義される信頼関数（2 に固定）
- このコマンドは IGMP スヌーピング有効で、IGMPv2 または IGMPv3 スヌーピングが使用されている時のみ効果があります。

例

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

ip igmp snooping vlan last-memb-query-count

システムがこれ以上ローカルメンバーがいないと想定する前に送出される、IGMP プロキシ group-specific または group-and-source-specific クエリメッセージの数を設定します。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping vlan *vlan-id* last-memb-query-count *count*
no ip igmp snooping vlan *vlan-id* last-memb-query-count

- *vlan-id* — VLAN ID（範囲：1-4093）
- *count* — プロキシ group-specific または group-and-sourcespecific クエリメッセージの数（範囲：1-255）

初期設定

2

コマンドモード

Global Configuration

コマンド解説

- IGMP スヌーピングプロキシレポーティングまたは IGMP クエリが有効（P785）の場合に限り、このコマンドは効力を発揮します。

例

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7
Console(config)#
```

ip igmp snooping vlan last-memb-query-intvl

last-member-query 間隔を設定します。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping vlan *vlan-id* last-memb-query-intvl *interval*
no ip igmp snooping vlan *vlan-id* last-memb-query-intvl

- *vlan-id* — VLAN ID（範囲：1-4093）
- *interval* — group-specific または group-and-source-specific クエリメッセージの返答を待つ間隔（範囲：1-31744）

初期設定

10

コマンドモード

Global Configuration

コマンド解説

- このコマンドは IGMP スヌーピングプロキシレポーティングが有効時のみ効果があります。（P785）

例

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700
Console(config)#
```

ip igmp snooping vlan mrd

マルチキャストルータ solicitation メッセージの送信を有効にします。"no" を前に置くことでこれらのメッセージを無効にします。

文法

[no] ip igmp snooping vlan *vlan-id* mrd

- *vlan-id* — VLAN ID（範囲：1-4093）

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- Multicast Router Discovery (MRD) はマルチキャストルータアドバタイズメント、マルチキャストルータ要請およびマルチキャストルータを発見するために使うマルチキャストルータターミネーションメッセージを使用します。
デバイスがアドバタイズメントメッセージをマルチキャストルータから要請するために要請メッセージを送信します。これらのメッセージはダイレクトに付属されたリンクからマルチキャストルータを発見するために使用します。
マルチキャスト転送インタフェースが初期化または最初期化される時はいつも、要請メッセージも送信されます。
IP マルチキャスト転送および MRD 有効で、インタフェースの要請を受け取るとすぐにルータはアドバタイズメントで返答します。

例

```
Console(config)#no ip igmp snooping vlan 1 mrd
Console(config)#
```

ip igmp snooping vlan proxy-address

IGMP プロキシレポーティングに使用される、ローカルな通常クエリとレポートメッセージの静的アドレスを設定します。"no" を前に置くことで初期設定に戻します。

文法

[no] ip igmp snooping vlan *vlan-id* proxy-address *source-address*

- *vlan-id* — VLAN ID (範囲：1-4093)
- *source-address* — プロキシされた IGMP クエリとレポート、leave メッセージに使用するソースアドレス (有効な IP ユニキャストアドレス)

初期設定

0.0.0.0

コマンドモード

Global Configuration

例

```
Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8
Console(config)#
```

ip igmp snooping vlan proxy-query-interval

IGMP プロキシ通常クエリア送信間隔を設定します。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping vlan *vlan-id* proxy-query-interval *interval*
no ip igmp snooping vlan *vlan-id* proxy-query-interval

- *vlan-id* — VLAN ID（範囲：1-4093）
- *interval* — IGMP プロキシ通常クエリアを送信する間隔。（範囲：10-31744 秒）

初期設定

100（10 秒）

コマンドモード

Global Configuration

コマンド解説

- このコマンドで指定された間隔で、スイッチから IGMP 通常クエリメッセージが送信されます。このメッセージがダウンストリームホストで受信された時、全てのレシーバは合流したマルチキャストグループのために IGMP レポートを構築します。
- このコマンドは IGMP スヌーピングプロキシレポーティングが有効になっている時のみ効果があります。（P785）

例

```
Console(config)#ip igmp snooping vlan 1 proxy-query-interval 150
Console(config)#
```

ip igmp snooping vlan proxy-query-resp-intvl

システムがプロキシクエリアの返答を待つ最大時間。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping vlan *vlan-id* **proxy-query-resp-intvl** *interval*
no ip igmp snooping vlan *vlan-id* **proxy-query-resp-intvl**

- *vlan-id* — VLAN ID（範囲：1-4093）
- *interval* — システムがプロキシ通常クエリの返答を待つ最大時間（範囲：10-31744）

初期設定

100（10 秒）

コマンドモード

Global Configuration

コマンド解説

- このコマンドは IGMP スヌーピングプロキシレポーティングが有効になっている時のみ効果があります。（P785）

例

```
Console(config)#ip igmp snooping vlan 1 proxy-query-resp-intvl 20
Console(config)#
```


ip igmp snooping vlan static

ポートをマルチキャストグループに追加します。"no" を前に置くことでポートを削除します。

文法

[no] ip igmp snooping vlan *vlan-id* static *ip-address* *interface*

- *vlan-id* — VLAN ID（範囲：1-4093）
- *ip-address* — マルチキャストグループの IP アドレス
- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号（範囲：1-26）
 - port-channel *channel-id*（範囲：1-12）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 静的マルチキャストエントリはエイジアウトしません。
- マルチキャストエントリが特定の VLAN のインタフェースにアサインされた時、対応するトラフィックは VLAN 内のポートにのみ転送されます。

例

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

show ip igmp snooping

IGMP snooping の設定情報を表示します。

文法

show ip igmp snooping

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

表示される内容に関しては、P335 「IGMP Snooping とクエリパラメータの設定」を参照して下さい。

例

本例では現在の IGMP snooping の設定を表示しています。

```
Console#show ip igmp snooping
IGMP snooping                : Enabled
Router port expire time      : 300 s
Router alert check           : Disabled
Tcn flood                     : Disabled
Tcn query solicit            : Disabled
Unregistered data flood      : Disabled
Unsolicited report interval  : 400 s
Version exclusive            : Disabled
Version                      : 2
Proxy reporting               : Enabled

Vlan 1:
-----
IGMP snooping                : Enabled
IGMP snooping running status : Inactive
Immediate leave               : Disabled
Last member query interval   : 10 (1/10s)
Last member query count      : 2
Proxy query address           : 0.0.0.0
Version                      : Using global version (2)
Proxy query interval          : 125 s
Proxy query response interval : 100 (1/10s)
Version exclusive             : Disabled
General query suppression     : Disabled
Proxy reporting               : Using global status (Enabled)
Multicast Router Discovery    : Enabled
.
```

show ip igmp snooping group

既知のマルチキャストグループと、指定した VLAN インタフェースまたは全てのインタフェースにマップされたホストポートを表示します。

文法

show ip igmp snooping group [vlan *vlan-id* [user | igmpsnp]] [user | igmpsnp]

- *vlan-id* — VLAN ID（範囲：1-4093）
- **user** — ユーザ設定マルチキャストエントリのみ表示
- **igmpsnp** — IGMP スヌーピングで学習されたエントリのみ表示

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

メンバータイプは選択したオプションに依存し、IGMP またはユーザを含んで表示します。

例

```
Console#show ip igmp snooping group vlan 1
Bridge Multicast Forwarding Entry Count:0
VLAN      Group      Source      Port List
-----
1  224.1.1.12    *          Eth 1/ 9 (S)
1  224.1.1.12    *          Eth 1/10 (D)
Console#
```

4.21.2 静的マルチキャストルーティングコマンド

コマンド	機能	モード	ページ
ip igmp snooping VLAN mrouter	マルチキャストルータポートの追加	GC	P806
show ip igmp snooping mrouter	マルチキャストルータポートの表示	PE	P807

ip igmp snooping vlan mrouter

マルチキャストルータポートを静的に設定します。"no" を前に置くことで設定を削除します。

文法

ip igmp snooping vlan *vlan-id* **mrouter** *interface*

no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID（範囲：1-4093）
- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号（範囲：1-26）
 - port-channel *channel-id*（範囲：1-12）

初期設定

静的マルチキャストルータポートは設定されていません。

コマンドモード

Global Configuration

コマンド解説

ネットワーク接続状況により、IGMP スヌーピングでは常に IGMP クエリアが配置されません。したがって、IGMP クエリアがスイッチに接続された既知のマルチキャストルータ / スイッチである場合、インタフェースをすべてのマルチキャストグループに参加させる設定を手動で行えます。

例

本例では 11 番ポートを VLAN 1 のマルチキャストルータポートに設定しています。

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

静的設定及び動的学習によるマルチキャストルータポートの情報の表示を行います。

文法

show ip igmp snooping mrouter { vlan *vlan-id* }

- *vlan-id* — VLAN ID（範囲：1-4093）

初期設定

VLAN に設定されたすべてのマルチキャストルータポートを表示します。

コマンドモード

Privileged Exec

コマンド解説

マルチキャストルータポートとして表示されるタイプには静的及び動的の両方が含まれます。

例

本例では、VLAN 1 のマルチキャストルータに接続されたポートを表示します。

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Ports Type
-----
      1           Eth 1/10   Static
Console#
```

4.21.3 IGMP Filtering/Throttling コマンド

特定の定期購読契約に基づいた IP/TV サービス等の環境において、管理者が、エンドユーザーの入手できるマルチキャストサービスの制御を希望する場合があります。

IGMP フィルタリングは、指定されたスイッチポート上のマルチキャストサービスへのアクセス制限したり、同時にアクセスできるマルチキャストグループの数を調整することによって、この条件を満たすことが可能です。

IGMP フィルタリング機能を使用することにより、プロファイルを特定のマルチキャストグループのスイッチポートに割り当て、ポート単位でマルチキャスト加入をフィルタリングできます。

コマンド	機能	モード	ページ
ip igmp filter	スイッチで IGMP フィルタリング / スロットリングを有効	GC	P809
ip igmp profile	プロファイル番号の設定及び IGMP profile 設定モードへ移行	GC	P810
permit, deny	プロファイルアクセスモードを設定	IPC	P811
range	プロファイルのマルチキャストアドレスを設定	IPC	P812
ip igmp filter	IGMP フィルタプロファイルをインタフェースへアサイン	IC	P813
ip igmp max-groups	IGMP スロットリング番号を指定	IC	P814
ip igmp max-groups action	インタフェースのスロットリングアクションを設定	IC	P815
show ip igmp filter	IGMP フィルタリングステータスを表示	PE	P816
show ip igmp profile	IGMP プロファイルおよび設定の表示	PE	P817
show ip igmp throttle interface	インタフェースの IGMP スロットリング設定を表示	PE	P818

ip igmp filter (Global Configuration)

本コマンドは IGMP フィルタリングおよびスロットリングを、スイッチで有効にします。
"no" を前に置くことで機能を無効にします。

文法

ip igmp filter

no ip igmp filter

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- IGMP フィルタリングは、ポートで許可または拒否されるマルチキャストグループを指定するプロファイルをスイッチポートに割り当てることを可能にします。IGMP フィルタプロファイルは 1 つ以上またはマルチキャストアドレスの範囲で含まれることが出来ませんが、一つのプロファイルのみポートに割り当てる事が可能です。
- 有効時、ポートで受信される IGMP join レポートはフィルタプロファイルにたいしてチェックされます。もし要求されたマルチキャストグループが許可された場合、IGMP join レポートは普通に転送されます。要求されたマルチキャストグループが拒否された場合、IGMP join レポートはドロップされます。
- IGMP フィルタリングとスロットリングは動的に学習されたマルチキャストグループにのみ適用され、制的に設定されたグループには適用されません。
- 転送されたマルチキャストトラフィックに MVR が使用される際、IGMP フィルタリング機能は同じマナーで稼働します。

例

