

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG
Management Guide

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide

本マニュアルについて

- 本マニュアルでは、FXC5148XG 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 3.0.4.0 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

電源を切る（電源コードを抜く）

接続ケーブルを抜く

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。
-

- ◆ 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
1.3 初期設定	6
2. 本機の管理.....	8
2.1 本機への接続.....	8
2.1.1 設定方法	8
2.1.2 接続手順	9
2.1.3 リモート接続	10
2.2 基本設定	11
2.2.1 コンソール接続	11
2.2.2 パスワードの設定	11
2.2.3 IP アドレスの設定	12
手動設定	12
動的設定	13
2.2.4 SNMP 管理アクセスを有効にする	14
コミュニティ名 (Community Strings).....	14
トラップ・レシーバ (Trap Receivers)	15
2.2.5 設定情報の保存	15
2.3 システムファイルの管理.....	17
3. Web インターフェース	18
3.1 Web インターフェースへの接続.....	18
3.2 Web インターフェースの操作方法	19
3.2.1 ホームページ	19
3.2.2 設定オプション	19
3.2.3 パネルの表示	20
3.2.4 メインメニュー	20
3.3 基本設定	24
3.3.1 システム情報の表示	24
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	25
3.3.3 ブリッジ拡張機能の表示	27
3.3.4 IP アドレスの設定	28
手動での IP アドレスの設定	29

DHCP 又は BOOTP による IP アドレスの設定	30
DHCP の更新	30
3.3.5 ファームウェアの管理	31
システムソフトウェアのダウンロード	31
3.3.6 設定情報ファイルの保存・復元	33
設定情報ファイルのダウンロード	34
3.3.7 コンソールポートの設定	35
3.3.8 Telnet の設定	36
3.3.9 Event Logging の設定	37
syslog の設定	37
リモートログの設定	39
ログメッセージの表示	40
3.3.10 再起動	41
3.3.11 システムクロック設定	41
SNTP 設定	41
タイムゾーンの設定	41
3.4 SNMP	43
3.4.1 SNMP エージェントを有効にする	44
3.4.2 コミュニティ名の設定	45
3.4.3 トラップマネージャ・トラップタイプの指定	46
3.4.4 SNMPv3 マネージメントアクセスの設定	49
ローカルエンジン ID の設定	49
リモートエンジン ID の設定	50
SNMPv3 ユーザーの設定	51
SNMPv3 リモートユーザーの設定	53
SNMPv3 グループの設定	54
SNMPv3 ビューの設定	56
3.5 ユーザ認証	58
3.5.1 ユーザアカウントの設定	58
3.5.2 ローカル / リモート認証ログオン設定	60
3.5.3 HTTPS 設定	63
サイト証明書の設定変更	64
3.5.4 Secure Shell 設定	65
ホストキーペアの生成	67
SSH サーバ設定	68
3.5.5 ポートセキュリティの設定	70
3.5.6 802.1x ポート認証	72
802.1x グローバルセッティングの表示	73
802.1x グローバルセッティングの設定	73
802.1X 認証ポート設定に関する設定	74
IEEE802.1x 統計情報の表示	76
3.5.7 管理アドレスのアドレスフィルタリング	77
3.6 ACL (Access Control Lists)	79

目次

3.6.1	ACL の設定	79
	ACL 名およびタイプの設定	80
	Standard IP ACL の設定	80
	Extended IP ACL の設定	82
3.6.2	ACL へのポートのバインド	84
3.7	ポート設定	85
3.7.1	接続状況の表示	85
3.7.2	インターフェース接続の設定	86
3.7.3	トランクグループの設定	89
	静的トランクの設定	90
	LACP 設定	91
	LACP パラメータ設定	92
	LACP ポートカウンターの表示	94
	ローカル側の LACP 設定及びステータスの表示	94
	リモート側の LACP 設定及びステータスの表示	96
3.7.4	ブロードキャストストームのしきい値の設定	97
3.7.5	ポートミラーリングの設定	99
3.7.6	帯域制御	100
3.7.7	ポート統計情報表示	101
3.8	アドレステーブル	105
3.8.1	動的アドレステーブルの設定	105
3.8.2	アドレステーブルの表示	106
3.8.3	エージングタイムの変更	107
3.9	スパニングツリーアルゴリズム	108
3.9.1	グローバル設定の表示	109
3.9.2	グローバル設定	110
3.9.3	インターフェース設定の表示	114
3.9.4	インターフェース設定	116
3.9.5	MSTP 設定 (MSTP VLAN Configuration)	118
3.9.6	MSTP インターフェース設定の表示	120
3.9.7	MSTP インターフェースの設定	121
3.10	VLAN	123
	VLAN へポートの割り当て	124
	タグ付・タグなしフレームの送信	125
3.10.1	GVRP の有効・無効 (Global Setting)	126
3.10.2	VLAN 基本情報の表示	126
3.10.3	現在の VLAN 表示	127
3.10.4	VLAN の作成	128
3.10.5	VLAN への静的メンバーの追加 (VLAN Index)	129
3.10.6	VLAN への静的メンバーの追加 (Port Index)	131
3.10.7	インターフェースの VLAN 動作の設定	132
3.10.8	プライベート VLAN の設定	134

現在のプライベート VLAN の表示	135
プライベート VLAN の設定	136
VLAN の関連付け	137
プライベート VLAN インタフェース情報の表示	138
プライベート VLAN インタフェースの設定	139
3.11 プライオリティ	141
3.11.1 インターフェースへのデフォルトプライオリティの設定	141
3.11.2 Egress キューへの CoS 値のマッピング	142
3.11.3 キューモードの選択	144
トラフィッククラスのサービスウェイトの設定	145
3.11.4 レイヤ 3/4 プライオリティの設定	146
CoS 値へのレイヤ 3/4 プライオリティのマッピング	146
DSCP プライオリティの選択	146
3.11.5 DSCP プライオリティのマッピング	146
3.12 マルチキャストフィルタリング	150
3.12.1 レイヤ 2 IGMP (Snooping and Query)	150
IGMP Snooping Query パラメータの設定	151
マルチキャストルータに接続されたインターフェースの表示	153
マルチキャストルータに接続するインターフェースの設定	154
マルチキャストサービスのポートメンバー表示	155
マルチキャストサービスへのポートの指定	156
4. コマンドラインインターフェース	158
4.1 コマンドラインインターフェースの利用	158
4.1.1 コマンドラインインターフェースへのアクセス	158
4.1.2 コンソール接続	158
4.1.3 Telnet 接続	159
4.2 コマンド入力	160
4.2.1 キーワードと引数	160
4.2.2 コマンドの省略	160
4.2.3 コマンドの補完	160
4.2.4 コマンド上でのヘルプの表示	160
コマンドの表示	161
4.2.5 キーワードの検索	162
4.2.6 コマンドのキャンセル	162
4.2.7 コマンド入力履歴の利用	162
4.2.8 コマンドモード	162
4.2.9 Exec コマンド	163
4.2.10 Configuration コマンド	163
4.2.11 コマンドラインプロセス	165
4.3 コマンドグループ	166

4.4	Line (ラインコマンド).....	168
	Line	169
	login	170
	password	171
	timeout login response	172
	exec-timeout	173
	password-thresh	174
	silent-time	175
	databits	175
	parity	176
	speed	177
	stopbits	177
	disconnect	178
	show line	178
4.5	General (一般コマンド).....	180
	enable	180
	disable	181
	configure	182
	show history	182
	reload	183
	end	184
	exit	184
	quit	185
4.6	システム管理.....	186
4.6.1	Device Designation コマンド	186
	prompt	187
	hostname	187
4.6.2	ユーザーアクセスコマンド	188
	username	188
	enable password	189
4.6.3	IP フィルターコマンド	190
	management	190
	show management	191
4.6.4	Web サーバーコマンド	192
	ip http port	192
	ip http server	193
	ip http secure-server	194
	ip http secure-port	195
4.6.5	Telnet サーバーコマンド	196
	ip telnet port	196
	ip telnet server	196
4.6.6	Secure Shell コマンド	198
	ip ssh server	200
	ip ssh timeout	201

ip ssh authentication-retries.....	202
ip ssh server-key size	203
delete public-key.....	204
ip ssh crypto host-key generate.....	204
ip ssh crypto zeroize.....	205
ip ssh save host-key	206
show ip ssh.....	206
show ssh.....	207
show public-key	208
4.6.7 Event Logging コマンド	209
logging on	209
logging history	210
logging host	211
logging facility	211
logging trap	212
clear logging	213
show logging.....	214
show log	215
4.6.8 SMTP アラートコマンド	217
logging sendmail host.....	217
logging sendmail level	218
logging sendmail source-email	219
logging sendmail destination-email	219
logging sendmail.....	220
show logging sendmail	220
4.6.9 Time コマンド	221
sntp client	221
sntp server	222
sntp poll	223
show sntp	224
clock timezone.....	224
calendar set.....	225
show calendar	226
4.6.10 システム情報の表示	227
show startup-config	227
show running-config	229
show system	231
show users	232
show version.....	233
4.6.11 フレームサイズコマンド	234
jumbo frame.....	234
4.7 ファイル管理 (Flash/File).....	235
copy	235
delete.....	238
dir.....	239

boot system	240
4.8 ユーザ認証	241
4.8.1 認証コマンド	241
Authentication login	241
4.8.2 authentication enable コマンド	242
4.8.3 Radius クライアントコマンド	243
radius-server host	244
radius-server port	245
radius-server key	245
radius-server retransmit	246
radius-server timeout	246
show radius-server	247
4.8.4 TACACS+ クライアントコマンド	248
tacacs-server host	248
tacacs-server port	249
tacacs-server key	249
show tacacs-server	250
4.8.5 ポートセキュリティコマンド	251
port security	251
4.8.6 802.1x ポート認証コマンド	253
dot1x system-auth-control	253
dot1x default	254
dot1x max-req	254
dot1x port-control	255
dot1x operation-mode	255
dot1x re-authenticate	256
dot1x re-authentication	257
dot1x timeout quiet-period	257
dot1x timeout re-authperiod	258
dot1x timeout tx-period	258
show dot1x	259
4.9 ACL (Access Control Lists)	262
4.9.1 IP ACL コマンド	263
access-list ip	263
permit,deny (Standard ACL)	264
permit,deny (Extended ACL)	265
show ip access-list	266
ip access-group	267
show ip access-group	268
map access-list ip	268
show map access-list ip	269
4.9.2 ACL 情報の表示	270
show access-list	270
show access-group	270

4.10	SNMP	271
	snmp-server.....	271
	show snmp	272
	snmp-server community	273
	snmp-server contact	274
	snmp-server location	274
	snmp-server host.....	275
	snmp-server enable traps.....	277
	snmp-server engine-id.....	278
	show snmp engine-id.....	279
	snmp-server view	280
	show snmp view	281
	snmp-server group	282
	show snmp group	283
	snmp-server user.....	285
	show snmp user	286
4.11	インターフェース.....	288
	interface	288
	description	289
	speed-duplex	290
	negotiation	291
	capabilities	292
	flow control	293
	shutdown	294
	switchport broadcast packet-rate.....	294
	clear counters	295
	show interfaces status	296
	show interfaces counters	297
	show interfaces switchport	299
4.12	ポートミラーリング	301
	port monitor	301
	show port monitor	302
4.13	帯域制御.....	303
	rate-limit	303
4.14	リンクアグリゲーション	304
	channel-group.....	305
	lacp	306
	lacp system-priority.....	307
	ladp admin-key (Ethernet Interface).....	308
	ladp admin-key (Port Channel).....	309
	lacp port-priority	310
	show lacp.....	311
4.15	アドレステーブル.....	315

mac-address-table static	315
clear mac-address-table dynamic.....	316
show mac-address-table	317
mac-address-table aging-time	318
show mac-address-table aging-time	318
4.16 スパニングツリー.....	319
spanning-tree.....	320
spanning-tree mode.....	320
spanning-tree forward-time.....	322
spanning-tree hello-time	322
spanning-tree max-age.....	323
spanning-tree priority	324
spanning-tree pathcost method	324
spanning-tree transmission-limit.....	325
spanning-tree mst-configuration	326
mst vlan	326
mst priority	327
name.....	328
revision	329
max-hops	330
spanning-tree spanning-disabled	330
spanning-tree cost.....	331
spanning-tree port-priority	332
spanning-tree edge-port	333
spanning-tree portfast.....	334
spanning-tree link-type	335
spanning-tree mst cost	336
spanning-tree mst port-priority.....	337
spanning-tree protocol-migration.....	338
show spanning-tree mst configuration.....	341
4.17 VLAN.....	342
4.17.1 VLAN グループの設定	342
vlan database	342
vlan	343
4.17.2 VLAN インターフェースの設定.....	344
interface vlan	344
switchport mode	345
switchport acceptable-frame-types.....	346
switchport ingress-filtering	347
switchport native vlan	348
switchport allowed vlan.....	349
switchport forbidden vlan.....	350
4.17.3 VLAN 情報の表示	351
show vlan.....	351

4.17.4	プライベート VLAN の設定	353
	Private vlan	355
	private vlan association	356
	switchport mode private-vlan	357
	switchport private-vlan host-association	358
	switchport private-vlan isolated	358
	switchport private-vlan mapping	359
	show vlan private-vlan	360
4.17.5	LEC (Learning Equivalent Class) コマンド	361
	lec	361
4.18	GVRP (GARP VLAN Registration Protocol)	363
	bridge-ext gvrp	363
	show bridge-ext	364
	switchport gvrp	364
	show gvrp configuration	365
	garp timer	365
	show garp timer	367
4.19	プライオリティ	368
4.19.1	プライオリティ コマンド (Layer 2)	368
	queue mode	369
	switchport priority default	370
	queue bandwidth	371
	queue cos-map	372
	show queue mode	373
	show queue bandwidth	373
	show queue cos-map	374
4.19.2	プライオリティ コマンド (Layer 3 and 4)	375
	map ip dscp (Global Configuration)	375
	map ip dscp (interface Configuration)	376
	show map ip dscp	377
4.20	マルチキャストフィルタリング	378
4.20.1	IGMP Snooping コマンド	378
	ip igmp snooping	378
	ip igmp snooping vlan static	379
	ip igmp snooping version	379
	show ip igmp snooping	380
	show mac-address-table multicast	381
4.20.2	IGMP Query コマンド (Layer2)	382
	ip igmp snooping querier	382
	ip igmp snooping query-coount	383
	ip igmp snooping query-interval	384
	ip igmp snooping query-max-response-time	385
	ip igmp snooping router-port-expiretime	386
4.20.3	静的マルチキャストルーティング コマンド	387

目次

ip igmp snooping vlan mrouter	387
show ip igmp snooping mrouter.....	388
4.21 IP インターフェース	389
4.21.1 基本 IP 設定	389
ip address	389
ip default-gateway	390
ip dhcp restart.....	391
show ip interface.....	392
show ip redirects.....	392
ping.....	393
付録 A. トラブルシューティング	395
Telnet 又は Web ブラウザ、SNMP ソフトウェアから接続できない。.....	395
セキュアシェルを使用した接続ができない。.....	395
シリアルポート接続から内蔵の設定プログラムに接続できない。.....	396
パスワードを無くしてしまった、又は忘れてしまった。.....	396
付録 B. グロッサリー（用語説明）.....	398

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	TFTP サーバによるバックアップ可能
Authentication	Console, Telnet, web ユーザ名 / パスワード, RADIUS, TACACS+ Web HTTPS; Telnet SSH SNMP コミュニティ名、IP アドレスフィルタリング Port IEEE802.1x 認証, MAC アドレスフィルタリング
Access Control Lists	最大 32IP ACL サポート
DHCP Client	サポート
Port Configuration	スピード、通信方式、フローコントロール
Rate Limiting	入力帯域制御
Port Mirroring	1 つの分析ポートに対する 1 ポートのミラーリング
Port Trunking	Static 及び LACP による最大 25 トランク
Broadcast Storm Control	サポート
Static Address	最大登録可能 MAC アドレス数 8k
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 Protocol	STP、Rapid STP (RSTP)、Multiple STP (MSTP)
Virtual VLANs	IEEE802.1Q タグ付 VLAN/ ポートベース VLAN / プライベート VLAN (最大 256 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、DSCP、TCP/UDP ポート
Multicast Filtering	IGMP Snooping、Query

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、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 では IP アドレス、プロトコル、TCP/UDP ポート番号によるパケット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。

帯域制御 /Rate Limiting

各インタフェースにおいて送信及び受信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。

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 プローブを接続し、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。

本機では最大 25 グループのトランクをサポートしています。

ブロードキャストストームコントロール /Broadcast Storm Control

ブロードキャストストームコントロール機能は、ブロード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パケットを制限することができます。ブロードキャスト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 1.5MB 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

格別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。

スパンニングツリープロトコル / Spanning Tree Protocol

本機は 3 種類のスパン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 256 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。

プライオリティ /Traffic Prioritization

本機では 4 段階のキューと 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。

1.3 初期設定

本機の初期設定は設定ファイル "Factory_Default_Config.cfg" に保存されています。
本機を初期設定にリセットするためには、"Factory_Default_Config.cfg" を起動設定ファイルとします。

詳細は P3-17 「設定情報ファイルの保存・復元」を参照して下さい。

基本的な設定項目の初期設定は以下の表の通りです。

機能	パラメータ	初期設定
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0(disabled)
Authentication	Privileged Exec Level	Username"admin" Password"admin"
	Normal Exec Level	Username"guest" Password"guest"
	Enable Privileged Exec from Normal Exec Level	Password"super"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443
SNMP	Community Strings	"public"(read only) "private"(read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input limits	Disabled
Port Trunking	Static Trunks	None
	LACP(all ports)	Disabled

Broadcaststorm Protection	Status	Enabled(all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Algorithm	Status	Enabled,RSTP (Defaults:All values based on IEEE 802.1w)
	Fast Forwarding(Edge Port)	Disabled
Address Table	Aging Time	300seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Enabled
	Switchport Mode(Egress mode)	Hybrid:tagged/untagged frames
	GVRP(global)	Disabled
	GVRP(port interface)	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Weighted Round Robin	Queue:0 1 2 3 4 5 6 7 Weight:1 2 4 6 8 10 12 14
	IP DSCP Priority	Disabled
IP Settings	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Client Enabled
	BOOTP	Disabled
Multicast Filtering	IGMP Snooping	Snooping:Enabled Querier:Enabled
System Log	Status	Enabled
	Messages Logged	Levels 0-6 (all)
	Messages Logged to flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled(but server defined)
SNTP	Clock Synchronization	Disabled

2. 本機の管理

2.1 本機への接続

2.1.1 設定方法

FXC5148XG 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] 初期設定では、本機に対し IP アドレスは設定されていません。IP アドレスの設定を行うには 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、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。

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 (最大 16 ユーザ)
- ◆ 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
- ◆ IEEE802.1Q 準拠のタグ付 VLAN (最大 256 グループ)
- ◆ GVRP 有効
- ◆ IGMP マルチキャストフィルタリング設定

- ◆ TFTP 経由のファームウェアのアップロード及びダウンロード
- ◆ TFTP 経由の設定情報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
- ◆ 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)

エミュレーション -- VT100

通信速度 ----- 9600 ボー (baud)

データビット ----- 8bit

パリティ ----- なし

ストップビット ----- 1bit

フロー制御 ----- なし

[注意] ハイパーターミナルを使用する場合、" ファンクションキー、方向キー、Ctrl キーの使い方 " で "Windows キー " ではなく " ターミナルキー " を選択して下さい。Windows2000 では Windows2000 Service Pack2 以上でハイパーターミナルの VT100 エミュレーションのバグが修正されています。Windows2000 でハイパーターミナルを使用する場合、Service Pack2 以上がインストールされていることを確認して下さい。

(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。

- [注意]** コンソール接続に関する設定の詳細は P168 「Line (ラインコマンド)」を参照して下さい。
CLI の使い方は P158 「コマンドラインインターフェース」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 P166 「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、BOOTP 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。

初期設定では本機に 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場合や、DHCP、BOOTP を用いて自動的に IP アドレスの設定を行う場合の設定方法は P12 「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 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)。

- [注意]** 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 8 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。

[注意] "0" は平文パスワード、"7" は暗号化されたパスワードを入力します。

```
Username: admin
Password:

CLI session with the FXC5148XG 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はない場合には、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。

[注意] 1 つの VLAN インタフェースにのみ IP アドレスを設定することができます（初期設定では VLAN1）。IP アドレスを設定した VLAN が管理機能にアクセスできる唯一の管理 VLAN となります。他の VLAN に対して IP アドレスを設定した場合、元の IP アドレスは無効となり、新たに IP アドレスを設定した VLAN が管理機能にアクセス可能な管理 VLAN となります。

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] 本機の初期設定では IP アドレスは設定されていません。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
- ・デフォルトゲートウェイ
- ・サブネットマスク

IP 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、管理者モード (Privileged Exec) 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)#
```

動的設定

"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。
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。
- (2) global configuration モードに戻るために、"end" と入力し、<Enter> キーを押します。

- (3) ブロードキャストサービスのリクエストを送信するために、"ip dhcp restart client" 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 client
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.
```

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することが可能です。

[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。

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)#
```

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・レシーバの設定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 host host-address community-string" と入力し <Enter> キーを押します。"host-address" にはトラップ・レシーバの IP アドレスを、"community-string" にはホストのコミュニティ名を入力します。
- (2) SNMP に情報を送信するためには 1 つ以上のトラップコマンドを設定する必要があります。"snmp-server enable traps type" と入力し、<Enter> キーを押します。
"type" には "authentication" か "link-up-down" のどちらかを入力します。

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

2.2.5 設定情報の保存

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。

設定ファイルの保存は以下の手順で行います：

- (1) 管理者モード (Privileged Exec) で "copy running-config startup-config" と入力し、<Enter> キーを押します。
- (2) 起動設定ファイル名前を入力し、<Enter> キーを押します。

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

\Write to FLASH finish.
Success.