```
Console(config)#ip igmp filter
Console(config)#
```

ip igmp profile

本コマンドを実行することで、IGMP フィルタプロファイル番号の作成を行うと共に、IGMP プロファイル設定モード（IPC モード）へ移行します。
"no" を前に置くことでプロファイル番号を削除します。

文法

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

- *profile-number*— IGMP フィルタプロファイル番号（範囲：1-4294967295）

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```


permit, deny

IGMP フィルタプロファイルにアクセスモードを設定します。

文法

permit | deny

初期設定

Deny

コマンドモード

IGMP Profile Configuration

コマンド解説

- それぞれのプロフィールはひとつのアクセスモードが設定されます。(許可もしくは拒否)
- アクセスモードが許可に設定時、マルチキャストグループが制御されたコントロール範囲に一致した場合、IGMP join レポートが処理されます。拒否に設定時、マルチキャストグループが制御されたコントロール範囲に一致しない場合のみ、IGMP join レポートが処理されます。

例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range

プロファイルの、マルチキャストグループアドレスを設定します。

"no" を前に置くことでプロファイルからアドレスを削除します。

文法

range *low-ip-address* { *high-ip-address* }

no range *low-ip-address* { *high-ip-address* }

- *low-ip-address*— マルチキャストグループ IP アドレス、または指定する範囲の最初の IP アドレス
- *high-ip-address*— 指定する範囲の最後の IP アドレス

初期設定

なし

コマンドモード

IGMP Profile Configuration

例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

ip igmp filter (Interface Configuration)

IGMP フィルタリングプロファイルを、スイッチ上のインタフェースに割り当てます。

"no" を前に置くことでインタフェースからプロファイルを取り除きます。

文法

ip igmp filter *profile-number*

no ip igmp filter { *profile-number* }

- *profile-number* — IGMP フィルタプロファイル番号（範囲：1-4294967295）

初期設定

なし

コマンドモード

Interface Configuration

コマンド解説

- インタフェースにアサインできるプロファイルは1つのみです。
- ポートがトランクのメンバーである場合、トランクは、最初にポートメンバーへ適用された設定を使用します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups

スイッチ上のインタフェースに、IGMP スロットリング番号を設定します。"no" を前に置くことで初期設定へ戻します。

文法

ip igmp max-groups *number*

no ip igmp max-groups

- *number*— インターフェイスが加入できる IGMP グループの最大数（範囲：1-255）

初期設定

255

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- ポートがトランクのメンバーである場合、トランクは、最初にポートメンバーへ適用された設定を使用します。
- IGMP スロットリングは、同時に加入が可能なマルチキャストグループポートの最大値を設定します。グループ数が、設定した最大値に達した時、スイッチは「どちらも拒否する」「置き換え」の内どちらかの処理を行うことができます。
「拒否する」設定になっている場合、全ての新規 IGMP join レポートは破棄されます。
「置き換え」設定になっている場合、スイッチはランダムに既存のグループを取り去り、新しいマルチキャストグループに置き換えます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action

スイッチ上のインタフェースに、IGMP スロットリングアクションを設定します。

文法

ip igmp max-groups action < replace | deny >

- replace —既存のマルチキャストグループは、新しいグループへ置き換えられます。
- deny —新規のレポートは破棄されます。

初期設定

Deny

コマンドモード

Interface Configuration

コマンド解説

- IGMP スロットリングは、同時に加入が可能なマルチキャストグループポートの最大値を設定します。グループ数が、設定した最大値に達した時、スイッチは「どちらも拒否する」「置き換え」の内どちらかの処理を行うことができます。
「拒否する」設定になっている場合、全ての新規 IGMP join レポートは破棄されます。
「置き換え」設定になっている場合、スイッチはランダムに既存のグループを取り去り、新しいマルチキャストグループに置き換えます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

show ip igmp filter

グローバルおよび、インタフェースの IGMP フィルタリング設定を表示します。

文法

show ip igmp filter { interface *interface* }

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show ip igmp filter
IGMP filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
-----
IGMP Profile 19
Deny
range 239.1.1.1 239.1.1.1
range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile

スイッチ上の IGMP フィルタリングプロファイルを表示します。

文法

show ip igmp profile [*profile-number*]

- *profile-number*—既存の IGMP フィルタプロファイル番号（範囲：1-4294967295）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
Deny
range 239.1.1.1 239.1.1.1
range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp throttle interface

IGMP スロットリングのインタフェース設定を表示します。

文法

show ip igmp throttle interface { *interface* }

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

初期設定

なし

コマンドモード

Privileged Exec

例

本例では、VLAN 1 のマルチキャストルータに接続されたポートを表示します。

```
Console#show ip igmp throttle interface ethernet 1/1
Eth 1/1 Information
Status : TRUE
Action : Deny
Max Multicast Groups : 32
Current Multicast Groups : 0
Console#
```


4.21.4 MVR の設定

この章は Multicast VLAN Registration(MVR) を設定するために使用されるコマンドを記載しています。

サービスプロバイダーのネットワークを通して広いシングルネットワークの VLAN にマルチキャストトラフィック（例：テレビのチャンネル）を送信することができます。

MVR VLAN に入ったどのマルチキャストトラフィックもすべての Subscribers に送信することができます。これは動的な監視に必要なオーバーヘッドのプロセスを著しく減少させ、正常なマルチキャスト VLAN の配信ツリーを確立します。

また、MVR は他の VLAN から Subscribers が属する VLAN にマルチキャストトラフィックだけを通過させることによって、VLAN を分割することによるユーザーの分離とデータ保護機能を維持します。

コマンド	機能	モード	ページ
mvr	MVR の有効、および MVR グループアドレスや MVR VLAN ID を静的に構成	GC	P820
mvr immediate-leave	即時離脱機能を有効化	IC	P821
mvr type	インタフェースを MVR レシーバまたはソースポートとして設定	IC	P822
mvr vlan group	マルチキャストグループをポートへ静的にバインド	IC	P823
show mvr	MVR 設定、MVR VLAN 関連のインタフェース、MVR VLAN に割り当てられたマルチキャストグループアドレスを表示	PE	P824

mvr

このコマンドはスイッチ上で Multicast VLAN Registration(MVR) を有効にします。group オプションで MVR マルチキャストグループの IP アドレスを静的に構成します。VLAN オプションで MVR VLAN の ID を設定します。オプションなしでこのコマンドに no を付けると MVR 機能を無効にします。group オプションと同時に no を付けると特定のアドレス、もしくは複数のアドレスを消去します。vlan キーワードに no を付けると MVR VLAN ID の設定はデフォルトに戻ります。

文法

mvr { group *ip-address* { count } | vlan *vlan-id* }

no mvr { group *ip-address* { count } }

- *ip-address* — MVR マルチキャストグループの IP アドレス
(範囲：224.0.1.0-239.255.255.255)
- *count* — 連続する MVR グループアドレスの番号 (範囲：1-1024)
- *vlan-id* — MVR VLAN ID (範囲：1-4093)

初期設定

MVR：無効

MVR グループアドレス：未定義

連続アドレスの初期番号：0

MVR VLAN ID：1

コマンドモード

Global Configuration

コマンド解説

- mvr group コマンドを使用して MVR VLAN に参加するすべてのマルチキャストグループアドレスを静的に構成することができます。MVR グループに関連付けられたどのマルチキャストデータもすべてのソースポートから、マルチキャストのデータを受信するよう登録されたすべてのレシーバーポートに送信されます。
- 224.0.0.0 ～ 239.255.255.255 の範囲の IP アドレスはマルチキャストストリームとして使用されます。予約された IP マルチキャストアドレス (224.0.0.0 ～ 224.0.0.255) は MVR グループアドレスとして使用することができません。
- MVR ソースポートは、"switchport allowed vlan" コマンド (P715) と "switchport native vlan" コマンド (P718) を使用して MVR VLAN のメンバーとして設定が可能ですが、MVR レシーバポートはこの VLAN のメンバーとして静的に設定することは出来ません。

例

本例では、VLAN 1 のマルチキャストルータに接続されたポートを表示します。

```
Console(config)#mvr
Console(config)#mvr group 228.1.23.1 10
Console(config)#
```

mvr immediate-leave

このコマンドは、グループの Leave メッセージ受信した後、直ちにインタフェースをマルチキャストストリームから取り除くように設定します。"no" を前につけることで設定を初期値に戻します。

文法

mvr immediate-leave
no mvr immediate-leave

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- Immediate leave はレシーバポートにのみ適用可能です。
有効時、レシーバポートは leave メッセージで確認されたマルチキャストグループから直ちに除外されます。
無効時、スイッチはグループに指定されたクエリをレシーバポートに送信することによって標準ルールに従い、ポートをグループリストから取り除く前に、マルチキャストグループに残っている加入者の有無を決定するために返答を待ちます。

例

レシーバポートで Immediate leave を有効にしています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr immediate-leave
Console(config-if)#
```

mvr type

インタフェースを MVR レシーバまたはソースポートとして設定します。"no" を前に置くことで初期設定に戻します。

文法

mvr type < receiver | source >

no mvr type < receiver | source >

- receiver —インタフェースをマルチキャストデータを受信出来る、サブスクライバポートとして設定。
- source —インタフェースを設定されたマルチキャストグループのマルチキャストデータの送受信が可能なアップリンクポートに設定。

初期設定

ポートタイプは未定義

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- MVR レシーバまたはソースポートに設定されていないポートは、マルチキャストフィルタリングのスタンダードルールを使用し、マルチキャストグループに参加または脱退するために IGMP スヌーピングを使用出来ます。
- レシーバポートは異なる VLAN に属することが可能ですが、MVR VLAN のメンバーとしては設定されません。IGMP スヌーピングはレシーバポートが動的に MVR VLAN を通してソースを持つマルチキャストグループに加入 / 脱退を可能にするために使用されます。また、MVR レシーバポートの VLAN メンバーシップをトランクモードには設定出来ないことにご注意下さい。(see the switchport mode command).
- IGMP スヌーピングは、サブスクライバの MVR グループへの動的参加または脱退を可能にするため、有効にしなくてはなりません。(see the ip igmp snooping command)IGMPv2 または 3 ホストのみがマルチキャスト Join または leave メッセージを発行できることにご注意ください。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#
```

mvr vlan group

マルチキャストグループを、ホストの安定したセットに割り当てられ、長期マルチキャストストリームを受信するポートに静的にバインドします。"no" を前に置くことで初期設定に戻します。

文法

mvr vlan *vlan-id* **group** *ip-address*

- *vlan-id* — 指定されたマルチキャストトラフィックがフラッドされるレシーバ VLAN (範囲：1-4093)
- **group** — 選択されたポートへ送信されるマルチキャストサービスを定義
- IP アドレス (範囲：224.0.1.0 - 239.255.255.255)

初期設定

設定されたマルチキャストグループにメンバーはいません。

コマンドモード

Interface Configuration (Ethernet、Port Channel)

コマンド解説

- このコマンドを使用し、マルチキャストグループをレシーバポートに静的に割り当てることが可能です。
- IP アドレス範囲 224.0.0.0 ~ 239.255.255.255 はマルチキャストストリームに使用されます。MVR グループアドレスは予約されている 224.0.0.x の IP マルチキャストアドレス範囲内にすることは出来ません。
- IGMP スヌーピングは、サブスクライバの MVR グループへの動的参加または脱退を可能にするため、有効にしなくてはなりません。(see the ip igmp snooping command)IGMPv2 または 3 ホストのみがマルチキャスト Join または leave メッセージを発行できることにご注意ください。

例

The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#mvr vlan 3 group 225.0.0.5
Console(config-if)#
```

show mvr

MVR の情報を表示します。

文法

show mvr { interface *interface* | members { *ip-address* } }

- *interface*
 - ethernet *unit/port*
 - unit* — ユニット番号 "1"
 - port* — ポート番号 (範囲：1-26)
 - port-channel *channel-id* (範囲：1-12)
- *ip-address* — MVR マルチキャストグループの IP アドレス
(範囲：224.0.1.0-239.255.255.255)

初期設定

なし

コマンド解説

- キーワード無しでここコマンドを入力すると、MVR のグローバル設定を表示します。
"interface" キーワードを使用した場合、MVR VLAN に接続されたインタフェースについての情報を表示します。"member" キーワードを使用した場合、MVR VLAN に接続されたマルチキャストグループについての情報を表示します。

例

グローバル MVR 設定を表示します。

```
Console#show mvr
MVR Config Status   : Enabled
MVR Running Status  : Active
MVR Multicast VLAN   : 1
MVR Group Address    : 225.0.0.5
MVR Group Count      : 10
Console#
```

項目	解説
MVR Config Status	MVR がスイッチ上で有効であるかを表示
MVR Running Status	MVR 環境の中のすべての必要条件が満たされているかを表示
MVR Multicast VLAN	全ての MVR マルチキャストトラフィックを転送される VLAN
MVR Group Address	マルチキャストサービスを全ての付属するサブスクライバに送信
MVR Group Count	連続した MVR グループアドレス数