Console#
```

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 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 P3-17「設定ファイルの保存・復元」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 P3-15「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)。このコードは、さらにコンソールポートを通してシステムへのファームウェア・ファイル直接アップロードする機能を提供します。
詳細に関しては、付-2「シリアルポート経由のファームウェアアップグレード」を参照して下さい。

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。

3. Web インターフェース

3.1 Web インターフェースへの接続

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第 4 章「コマンドラインインタフェース」を参照して下さい。

[注意] 一部、Web インタフェースでは設定できず、CLI 経由でのみ設定できる項目があります。Web インタフェースで設定できない内容に関しては CLI を利用し、設定を行って下さい。

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 P3-13「IP アドレスの設定」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 P3-82「インタフェース設定」を参照して下さい)

3.2 Web インター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] 又は [Apply Changes] 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
Refresh	ページの内容を最新の情報に更新する
Apply	入力した値を本機に反映させる
Apply Changes	入力した値を本機に反映させる

[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]

Web インターフェース

Web インターフェースの操作方法

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。

[注意] Internet Explorer5.0 を使用する場合は、設定の変更後にブラウザの更新ボタンを使用し、画面上に表示されている情報の更新を手動で行う必要があります。

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 P3-56「インタフェース接続の設定」で解説している各ポートの設定ページが表示されます。



3.2.4 メインメニュー

Web インタフェースを使用することで、システムパラメータの設定、本機全体や各ポートの管理、又はネットワーク状況の監視を行うことができます。次ページの表は、Web インタフェースで利用できる内容の一覧を示しています。

メニュー	解説	ページ
System		P24
System Information	コンタクト情報を含むシステム基本情報の表示	P24
Switch Information	ポート数、ハードウェア / ファームウェアバージョン、電源状態の表示	P25
Bridge Extension	拡張ブリッジパラメータの表示	P27
IP Configuration	管理アクセス用 IP アドレスの設定	P28
File		P31
Copy	ファイル転送及びコピー	P31
Delete	フラッシュメモリからファイルを削除	P31
Set Startup	起動ファイルの設定	P31
Reset	本機の再起動	P41
SNTP		P41
Configuration	SNTP クライアント設定 (ブロードキャスト / サーバ設定モード)	P41
Clock Time Zone	タイムゾーン設定	P41
SNMP		P43
Configuration	コミュニティ名及びトラップ設定	P45
Security		P58
User Accounts	ユーザへのパスワードの設定	P58

Authentication Settings	RADIUS/TACACS 認証の設定	P60
HTTPS Settings	セキュア HTTP(HTTPS) の設定	P63
SSH		P65
Host-Key Settings	host key(public/private) の生成	P67
Settings	Secure Shell サーバー	P68
Port Security	セキュリティ侵害対応、登録 MAC アドレス数設定、ステータスなど各ポートのセキュリティ設定	P70
802.1x	ポート認証	P70
Information	全体設定の表示	P72
Configuration	パラメータの設定	P72
Port Configuration	各ポートの認証モードの設定	P72
Statistics	指定ポートの統計情報の表示	P76
ACL		P79
Configuration	IP 及び MAC アドレスベースのパケットフィルタリング設定	P79
Port Binding	ACL へのポートの登録	P84
IP Filter	Web、SNMP、Telnet 経由での管理用クライアントの IP アドレスの設定	P77
Port		P85
Port Information	ポート接続状況の表示	P85
Trunk Information	トランク接続状況の表示	P85
Port Configuration	ポート接続設定	P86
Trunk Configuration	トランク接続の設定	P89
Trunk Membership	静的トランクに追加するポートの指定	P90
LACP		P91
Configuration	ポートへの動的なトランクへの参加の許可	P91
Aggregation Port	system priority、admin key、port priority の設定	P92
Port Counters Information	LACP プロトコルメッセージ統計情報の表示	P94
Port Internal Information	ローカル側のオペレーション状態の設定及び表示	P94
Port Neighbors Information	リモート側のオペレーション状態の設定及び表示	P96
Port Broadcast Control	各ポートのブロードキャストストームのしきい値の設定	P97
Trunk Broadcast Control	各トランクのブロードキャストストームのしきい値の設定	P97
Mirror Port Configuration	ミラーリングのソース及びターゲットポートの設定	P99
Rate Limit		P100
Input Port Configuration	各ポートの入力帯域制御	P100

Web インターフェース

Web インターフェースの操作方法

	Input Trunk Configuration	各トランクの入力帯域制御	P100
	Port Statistics	イーサネット及び RMON ポート統計情報の表示	P101
	Address Table		P105
	Static Addresses	インタフェースのアドレス又は VLAN の表示	P106
	Dynamic Addresses	アドレステーブルでの静的入力の表示又は編集	P105
	Address Aging	動的学習アドレスのタイムアウト時間の設定	P107
	Spanning Tree		P108
	STA		P108
	Information	ブリッジに使用される STA データの表示	P109
	Configuration	STA、RSTP、MSTP のグローバルブリッジの設定	P110
	Port Information	STA の個々のポートの設定情報	P114
	Trunk Information	STA の個々のトランクの設定情報	P114
	Port Configuration	STA の個々のポートの設定	P116
	Trunk Configuration	STA の個々のトランクの設定	P116
	MSTP		P118
	VLAN Configuration	STA でのプライオリティと VLAN の設定	P118
	Port Information	特定の MSTP でのポート設定の表示	P120
	Trunk Information	特定の MSTP でのトランク設定の表示	P120
	Port Configuration	特定の MSTP でのポートの設定	P121
	Trunk Configuration	特定の MSTP でのトランクの設定	P121
	VLAN		P123
	802.1Q VLAN		P123
	GVRP Status	GVRP の有効化	P126
	Basic Information	本機でサポートしている VLAN タイプの表示	P126
	Current Table	各 VLAN の所属する現在のポートとタグのサポート状況の表示	P127
	Static List	VLAN グループの構成及び解除	P128
	Static Table	既存 VLAN の設定変更	P129
	Static Membership	インタフェースのメンバーシップタイプ設定	P131
	Port Configuration	デフォルト PVID と VLAN 属性の設定	P132
	Trunk Configuration	デフォルトトランク PVID と VLAN 属性の設定	P132
	Private VLAN		P134
	Information	プライベート VLAN 機能情報の表示	P135
	Configuration	プライマリ VLAN 又はコミュニティ VLAN の作成 / 削除	P136
	Association	各コミュニティ VLAN のプライマリ VLAN への関連付け	P137

Port Information	VLAN ポートタイプ及び関連付けられたプライマリ / セカンダリ VLAN の表示	P138
Port Configuration	プライベート VLAN インタフェースタイプの設定 及びインタフェースのプライベート VLAN との関連付け	P139
Trunk Information	VLAN ポートタイプ及び関連付けられたプライマリ / セカンダリ VLAN の表示	P138
Trunk Configuration	プライベート VLAN インタフェースタイプの設定 及びインタフェースのプライベート VLAN との関連付け	P139
Priority		P141
Default Port Priority	各ポートのデフォルトプライオリティの設定	P141
Default Trunk Priority	各トランクのデフォルトプライオリティの設定	P141
Traffic Classes	出力キューの IEEE802.1p プライオリティタグのマッピング	P142
Queue Mode	キューモードの設定	P144
Queue Scheduling	重み付けラウンドロビンキューの設定	P145
DSCP Priority Status	DSCP プライオリティの有効・無効化	P146
IP DSCP Priority	IP DSCP の CoS 値へのマッピング設定	P146
ACL CoS Priority	ACL ルールに一致するフレームのアウトプット キューと CoS 値の変更	P146
IGMP Snooping		P150
IGMP Configuration	ルチキャストフィルタリングの有効化、マルチ キャストクエリのパラメータの設定	P150
Multicast Router Port Information	Port Information 各 VLAN ID の隣接したマルチキャスト ルータ又はスイッチに接続されたポートを表示	P153
Static Multicast Router Port Configuration	隣接したマルチキャストルータ又はスイッチに接 続したポートの割り当て	P154
IP Multicast Registration Table	マルチキャスト IP アドレスと VLAN ID を含む本 機で使用中の全てのマルチキャストグループの表 示	P155
IGMP Member Port Table	選択された VLAN に関連したマルチキャストアド レス	P156

3.3 基本設定

3.3.1 システム情報の表示

本機に名前、設置場所及びコンタクト情報を設定することにより、管理する際に本機の識別を容易に行うことができます。

設定・表示項目

System Name

本機に設定した名前

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

Location

本機の設置場所

Contact

管理者のコンタクト情報

System Up Time

管理システムを起動してからの時間

設定方法

[System] [System Information] をクリックします。system name (システム名) location (設置場所) 及び Contact (管理者のコンタクト情報) を入力し、[Apply] ボタンをクリックします。

(このページは Telnet を利用し CLI にアクセスするための [Telnet] ボタンがあります)

The screenshot displays the 'FXC5148XG L2 GE Switch Manager' web interface. On the left is a navigation tree with categories like Home, System, Switch Information, Bridge Extension, IP Configuration, File, Line, Log, Reset, SNMP, and Security. The 'System' category is expanded, showing 'System Information' as the selected item. The main content area contains a form with the following fields: 'System Name' (empty), 'Object ID' (1.3.6.1.4.1.202.20.56), 'Location' (empty), 'Contact' (empty), and 'System Up Time' (0 days, 0 hours, 28 minutes, and 41.46 seconds). At the bottom of the form are buttons for 'Apply', 'Revert', 'Help', and 'Logout'. Below the form, there are three links: 'Telnet' (Connect to textual user interface), 'Support' (Send mail to technical support), and 'Contact' (Connect to FXC Web Page).

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

設定・表示項目

[Main Board](ハードウェア本体)

Serial Number

本機のシリアルナンバー

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

内蔵電源のステータス

[Management Software](管理ソフトウェア)

Loader Version

Loader Code のバージョン

Boot-ROM Version

Power-On Self-Test (POST) 及び boot code のバージョン数

Operation Code Version

runtime code のバージョン

[Expansion Slot](拡張スロット)

Expansion Slot 1/2

拡張スロットの状態 (RJ-45, SFP)

*CLI では以下の情報が追加されます。

◆ **Unit Number**

ユニット番号の指定 (1)

◆ Redundant Power Status

リタンダント電源のステータス

設定方法

[System] [Switch Information] をクリックすると表示されます。

The screenshot displays the 'Switch Information' page in a web interface. On the left is a navigation tree with categories like Home, System, File, Line, Log, Reset, and various protocols. The main area is titled 'Switch Information' and contains three sections: 'Main Board', 'Management Software', and 'Expansion Slot', each with a table of details.

Main Board:	
Serial Number	0012CF0B0D00
Number of Ports	50
Hardware Version	R01
Internal Power Status	Not Present
Redundant Power Status	Inactive

Management Software:	
Loader Version	1.0.0.7
Boot-ROM Version	1.0.0.8
Operation Code Version	2.3.4.4

Expansion Slot:	
Expansion Slot 1	Ten Giga Port Module
Expansion Slot 2	Not Present

3.3.3 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。

変数の表示を行うために、ブリッジ MIB 拡張設定にアクセスすることができます。

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、P3-101「Class of Service 設定」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 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。

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（P3-89「VLAN 設定」を参照して下さい）

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（??? を参照して下さい）

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

[System] [Bridge Extension Configuration] をクリックすると表示されます。

Bridge Extension Configuration

Bridge Capability

Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	SVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

GMRP ☐ Enabled

3.3.4 IP アドレスの設定

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 :0.0.0.0、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(1-4096)。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：0.0.0.0）

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：255.0.0.0）

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。

手動での IP アドレスの設定

設定方法

[System] [IP Configuration] をクリックします。管理端末を接続する VLAN を選択し、"IP Address Mode" を Static にします。IP Address、Subnet Mask、Gateway IP Address を入力し、[Apply] をクリックします。

IP Configuration

Management VLAN	1
IP Address Mode	Static
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00-12-CF-0B-0D-00

Restart DHCP

DHCP 又は BOOTP による IP アドレスの設定

DHCP 又は BOOTP サービスが利用可能な環境では、それらのサービスを利用し動的に IP アドレスの設定を行うことができます。

設定方法

[System] [IP Configuration] をクリックします。管理端末を接続する VLAN を選択し、"IP Address Mode" を DHCP 又は BOOTP にし [Apply] をクリックします。その後 [Restart DHCP] ボタンをクリックすることで、直ちに新しい IP アドレスのリクエストを送信します。また次回以降、本機を再起動した際に IP アドレスのリクエストを送信します。

IP Configuration

Management VLAN	1
IP Address Mode	DHCP
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00-12-CF-0B-0D-00

Restart DHCP

【注意】 IP アドレスの設定が変更され管理アクセスが切断された場合には、コンソール接続を行ない "show ip interface" コマンドを使用することで、新しい IP アドレスを確認することができます。

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。

設定方法

DHCP サービスを利用して IP アドレスが割り当てられ、すでに IP アドレスが利用できなくなっている場合には、Web インタフェースからの IP アドレスの更新はできません。以前の IP アドレスが利用可能な場合は、Web インタフェースを使い [Restart DHCP] ボタンから IP アドレスのリクエストを行うことができます。

3.3.5 ファームウェアの管理

TFTP サーバを使用したファームウェアのダウンロード及びアップロードを行うことができます。TFTP サーバ上に runtime code を保存することにより、後で本機の復元を行う際にダウンロードすることができます。また、以前のバージョンのファームウェアを上書きすることなく、新しいファームウェアを使用することができます。

設定・表示項目

File Transfer Method

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。

- **file to file** 本機のディレクトリに新たなファイル名を付けて、ファームウェアをコピーします。
- **file to tftp** 本機から TFTP サーバへファイルをコピーします。
- **tftp to file** TFTP サーバから本機へファイルをコピーします。

TFTP Server IP Address

TFTP サーバの IP アドレス

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)

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] runtime ファイルは最大 2 つまでしか保存できません。起動ファイルに指定されているファイルは削除することができません。

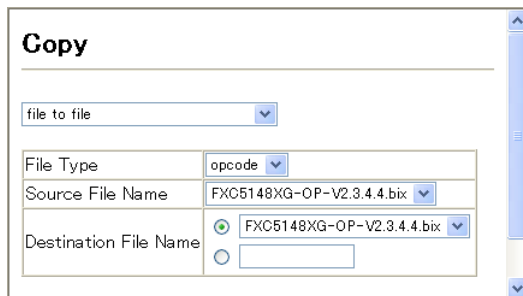
システムソフトウェアのダウンロード

runtime code をダウンロードする場合、現在のイメージと置き換えるために現在のファイルを Destination File Name として指定することができます。また、現在の runtime code ファイルと異なるファイル名を使用し本体にダウンロードし、その後ダウンロードしたファイルを起動ファイルに設定することもできます。

設定方法

[System] [File] [Firmware] をクリックします。TFTP Server IP Address (TFTP サーバの IP アドレス) と Source File Name (ダウンロードするファイル名) を入力します。Destination File Name (ダウンロード先のファイル名) で、本機内の既存のファイルを上書きする場合には既存ファイルを選択し、新しいファイルとして保存する場合にはファイル名

を指定します。その後、[Transfer from Server] をクリックします。新しいファームウェアを使用するためには本機の再起動を行います。



Copy

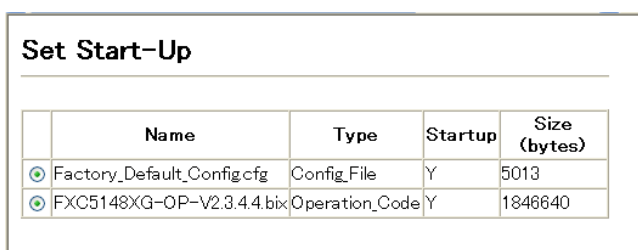
file to file

File Type: opcode

Source File Name: FXC5148XG-OP-V2.3.4.4.bix

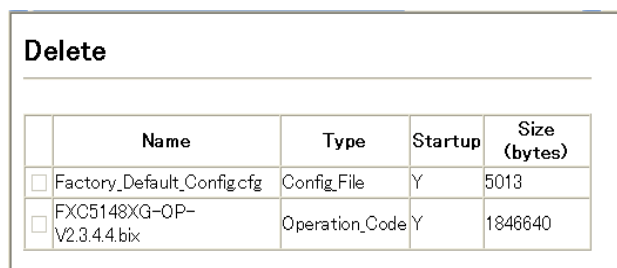
Destination File Name: FXC5148XG-OP-V2.3.4.4.bix

現在の runtime code ファイルと異なる名前ダウンロードを行った場合には、新しくダウンロードしたファイルを、起動ファイルとして使用される Operation Code する必要があります。ドロップダウンボックスから新しいファイル名を選択します。その後、[Apply Changes] をクリックします。新しいファームウェアを使用するためには本機の再起動を行います。



	Name	Type	Startup	Size (bytes)
<input checked="" type="checkbox"/>	Factory_Default_Config.cfg	Config_File	Y	5013
<input checked="" type="checkbox"/>	FXC5148XG-OP-V2.3.4.4.bix	Operation_Code	Y	1846640

ファイルを削除するには、[System] [File] [Delete] をクリックします。チェックボックスをクリックして削除するファイル名をリストから選択し、[Apply] をクリックします。起動ファイルとして指定されているファイルは削除できないことに注意して下さい。



	Name	Type	Startup	Size (bytes)
<input type="checkbox"/>	Factory_Default_Config.cfg	Config_File	Y	5013
<input type="checkbox"/>	FXC5148XG-OP-V2.3.4.4.bix	Operation_Code	Y	1846640

3.3.6 設定情報ファイルの保存・復元

TFTP サーバを使用し、設定情報ファイルをダウンロード又はアップロードする事ができます。アップロードした設定情報ファイルは後からダウンロードし、本機の設定を復元するために使用することができます。

設定・表示項目

File Transfer Method

設定情報ファイルコピーの操作方法。下記のオプションがあります。

- **file to file** 新たなファイル名を付けて本機のディレクトリへコピーします。
- **file to running-config** 本機の実行中の設定ファイルへコピーします。
- **file to startup-config** 本機の実行中の設定ファイルを起動設定ファイルへコピーします。
- **file to tftp** 本機から TFTP サーバへファイルをコピーします。
- **running-config to file** 実行中の設定ファイルをコピーします。
- **running-config to startup-config** 実行中の設定ファイルを起動設定ファイルへコピーします。
- **running-config to tftp** 実行中の設定ファイルを TFTP サーバへコピーします。
- **startup-config to file** 起動設定ファイルを本機の実行中の設定ファイルへコピーします。
- **startup-config to running-config** 起動設定ファイルを本機の実行中の設定ファイルへコピーします。
- **startup-config to tftp** 起動設定ファイルを TFTP サーバへコピーします。
- **tftp to file** TFTP サーバから本機へファイルをコピーします。
- **tftp to running-config** TFTP サーバから本機の実行中の設定ファイルへコピーします。
- **tftp to startup-config** TFTP サーバから本機の起動設定ファイルへコピーします。

TFTP Server IP Address

TFTP サーバの IP アドレス

File Type

設定情報をコピーするための config (設定ファイル)

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] 本機内に保存可能な設定ファイルの最大数はフラッシュメモリの容量に依存します。

設定情報ファイルのダウンロード

設定ファイルは新しいファイル名で保存し、起動ファイルとして設定できる他に、現在の起動設定ファイルを保存先に指定することで直接起動設定ファイルを置き換えることができます。但し、"Factory_Default_Config.cfg" ファイルは TFTP サーバへコピーすることはできません。設定ファイルをダウンロードする際に、ダウンロード先のファイル名として指定し、新しいファイルに置き換えることはできません。

設定方法

[System] [File] [Configuration] をクリックします。TFTP Server IP Address (TFTP サーバの IP アドレス) と Source File Name (ダウンロードするファイル名) を入力します。Destination File Name (ダウンロード先のファイル名) で、本機内の既存のファイルを上書きする場合には既存ファイルを選択し、新しいファイルとして保存する場合にはファイル名を指定します。その後、[Transfer from Server] をクリックします。

Copy

http to startup-config

TFTP Server IP Address

192.168.1.23

Source File Name

config-startup

Startup File Name

☐ Factory_Default_Config.cfg

☒ startup

現在の起動設定ファイルと異なる名前でダウンロードを行った場合には、新しくダウンロードしたファイルを、起動ファイルとして使用される設定ファイルにする必要があります。ドロップダウンボックスから新しいファイル名を選択します。その後、[Apply Changes] をクリックします。新しい設定を使用するためには本機の再起動を行います。

Set Start-Up

	Name	Type	Startup	Size(bytes)
<input type="radio"/>	Factory_Default_Config.cfg	Config_File	N	5197
<input checked="" type="radio"/>	startup	Config_File	Y	5571
<input checked="" type="radio"/>	V2271.F	Operation_Code	Y	1761944

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 インター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

ユーザ入力の実行タイムアウト時間。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：0 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 응답しなくなります（範囲：0-120 回、初期設定：3 回）

Silent Time

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：0 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）

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、115200 bps、初期設定：9600 bps）

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）

設定方法

[System] [Line] [Console] をクリックします。コンソールポート接続パラメータを設定します。その後、[Apply] をクリックします。

Console		
Login Timeout (0-300)	<input type="text" value="0"/>	secs (0 : Disabled)
Exec Timeout (0-65535)	<input type="text" value="0"/>	secs (0 : Disabled)
Password Threshold (0-120)	<input type="text" value="3"/>	(0 : Disabled)
Silent Time (0-65535)	<input type="text" value="0"/>	secs (0 : Disabled)
Data Bits	<input type="text" value="8"/>	
Parity	<input type="text" value="None"/>	
Speed	<input type="text" value="9600"/>	
Stop Bits	<input type="text" value="1"/>	

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、又は 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)

Telnet Port Number

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)

設定方法

[System] [Line] [Telnet] をクリックします。Telnet 接続のためのパラメータを設定します。その後、[Apply] をクリックします。

Telnet	
Telnet Status	<input checked="" type="checkbox"/> Enabled
Telnet Port Number	<input type="text" value="23"/>
Login Timeout (0-300)	<input type="text" value="300"/> secs (0 : Disabled)
Exec Timeout (0-65535)	<input type="text" value="600"/> secs (0 : Disabled)
Password Threshold (0-120)	<input type="text" value="3"/> (0 : Disabled)

3.3.9 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 Level 2, 5, 6 のみサポートしています。

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：6）

[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

[System] [Log] [System Logs] をクリックします。"System Log Status" を指定し、RAM/ フラッシュメモリに保存するイベントメッセージを設定します。その後、[Apply] をクリックします。

System Logs

System Log Status	<input checked="" type="checkbox"/> Enabled
Flash Level (0-7)	<input type="text" value="0"/>
Ram Level (0-7)	<input type="text" value="0"/>

リモートログの設定

Remote Logs 画面では、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：有効）

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

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：6）

Host IP List

syslog メッセージを受け取るリモート syslog サーバの IP アドレスのリストを表示します。Host IP アドレスの上限は 5 つです。

Host IP Address

Host IP List に追加するリモート syslog サーバの IP アドレス。

設定方法

[System] [Log] [Remote Logs] をクリックします。"Host IP List" に IP アドレスを指定するには、"Host IP Address" に追加する IP アドレスを入力し、[Add] をクリックします。IP アドレスを削除するには、"Host IP List" から削除する IP アドレスをクリックし、その後 [Remove] をクリックします。

Remote Logs

Remote Log Status	<input checked="" type="checkbox"/> Enabled
Logging Facility (16-23)	<input type="text" value="23"/>
Logging Trap (0-7)	<input type="text" value="6"/>

Host IP Address:

Current:
Host IP List
(none)

New:
Host IP Address

ログメッセージの表示

Logs 画面では、保存されているシステム / イベントメッセージを表示できます。本体の RAM (電源投入時には消去されます) に一時的に保存されるメッセージは 2048 エントリです。フラッシュメモリに永久的に保存されるメッセージは 4096 エントリです。

設定方法

[System] [Log] [Logs] をクリックします。

Logs

Log Messages: Level :6, Module:6, functions:1, error number:1 Information:VLAN 1 link-up notification. _____
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:STP topology change notification. _____
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, redundant power change to good. _____
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, main power change to not exist. _____
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, Port 3 link-up notification. _____
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:System coldStart notification. _____

3.3.10 再起動

設定方法

[System] [Reset] をクリックします。[Reset] ボタンを押して、本機の再起動を行います。再起動の確認を促すプロンプトが表示されたら、確認して実行します。



【注意】 再起動時には Power-On Self-Test が実行されます。

3.3.11 システムクロック設定

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、CLI から手動で時刻の設定を行うこともできます（詳細は P4-61「Calendar Set」を参照）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。

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。

【注意】 SNTP 設定は CLI からのみ可能です。設定方法については P221「Time コマンド」を参照ください。

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。

設定・表示項目

Current Time

現在時刻の表示

Name

タイムゾーンに対する名称を設定します。(設定範囲 : 1-29 文字)

Hours (0-12)

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。

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。

設定方法

[SNTP] [Clock Time Zone] をクリックします。UTC との時差を設定し [Apply] をクリックします。

Clock Time Zone	
Current Time	Jan 1 01:45:52 2001
Name	<input type="text" value="Atlantic"/>
Hours (0-12)	<input type="text" value="4"/>
Minutes (0-59)	<input type="text" value="0"/>
Direction	<input checked="" type="radio"/> Before-UTC <input type="radio"/> After-UTC

3.4 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。

以下の表は、使用可能なセキュリティモデルとレベルの組み合わせおよび本機の初期設定を示します。

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuth NoPriv	public (read only)	defaultview	none	none	コミュニティ名のみ
v1	noAuth NoPriv	private (read only)	defaultview	defaultview	none	コミュニティ名のみ
v1	noAuth NoPriv	user defined	user defined	user defined	user defined	コミュニティ名のみ
v2c	noAuth NoPriv	public (read only)	defaultview	none	none	コミュニティ名のみ
v2c	noAuth NoPriv	private (read/write)	defaultview	defaultview	none	コミュニティ名のみ
v2c	noAuth NoPriv	user defined	user defined	user defined	user defined	コミュニティ名のみ
v3	noAuth NoPriv	user defined	user defined	user defined	user defined	ユーザ名のマッチングのみ
v3	Auth NoPriv	user defined	user defined	user defined	user defined	MD5 または SHA アルゴリズムに基づくユーザー認証
v3	Auth Priv	user defined	user defined	user defined	user defined	MD5 または SHA アルゴリズムに基づく認証機能および DES56bit 暗号化機能

事前に定義されているグループとビューは削除および変更が可能です

3.4.1 SNMP エージェントを有効にする

SNMPv3 サービスを有効にします

設定・表示項目

SNMP 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

設定方法

[SNMP] [Agent Status] をクリックします。[Enable] 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。



SNMP Agent Status

Snmp Agent Status ☒ Enabled

3.4.2 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

SNMP Community Capability

本機が最大5つのコミュニティ名をサポートしていることを表しています

Current

現在設定されているコミュニティ名のリスト

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)

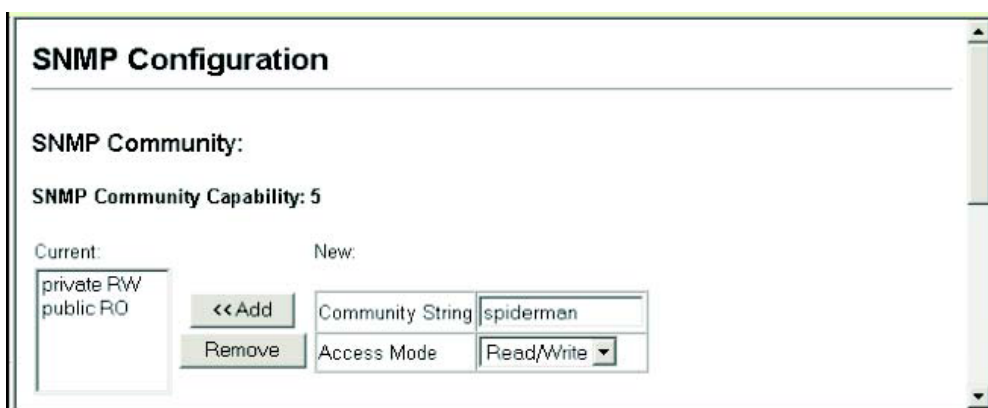
Access Mode

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

[SNMP] [Configuration] をクリックします。コミュニティ名の追加を行う場合は [Community String] 欄に新しいコミュニティ名を入力し、Access Mode ダウンリストからアクセス権を選択し、[Add] をクリックします。



3.4.3 トラップマネージャ・トラップタイプの指定

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

- ◆ 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する際には (authNoPriv または authPriv) 最初に P51 「SNMPv3 ユーザーの設定」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。
- ◆ 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。

[注意] 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。

設定・表示項目

Trap Manager Capability

本機が最大 5 つのトラップマネージャをサポートしていることを表しています

Current

登録されているトラップマネージャのリスト

Trap Manager IP Address

トラップを受信するホストの IP アドレス

Trap Manager Community String

トラップ送信時のコミュニティ名 (設定範囲: 1-32 文字、大文字小文字は区別されます)

Trap UDP Port

トラップマネージャが使用する UDP ポートを指定します (初期設定: 162)

Trap Version

送信するトラップのバージョン (SNMP v1 又は SNMP v2、v3 初期設定: SNMP v1)

Trap Security Level

Trap Version で v3 が指定されている場合、以下のセキュリティレベルの中からひとつを選択します。(初期設定：noAuthNoPriv)

- noAuthNoPriv - 認証も暗号化も行いません
- AuthNoPriv - ユーザー認証を行います、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 - 認証と暗号化の両方を行います。(v3 セキュリティモデルでのみ設定可)

Trap Inform

インフォームの有効/無効(v2c または v3 ホスト設定時のみ使用可)

- Timeout - 再送までの待ち時間(設定範囲：0-2147483647 センチセカンド)
(初期設定：1500 センチセカンド)
- Retry times - 再送を行う最大回数(設定範囲：0-255 初期設定：3 回)

Enable 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)

Enable 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)

設定方法

[SNMP] [Configuration] をクリックします。[Trap Managers] で、トラップを受信するトラップマネージャの IP アドレス (Trap Manager IP Address)、コミュニティ名 (Trap Manager Community String) を入力します。

SNMP バージョン (SNMP Version) を指定し、バージョン 3 を選択時のみ (Trap Security Level) の設定を行います。

インフォームを使用する場合は (Trap Inform) の設定を行います。

[Add] をクリックすると、左側の (Current) リストに新しいマネージャが追加されます。トラップの種類 (認証時、Link-up/down) の変更を行う場合はチェックボックスで選択します。設定完了後、[Apply] をクリックします。

トラップマネージャを削除する場合は、リストからマネージャを選択し [Remove] をクリックします。

Trap Managers:

Trap Manager Capability: 5

Current:

(none)

<< Add

Remove

New:

Trap Manager IP Address	<input type="text"/>
Trap Manager Community String	<input type="text"/>
Trap UDP Port	<input type="text" value="162"/>
Trap Version	<input type="text" value="1"/>
Trap Security Level	<input type="text" value="noAuthNoPriv"/>
<input type="checkbox"/> Trap Inform	<div>Timeout (0-2147483647) <input type="text" value="1"/> (1/100 secs)</div> <div>Retry times (0-255) <input type="text"/></div>

Enable Authentication Traps: ☒

Enable Link-up and Link-down Traps: ☒

3.4.4 SNMPv3 マネージメントアクセスの設定

スイッチへ SNMPv3 マネージメントアクセスを行う際には以下の手順で設定します。

- (1) エンジン ID の設定を行います。エンジン ID の設定は必ず一番最初に行ってください。(デフォルトエンジン ID を使用する場合は、この手順は必要ありません)
- (2) ビューの設定を行います。ビューを基に、読み込み専用・書き込み許可などのアクセス制御が行われます。
- (3) グループを設定します。セキュリティモデルの選択および(2)で設定したビューを使用し、グループに所属する全ユーザーのアクセス制限を定義します。
- (4) ユーザーを作成し、所属するグループを決定します。

ローカルエンジン ID の設定

SNMP 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。

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せん。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。

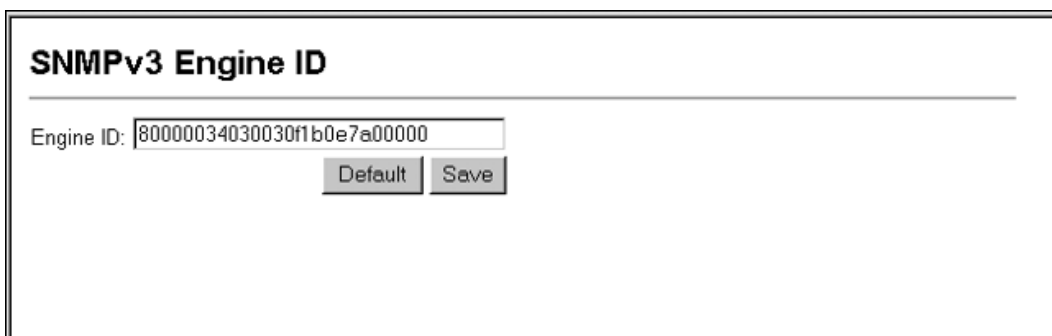
設定・表示項目

Engine ID

エンジン ID を設定します。

設定方法

[SNMP] [SNMPv3 Engine ID] をクリックします。Engine ID を入力し、[Save] をクリックします。デフォルト値を使用する場合には [Default] ボタンをクリックします。



The image shows a web interface window titled "SNMPv3 Engine ID". Inside the window, there is a label "Engine ID:" followed by a text input field containing the hexadecimal value "80000034030030f1b0e7a00000". Below the input field are two buttons: "Default" and "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。

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 P46 「トラップマネージャ・トラップタイプの指定」および P53 「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

リモートエンジン ID を設定します。

Remote IP Host

リモートデバイスの IP アドレスを設定します。

設定方法

[SNMP] [SNMPv3 Remote Engine ID] をクリックします。Engine ID、Remote IP Host を入力し、[Add] をクリックします。ID を削除する場合には [Remove] をクリックします。

SNMPv3 Remote Engine ID		
Remote Engine ID	Remote IP Host	Action
80000000030004e2b316c54321	192.168.1.19	<input type="button" value="Remove"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

SNMPv3 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 初期設定 : v1)

Security Level

セキュリティレベル

- noAuthNoPriv - 認証も暗号化も行いません (v3 セキュリティモデルの初期設定値)
- 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)

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

暗号化用パスワード。(最小 8 文字)

Change Group...

ユーザーの所属グループを変更します

設定方法

[SNMP] [SNMPv3 Users] をクリックします。新しいユーザーを登録する場合、[New...] をクリックします。[SNMPv3 Users--New] のページが表示されます。(User Name)(Group Name)(Security Model)(Security Label)(User Authentication)(Data Privacy) の設定を行い、[Add] をクリックします。[SNMPv3 Users] のページに戻り、登録したユーザーがリストに追加されます。変更を行う場合には [Change Group] をクリックすると [SNMPv3 Users--Edit] のページへ移動します。ユーザーを削除する場合には、削除したいユーザー名のチェックボックスへチェックを入れ、[Delete] をクリックします。

The image shows three overlapping screenshots of the SNMPv3 Users web interface:

- SNMPv3 Users (Main List):** Displays a table of users and their settings. It includes 'New...' and 'Delete' buttons.
- SNMPv3 Users -- New:** A form for creating a new user with fields for User Name, Group Name, Security Model, Security Level, User Authentication, and Data Privacy.
- SNMPv3 Users -- Edit:** A form for editing an existing user, showing the current values for the selected user.

	User Name	Group Name	Model	Level	Authentication	Privacy	Actions
<input type="checkbox"/>	david	DefaultROGroup	V1	noAuthNoPriv	None	None	Change Group...
<input type="checkbox"/>	chris	snmpv3users	V3	authPriv	MD5	DES56	Change Group...
<input type="checkbox"/>	steve	snmpv3users	V3	authNoPriv	MD5	None	Change Group...

SNMPv3 Users -- New

SNMPv3 User:

User Name:

Group Name: ☐ ☒ snmpv3users

Security Model:

Security Level:

User Authentication:

Authentication Protocol:

Authentication Password:

Data Privacy:

Privacy Protocol:

Privacy Password:

SNMPv3 Users -- Edit

User Name: david

Group Name: ☐ ☒ DefaultROGroup

SNMPv3 リモートユーザーの設定

それぞれの SNMPv3 ユーザーは固有の名前を持ちます。

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 ユーザーへ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 P46 「トラップマネージャ・トラップタイプの指定」および P50 「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)

Engine ID

リモートデバイス上に設定されているエンジン ID を表示します (P50 参照)

Remote IP

リモートデバイスの IP アドレス

Security Model

セキュリティモデル (v1,v2c,v3 初期設定 : v1)

Security Label

セキュリティレベル

- noAuthNoPriv - 認証も暗号化も行いません (v3 セキュリティモデルの初期設定値)
- 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)

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

暗号化用パスワード。(最小 8 文字)

設定方法

[SNMP] [SNMPv3 Remote Users] をクリックします。新しいユーザーを登録する場合、[New...] をクリックします。[SNMPv3 Remote Users--New] のページが表示されます。(User Name)(Group Name)(Security Model)(Security Level)(User Authentication)(Data Privacy) の設定を行い、[Add] をクリックします。[SNMPv3 Remote Users] のページに戻り、登録したユーザーがリストに追加されます。ユーザーを削除する場合には、削除したいユーザー名のチェックボックスへチェックを入れ、[Delete] をクリックします。

	User Name	Group Name	Engine ID	Model	Level	Authentication	Privacy
<input type="checkbox"/>	mark	r&d	80000000030004#2b316c54321	V3	noAuthNoPriv	None	None

SNMPv3 Remote Users -- New

SNMPV3 User:

User Name:

Group Name: ☐ ☐ public

Remote IP:

Security Model:

Security Level:

User Authentication:

Authentication Protocol:

Authentication Password:

Data Privacy:

Privacy Protocol:

Privacy Password:

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)

Model

セキュリティモデル (1,v2c,v3)

Label

- noAuthNoPriv - 認証も暗号化も行いません
- AuthNoPriv - 認証を行います但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

Write View

Write アクセスのビューを設定します

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。

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
authenticationFailure	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>	
swPowerStatusChangeTrap	1.3.6.1.4.1.202.20.56.63.2.1.0.1
swIpFilterRejectTrap	1.3.6.1.4.1.202.20.56.63.2.1.0.40
swSntpConnFailureTrap	1.3.6.1.4.1.202.20.56.63.2.1.0.41
pethPsePortOnOffNotification	1.3.6.1.4.1.202.20.56.63.2.1.0.43
pethPsePortPowerMaintenanceStatus Notification	1.3.6.1.4.1.202.20.56.63.2.1.0.44
pethMainPowerUsageOnNotification	1.3.6.1.4.1.202.20.56.63.2.1.0.45
pethMainPowerUsageOffNotification	1.3.6.1.4.1.202.20.56.63.2.1.0.46

設定方法

[SNMP] [SNMPv3 Groups] をクリックします。新しいグループを登録する場合、[New...] をクリックします。(Group Name)(Security Model)(Security Label)(Read View)(Write View)(Notify View) の設定を行い、[Add] をクリックします。[SNMPv3 Groups] のページに戻り、登録したグループがリストに追加されます。グループを削除する場合には、削除したいグループ名のチェックボックスへチェックを入れ、[Delete] をクリックします。

SNMPv3 Groups

New... Delete

	Group Name	Model	Level	Read View	Write View	Notify View
<input type="checkbox"/>	public	V1	noAuthNoPriv	defaultview	none	none
<input type="checkbox"/>	public	V2C	noAuthNoPriv	defaultview	none	none
<input type="checkbox"/>	private	V1	noAuthNoPriv	defaultview	defaultview	none
<input type="checkbox"/>	private	V2C	noAuthNoPriv	defaultview	defaultview	none
<input type="checkbox"/>	secure-users	V3	authPriv	defaultview	defaultview	defaultview

Group Properties:

Group Name:

Security Model:

Security Level:

SNMPv3 Views:

Read View: ☒ ☐ defaultview

Write View: ☒ ☐ defaultview

Notify View: ☒ ☐ defaultview

Back Add

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

View Name

SNMP ビュー名（1-64 文字）

View OID Subtrees

ビューの内容が表示されます

Edit OID Subtrees

既存のビューの編集ができます

OID Subtrees

参照可能にする MIB ツリーの OID。ワイルドカードを使用してマスクを設定することも可能です

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

[SNMP] [SNMPv3 Views] をクリックします。新しいビューを登録する場合、[New...] をクリックします。(View Name)(OID Subtree)(Type) の設定を行い、[Add] をクリックします。設定後は [Back] で [SNMPv3 Views] のページに戻ります。

グループを削除する場合には、削除したいグループ名のチェックボックスへチェックを入れ、[Delete] をクリックします。

(OID Subtree) をクリックすると View の情報が表示されます。

編集を行う場合には (Edit OID Subtree) をクリックします。

The screenshot displays the 'SNMPv3 Views' management interface. At the top, there are 'New...' and 'Delete' buttons. Below them is a table listing existing views:

	Name	OID Subtrees	Actions
<input type="checkbox"/>	readaccess	View OID Subtrees	[Edit OID Subtrees...]
<input type="checkbox"/>	defaultview	View OID Subtrees	[Edit OID Subtrees...]
<input type="checkbox"/>	writeaccess	View OID Subtrees	[Edit OID Subtrees...]

Arrows from the 'View OID Subtrees' links point to two other panels. The 'SNMPv3 Views -- View' panel shows details for the 'readaccess' view:

View : readaccess

OID Subtree	Type
1.3.6.1.2	Included

Below this table is a 'Back' button. The 'SNMPv3 View -- Edit' panel is used for creating or modifying views. It includes fields for 'View Name', 'Current' (a list box showing '1 (Included)'), and 'New' (with fields for 'OID Subtree' and 'Type' set to 'Included'). There are '<< Add', 'Remove', and 'Back' buttons.

3.5 ユーザ認証

本機の管理アクセスへは以下の方法により制限を行えます。

- ◆ **パスワード** 本機内部において各ユーザのアクセス権の設定を行うことができます。
- ◆ **認証設定** リモート認証サーバを利用しユーザのアクセス権の設定を行います。
- ◆ **HTTPS** HTTPS を利用したセキュリティを確保した Web アクセスを行えます。
- ◆ **SSH** secure shell を利用したセキュリティを確保した Telnet アクセスを行えます。
- ◆ **ポートセキュリティ** 各ポートに MAC アドレスによるセキュリティを提供します。
- ◆ **IEEE802.1x** IEEE802.1x ポート認証により各ポートのアクセスをコントロールします。
- ◆ **IP フィルタ** Web、SNMP、Telnet への管理アクセスをフィルタリングします。

3.5.1 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。

ユーザ名は CLI を使用した場合のみ利用、変更可能です。

設定・表示項目

Account List

登録されているユーザアカウントと、各アカウントに関連付けられているアクセスレベルのリスト（初期設定：admin 及び guest）

New Account

新たに追加するユーザアカウント情報

- **User Name** ユーザ名（最大文字数：8 文字、最大ユーザ数：16 人）
- **Access Level** ユーザのアクセスレベル（オプション：Normal, Privileged）
- **Password** ユーザのパスワード（範囲：0-8 文字、大文字と小文字は区別されます）

Change Password

既存ユーザアカウントのパスワードを変更します。

Add/Remove

ユーザアカウントのリストへの追加、又はリストからの削除を行います。

設定方法

[Security] [User Accounts] をクリックします。新規のユーザアカウントを設定するには、ユーザ名 (User Name)、ユーザのアクセスレベル (Access Level) を設定します。パスワード (Password) を入力し、再確認のためにパスワード (Confirm Password) を再度入力します。[Add] をクリックすると、新規のユーザアカウントは保存され [Account List] 欄に追加されます。既存ユーザアカウントのパスワードを変更する場合は、[Change Password] 欄にユーザ名 (User Name) 及び新たなパスワード (New Password) を入力し、再確認のためにパスワード (Confirm Password) を再度入力して [Change] をクリックします。

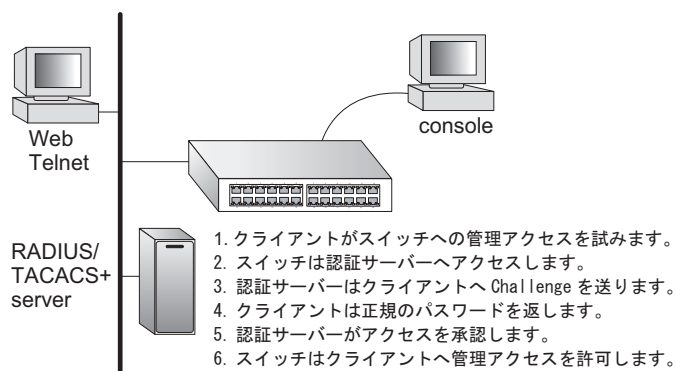
User Accounts	
Account List admin (Privileged) guest (Normal)	New Account User Name: bob Access Level: Normal Password: <input type="password"/> Confirm Password: <input type="password"/>
<input type="button" value="Add"/>	<input type="button" value="Remove"/>
Change Password User Name: <input type="text"/> New Password: <input type="password"/> Confirm Password: <input type="password"/> <input type="button" value="Change"/>	

3.5.2 ローカル / リモート認証ログオン設定

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

- ◆ 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。
- ◆ 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。
- ◆ 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]** 表示された最大 3 つの認証方法を利用します。

RADIUS 設定

Global

RADIUS サーバの設定をグローバルに適用します。

ServerIndex

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 Port Number

RADIUS サーバで使用される UDP ポート番号 (1-65535、初期設定 :1812)

Secret Text String

ログインアクセス認証に使用される暗号キー。間にスペースを入れないで下さい (最大文字数 :20 文字)

Number of Server Transmits

RADIUS サーバに対し認証リクエストを送信する回数 (範囲 :1-30、初期設定 :2)

Timeout for a reply

認証リクエストを再送信する前に RADIUS サーバからの応答を待つ待機時間 (秒) (範囲 :1-65535、初期設定 :5)

TACACS+ 設定

Server IP Address

TACACS+ サーバの IP アドレス (初期設定 : 10.11.12.13)

Server Port Number

TACACS+ サーバで使用される TCP ポート番号 (1-65535、初期設定 :49)

Secret Text String

ログインアクセス認証に使用される暗号キー。間にスペースを入れないで下さい (最大文字数 :20 文字)

[注意] 本機内部の認証データベースは CLI を使用し、ユーザ名とパスワードを入力することで設定が行えます。

設定方法

[Security] [Authentication Settings] をクリックします。Authentication (認証方式) を選択し、RADIUS 及び TACACS+ を選択した場合には、それぞれの認証に必要なパラメータを入力し、[Apply] をクリックします。

Authentication Settings

Authentication

Local

RADIUS Settings:

☒ Global | ServerIndex: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Server Port Number (1-65535)

1812

Secret Text String

Number of Server Transmits (1-30)

2

Timeout for a reply (1-65535)

5

(sec)

TACACS Settings:

Server IP Address

10.11.12.13

Server Port Number (1-65535)

49

Secret Text String

3.5.3 HTTPS 設定

Secure Socket Layer(SSL) を使った Secure Hypertext Transfer Protocol(HTTPS) によって本機の Web インタフェースに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 又は NetscapeNavigator 4.x 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 表文字 3 Explorer 5.0 以上	Windows 98、Windows NT (サービスパック 6A)、 Windows 2000、Windows XP
Netscape Navigator 表文字 3 4.76 以上	Windows 98、Windows NT (サービスパック 6A)、 Windows 2000、Windows XP、Solaris 2.6

安全なサイトの証明を指定するためには、P64 「サイト証明書の設定変更」を参照して下さい。

設定・表示項目

HTTPS Status

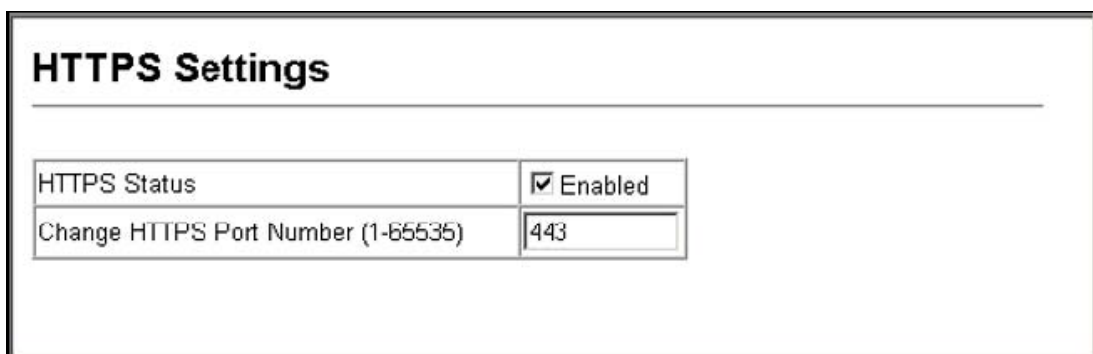
HTTPS サーバ機能を有効または無効に設定します (初期設定 : 有効 (Enabled))

Change HTTPS Port Number

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

[Security] [HTTPS Settings] をクリックします。HTTPS を有効にするためには、HTTPS Status で Enabled を選択します。ポート番号を指定し、[Apply] をクリックします。



HTTPS Settings	
HTTPS Status	<input checked="" type="checkbox"/> Enabled
Change HTTPS Port Number (1-65535)	<input type="text" value="443"/>

サイト証明書の設定変更

TTPS 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を入手し、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 サーバを使用してコンソール接続の CLI により既存の証明書と置き換えます。証明書の設定を行う CLI の手順は以下の通りです。

```
Console#copy tftp https-certificate 3-21
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

【注意】 証明書の変更を行った後に本機の再起動を行わないと、新しい証明書は有効になりません。再起動は CLI を使用し以下の手順で行います。

```
Console#reload
```

3.5.4 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
1568499540186766925933394677505461732531367489083654725415020245593
199868544358361651999923329781766065830956
1082591321289023376546801726272571413428762941301196195566782
5956641048695742788814620651941746772984865468615717739390164779355
9423035774130980227370877945452408397175264635805817671670957480477
6117
```

- (3) **クライアント公開キーの本機への取り込み** P4-91 「copy tftp public-key」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

1341081685609893921040944920155425347631641921872958921143173880055
53616163105177594083868631109291232226828519254374603100937187721199
69631781366277414168985132049117204830339254324101637997592371449011
9380060902539484084827178194372288402533115952134861022902978982721
353267131629432532818915045306393916643 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。
- 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。

[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。

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。

設定・表示項目

Public-Key of Host-Key

ホストへのパブリックキー

- **RSA**: 最初のフィールドはホストキーのサイズ (1024) を表しています。2 番目のフィールドはエンコードされたパブリック指数 (65537)、最後の値はエンコードされた係数を表しています。
- **DSA**: 最初のフィールドはデジタル署名標準(DSS)に基づく SSHによって私用される暗号化方法を表示します。最後の値はエンコードされた係数を表します。

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 : RSA)

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。

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。

Generate

ホストキーペアを生成します。SSH サーバ設定ページで SSH サーバを有効にする前に、ホストキーペアを生成する必要があります。

Clear

RAM 及びフラッシュメモリの両方に保存されているホストキーを削除します。

設定方法

[Security] [SSH Host-Key Settings] をクリックします。ドロップダウンボックスからホストキータイプ (host-key type) を選択し、必要に応じて save the host key from memory to flash にチェックを入れます。その後、[Generate] をクリックし、キーの生成を行ないます。

SSH Host-Key Settings

Public-Key of Host-Key

Host-Key Type	Public-Key
RSA	1024 65537 130917897267478961615211171276497919629621155164242768028072510384048338276358290698941935742287566 1853076228099531413921379002210394737439417368512447371756369962704297907064627111321882467751081589 0431586319348654200209463340676128115040594681146475925732650943840347858370753955264123928004845007 811621891
DSA	ssh-dss AAAAB3NzaC1kc3MAAACBAJBVdKZjkiKEEBU3Ak1Fz72nOPsvP8BDqF2eZeNx17DQ/N4hYx/W427x1AwJ1/dEO4io8fhOdcHZUb kQX00BdqU9/IuvMNd+AEWx5nwoZDZrLWUyNJDowHOGpKvVSmVcIkIjz1FrQs6XTaC1r3ODWbovF0sc1ld+Jj3DC4tXq1AAAAFQC yPELSe2E3SO3Q+P32+SfpbFA+cQAAAIArYRgej1/ZfBvVhC9M/XuIVfApHEDY18fcrzpElcSeBaIeE53gcHGuQsvRLGH+ZC1VV1ds 8VYKHAUFGFNTKOGCGnhVQMjXbsEzGKRqKI7nWt2Otkk4zZRD0twyP5vCQAre3b1Ud1/eB2q7o3jvnruck0Xv1QoWPD50IpJX5op QuAAAIBSHK3JwNa9pNCT360xZH14sqgVbu7Gv5GVuxH6zaY9Z2HPSuDVvIS5wUenchwCaRpGfOJ11VWHEmtcgeFZrAw5G3OY4iAR qGqNc9plvL4aVnxhRdx902H1WkjhWSHOPVH4Cw2FLHpfBBnPL3HHqrVRYjNYBxJPaqV0ZK6lknaGHQ==

Host-Key Type: Both

☒ Save Host-Key from Memory to Flash

Generate Clear

SSH サーバ設定

認証用の SSH サーバの設定

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 (Disabled))

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、Version 1.5 と 2.0 の両方をサポートしています。

SSH 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))

SSH 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)

SSH 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）

- 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。
- 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

[Security] [SSH Settings] をクリックします。SSH を有効にし、必要に応じて各項目の設定を行い、[Apply] をクリックします。SSH サーバを有効にする際は、事前に SSH Host-Key Settings page で host key pair を生成する必要があります。

SSH Server Settings	
SSH Server Status	<input type="checkbox"/> Enabled
Version	2.0
SSH Authentication Timeout (1-120)	<input type="text" value="120"/> seconds
SSH Authentication Retries (1-5)	<input type="text" value="3"/>
SSH Server-Key Size (512-896)	<input type="text" value="768"/>

3.5.5 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ネットワークにアクセスする事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。Static Address Table (P3-76) 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。
 - ポートモニタリングに使用できません。
 - マルチ VLAN ポートにはできません。
 - LACP 又は静的トラUNKポートに設定できません。
 - HUB 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、P85 「ポート設定」からポートの有効化を行なってください。

設定・表示項目

Port

ポート番号

Name

ポート説明

Action

- **None** 動作が行なわれません（初期設定ではこの設定になっています）
- **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 (Disabled)

Max MAC Count

ポートが学習可能な MAC アドレス数（設定範囲：0-20、0 は学習の無効）

Trunk

ポートがトランクされている場合のトランク番号

設定方法

[Security] [Port Security] をクリックします。ポートのセキュリティを有効にするには、設定を行うポート番号の Action を選択し、Security Status チェックボックスをオンにし、最大 MAC アドレス数を設定し、[Apply] をクリックします。

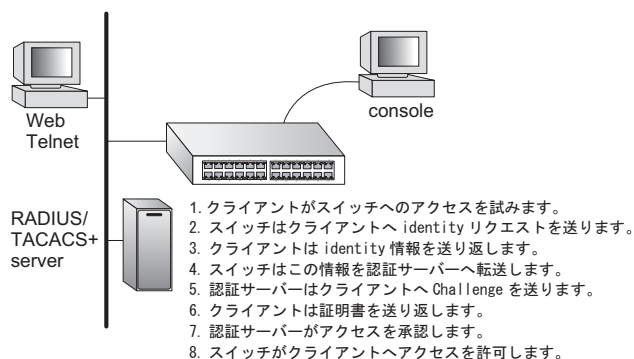
Configuration:

Port	Name	Action	Security Status	Max MAC Count (0-1024)	Trunk
1		None	<input type="checkbox"/> Enabled	0	
2		None	<input type="checkbox"/> Enabled	0	
3		None	<input type="checkbox"/> Enabled	0	
4		None	<input type="checkbox"/> Enabled	0	
5		Trap and Shutdown	<input checked="" type="checkbox"/> Enabled	20	
6		None	<input type="checkbox"/> Enabled	0	

3.5.6 802.1x 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す。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。

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 グローバルセッティングの表示

802.1X プロトコルはクライアントの認証を可能にします。

設定・表示項目

802.1X System Authentication Control

スイッチに対する 802.1X の設定

設定方法

[Security] [802.1x Information] をクリックします。

802.1X Information	
<hr/>	
802.1X System Authentication Control	Disabled

802.1x グローバルセッティングの設定

dot1X プロトコルはポート認証を可能にします。ポートをアクティブに設定する前に、スイッチに対し 802.1X プロトコルを有効に設定する必要があります。

設定・表示項目

802.1X System Authentication Control

802.1X の設定（初期設定：無効）

設定方法

[Security] [802.1X] [Configuration] をクリックします。スイッチに対する 802.1X を有効に設定し、[Apply] をクリックします。

802.1X Configuration	
<hr/>	
802.1X System Authentication Control	<input checked="" type="checkbox"/> Enabled

802.1X 認証ポート設定に関する設定

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。

設定・表示項目

Port

ポート番号

Status

ポートの認証の有効 / 無効

Operation Mode

1 台又は複数のクライアントが IEEE802.1x 認証ポートにアクセスすることを設定します（設定範囲：Single-Host、Multi-Host、初期設定：Single-Host）

Max 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）

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。

Re-authen

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）

Max-Req

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）

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（範囲：1-65535 秒、初期設定：60 秒）

Re-authen 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）

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）

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。
- **Blank** IEEE802.1x がポートで無効化されている場合は空欄となります。

Supplicant

接続されたクライアントの MAC アドレス

Trunk

トランク設定がされている場合に表示

設定方法

[Security] [802.1x] [Port Configuration] をクリックします。必要に応じてパラメータを変更し、[Apply] をクリックします。

802.1X Port Configuration												
Port	Status	Operation Mode	Max Count (1-1024)	Mode	Re-authen	Max Req	Quiet Period	Re-authen Period	Tx Period	Authorized	Supplicant	Trunk
1	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30	Yes	00-00-00-00-00-00	
2	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
3	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
4	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
5	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
6	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
7	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
8	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
9	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
10	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
11	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	
12	Disabled	Single-Host	5	Force-Authorized	<input type="checkbox"/> Enable	2	60	3600	30		00-00-00-00-00-00	

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
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 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
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
Tx EAPOL Total	全 EAPOL フレームの送信数
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

[Security] [802.1x statistics] をクリックします。ポートを選択し、[Query] をクリックします。[Refresh] をクリックすると最新の情報に更新されます。

802.1X Statistics

Port

Query

Rx EAPOL Start	0	Rx EAP LenError	0
Rx EAPOL Logoff	0	Rx Last EAPOLVer	0
Rx EAPOL Invalid	0	Rx Last EAPOLSrc	00-00-00-00-00-00
Rx EAPOL Total	0	Tx EAPOL Total	0
Rx EAP Resp/Id	0	Tx EAP Req/Id	0
Rx EAP Resp/Oth	0	Tx EAP Req/Oth	0

Refresh

3.5.7 管理アドレスのアドレスフィルタリング

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 16 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、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

Web IP Filter

Web グループの IP アドレス

SNMP IP Filter

SNMP グループの IP アドレス

Telnet IP Filter

Telnet グループの IP アドレス

IP Filter List

そのインタフェースに接続が許可されている IP アドレス

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

Add/Remove Filtering Entry

IP アドレスをリストへ追加または削除

設定方法

[Security] [IP Filter] をクリックします。そのインタフェースに管理アクセスを許可する IP アドレスを 1 つまたは範囲で指定し、[Add IP Filtering Entry] をクリックしてフィルタリストを更新します。

The screenshot shows a web interface titled "IP Filter". Below the title is a section labeled "Web IP Filter". Inside this section, there is a table with two columns. The first column is labeled "Web IP Filter List" and contains a single entry "(none)". The second column is empty. Below the table, there are two input fields: "Start IP Address" and "End IP Address". At the bottom of the interface, there are two buttons: "Add Web IP Filtering Entry" and "Remove Web IP Filtering Entry".

Web IP Filter	
Web IP Filter List	(none)
Start IP Address	<input type="text"/>
End IP Address	<input type="text"/>

3.6 ACL (Access Control Lists)

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。

3.6.1 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て許可 (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落とします。リスト上の許可ルールに一致しない場合、パケットは落とされ、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。

- ◆ 各 ACL は最大 60 ルールまで設定可能です。
- ◆ 本機は ingress (入力) フィルタリングの ACL のみをサポートしています。但し、1 個の IP ACL を任意のポートに、1 個の MAC ACL をイングレスフィルタリング全体にバインド可能です。つまり、1 つのインタフェースに対して、1 個の ACL のみバインドできます。

有効な ACL は以下の順番で実行されます。

- (1) 入力ポートの入力 IP ACL のユーザに定義されたルール
- (2) 入力ポートの入力 IP ACL のデフォルトルール (permit any any)
- (3) 明確なルールに一致しない場合、暗黙のデフォルトルール (permit all)

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

Name

ACL 名 (4 文字以上 15 文字以内)

Type

- **Standard** ソース IP アドレスに基づくフィルタリングを行なう IP ACL モード
- **Extended** 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なう IP ACL モード

設定方法

[Security] [ACL] [Configuration] をクリックします。[Name] に ACL 名を入力し、[Type] をリストから選択します (IP Standard, IP Extended, MAC)。その後、[Add] をクリックし、新規リストの設定ページを開きます。



Standard IP ACL の設定

設定・表示項目

Action

ACL のルールが「permit (許可)」か「deny (拒否)」を選択します (初期設定 : Permit ルール)

IP

ソース IP アドレスの指定を行ないます。"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)

Address

ソース IP アドレス

SubnetMask

サブネットマスク

設定方法

「許可」又は「拒否」の動作を設定し、その後アドレスタイプを Any, Host, IP から選択します。"Host" を選択した場合には特定の IP アドレスを指定します。"IP" を選択した場合には IP アドレスの範囲を指定するためにサブネットアドレスとマスクを設定します。その後 [Add] をクリックします。

Standard ACL

Name: david

Action	IP Address	Subnet Mask	Remove
Permit	10.1.1.21	255.255.255.255	<input type="button" value="Remove"/>

Action

Permit

Address Type

IP

IP Address

168.92.16.0

Subnet Mask

255.255.240.0

Extended IP ACL の設定

設定・表示項目

Action

ACL のルールが「permit (許可)」か「deny(拒否)」を選択します (初期設定 : Permit ルー

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 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

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)

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)

設定方法

(permit/deny の) 動作を指定します。ソース及び / 又はディスティネーションアドレスを指定し、アドレスタイプ ((Any, Host, IP) を選択します。"Host" を選択した場合、特定のアドレスを入力します。"IP" を選択した場合、アドレス範囲を指定するためにサブネットアドレスとマスクを指定します。プロトコルタイプ等のその他の必要項目を設定し、[Add] をクリックします。

Extended ACL

Name: ACL1

Action	Source IP Address	Source Subnet Mask	Destination IP Address	Destination Subnet Mask	Protocol	Source Port	Destination Port	Remove
Action	<div>Permit</div>							
Source Address Type	<div>Any</div>							
Source IP Address	<div>0.0.0.0</div>							
Source Subnet Mask	<div>0.0.0.0</div>							
Destination Address Type	<div>Any</div>							
Destination IP Address	<div>0.0.0.0</div>							
Destination Subnet Mask	<div>0.0.0.0</div>							
Protocol	<div> <input checked="" type="radio"/> TCP (6) <input type="radio"/> UDP (17) <input type="radio"/> Others </div>							
Source Port (0-65535)	<div> <input checked="" type="radio"/> Range: <div></div> ~ <div></div> </div>							
Destination Port (0-65535)	<div> <input checked="" type="radio"/> Range: <div></div> ~ <div></div> </div>							
<div>Add</div>								

3.6.2 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。ACL は 1 つを任意のポートに指定できます。

機能解説

本機では ingress (入力) ACL をサポートします。1 個の IP ACL を任意のポートバインド可能です。

設定・表示項目

Port

ポート又は拡張モジュールスロット (範囲 : 1-50)

IP (IN)

ポート (ingress) にバインドする IP ACL ルール

ACL NAME

ACL 名

設定方法

[Security] [ACL] [Port Binding] をクリックします。ACL をバインドするポートに対して "Enable" フィールドにチェックを入れ、ドロップダウンリストから ACL を選択します。その後、[Apply] をクリックします。

Port	IP (IN)
1	<input type="checkbox"/> Enabled (none)
2	<input type="checkbox"/> Enabled (none)
3	<input type="checkbox"/> Enabled (none)
4	<input type="checkbox"/> Enabled (none)
5	<input type="checkbox"/> Enabled (none)
6	<input type="checkbox"/> Enabled (none)
7	<input type="checkbox"/> Enabled (none)
8	<input type="checkbox"/> Enabled (none)
9	<input type="checkbox"/> Enabled (none)

3.7 ポート設定

3.7.1 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 Port Information 及び Trunk Information 画面を使用することができます。

設定・表示項目

Name

インタフェースラベルの表示

Type

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

Admin Status

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

Speed/Duplex Status

通信速度及び通信方式の表示 (Auto, Fixed)

Flow Control Status

使用中のフロー制御の種類を表示 (IEEE 802.3x, Back-Pressure, None)

Autonegotiation

オートネゴシエーションの有効 / 無効の表示

Trunk Member

ポートのトランク状態の表示 (Port Information ページのみ)

Creation

トランクが LACP を使用して動的に設定されているか、手動で設定されているかの表示
(Trunk Information ページのみ)

設定方法

[Port] [Port Information] 又は [Trunk Information] をクリックします。必要なインタフェースの設定の変更し、[Apply] をクリックします。

Port Information								
Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Trunk Member
1		100Base-TX	Enabled	Up	100full	None	Enabled	
2		100Base-TX	Enabled	Down	100full	None	Enabled	
3		100Base-TX	Enabled	Up	100full	None	Enabled	
4		100Base-TX	Enabled	Down	100full	None	Enabled	
5		100Base-TX	Enabled	Down	100full	None	Enabled	
6		100Base-TX	Enabled	Down	100full	None	Enabled	
7		100Base-TX	Enabled	Down	100full	None	Enabled	
8		100Base-TX	Enabled	Down	100full	None	Enabled	
9		100Base-TX	Enabled	Down	100full	None	Enabled	
10		100Base-TX	Enabled	Down	100full	None	Enabled	
11		100Base-TX	Enabled	Down	100full	None	Enabled	
12		100Base-TX	Enabled	Down	100full	None	Enabled	
13		100Base-TX	Enabled	Down	100full	None	Enabled	

3.7.2 インターフェース接続の設定

Trunk Configuration (トランク設定) ページ及び Port Configuration (ポート設定) ページから、インタフェースの有効/無効、手動での通信速度及び通信方式、フローコントロール、オートネゴシエーションの設定及びインタフェースの対応機能を設定することができます。

設定・表示項目

Name

各インタフェースに管理識別用に名前をつけることができます (1-64 文字)

Admin

コリジョンの多発などの場合にインタフェースを手動で無効にすることができます。問題が解決した後に、再度インタフェースを有効にすることができます。また、セキュリティのためにインタフェースを無効にすることもできます。

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。

Autonegotiation(Port Capabilities)

オートネゴシエーションを有効又は無効にします。また、オートネゴシエーション時のポートの対応機能を通知する設定を行います。以下の機能がサポートされています。

- **10half** 10 Mbps half-duplex で動作します。
- **10full** 10 Mbps full-duplex で動作します。
- **100half** 100 Mbps half-duplex で動作します。
- **100full** 100 Mbps full-duplex で動作します。
- **1000full** 1000 Mbps full-duplex で動作します。
- **Sym (Gigabit only)** ポーズフレームの送受信をする場合この項目をチェックします。また、非対称ポーズフレームにより送信者と受信者がオートネゴシエーションを行う場合はチェックを外します（現在のスイッチチップでは対称ポーズフレームのみサポートしています）
- **FC** フローコントロールをサポートします。フローコントロールはバッファがいっぱいの場合に本機へ直接接続される終端端末及びセグメントからの "blocking" トラフィックにより、フレームロス进行を解消します。フローコントロールの有効時には、half-duplex ではバックプレッシャが、full-duplex では IEEE 802.3x が利用されます（障害回避などのために必要な場合以外は、ハブへの接続時にはフローコントロールを無効にしてください。フローコントロールを有効にした場合、バックプレッシャのジャミング信号により、ハブが接続されたセグメント全体のパフォーマンスを低下させる可能性があります）
（初期設定：オートネゴシエーション：有効
100BASE-TX - 10half, 10full, 100half, 100full、1000BASE-T - 10half, 10full, 100half, 100full, 1000full、1000BASE-SX/LX/LH - 1000full が対応機能として通知されます）

Trunk

ポートがトランクメンバーの場合に表示されます。トランクの設定及びポートメンバーの選択は、P89「トランクグループの設定」を参照して下さい。

[注意] ポートの設定を手動で行ない、Speed/Duplex Mode 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。

設定方法

[Port] [Port Configuration] 又は [Trunk Configuration] をクリックします。必要なインターフェースの設定を変更し [Apply] をクリックします。

Port Configuration

Port	Name	Admin	Speed Duplex	Flow Control	Autonegotiation	Trunk
1		<input checked="" type="checkbox"/> Enabled	100full	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input type="checkbox"/> FC	
2		<input checked="" type="checkbox"/> Enabled	100full	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input type="checkbox"/> FC	
3		<input checked="" type="checkbox"/> Enabled	100full	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input type="checkbox"/> FC	
4		<input checked="" type="checkbox"/> Enabled	100full	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input type="checkbox"/> FC	

3.7.3 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 4 つの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 ポートの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

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

Member List (Current)

既存のトランク情報 (トランク ID、ユニット番号、ポート番号)

New

新規にトランクを作成するための入力欄

- **Trunk** トランク識別子 (範囲: 1-25)
- **Port** ポート識別子 (範囲: 1-50)

設定方法

[Port] [Trunk Membership] をクリックします。1 から 25 のトランク ID を Trunk に入力し、スクロールダウンリストからポート番号を選択し [Add] をクリックします。Member List へのポートの追加が完了した後、[Apply] をクリックします。

Trunk Membership

Member List:

Current: New:

(none)

<<Add Remove

Trunk (1-25) Port 1

LACP 設定

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。
- ◆ LACP により動的なトランクグループに設定されたトランク情報は、Member List 画面又は Trunk Membership 画面でも確認できます (P89)

設定・表示項目

Member List (Current)

既存のトランク情報 (ユニット番号、ポート番号)

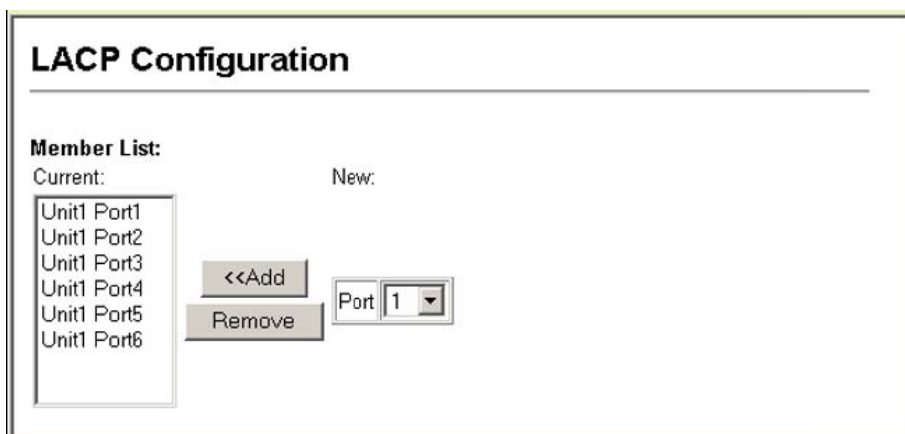
New

新規にトランクを作成するための入力欄

- **Port** ポート識別子 (範囲 : 1-50)

設定方法

[Port] [LACP] [Configuration] をクリックします。スクロールダウンリストからポートを選択し、[Add] をクリックします。Member List へのポートの追加が完了した後、[Apply] をクリックします。



LACP パラメータ設定

ポートチャンネルの動的設定 同一のポートチャンネルに指定されたポートは以下の条件を満たす必要があります。

- ◆ ポートは同一の LACP システムプライオリティです。
- ◆ ポートは同一の LACP ポートアドミンキーです。
- ◆ 「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。

[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

Set Port Actor 本メニューは LACP のローカル側（本機上）の設定を行ないます。

Port

ポート番号（範囲：1-50）

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）

- 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。
- 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。

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）

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）

Set Port Partner 本メニューは LACP のリモート側（接続された機器上のポート）の設定を行ないます。コマンドの意味は *Port Actor* と同様です。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。

設定方法

[Port] [LACP] [Aggregation Port] をクリックします。Port Actor のための System Priority, Admin Key, Port Priority の設定を行ないます。その他に Port Partner の設定を行なうこともできます（これらの設定は Port Partner の管理状態に対応し、次回の本機に対する LACP まで有効なりません）。すべての設定が完了後、[Apply] をクリックします。

The screenshot shows a web interface window titled "Aggregation Port". Inside, there is a section labeled "Set Port Actor:" followed by a table with 4 columns: "Port", "System Priority (0-65535)", "Admin Key (0-65535)", and "Port Priority (0-65535)". The table contains 9 rows of data.

Port	System Priority (0-65535)	Admin Key (0-65535)	Port Priority (0-65535)
1	3	120	32768
2	3	120	32768
3	3	120	32768
4	3	120	32768
5	3	120	32768
6	3	120	32768
7	3	120	32768
8	3	120	32768
9	3	120	512

LACP ポートカウンターの表示

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。

カウンター情報

項目	解説
LACPDU Sent	チャンネルグループから送信された有効な LACPDU の数
LACPDU 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
LACPDU 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
LACPDU 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

[Port] [LACP] [Port Counters Information] をクリックします。メンバーポートを選択すると関連する情報が表示されます。

LACP Port Counters Information

Member Port 1

Trunk ID : 2

LACPDU Sent	307	LACPDU Receive	296
Marker Sent	0	Marker Receive	0
Marker Unknown Pkts	0	Marker Illegal Pkts	0

ローカル側の LACP 設定及びステータスの表示

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
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

内部設定情報

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 State, Oper State	<p>Actor の管理値又は運用値の状態のパラメータ。</p> <ul style="list-style-type: none"> ◆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

[Port] [LACP] [Port Internal Information] をクリックします。port channel を選択すると関連する情報が表示されます。

LACP Port Internal Information

Interface Port 3

Trunk ID : 1

LACP System Priority	32738	LACP Port Priority	32768
Admin Key	3	Oper Key	3
LACPDUS Interval (secs)	30 seconds		
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✓	Oper State : Defaulted	
Admin State : Distributing		Oper State : Distributing	✓
Admin State : Collecting		Oper State : Collecting	✓
Admin State : Synchronization		Oper State : Synchronization	✓
Admin State : Aggregation	✓	Oper State : Aggregation	✓
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity	✓	Oper State : LACP-Activity	✓

リモート側の LACP 設定及びステータスの表示

LACP のリモート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。

隣接設定情報

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

[Port] [LACP] [Port Neighbors Information] をクリックします。表示する port channel を選択すると関連情報が表示されます。

LACP Port Neighbors Information

Interface
Port
2

Trunk ID : 1

Partner Admin System ID	32768, 00-00-00-00-00-00	Partner Oper System ID	32768, 00-12-CF-DF-9E-C0
Partner Admin Port Number	58	Partner Oper Port Number	2
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	4
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✓	Oper State : Defaulted	
Admin State : Distributing	✓	Oper State : Distributing	✓
Admin State : Collecting	✓	Oper State : Collecting	✓
Admin State : Synchronization	✓	Oper State : Synchronization	✓
Admin State : Aggregation		Oper State : Aggregation	✓
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	✓

3.7.4 ブロードキャストストームのしきい値の設定

ブロードキャストストームはネットワーク上のデバイスが誤作動した場合や、アプリケーションプログラムの設計が正しくない場合、適切に構成されていない時に起こります。ネットワーク上で過度のブロードキャストトラフィックが発生した場合、ネットワークの性能は大幅に低下し、通信が完全に中断されることがあります。

各ポートの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により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できます。指定されたしきい値を超えたブロードキャストパケットはドロップされます。

機能解説

- ◆ ブロードキャストストーム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を与えません。
- ◆ 指定されたしきい値はすべてのポートに適用されます。

設定・表示項目

Threshold

ポートを通過するブロードキャストパケットの毎秒当たりのパケット数をしきい値で設定できます（範囲：240-1488100 パケット / 秒）

Port

ポート番号

Type

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

Protect Status

ブロードキャストストームコントロールの有効 / 無効（初期設定：有効）

Trunk

トランクメンバーのポートの場合表示

設定方法

[Port] [Port Broadcast Control] をクリックします。Threshold (しきい値) を設定し、[Apply] をクリックします。

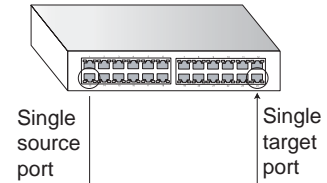
Broadcast Control

Threshold (240~1488100) packets/sec

Port	Type	Protect Status	Trunk
1	1000Base-TX	<input checked="" type="checkbox"/> Enabled	
2	1000Base-TX	<input checked="" type="checkbox"/> Enabled	
3	1000Base-TX	<input checked="" type="checkbox"/> Enabled	
4	1000Base-TX	<input checked="" type="checkbox"/> Enabled	
5	1000Base-TX	<input checked="" type="checkbox"/> Enabled	
6	1000Base-TX	<input checked="" type="checkbox"/> Enabled	
7	1000Base-TX	<input checked="" type="checkbox"/> Enabled	
8	1000Base-TX	<input checked="" type="checkbox"/> Enabled	
9	1000Base-TX	<input checked="" type="checkbox"/> Enabled	
10	1000Base-TX	<input checked="" type="checkbox"/> Enabled	

3.7.5 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ことができます。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

- ◆ 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。
- ◆ 当機器は、ソースポートとターゲットポートは一對一のミラーリングとなります。
- ◆ ソースポートとターゲットポートは同じ VLAN 内に所属する必要があります。

設定・表示項目

Mirror Sessions

現在のミラーセッションの一覧を表示します。

Source Port

通信がモニターされるソースポート

Type

モニターを行う通信の種類。

Rx（受信）、Tx（送信）（初期設定：Rx）

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

設定方法

[Port] [Mirror] をクリックします。Source Port (ソースポート) 及び Type (ミラーリングするトラフィックタイプ) そして Target Port (ターゲットポート) を指定し、[Add] をクリックします。

The screenshot shows a web interface titled "Mirror Port Configuration". It features a "Mirror Sessions:" section with a text box containing "Source: 1/10 Both Destination: 1/13". Below this text box are two buttons: "<<Add" and "Remove". To the right of the "Mirror Sessions:" section is a "New:" section with three dropdown menus: "Source Port" (set to 1), "Type" (set to Rx), and "Target Port" (set to 1).

3.7.6 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 又は Trunk

ポート番号

Rate Limit Status

帯域制御の有効 / 無効 (初期設定 : 無効)

Rate Limit (1-100)%

インタフェースの帯域の設定を行います。

設定方法

[Port] [Rate Limit] [Input Port/Trunk Configuration] をクリックします。各インタフェースに対して [Rate Limit Status] を選択し、[Rate Limit Level] を設定し、rate limit（帯域制御）の値を設定し、[Apply] をクリックします。

Input Rate Limit Port Configuration

Port	Input Rate Limit Status	Input Rate Limit (1-100)%	Trunk
1	<input type="checkbox"/> Enabled	<input type="text" value="100"/>	
2	<input type="checkbox"/> Enabled	<input type="text" value="100"/>	
3	<input type="checkbox"/> Enabled	<input type="text" value="100"/>	
4	<input type="checkbox"/> Enabled	<input type="text" value="100"/>	
5	<input type="checkbox"/> Enabled	<input type="text" value="100"/>	
6	<input type="checkbox"/> Enabled	<input type="text" value="100"/>	
7	<input type="checkbox"/> Enabled	<input type="text" value="100"/>	
8	<input type="checkbox"/> Enabled	<input type="text" value="100"/>	

3.7.7 ポート統計情報表示

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。

統計値

パラメータ	解説
<i>Interface Statistics</i>	
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
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
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
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
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
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。
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。
Transmit 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。
Transmit 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)
Transmit 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)
Transmit 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)
Transmit 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。
Transmit 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
<i>Etherlike Statistics</i>	
Alignment Errors	整合性エラー数 (同期ミスデータパケット)
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
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。
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。
Single Collision	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
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
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
Carrier Sense Errors	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

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
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
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
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
<i>RMON Statistics</i>	
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
Received Bytes	ネットワークから受信した総バイト数。本統計情報は容易なイーサネット利用状況の目安となります。
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 Frames	受信したすべてのフレーム数 (不良フレーム、ブロードキャストフレーム、マルチキャストフレーム)
Broadcast Frames	受信した正常なフレームのうちブロードキャストアドレスに転送したフレーム数。マルチキャストパケットは含まない。
Multicast Frames	信した正常なフレームのうち、このマルチキャストアドレスに転送したフレーム数
CRC/Alignment Errors	CRC/ 配列エラー数 (FCS 又は配列エラー)
Undersize Frames	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フレーム数で、その他の点では正常な受信フレーム数
Oversize Frames	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フレームで、その他の点では正常な受信フレーム数
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
64 Bytes Frames	不良パケットを含む送受信トータルフレーム数 (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 Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames	不良パケットを含む送受信トータルフレーム数で、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

[Port] [Port Statistics] をクリックします。表示するインタフェースを選択し [Query] をクリックします。

ページ下部の Refresh ボタンを使用することで、表示されている内容を最新の情報に更新することができます。

Port Statistics

Interface ☒ Port ☐ Trunk

Query

Interface Statistics:

Received Octets	15020	Received Unicast Packets	0
Received Multicast Packets	177	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	168087
Transmit Unicast Packets	0	Transmit Multicast Packets	2420
Transmit Broadcast Packets	47	Transmit Discarded Packets	0
Transmit Errors	0		

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

Refresh

3.8 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。

3.8.1 動的アドレステーブルの設定

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。

設定・表示項目

Static Address Counts

手動設定した静的アドレス数 *Web のみ

Current Static Address Table

静的アドレスの一覧

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

VLAN

VLAN ID(1-4094)

設定方法

[Address Table] [Static Addresses] をクリックします。インタフェース、MAC アドレス及び VLAN を設定し、[Add Static Address] をクリックします。

Static Addresses		
Static Address Counts	<input type="text" value="1"/>	
Current Static Address Table	00-E0-29-94-34-DE, VLAN 1, Unit 1, Port 1, Permanent	
Interface	<input checked="" type="radio"/> Port <input type="text" value="1"/>	<input type="radio"/> Trunk <input type="text"/>
MAC Address (XX-XX-XX-XX-XX-XX)	<input type="text"/>	
VLAN	<input type="text" value="1"/>	
<input type="button" value="Add Static Address"/> <input type="button" value="Remove Static Address"/>		

3.8.2 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

Interface

ポート又はトランク

MAC Address

インタフェースの MAC アドレス

VLAN

VLAN ID (1-4094)

Address Table 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

Dynamic Address Counts

動的に学習する MAC アドレス数

Current Dynamic Address Table

動的に学習された MAC アドレスのリスト

設定方法

[Address Table] [Dynamic Addresses] をクリックします。Query By (検索を行う種類) を Interface、MAC Address 又は VLAN から選択し、Address Table Sort Key (表示するアドレスの分類方法) を指定し、[Query] をクリックします。

Dynamic Addresses

Query by:

☐ Interface

☒ Port

☐ Trunk

☐ MAC Address

☐ VLAN

Address Table Sort Key

Address

Query

Dynamic Address Table	
Dynamic Address Counts	1
Current Dynamic Address Table	00-01-80-4B-82-93, VLAN 1, Unit 1, Port 1, Dynamic

3.8.3 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：10-30000 秒、初期設定：300 秒）

設定方法

[Address Table] [Address Aging] をクリックします。新しい Aging Time（エージングタイム）を設定し、[Apply] をクリックします。

Address Aging	
Aging Status	<input checked="" type="checkbox"/> Enabled
Aging Time (10-30000):	<input type="text" value="300"/> seconds

3.9 スパニングツリーアルゴリズム

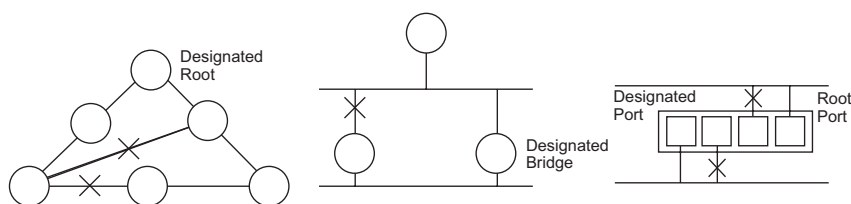
スパニングツリープロトコル STP はネットワークのループを防ぎ、また、スイッチ、ブリッジ及びルータ間のバックアップリンクを確保するために使用します。

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。

3.9.1 グローバル設定の表示

STP 情報ページから現在の STP の情報を確認することができます。

設定・表示項目

Spanning Tree State

STP が有効で STP ネットワークに参加しているかを表示します。

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。

Max Age

本機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（秒）が表示されます。

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すべての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。

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）が表示されます。

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）で表示されます。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。

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** ルートに最も近いポートの番号が表示されます。ルートデバイスとの通信は、このポートを介して行われます。ルートポートが存在しない場合は、本機がスパニングツリーネットワーク上のルートデバイスとして設定されたことを表します。
- **Root Path Cost** 本機のルートポートからルートデバイスまでのパスコストが表示されます。

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

[Spanning Tree] [STA Information] をクリックします。現在の STP 情報が表示されます。

STA Information			
Spanning Tree:			
Spanning Tree State	Enabled	Designated Root	32768.0012CF0B0D00
Bridge ID	32768.0012CF0B0D00	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	1
Forward Delay	15	Last Topology Change	0 d 0 h 16 min 23 s

3.9.2 グローバル設定

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、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。
 - 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

グローバル設定の基本設定

Spanning Tree State

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 Stree Protocol(IEEE 802.1w)
- **MSTP** Multiple Spanning Stree 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))

ルート機器設定

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 $[2 \times (\text{Forward Delay}-1)]$ 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)

RSTP 設定

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の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
- 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)