例

インタフェース情報を表示します。

```

Console#show mvr interface
Port      Type      Status      Immediate      Static Group Address
-----
Eth1/ 2   Source    Active/Up
Eth1/ 3   Source    Inactive/Down
Eth1/ 1   Receiver  Active/Up      Disabled      225.0.0.1 (VLAN1)
                                           225.0.0.9 (VLAN3)
Eth1/ 4   Receiver  Active/Down    Disabled
Console#

```

項目	解説
Port	MVR VLAN に付加されているインタフェース
Type	MVR ポートタイプ
Status	MVR がスイッチで有効の場合 “ACTIVE ” レシーバポートの MVR が “ACTIVE ” の場合、加入者が MVR グループの内ひとつからマルチキャストトラフィック を受信中、またはマルチキャストグループはインタフェース に静的にアサイン
Immediate Leave	即時脱退の有効 / 無効
Static Group Address	インタフェースとレシーバ VLAN にアサインされた、静的 MVR グループを表示

例

```

Console#show mvr members
MVR Forwarding Entry Count:1
Group Address      Source Address      VLAN      Forwarding Port
-----
225.0.0.9          *                    2          Eth1/ 1 (VLAN3)   Eth1/ 2 (VLAN2)
Console#

```

項目	解説
MVR Forwarding Entry Count	現在 MVR VLAN から転送されているマルチキャストサービス数。
Group Address	MVR VLAN にアサインされているマルチキャストグループ。
Source Address	マルチキャストサービスのソースアドレスを示すか、グループアドレスが静的に割り当てられている場合にアスタリスクを表示。
VLAN	マルチキャストサービスを受信している MVR VLAN を表示。
Forwarding Port	MVR VLAN を通してマルチキャストサービスを提供される、 インタフェースとサブスクライバを表示。また、サービスを受ける VLAN も表示。もしグループアドレスが静的に割り当てられた場合は、MVR VLAN と異なることがあります。

4.22 LLDP コマンド

Link Layer Discovery Protocol (LLDP) はローカルブロードキャストドメインの中の接続デバイスについての基本的な情報を発見するために使用します。LLDP はレイヤ 2 のプロトコルであり、デバイスについての情報を周期的なブロードキャストで伝達します。伝達された情報は IEEE802.1ab に従って Type Length Value (TLV) で表され、そこにはデバイス自身の識別情報、能力、設定情報の詳細が含まれています。また LLDP は発見した近隣のネットワークノードについて集められた情報の保存方法と管理方法を定義します。

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) は VoIP やスイッチのようなエンドポイントのデバイスを管理するための拡張された LLDP です。LLDP-MED の TLV はネットワークポリシー、電力、インベントリ、デバイスのロケーションの詳細情報を伝達します。LLDP と LLDP-MED の情報は、トラブルシューティングの簡易化、ネットワーク管理の改善、間違いのないネットワークトポロジを維持するため、SNMP アプリケーションによって使用することができます。

コマンド	機能	モード	ページ
lldp	スイッチで LLDP を有効	GC	P827
lldp holdtime-multiplier	TTL(time-to-live) 値の設定	GC	P828
lldp notification-interval	LLDP の変更に関する SNMP 通知送信の間隔を設定	GC	P829
lldp refresh-interval	LLDP 配信の転送間隔を設定	GC	P829
lldp reinit-delay	LLDP ポートが無効またはリンクダウン時の再初期化までの待ち時間を設定	GC	P830
lldp tx-delay	ローカル LLDP MIB の変数に变化が起こった後に、アドバイズメントを送信するまでの時間を設定します	GC	P830
lldp admin-status	LLDP メッセージの送信・受信のモードを有効	IC	P831
lldp basic-tlv management-ip-address	TLV Type "management-ip-address" を設定	IC	P831
lldp basic-tlv port-description	TLV Type "port-description" を設定	IC	P832
lldp basic-tlv system-capabilities	TLV Type "system-capabilities" を設定	IC	P832
lldp basic-tlv system-description	TLV Type "system-description" を設定	IC	P833
lldp basic-tlv system-name	TLV Type "system-name" を設定	IC	P834
lldp dot1-tlv proto-ident*	lldp dot1-TLV" proto-ident" を設定	IC	P834
lldp dot1-tlv proto-vid*	lldp dot1-TLV" proto-vid" を設定	IC	P835
lldp dot1-tlv pvid*	lldp dot1-TLV"pvid" を設定	IC	P835
lldp dot1-tlv vlan-name*	lldp dot1-TLV"vlan-name" を設定	IC	P836

lldp dot3-tlv link-agg	lldp dot3-TLV“link-agg”を設定	IC	P836
lldp dot3-tlv mac-phy	lldp dot3-TLV“mac-phy”を設定	IC	P837
lldp dot3-tlv max-frame	lldp dot3-TLV“max-frame”を設定	IC	P837
lldp notification	LLDP と LLDP-MED の変更について SNMP トラップ通知の送信を有効	IC	P838
show lldp config	LLDP 設定の表示	PE	P839
show lldp info local-device	LLDP ローカルデバイス情報を表示	PE	P840
show lldp info remote-device	LLDP リモートデバイス情報を表示	PE	P841
show lldp info statistics	LLDP 統計情報を表示	PE	P842

lldp

スイッチで LLDP を有効にします。"no" を前に置くことで機能を無効にします。

文法

lldp

no lldp

初期設定

有効

コマンドモード

Global Configuration

例

```
Console (config) #lldp
Console (config) #
```

lldp holdtime-multiplier

LLDP のアドバタイズメントで送信された Time-To-Live (TTL) 値を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

- *value* - TTL 値を設定します。TTL は秒で表され、下の数式で計算します。
 $\text{Transmission Interval} \times \text{Hold Time Multiplier} \leq 65536$
(範囲：2 - 10)

初期設定

Holdtime multiplier：4

TTL：4 × 30 = 120 秒

コマンドモード

Global Configuration

コマンド解説

TTL は、タイムリーな方法でアップデートが送信されない場合、送信した LLDP エージェントに関係のあるすべての情報をどのくらいの期間維持するかを受信した LLDP エージェントに伝達します。

例

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

lldp notification-interval

LLDP MIB の変更を行い、SNMP 通知が送信されるまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp notification-interval *seconds*

no lldp notification-interval

- *seconds* - SNMP 通知が送られる周期的な間隔を指定します
(範囲：5 ～ 3600 秒 初期設定 5 秒)

初期設定

5 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp notification-interval 30
Console(config)#
```

lldp refresh-interval

LLDP アドバタイズが送信されるまでの間隔を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp refresh-interval *seconds*

no lldp refresh-delay

- *seconds* - LLDP アドバタイズが送信されるまでの間隔を指定します
(範囲：5 ～ 32768 秒)

初期設定

30 秒

コマンドモード

Global Configuration

コマンド解説

refresh-interval × Hold Time Multiplier ≤ 65536

例

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

lldp reinit-delay

LLDP ポートが無効になるかリンクダウンした後、再初期化を試みるまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp reinit-delay *seconds*

no lldp reinit-delay

- *seconds* - 再初期化を試みるまでの時間を指定します（範囲：1-10 秒）

初期設定

2 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay

ローカル LLDP MIB の変数に変化が起こった後に引き続き、アドバタイズメントを送信するまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp tx-delay *seconds*

no lldp tx-delay

- *seconds* - アドバタイズメントを送信するまでの時間を設定を指定します（範囲：1-8192 秒）

初期設定

2 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status

個別のインターフェースに対し、メッセージの内容を指定するために LLDP ポート・トラнкの設定を行います。"no" を前に置くことでこの機能を無効にします。

文法

lldp admin-status < rx-only | tx-only | tx-rx >

no lldp admin-status

- rx-only - LLDP PDUs. 受信のみ
- tx-only - LLDP PDUs. 送信のみ
- tx-rx - LLDP PDUs. 送受信

初期設定

tx-rx

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp basic-tlv management-ip-address

LLDP 有効ポートで "management-ip-address" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv management-ip-address

no lldp basic-tlv management-ip-address

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- management-ip-address には、スイッチの IPv4 アドレスが含まれます。スイッチに管理用のアドレスがない場合、アドレスはスイッチの CPU の MAC アドレスが、このアドバタイズメントを送信するポートの MAC アドレスになります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description

LLDP 有効ポートで "port-description" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv port-description
no lldp basic-tlv port-description

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- port-description には、RFC2863 の ifDescr オブジェクトで規定されています。これには製造者、スイッチの製品名、インターフェースのハードウェアとソフトウェアのバージョンが含まれます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

lldp basic-tlv system-capabilities

LLDP 有効ポートで "system-capabilities" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv system-capabilities
no lldp basic-tlv system-capabilities

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- system-capabilities には、システムの主な機能が含まれます。この情報には機能自体が有効かどうかは関係ありません。この TLV によってアドバタイズされる情報は IEEE802.1AB 規格に記述されています。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description

LLDP 有効ポートで "system-description" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv system-description

no lldp basic-tlv system-description

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

system-description は RFC3418 の sysDescr オブジェクトで規定されています。システムのハードウェア、オペレーティングソフト、ネットワーキングソフトのフルネームとバージョンが含まれています。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name

LLDP 有効ポートで "system-name" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv system-name
no lldp basic-tlv system-name

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- System-name は RFC3418 の sysName オブジェクトで規定されています。システムの管理用に割り当てられた名前が含まれます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dot1-tlv proto-ident

LLDP 有効ポートで "proto-ident" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv proto-ident
no lldp dot1-tlv proto-ident

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```


lldp dot1-tlv proto-vid

LLDP 有効ポートで "proto-vid" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

```
lldp dot1-tlv proto-vid  
no lldp dot1-tlv proto-vid
```

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ポートベースおよびプロトコルベース VLAN 情報をアドバタイズします。
詳細については P712 「VLAN インタフェースの設定」および P730 「プロトコル VLAN の設定」を参照してください。

例

```
Console(config)#inter ethernet 1/1  
Console(config-if)#no lldp dot1-tlv proto-vid  
Console(config-if)#
```

lldp dot1-tlv pvid

LLDP 有効ポートで "pvid" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

```
lldp dot1-tlv pvid  
no lldp dot1-tlv pvid
```

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- PVID 情報をアドバタイズします。
詳細については P718 「switchport native vlan」を参照してください。

例

```
Console(config)#interface ethernet 1/1  
Console(config-if)#no lldp dot1-tlv pvid  
Console(config-if)#
```

lldp dot1-tlv vlan-name

LLDP 有効ポートで "vlan-name" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv vlan-name
no lldp dot1-tlv vlan-name

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 指定したインタフェースが割り当てられた、全ての VLAN 名をアドバタイズします。
VLAN については P715 「switchport allowed vlan」 および P731 「protocol-vlan protocol-group (Configuring Groups)」を参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg

LLDP 有効ポートで "link-agg" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot3-tlv link-agg
no lldp dot3-tlv link-agg

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- リンクアグリゲーションステータスをアドバタイズします。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy

LLDP 有効ポートで "mac-phy" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

```
lldp dot3-tlv mac-phy  
no lldp dot3-tlv mac-phy
```

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- MAC/PHY 設定およびステータスをアドバタイズします。

例

```
Console(config)#interface ethernet 1/1  
Console(config-if)#no lldp dot3-tlv mac-phy  
Console(config-if)#
```

lldp dot3-tlv max-frame

LLDP 有効ポートで "max-frame" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

```
lldp dot3-tlv max-frame  
no lldp dot3-tlv max-frame
```

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 最大フレームサイズ情報をアドバタイズします。フレームサイズについての詳細は P386 「フレームサイズコマンド」を参照してください。

例

```
Console(config)#interface ethernet 1/1  
Console(config-if)#lldp dot3-tlv max-frame  
Console(config-if)#
```

lldp notification

LLDP 変更について SNMP トラップ通知の送信を可能にします。"no" を前に置くことでこの機能を無効にします。

文法

lldp notification
no lldp notification

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

show lldp config

全てのポートの LLDP 設定を表示します。

文法

show lldp config [detail interface]

- *detail* — 設定サマリを表示
- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-5)

コマンドモード

Privileged Exec

例

```
Console#show lldp config

LLDP Global Configuration

LLDP Enabled                : Yes
LLDP Transmit interval     : 30 sec.
LLDP Hold Time Multiplier  : 4
LLDP Delay Interval        : 2 sec.
LLDP Re-initialization Delay : 2 sec.
LLDP Notification Interval  : 5 sec.