Configuration Digest

MD5 の署名キー。

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 (初期設定 : 65)

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)

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)

* MST name 及び revision number は MST の特定を行なうため、どちらも必要となります。

設定方法

[Spanning Tree] [STA Configuration] をクリックします。必要な設定項目を変更し、[Apply] をクリックします。

STA Configuration	
Switch:	
Spanning Tree State	<input checked="" type="checkbox"/> Enabled
Spanning Tree Type	MSTP ▼
Priority (0-61440), in steps of 4096	32768
When the Switch Becomes Root:	
Input Format: $2 * (\text{hello time} + 1) \leq \text{max age} \leq 2 * (\text{forward delay} - 1)$	
Hello Time (1-10)	2 seconds
Maximum Age (6-40)	20 seconds
Forward Delay (4-30)	15 seconds
RSTP Configuration:	
Path Cost Method	Long ▼
Transmission Limit (1-10)	3
MSTP Configuration:	
Max Instance Numbers	65
Configuration Digest	0xAC36177F50283CD4B83821D8AB26DE62
Region Revision (0-65535)	0
Region Name	00 13 f7 15 b2 e0
Max Hop Count (1-40)	20

3.9.3 インター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 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 Eddge 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トポ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。

Trunk Member

トランクメンバーに設定されているかどうかを表示します。(STA Port Information ページのみ)

設定方法

[Spanning Tree] [STA] [Port Information] 又は [Trunk Information] をクリックします。

STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Discarding	0	0	32768.0.0013F715B2E0	128.1	10000	Point-to-Point	Disabled	Disabled	
2	Enabled	Discarding	0	0	32768.0.0013F715B2E0	128.2	10000	Point-to-Point	Disabled	Disabled	
3	Enabled	Discarding	0	0	32768.0.0013F715B2E0	128.3	10000	Point-to-Point	Disabled	Disabled	
4	Enabled	Discarding	0	0	32768.0.0013F715B2E0	128.4	10000	Point-to-Point	Disabled	Disabled	
5	Enabled	Discarding	0	0	32768.0.0013F715B2E0	128.5	10000	Point-to-Point	Disabled	Disabled	
6	Enabled	Discarding	0	0	32768.0.0013F715B2E0	128.6	10000	Point-to-Point	Disabled	Disabled	
7	Enabled	Discarding	0	0	32768.0.0013F715B2E0	128.7	10000	Point-to-Point	Disabled	Disabled	

3.9.4 インターフェース設定

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ーフェースの 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 "インターフェース" 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。

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 P114 「インター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。

Trunk

トランクメンバーに設定されているかどうかを表示します。

(STA Port Configuration ページのみ)

以下の設定は変更することができます。

Spanning Tree

インターフェースの STA の有効 / 無効を設定します (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)

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)

- **設定範囲 :**

Ethernet: 200,000-20,000,000
Fast Ethernet: 20,000-2,000,000
Gigabit Ethernet: 2,000-200,000

- **初期設定 :**

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

[注意] パスコスト方式が short に設定された場合、最大パスコストは 65,535 となります。

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。

Admin Edge Port (Fast Forwarding)

ブリッジ型 LAN の終端、もしくはノードの終端にインタフェースが接続されている場合、本機能を有効にすることができます。

ノードの終端ではループが起きないため、直接、転送状態にすることができます。Edge Port を指定することにより、ワークステーションやサーバなどのデバイスへの迅速な転送を提供し、以前の転送アドレステーブルを保持することにより、スパニングツリー再構築時のタイムアウト時間を削減します。

但し、必ずノードの終端デバイスに接続されているポートのみで Edge Port を有効にして下さい (初期設定 : 有効)

Migration

設定及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 又は STP 互換) の再確認を行うことができます。

設定方法

[Spanning Tree] [STA] [Port Configuration] 又は [Trunk Configuration] をクリックします。必要な設定項目を変更し、[Apply] をクリックします。

Port	Spanning Tree	STA State	Priority (0-240), in steps of 16	Path Cost (1-200000000)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	<input checked="" type="checkbox"/> Enabled	Forwarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
2	<input checked="" type="checkbox"/> Enabled	Discarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
3	<input checked="" type="checkbox"/> Enabled	Discarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
4	<input checked="" type="checkbox"/> Enabled	Discarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
5	<input checked="" type="checkbox"/> Enabled	Discarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
6	<input checked="" type="checkbox"/> Enabled	Discarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	

3.9.5 MSTP 設定 (MSTP VLAN Configuration)

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 65 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 (P110 「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 Instance

スパニングツリーのインスタンス ID (初期設定 : 0)

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）

VLANs in MST Instance

インスタンスに指定された VLAN

MST ID

設定のためのインスタンス ID（設定範囲：0-57、初期設定：0）

VLAN ID

MST インスタンスに指定する VLAN ID（設定範囲：1-4093）

他の項目は、P114「インターフェース設定の表示」を参照して下さい。

設定方法

[Spanning Tree] [MSTP] [VLAN Configuration] をクリックします。リストから MST インスタンス ID を選択し、インスタンスプライオリティを設定し、[Add] をクリックします。MST インスタンスに VLAN を加えるには、インスタンス ID と VLAN ID を入力し、[Add] をクリックします。

MSTP Vlan Configuration

MST Instance ID: 2

Spanning Tree State	Enabled	Designated Root	4096.2.0000E9313131
Bridge ID	4096.0.0000E9313131	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	0
Forward Delay	15	Last Topology Change	0 d 0 h 4 min 14 s

Priority (0-61440) 4096

MSTP Vlan Configuration:

Vlan in MST Instance:

Vlan 2

Remove

MST Id (0-57): Vlan Id:

Add

3.9.6 MSTP インターフェース設定の表示

MSTP ポート/トランク情報ページでは、選択した MST インスタンスの現在のステータスを表示することができます。

設定・表示項目

MST Instance ID

インスタンス ID (設定範囲 : 0-4094、初期設定 : 0)

[注意] 他の項目に関しては P3-80 「インタフェース設定の表示」を参照して下さい。

設定方法

[Spanning Tree] [MSTP] [Port Information] 又は [Trunk Information] をクリックします。
MST インスタンスを選択し、現在の Spanning Tree の値を表示します。

MSTP Port Information										
MST Instance ID: <input type="text" value="0"/>										
Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Discarding	0	0	32768.0.0013F715B2E0	128.1	10000	Point-to-Point	Disabled	Disabled	
2	Discarding	0	0	32768.0.0013F715B2E0	128.2	10000	Point-to-Point	Disabled	Disabled	
3	Discarding	0	0	32768.0.0013F715B2E0	128.3	10000	Point-to-Point	Disabled	Disabled	
4	Discarding	0	0	32768.0.0013F715B2E0	128.4	10000	Point-to-Point	Disabled	Disabled	
5	Discarding	0	0	32768.0.0013F715B2E0	128.5	10000	Point-to-Point	Disabled	Disabled	

3.9.7 MSTP インターフェースの設定

MSTP ポート / トランク設定により 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

以下の項目は設定を変更できません。

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 P3-135 「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。

Trunk Member

トランクメンバーに設定されているかどうかを表示します。

(STA Port Configuration ページのみ)

以下の項目は設定を変更できます。

MST Instance ID

設定のインスタンス ID (設定範囲：0-4094、初期設定：0)

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なります (初期設定：128、範囲：0-240 の 16 ずつ)

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)

- 設定範囲：

Ethernet: 200,000-20,000,000

Fast Ethernet: 20,000-2,000,000

Gigabit Ethernet: 2,000-200,000

- 初期設定：

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

[注意] パスコスト方式が short に設定された場合、最大パスコストは 65,535 となります。

設定方法

[Spanning Tree] [MSTP] [Port Configuration] 又は [Trunk Configuration] をクリックします。インタフェースのプライオリティ及びパスコストを設定し、[Apply] をクリックします。

Port	STA State	Priority (0-240)	MST Path Cost (1-200000000)	Trunk
1	Forwarding	128	100000	
2	Discarding	128	10000	
3	Discarding	128	10000	
4	Discarding	0	50	
5	Discarding	128	10000	

3.10 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 256VLAN 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 へポートの割り当て

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。

[注意] 本機の VLAN の仕様については、P342「VLAN」も併せてご参照下さい。

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。

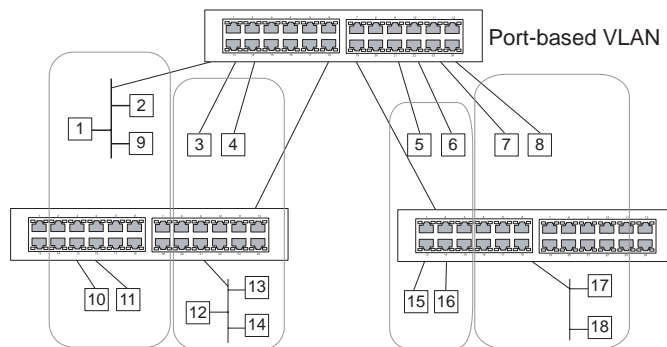
VLAN に割り当てられたユーザグループが、他の VLAN と分けられたブロードキャストドメインとなります。パケットは同じ VLAN 内の指定されたポート間でのみ送信されます。タグなし VLAN は手動でのユーザグループ又はサブネットの分割が行えます。また、GVRP を使用した IEEE802.3 タグ VLAN により、完全に自動化した VLAN 登録を行うことも可能となります。

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・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。

3.10.1 GVRP の有効・無効 (Global Setting)

GARP VLAN Registration Protocol (GVRP) は、VLAN 情報の交換を行いネットワーク上の VLAN メンバーポートの登録を行なう方法を定義します。VLAN はネットワーク上のホストデバイスにより発行された join メッセージにより、自動的に設定されます。自動的な VLAN の登録を許可するためには、GVRP を有効にする必要があります (初期設定: Disabled)

設定方法

[VLAN] [802.1Q VLAN] [GVRP Status] をクリックします。GVRP を有効 (Enable) 又は無効 (Disable) に設定し、[Apply] をクリックします。

GVRP Status	
GVRP	<input checked="" type="checkbox"/> Enable

3.10.2 VLAN 基本情報の表示

VLAN 基本情報ページでは本機でサポートしている VLAN の種類などの基本的な情報を表示します。

設定・表示項目

VLAN Version Number

本機で使用している IEEE 802.1Q 標準の VLAN のバージョン

Maximum VLAN ID

本機で認識可能な VLAN ID の最大値

Maximum Number of Supported VLANs

本機で設定することのできる最大 VLAN 数

設定方法

[VLAN] [802.1Q VLAN] [Basic Information] をクリックします。

VLAN Basic Information	
VLAN Version Number	1
Maximum VLAN ID	4094
Maximum Number of Supported VLANs	255

3.10.3 現在の VLAN 表示

VLAN Current Table は、現在の各 VLAN のポートメンバー及びポートが VLAN タギングに対応しているかを表示します。複数のスイッチ間の大きな VLAN グループに参加するポートは VLAN タギングを使う必要があります。しかし、1 台又は 2 台程度のスイッチによる VLAN を作成する場合には、VLAN タギングを無効にすることができます。

設定・表示項目

VLAN ID

設定されている VLAN の ID (1-4094)

Up Time at Creation

VLAN が作成されてからの経過時間

Status

VLAN の設定方法：

- Dynamic GVRP GVRP を使用しての自動学習
- Permanent 静的な手動設定

Egress Ports

すべての VLAN ポートメンバー

Untagged Ports

タグなし VLAN ポートメンバー

設定方法

[VLAN] [802.1Q VLAN] [Current Table] をクリックします。スクロールダウンリストから VLAN ID を選択します。

The screenshot shows the 'VLAN Current Table' configuration window. It includes a 'VLAN ID' dropdown menu set to '1'. Below it, 'Up Time at Creation' is displayed as '0 d 0 h 0 min 18 s' and 'Status' is set to 'Permanent'. There are two sections for port configuration: 'Egress Ports' and 'Untagged Ports'. Each section contains a list of ports from 'Unit1 Port1' to 'Unit1 Port8' with checkboxes for selection. The 'Egress Ports' section has all ports selected, while the 'Untagged Ports' section has none selected.

3.10.4 VLAN の作成

VLAN Static List を使用し、VLAN グループの作成及び削除が行えます。外部のネットワーク機器へ本機で使用されている VLAN グループに関する情報を伝えるため、これらの VLAN グループそれぞれに VLAN ID を設定する必要があります。

設定・表示項目

Current

このシステムを作成する全ての現在の VLAN グループを表示します。最大 256 個の VLAN グループを設定することができます。VLAN 1 はデフォルトタグなし VLAN です。

New

新しい VLAN グループの名前及び ID を設定します。(VLAN 名は本機で管理用に利用され、VLAN タグには記載されません)

VLAN ID

設定した VLAN の ID (1 から 4094)

VLAN Name

VLAN 名 (1 から 32 文字)

Status (Web)

この VLAN を有効にします。

- **Enable:** VLAN は使用することができます。
- **Disable:** VLAN は停止されます。

Status (CLI)

この VLAN を有効にします。

- **Active:** VLAN は使用することができます。
- **Suspend:** VLAN は停止されます。

Add

リストに新しい VLAN グループを追加します。

Remove

リストから VLAN グループを削除します。ポートがタグなしポートとしてこのグループに割り当てられている場合、タグなしポートとして VLAN 1 に割り当てられます。

設定方法

[VLAN] [802.1Q VLAN] [Static List] をクリックします。VLAN ID と VLAN Name を入力し VLAN をアクティブにするために Enable チェックボックスをチェックし、[Add] をクリックします。

VLAN Static List

Current:		New:
1, DefaultVlan, Enabled	<<Add	VLAN ID (1-4094) 2
	Remove	VLAN Name R&D
		Status <input checked="" type="checkbox"/> Enabled

3.10.5 VLAN への静的メンバーの追加 (VLAN Index)

ポートメニューを使用し、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。

[注意] P131 「VLAN への静的メンバーの追加 (Port Index)」でも、ポートインデックスを元に VLAN グループの設定を行なうことができますが、タグ付としてしかポートの追加はできません。

[注意] VLAN 1 は本機のすべてのポートが参加するデフォルトタグなし VLAN です。P132 「インターフェースの VLAN 動作の設定」にあるデフォルトポート VLAN ID を変更することにより修正することができます。

設定・表示項目

VLAN

設定された VLAN ID (1 から 4094)

Name

VLAN 名 (1 から 32 文字)

Status

この VLAN が有効か無効かを表示します。

- **Enable:** VLAN は使用することができます。
- **Disable:** VLAN は停止されます。

Port

ポート番号

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 P2-97 「GVRP」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。
- **Trunk Member**

ポートがトランクメンバーの場合に表示されます。VLAN でのトランクを追加するためには、ページ下部のテーブルを使用します。

設定方法

[VLAN] [802.1QVLAN] [Static Table] をクリックします。スクロールダウンリストから VLAN ID を選択します。VLAN の Name と Status を必要に応じて変更します。各ポート又はトランクの適切なラジオボタンをマークしメンバーシップの種類を選択して、[Apply] をクリックします。

VLAN Static Table

VLAN: 2

Name R&D

Status ☒ Enable

Port	Tagged	Untagged	Forbidden	None	Trunk Member
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	

3.10.6 VLAN への静的メンバーの追加 (Port Index)

静的 VLAN メンバーシップを使用し、VLAN グループを選択したインタフェースにタグ付メンバーとして追加します。

設定・表示項目

Interface

ポート又はトランク番号

Member

選択されたインタフェースがタグ付メンバーとして登録されている VLAN

Non-Member

選択されたインタフェースがタグ付メンバーとして登録されていない VLAN

設定方法

[VLAN] [802.1Q VLAN] [Static Membership] をクリックします。スクロールダウンリストからインタフェースを選択します。[Query] をクリックし、インタフェースのメンバーシップインフォメーションを表示します。VLAN ID を選択し、インタフェースをタグ付メンバーとして追加するために [Add] をクリックします。インタフェース削除する場合には [Remove] をクリックします。

各インタフェースの VLAN メンバーシップの設定後、[Apply] をクリックします。

The screenshot displays the 'VLAN Static Membership by Port' configuration page. At the top, there's a title. Below it, the 'Interface' is set to 'Port 3' and 'Trunk' is selected. A 'Query' button is present. The 'Member' list contains 'Vlan 1', and the 'Non-Member' list contains 'Vlan 2'. Between these lists are buttons for '<< Add' and 'Remove >>'.

3.10.7 インターフェースの VLAN 動作の設定

デフォルト VLAN ID、利用可能なフレームの種類、イングレスフィルタリング、GVRP ステータス及び GARP タイマーを含む各インターフェースの VLAN に関する動作の設定を行うことができます。

機能解説

- ◆ GVRP GARP VLAN 登録プロトコルはネットワークを通るインターフェースの VLAN メンバーを自動的に登録するために VLAN 情報を交換するためのスイッチへの方法を決定します。
- ◆ GARP グループアドレス登録プロトコルはブリッジ LAN 内のクライアントサービスのためにクライアント属性を登録または登録の取り消しのための GVRP により使用されます。GARP タイマーの初期値はメディアアクセス方法又はデータ転送速度の独立したものです。これらの値は GVRP 登録又は登録の取り消しの問題に直面しない限り変更されません。

設定・表示項目

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)

- インターフェースが 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、インター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」(129 ページの「VLAN への静的メンバーの追加 (VLAN Index)」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。

例) Port1 の PVID を "30" に設定する場合

- Static Table にて、Port1 を VLAN30 の Tag なしメンバーの設定する。
- Port Configuration にて、Port1 の PVID を "30" に設定する。

* あらかじめ、Static List にて VLAN30 を作成しておいてください。

Acceptable Frame Type(受け入れ可能なフレームの種類)

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常に Enabled になります。
- 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。

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（P3-11「ブリッジ拡張機能の表示」を参照してください）。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：有効）

GARP Join Timer*

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 から 1000 センチセカンド、初期設定：20）

GARP Leave Timer*

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 から 3000 センチセカンド、初期設定：60）

GARP LeaveAll Timer*

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 から 18000 センチセカンド、初期設定：1000）

* GARP タイマー設定は以下の規則に沿って設定して下さい：

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

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）

- 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。
- 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。

Trunk Member

ポートがトランクメンバーの場合に表示されます。VLAN でのトランクを追加するためには、ページ下部のテーブルを使用します。

設定方法

[VLAN] [802.1Q VLAN] [Port Configuration] 又は [VLAN Trunk Configuration] をクリックします。各インタフェースで必要な項目を設定し [Apply] をクリックします。

VLAN Port Configuration									
Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer (Centi Seconds) (20-1000)	GARP Leave Timer (Centi Seconds) (60-3000)	GARP LeaveAll Timer (Centi Seconds) (500-18000)	Mode	Trunk Member
1	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000	Hybrid	
2	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000	Hybrid	
3	3	Tagged	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000	Hybrid	
4	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000	Hybrid	
5	1	ALL	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	30	90	2000	Hybrid	
6	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000	Hybrid	

3.10.8 プライベート VLAN の設定

プライベート VLAN は、ポートベースでのセキュリティの確保と VLAN 内のポート間の分離を行うことができます。本機はプライマリ VLAN と、セカンダリ VLAN の 2 種類をサポートしています。プライマリ VLAN には無差別ポートがあり、このポートは同じプライベート VLAN に所属する他のポートと通信が可能です。セカンダリ (コミュニティ) VLAN にはコミュニティポートがあり、このポートは同じセカンダリ VLAN 内の他のホスト、又は関連付けを行ったプライマリ VLAN の任意の無差別ポートとのみ通信が可能です。独立 VLAN は、1 つの無差別ポートと 1 つ以上の独立 (又はホスト) ポートから構成される、単一のスタンドアロンの VLAN です。いずれの VLAN も無差別ポートはインターネットなど外部ネットワークからのアクセスが可能ですが、コミュニティ / 独立ポートはローカルユーザからのアクセスのみに制限されます。

本機には複数のプライマリ VLAN を設定でき、又複数のコミュニティ VLAN を各プライマリ VLAN と関連付けできます。独立 VLAN も 1 つ以上設定できます (プライベート VLAN と通常の VLAN は同一スイッチ内に同時に構成することができることに注意して下さい)

プライマリグループ、セカンダリグループに設定するには、次の方法で行います。

- (1) Private VLAN Configuration 画面 (P3-100) で 1 つ以上のコミュニティ VLAN と、VLAN グループ以外のトラフィックのやり取りをするプライマリ VLAN を 1 つ指定します。
- (2) Private VLAN Association 画面 (P137) で、セカンダリ (コミュニティ) VLAN とプライマリ VLAN とのマッピングを行ないます。

- (3) Private VLAN Port Configuration 画面 (P136) でポートの種類を Promiscuous (プライマリ VLAN のすべてのポートへアクセス可能な無差別ポート) 又は Host (コミュニティ VLAN から、又コミュニティ VLAN 以外の場合は無差別ポートへのアクセスのみ可能) から指定します。その後、任意の無差別ポートをプライマリ VLAN とコミュニティ VLAN のホストポートに指定します。

独立 VLAN に設定するには、次の方法で行います。

- (1) Private VLAN Configuration 画面 (P136) ですべてのトラフィックが経由する無差別ポートを 1 つ設定します。
- (2) Private VLAN Port Configuration 画面 (P139) でポートの種類を Promiscuous (外部ネットワークとの単一の経路となる) 又は Isolated (同一 VLAN の無差別ポートへのアクセスのみ可能) から指定します。その後、設定した無差別ポートと独立 (ホスト) ポートを独立 VLAN に指定します。

現在のプライベート VLAN の表示

Private VLAN Information 画面に、プライマリ VLAN、コミュニティ VLAN、独立 VLAN、各 VLAN に関連付けられたインタフェースなど、本機に設定したプライベート VLAN 情報を表示します。

設定・表示項目

VLAN ID

表示する VLAN ID (1-4094) と VLAN の種類

Primary VLAN

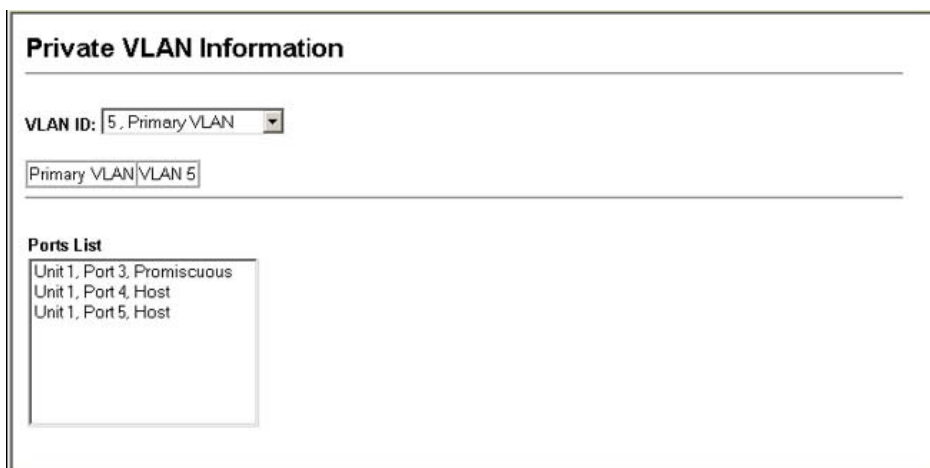
表示している VLAN ID に関連付けされている VLAN。プライマリ VLAN の場合は自身の VLAN ID を、コミュニティ VLAN の場合は関連付けされているプライマリ VLAN ID を、又独立 VLAN はスタンドアロンの VLAN を表示します。

Ports List

表示しているプライベート VLAN に所属するポート (ポートの種類)

設定方法

[VLAN] [Private VLAN] [Information] をクリックします。ドロップダウンリストから表示させたいポートを選択します。



The screenshot shows the 'Private VLAN Information' configuration window. It contains a 'VLAN ID' dropdown menu with '5, Primary VLAN' selected. Below it is a text field containing 'Primary VLAN|VLAN 5'. At the bottom, there is a 'Ports List' box containing three entries: 'Unit 1, Port 3, Promiscuous', 'Unit 1, Port 4, Host', and 'Unit 1, Port 5, Host'.

プライベート VLAN の設定

Private VLAN Configuration 画面で、プライマリ VLAN、コミュニティ VLAN、独立 VLAN の作成、削除を行います。

設定・表示項目

VLAN ID

設定する VLAN ID (1-4094)

Type

プライベート VLAN には次の 3 つの種類があります。

- **Primary** セカンダリ (コミュニティ) VLAN 内で、無差別ポートとコミュニティポート間でデータをやり取りします。
- **Community** 関連付けたプライマリ VLAN 内で、無差別ポートとコミュニティポート間でデータをやり取りします。
- **Isolated** その VLAN 内で、無差別ポートと独立ポート間のみでデータをやり取りします。同一 VLAN 内の独立ポート同士の通信は遮断されます。

Current

設定済みの VLAN のリスト

設定方法

[VLAN] [Private VLAN] [Configuration] をクリックします。VLAN ID に VLAN ID 番号を入力し、Type から Primary、Isolated、Community を選択し、その後 [Add] をクリックします。本機に設定したプライベート VLAN を削除するには、削除する項目を Current リストから選択して反転表示させ、[Remove] をクリックします。VLAN を削除する前にその VLAN に所属するポートをすべて削除しておかなくてはなりません。

The screenshot shows the 'Private VLAN Configuration' window. On the left, under 'Current:', there is a list box containing three items: '5, Primary VLAN', '6, Community VLAN', and '7, Community VLAN'. To the right of this list are two buttons: '<<Add' and 'Remove'. Further right, under 'New:', there are two input fields. The first is labeled 'VLAN ID (1-4094)' and is empty. The second is labeled 'Type' and has a dropdown menu currently set to 'Primary'.

VLAN の関連付け

コミュニティ VLAN とプライマリ VLAN は関連付けを行う必要があります。

設定・表示項目

Primary VLAN ID

プライマリ VLAN ID (1-4094)

Association

選択したプライマリ VLAN と既に関連付けられているコミュニティ VLAN

Non-Association

選択したプライマリ VLAN と関連付けられていないコミュニティ VLAN

設定方法

[VLAN] [Private VLAN] [Association] をクリックします。Primary VLAN ID ドロップダウンボックスから設定するプライマリ VLAN を選択します。Non-Association リストボックスの 1 つまたは複数のコミュニティ VLAN を選択して反転表示させ、[Add] をクリックします。コミュニティ VLAN が選択したプライマリ VLAN に関連付けられます（コミュニティ VLAN は 1 つのプライマリ VLAN にしか所属できません）。



The image shows a web interface window titled "Private VLAN Association". It contains a "Primary VLAN ID:" dropdown menu with the value "5" selected. Below this are two list boxes: "Association:" containing "(none)" and "Non-Association:" containing "6. Community Vlan" and "7. Community Vlan". Between the lists are two buttons: "<<Add" and "Remove".

【注意】 本機の仕様では、全てのパケットは初期設定で所属 VLAN のタグ付きとなります。そのため、本機に直接接続した PC 同士は、異なる VLAN 間（例：Primary VLAN10 と Community VLAN20）での通信は Association の有無にかかわらず不可となります。

プライベート VLAN インタフェース情報の表示

Private VLAN Port Information 及び Private VLAN Trunk Information 画面で、プライベート VLAN に関連付けられているインタフェース情報を表示します。

設定・表示項目

Port 又は Trunk

本機のインタフェース

PVLAN Port Type

プライベート VLAN のポートの種類を表示します。

- **Normal** このポートはプライベート VLAN での設定はありません。
- **Host** コミュニティポートに設定されており、同一コミュニティ VLAN に所属するポートと、又は指定された無差別ポートとのみ通信が可能です。あるいは、独立ポートに設定されており、同一の独立 VLAN に所属する無差別ポートとのみ通信が可能です。
- **Promiscuous** 無差別ポートに設定されており、プライベート VLAN 内のすべてのポートと通信が可能です。

Primary VLAN

セカンダリ (コミュニティ) VLAN 内で、無差別ポート同士、又は無差別ポートとコミュニティポート間でデータをやり取りします。

Community VLAN

コミュニティ VLAN。コミュニティポート間、又はコミュニティポートと指定した無差別ポート間でデータをやり取りします。

Isolated VLAN

特定の VLAN の独立ポートと無差別ポート間のみでデータをやり取りします。同一 VLAN 内の独立ポート同士の通信は遮断されます。

Trunk

トランク識別子 (Port Information 画面のみ)

設定方法

[VLAN] [Private VLAN] [Port Information] 又は [Trunk Information] をクリックします。

Private VLAN Port Information					
Port	PVLAN Port Type	Primary VLAN	Community VLAN	Isolated VLAN	Trunk
1	Normal				
2	Normal				
3	Promiscuous	5			
4	Host		6		
5	Host		6		
6	Normal				
7	Normal				
8	Normal				

プライベート VLAN インタフェースの設定

Private VLAN Port Configuration 及び Private VLAN Trunk Configuration 画面で、プライベート VLAN のインタフェース種類の設定と、インタフェースのプライベート VLAN への割り当てを行います。

設定・表示項目

Port 又は Trunk

本機のインタフェース

PVLAN Port Type

プライベート VLAN のポートの種類を設定します。

- **Normal** このポートはプライベート VLAN に割り当てません。

- **Host** コミュニティポート又は独立ポートに設定します。コミュニティポートは、同一コミュニティ VLAN に所属するポートと、又は指定された無差別ポートとのみ通信が可能です。独立ポートは、同一の独立 VLAN に所属する無差別ポートとのみ通信が可能で、他の Host ポートとは通信できません。
- **Promiscuous** 無差別ポートに設定します。プライベート VLAN 内のすべてのポートと通信が可能です。

Primary VLAN

関連付けたセカンダリ (コミュニティ) VLAN 内で、無差別ポート同士、又は無差別ポートとコミュニティポート間でデータをやり取りします。

Community VLAN

コミュニティ VLAN。コミュニティポート間、又はコミュニティポートと指定した無差別ポート間でデータをやり取りします。PVLAN Port Type を "Host" に設定し、関連付けたコミュニティ VLAN を設定します。

Isolated VLAN

特定の VLAN の独立ポートと無差別ポート間のみでデータをやり取りします。同一 VLAN 内の独立ポート同士の通信は遮断されます。PVLAN Port Type を "Host" に設定し、"Isolated VLAN" チェックボックスをクリックして独立 VLAN を設定し、ドロップダウンリストから VLAN を設定します。

設定方法

[VLAN] [Private VLAN] [Port Configuration] 又は [Trunk Configuration] をクリックします。プライベート VLAN に所属させるポートを PVLAN Port Type で設定します。無差別ポートをプライマリ VLAN または独立 VLAN に割り当てます。ホストポートをコミュニティ VLAN または独立 VLAN に割り当てます。すべてのポートを設定したら、[Apply] をクリックします。

Private VLAN Port Configuration

Port	PVLAN Port Type	Primary VLAN	Community VLAN	Isolated VLAN	Trunk
1	Normal	(none)	(none)	<input type="checkbox"/> (none)	
2	Normal	(none)	(none)	<input type="checkbox"/> (none)	
3	Promiscuous	5	(none)	<input type="checkbox"/> (none)	
4	Host	(none)	6	<input type="checkbox"/> (none)	
5	Host	(none)	6	<input type="checkbox"/> (none)	
6	Normal	(none)	(none)	<input type="checkbox"/> (none)	
7	Normal	(none)	(none)	<input type="checkbox"/> (none)	
8	Normal	(none)	(none)	<input type="checkbox"/> (none)	

3.11 プライオリティ

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 8 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。各インター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。

3.11.1 インターフェースへのデフォルトプライオリティの設定

各インター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 8 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 のタグなしメンバーの場合、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

Default Priority

各インターフェースの受信されたタグな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)

Number of Egress Traffic Classes

各ポートに割り当てられたキューバッファの値

設定方法

[Priority] [Default Port Priority] 又は [Default Trunk Priority] をクリックします。インターフェースのデフォルトプライオリティを変更し、[Apply] をクリックします。

Default Port Priority

Port	Default Priority (0-7)	Number of Egress Traffic Classes	Trunk
1	<input type="text" value="0"/>	8	
2	<input type="text" value="0"/>	8	
3	<input type="text" value="0"/>	8	
4	<input type="text" value="0"/>	8	
5	<input type="text" value="0"/>	8	
6	<input type="text" value="0"/>	8	
7	<input type="text" value="0"/>	8	

3.11.2 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。

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

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

設定・表示項目

Priority

CoS 値 (範囲 :0 から 7、7 が最高プライオリティ)

Traffic Class

アウトプットキューバッファ (範囲 :0 から 7、7 が最高 CoS プライオリティキュー)

設定方法

[Priority] [Traffic Classes] をクリックします。各インタフェースのアウトプットキューへプライオリティ (Traffic Class) を割り当て、[Apply] をクリックします。

Traffic Classes

Priority	Traffic Class
0	<input type="text" value="1"/> (0-7)
1	<input type="text" value="0"/> (0-7)
2	<input type="text" value="2"/> (0-7)
3	<input type="text" value="3"/> (0-7)
4	<input type="text" value="4"/> (0-7)
5	<input type="text" value="5"/> (0-7)
6	<input type="text" value="6"/> (0-7)
7	<input type="text" value="7"/> (0-7)

3.11.3 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 ルールにより生じる HOL Blocking を防ぐことができます（初期設定では WRR に設定されています）

設定・表示項目

WRR

Weighted Round-Robin ではイングレスポートの帯域を それぞれの 0-7 のキューに対して 1, 2, 4, 6, 8, 10, 12, 14 のスケジューリングウェイトを設定し共有します。

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

設定方法

[Priority] [Queue Mode] をクリックします。Strict 又は WRR を選択し、[Apply] をクリックします。



The screenshot shows a web interface for configuring the queue mode. At the top, there is a header 'Queue Mode'. Below it, there is a dropdown menu with the label 'Queue Mode' and the value 'WRR' selected. The dropdown is enclosed in a rectangular box.

トラフィッククラスのスービスウェイトの設定

本機は各プライオリティキューの提供をする時に重み付けラウンドロビン (WRR) アルゴリズムを使用しています。P142 「Egress キューへの CoS 値のマッピング」に記載されているように、トラフィッククラスは各ポートに供給された 8 つの Egress キューのうちの一つにマッピングされます。これらのキューと対応しているトラフィックプライオリティのそれぞれへのウェイトを割り当てることができます。このウェイトは、各キューがサービスに登録され、それにより、特定のプライオリティ値に応じたソフトウェア・アプリケーション毎のレスポンス時間に影響する頻度が設定されます。

設定・表示項目

WRR Setting Table

各トラフィッククラス (キュー) のウェイトの値を表します。

Weight Value

選択されたトラフィッククラスの新しいウェイトを設定します。(範囲:1-15)

設定方法

[Priority] [Queue Scheduling] をクリックします。インタフェースを選択し、トラフィッククラスを選択します。ウェイト値を入力後、[Apply] をクリックします。

Queue Scheduling

WRR Setting Table	<div>Traffic Class 0 - weight 1 Traffic Class 1 - weight 2 Traffic Class 2 - weight 4 Traffic Class 3 - weight 6 Traffic Class 4 - weight 8</div>
Weight Value (1-31)	<input type="text"/>

3.11.4 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。

異なったプライオリティ情報が通信に含まれている可能性があるため、本機は次の方法で出力キューへプライオリティ値をマッピングしています：

- ◆ プライオリティマッピングの優先順位は DSCP プライオリティ、デフォルトポートプライオリティの順番となります。

DSCP プライオリティの選択

本機は、DSCP プライオリティによるサービスの有効 / 無効を設定することができます。

設定・表示項目

Enabled

DSCP のサービスを有効にします。(初期設定：無効)

IP DSCP

DSCP を使用し L3/L4 プライオリティをマッピングします。

設定方法

[Priority] [IP DSCP Priority Status] をクリックします。DSCP Priority Status メニューから Enabled にチェックを入れます。その後 [Apply] をクリックします。

IP DSCP Priority Status	
IP DSCP Priority Status	<input type="checkbox"/> Enabled

3.11.5 DSCP プライオリティのマッピング

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。DSCP 初期設定値は次の表で定められます。指定されていない全ての DSCP 値は CoS 値 0 にマッピングされます：

IP DSCP 値	CoS 値
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

設定・表示項目

DSCP Priority Table

CoS 値と各 DSCP プライオリティの相関マップを表示します。

Class of Service Value

選択された DSCP プライオリティ値へ CoS 値をマッピングします。"0" が低いプライオリティ、"7" が高いプライオリティを示します。

[注意] IP DSCP 設定はすべてのインタフェースに対して有効となります。

設定方法

[Priority] [IP DSCP Priority] をクリックします。DSCP Priority Table から DSCP プライオリティ値を選択し、Class of Service Value 欄で値を入力し、[Apply] をクリックします。

IP DSCP Priority

DSCP Priority Table

DSCP 0 - CoS 0

DSCP 1 - CoS 0

DSCP 2 - CoS 0

DSCP 3 - CoS 0

DSCP 4 - CoS 0

DSCP 5 - CoS 0

DSCP 6 - CoS 0

Class of Service Value (0-7)

Restore Default

ACL への CoS 値のマッピング

ACL CoS マッピングページでは、ACL ルールに一致したパケットに対する出力キューの設定が以下の表に基づき設定を行うことができます。指定した CoS 値は一致したパケットの出力キューにのみ機能し、パケット自体に CoS 値が記入されることはありません。詳細は P142「Egress キューへの CoS 値のマッピング」を参照して下さい。

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

機能解説

CoS 値をルールにマッピングする前に ACL マスクの設定を行なう必要があります。

設定・表示項目

Port

ポート番号

Name*

ACL 名

Type

ACL タイプ

CoS Priority

ACL ルールに一致するパケットの CoS 値（設定範囲：0-7）

ACL CoS Priority Mapping

設定情報を表示します

* 詳細は P79「ACL の設定」を参照して下さい。

設定方法

[Priority] [ACL CoS Priority] をクリックします。各ポートへのマッピングを有効にします。
スクロールダウンリストから ACL を選択し、[Apply] をクリックします。

ACL CoS Priority

ACL CoS Priority Configure

Port	Name,Type	CoS Priority (0-7)	
1	bill,IP		Add

ACL CoS Priority Mapping

Port	Name	Type	CoS Priority	
1	bill	IP	0	Remove

3.12 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/スイッチ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。

3.12.1 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。

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。

IGMP Snooping Query 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

- ◆ GMP 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、それによってマルチキャストフィルタの設定を行います。
- ◆ IGMP Query 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 Status

有効にした場合、本機はネットワークの通信を監視し、マルチキャストトラフィックを必要とするホストを特定します。これは IGMP Snooping と呼ばれます。

(初期設定 : 有効 (Enabled))

Act as IGMP Querier

有効にした場合、本機はクエリアとして機能し、ホストに対しマルチキャストトラフィックが必要かを聞きます。

(初期設定 : 有効 (Enabled))

IGMP Query Count

応答を受けて、レポートの要求を開始するまで送信するクエリの最大数を入力します。

(2-10、初期設定 : 2)

IGMP Query Interval

IGMP クエリメッセージを送信する間隔 (秒) を指定します (60-125、初期設定 : 125)

IGMP Report Delay

IP マルチキャストアドレスのレポートをポートで受信してから、IGMP クエリがそのポートから送信され、リストからエントリーが削除されるまでの時間（秒）を設定します（5-25、初期設定：10）

IGMP Query Timeout

前のクエリアが停止した後、クエリパケットを受信していたルータポートが無効と判断されるまでの時間（秒）を設定します（300-500、初期設定：300）

IGMP Version

ネットワーク上の他のデバイスと互換性のある IGMP バージョンの設定を行います（1-2、初期設定：2）

[注意] サブネット上のすべてのデバイスが同じバージョンをサポートしている必要があります。

[注意] IGMP Report Delay 及び IGMP Query Timeout は IGMP v2 でのみサポートされます。

設定方法

[IGMP Snooping] [IGMP Configuration] をクリックします。必要な IGMP の設定を行い、[Apply] をクリックします。（以下の画面では初期設定を表示しています。）

IGMP Configuration	
IGMP Status	<input checked="" type="checkbox"/> Enabled
Act as IGMP Querier	<input checked="" type="checkbox"/> Enabled
IGMP Query Count (2-10)	<input type="text" value="2"/>
IGMP Query Interval (60-125)	<input type="text" value="125"/> seconds
IGMP Report Delay (5-25)	<input type="text" value="10"/> seconds
IGMP Query Timeout (300-500)	<input type="text" value="300"/> seconds
IGMP Version (1,2)	<input type="text" value="2"/>

マルチキャストルータに接続されたインターフェースの表示

マルチキャストルータは、IGMP からの情報に加え、インターネットでの IP マルチキャストを行うため DVMRP、PIM 等のマルチキャスト・ルーティング・プロトコルを使用します。

ルータは、本機により動的に設定されるか、静的にインターフェースの追加を行うことができます。

Multicast Router Port Information ページでは、各 VLAN ID で隣接するマルチキャストルータ / スイッチの接続されたポートを表示します。

設定・表示項目

VLAN ID

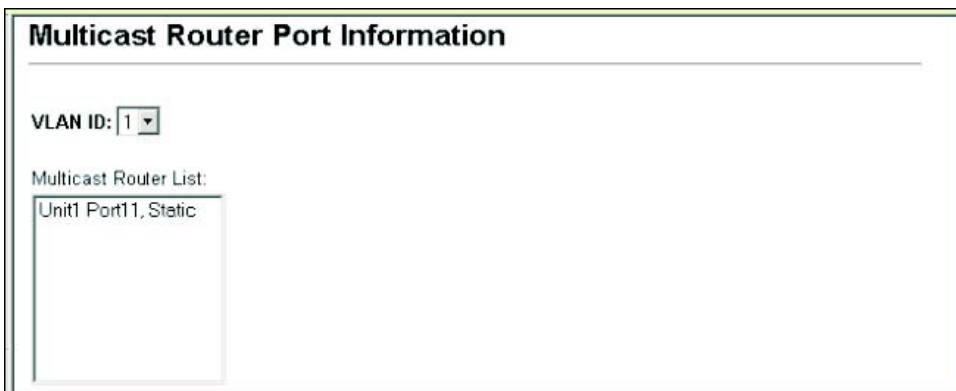
リストを表示させる VLAN ID (1-4094)

Multicast Router List

動的及び静的に設定されたマルチキャストルータの設定情報

設定方法

[IGMP Snooping] [Multicast Router Port Information] をクリックします。スクロールダウンリストから VLAN ID を選択すると、関連するマルチキャストルータの情報を表示されます。



Multicast Router Port Information

VLAN ID:

Multicast Router List:

Unit1 Port11, Static

マルチキャストルータに接続するインターフェースの設定

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

Interface

ポート (Port) 又はトランク (Trunk) をスクロールダウンリストから選択します。

VLAN ID

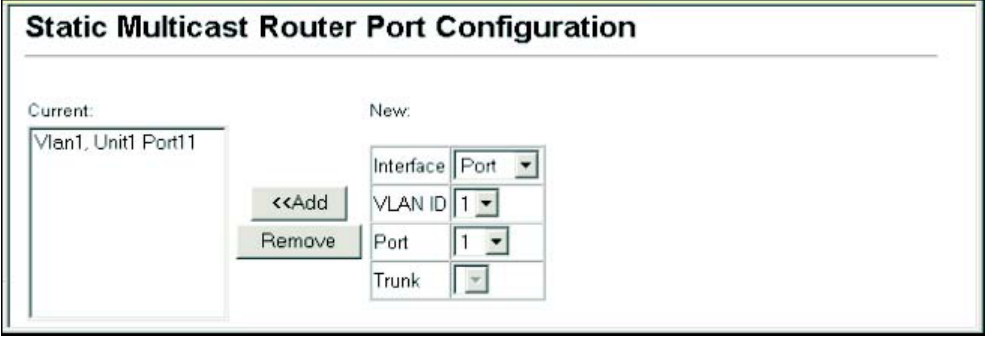
マルチキャストルータ/スイッチから送られるマルチキャストトラフィックを受信し、転送する VLAN を選択します。

Port 又は 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

[IGMP Snooping] [Static Multicast Router Port Configuration] をクリックします。マルチキャストルータに接続されたインタフェースとマルチキャストトラフィックを送受信する VLAN を指定し、[Add] をクリックします。すべての設定が完了後、[Apply] をクリックします。



The image shows a web interface window titled "Static Multicast Router Port Configuration". It contains two main sections: "Current:" and "New:". The "Current:" section has a text box containing "Vlan1, Unit1 Port11". The "New:" section contains a form with four fields: "Interface" (a dropdown menu with "Port" selected), "VLAN ID" (a dropdown menu with "1" selected), "Port" (a dropdown menu with "1" selected), and "Trunk" (a dropdown menu). Between the "Current:" and "New:" sections are two buttons: "<<Add" and "Remove".

マルチキャストサービスのポートメンバー表示

マルチキャスト IP アドレス及び VLAN を指定し、関連するポートメンバーを表示します。

設定・表示項目

VLAN ID

ポートメンバーを表示する VLAN を選択します。

Multicast IP Address

マルチキャストサービスを行う IP アドレスを選択します。

Multicast Group Port List

VLAN グループに所属し、マルチキャストサービスが送信されるポートが表示されます。

設定方法

[IGMP Snooping] [IP Multicast Registration Table] をクリックします。VLAN ID とマルチキャスト IP アドレスを選択すると、マルチキャストサービスが送信されるすべてのポートが表示されます。

IP Multicast Registration Table

VLAN ID:

1

Multicast IP Address:

224.1.1.12

Multicast Group Port List:

Unit1 Port1, User

マルチキャストサービスへのポートの指定

マルチキャストフィルタリングは、P151「IGMP Snooping Query 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

Interface

ポート (Port) 又はトランク (Trunk) をスクロールダウンリストで選択します。

VLAN ID

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。

Multicast IP Address

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。

Port 又は 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。

設定方法

[IGMP Snooping] [IGMP Member Port Table] をクリックします。マルチキャストサービスに参加させるインタフェース、マルチキャストサービスを転送する VLAN、マルチキャスト IP アドレスを指定し、[Add] をクリックします。すべての設定が終了後、[Apply] をクリックします。

The screenshot shows the 'IGMP Member Port Table' configuration window. On the left, under 'IGMP Member Port List:', there is a table with one entry: 'VLAN 1, 224.1.1.12, Unit 1, Port 1'. Below this table are two buttons: '<<Add' and 'Remove'. On the right, under 'New Static IGMP Member Port:', there is a form with the following fields: 'Interface' (a dropdown menu showing 'Port'), 'VLAN ID' (a dropdown menu showing '1'), 'Multicast IP' (a text input field), 'Port' (a dropdown menu showing '1'), and 'Trunk' (a dropdown menu showing a checked box).

4. コマンドラインインターフェース

4.1 コマンドラインインターフェースの利用

4.1.1 コマンドラインインター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。