LLDP Port Configuration
Port      Admin Status Notification Enabled
-----
Eth 1/1   Tx-Rx          False
Eth 1/2   Tx-Rx          False
Eth 1/3   Tx-Rx          False
Eth 1/4   Tx-Rx          False
Eth 1/5   Tx-Rx          False
.
.
.
Console#
```

show lldp info local-device

スイッチについての情報を表示します。

文法

show lldp info local-device [detail interface]

- *detail* — 詳細情報を表示
- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

例

```
Console#show lldp info local-device

LLDP Local System Information
Chassis Type                : MAC Address
Chassis ID                  : 00-1A-7E-AB-FD-12
System Name                 :
System Description          : FXC3326
System Capabilities Support : Bridge
System Capabilities Enabled : Bridge
Management Address          : 192.168.1.10 (IPv4)

LLDP Port Information
  Port    PortID Type    PortID    Port Description
  -----
Eth 1/1   MAC Address   00-1A-7E-AB-FD-13 Ethernet Port on unit 1, port 1
Eth 1/2   MAC Address   00-1A-7E-AB-FD-14 Ethernet Port on unit 1, port 2
Eth 1/3   MAC Address   00-1A-7E-AB-FD-15 Ethernet Port on unit 1, port 3
Eth 1/4   MAC Address   00-1A-7E-AB-FD-16 Ethernet Port on unit 1, port 4
Eth 1/5   MAC Address   00-1A-7E-AB-FD-17 Ethernet Port on unit 1, port 5
LLDP Port Information
.
.
.
Console#
```

show lldp info remote-device

ローカルスイッチの指定されたポートに接続された、LLDP が有効のデバイスについての詳細情報を表示します。

文法

show lldp info remote-device [detail interface]

- *detail* — 詳細情報を表示
- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

例

```

Console#show lldp info remote-device

LLDP Remote Devices Information

Interface Chassis ID          Port ID          System Name
-----
Eth 1/1    00-01-02-03-04-05    00-01-02-03-04-06

Console#show lldp info remote-device detail ethernet 1/1

LLDP Remote Devices Information Detail
-----
Local PortName      : Eth 1/1
Chassis Type        : MAC Address
Chassis Id          : 00-01-02-03-04-05
PortID Type         : MAC Address
PortID              : 00-01-02-03-04-06
SysName             :
SysDescr            : 24PORT GIGABIT L2 INTELLIGENT SWITCH
PortDescr           : Ethernet Port on unit 1, port 1
SystemCapSupported  : Bridge
SystemCapEnabled    : Bridge
Remote Management Address :
00-01-02-03-04-05 (MAC Address)
Console#

```

show lldp info statistics

このスイッチに接続されている LLDP が有効なすべてのデバイスの統計を表示します。

文法

show lldp info statistics [detail interface]

- *detail* — 詳細情報を表示
- *interface*
 - ethernet *unit/port*
 - *unit* — ユニット番号 "1"
 - *port* — ポート番号 (範囲: 1-26)
 - port-channel *channel-id* (範囲: 1-12)

コマンドモード

Privileged Exec

例

```
Console#show lldp info statistics

LLDP Device Statistics

Neighbor Entries List Last Updated : 0 seconds
New Neighbor Entries Count          : 0
Neighbor Entries Deleted Count      : 0
Neighbor Entries Dropped Count      : 0
Neighbor Entries Ageout Count       : 0

Port      NumFramesRecvd  NumFramesSent  NumFramesDiscarded
-----
Eth 1/1    0                0                0
Eth 1/2    0                0                0
Eth 1/3    0                0                0
Eth 1/4    0                0                0
Eth 1/5    0                0                0
.
.
.
Console#
```


4.23 DNS (Domain Name Server)

本コマンドは DNS(Domain Naming System) サービスの設定を行ないます。ドメイン名と IP アドレスのマッピングを行なう DNS テーブルの手動での設定を行なえる他、デフォルトドメイン名の設定又はアドレス変換を行なうための複数のネームサーバの指定を行なうことができます。

DNS は "ip name-server" コマンドを使用し最低 1 つのネームサーバを指定しなければ有効にすることはできません。また、ドメインルックアップは " ip domain-lookup" コマンドにより有効にします

コマンド	機能	モード	ページ
ip domain-list	不完全なホスト用のデフォルトドメイン名リストの設定	GC	P844
ip domain-lookup	DNS によるホスト名→アドレス変換の有効化	GC	P845
ip domain-name	不完全なホスト用のデフォルトドメイン名の設定	GC	P846
ip host	静的 IPv4 ホスト名からアドレスへのマッピングを作成	GC	P847
ip name-server	ホスト名→アドレス変換のための 1 つ又は複数のネームサーバの指定	GC	P848
ipv6 host	Creates a static IPv6 host name-to-address mapping	GC	P849
clear dns cache	DNS キャッシュのエントリのクリア	PE	P849
clear host	ホスト名→アドレステーブルからのエントリの削除	PE	P846
show dns	DNS サービスの設定の表示	PE	P850
show dns cache	DNS キャッシュのエントリの表示	PE	P851
show hosts	静的ホスト名→アドレスマッピングテーブルの表示	PE	P852

コマンドラインインタフェース

DNS (Domain Name Server)

ip domain-list

このコマンドは、不完全なホスト名に追加するドメイン名のリストを設定します。"no" を前に置くことでリストからドメイン名を削除します。

文法

ip domain-list *name*

no ip domain-list *name*

- *name* — ホスト名。ドメイン名とホスト名の間のドット (.) は入力しないで下さい (設定範囲：1-68 文字)

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- ドメイン名はリストの最後に追加されます。
- 本機の DNS サーバが不完全なホスト名を受信し、ドメイン名リストが指定された場合、本機は追加するリスト内の各ドメイン名をホスト名に加え、一致する特定のネームサーバを確認して、ドメインリストにより動作します。
- ドメインリストがない場合、デフォルトドメイン名が使用されます。ドメインリストがある場合には、デフォルトドメイン名は使用されません。

例

本例では、現在のリストに 2 つのドメイン名を追加し、その後リストを表示しています。

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
Console#
```

関連するコマンド

ip domain-name (P846)

ip domain-lookup

DNS ホスト名・アドレス変換を有効にします。"no" を前に置くことで DNS を無効にします。

文法

```
ip domain-lookup
no ip domain-lookup
```

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- DNS を有効にする前に最低 1 つのネームサーバを指定する必要があります。
- すべてのネームサーバが削除された場合には DNS は自動的に無効になります。

例

本例では、DNS を有効にし、設定を表示しています。

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

関連するコマンド

ip domain-name (P846)
ip name-server (P848)

コマンドラインインタフェース

DNS (Domain Name Server)

ip domain-name

不完全なホスト名に追加するデフォルトドメイン名を設定します。

"no" を前に置くことでドメイン名を削除します。

文法

ip domain-name *name*

no ip domain-name

- *name* — ホスト名。ドメイン名とホスト名の間のドット (.) は入力しないで下さい
(設定範囲：1-127 文字)

初期設定

なし

例

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Disabled
Default Domain Name:
    sample.com
Domain Name List:
Name Server List:
Console#
```

関連するコマンド

ip domain-list (P844)

ip name-server (P848)

ip domain-lookup (P845)

ip host

ホスト名を IPv4 アドレスへマップする DNS テーブルに、静的エントリを作成します。
"no" を前に置くことでエントリを削除します。

文法

ip host *name address*

no ip host *name address*

- *name* — ホスト名（設定範囲：1-100 文字）
- *address* — 対応する IPv4 アドレス

初期設定

静的エントリなし

コマンドモード

Global Configuration

コマンド解説

サーバや他のネットワーク機器は複数の IP アドレスによる複数接続をサポートしています。
2 つ以上の IP アドレスを静的テーブルやネームサーバからの応答によりホスト名と関連付けする場合、DNS クライアントは接続が確立するまで各アドレスに接続を試みます。

例

2 つのアドレスをホスト名にマッピングしています。

```
Console(config)#ip host rd5 192.168.1.55
Console(config)#end
Console#show host
No.   Flag Type      IP Address          TTL   Domain
-----
0     2 Address 192.168.1.55          rd5
Console#
```

コマンドラインインタフェース

DNS (Domain Name Server)

ip name-server

ドメイン名解決のために 1 つ又は複数のドメインネームサーバのアドレスを指定します。
"no" を前に置くことでリストからネームサーバを削除します。

文法

ip name-server *server-address1* [*server-address2* ... *server-address6*]

no ip name-server *server-address1* [*server-address2* ... *server-address6*]

- *server-address1* — ドメインネームサーバの IP アドレス
- *server-address2* ... *server-address6* — ドメインネームサーバの IP アドレス (追加分)

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

応答を受信するまで、又はリストの最後に到達するまで、リスト内のネームサーバに対して順番にリクエストを送信します。

例

応答を受信するまで、又はリストの最後に到達するまで、リスト内のネームサーバに対して順番にリクエストを送信します。

```
Console(config)#ip name-server 192.168.1.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
192.168.1.55
10.1.0.55
Console#
```

関連するコマンド

ip domain-name (P846)

ip domain-lookup (P845)

ipv6 host

ホスト名を IPv6 アドレスへマップする、DNS テーブルの静的エントリを作成します。"no" を前に置くことでエントリを削除します。

文法

ipv6 host *name* *ipv6-address*

no ip host *name* *address*

- *name* — ホスト名（設定範囲：1-100 文字）
- *ipv6-address* — 対応する IPv6 アドレス。このアドレスは、RFC2373 “IPv6 Addressing Architecture” に従ってフォーマットされなくてはなりません。8 つの 16 ビット 16 進数をコロンで区切った値を使用します。アドレス内の不適格なフィールドを満たす為に必要とされるゼロの適切な数を示すため、1 つのダブルコロンが使用されます。

初期設定

静的エントリなし

コマンドモード

Global Configuration

例

This example maps an IPv6 address to a host name.

```
Console(config)#ipv6 host rd5 2001:0:0db8:1::12
Console(config)#end
Console#show host
No.   Flag Type      IP Address          TTL   Domain
-----
0     2 Address 2001:0:DB8:1::12    rd5
Console#
```

clear dns cache

DNS キャッシュのすべての値をクリアします。

コマンドモード

Privileged Exec

例

```
Console#clear dns cache
Console#show dns cache
NO      FLAG      TYPE      IP      TTL      DOMAIN
Console#
```

コマンドラインインタフェース

DNS (Domain Name Server)

clear host

DNS テーブルのエントリを削除します。

文法

clear host {*name* | *}

- *name* — ホスト名（設定範囲：1-100 文字）
- * — すべてのエントリを削除

初期設定

なし

コマンドモード

Privileged Exec

例

本例ではすべての DNS テーブルのエントリを削除しています。

```
Console#clear host *
Console#
```

show dns

DNS サーバの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```


show dns cache

DNS キャッシュの内容を表示します。

コマンドモード

Privileged Exec

例

```

Console#show dns cache
No.      Flag      Type      IP Address      TTL      Domain
-----
      3        4   Host      209.131.36.158   115     www-real.wal.b.yahoo.com
      4        4  CNAME      POINTER TO:3     115     www.yahoo.com
      5        4  CNAME      POINTER TO:3     115     www.wal.b.yahoo.com
Console#
  
```

項目	解説
NO	各リソースレコードのエントリ番号
FLAG	キャッシュエントリのフラグは常に "4"
TYPE	標準的又はプライマリ名が指定された「CNAME」、既存のエントリと同じ IP アドレスをマッピングされている多数のドメイン名が指定された「ALIAS」
IP Address	レコードに関連した IP アドレス
TTL	ネームサーバにより報告された生存可能時間
DOMAIN	レコードに関連するドメイン名

コマンドラインインタフェース

DNS (Domain Name Server)

show hosts

静的ホスト名-アドレスマッピングテーブルを表示します。

コマンドモード

Privileged Exec

例

以前に設定されたエントリと同じアドレスがマッピングされた場合、ホスト名はエイリアスとして表示されます。

```
Console(config)#ipv6 host rd6 2001:0db8:1::12
Console(config)#end
Console# show host
No.   Flag Type      IP Address          TTL   Domain
-----
0     2 Address 192.168.1.55         rd5
1     2 Address 2001:DB8:1::12      rd6
Console#
```

項目	解説
NO	各リソースレコードのエントリ番号
FLAG	静的エントリのフラグは "2"、またはキャッシュに保存される動的エントリは "4"
TYPE	オーナーのプライマリ名を指定する "Address" を含み、既存のエントリに IP アドレスと同様にマップされる複数のドメイン名（またはエイリアス）を指定する "CHAME"
IP Address	レコードに関連した IP アドレス
TTL	ネームサーバにより報告された生存可能時間
DOMAIN	レコードに関連するドメイン名

4.24 DHCP

以下のコマンドは、Dynamic Host Configuration Protocol (DHCP) クライアント機能の設定を行うために使用します。

コマンドグループ	機能	ページ
DHCP Client	インタフェースが動的に IP アドレス情報を取得することを可能にします	P853

4.24.1 DHCP クライアント

スイッチの VLAN インタフェースが動的に IP アドレス情報を取得することを可能にします。

[注意] 現在のソフトウェアリリースでは、IP アドレスプレフィックスの DHCPv6 状態を持つ設定はサポートされていません。もし、ルータアダプタイズメントが " other stateful configuration" フラグセットを持つ場合、スイッチは DHCPv6 サーバから、その他の非アドレス設定情報（デフォルトゲートウェイ等）を獲得しようと試みます。

コマンド	機能	モード	ページ
<i>IPv4 DHCP</i>			
ip dhcp client class-id	インタフェースの DHCP クライアント識別子を指定	IC	P854
ip dhcp restart client	BOOTP または DHCP クライアントリクエストを受け入れ	PE	P855
<i>IPv6 DHCP</i>			
ipv6 dhcp restart client vlan	DHCPv6 クライアントリクエストを受け入れ	PE	P856
show ipv6 dhcp duid	スイッチの DHCP の一意な識別子を表示	PE	P857
show ipv6 dhcp vlan	指定したインタフェースの DHCPv6 情報を表示	PE	P857

ip dhcp client class-id

現在のインタフェースの DHCP クライアントベンダクラス識別子を指定します。"no" を使用することで識別子を削除します。

文法

ip dhcp client class-id { *text text* | *hex hex* }

no ip dhcp client class-id

- *text* — テキストストリング（範囲：1-32 文字）
- *hex* — 16 進数値

初期設定

なし

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- サーバは TFTP サーバ名とブートファイルを含むオプション 66 属性を要約したオプション 43 情報で返答します。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

関連するコマンド

ip dhcp restart client (P855)

ip dhcp restart client

BOOTP または DHCP クライアントリクエストを適用します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- "ip address" コマンドで、BOOTP または DHCP モードにセットされている IP インタフェースに BOOTP または DHCP クライアントリクエストを発行します。
- DHCP はサーバーに、利用可能な場合にクライアントの前のアドレスを再割り当てするよう要求します。
- BOOTP または DHCP サーバが別のドメインへ移動された場合、クライアントに提供されるアドレスのネットワーク部は新しいドメインを基にします。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console(config)#ex
Console#ip dhcp restart client
Console#show ip interface
Vlan 1 is Administrative Up - Link Up
  Address is 00-12-CF-F3-DE-46 (via 00-12-CF-F3-DE-46)
  Index: 1001, MTU: 1500, Bandwidth: 1g
  Address Mode is DHCP
  IP Address: 192.168.0.9 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

関連するコマンド

ip address (P859)

ipv6 dhcp restart client vlan

DHCPv6 クライアントリクエストを提出します。

文法

ipv6 dhcp restart client vlan *vlan-id*

- *vlan-id* — VLAN ID（範囲：1-4093）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- DHCP クライアントプロセスが有効で、プレフィックスの獲得に成功したら、プレフィックスは IPv6 通常プレフィックスプールに保存されます。他のコマンドとアプリケーション（ipv6 アドレスコマンドなど）は、通常プレフィックスプールでプレフィックスを参照することができます。
- DHCPv6 クライアントは、DNS サーバアドレスのような個々のクライアントの動的状態を保持する必要がないパラメータの設定もリクエストすることができます。

例

```
Console#ipv6 dhcp restart client vlan 1
Console#
```

関連するコマンド

ipv6 address (P868)

show ipv6 dhcp duuid

スイッチの DHCP 一意の識別子を表示します。

コマンドモード

Privileged Exec

コマンド解説

- DHCPv6 クライアントとサービスは、クライアント識別子とサーバー識別子オプションを含む、DHCP Unique Identifier (DUID) によって識別されます。静的または動的アドレスプレフィックスは、クライアントの DUID を基に DHCPv6 サーバによって割り当てられます。

例

```
Console#show ipv6 dhcp duuid
DHCPv6 Unique Identifier (DUID): 0001-0001-4A8158B4-00E00C0000FD
Console#
```

show ipv6 dhcp vlan

指定されたインタフェースの DHCPv6 情報を表示します。

文法

show ipv6 dhcp vlan *vlan-id*

- *vlan-id* — VLAN ID (範囲：1-4093)

コマンドモード

Privileged Exec

例

```
Console#show ipv6 dhcp vlan 1
VLAN 1 is in DHCP client mode, Rapid-Commit
List of known servers:
  Server address : FE80::250:FCFF:FEF9:A494
  DUID           : 0001-0001-48CFB0D5-F48F2A006801

  Server address : FE80::250:FCFF:FEF9:A405
  DUID           : 0001-0001-38CF5AB0-F48F2A003917
Console#
```

4.25 IP インタフェース

IP アドレスは本機へのネットワーク経由での管理用アクセスの際に使用されます。初期設定では DHCP を使用して IP アドレスの取得を行う設定になっています。IP アドレスは手動で設定することも、又 BOOTP/DHCP サーバから電源投入時に自動的に取得することもできます。また、他のセグメントから本機へのアクセスを行うためにはデフォルトゲートウェイの設定も必要となります。

初期設定では、本機の VLAN1 の IPv4 アドレスは DHCP 経由で取得されます。また、本装置と異なるネットワークセグメントにある管理ステーション間の、IPv4 または IPv6 デフォルトゲートウェイを確立する必要があります。

コマンドグループ	機能	ページ
IPv4 Interface	スイッチの IPv4 アドレスを設定	P858
ARP Configuration	静的、動的、プロキシ ARP サービスの設定	P864
IPv6 Interface	スイッチの IPv6 アドレスを設定	P866

4.25.1 IPv4 インタフェース設定

コマンド	機能	モード	ページ
ip address	本機への IP アドレスの設定	IC	P859
ip default-gateway	本機と管理端末を接続するためのゲートウェイ設定の表示	GC	P860
show ip default-gateway	本機のデフォルトゲートウェイ設定の表示	PE	P860
show ip interface	本機の IP 設定の表示	PE	P861
traceroute	パケットが指定されたホストに取るルートを表示	PE	P862
ping	ネットワーク上の他のノードへの ICMP echo リクエストパケットの送信	NE,PE	P863

ip address

本機への IP アドレスの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

ip address [*ip-address netmask* | bootp | dhcp]

no ip address

- *ip-address* — IP アドレス
- *netmask* — サブネットマスク
- bootp — IP アドレスを BOOTP から取得します。
- dhcp — IP アドレスを DHCP から取得します。

初期設定

DHCP クライアント

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 管理用にネットワーク経由で本機へアクセスする場合、IP アドレスの設定が必須となります。手動で IP アドレスを入力する方法と、BOOTP、DHCP を使用して自動で IP アドレスを取得する方法があります。
- bootp 又は dhcp を選択した場合、BOOTP 又は DHCP からの応答があるまで IP アドレスは設定されません。IP アドレスを取得するためのリクエストは周期的にブロードキャストで送信されます (BOOTP 及び DHCP によって取得できるのは IP アドレス、サブネットマスク及びデフォルトゲートウェイの値です)
BOOTP 又は DHCP に対するブロードキャストリクエストは "ip dhcp restart" コマンドを使用するか、本機を再起動させた場合に行われます。

例

本例では、VLAN 1 に対して IP アドレスを設定しています。

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

関連するコマンド

ip dhcp restart client (P855)

ipv6 address (P868)

ip default-gateway

セグメントがわかれたスイッチと管理端末を接続するためのデフォルトゲートウェイの設定を行います。"no" を前に置くことでデフォルトゲートウェイを削除します。

文法

ip default-gateway *gateway*
no ip default-gateway

- *gateway* — デフォルトゲートウェイの IP アドレス

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

異なるセグメントに管理端末が設置されている場合には必ず設定する必要があります。

例

本例ではデフォルトゲートウェイの設定を行っています。

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

関連するコマンド

ipv6 default-gateway (P867)

show ip default-gateway

デフォルトゲートウェイの設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show ip default-gateway
ip default gateway 10.1.0.254
Console#
```

関連するコマンド

show ipv6 default-gateway (P876)

show ip interface

IP インタフェースの設定を表示します。

初期設定

すべてのインタフェース

コマンドモード

Privileged Exec

例

```
Console#show ip interface
Vlan 1 is Administrative Up - Link Down
  Address is 00-12-CF-F3-DE-46 (via 00-12-CF-F3-DE-46)
  Index: 1001, MTU: 1500, Bandwidth: 1g
  Address Mode is User specified
  IP Address: 192.168.1.1 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

関連するコマンド

ip address (P859)

show ipv6 interface (P877)

traceroute

This command shows the route packets take to the specified destination.

文法

traceroute *host*

- *host* — IP アドレスまたはホストエイリアス

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- "traceroute" コマンドは指定されたディスティネーションへの到達に取るパスを決定するために使用されます。

例

```
Console#traceroute 192.168.0.1
Press "ESC" to abort.

Source address:      192.168.0.9
Destination address: 192.168.0.1

Hop    IP Address      Packet 1      Packet 2      Packet 3
-----
  1    192.168.0.1    <10 ms       <10 ms       <10 ms

Trace completed.
Console#
```

ping

ネットワーク上の他のノードに対し ICMP echo リクエストパケットを送信します。

文法

ping *host* { *count count* } { *size size* }

- *host* — ホストの IP アドレス / エイリアス
- *count* — 送信するパケット数 (範囲: 1-16、初期設定: 5)
- *size* — パケットのサイズ (bytes) (範囲 32-512、初期設定: 32)
ヘッダ情報が付加されるため、実際のパケットサイズは設定した値より 8bytes 大きくなります。

初期設定

Count: 5

Size: 32bytes

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- ping コマンドを使用することでネットワークの他の場所 (端末など) に接続されているか確認することができます。
- ping コマンドの結果は以下のような内容となります:
 - Normal response — 正常なレスポンスは、ネットワークの状態に依存して、1 ~ 10 秒で生じます
 - Destination does not respond — ホストが応答しない場合、"timeout" が 10 秒以内に表示されます
 - Destination unreachable — 目的のホストに対するゲートウェイが見つからない場合
 - Network or host unreachable — ゲートウェイが目的となるルートテーブルを見つけれない場合
- < ESC > キーを押すと Ping が中断されます。

例

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
Ping statistics for 10.1.0.9:
5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
Minimum = 10 ms, Maximum = 20 ms, Average = 10 ms
Console#
```

関連するコマンド

interface (P602)

4.25.2 ARP 設定

arp timeout	動的エントリが ARP キャッシュに残る時間を設定	GC	P864
clear arp-cache	ARP キャッシュから全ての動的エントリを削除	PE	P865
show arp	ARP キャッシュを表示	NE,PE	P860

arp timeout

Address Resolution Protocol (ARP) キャッシュの動的エントリのエージングタイムを設定します。"no" を前に置くことで、タイムアウトを初期値に戻します。

文法

arp timeout *seconds*

no arp timeout

- *seconds* — 動的エントリが ARP キャッシュに残る時間（範囲：300-86400 秒）

初期設定

1200 秒（20 分）

コマンドモード

Global Configuration

コマンド解説

- ARP エントリの期限が切れる時、それはキャッシュから削除され、MAC アドレスを再確立するために ARP リクエストパケットが送られます。
- エージングタイムは 動的エントリが、キャッシュにどれだけの間残るかを決定します。タイムアウトが短すぎると、テーブルからアドレスが頻繁にクリアされてしまうため、ルーターが ARP リクエストを繰り返すことによってリソースを消費してしまいます。

例

```
Console(config)#arp timeout 900
Console(config)#
```

clear arp-cache

Address Resolution Protocol (ARP) キャッシュから全ての動的エントリを削除します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp

ARP キャッシュを表示します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 本コマンドは対応する IP アドレス、MAC アドレス、タイプ（動的または other）、VLAN インタフェースを含む、ARP キャッシュについての情報を表示します。エントリタイプ "other" は本機のローカルアドレスを示します。