```
User Access Verification

Username: admin
Password:
CLI session with the switch 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] 工場出荷時設定では本機には IP アドレスは設定されていません。

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 SMC8642T 1 is opened.
To end the CLI session, enter [Exit].

Vty-0#
```

[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 コマンドの補完

コマンドを入力している途中で Tab キーを押すと、CLI が自動的にコマンドの残りを補完し、キーワードが入力されます。例えば "**logging history**" コマンドを入力する際に、"**log**" と入力して Tab キーを押すと "**logging**" とキーワードがすべて入力されます。

4.2.4 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
  bridge-ext        Bridge extension information
  calendar          Date and time information
  dot1x             802.1X content
  garp              GARP properties
  gvrp              GVRP interface information
  history           History information
  interfaces        Interface information
  ip                IP information
  lacp              LACP statistic
  lec               Logical Equivalency Classes
  line              TTY line information
  log               Login records
  logging           Login setting
  mac-address-table Configuration of the address table
  management        Management IP filter
  map               Maps priority
  port              Port Characteristics
  public-key        Public Key information
  queue             Priority queue information
  radius-server     RADIUS server information
  rate-limit        Configures rate-limits
  running-config    Information on the running configuration
  snmp              Simple Network Management Protocol statistics
  sntp              Simple Network Time Protocol configuration
  spanning-tree     Spanning-tree configuration
  ssh               Secure shell server connections
  startup-config    Startup system configuration
  system            System Information
  tacacs-server     TACACS server settings
  tech-support      Technical information
  users             Information about terminal lines
  version           System hardware and software versions
  vlan              Virtual LAN settings
Console#show
```

"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 ?
  countersInterface counters information
  statusInterface status information
  switchportInterface switchport information
Console#
```

4.2.5 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  
system  
Console#show s
```

4.2.6 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。

4.2.7 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。

4.2.8 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を行います。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
		Interface
		Line
		Multiple Spanning Tree
		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。

4.2.9 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 switch is opened.
To end the CLI session, enter [Exit].

Console#
```

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

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

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

4.2.10 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。

電源を切った場合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。

コマンドラインインターフェース コマンド入力

- ◆ **Interface Configuration** "speed-duplex"や"negotiation"コマンドなどポート設定を行うためのモードです。
- ◆ **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。
- ◆ **VLAN Configuration** VLAN グループを設定するためのモードです。
- ◆ **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。

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)#	P168
Access Control List	access-list ip standard access-list ip extended	Console(config-std-acl) Console(config-ext-acl)	P262
Interface	interface {ethernet <i>port</i> port-channel <i>id</i> vlan <i>id</i> }	Console(config-if)#	P288
VLAN	vlan database	Console(config-vlan)#	P342
MSTP	spanning-tree mst-configuration	Console(config-mstp)#	P326

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)#
```

4.2.11 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
Line	ボーレートやタイムアウト時間などシリアルポート及び Telnet を使用した本機への接続に関する設定	P168
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	P180
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	P186
Flash/File	ファームウェアコードやスイッチの設定ファイルに関連したコマンド	P235
Authentication	IEEE802.1x 及びポートセキュリティのリモート認証に関連したコマンド	P241
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	P262
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	P271
Interface	Trunk、LACP や VLAN など各ポートの設定	P288
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	P301
Rate Limit	通信の最大送受信帯域のコントロール	P303
Link Aggregation	複数ポートをグループ化するポートトラunk及び Link Aggregation Control Protocol (LACP) の設定	P304
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	P315
Spanning Tree	STA 設定	P319
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	P342
GVRP and Bridge Extension	動的な VLAN の設定を行うための GVRP の設定、ブリッジ拡張 MIB の設定	P363
Priority	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	P368
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	P378
IP Interface	管理アクセス用 IP アドレスの設定	P389

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。

NE (Normal Exec)

PE (Privileged Exec)

GC (Global Configuration)

ACL (Access Control List Configuration)

IC (Interface Configuration)

LC (Line Configuration)

VC (VLAN Database Configuration)

コマンドラインインターフェース

Line (ラインコマンド)

4.4 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	P169
login	コンソール接続時のパスワードの有効化	LC	P170
password	コンソール接続時のパスワードの設定	LC	P171
timeout login response	CLI のログイン入力待ち時間の設定	LC	P172
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	P173
password-thresh	パスワード入力時のリトライ数の設定	LC	P174
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	P175
databits*	各文字あたりのデータビットの設定	LC	P175
parity*	パリティビット生成の設定	LC	P176
speed*	ボーレートの設定	LC	P177
stopbits*	1byte あたりのストップビット値の設定	LC	P177
disconnect	Line 接続を終了	PE	P178
show line	ターミナル接続の設定情報を表示	NE,PE	P178

* コンソール接続にのみ反映されます。

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 (P178)

show users (P232)

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 (P188)

password (P171)

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 (P170)

password-thresh (P174)

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 : 600 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)#
```

関連するコマンド

silent-time (P175)

exec-timeout (P173)

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

CLI : タイムアウト設定なし

Telnet : 600 秒 (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)#
```

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

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。
- ♦ 本コマンドはコンソール接続と Telnet 接続の両方に有効です。

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 (P175)

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 (P174)

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 (P176)

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** No parity
- ♦ **even** Even parity
- ♦ **odd** Odd parity

初期設定

No parity

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)#
```

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 (9600, 57600, 38400, 19200, 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

本例では 57600bps に設定しています。

```
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}

- ♦ 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)#
```

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 (P207)

show users (P232)

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
Interactive timeout: Disabled
Silent time: Disabled
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1

Vty configuration:
Password threshold: 3 times
Interactive timeout: 65535
Console#
```

4.5 General (一般コマンド)

コマンド	機能	モード	ページ
enable	Privileged モードの有効化	NE	P180
disable	Privileged モードから Normal モードへの変更	PE	P181
configure	Global Configuration モードの有効化	PE	P182
show history	コマンド履歴バッファの表示	NE,PE	P182
reload	本機の再起動	PE	P183
end	Privileged Exec モードへの変更	GC,IC,LC,VC	P184
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	P184
quit	CLI セッションを終了	NE,PE	P185

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 P162 「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、P189 「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 (P181)

enable password (P189)

disable

Privileged Exec から Normal Exec に変更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 P162 「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 (P180)

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 P162 「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 (P184)

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)#
```

reload

システムの再起動を行う際に利用します。

[注意] 再起動時には Power-On Self-test が実行されます。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

システム全体の再起動を行います。

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
```

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

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:
```

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

コマンド解説

"quit"、"exit" コマンドはどちらも Configuration モードを終了する際に利用できます。

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:
```

4.6 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	P186
User Access	管理アクセスユーザ名及びパスワード設定	P188
IP Filter	管理アクセスを許可する IP アドレスの設定	P190
Web Server	Web ブラウザ経由での管理アクセスの有効化	P192
Telnet Server	Telnet 経由での管理アクセスの有効化	P196
Secure Shell	セキュリティを確保した SSH 接続	P198
Event Logging	エラーメッセージログ設定	P209
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	P221
System Status	管理者やシステムバージョン、システム情報の表示	P227
Frame Size	ジャンボフレームサポートの有効化	P234

4.6.1 Device Designation コマンド

コマンド	機能	モード	ページ
prompt	PE/NE モードで使用するプロンプトのカスタマイズ	GC	P187
hostname	ホスト名の設定	GC	P187
snmp-server contact	システムコンタクト者の設定	GC	P274
snmp-server location	システムロケーションの設定	GC	P274

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)#
```

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" を前に置くことで初期設定に戻ります。

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)#
```

4.6.2 ユーザーアクセスコマンド

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、P171「password」や P241「認証コマンド」、P253「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
username	ログインするためのユーザ名の設定	GC	P188
enable password	各アクセスレベルのパスワードの設定	GC	P189

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 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

- ◆ 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)#
```

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 8 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。P180 「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 (P180)

authentication enabled (P242)

4.6.3 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	P190
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	P191

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

[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いません。
- ◆ 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

本例では、表示されている IP アドレス及び IP アドレスグループからの接続を許可する設定を行なっています。

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

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#
```

4.6.4 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 インターフェースに使用するポートの設定	GC	P192
ip http server	管理用 Web インターフェースの使用	GC	P193
ip http secure-server	セキュア HTTP (HTTPS) サーバの使用	GC	P194
ip http secure-port	HTTPS 接続に使用するポートの設定	GC	P195

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 (P193)

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

[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 (P192)

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

[no] ip http secure-server

初期設定

有効

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 及び Netscape Navigator 4.x のステータスバーに鍵マークが表示されます。
- ◆ 以下の Web ブラウザ、OS 環境で HTTPS をサポートしています。

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
Netscape Navigator 4.7 以上	Windows 98、Windows NT (サービスパック 6a) Windows 2000、Windows XP、Solaris 2.6

セキュアサイト証明の詳細は P64 「サイト証明書の設定変更」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 (P195)

copy tftp https-certificate (P235)

ip http secure-port

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 (P194)

copy tftp https-certificate (P235)

4.6.5 Telnet サーバーコマンド

コマンド	機能	モード	ページ
ip telnet port	Telnet インタフェースに使用するポートの設定	GC	P196
ip telnet server	管理用 Telnet インタフェースの使用	GC	P196

ip telnet port

Telnet 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 telnet port *port-number*

no ip telnet port

- ◆ *port-number* Telnet インタフェースに使用する 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)#
```

関連するコマンド

ip telnet server (P196)

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

[no] ip http server

初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#ip telnet server  
Console(config)#
```

関連するコマンド

ip telnet port (P196)

4.6.6 Secure Shell コマンド

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。

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 server	SSH サーバの使用	GC	P200
ip ssh timeout	SSH サーバの認証タイムアウト設定	GC	P201
ip ssh authentication-retries	クライアントに許可するリトライ数の設定	GC	P202
ip ssh server-key size	SSH サーバキーサイズの設定	GC	P203
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	P235
delete public-key	特定ユーザの公開キーの削除	PE	P204
ip ssh crypto host-key generate	ホストキーの生成	PE	P204
ip ssh crypto zeroize	RAM からのホストキーの削除	PE	P205
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	P206
disconnect	ライン接続の終了	PE	P178
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	P206
show ssh	SSH セッション状態の表示	PE	P207
show public-key	特定のユーザ又はホストの公開キーの表示	PE	P208
show users	SSH ユーザ、アクセスレベル、公開キータイプの表示	PE	P232

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** "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
1568499540186766925933394677505461732531367489083654725415020245593199868544358361
651999923329781766065830956
1082591321289023376546801726272571413428762941301196195566782
5956641048695742788814620651941746772984865468615717739390164779355942303577413098
02273708779454524083971752646358058176716709574804776117
```

- (3) **クライアント公開キーの本機への取り込み** P4-69"copy tftp public-key" 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
1341081685609893921040944920155425347631641921872958921143173880055536161631051775
9408386863110929123222682851925437460310093718772119969631781366277414168985132049
1172048303392543241016379975923714490119380060902539484084827178194372288402533115
952134861022902978982721353267131629432532818915045306393916643 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。

- クライアントが公開キーを本機に送ります。
- 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。
- 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。
- 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。
- 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 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

[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 (P204)

show ssh (P207)

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

120 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せん。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 (P173)

show ip ssh (P206)

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 (P206)

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)#
```

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 (P205)

ip ssh save host-key (P206)

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ください。

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 [dsa | rsa]

- ♦ **dsa** DSA キータイプ
- ♦ **rsa** RSA キータイプ

初期設定

DSA 及び RSA キーの両方を保存

コマンドモード

Privileged Exec

例

```
Console#ip ssh save host-key dsa
Console#
```

関連するコマンド

ip ssh crypto host-key generate (P204)

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 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
Encryption	暗号化方式はクライアントとサーバの間で自動的に情報交換を行ない設定します。 SSH v1.5 の選択肢 : DES, 3DES SSH v2.0 の選択肢は client-to-server (ctos) 及び server-to-client (stoc) の 2 種類の方式をサポートします : aes128-cbc-hmac-sha1 aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1 3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1 aes128-cbc-hmac-md5 aes192-cbc-hmac-md5 aes256-cbc-hmac-md5 3des-cbc-hmac-md5 blowfish-cbc-hmac-md5 用語集 : DES Data Encryption Standard (56-bit key) 3DES Triple-DES (Uses three iterations of DES, 112-bit key) aes Advanced Encryption Standard (160 or 224-bit key) blowfish Blowfish (32-448 bit key) cbc cypher-block chaining sha1 Secure Hash Algorithm 1 (160-bit hashes) md5 Message Digest algorithm number 5 (128-bit hashes)

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
156849954018676692593339467750546173253136748908365472541502024559319
986854435836165199992332978176606583095861082591321289023376546801726
272571413428762941301196195566782595664104869574278881462065194174677
298486546861571773939016477935594230357741309802273708779454524083971
752646358058176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/
Dg0h2HxcYV44sXZ2JXhamLK6P8bvuiyacWbUW/
a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XffAKxl5fwFfvJlPdOkFgzLGMinvSNYQwiQXbKT
BH0Z4mUZpE85PWxDZMacNBpjBrRAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAEAsy
5YWDC99ebYHNRj5kh47wY4i8cZvH+/
p9cnrfwFTMU01VFDly3IR2G395NLy5Qd7ZDxfA9mCofT/
yyEfbbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/
Kjw6BmiFq70+jAhf1Dg45loAc27s6TLdtnylwRq/
ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOyDbsloBfPuSAb4oAsyjKXKVYNLQkTLZ
fcFRu41bS2KV5LAWecsigF/+DjKGWtPNIQqabKgYCw2 o/
dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475
S7 w0W
Console#
```

4.6.7 Event Logging コマンド

コマンド	機能	モード	ページ
logging on	エラーメッセージログの設定	GC	P209
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	P210
logging host	syslog を送信するホストの IP アドレスの設定	GC	P211
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	P211
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	P212
clear logging	ログバッファのクリア	PE	P213
show logging	ログ関連情報の表示	PE	P214
show log	ログメッセージの表示	PE	P215

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

[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 (P210)

clear logging (P213)

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 Level 0 までのメッセージが保存されます（選択した Level は含まれます）

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

現在のファームウェアでは Level 2,5,6 のみサポートしています。

初期設定

Flash: errors (level 3 - 0)

RAM: warnings (level 6 - 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

[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 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

[no] logging facility *type*

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 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 (選択した Level は含まれます)

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

有効 (レベル : 6-0)

コマンドモード

Global Configuration

コマンド解説

- ◆ レベルを指定することによって、syslog サーバへの送信を有効に設定し、選択した Level から Level0 までのメッセージが保存されます（選択した Level は含まれます）
- ◆ 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 4
Console(config)#
```

clear logging

ログをバッファから削除するコマンドです。

文法

clear logging [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 logging
Console#
```

関連するコマンド

show logging (P214)

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 (P4-74)
- ◆ **trap** syslog サーバに送信されたメッセージ

初期設定

なし

コマンドモード

Privileged Exec

例

本例では、syslog が有効で、フラッシュメモリのメッセージレベルは "errors" (初期値 3-0)、RAM へのメッセージレベルは "debugging" (初期値 7-0) と設定しており、1 つのサンプルエラーが表示されています。

```
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
Messages	メモリに保存されているイベントメッセージ

本例では、トラップ機能の設定を表示しています。

```
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 コマンドにより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 コマンドによるリモートサーバに送信される syslog メッセージのファシリティタイプ
REMOTELOG level type	logging trap コマンドによるリモートサーバに送信される syslog メッセージのしきい値
REMOTELOG server IP address	logging host コマンドによる syslog サーバの IP アドレス

関連するコマンド

show logging sendmail (P220)

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} [login] [tail]

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

tail 最新の履歴から表示

login ログインに関する履歴のみ表示

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#
```

4.6.8 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 host	アラートメッセージを受信する SMTP サーバ	GC	P217
logging sendmail level	アラートメッセージのしきい値設定	GC	P218
logging sendmail source-email	メールの " From " 行に入力されるアドレスの設定	GC	P219
logging sendmail destination-email	メール受信者の設定	GC	P219
logging sendmail	SMTP イベントハンドリングの有効化	GC	P220
show logging sendmail	SMTP イベントハンドラ設定の表示	NE,PE	P220

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

[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

None

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 (P4-50)。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 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。

文法

logging sendmail source-email *email-address*

- ♦ *email-address* アラートメッセージの送信元アドレス（設定範囲：0-41 文字）

初期設定

None

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)#
```

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

None

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

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

[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)#
```

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: 7

SMTP destination email addresses
-----
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enable

Console#
```

4.6.9 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 client	特定のタイムサーバからの時刻の取得	GC	P221
sntp server	タイムサーバの指定	GC	P222
sntp poll	リクエスト送信間隔の設定	GC	P223
show sntp	SNTP 設定の表示	NE,PE	P224
clock timezone	本機内部時刻のタイムゾーンの設定	GC	P224
calendar set	システム日時の設定	PE	P225
show calendar	現在の時刻及び設定の表示	NE,PE	P226

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

[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ないます。

例

```
Console(config)#ntp server 10.1.0.19
Console(config)#ntp poll 60
Console(config)#ntp client
Console(config)#end
Console#show ntp
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
Current server:10.1.0.19
Console#
```

関連するコマンド

ntp server (P222)

ntp poll (P223)

show ntp (P224)

ntp 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" を引数とすることによりすべてのタイムサーバを削除します。

文法

ntp server [*ip1* [*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。"ntp 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)#ntp server 10.1.0.19
Console#
```


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 *hours*

no sntp poll

♦ *seconds* リクエスト間隔（設定範囲：1-4 時間）

初期設定

1 時間

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にのみ有効となります。

例

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

関連するコマンド

sntp client (P221)

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:137.92.140.80.0.0.0.0.0.0.0.0.0
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いません。

文法

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- ♦ *name* タイムゾーン名 (範囲: 1-29 文字)
- ♦ *hours* UTC との時間差 (時間) (範囲: 1-12 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の (UTC より早い) 場合
- ♦ *after-utc* UTC からのタイムゾーンの時差がプラスの (UTC より遅い) 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 (P224)

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 15:12:34, February 1st, 2002 に設定しています。

```
Console#calendar set 15:12:34 1 February 2002
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 set
15:12:34 February 1 2002
Console#
```

4.6.10 システム情報の表示

コマンド	機能	モード	ページ
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	P227
show running-config	実行中の設定ファイルの表示	PE	P229
show system	システム情報の表示	NE,PE	P231
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	P232
show version	システムバージョン情報の表示	NE,PE	P233

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。

初期設定

なし

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：
 - 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
 - VLAN の IP アドレス設定
 - スパニングツリー設定
 - コンソール及び Telnet に関する設定

例

```
Console#show startup-config
building startup-config, please wait.....
!
!
username admin access-level 15
username admin password 0 admin
!
username guest access-level 0
username guest password 0 guest
!
enable password level 15 0 super
!
snmp-server community public ro
snmp-server community private rw
!
logging history ram 6
logging history flash 3
!
vlan database
  vlan 1 name DefaultVlan media ethernet state active
!
interface ethernet 1/1
switchport allowed vlan add 1 untagged
switchport native vlan 1
.
.
.
interface vlan 1
  ip address dhcp
!
line console
!
line vty
!
end

Console#
```

関連するコマンド

show running-config (P229)

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
 - SNTP サーバの設定
 - タイムゾーンの設定
 - SNMP コミュニティ名
 - ユーザ (ユーザ名及びアクセスレベル)
 - イベントログの設定
 - 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
 - 本機の IP アドレス設定
 - IP DSCP の設定
 - コンソール及び Telnet に関する設定

例

```
Console#show running-config
building startup-config, please wait.....
!
phyomap 00-12-cf-ce-2a-20 00-00-00-00-00-00 00-00-00-00-00-00
00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-
00-00 00-00-00-00-00-00
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
clock timezone hours 0 minute 0 after-UTC
!
!
SNMP-server community private rw
SNMP-server community public ro
!
!
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
!
!
logging history ram 6
logging history flash 3
!
!
vlan database
  vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
  switchport allowed vlan add 1 untagged
  switchport native vlan 1 .
.
.
interface VLAN 1
  IP address DHCP
!
no map IP DSCP
!
!
line console
!
line vty
!
end

Console#
```

関連するコマンド

show startup-config (P227)

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詳細は P3-10「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、又はサポートまで連絡して下さい。

例

```
Console#show system
System description: FXC5148XG L2 GE Switch
System OID string: 1.3.6.1.4.1.259.6.10.72
System information
  System Up time: 0 days, 0 hours, 2 minutes, and 34.45 seconds
  System Name: [NONE]
  System Location: [NONE]
  System Contact: [NONE]
  MAC address: 00-12-CF-0B-0D-00
  Web server: enabled
  Web server port: 80
  Web secure server: enabled
  Web secure server port: 443
  Telnet server : enable
  Telnet port : 23
  Jumbo Frame : Disabled
  POST result
  UART Loopback Test ..... PASS
  DRAM Test ..... PASS
  Timer Test ..... PASS
  PCI Device 1 Test ..... PASS
  I2C Bus Initialization ..... PASS
  Switch Int Loopback Test ..... PASS
  Fan Speed Test ..... PASS

Done All Pass.
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
Username accounts:
Username Privilege Public-Key
-----
admin      15      None
guest      0      None
steve      15      RSA

Online users:
Line      Username  Idle time (h:m:s)  Remote IP addr.
-----
0 console admin      0:14:14
* 1 VTY 0   admin      0:00:00      192.168.1.19
2 SSH 1    steve      0:00:06      192.168.1.19

Web online users:
Line      Remote IP addr  Username  Idle time (h:m:s).
-----
1 HTTP    192.168.1.19   admin      0:00:00

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 「システム情報の表示」を参照して下さい。

例

```
Console#show version
Serial number:          S416000937
Service tag:
Hardware version:       R01
Module A type:          1000BaseT
Module B type:          1000BaseT
Number of ports:        50
Main power status:      up
Redundant power status :not present
Loader version:         1.0.0.7
Boot ROM version:       1.0.0.8
Operation code version: 2.3.4.4
Console#
```

4.6.11 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	P234

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

[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 9216byte 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 1500byte 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。
- ◆ ジャンボフレームを使用すると、ブロードキャスト制御の最大しきい値が毎秒 64 パケットに制限されます。（詳細は、P294 「switchport broadcast packet-rate」コマンドを参照して下さい）
- ◆ ジャンボフレームの現在の設定内容は "show system" コマンドで確認ができます。

[注意] ジャンボフレームは CLI でのみ設定が可能です。

例

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

4.7 ファイル管理 (Flash/File)

ここで解説するコマンドはシステムコードや設定ファイルの管理を行うためのコマンドです。

コマンド	機能	モード	ページ
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	P235
delete	ファイルやコードイメージの削除	PE	P238
dir	フラッシュメモリ内のファイルの一覧の表示	PE	P239
boot system	システム起動ファイル、イメージの設定	GC	P240

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、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 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 | running-config | startup-config | tftp | unit}

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

copy startup-config {file | 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
- ◆ **running-config** 実行中の設定をコピーするキーワード
- ◆ **startup-config** システムの初期化に使用する設定
- ◆ **tftp** TFTP サーバから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、P4-38 の "Secure Shell" コマンドを参照)
- ◆ **unit** ユニットの指定 "1"

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TFTPサーバ上では137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イメージはTFTPサーバからのアップロード及びダウンロードはできません。ブートROMまたは診断用イメージのダウンロードを行うためには新規のファームウェアに関するリリースノートの解説か、又は代理店の指示に従う必要があります。
- ◆ "http-certificate"の設定については、P3-37の「サイト証明書の設定変更」を参照して下さい。HTTPSを用い、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、P4-35の"ip http secure-server"コマンドの解説を参照して下さい。

例

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#
```

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 [*unit*:]*filename*

- ◆ *filename* 設定ファイル又はイメージファイル名
- ◆ *unit* ユニットの指定 "1"

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- ◆ スタートアップ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。
- ◆ ユニットの指定の後にはコロン (:) が必要です。

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 (P239)

delete public-key (P204)

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[*unit*:] [**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。
- ◆ *unit* ユニットの指定 "1"

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	内容
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
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 1:
  file name                file type        startup  size (byte)
-----
Unit1:
FXC5148XG-DIAG-V1.0.0.8.bix Boot-Rom image      Y         214124
FXC5148XG-OP-V2.3.4.4.bix  Operation Code      Y        1761944
Factory_Default_Config.cfg  Config File         Y          5197
-----
Total free space: 5242880
Console#
```

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 [*unit*:]{**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** Run-time operation code
- ♦ *filename* ファイル又はイメージ名
- ♦ *unit* ユニットの指定 "1"

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- ♦ ファイルタイプの後にはコロンの (:) が必ず必要です。
- ♦ 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 (P239)

4.8 ユーザ認証

システム管理のためのユーザログインはローカル及び認証サーバを用いたユーザ認証が利用可能です。

また、IEEE802.1X を利用したポートベース認証によるユーザのネットワークへのアクセス管理も可能です。

コマンドグループ	機能	ページ
Authentication Sequence	ログイン認証方式と優先順位の設定	P241
RADIUS Client	RADIUS サーバ認証の設定	P243
TACACS+ Client	TACACS+ サーバ認証の設定	P248
Port Security	ポートへのセキュアアドレスの設定	P251
Port Authentication	IEEE802.1X によるポート認証の設定	P253

4.8.1 認証コマンド

コマンド	機能	モード	ページ
Authentication login	認証方法と優先順位の設定	GC	P241
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	P241

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 (P188) ローカルのユーザ名及びパスワードの設定

4.8.2 authentication enable コマンド

"enable" コマンド (P180) 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 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 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 (P180) コマンドモード変更のためのパスワードの設定

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 host	RADIUS サーバの設定	GC	P244
radius-server port	RADIUS サーバのポートの設定	GC	P245
radius-server key	RADIUS 暗号キーの設定	GC	P245
radius-server retransmit	リトライ回数の設定	GC	P246
radius-server timeout	認証リクエストの間隔の設定	GC	P246
show radius-server	RADIUS 関連設定情報の表示	PE	P247

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

[no] radius-server index host {host_ip_address | host_alias}

[auth-port auth_port] [timeout timeout] [retransmit retransmit][key key]

- ♦ *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
- ♦ *host_alias* RADIUS サーバの名前（最大 20 文字）
- ♦ *port_number* RADIUS サーバの認証用 UDP ポート番号（範囲：1-65535）
- ♦ *timeout* 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 秒）
- ♦ *retransmit* RADIUS サーバに対するログインアクセスをリトライできる回数（範囲：1-30）
- ♦ *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。間にスペースは入れられません（最大 20 文字）

初期設定

- ♦ auth-port : 1812
- ♦ timeout : 5
- ♦ 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 port

RADIUS 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

radius-server port *port_number*

no radius-server port

- ◆ *port_number* RADIUS サーバの認証用 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 port 181
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 20 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* RADIUS サーバに対するログインアクセスをリトライできる回数 (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

```
Remote RADIUS server configuration:

Global settings
  Communication key with RADIUS server:
  Server port number: 1812
  Retransmit times: 2
  Request timeout: 5

Sever 1:
  Server IP address: 192.168.1.1
  Communication key with RADIUS server: *****
  Server port number: 181
  Retransmit times: 2
  Request timeout: 5

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 host	TACACS+ サーバの設定	GC	P248
tacacs-server port	TACACS+ サーバのポートの設定	GC	P249
tacacs-server key	TACACS+ 暗号キーの設定	GC	P249
show tacacs-server	TACACS+ 関連設定情報の表示	GC	P250

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 host *host_ip_address*

no tacacs-server host

♦ *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 host 192.168.1.25
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)#
```

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 20 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)#
```

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:
  Server IP address: 10.11.12.13
  Communication key with TACACS server: *****
  Server port number: 49
Console#
```

4.8.5 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
port security	ポートセキュリティの設定	IC	P251
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	P315
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	P317

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)

初期設定

- ◆ Status : 無効 (Disabled)
- ◆ 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。
- ♦ ポートセキュリティを無効に設定し、最大アドレス学習数を初期設定値に戻すには、"no port security max-mac-count" コマンドを使用します。
- ♦ 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：
 - ポートミラーリングは使用できません。
 - 複数の VLAN に所属できません。
 - 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
```

関連するコマンド

shutdown (P294)

mac-address-table static (P315)

show mac-address-table (P317)

4.8.6 802.1x 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
dot1x system-auth-control	dot1x をスイッチ全体に有効に設定	GC	P253
dot1x default	dot1x の設定値をすべて初期設定に戻します。	GC	P254
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	P254
dot1x port-control	ポートへの dot1x モードの設定	IC	P255
dot1x operation-mode	dot1x ポートへの接続可能ホスト数の設定	IC	P255
dot1x re-authenticate	特定ポートへの再認証の強制	PE	P256
dot1x re-authentication	全ポートへの再認証の強制	GC	P257
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	P257
dot1x timeout re-authperiod	接続済みクライアントの再認証間隔の設定	GC	P258
dot1x timeout tx-period	認証中の EAP パケットの再送信間隔の設定	GC	P258
show dot1x	dot1x 関連情報の表示	PE	P259

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

[no] dot1x system-auth-control

初期設定

無効 (Disabled)

コマンドモード

Global Configuration

例

```
Console(config)#dot1x system-auth-control
Console(config)#
```

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 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 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 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*]}

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）

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 "dot1x port-control" コマンド (P4-89) 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。

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
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 : 1-50)

コマンドモード

Privileged Exec

例

```
Console#dot1x re-authenticate
Console#
```

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

[no] dot1x re-authentication

コマンドモード

Interface Configuration

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 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)#
```

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*
 - $\text{\AA}/\text{unit}$ ユニット番号 “1”
 - $\text{\AA}/\text{port}$ ポート番号 (範囲 : 50)

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。

- ♦ *Global 802.1X Parameters* 本機全体に対する、802.1X ポート認証の有効 / 無効
- ♦ *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
 - Status ポートアクセスコントロールの管理状態
 - Operation Mode dot1x operation-mode (P4-90) の設定値
 - Mode dot1x port-control で設定する dot1x モード (P4-89)
 - 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。
 - reauth-enabled - 周期的な再認証 (P4-91)
 - reauth-period - 接続されたクライアントに再認証を要求する間隔 (P4-92)
 - 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 (P4-92)
 - tx-period - 認証時に EAP パケットの再送信を行う間隔 (P4-93)
 - 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 - 再認証の最大回数
 - max-req - 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 (P4-89)
 - Status - 認証ステータス (許可又は禁止)
 - 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
 - Max Count - ポートに接続可能な最大ホスト数 (P4-90)

- 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 (P4-89)
 - Supplicant - 認証されたクライアントの MAC アドレス
 - 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た整数値 (0-255)
- ♦ *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
 - ♦ *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
.
.
.
1/52           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

Authenticator State Machine
State                Authenticated
Reauth Count         0

Backend State Machine
State                Idle
Request Count        0
Identifier(Server) 2

Reauthentication State Machine
State                Initialize
.
.
.
802.1X is disabled on port 1/52
Console#

```

4.9 ACL (Access Control Lists)

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 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。

Access Control Lists

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て許可 (Permit) 又は拒否 (Deny) するためのリストです。

本機では入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落とします。リスト上の許可ルールに一致しない場合、パケットは落とされ、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。

本機には 2 つのフィルタリングモードがあります。

- ◆ Standard IP ACL mode (STD-ACL) ソース IP アドレスに基づくフィルタリングを行う IP ACL モード
- ◆ Extended IP ACL mode (EXT-ACL) 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 ポート番号に基づくフィルタリングを行う IP ACL モード

ACL は以下の制限があります。

- ◆ 各 ACL は最大 32 ルールまで設定可能です。
- ◆ 最大 ACL 設定数は 88 個です。
- ◆ 但し、リソースの制限により、ポートに結び付けられた規則の数の平均は 20 を超えないようにして下さい。
- ◆ 本機は ingress (入力) ACL のみをサポートしています。1 個の IP ACL を任意の ingress (入力) ポートにバインドできます。

有効な ACL は以下の順番で実行されます。

- (1) 入力ポートの入力 IP ACL のユーザに定義されたルール
- (2) 入力ポートの入力 IP ACL のデフォルトルール (permit any any)
- (3) 明確なルールに一致しない場合、暗黙のデフォルトルール (permit all)

コマンドグループ	機能	ページ
IP 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	P263
ACL Information	ACL 及び関連するルールの表示。各ポートの ACL の表示	P270

4.9.1 IP ACL コマンド

コマンド	機能	モード	ページ
access-list IP	IP ACL の作成と configuration mode への移行	GC	P263
permit,deny	ソース IP アドレスが一致するパケットのフィルタリング	STD-ACL	P264
permit,deny	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 ポート番号に基づくフィルタリング	EXT-ACL	P265
show ip access-list	設定済み IP ACL のルールの表示	PE	P266
ip access-group	IP ACL へのポートの追加	IC	P267
show ip access-group	IP ACL に指定したポートの表示	PE	P268
map access-list ip	ACL ルールと一致するパケットへの出力キューの CoS 値の設定	IC	P268
show map access-list ip	インタフェースのアクセスリストにマッピングされた CoS 値の表示	PE	P269

access-list ip

IP ACL を追加し、スタンダード又は拡張 IP 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

[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 ポート番号に基づくフィルタリングを行う ACL
- ◆ *acl_name* ACL 名 (4 文字以上 15 文字以内)

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。

コマンドラインインターフェース

ACL (Access Control Lists)

- ◆ 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 32 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 (P264)

ip access-group (P267)

show ip access-list (P266)

permit,deny (Standard ACL)

スタンダード IP 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

[no] {permit | deny} {any | source bitmask | host source}

- ◆ **any** 全ての 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

初期設定

なし

コマンドモード

Standard 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 (P263)

permit,deny (Extended ACL)

拡張 IP 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}
      [source-port sport [end]] [destination-port dport [end]]
```

```
[no] {permit | deny} tcp
      {any | source address-bitmask | host source}
      {any | destination address-bitmask | host destination}
      [source-port sport [end]] [destination-port dport [end]]
```

- ◆ *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
- ◆ *sport* プロトコル * ソースポート番号 (範囲 : 0-65535)
- ◆ *dscp* DSCP プライオリティレベル (範囲 : 0-63)
- ◆ *end* プロトコルポート範囲の上限 (範囲 : 0-65535)

初期設定

なし

コマンドモード

Extended 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、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 (P263)

show ip access-list

設定済みの IP 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 (4 文字以上 15 文字以内)

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#
```

ip access-group

IP 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

[no] ip access-group *acl_name* in

◆ *acl_name* [ACL名] (4 文字以上 15 文字以内)

◆ **in** 入力パケットへのリスト

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- ◆ 1 つのポートは 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)#int eth 1/25
Console(config-if)#ip access-group david in
Console(config-if)#
```

関連するコマンド

show ip access-list (P266)

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 1/25
  IP access-list david in
Console#
```

関連するコマンド

ip access-group (P267)

map access-list ip

ACL ルールに一致するパケットの出力キューを設定します。指定された CoS 値は一致したパケットの出力キューにのみ使用され、パケットには変更が加えられません。"no" を前に置くことで CoS マッピングを削除します。

文法

[no] map access-list ip *acl_name* **cos** *cos-value*

- ◆ *acl_name* ACL 名 (4 文字以上 15 文字以内)
- ◆ *cos-value* CoS 値 (範囲 : 0-7)

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

指定された ACL のルールと一致するパケットは、下の表に基づき出力キューがマッピングされます。CoS 値の詳細は P372 「queue cos-map」を参照して下さい。

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

例

```
Console(config)#interface ethernet 1/25
Console(config-if)#map access-list ip david cos 0
Console(config-if)#
```

関連するコマンド

queue cos-map (P372)

show map access-list ip (P269)

show map access-list ip

インタフェースの IP ACL にマッピングされた CoS 値を表示します。CoS 値は ACL ルールに一致するパケットの出力キューを決定します。

文法

show map access-list ip [*interface*]

- ◆ *interface*
 - **ethernet** *unit/port*
 - *unit* ユニット番号 "1"
 - *port* ポート番号

コマンドモード

Privileged Exec

例

```
Console#show map access-list ip
Eth 1/25
  access-list ip david cos 0
Console#
```

関連するコマンド

map access-list ip (P268)

コマンドラインインターフェース

ACL (Access Control Lists)

4.9.2 ACL 情報の表示

コマンド	機能	モード	ページ
show access-list	全ての ACL と関連するルールの表示	PE	P270
show access-group	ソース IP アドレスが一致するパケットのフィルタリング	PE	P270

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#
```

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 1/1
IP access-list jerry in
.
.
.
Interface ethernet 1/52
IP access-list jerry in
Console#
```


4.10 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
snmp-server	SNMP サーバーを有効化	GC	P271
show snmp	SNMP の設定情報を表示	NE,PE	P272
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	P273
snmp-server contact	システムコンタクト情報の設定	GC	P274
snmp-server location	システム設置情報の設定	GC	P274
snmp-server host	SNMP メッセージを受信するホストの設定	GC	P275
snmp-server enable traps	SNMP メッセージを受信するホストの有効化	GC	P277
snmp-server engine-id	エンジン ID の設定	GC	P278
show snmp engine-id	エンジン ID の表示	PE	P279
snmp-server view	ビューの設定	GC	P280
show snmp view	ビューの表示	PE	P281
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	P282
show snmp group	グループの表示	PE	P283
snmp-server user	SNMP v3 グループへユーザーの追加	GC	P285
show snmp user	SNMP v3 ユーザーの表示	PE	P286

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

[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) #
```

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 traps:
Authentication: enabled
Link-up-down: enabled

SNMP communities:
1. private, and the privilege is read-write
2. public, and the privilege is read-only

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 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

コマンド解説

"snmp-server community" コマンドは SNMP を有効にします。"no snmp-server community" コマンドは SNMP を無効にします。

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)#
```

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)#
```

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 [**1** | **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 P43 「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

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。

[注意] 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、トラップまたはトラップ通知の使用を決定してください。

- ◆ 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 P285 「snmp-server 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 (P277)

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 (P275)

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

[no] snmp-server engine-id { local | remote *IP Address* } engine-id

- ◆ **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 エンジンとはメッセージ再送、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 P275 「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 engineID local 12345
Console(config)#snmp-server engineID remote 54321 192.168.1.19
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

Field	Description
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#

```

関連するコマンド

snmp-server engine-ID (P278)

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

[no] snmp-server view *view-name oid-tree {included | excluded}*

- ◆ *view-name* ビューの名前（1-64 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
- ◆ **included** *oid-tree* で指定した OID を参照可能な範囲に含む
- ◆ **excluded** *oid-tree* で指定した OID を参照可能な範囲に含まない