例

```
Console#show arp

IP Address      MAC Address      Type      Interface
-----
192.168.0.1     00-01-ec-f8-d8-c6  dynamic      1
192.168.0.2     00-12-cf-12-34-56  other        1
192.168.0.3     00-10-b5-62-03-74  dynamic      1

Total entry : 3
Console#
```

4.25.3 IPv6 インタフェース設定

本機は以下の IPv6 インタフェースコマンドをサポートしています。

コマンド	機能	モード	ページ
インタフェースアドレス設定とユーティリティ			
ipv6 default-gateway	トラフィックの IPv6 デフォルトゲートウェイを設定	GC	P867
ipv6 address	IPv6 グローバルユニキャストアドレスの設定と、インタフェースの IPv6 を有効化	IC	P868
ipv6 address autoconfig	インタフェースの IPv6 グローバルユニキャストアドレスの自動設定と、インタフェースの IPv6 有効化	IC	P870
ipv6 address eui-64	ローオーダー 64 ビットの EUI-64 インタフェース ID を使用して、インタフェースの IPv6 グローバルユニキャストアドレスを設定と、インタフェースの IPv6 有効化	IC	P871
ipv6 address link-local	インタフェースの IPv6 リンクローカルアドレスの設定と、インタフェースの IPv6 有効化	IC	P873
ipv6 enable	明示的 IPv6 アドレスで設定されていないインタフェースで IPv6 を有効化	IC	P874
ipv6 mtu	インタフェースに送られる IPv6 パケットの maximum transmission unit (MTU) のサイズを設定	IC	P875
show ipv6 default-gateway	現在の IPv6 デフォルトゲートウェイを表示	NE,PE	P876
show ipv6 interface	ユーザビリティおよび IPv6 インタフェースを表示	NE,PE	P877
show ipv6 mtu	IPv6 インタフェースの maximum transmission unit (MTU) 情報を表示	NE,PE	P879
show ipv6 traffic	IPv6 トラフィックの統計を表示	NE,PE	P880
clear ipv6 traffic	IPv6 トラフィックカウンタをリセット	PE	P885
ping6	ネットワーク上の他のノードに IPv6 ICMP エコーリクエストパケットを送信	PE	P886
近隣探索			
ipv6 nd dad attempts	重複アドレス検出の間に送信する、連続した近隣要請メッセージの数を設定	IC	P887
ipv6 nd ns-interval	インタフェースの IPv6 近隣要請再転送の間の間隔を設定	IC	P889
ipv6 nd reachable-time	いずれかの到達可能性確認イベントが起こった後、リモート IPv6 ノードが到着可能であると推測される時間を設定	IC	P890
clear ipv6 neighbors	IPv6 近隣探索キャッシュの全ての動的エントリを削除	PE	P890
show ipv6 neighbors	IPv6 近隣探索キャッシュの情報を表示	PE	P891

ipv6 default-gateway

送信先が異なるネットワークセグメントにある場合に使用する、IPv6 デフォルトゲートウェイを設定します。"no" を前に置くことで、前に設定されたデフォルトゲートウェイを削除します。

文法

ipv6 default-gateway *ipv6-address*

no ipv6 address

- *ipv6-address* — 送信先が異なるネットワークセグメントにある場合に使用する、デフォルトネクストホップルータの IPv6 アドレス

初期設定

デフォルトゲートウェイは定義されていません。

コマンドモード

Global Configuration

コマンド解説

- 全ての IPv6 アドレスは、RFC2373"IPv6 Addressing Architecture" に従ってフォーマットされなくてはなりません。8 つの 16 ビット 16 進数をコロンで区切った値を使用します。アドレス内の不適格なフィールドを満たす為に必要とされるゼロの適切な数を示すため、1 つのダブルコロンが使用されます。
- 同じリンクローカルアドレスが、異なるゾーンの異なるインタフェース / ノードで使用されます (RFC4007)。従って、リンクローカルアドレスを指定する際、% の後に VLAN 識別子を示すゾーン ID 情報を含みます。
例えば、FE80::7272%1 は Ping が送られるインタフェースとして VLAN1 を識別します。
- 送信先が異なるネットワークセグメントにあり、IPv6 アドレスがアサインされている場合、IPv6 デフォルトゲートウェイを定義する必要があります。
- ゲートウェイに直接接続されているネットワークインタフェースが、スイッチ上に設定された場合、IPv6 デフォルトゲートウェイは設定に成功します。

例

```
Console(config)#ipv6 default-gateway 2009::6780
Console(config)#
```

関連するコマンド

show ipv6 default-gateway (P876)

ip default-gateway (P860)

ipv6 address

IPv6 グローバルユニキャストアドレスの設定と、インタフェースの IPv6 を有効にします。引数無しで "no" を前に置くことで、インタフェースの全ての IPv6 アドレスを削除します。"no" を前に置き IPv6 アドレスを指定することで、インタフェースからこのアドレスを削除します。

文法

[no] ipv6 address *ipv6-address / prefix-length*

- *ipv6-address* — ネットワークプレフィックスとホストアドレスビットを含む、フル IPv6 アドレス。
- *prefix-length* — いくつかの連続的なアドレスのビット（左から）から構成されているかを示す 10 進数値（アドレスのネットワーク部）

初期設定

デフォルトゲートウェイは定義されていません。

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 全ての IPv6 アドレスは、RFC2373"IPv6 Addressing Architecture" に従ってフォーマットされなくてはなりません。8 つの 16 ビット 16 進数をコロンで区切った値を使用します。アドレス内の不適格なフィールドを満たす為に必要とされるゼロの適切な数を示すために 1 つのダブルコロンが使用されます。
- 複数のサブネットを持つ、大きなネットワークに接続する場合、グローバルユニキャストアドレスを設定する必要があります。このアドレスはここで説明するコマンドによって手動で設定するか、" ipv6 address autoconfig" コマンド（P870）を使用して自動で設定することが出来ます。
- リンクローカルアドレスがまだこのインタフェースに割り当てられていない場合、このコマンドは指定した静的グローバルユニキャストアドレスを割り当て、インタフェースのリンクローカルユニキャストアドレスを動的に生成します。（リンクローカルアドレスは FE80 のプレフィックスアドレスと、スイッチの EUI-64 フォーマットで修正された MAC アドレスを基にしたホスト部から作成されます。）
- 重複アドレスが検出された場合、コンソールへ警告メッセージが送られます。

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::72/96
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
    FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
    2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
    FF02::1:FF00:72
    FF02::1:FF00:FD
    FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

関連するコマンド

ipv6 address eui-64 (P871)
ipv6 address autoconfig (P870)
show ipv6 interface (P877)
ip address (P859)

ipv6 address autoconfig

インタフェース上での IPv6 アドレスのステートレスオートネゴシエーションとインタフェースの IPv6 を有効にします。アドレスのネットワーク部は、IPv6 ルータアドバタイズメントメッセージで受信されるプレフィックスを基にします。ホスト部はインタフェース識別子から編集された EUI-64 を基にしています。"no" を前に置くことでこのコマンドで生成されたアドレスを削除します。

文法

ipv6 address autoconfig
no ipv6 address autoconfig

初期設定

IPv6 アドレスは定義されていません。

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ・ リンクローカルアドレスがまだこのインタフェースに割り当てられていない場合、このコマンドは指定した静的グローバルユニキャストアドレスを割り当て、インタフェースのリンクローカルユニキャストアドレスを動的に生成します。(リンクローカルアドレスは FE80 のプレフィックスアドレスと、スイッチの EUI-64 フォーマットで修正された MAC アドレスを基にしたホスト部から作成されます。)
- ・ 重複アドレスが検出された場合、コンソールへ警告メッセージが送られます。
- ・ ルータアドバタイズメントが "other stateful configuration" フラグセットを持つ場合、スイッチは他の非アドレス設定情報を獲得しようと試みます (デフォルトゲートウェイ等)

例

```
Console(config-if)#ipv6 address autoconfig
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7272:2E0:CFF:FE00:FD/64, subnet is 2001:DB8:2222:7272::/
  64 [AUTOCONFIG]
    valid lifetime 2591628 preferred lifetime 604428
Joined group address(es):
  FF02::1:FF00:FD
  FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

関連するコマンド

ipv6 address (P868)
show ipv6 interface (P877)

ipv6 address eui-64

ローオーダー 64 ビットの EUI-64 インタフェース ID を使用するインタフェースの、IPv6 アドレスを設定し、インタフェース上で IPv6 を有効にします。引数無しで "no" を前に置くことで、インタフェースから、手動設定された全ての IPv6 アドレスを削除します。"no" を前に置き IPv6 アドレスを指定することで、インタフェースからこのアドレスを削除します。

文法

ipv6 address *ipv6-prefix / prefix-length* eui-64
no ipv6 address [*ipv6-prefix / prefix-length* eui-64]

- *ipv6-prefix* — インタフェースにアサインされたアドレスの IPv6 ネットワーク部
- *prefix-length* — いくつかの連続的なアドレスのビット（左から）から構成されているかを示す 10 進数値（アドレスのネットワーク部）

初期設定

IPv6 アドレスは定義されていません。

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- プレフィックスは、RFC2373"IPv6 Addressing Architecture" に従ってフォーマットされなくてはなりません。8 つの 16 ビット 16 進数をコロンで区切った値を使用します。アドレス内の不適格なフィールドを満たす為に必要とされるゼロの適切な数を示すため、1 つのダブルコロンが使用されます。
- リンクローカルアドレスがまだこのインタフェースに割り当てられていない場合、このコマンドは指定した静的グローバルユニキャストアドレスを割り当て、インタフェースのリンクローカルユニキャストアドレスを動的に生成します。（リンクローカルアドレスは FE80 のプレフィックスアドレスと、スイッチの EUI-64 フォーマットで修正された MAC アドレスを基にしたホスト部から作成されます。）
- IPv6 プレフィックスで指定された値は、指定されたプレフィックス長が 64 ビット以下の場合、ハイオーダーホストビットの幾つかを含むことにご注意ください。指定されたプレフィックス長が 64 ビットを超える場合、アドレスのネットワーク部はインタフェース識別子より優先されます。
- 重複アドレスが検出された場合、コンソールへ警告メッセージが送られます。
- IPv6 アドレスの長さは 16 バイトで、最下位 8 バイトが一般に装置の MAC アドレスに基づいてユニークなホスト識別子を形成します。EUI-64 仕様は拡張された 8 バイト MAC アドレスを使用するデバイスのために設計されています。依然 6 バイト MAC アドレス（EUI-48 フォーマットとして知られる）を使用するデバイスのため、それはアドレスのユニバーサル / ローカルビットを反転し、上下の MAC アドレスの 3 バイトの間に 16 進数 FFFE を挿入することによって、EUI-64 フォーマットに変換されなくてはなりません。
例えば、もしデバイスが 28-9F-18-1C-82-35 の EUI-48 アドレスを持つ場合、グローバル / ローカルビットは 28 を 2A に変えている EUI-64 必要条件を満たす為、最初に反転されなくてはなりません。そして、2 バイト FFFE が OUI（Organizationally

コマンドラインインタフェース

IP インタフェース

Unique Identifier または Company Identifier) の間に挿入され、残りのアドレスが、2A-9F-18-FF-FE-1C-82-35 のモディファイド EUI-64 インタフェース識別子を結果としてもたします。

- インタフェース異なるサブネットに付属する限り、このホストアドレッシングメソッドは、同じインタフェース識別子が1つのデバイスの複数の IP インタフェースに使用されることを可能にします。

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
    FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
    2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/
64[EUI]
    2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
    FF02::1:FF00:72
    FF02::1:FF00:FD
    FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

関連するコマンド

ipv6 address autoconfig (P870)

show ipv6 interface (P877)

ipv6 address link-local

インタフェースの IPv6 リンクローカルアドレスを設定し、インタフェース上の IPv6 を有効にします。引数無しで "no" を前に置くことで、インタフェースから、手動設定された全ての IPv6 アドレスを削除します。"no" を前に置き IPv6 アドレスを指定することで、インタフェースからこのアドレスを削除します。

文法

ipv6 address *ipv6-address* **link-local**

no ipv6 address [*ipv6-address* **link-local**]

- *ipv6-address* —インタフェースにアサインされる IPv6 アドレス

初期設定

IPv6 アドレスは定義されていません。

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 指定されるアドレスは、RFC2373"IPv6 Addressing Architecture" に従ってフォーマットされなくてはなりません。8 つの 16 ビット 16 進数をコロンで区切った値を使用します。アドレス内の不適格なフィールドを満たす為に必要とされるゼロの適切な数を示すため、1 つのダブルコロンが使用され、アドレスプレフィックスは FE80 になります。
- このコマンドで指定されたアドレスは、インタフェースに自動で生成されたリンクローカルアドレスを置き換えます。
- インタフェースごとに複数の IPv6 グローバルユニキャストアドレスを設定できますが、インタフェースに付きリンクローカルアドレスは 1 つのみです。
- 重複アドレスが検出された場合、コンソールへ警告メッセージが送られます。

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::269:3EF9:FE19:6779/64
Global unicast address(es):
  2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
  FF02::1:FF19:6779
  FF02::1:FF00:72
  FF02::1:FF00:FD
  FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
Console#
```