初期設定

デフォルトビュー

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 インターフェーステーブル、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 インター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트리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 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

Field	Description
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#
```

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
- ◆ **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 P43 「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: public5 (read only), private6 (read/write)

readview - 全てのオブジェクトは Internet OID space (1.3.6.1) 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、「snmp-server 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しい情報については P54 「SNMPv3 グループの設定」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 P277 「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)#
```

show snmp group

本機は 4 つのデフォルトグループを提供します。

- ◆ SNMPv1 read-only access
- ◆ read/write access
- ◆ SNMPv2c read-only access
- ◆ read/write access

文法

show snmp group

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
groupname	グループ名
security model	セキュリティモデル
readview	read ビュー
writeview	write ビュー
notifyview	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: 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#
```

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 }
```

- ◆ *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** 暗号化されたパスワードの入力を受け入れます
- ◆ **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* 認証用パスワード
- ◆ **priv des56** DES56bit データ暗号化方式を使用します
- ◆ *priv-password* 暗号化用パスワード。暗号化オプションが使用されていない場合はプレーンテキストを入力してください。暗号化オプションが使用されている場合は暗号化パスワードを入力してください。

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。その後に「snmp-server 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 P46 「トラップマネージャ・トラップタイプの指定」および P53 「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 group r&d v3 auth md5
greenpeace priv des56 einstien
Console(config)#snmp-server user mark group r&d remote
192.168.1.19 v3 auth md5 greenpeace priv des56 einstien
Console(config)#
```

show snmp user

SNMP ユーザー情報を表示します。

文法

show snmp user

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
Engineld	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#
```

4.11 インターフェース

コマンド	機能	モード	ページ
interface	本機の DHCP クライアント ID の指定	GC	P288
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	P289
speed-duplex	インタフェースの解説	IC	P290
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	P291
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	P292
flowcontrol	インタフェースへのフローコントロール設定	IC	P293
shutdown	インタフェースの無効	IC	P294
switchport broadcast packet-rate	ロードキャストストームコントロールの設定	IC	P294
clear counters	インタフェースの統計情報のクリア	PE	P295
show interfaces status	インタフェースの設定状況を表示	NE,PE	P296
show interfaces counters	インタフェースの統計情報の表示	NE,PE	P297
show interfaces switchport	インタフェースの管理、運用状況の表示	NE,PE	P299

interface

インタフェースの設定及び interface configuration モードへの変更が行えます。"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 port-channel *channel-id*

- ♦ *interface*
 - **ethernet** *unit/port*
 - *unit* ユニット番号 "1"
 - *port* ポート番号 (範囲: 1-50)
 - **port-channel** *channel-id* Channel ID (1-25)
 - **vlan** *vlan-id* VLAN ID (1-4094)

初期設定

なし

コマンドモード

Global Configuration

例

本例では 24 番ポートの指定を行っています。

```
Console(config)#interface ethernet 1/24
Console(config-if)#
```

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、24 番ポートに解説を加えている設定です。

```
Console(config)#interface ethernet 1/24
Console(config-if)#description RD-SW#3
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 {1000full | 100full | 100half | 10full 10half}

no speed-duplex

- ◆ **1000full** 1000 Mbps full-duplex 固定
- ◆ **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の際、各ポートの初期設定は 100BASE-TX の場合は "100half"、ギガビットイーサネットの場合は "1000full" となります。

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 (P291)

capabilities (P292)

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

[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 11 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 1/11
Console(config-if)#negotiation
Console(config-if)#
```

関連するコマンド

capabilities (P292)

speed-duplex (P290)

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 port-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)#
```

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

[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 (P291)

capabilities (flowcontrol, symmetric) (P292)

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

[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)#
```

switchport broadcast packet-rate

ブロードキャストストームコントロールの設定を行います。"no" を前に置くことで本機能を無効にします。

文法

switchport broadcast octet-rate *rate*

no switchport broadcast

♦ *rate* ブロードキャストパケットのしきい値 (オクテット / 秒) (範囲 : 240-1488100)

初期設定

有効 (全ポート)

パケットレートの上限 : 32000 パケット / 秒

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- ◆ ブロードキャストトラフィックが指定したしきい値を超えた場合、超えたパケットに関しては破棄されます。
- ◆ 本機能の有効 / 無効の切り替えはポート毎に行えます。但し、しきい値に関してはすべてのポートで同じ設定となります。

例

本例では 5 番ポートに 600pps のしきい値を設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast octet-rate 600
Console(config-if)#
```

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: 1-50)
 - **port-channel** *channel-id* (範囲: 1-25)

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 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: 1-50)
 - **port-channel** *channel-id* (範囲: 1-25)

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 P3-58「接続状況の表示」を参照して下さい。

例

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
Basic information:
  Port type:          100TX
  Mac address:        00-30-F1-D3-26-05
Configuration:
  Name:
  Port admin:         Up
  Speed-duplex:        Auto
  Capabilities:        10half, 10full, 100half, 100full,
  Broadcast storm:     Enabled
  Broadcast storm limit: 500packets/second
  Flow control:        Disabled
  LACP:               Disabled
  Port security:       Disabled
  Max MAC count:       0
  Port security action: None
Current status:
  Link status:         Up
  Operation speed-duplex: 100full
  Flow control type:   None
Console#show interfaces status vlan 1
Information of VLAN 1
MAC address:          00-00-AB-CD-00-00
Console#
```

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 "1"
 - **port-channel** *channel-id* (範囲 : 1-25)

初期設定

すべてのポートのカウンを表示します。

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 P2-75「ポート統計情報の表示」を参照して下さい。

例

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
Iftable stats:
  Octets input: 30658, Octets output: 196550
  Unicast input: 6, Unicast output: 5
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
Ether-like stats:
  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
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
RMON stats:
  Drop events: 0, Octets: 227208, Packets: 3338
  Broadcast pkts: 263, Multi-cast pkts: 3064
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
  Packet size 128 to 255 octets: 4, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
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: 1-50)
 - **port-channel** *channel-id* (範囲: 1-25)

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 24 番ポートの情報を表示しています。

```
Console#show interfaces switchport ethernet 1/2
Broadcast threshold: Enabled, 600 octets/second
LACP status: Enabled
Ingress rate limit: disable, 100percent
VLAN membership mode: Hybrid
Ingress rule: Enabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 0
GVRP status: Disabled
Allowed Vlan: 1(u),
Forbidden Vlan:
Private-VLAN mode: NONE
Private-VLAN host-association: NONE
Private-VLAN mapping: NONE
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 (P294 参照)
Lacp status	LACP の有効 / 無効 (P306 参照)
Ingress rate limit	帯域制御の有効 / 無効。現在の設定 (P303 参照)
VLAN membership mode	トランク又は Hybrid のメンバーモードを表示 (P345 参照)
Ingress rule	イングレスフィルタの有効 / 無効の表示 (P347 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 (P346 参照)
Native VLAN	デフォルトポート VLAN ID の表示 (P348 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 (P368 参照)
Gvrp status	GVRP の有効 / 無効 (P364 参照)
Allowed Vlan	参加している VLAN の表示。"(u)" はタグなし、"(t)" はタグ (P349 参照)
Forbidden Vlan	GVRP によって動的に参加できない VLAN の表示 (P350 参照)
Private VLAN mode	プライベート VLAN モードがホスト、無差別、なしのいずれなのか (P355 参照)
Private VLAN host-association	ポートが関連付けられているセカンダリ (コミュニティ) VLAN (P358 参照)
Private VLAN mapping	Private VLAN mapping 無差別ポートにマッピングされているプライマリ VLAN (P359 参照)

4.12 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	P301
show port monitor	ミラーポートの設定の表示	PE	P302

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*]

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: 1-50)
- ◆ *rx* 受信パケットのミラー
- ◆ *tx* 送信パケットのミラー

初期設定

なし

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います。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。
- ◆ 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。
- ◆ 単一のミラーセッションのみを作成することができます。
- ◆ ディスティネーションポートとソースポートは同一の VLAN に所属している必要があります。

例

本例では 6 番から 11 番ポートへのミラーを行います。

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 rx
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*]

- ◆ *interface*
 - **ethernet** *unit/port*
 - *unit* ユニット番号 "1"
 - *port* ポート番号 (範囲: 1-50)

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

本コマンドを使用することで現在設定されているソースポート、ディスティネーションポート、ミラーモード (RX, TX) の表示を行います。

例

本例では 6 番から 11 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 1/11
Console(config-if)#port monitor ethernet 1/6 rx
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination port(listen port) :Eth1/11
Source port(monitored port)   :Eth1/6
Mode                           :RX
Console#
```


4.13 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	P303

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} [rate]

no rate-limit {input }

- ◆ **input** 入力帯域 (レート)
- ◆ **rate** パーセンテージ (1-100)

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 50
Console(config-if)#
```

4.14 リンクアグリゲーション

バンド幅拡張のため、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。又、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。

本機では最大 25 トランクグループをサポートします。

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
<i>Manual Configuration Commands</i>			
interface port-channel	interface configuration モードへの移動とトランク設定	GC	P288
channel-group	トランクへのポートの追加	IC	P305
<i>Dynamic Configuration Command</i>			
lacp	現在のインタフェースでの LACP の設定	IC	P306
lacp system-priority	ポート LACP システムプライオリティの設定	IC (Ethernet)	P307
lacp admin-key	ポートアドミンキーの設定	IC (Ethernet)	P308
lacp admin-key	ポートチャンネルアドミンキーの設定	IC(Port Channel)	P309
lacp port-priority	LACP ポートプライオリティの設定	IC (Ethernet)	P310
<i>Trunk Status Display Command</i>			
show interfaces status port-channel	トランク情報の表示	NE,PE	P296
show lacp	LACP 関連情報の表示	PE	P311

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、グループのインター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: 1-25)

初期設定

現在のポートがその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 を現在のインター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

[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、11 から 13 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 1/11
Console(config-if)#lACP
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lACP
Console(config-if)#exit
Console(config)#interface ethernet 1/13
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 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)#
```

larp 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)#
```

ladp admin-key (Port Channel)

ポートチャンネル 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 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 admin-key 3
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
```


show lacp

LACP 情報の表示を行います。

文法

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sysid**}

- ◆ *port-channel* リンクアグリゲーショングループ ID (範囲 : 1-4)
- ◆ **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
- ◆ **sysid** 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/ 1
-----
LACPDU's Sent : 21
LACPDU's Received : 21
Marker Sent : 0
Marker Received : 0
LACPDU's Unknown Pkts : 0
LACPDU's Illegal Pkts : 0
```

コマンドラインインターフェース リンクアグリゲーション

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

例

```

Console#show lacp 1 internal
Port channel : 1
-----
Oper Key : 4
Admin Key : 0
Eth 1/1
-----
LACPDUs 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
LACPDUs 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	<p>Actor の管理値又は運用値の状態のパラメータ。</p> <ul style="list-style-type: none"> ♦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

```

コマンドラインインターフェース リンクアグリゲーション

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
	4	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 形成します。

4.15 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 static	VLAN ポートへの MAC アドレスの静的なマッピング	GC	P315
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	P316
show mac-address-table	転送データベースに登録された情報の表示	PE	P317
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	P318
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	P318

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 : 1-50)
- ◆ **port-channel** *channel-id* (範囲 : 1-25)
- ◆ **vlan** *vlan-id* VLAN ID (1-4094)
- ◆ *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

コマンドラインインターフェース アドレステーブル

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)#
```

clear mac-address-table dynamic

転送データベース上に登録してあるすべての MAC アドレスを削除します。また、すべての送受信情報を削除します。

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* アドレス内のビット数
- ♦ *interface*
 - **ethernet** *unit/port*
 - *unit* ユニット番号 "1"
 - *port* ポート番号 (範囲 : 1-50)
- ♦ **port-channel** *channel-id* (範囲 : 1-25)
- ♦ *vlan-id* VLAN ID (1-4094)
- ♦ **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

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#
```

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 (10-30000 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 sec
Console(config)#
```

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 time: 100 sec.
Console#
```


4.16 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	P320
spanning-tree mode	STP/RSTP/MSTP モードの選択	GC	P320
spanning-tree forward-time	スパニングツリーブリッジ転送時間の設定	GC	P322
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	P322
spanning-tree max-age	スパニングツリーブリッジ最長時間の設定	GC	P323
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	P324
spanning-tree path-cost method	RSTP/MSTP のパスコスト方法の設定	GC	P324
spanning-tree transmission-limit	RSTP/MSTP の送信リミットの設定	GC	P325
spanning-tree-mst-configuration	MSTP 設定モードの変更	GC	P326
mst vlan	スパニングツリーインスタンスへの VLAN の追加	MST	P326
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	P327
name	MST 名の設定	MST	P328
revision	MST リビジョンナンバーの設定	MST	P329
max-hops	BPDU が破棄される前最大ホップ数の設定	MST	P330
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	P330
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	P331
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	P332
spanning-tree edge-port	エッジポートへのポートファストの有効化	IC	P333
spanning-tree portfast	インタフェースのポートファストの設定	IC	P334
spanning-tree link-type	RSTP/MSTP のリンクタイプを設定	IC	P335
spanning-tree mst cost	MST インスタンスのパスコストの設定	IC	P336
spanning-tree mst port-priority	MST インスタンスプライオリティの設定	IC	P337
spanning-tree protocol-migration	適切な BPDU フォーマットの再確認	PE	P338
show spanning-tree	スパニングツリーの設定を表示	PE	P338
show spanning-treemst configuration	MST 設定の表示	PE	P341

spanning-tree

本機に対して 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

[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 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}

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 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：1-10 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)#
```

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)#
```

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 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。pathcost は port priority よりも優先されます。

例

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

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)#
```

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)#
```

関連するコマンド

mst vlan (P326)

mst priority (P327)

name (P328)

revision (P329)

max-hops (P330)

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。

[注意] MST の設定を行う際には、事前に **spanning-tree mode** を **mstp** に選択してください。(P320 「spanning-tree mode」を参照)

例

```
Console(config-mstp)#mst 1 vlan 2-5
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)#
```

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 (32 文字以内)

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 (P329)

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）

初期設定

0

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 (P328)

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)#
```

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

[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 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)

推奨する値は以下の通りです。

- Ethernet (10Mbps): 200,000-20,000,000
- Fast Ethernet (100Mbps): 20,000-2,000,000
- Gigabit Ethernet (1Gbps): 2,000-200,000

初期設定

- ♦ Ethernet half duplex: 2,000,000、full duplex: 1,000,000、トランク : 500,000
- ♦ Fast Ethernet half duplex: 200,000、full duplex: 100,000、トランク : 50,000
- ♦ Gigabit Ethernet full duplex: 10,000、トランク : 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 5000
Console(config-if)#
```

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（範囲：16 間隔で 0-240 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 128
Console(config-if)#
```

関連するコマンド

spanning-tree cost (P331)

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

[no] spanning-tree edge-port

初期設定

無効 (Disabled)

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。)
- ◆ 本コマンドは "spanning-tree portfast" コマンドと同一の機能です。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

関連するコマンド

spanning-tree portfast (P334)

spanning-tree portfast

ポートをポートファストに指定します。"no" を前に置くことで本機能を無効にします。

文法

[no] spanning-tree portfast

初期設定

無効 (Disabled)

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）
- ◆ 本コマンドは "spanning-tree edge-port" コマンドと同じ機能を有します。本コマンドは旧製品との互換性を保つために用意されており、将来のファームウェアでは使用できなくなる可能性があります。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree portfast
Console(config-if)#
```

関連するコマンド

spanning-tree edge-port (P333)

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** シェアードミディアム

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 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)
推奨する値は以下の通りです。
 - Ethernet (10Mbps): 200,000-20,000,000
 - Fast Ethernet (100Mbps): 20,000-2,000,000
 - Gigabit Ethernet (1Gbps): 2,000-200,000

初期設定

- ♦ Ethernet half duplex: 2,000,000、full duplex: 1,000,000、トランク : 500,000
- ♦ Fast Ethernet half duplex: 200,000、full duplex: 100,000、トランク : 50,000
- ♦ Gigabit Ethernet full duplex: 10,000、トランク : 5,000

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 (P337)

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ないます。"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 (16 飛ばしでの 0-240 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 (P336)

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 : 1-50)
 - **port-channel** *channel-id* (範囲 : 1-25)

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

show spanning-tree ethernet *unit / port*

show spanning-tree port-channel *channel-id*

show spanning-tree mst *instance-id*

- ◆ **ethernet** *unit / port*
 - *unit* ユニット番号 "1"
 - *port* ポート番号 (範囲 : 1-50)
- ◆ **port-channel** *channel-id* (範囲 : 1-25)
- ◆ **mst** *instance-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 P110 「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 P114 「インター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:                MSTP
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:                   32768.0.0013F715B2E0
Current Root Port:                  0
Current Root Cost:                  0
Number of Topology Changes:         1
Last Topology Change Time (sec.): 18819
Transmission Limit:                 3
Path Cost Method:                   Long
-----
Eth 1/ 1 Information
-----
Admin Status:                       Enabled
Role:                                Disabled
State:                               Discarding
External Admin Path Cost: 10000
Internal Admin Path Cost: 10000
External Oper Path Cost: 10000
Internal Oper Path Cost: 10000
Priority:                            128
Designated Cost:                     0
Designated Port:                     128.1
Designated Root:                     32768.0.0013F715B2E0
Designated Bridge:                   32768.0.0013F715B2E0
Fast Forwarding:                     Disabled
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
.
.
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:XSTP REGION 0
Revision level:0

Instance Vlans
-----
      1      2
Console#
```

4.17 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
Editing VLAN Groups	VLAN 名、VID、状態を含む VLAN の設定	P342
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	P344
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	P351
Configuring Private VLANs	アップリンク、ダウンリンクポートを含むプライベート VLAN の設定	P353

4.17.1 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	P342
VLAN	VID,VLAN 名、ステートなど VLAN の設定	VC	P343

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 (P351)

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**}]

no vlan *vlan-id* [**name** | **state**]

- ◆ *vlan-id* 設定する VLAN ID (範囲 : 1-4094)
- ◆ **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。

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 256VLAN の設定が可能です。

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 (P351)

4.17.2 VLAN インターフェースの設定

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	P344
switchport mode	インタフェースの VLAN メンバーモードの設定	IC	P345
switchport acceptableframe 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	P346
switchport ingress-filtering	インタフェースへの入力フィルタの有効化	IC	P347
switchport native vlan	インタフェースの PVID(native VLAN) の設定	IC	P348
switchport allowed vlan	インタフェースに関連した VLAN の設定	IC	P349
switchport gvrp	インタフェースへの GVRP の有効化	IC	P364
switchport forbidden vlan	インタフェースの登録を禁止する VLAN の設定	IC	P350
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	P370

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。

文法

interface vlan *vlan-id*

- ◆ *vlan-id* 設定する VLAN ID (範囲 : 1-4094)

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 (P351)

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 {trunk | hybrid| private-vlan}

no switchport mode

- ♦ **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。
- ♦ **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。
- ♦ **private-vlan** 詳細については、P4-174 の "switchport mode private-vlan" を参照して下さい。

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)

例

本例では、1 番ポートの configuration モードの設定を行い、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)#
```

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 (P345)

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。

[注意] 本機の Ingress filtering は常に有効です。無効に設定することはできませんが、Ingress filtering コマンドは常に利用可能になっており、"no switchport ingress-filtering" コマンドも入力が可能です。使用時には "Note:Failed to ingress-filtering on ethernet interface!" のエラーが出て、設定変更不可能となります。

文法

switch port ingress-filtering

初期設定

無効 (Disabled)

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 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 : 1-4094)

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、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)#
```

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。

[注意] 各ポートは、1つのタグなし VLAN にのみ所属することができ、この VLAN がポートの PVID となります。2つ目のタグなし VLAN に所属させた場合、最初に Tag なしとして所属していた VLAN は、自動的に Tag 付きへ変わり、2つ目の VLAN がポートの PVID に設定されます。

また、"no switchport allowed vlan" コマンドを使用し、VLAN の所属から外れた場合は、ポートの PVID はタグなしの VLAN1 に変更されます。

Tag 付き VLAN に関しては、各ポートが複数の VLAN に所属することが可能です。

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：1-4094）

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。

- ◆ ポートへの接続装置にかかわらず、タグなし VLAN メンバーを追加することができます。初期設定では VLAN1 となります。
各ポートは 1 つのタグなし VLAN にしか所属できないので、もし 2 つ目の VLAN がタグなしと定義された場合、もう一方の VLAN は自動的にタグつきに変更されます。
またポートの PVID もこの VLAN ID へ変更されます。

例

本例では、1 番ポートのタグ付 VLAN 許可リストに VLAN2,5,6 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 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：1-4094）

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)#
```


4.17.3 VLAN 情報の表示

コマンド	機能	モード	ページ
show vlan	VLAN 情報の表示	NE,PE	P351
show interfaces status vlan	特定 VLAN インタフェースの状態の表示	NE,PE	P296
show interfaces switchport	インタフェースの管理、運用状態の表示	NE,PE	P299

show vlan

VLAN 情報の表示を行います。

文法

show vlan [*id vlan-id* | **name** *vlan-name* | **private-lan**

private-vlan-type]

- ♦ **id** VLAN ID が続くキーワード
vlan-id 表示する VLAN ID (範囲 : 1-4093)
- ♦ **name** VLAN 名が続くキーワード
vlan-name 1-32 文字の VLAN 名
- ♦ **private-vlan** 本コマンドに関する詳細は、P4-177 の "show vlan private-vlan" コマンドを参照して下さい。
private-van-type プライベート VLAN の種類 (オプション : Community、Isolated、Primary)

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 Channel: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#
```

4.17.4 プライベート VLAN の設定

プライベート VLAN は、ポートベースでのセキュリティの確保と VLAN 内のポート間の分離を行うことができます。本機はプライマリ VLAN と、セカンダリ VLAN の 2 種類をサポートしています。プライマリ VLAN には無差別ポートがあり、このポートは同じプライベート VLAN に所属する他のポートと通信が可能です。セカンダリ (コミュニティ) VLAN にはコミュニティポートがあり、このポートは同じセカンダリ VLAN 内の他のホスト、又は関連付けを行ったプライマリ VLAN の任意の無差別ポートとのみ通信が可能です。独立 VLAN は、1 つの無差別ポートと 1 つ以上の独立 (又はホスト) ポートから構成される、単一のスタンドアロンの VLAN です。いずれの VLAN も無差別ポートはインターネットなど外部ネットワークからのアクセスが可能です。コミュニティ / 独立ポートはローカルユーザからのアクセスのみに制限されます。

本機には複数のプライマリ VLAN を設定でき、又複数のコミュニティ VLAN を各プライマリ VLAN と関連付けできます。独立 VLAN も 1 つ以上設定できます (プライベート VLAN と通常の VLAN は同一スイッチ内に同時に構成することができることに注意して下さい)

コマンド	機能	モード	ページ
<i>Edit Private VLAN グループ</i>			
private-vlan	プライマリ、コミュニティ、独立 VLAN の追加と削除	VC	P355
private-vlan association	コミュニティ VLAN とプライマリ VLAN の関連付け	VC	P356
<i>Configure Private VLAN Interface</i>			
switchport mode private-vlan	インタフェースへのホストモード / 無差別モードの指定	IC	P357
switchport private-vlan host-association	インタフェースのセカンダリ VLAN への関連付け	IC	P358
switchport private-vlan isolated	インタフェースの独立 VLAN への関連付け	IC	P358
switchport private-vlan mapping	インタフェースのプライマリ VLAN へのマッピング	IC	P359
<i>プライベート VLAN の表示</i>			
show vlan private-vlan	プライベート VLAN の情報を表示	NE,PE	P360

プライマリ / セカンダリに関連付けられたグループに設定するには、以下の手順で行います。

- (1) "private-vlan" コマンドを使用し、1 つ以上のコミュニティ VLAN と、コミュニティグループ以外のトラフィックのやり取りをお行うプライマリ VLAN を 1 つ指定します。
- (2) "private-vlan association" コマンドを使用し、コミュニティ VLAN とプライマリ VLAN とのマッピングを行います。
- (3) "switchport mode private-vlan" コマンドを使用し、ポートを無差別（プライマリ VLAN のすべてのポートと通信が可能）又はホスト（コミュニティポートなど）に指定します。
- (4) "switchport private-vlan host-association" コマンドを使用し、ポートをセカンダリ VLAN に割り当てます。
- (5) "switchport private-vlan mapping" コマンドを使用し、ポートをプライマリ VLAN に割り当てます。
- (6) "show vlan private-vlan" コマンドを使用し、設定内容を確認します。

独立 VLAN を設定するには、以下の手順で行います。

- (1) "private-vlan" コマンドを使用し、独立 VLAN を指定します。独立 VLAN には、1 つの無差別ポートと 1 つ以上の独立ポートが所属しています。
- (2) "switchport mode private-vlan" コマンドを使用し、ポートを無差別（プライマリ VLAN のすべてのポートと通信が可能）又はホスト（コミュニティポートなど）に指定します。
- (3) "switchport private-vlan isolated" コマンドを使用し、ポートを独立 VLAN に指定します。
- (4) "show vlan private-vlan" コマンドを使用し、設定内容を確認します。

Private vlan

プライベート VLAN（プライマリ、コミュニティ、独立）を作成します。"no" を前に置くことで、プライベート VLAN を削除します。

文法

private-vlan *vlan-id* {**community** | **primary** | **isolated**}

no private-vlan *vlan-id*

- ♦ *vlan-id* プライベート VLAN の ID（範囲：1-4094）
- ♦ **community** 同一の VLAN に所属するホストか、又は関連付けられたプライマリ VLAN に所属する無差別ポートのみに通信が制限される VLAN
- ♦ **primary** 1 つ以上のコミュニティ VLAN を所有し、コミュニティ VLAN と他との通信のやり取りを行う VLAN
- ♦ **isolated** 独立 VLAN。独立ポートに関連付けられたポートは、同じ VLAN に所属する無差別ポートとのみ通信が可能

初期設定

なし

初期設定

VLAN Configuration

コマンド解説

- ♦ プライベート VLAN は、同一のコミュニティ VLAN 又は同一の独立 VLAN に所属するポート宛に、或いは VLAN 外の場合は無差別ポート宛に、通信先を制限する場合に使用します。コミュニティ VLAN を使用する場合、無差別ポートを所有する "プライマリ" VLAN とマッピングされなくてはなりません。独立 VLAN を使用する場合、単一の無差別ポートを所有するように設定しなくてはなりません。
- ♦ プライベート VLAN におけるポートの所属方法は静的な設定で行います。一度ポートがプライベート VLAN に所属すると、GVRP で他の VLAN に動的に移動できなくなります。
- ♦ プライベート VLAN をトランクモードに設定することはできません P345 「switchport mode」コマンドを参照して下さい)

例

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#
```

private vlan association

プライマリ VLAN をセカンダリ（コミュニティ）VLAN に関連付けます。"no" を前に置くことで、指定したプライマリ VLAN に関連付けられていたものがすべて削除されます。

文法

private vlan *primary-vlan-id* **association** {*secondary-vlan-id* |

add *secondary-vlan-id* | **remove** *secondary-vlan-id*}

no private vlan *primary-vlan-id* **association**

- ♦ *primary-vlan-id* プライマリ VLAN の ID（範囲：1-4094）
- ♦ *secondary-vlan-id* セカンダリ（コミュニティ）VLAN（範囲：1-4094）

初期設定

なし

コマンドモード

VLAN Configuration

コマンド解説

- ♦ セカンダリ VLAN は所属メンバーのセキュリティを確保します。関連付けられたプライマリ VLAN はプライマリ VLAN 内で他のネットワークとの、又は（無差別ポートを介した）プライマリ VLAN の外の宛先との、共通のインタフェース（無差別ポート）となります。

例

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

[注意] 本機の仕様では、全てのパケットは初期設定で所属 VLAN のタグ付きとなります。そのため、本機に直接接続した PC 同士は、異なる VLAN 間（例：Primary VLAN10 と Community VLAN20）での通信は Association の有無にかかわらず不可となります。

switchport mode private-vlan

インタフェースにプライベート VLAN 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

switchport mode private-vlan {host | promiscuous}

no switchport mode private-vlan

- ◆ **host** コミュニティ VLAN または独立 VLAN に割り当て可能なポートに設定します。
- ◆ **promiscuous** 関連付けられたセカンダリ VLAN に所属するすべてのポートと、又同じプライマリ VLAN に所属する他のすべての無差別ポートと通信可能なポートに設定します。

初期設定

Normal VLAN

コマンドモード

Interface Configuration (Ethernet、Port Channel)

コマンド解説

- ◆ プライマリ VLAN に無差別ポートを割り当てるには、"switch port private-vlan mapping" コマンドを使用します。ホストポートをコミュニティ VLAN に割り付けるには、"private-vlan host association" コマンドを使用します。
- ◆ 無差別ポート又はホストポートを独立 VLAN に割り当てるには、"switch port private-vlan isolated" コマンドを使用します。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config-if)#
```

switchport private-vlan host-association

インタフェースにセカンダリ VLAN を関連付けます。"no" を前に置くことで、関連付けを削除します。

文法

switchport private-vlan host-association *secondary-vlan-id*

no switchport private-vlan host-association

- ♦ *secondary-vlan-id* セカンダリ (コミュニティ) VLAN の ID (範囲 : 1-4094)

初期設定

なし

コマンドモード

Interface Configuration (Ethernet、Port Channel)

コマンド解説

- ♦ セカンダリ VLAN に割り当てたすべてのポートはグループメンバー間で通信できますが、グループ外との通信は関連付けたプライマリ VLAN の無差別ポート経由で行わなくてはなりません。

例

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config-if)#
```

switchport private-vlan isolated

インタフェースを独立 VLAN に割り当てます。"no" を前に置くことで、割り当てを解除します。

文法

switchport private-vlan isolated *isolated-vlan-id*

no switchport private-vlan isolated

- ♦ *isolated-vlan-id* - 独立 VLAN の ID (範囲 : 1-4094)

初期設定

なし

コマンドモード

Interface Configuration (Ethernet、Port Channel)

コマンド解説

独立 VLAN に割り当てたホストポートはグループメンバー間で通信できないため、グループ外との通信は無差別ポート経由で行わなくてはなりません。

例

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan isolated 3
Console(config-if)#
```

switchport private-vlan mapping

インタフェースをプライマリ VLAN にマッピングします。"no" を前に置くことで、マッピングを削除します。

文法

switchport private-vlan mapping *primary-vlan-id*

no switchport private-vlan mapping

- ♦ *primary-vlan-id* - プライマリ VLAN の ID (範囲 : 1-4094)

初期設定

なし

コマンドモード

Interface Configuration (Ethernet、Port Channel)

コマンド解説

- ♦ セカンダリ VLAN に割り当てた無差別ポートは同一 VLAN 内の他の無差別ポートと、又関連付けたセカンダリ VLAN 内のグループメンバーと通信できます。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config-if)#
```

show vlan private-vlan

本機におけるプライベート VLAN の設定情報を表示します。

文法

show vlan private-vlan [community | isolated | primary]

- ♦ **community** - コミュニティ VLAN をすべて表示します。関連付けられたプライベート VLAN、割り当てられたホストポート情報も一緒に表示します。
- ♦ **isolated** - 独立 VLAN を表示します。割り当てられた無差別ポートとホストポート情報も一緒に表示します。"Primary" 又は "Secondary" フィールドに表示しているのは、独立 VLAN の ID 番号です。
- ♦ **primary** - プライマリ VLAN をすべて表示します。割り当てられた無差別ポート情報も一緒に表示します。

初期設定

なし

コマンドモード

Privileged Executive

例

```
Console#show vlan private-vlan
Primary    Secondary    Type          Interfaces
-----
          5              primary      Eth1/ 3
          5              community    Eth1/ 4  Eth1/ 5
          0              isolated
Console#
```

4.17.5 LEC (Learning Equivalent Class) コマンド

コマンド	機能	モード	ページ
lec	LEC 機能の利用	GC	P361

lec

lec (Learning Equivalent Class) 機能を有効にします。"no" を前に置くことで無効となります。

文法

lec auto

no lec

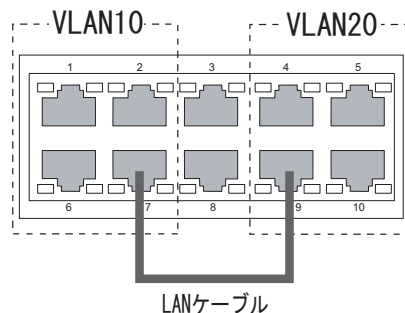
初期設定

無効

コマンドモード

Global Configuration

コマンド解説



本機はSVLスイッチであり、MACアドレス・テーブルはインデックスの一部としてVLAN IDを使用しません。アドレスが学習された時、それは全てのVLANに知らされます。もし、別のVLANに属するポートに同じアドレスが出現した場合、学習されているMACアドレスは元のポートから新しいポートまで移動します。新しいアドレスエントリを作成することはありません。

本機のもうひとつの特徴としてソフトウェア学習アプローチがあります。新しいアドレスが登録されるか、ソースポートが変更された時に、ソフトウェアはそれをCPUへ送り、CPUはアドレスをハードウェアアドレス・テーブルに挿入するという動作を行います。そのため、ポート運動のボリュームが大きい場合、スイッチ全体の性能へ影響が出る場合があります。全てのパケットバッファはアドレス学習に使われ、通常のスイッチ機能が使用可能な分はなくなるからです。

このような仕様により、本機では上図のような構成において、ポート1とポート5間等での通信を行うことはできません。

この問題を解決するため、本機は、擬似的に Individual VLAN Learning の効果を実現することにより、同じアドレスの出現がポート移動として扱われるのを防ぎ、パケットを正しく各デスティネーションポートへ送ることができる機能を持っています。

この機能を "learning equivalent class" または "lec" と呼びます。

設定例 *上図参照下さい。

- (1) ポート 1,2,6,7 を VLAN10 のメンバーにし、native VLAN ID を 10 に設定します。
- (2) ポート 4,5,9,10 を VLAN20 のメンバーにし、native VLAN ID を 20 に設定します。
- (3) これら以外の VLAN メンバーシップはこのスイッチに存在させないでください。
- (4) ポート 7 と 9 をケーブルで接続します。これらが VLAN ブリッジポートです。
- (5) スパニングツリー機能を無効に設定してください。
- (6) 以上の設定により、ポート 1,2,6 とポート 4,5,10 間での通信が可能になります。

[注意] 本構成を有効にする為には、スパニングツリー機能を無効にしなければなりません。

[注意] 設定例以外の構成はサポートされていません。

[注意] LEC 機能によりコントロール可能な VLAN は 2 つまでです。3 つ以上の VLAN はサポートされていません。

[注意] LEC 機能は CLI でのみ設定が可能です。

例

```
Console(config)#lec auto
Console(config)#
```

4.18 GVRP (GARP VLAN Registration Protocol)

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	P363
show bridge-ext	bridge extension 情報の表示	PE	P364
switchport gvrp	インタフェースへの GVRP の有効化	IC	P364
switchport forbidden vlan	インタフェースへの登録禁止 VLAN の設定	IC	P350
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	P365
garp timer	選択した機能への GARP タイマーの設定	IC	P365
show garp timer	選択した機能への GARP タイマーの表示	NE,PE	P367

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 (Disabled)

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)#
```

show bridge-ext

bridge extension 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 P126 「VLAN 基本情報の表示」及び P27 「ブリッジ拡張機能の表示」を参照して下さい。

例

```
Console#show bridge-ext
Max support vlan numbers:          256
Max support vlan ID:               4094
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:                Enabled
GMRP:                              Disabled
Console#
```

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

[no] switchport gvrp

初期設定

無効 (Disabled)

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 gvrp configuration

GVRP が有効かどうかを表示します。

文法

show gvrp configuration [*interface*]

- ◆ *interface*
 - **ethernet** *unit/port*
 - \bar{A} /*unit* ユニット番号 "1"
 - \bar{A} /*port* ポート番号 (範囲 : 1-50)
 - **port-channel** *channel-id* (範囲 : 1-25)

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#
```

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値に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 (P367)

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*
 \AA /*unit* ユニット番号 "1"
 \AA /*port* ポート番号 (範囲 : 1-50)
 - **port-channel** *channel-id* (範囲 : 1-25)

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:      100 centiseconds
Leave timer:      60 centiseconds
Leaveall timer: 1000 centiseconds
Console#
```

関連するコマンド

garp timer (P365)

4.19 プライオリティ

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	P368
Priority (Layer 3 and 4)	TCP ポート、IP DSCP タグの CoS 値への設定	P375

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
<i>Layer 2 Priority Commands</i>			
queue mode	キューモードを "strict" 又は " Weighted Round-Robin (WRR)" に設定	GC	P369
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	P370
queue bandwidth	プライオリティキューに重み付けラウンドロビン を指定	GC	P371
queue cos map	プライオリティキューに Class of Service(CoS) を指定	IC	P372
show queue mode	現在のキューモードを表示	PE	P373
show queue bandwidth	プライオリティキューの重み付けラウンドロビン を表示	PE	P373
show queue cos-map	CoS マップの表示	PE	P374
show interfaces switchport	インタフェースの管理、運用ステータスの表示	PE	P299

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}

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ェイト 1、2、4、6 を設定し、その値に応じて帯域を共有します。

初期設定

WRR(Weighted Round Robin)

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ェイト 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。

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)#
```

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

プライオリティの設定はしてありません。タグなしフレームへの初期設定値は 0 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

- ◆ 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 IEEE802.1Q 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 8 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
```

queue bandwidth

4 つの CoS に対し重み付けラウンドロビン (Weighted Round-Robin / WRR) による重み付けを行います。"no" を前に置くことで初期設定に戻します。

文法

queue bandwidth *weight1...weight8*

no queue bandwidth

- ◆ *weight1...weight8* キュー 0 ~ 7 の WRR スケジューラで使用する重みの比率 (範囲 : 1-15)

初期設定

1、2、4、6 がそれぞれキュー 0-7 に対応しています。キュー 0 は設定できません。

コマンドモード

Global Configuration

コマンド解説

WRR はスケジューリングされた重さでの出力ポートでのバンド幅の共用を許可します。

例

本例では WRR の重み付けを行っています。

```
Console(config)#queue bandwidth 6 9 12
Console(config)#
```

関連するコマンド

show queue bandwidth (P373)

queue cos-map

CoS 値をハードウェア出力キューのプライオリティキュー 0-7 に対応させます。"no" を前に置くことで初期設定に戻します。

文法

queue cos-map *queue_id* [*cos1* ... *cosn*]

no queue cos-map

- ◆ *queue_id* Å\ CoS プライオリティキュー ID
 - 0-7 の値で 3 が最高の CoS プライオリティキュー
- ◆ *cos1* .. *cosn* キュー ID にマッピングする CoS 値。スペースでわけられた数字のリスト。CoS 値は 0-7 までの値で、7 が最高のプライオリティ

初期設定

各ポートに対し重み付けラウンドロビンと共に 4 段階のプライオリティキューの CoS をサポートします。8 つにわけられたトラフィッククラスが IEEE802.1p で定義されています。定義されたプライオリティレベルは IEEE802.1p 標準の推奨された以下のテーブルにより設定されます。

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

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ◆ 入力ポートで指定した CoS 値は出力ポートで使用されます。
- ◆ 本コマンドでは全インタフェースの CoS プライオリティを設定します。

例

本例では、CoS 値 0、1、2 を出力キュー 0 に、CoS 値 3 を出力キュー 1 に、CoS 値 4、5 を出力キュー 2 に、CoS 値 6、7 を出力キュー 3 に設定しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#end
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
CoS Value      : 0 1 2 3 4 5 6 7
Priority Queue: 0 0 0 1 2 2 3 3
Console#
```

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: wrr
Console#
```

show queue bandwidth

ラウンドロビン (WRR) バンド幅を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show queue bandwidth
Queue ID Weight
-----
0      1
1      2
2      4
3      6
Console#
```

show queue cos-map

CoS プライオリティマップを表示します。

文法

show queue cos-map [*interface*]

- ♦ *interface*
 - **ethernet** *unit/port*
 \mathring{A} /*unit* ユニット番号 "1"
 \mathring{A} /*port* ポート番号 (範囲: 1-50)
 - **port-channel** *channel-id* (範囲: 1-25)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
CoS Value      : 0 1 2 3 4 5 6 7
Priority Queue: 0 0 0 1 2 2 3 3
Console#
```


4.19.2 プライオリティコマンド (Layer 3 and 4)

コマンド	機能	モード	ページ
map ip dscp	IP DSCP CoS マップの有効化	GC	P375
map ip dscp	IP DSCP CoS のマップ	IC	P376
map access-list ip	パケットが ACL ルールに一致するよう、CoS 値と各出力キューとを設定	IC	P268
show map ip dscp	IP DSCP マップの表示	PE	P377
show mapaccess-list ip	インタフェースのアクセスリストにマッピングされた CoS 値の表示	PE	P269

map ip dscp (Global Configuration)

IP DSCP (Differentiated Services Code Point mapping) マッピ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

[no] map ip dscp

no map ip dscp

初期設定

無効 (Disabled)

コマンドモード

Global Configuration

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、ポートプライオリティです。

例

本例では本機に IP DSCP マッピングを有効にしています。

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (interface Configuration)

IP DSCP (Differentiated Services Code Point) 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

map ip dscp *dscp-value* **cos** *cos-value*

no map ip dscp

- ♦ *dscp-value* 8-bit DSCP 値 (範囲 : 0-63)
- ♦ *cos-value* CoS 値 (範囲 : 0-7)

初期設定

下記の表は初期設定のマッピングです。マッピングされない DSCP 値はすべて CoS 値 0 に設定されます。

IP DSCP 値	CoS 値
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

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、ポートプライオリティです。
- ♦ DSCP プライオリティは IEEE802.1p 標準で推奨されている CoS 初期値にマッピングされ、その後、それに続けて 4 つのハードウェアプライオリティキューにマッピングされます。
- ♦ このコマンドは、すべてのインタフェースの IP DSCP プライオリティを設定します。

例

本例では IP DSCP 値 1 を CoS 値 0 に設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip dscp

IP DSCP プライオリティマップの表示を行います。

文法

show map ip dscp [*interface*]

- ◆ *interface*
 - **ethernet** *unit/port*
 - *unit* ユニット番号 "1"
 - *port* ポート番号 (範囲: 1-50)
 - **port-channel** *channel-id* (範囲: 1-4)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: enabled

Port          DSCP  COS
-----
Eth 1/ 1      0    0
Eth 1/ 1      1    0
Eth 1/ 1      2    0
Eth 1/ 1      3    0
.
.
Eth 1/ 1      61   0
Eth 1/ 1      62   0
Eth 1/ 1      63   0
Console#
```

関連するコマンド

map ip dscp (Global Configuration) (P375)

map ip dscp (Interface Configuration) (P376)

4.20 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	P378
IGMP Query	レイヤ 2 でのマルチキャストフィルタリングの IGMP query パラメータの設定	P382
Static Multicast Routing	静的マルチキャストルータポートの設定	P387

4.20.1 IGMP Snooping コマンド

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

[no] ip igmp snooping

初期設定

有効 (Enabled)

コマンドモード

Global Configuration

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 vlan static

マルチキャストグループにポートを追加します。"no" を前に置くことでグループからポートを削除します。

文法

ip igmp snooping vlan *vlan-id* **static** *ip-address* *interface*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* *interface*

- ♦ *vlan-id* VLAN ID (範囲 : 1-4094)
- ♦ *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 : 1-50)
 - **port-channel** *channel-id* (範囲 : 1-25)

初期設定

なし

コマンドモード

Global Configuration

例

本例ではポートにマルチキャストグループを静的に設定しています。

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
ethernet 1/5
Console(config)#
```

ip igmp snooping version

IGMP snooping の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 version {1 | 2}

no ip igmp snooping version

- ♦ **1** IGMP Version 1
- ♦ **2** IGMP Version 2

初期設定

IGMP Version 2

コマンドモード

Global Configuration

コマンド解説

- ◆ サブネット上のすべてのシステムが同じバージョンをサポートする必要があります。もし既存のデバイスが Version 1 しかサポートしていない場合、本機に対しても Version 1 を設定します。
- ◆ "ip igmp query-max-response-time" コマンド及び "ip igmp router-port-expire-time" コマンドは Version 2 でしか使えません。

例

本例では IGMP Version 1 に設定しています。

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

show ip igmp snooping

IGMP snooping の設定情報を表示します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

表示される内容に関しては、P151 「IGMP Snooping Query 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
Service status: Enabled
Querier status: Enabled
Query count: 2
Query interval: 125 sec
Query max response time: 10 sec
Router port expire time: 300 sec
IGMP snooping version: Version 2
Console#
```

show mac-address-table multicast

マルチキャストアドレスとして認識されているリストを表示します。

文法

show mac-address-table multicast [*vlan vlan-id*]

[user | igmp-snooping]

- ♦ *vlan-id* VLAN ID (範囲 : 1-4094)
- ♦ **user** ユーザ設定のマルチキャストエントリのみ表示
- ♦ **igmp-snooping** IGMP snooping によって学習されたアドレスのみ表示

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

メンバーの種類は選択したオプションにより IGMP 又は USER を含む表示がされます。

例

本例では VLAN 1 で IGMP snooping により登録されたマルチキャストエントリを表示しています。

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
VLAN M'cast IP addr. Member ports Type
-----
   1         224.1.2.3      Eth1/11    IGMP
Console#
```

4.20.2 IGMP Query コマンド (Layer2)

コマンド	機能	モード	ページ
ip igmp snooping querier	IGMP snooping クエリアとしての動作の有効化	GC	P382
ip igmp snooping query-count	クエリーカウントの設定	GC	P383
ip igmp snooping query-interval	クエリー間隔の設定	GC	P384
ip igmp snooping query-maxresponse-time	レポート遅延の設定	GC	P385
ip igmp snooping router-port-expire-time	クエリータイムアウトの設定	GC	P386

ip igmp snooping querier

IGMP snooping クエリアとしての機能を有効にします。"no" を前に置くことで機能を無効にします。

文法

[no] ip igmp snooping querier

初期設定

有効 (Enabled)

コマンドモード

Global Configuration

コマンド解説

有効にした場合、本機はクエリアとして機能します。クエリアはマルチキャストトラフィックを受け取る必要があるかどうか、ホストに質問します。

例

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

クエリーカウン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

ip igmp snooping query-count *count*

no ip igmp snooping query-count

- ♦ *count* マルチキャストグループからクライアントを除外する前に、スイッチからクエリー送信する最大回数（範囲：2-10）

初期設定

2 回

コマンドモード

Global Configuration

コマンド解説

クエリーカウントではマルチキャストクライアントからの応答をクエリアが待つ回数を定めます。クエリアが本コマンドで定義された数のクエリーを送り、クライアントからの応答がなかった場合、"**ip igmp snooping query-max-response-time**" コマンドで指定したカウントダウンタイマーがスタートします。

カウントダウンが終わり、クライアントからの応答がない場合、クライアントがマルチキャストグループからはずれたと判断されます。

例

本例では、クエリーカウントを 10 に設定しています。

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

関連するコマンド

ip igmp snooping query-max-response-time (P385)

ip igmp snooping query-interval

クエリ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

ip igmp snooping query-interval *seconds*

no ip igmp snooping query-interval

- ♦ *seconds* IGMP クエリを送信する間隔（範囲：60-125）

初期設定

125（秒）

コマンドモード

Global Configuration

例

本例ではクエリ間隔を 100 秒に設定しています。

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

クエリ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

ip igmp snooping query-interval *seconds*

no ip igmp snooping query-interval

- ♦ *seconds* IGMP クエリを送信する間隔（範囲：5-25）

初期設定

10（秒）

コマンドモード

Global Configuration

コマンド解説

- ♦ 本機能を有効にするには IGMP v2 を使用する必要があります。
- ♦ クエリ後のマルチキャストクライアントからの正式な回答があるまでの待ち時間を設定します。クエリアが送信するクエリ数を "ip igmp snooping query-count" コマンドを使用して設定している場合、クライアントからの応答がないとカウントダウンタイマーが本コマンドで設定した値でスタートします。カウントダウンが終わり、クライアントからの応答がない場合、クライアントがマルチキャストグループからはずれたと判断されます。

例

本例では、最大返答時間を 20 秒に設定しています。

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

ip igmp snooping router-port-expiretime

クエリー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* クエリーパケットを受信していたルータポートが無効になると判断される前の待機時間（範囲：300-500（秒））

初期設定

300（秒）

コマンドモード

Global Configuration

コマンド解説

本機能を有効にするには IGMP v2 を使用する必要があります。

例

本例では、タイムアウト時間を 300（秒）に設定しています。

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

関連するコマンド

ip igmp snooping version (P379)

4.20.3 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	P387
show ip igmp snooping mrouter	マルチキャストルータポートの表示	PE	P388

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 : 1-4094)
- ◆ *interface*
 - **ethernet** *unit/port*
 - A/unit* ユニット番号 "1"
 - A/port* ポート番号 (範囲 : 1-50)
 - **port-channel** *channel-id* (範囲 : 1-25)

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 snooping 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 : 1-4094)

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 1/11   Static
 2                Eth 1/12   Static
Console#
```

4.21 IP インターフェース

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。

4.21.1 基本 IP 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	P389
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	P390
ip dhcp restart	BOOTP/DHCP クライアントリクエストの送信	PE	P391
show ip interface	本機の IP 設定の表示	PE	P392
show ip redirects	本機のデフォルトゲートウェイ設定の表示	PE	P392
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	P393

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

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。

[注意] IP アドレスは VLAN インタフェース 1 つのみに割り当てできます (初期設定では VLAN1 に割り当てられています) ここで設定した VLAN が管理用の VLAN となり、この VLAN を介してのみ本機への管理アクセスが可能になります。IP アドレスを他の VLAN に割り当てると、新たに割り当てた IP アドレスが既存の IP アドレスを上書きし、新たな管理 VLAN として機能します。

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 (P391)

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

show ip redirects (P392)

ip dhcp restart

BOOTP/DHCP クライアントリクエストを送信します。

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 又は DHCP に設定済みの IP インタフェースに対し、BOOTP/DHCP クライアントリクエストを送信します。
- ◆ DHCP は、有効な場合、サーバにクライアントの最後の IP アドレスを再付与するよう要求します。
- ◆ DHCP/BOOTP サーバが別のドメインに移動した場合、クライアントに付与されていた IP アドレスのネットワーク部は新たなドメインの IP アドレスとなります。

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)#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: DHCP.
Console#
```

関連するコマンド

ip address (P389)

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
IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
and address mode: User specified.
Console#
```

関連するコマンド

show ip redirects (P392)

show ip redirects

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 redirects
ip default gateway 10.1.0.254
Console#
```

関連するコマンド

ip default-gateway (P390)

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

設定されたホストはありません。

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: 0 ms
Ping statistics for 10.1.0.9:
    5 packets transmitted, 5 packets received (100%), 0 packets lost
    (0%)
Approximate round trip times:
    Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

関連するコマンド

interface (P288)

付録 A. トラブルシューティング

Telnet 又は Web ブラウザ、SNMP ソフトウェアから接続できない。

- ◆ スイッチに電源が投入されていることを確認して下さい。
- ◆ 管理端末とスイッチを接続するネットワークケーブルが、正しく接続されていることを確認して下さい。
- ◆ スイッチとの接続と接続先のポートが、無効になっていないか確認して下さい。
- ◆ 有効な 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が設定されたエージェントであることを確認して下さい。
- ◆ 管理端末が管理 VLAN (初期設定では VLAN 1) に接続していることを確認して下さい。
- ◆ 管理端末の IP アドレスが、スイッチが接続している IP インタフェースと同じサブネットの IP アドレスであることを確認して下さい。
- ◆ タグ付 VLAN グループに所属する IP アドレスを使用してスイッチへの接続を行おうとしている場合は、管理端末、及びネットワークへの接続を中継するスイッチに接続しているポートの設定が正しいタグになっていることを確認して下さい。
- ◆ Telnet で接続できない場合は、同時に接続できる Telnet セッション数の最大値を超過している可能性があります。
- ◆ 時間を置いて再度接続してみてください。

セキュアシェルを使用した接続ができない。

- ◆ SSH での接続ができない場合は、同時に接続できる Telnet/SSH セッション数の最大値を超過している可能性があります。
- ◆ 時間を置いて再度接続してみてください。
- ◆ SSH サーバの制御パラメータがスイッチに対して正しく設定されており、SSH クライアントソフトウェアが管理端末に対して正しく設定されていることを確認して下さい。
- ◆ スイッチの公開キーを生成し、このキーを SSH クライアントに提供していることを確認して下さい。
- ◆ 各 SSH ユーザアカウント (ユーザ名、認証レベル、パスワードを含む) を設定していることを確認して下さい。

- ♦（公開キーによる認証機能を使用している場合）クライアントの公開キーをスイッチに取り込んでいることを確認して下さい。

シリアルポート接続から内蔵の設定プログラムに接続できない。

- ♦ ターミナルエミュレーションプログラムが、以下の通り設定されていることを確認して下さい。

ターミナル：VT100 互換
データビット：8 ビット
ストップビット：1 ビット
パリティ：なし
通信速度：9600 bps

- ♦ 同梱のシリアルケーブルを使用していることを確認して下さい。

パスワードを無くしてしまった、又は忘れてしまった。

- ♦ お買い上げの販売店または、当社指定のサービス窓口にご連絡下さい。

■ 付録 B. グロッサリー（用語説明） ■

和文表記	英語表記	説明
ACL (アクセスコントロールリスト)	ACL (Access Control List)	個々のネットワーク利用者が持つアクセス権限や、アクセス可能なサーバやファイルなどを列挙したリスト。ネットワーク上の機器や情報の利用権限を一元管理する為に利用。
ARP	ARP (Address Resolution Protocol)	TCP/IP で LAN 上の通信をする時に、相手側機器の MAC アドレスを知るために使用される通信手順のこと。
BOOTP	BOOTP (Boot Protocol)	TCP/IP ネットワークのクライアントマシンにおいて、IP アドレスやホスト名、ドメイン名等のパラメータを、サーバから自動的にロードしてくるためのプロトコル。
CoS	CoS (Class of Service)	通信品質の保証や帯域確保などを実現する QoS 技術の一種。
CLI (コマンドラインインターフェース)	CLI (Command Line Interface)	コマンド入力により機器の設定・管理を行うインターフェース
CRC	CRC (Cyclic Redundancy Check)	巡回冗長検査の略。連続して出現する誤りの検出が可能な検出方式。
DSCP	DSCP (Differentiated Services Code Point Service)	それぞれのサービスに合った転送処理を行うために、ルータなどの動作を決めるコード。IP フローの IP ヘッダ内 DS Field の上位 6 ビット。
DHCP	DHCP (Dynamic Host Control Protocol)	IP アドレスをホストに自動的に付与するサービス。DHCP サーバが IP アドレスを管理、付与し、DHCP クライアントが IP アドレスを割り振られる。
EAPOL	EAPOL (Extensible Authentication Protocol over LAN)	LAN 上で動作する拡張可能な認証プロトコル。IEEE802.1X に規定されている EAP のメッセージを LAN 上で伝送する為のしくみ。
GARP	GARP (Generic Attribute Registration Protocol)	イーサネット接続時に、複数の機器どうして情報を交換する手順。
GVRP	GVRP (GARP VLAN Registration Protocol)	V-LAN グループに関する各種設定情報を機器間でやりとりする手順。
ICMP	ICMP (Internet Control Message Protocol)	IP のエラーメッセージや制御メッセージを転送するプロトコル。TCP/IP で接続されたコンピュータやネットワーク機器間で、互いの状態を確認するために用いられる。

和文表記	英語表記	説明
IEEE 802.1D	IEEE 802.1D	「STP（スパニングツリープロトコル）」を参照
IEEE 802.1Q	IEEE 802.1Q	「タグ VLAN」を参照
IEEE 802.1X	IEEE 802.1X	ユーザ ID 及びパスワードを使用した、ポート単位でのアクセス制御について定めている。この規格に準拠すると、ネットワークへのアクセス時にユーザ認証を行うことが可能になる。
IEEE 802.3ad	IEEE 802.3ad	「LACP」を参照
IEEE 802.3x	IEEE 802.3x	「フローコントロール」を参照
IGMP	IGMP (Internet Group Management Protocol)	同一のデータを複数のホストに効率よく配送する IP マルチキャストで、配送を受けるために構成されるホストのグループを制御するためのプロトコル。
IGMP Snooping	IGMP Snooping	IP マルチキャストルータと IP マルチキャストグループの間で伝送される IGMP Query と IGMP Report のパケットのスヌーピングを行い、IP マルチキャストグループのメンバを識別する。
IVL	IVL (Independent VLAN Learning)	VLAN 学習方式。個々の VLAN ごとに Mac Address Table を持つ。
LACP	LACP (Link Aggregation Control Protocol)	ポートトラंकを実現する方法の 1 つです。LACP (Link Aggregation Control Protocol、IEEE 802.3ad) を有効に設定している機器同士がネゴシエーションを行い、トラंकグループを形成します。
LED	LED (Light Emitting Diode)	発光ダイオード。表示する色や点灯の状態によってリンク状態を示す。
MAC アドレス	MAC Address (Media Access Controller Address)	ネットワークでホストを識別するために設定されるハードウェアアドレス。
MD5	MD5 (Message-Digest Algorithm)	認証やデジタル署名などに使われるハッシュ関数（一方方向要約関数）のひとつ。原文を元に固定長の「ハッシュ値」を発生し、通信経路の両端で比較することで、通信途中で原文が改ざんされていないかを検出することができる。
MIB	MIB (Management Information Base)	SNMP で管理されるネットワーク機器が、自分の状態を外部に知らせるために公開する情報のこと。
NIC	NIC (Network Interface Card)	ネットワークインターフェースカード。LAN で利用されるカード類の総称。
NTP	NTP (Network Time Protocol)	コンピュータの内部時計を、ネットワークを介して正しく調整するプロトコル。

グロッサリー（用語説明）

和文表記	英語表記	説明
OSI	OSI (Open Systems Interconnection)	ISO が標準化した、様々のシステムを相互接続するための概念。7 つの階層とそのプロトコルを規定している。
PING	PING (Packet INternet Groper)	ネットワーク上のコンピュータが通信可能な状態かどうか確かめるためのプログラム。
PVID	PVID (Port VLAN ID)	ポートベース VLAN ID
QoS	QoS (Quality of Service)	通信の品質を守るための制御方法や技術のこと。
RADIUS	RADIUS (Remote Authentication Dial-in User Service)	ダイヤルアップしてきたユーザーを、リモートアクセスサーバーが中央のサーバーと通信して認証し、要求されたシステムやサービスへのアクセスを許可する、クライアント / サーバー型のプロトコルおよびソフトウェア。
RFC	RFC (Request For Comment)	TCP/IP に関する仕様を記述している公開文書です。
RMON	RMON (Remote Monitoring)	遠隔地にある LAN のトラフィックやエラーなどの通信状況を監視する機能。SNMP の拡張機能として提供される。
RO	RO (Read Only)	読み出しのみ
RSTP	RSTP (Rapid Spanning Tree Protocol)	STP が改良されたもの。RSTP では BPDU のやり取りをタイマではなくハンドシェイク方式で行っているため、STP でかかっていた再構築時の収束時間が短くなる。
RW	RW (Read Write)	読み出しと書き込み
RX	RX (Receive)	受信
SNMP	SNMP (Simple Network Management Protocol)	ネットワークに接続する機器や PC などの監視や設定をネットワーク経由で行うためのプロトコル。SNMP では、SNMP マネージャがマネジメントを行う機器で、SNMP エージェントがそのマネジメントの対象となる。SNMP マネージャは、ネットワークを介して SNMP エージェントの MIB (Management Information Base) 情報を取得したり、設定することによって、各機器の適切なマネジメントを行い、SNMP エージェントは、SNMP マネージャからの要求への返答、自発的に状態を通知 (トラップ) を行う。
SNTP	SNTP (Simple Network Time Protocol)	TCP/IP ネットワークを通じてコンピュータの時刻を同期させるプロトコルの一つで、SNTP は NTP の仕様のうち複雑な部分を省略し、クライアントがサーバに正確な時刻を問い合わせる用途に特化している。
SSH	SSH (Secure Shell)	ネットワークを介して別のコンピュータへのログイン、遠隔地のマシンでコマンドを実行、他のマシンへファイルを移動等に使用されるプログラム。ネットワーク上を流れるデータは暗号化されるため、インターネット経由でも一連の操作を安全に行なうことができる。

和文表記	英語表記	説明
STP（スパンニングツリープロトコル）	STP (Spanning Tree Protocol)	ネットワーク内のループを回避するサービス。スイッチやハブは、ブロードキャストフレームを受信すると、それぞれが接続しているすべての機器のポートに対してブロードキャストフレームを送信する。ネットワークに接続している機器同士が複数の経路で接続している場合、これによってブロードキャストストームが発生してしまう。これを回避するのが STP（Spanning Tree Protocol）で、IEEE 802.1D で規定。
SVL	SVL (Shared VLAN Learning)	VLAN 学習方式。全 VLAN が一つの Mac Address Table を共有。
TACACS+	TACACS+ (Terminal Access Controller Access Control System Plus)	NAS(Network Access Server) に対して認証・課金を提供するプロトコル。ユーザーパスワードは、別個のルーターではなく中央のデータベースで管理される。
Telnet	Telnet	TCP/IP ネットワークにおいて、ネットワークにつながれたコンピュータを遠隔操作するための標準方式。
TFTP	TFTP (Trivial File Transfer Protocol)	Trivial File Transfer Protocol の略。ファイル転送用のインターネットユーティリティです。UDP 上で動作する、簡易なファイル転送プロトコルのこと。
TX	TX (Transmit)	送信
UDP	UDP (User Datagram Protocol)	信頼性よりも効率が重視されたコネクションレスのプロトコル。
VLAN	VLAN (Virtual LAN)	物理的な LAN とは別の論理的に構成された LAN、またはそれを実現する機能。VLAN を使用すると、実際に相互接続されていない機器が、同一のブロードキャストドメインに所属しているように通信を行うことが可能。
Xmodem	Xmodem	ファイル転送プロトコルの一つ。ファイル転送に伴う誤り検出・再送を行なうもの。
アウトバンド管理	Out-of-Band Management	主信号を伝送する回線の帯域を使用しないで実現する、ネットワーク管理手法。
タグ VLAN	Tag-based VLAN	データに「タグ」を付けて、データごとに送受信する VLAN を識別させる VLAN 構築方法。
トラップ	Trap	SNMP エージェントから SNMP マネージャに非同期に通知されるイベント通知。
トランク	Trunk	複数の回線を 1 つの論理的な回線にまとめる機能。たとえば、1Gbps の 4 つのポートを 1 つの論理的なトランクグループにまとめると、4Gbps の回線として使用できる。これにより、より広帯域での通信が可能になり、またこの 4 本のうちの 1 本が障害で断線した場合でも、残りの 3 本により通信環境が維持される。

グロッサリー（用語説明）

和文表記	英語表記	説明
プライベート VLAN	Private VLANs	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る。
フローコントロール	Flow Control	送信側のパケット送信を制御することにより、スイッチのバッファメモリが溢れることを予防し、ネットワークの帯域を有効利用する機能。
ポートミラーリング	Port Mirroring	1 つまたは複数のポートを指定し、この指定したポートの送受信パケットを別のポートにコピー（ミラーリング）する機能。この別のポートをミラーリングポートと呼び、ミラーリングポートを監視することにより、実際の通信に影響を与えることなくリアルタイムな通信の解析を行う。
ポートベース VLAN	Port-based VLAN	ポートを単位とする VLAN 構築方法。機器の物理的なポートに所属する VLAN を設定することによって、VLAN を識別。ポートベース VLAN では、1 つのポートは 1 つの VLAN のみに所属できる。
マルチキャスト	Multicast	ネットワーク内で、複数の相手を指定して同じデータを送信すること。これに対し、不特定多数の相手に向かってデータを送信することを「ブロードキャスト」、単一のアドレスを指定して特定の相手にデータを送信することを「ユニキャスト」という。
リンクアグリゲーション	Link Aggregation	広い意味でポートトランクと同じことを指す。しかし、厳密には、リンクアグリゲーションが IEEE802.3ad で規定されている LACP（Link Aggregation Control Protocol）によるトランク機能を指す場合もある。
レイヤー 2	Layer2	OSI モデルのレイヤ 2

FXC5148XG Management Guide (FXC06-DC-200019-R2.0)

初版 2006 年 10 月

2 版 2007 年 3 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
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG

Management Guide
FXC5148XG