関連するコマンド

ipv6 enable (P874)

show ipv6 interface (P877)

ipv6 enable

明示的 IPv6 アドレスで設定されていないインタフェース上で IPv6 を有効にします。"no" を前に置くことで、明示的 IPv6 アドレスで設定されていないインタフェース上で IPv6 を無効にします。

文法

ipv6 enable
no ipv6 enable

初期設定

無効

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- このコマンドは、現在の VLAN インタフェースで IPv6 を有効にし、自動的にリンクローカルユニキャストアドレスを生成します。アドレスプレフィックスは FE80 を使用し、アドレスのホスト部はスイッチの MAC アドレスを modified EUI-64 形式 (P871) に変換することによって生成されます。このアドレスタイプは同じローカルサブネットに付属する全てのデバイスのために、IPv6 上でのスイッチのアクセスを可能にします。
- 重複アドレスが検出された場合、コンソールへ警告メッセージが送られます。
- "no ipv6 enable" コマンドは、IPv6 アドレスで明示的に設定されたインタフェースの IPv6 を無効にしません。

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
    FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
    2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
    FF02::1:FF00:72
    FF02::1:FF00:FD
    FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

関連するコマンド

ipv6 address link-local (P873)
show ipv6 interface (P877)

ipv6 mtu

インタフェースで送られる IPv6 パケットの maximum transmission unit (MTU) のサイズを設定します。"no" を前に置くことで初期設定に戻します。

文法

ipv6 mtu *size*

no ipv6 mtu

- *size* —MTU サイズを指定（範囲：1280-65535 bytes）

初期設定

1500bytes

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- IPv6 ルータは、他のルータから転送された IPv6 パケットをフラグメントしませんが、IPv6 ルータへ接続されているエンドステーションから始まっているトラフィックはフラグメントします。
- 同じ物理媒体上の全ての装置は正確に稼動するために同じ MTU を使用します。
- MTU をセットする前に、インタフェースで IPv6 を有効にします。

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mtu 1280
Console(config-if)#
```

関連するコマンド

show ipv6 mtu (P879)

jumbo frame (P386)

コマンドラインインタフェース

IP インタフェース

show ipv6 default-gateway

現在の IPv6 デフォルトゲートウェイを表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show ipv6 default-gateway
IPv6 default gateway 2001:DB8:2222:7272::254

Console#
```

show ipv6 interface

このコマンドは、設定された IPv6 インタフェースを表示します。

文法

show ipv6 interface [brief [vlan *vlan-id* [*ipv6-prefix* / *prefix-length*]]]

- *brief* — IPv6 オペレーショナルステータスとそれぞれのインタフェースに設定されたアドレスの短い要約を表示
- *vlan-id* — VLAN ID（範囲：1-4093）
- *ipv6-prefix* — インタフェースにアサインされたアドレスの IPv6 ネットワーク部。プレフィックスは、RFC2373"IPv6 Addressing Architecture" に従ってフォーマットされなくてはなりません。8 つの 16 ビット 16 進数をコロンで区切った値を使用します。アドレス内の不適格なフィールドを満たす為に必要とされるゼロの適切な数を示すために 1 つのダブルコロンが使用されます。
- *prefix-length* — いくつかの連続的なアドレスのビット（左から）から構成されているかを示す 10 進数値（アドレスのネットワーク部）

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
  FF02::1:FF00:72
  FF02::1:FF00:FD
  FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

コマンドラインインタフェース

IP インタフェース

Ipv6 インタフェースの表示

項目	解説
VLAN	スイッチがこのインタフェースでパケットの送受信が行える時、"UP" がマークされます。ラインシグナルが無い時に "down"、またはインタフェースが管理者によって無効にされている時 "administratively down" がマークされます。
IPv6	スイッチがこのインタフェースで IP トラフィックの送受信を行える時、IPv6 は "enable" がマークされます。スイッチがインタフェースで IP トラフィックの送受信を行えない時は "disable" または、インタフェース上で重複アドレスが検出された時に "stalled" がマークされます。
Link-local address	このインタフェースに割り当てられているリンクローカルアドレスを表示
Global unicast address(es)	このインタフェースに割り当てられているグローバルユニキャストアドレスを表示
Joined group address(es)	インタフェースに割り当てられたユニキャストアドレスに加え、ホストはまた、全てのノードのマルチキャストアドレス FF01::1 (インタフェース - ローカル範囲) および FF02::1 (リンクローカル範囲) を聴取する必要があります。
ND DAD	(近隣探索) 重複アドレス検索が有効か無効かを示します。
number of DAD attempts	重複アドレス検索の間に、インタフェースで送られる連続する近隣要請メッセージの数
ND retransmit interval	重複アドレス検索の間に、インタフェースで送られる IPv6 近隣要請再送の間隔

この例はスイッチ上に設定された IPv6 アドレスの簡単なまとめを表示しています。

Console#show ipv6 interface brief			
Interface	VLAN	IPv6	IPv6 Address

VLAN 1	Up	Up	2001:DB8:2222:7273::72/96
VLAN 1	Up	Up	FE80::2E0:CFF:FE00:FD%1/64
Console#			

関連するコマンド

show ip interface (P861)

show ipv6 mtu

受容可能な MTU と共に、IGMP packet-too-big メッセージを本機に返す送信先の maximum transmission unit (MTU) キャッシュを表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show ipv6 mtu
MTU      Since      Destination Address
1400     00:04:21     5000:1::3
1280     00:04:50     FE80::203:A0FF:FED6:141D
Console#
```

IPv6 MTU の表示

項目	解説
MTU	この目的地から返させる ICMP "packet-too-big" メッセージに含まれる、調整された MTU
Since	ICMP "packet-too-big" メッセージがこの目的地から受信されてからの時間
Destination Address	ICMP "packet-too-big" メッセージが送られたアドレス

※スイッチに IPv6 アドレスが割り当てられていない場合、これらの情報は表示されません。

show ipv6 traffic

このスイッチを通過する、IPv6 トラフィックについての統計を表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received
    total received
    header errors
    too big errors
    no routes
    address errors
    unknown protocols
    truncated packets
    discards
    delivers
    reassembly request datagrams
    reassembled succeeded
    reassembled failed
IPv6 sent
    forwards datagrams
    15 requests
    discards
    no routes
    generated fragments
    fragment succeeded
    fragment failed
ICMPv6 Statistics:
ICMPv6 received
    input
    errors
    destination unreachable messages
    packet too big messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
    redirect messages
    group membership query messages
    group membership response messages
    group membership reduction messages
    router solicit messages
    router advertisement messages
    neighbor solicit messages
    neighbor advertisement messages
    redirect messages
```

(続く)

```
(続き)
ICMPv6 sent
    15 output
        destination unreachable messages
        packet too big messages
        time exceeded messages
        parameter problem message
        echo reply messages
    7 router solicit messages
    3 neighbor solicit messages
        neighbor advertisement messages
        redirect messages
        group membership response messages
        group membership reduction messages
UDP Statistics:
    neighbor advertisement messages
    redirect messages
    group membership response messages
    group membership reduction messages
UDP Statistics:
    input
    no port errors
    other errors
    output
Console#
```

IPv6 トラフィック

項目	解説
IPv6 統計の表示	
IPv6 受信	
total received	エラーで受信したものも含め、インタフェースで受信した入力データグラムの総数。
header errors	IPv6 ヘッダのエラーが原因で破棄された入力データグラムの数。バージョン番号の不一致、その他のフォーマットエラー、ホップ数の許容値超過、IPv6 オプションの処理で検出されたエラーなどが含まれます。
too big errors	サイズが送信インタフェースのリンク MTU を超えたために転送できなかった受信データグラムの数。
no routes	送信先に送信するためのルートが検出されなかったために破棄された入力データグラムの数。
address errors	IPv6 ヘッダの送信先フィールド内の IPv6 アドレスがこのエンティティで受信できる有効なアドレスでなかったために破棄された入力データグラムの数。このカウントには、無効なアドレス (::0 など) およびサポートされていないアドレス (未割り当てのプレフィックスを持つアドレスなど) も含まれます。IPv6 ルーターではなく、そのためにデータグラムを転送しないエンティティについては、このカウンタの値には破棄されたデータグラムの数も含まれます。送信先アドレスがローカルアドレスではなかったからです。

コマンドラインインタフェース

IP インタフェース

IPv6 トラフィック

unknown protocols	正常に受信したものの、プロトコルが不明であるか、サポートされていないことが原因で破棄されたローカルアドレス指定のデータグラムの数。このカウンタは、これらのデータグラムの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のデータグラムにとっては必ずしも入力インタフェースではない場合もあります。
truncated packets	データグラムフレームのデータ量が足りなかったために破棄された入力データグラムの数。
discards	処理の継続を妨げるような問題が発生していないにもかかわらず（バッファ領域の不足などの理由で）破棄された入力 IPv6 データグラムの数。このカウンタの値には、再構成の待機中に破棄されたデータグラムの数は含まれません。
delivers	IPv6 ユーザープロトコルに正常に送信されたデータグラムの総数（ICMP を含む）。このカウンタは、これらのデータグラムの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のデータグラムにとっては必ずしも入力インタフェースではない場合もあります。
reassembly request datagrams	このインタフェースで再構成される必要がある、受信した IPv6 フラグメントの数。このカウンタは、これらのフラグメントの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のフラグメントにとっては必ずしも入力インタフェースではない場合もあります。
reassembled succeeded	正常に再構成された IPv6 データグラムの数。このカウンタは、これらのデータグラムの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のフラグメントにとっては必ずしも入力インタフェースではない場合もあります。
reassembled failed	IPv6 再構成アルゴリズムによって検出されたエラーの数（タイムアウトなど、エラーの種類は問いません）。アルゴリズムによっては（特に RFC 815 内のアルゴリズム）フラグメントを受信時に結合してしまい、その数を追跡できないため、この値は必ずしも破棄された IPv6 フラグメントの数であるとは限りません。このカウンタは、これらのフラグメントの宛先のインタフェースでインクリメントされます。宛先のインタフェースは、一部のフラグメントにとっては必ずしも入力インタフェースではない場合もあります。
IPv6 送信	
forwards datagrams	このエンティティが受信し、最終送信先に転送した出力データグラムの数。IPv6 ルーターとして動作しないエンティティでは、このカウンタの値には、このエンティティを介して Source-Route（送信元ルート指定）され、Source-Route が適切に処理されたパケットの数のみが含まれます。正常に転送されたデータグラムの場合は、出力インタフェースのカウンタがインクリメントされます。

IPv6 トラフィック

requests	ローカル IPv6 ユーザプロトコル (ICMP を含む) がトランスミッションの要請で IPv6 に供給した pv6 データグラムの総数 "ipv6IfStatsOutForwDatagrams" でカウントされるデータグラムはこのカウンタに含まれません。
discards	処理の継続を妨げるような問題が発生していないにもかかわらず (バッファ領域の不足などの理由で) 破棄された入力 IPv6 データグラムの数。
no routes	送信先に送信するためのルートが検出されなかったために破棄された入力データグラムの数。
generated fragments	この出力インタフェースで行われたフラグメント化によって生成された出力データグラムフラグメントの数。
fragment succeeded	この出力インタフェースで正常にフラグメント化された IPv6 データグラムの数。
fragment failed	このインタフェースでフラグメント化できなかった出力データグラムの数。
ICMPv6 統計	
ICMPv6 受信	
input	インタフェースで受信した ICMP メッセージの総数。 ipv6IfIcmpInErrors によってカウントされたメッセージがすべて含まれます。このインタフェースは、ICMP メッセージの宛先とされたインタフェースであり、必ずしもメッセージにとっての入力インタフェースではない可能性があります。
errors	インタフェースで受信したものの ICMP 特有のエラー (無効な ICMP チェックサム、無効なメッセージ長など) があると判断された ICMP メッセージの総数
destination unreachable messages	インタフェースで受信した ICMP 送信先到達不能メッセージの数。
packet too big messages	インタフェースで受信した "ICMP Packet Too Big" (ICMP パケットが大きすぎます) メッセージの数。
time exceeded messages	インタフェースで受信した ICMP 時間超過メッセージの数。
parameter problem message	インタフェースで受信した ICMP パラメータ問題メッセージの数。
echo request messages	インタフェースで受信した ICMP エコー (要求) メッセージの数。
echo reply messages	インタフェースで受信した ICMP エコー応答メッセージの数。
redirect messages	インタフェースで受信したリダイレクトメッセージの数。
group membership query messages	インタフェースで受信した ICMPv6 グループメンバーシップクエリーメッセージの数。
group membership response messages	インタフェースで受信した ICMPv6 グループメンバーシップ応答メッセージの数。

コマンドラインインタフェース

IP インタフェース

IPv6 トラフィック

group membership reduction messages	インタフェースで受信した ICMPv6 グループメンバーシップ取り消しメッセージの数。
router solicit messages	インタフェースで受信した ICMP ルーター要請メッセージの数。
router advertisement messages	インタフェースで受信した ICMP ルーターアドバタイズメントメッセージの数。
neighbor solicit messages	インタフェースで受信した ICMP 近隣要請メッセージの数。
neighbor advertisement messages	インタフェースで受信した ICMP 近隣アドバタイズメントメッセージの数。
redirect messages	インタフェースで受信した ICMPv6 リダイレクトメッセージの数。
ICMPv6 送信	
output	このインタフェースが送信を試みた ICMP メッセージの総数。このカウンタ値には、icmpOutErrors によってカウントされる数が含まれます。
destination unreachable messages	インタフェースで送信された ICMP 送信先到達不能メッセージの数。
packet too big messages	インタフェースで送信された "ICMP Packet Too Big" (ICMP パケットが大きすぎます) メッセージの数。
time exceeded messages	インタフェースで送信された ICMP 時間超過メッセージの数。
parameter problem message	インタフェースで送信された ICMP パラメータ問題メッセージの数。
echo reply messages	インタフェースで送信された ICMP エコー応答メッセージの数。
router solicit messages	インタフェースで送信された ICMP ルーター要請メッセージの数。
neighbor advertisement messages	インタフェースで送信された ICMP 近隣アドバタイズメントメッセージの数。
redirect messages	送信されたリダイレクトメッセージの数。
group membership response messages	送信された ICMPv6 グループメンバーシップ応答メッセージの数。
group membership reduction messages	送信された ICMPv6 グループメンバーシップ取り消しメッセージの数。
UDP 統計	
input	UDP ユーザに送信された UDP データグラムの総数。
no port errors	受信された目的地ポートにアプリケーションが無かったデータグラムの総数
other errors	目的地ポートで、アプリケーションの欠如以外の理由で送信されることが出来なかった受信 UDP データグラムの数
output	このエンティティから送信された UDP データグラムの総数。

clear ipv6 traffic

IPv6 トラフィックカウンタをリセットします。

コマンドモード

Privileged Exec

コマンド解説

- このコマンドは、"ipv6 traffic" コマンドで表示される、全てのカウンタをリセットします。

例

```
Console#clear ipv6 traffic
Console#
```

ping6

ネットワークの他のノードへ (IPv6) ICMP エコーリクエストパケットを送信します。

文法

ping6 { *ipv6-address* | *host-name* } [*count count*] [*size size*]

- *ipv6-address* — 近隣装置の IPv6 アドレス。
- *host-name* — ドメインネームサーバを通して IPv6 アドレスの中に変換されることが可能なホスト名ストリング。
- *count* — 送信するパケットの数。 (範囲: 1-16)
- *size* — パケットのバイト数 (範囲: 48-18024 bytes)
ルータがヘッダ情報を付加する為、実際のパケットサイズは指定されたサイズよりも 8bytes 大きくなります。

初期設定

カウント: 5 回

サイズ: 100bytes

コマンドモード

Privileged Exec

コマンド解説

- ping6 コマンドは、ネットワーク上の他のサイトへ到達することができるかどうか、またはパス上に遅延が無いかを評価するために使用します。
- ホスト名に Ping を送る時、DNS サーバが有効 (see page 898) になっていることを確認してください。必要ならば、ローカル装置は同じく DNS 静的ホストテーブルで指定することが可能です。
- ホスト名で Ping6 を使用する時、スイッチは最初に、IPv6 アドレスの中でエイリアスの解決を試み、その後に IPv4 アドレスの中で解決を試みます。

例

```
Console#ping6 FE80::2E0:CFF:FE00:FC%1/64
Type ESC to abort.
PING to FE80::2E0:CFF:FE00:FC%1/64, by 5 32-byte payload ICMP packets,
  timeout is 3 seconds
response time: 20 ms [FE80::2E0:CFF:FE00:FC] seq_no: 1
response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 2
response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 3
response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 4
response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 5
Ping statistics for FE80::2E0:CFF:FE00:FC%1/64:
  5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 20 ms, Average = 4 ms
Console#
```

ipv6 nd dad attempts

重複アドレス検索中に、インタフェースで送信する連続した近隣要請メッセージの数を設定します。
"no" を前に置くことで初期設定に戻します。

文法

ipv6 nd dad attempts *count*

- *count* — このインタフェースに重複アドレスが存在するか否かを決定するために送られる、近隣要請メッセージの数（範囲：0-600）

初期設定

1

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 0 の値に設定することで、重複アドレス検索を無効にします。
- 重複アドレス検索は、新しいユニキャスト IPv6 アドレスがインタフェースに割り当てられる前に、既にネットワーク上に存在するかどうかを決定します。
- 重複アドレス検索は、休止状態のインタフェース上で停止します。（“vlan” コマンド（P711）を参照）インタフェースが休止状態になっている間、全てのユニキャスト IPv6 アドレスは "pending" ステータスでインタフェースに割り当てられます。インタフェースが管理上再開した時、重複アドレス検索が自動的に再稼動します。
- 再稼動するインタフェースは、インタフェースの全ての IPv6 ユニキャストアドレスの重複アドレス検索を再開します。重複アドレス検索がインタフェースのリンクローカルアドレスで実行されている間、他の IPv6 アドレスは "tentative" 状態で残ります。重複リンクローカルアドレスが見つからない場合、残りの IPv6 アドレスのために重複アドレス検出を開始します。
- インタフェースのリンクローカルアドレスが変更された場合、重複アドレス検出は新しいリンクローカルアドレスで行われますが、すでにインタフェースと関連付けられた IPv6 グローバルユニキャストアドレスに対しては行いません。

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is stalled.
Link-local address:
  FE80::200:E8FF:FE90:0/64 [TENTATIVE]
Global unicast address(es):
  009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64 [TENTATIVE]
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
Console#
```

関連するコマンド

ipv6 nd ns-interval (P889)
show ipv6 neighbors (P891)

ipv6 nd ns-interval

インタフェース上で IPv6 近隣要請メッセージが送信される間隔を設定します。"no" を前に置くことで設定を初期値に戻します。

文法

ipv6 nd ns-interval *milliseconds*
no ipv6 nd ns-interval

- *milliseconds* — IPv6 近隣要請メッセージが送信される間隔（範囲：1000-3600000）

初期設定

1000 ミリセカンド

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- このコマンドは、アドレス解決時または近隣の到達可能性を調べる時に、IPv6 近隣要請メッセージが送信される間隔を設定します。標準的な IPv6 オペレーションでは極端に短い間隔を使用するのを避けてください。

例

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 30000 milliseconds
Console#
```

関連するコマンド

show running-config (P380)

ipv6 nd reachable-time

いずれかの到着可能性確認イベント発生後、リモート IPv6 ノードが、到着可能であると推測される時間を設定します。

文法

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

- *milliseconds* — 到達可能性の確認を受けた後、ノードが到達可能であると推測可能な時間（範囲：1000-3600000）

初期設定

30000 ミリセカンド

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- このコマンドで設定されるタイムリミットは、スイッチが不在の近隣を発見することを可能にします。

例

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd reachable-time 1000
Console(config)#
```

clear ipv6 neighbors

IPv6 近隣探索キャッシュの全ての動的エントリを削除します。

コマンドモード

Privileged Exec

例

```
Console#clear ipv6 neighbors
Console#
```


show ipv6 neighbors

IPv6 近隣探索キャッシュの情報を表示します。

文法

show ipv6 neighbors [*vlan vlan-id* | *ipv6-address*]

- *vlan-id* — VLAN ID (Range: 1-4093)
- *ipv6-address* — 近隣装置の IPv6 アドレス。RFC2373"IPv6 Addressing Architecture" に従ってフォーマットされたリンクローカルアドレスとグローバルユニキャストアドレスのいずれかを指定できます。8つの16ビット16進数をコロンで区切った値を使用します。アドレス内の不適格なフィールドを満たす為に必要とされるゼロの適切な数を示すため、1つのダブルコロンが使用されます。

初期設定

全ての IPv6 近隣探索キャッシュエントリを表示。

コマンドモード

Privileged Exec

例

```
Console#show ipv6 neighbors
IPv6 Address      Age      Link-layer Addr  State  VLAN
2009:DB9:2229::79  666      00-00-E8-90-00-00 REACH  1
FE80::200:E8FF:FE90:0  671      00-00-E8-90-00-00 REACH  1
Console#
```

IPv6 ネイバーの表示

項目	解説
IPv6 Address	ネイバーの IPV6 アドレス
Age	アドレスが到達可能として実証されてからの時間（秒）静的エントリは "Permanent" と示されます。
Link-layer Addr	物理層 MA アドレス

IPv6 ネイバーの表示

State	近隣のキャッシュエントリの状態を指定します。IPv6 近隣検出キャッシュ内の動的エントリの状態は、以下のとおりです。 ♦INCOMP (Incomplete) – エントリ上でアドレス解決が実行中です。近隣要請メッセージが、ターゲットの要請されたマルチキャストアドレスに送信されましたが、対応する近隣アドバタイズメントメッセージがまだ受信されていません。 ♦REACH (到達可能) – 近隣への転送パスが正常に機能していることを示す確認メッセージ (正常) が、最後の Reachable Time (到達可能な時間) (ミリ秒) 内に受信されました。REACH (到達) 状態の間は、デバイスはパケットの送信中に特別な動作をしません。 ♦STALE – 転送パスが正常に機能していることを示す最後の確認メッセージ (正常) が受信されてから、ReachableTime (到達可能な時間) (ミリ秒) を超える時間が経過しました。STALE (期限切れ) 状態の間は、デバイスはパケットが送信されるまで特別な動作をしません。 ♦DELAY – 転送パスが正常に機能していることを示す最後の確認メッセージ (正常) が受信されてから、ReachableTime (到達可能な時間) (ミリ秒) を超える時間が経過しました。前回の DELAY_FIRST_PROBE_TIME 秒内にパケットが送信されました。DELAY (遅延) 状態に入ってから DELAY_FIRST_PROBE_TIME 秒内に到達可能性確認が受信されない場合は、近隣要求メッセージを送信し、状態を PROBE (調査) に変えます。 ♦PROBE – 到達可能性確認が受信されるまで、近隣要請メッセージを RetransTimer ミリ秒間隔で再送信することで、到達可能性確認がアクティブに求められます。 ♦UNKNO – 未知の状態。 以下の状態は静的エントリに使用されます。 ♦INCOMP (Incomplete) ♦REACH (Reachable)
VLAN	到達したアドレスの VLAN インタフェース。

関連するコマンド

show mac-address-table (P667)

FXC3326 Management Guide (FXC10-DC-200012-R1.0)

初版 2010 年 11 月

- ◆ 本ユーザマニュアルは、FXC 株式会社が制作したもので、全ての権利を弊社が所有します。弊社に無断で本書の一部、または全部を複製 / 転載することを禁じます。
 - ◆ 改良のため製品の仕様を予告なく変更することがありますが、ご了承ください。
 - ◆ 予告なく本書の一部または全体を修正、変更することがありますが、ご了承ください。
 - ◆ ユーザマニュアルの内容に関しましては、万全を期しておりますが、万一ご不明な点がございましたら、弊社サポートセンターまでご相談ください。
-

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326

Management Guide
FXC3326