Future X Communications

FXC9324XG Management Guide

CLI 設定

2017 年 2 月 Ver.1.3

FXC株式会社

本マニュアルについて

■ 本マニュアルでは、FXC9324XG の各種設定およびシステムの CLI による設定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、監視用の端末接続を行います。

コマンドラインの設定 ---------- 1

コマンドラインインタフェースの利用 1
コマンドラインインタフェースへのアクセス 1
コンソール接続 1
Telnet 接続 2

コマンド入力 3
キーワードと引数 3
コマンドの省略 3
コマンドの補完 3
コマンド上でのヘルプの表示 4
キーワードの検索 5
コマンドのキャンセル 5
コマンド入力履歴の利用 5
コマンドモード 6
Exec コマンド 6
Configuration コマンド 7
コマンドラインプロセス 9

コマンドグループ 10

General（一般コマンド） 12

システム管理 21
Device Designation コマンド 21
システム情報の表示 23
フレームサイズコマンド 32
FAN コントロール（ Flash/File ） 33
ファイル管理（ Flash/File ） 34
Line （ラインコマンド） 43
Event Logging コマンド 56
SMTP アラートコマンド 64
Time コマンド 69
タイムレンジ 76

SNMP コマンド 80

リモートモニタリング 106

フローサンプリング 113

ユーザ認証 119
ユーザーアカウント 119
認証コマンド 122
Radius クライアントコマンド 124
TACACS+ クライアントコマンド 129

AAA 132
Web サーバーコマンド 143
Telnet サーバーコマンド 147
Secure Shell コマンド 148
ポートセキュリティコマンド 160
IEEE802.1X ポート認証コマンド 162
管理 IP フィルターコマンド 172

セキュリティ対策 174
ポートセキュリティ 175
ネットワークアクセス (MAC アドレス認証) 180
WEB 認証 198
DHCP スヌーピング 204
IP ソースガード 215
ARP インスペクション 221

ACL（Access Control Lists） 232
IP ACL コマンド 232
MAC ACL コマンド 239
ACL 情報の表示 243

インタフェース設定モード 245

リンクアグリゲーション 267

ミラーポート 279

帯域制御 281

自動トラフィック制御 282

アドレステーブル 300

LLDP コマンド 304

スパニングツリー の設定 323

VLAN の設定 355
GVRP およびブリッジの拡張 356
VLAN グループの設定 361
VLAN インタフェースの設定 363
VLAN 情報の表示 370
IEEE802.1Q トンネリングの設定 371
ポートベースのトラフィックセグメンテーション 376
プロトコル VLAN の設定 383
サブネット VLAN の設定 388
MAC ベース VLAN の設定 390
音声 VLAN の設定 392

CoS (プライオリティ) 401
プライオリティコマンド（Layer 2）..... 401
プライオリティコマンド（Layer 3 and 4）..... 408

QoS 416

マルチキャストフィルタリング 427
IGMP Snooping コマンド 427
IGMP Query コマンド（Layer2）..... 434
静的マルチキャストルーティングコマンド 436
IGMP グループのフィルタリングとスロットリング 438

マルチキャスト VLAN の登録 453
IGMP (LAYER 3) 463
IGMP プロキシールーティング 476
MLD (LAYER 3) 479
MLD PROXY ROUTING 491

MLD スヌーピング 495
DNS 509

DHCP 518
DHCP Client 518
DHCP Relay 520
DHCP Server 522

VRRP 535
仮想ルータ冗長性プロトコル（VRRP）コマンド 535

IP インタフェース 545
IPv4 設定 545
ARP 552
UDP ヘルパー 556
IPv6 インタフェース 560
IPV6 から IPV4 へのトンネリング 592

IP ルーティング 603
グローバルルーティング設定 604
RIP 615

Open Shortest Path First (OSPFv2) 627

Open Shortest Path First (OSPFv3) 674

マルチキャストルーティングコマンド 708
マルチキャストルーティング 708
スタティックマルチキャストルーティング 717
PIM マルチキャストフィルタリング 719

1. コマンドラインの設定

1.1 コマンドラインインタフェースの利用

1.1.1 コマンドラインインタフェースへのアクセス

コンソールポート、又はネットワークから Telnet 経由で管理インタフェースにアクセスする場合、Unix のコマンドに似たコマンドキーとパラメータのプロンプト（コマンドラインインタフェース /CLI）により本機の設定を行います。

1.1.2 コンソール接続

コンソールポートへの接続は以下の手順で行います。

（1）コンソールプロンプトでユーザ名とパスワードを入力します。初期設定のユーザ名は "admin" と "guest"、パスワードも同じく "admin" と "guest" となっています。管理者ユーザ名とパスワード（初期設定ではどちらも "admin"）を入力した場合、CLI には "Console#" と表示され Privileged Exec モードとなります。一方ゲストユーザ名とパスワード（初期設定ではどちらも "guest"）を入力した場合、CLI には "Console>" と表示され Normal Exec モードとなります。

（2）ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。

（3）終了時には "quit" 又は "exit" コマンドを使用しセッションを終了します。

コンソールポートからシステムに接続すると以下のログイン画面が表示されます。

```
Username: admin
Password:

      CLI session with the FXC9324XG is opened.
      To end the CLI session, enter [Exit].

Console#
```

1.1.3 Telnet 接続

Telnet を利用するとネットワーク経由での管理が可能となります。Telnet を行うには管理端末側と本機側のどちらにも IP アドレスを事前に設定する必要があります。また、異なるサブネットからアクセスする場合にはデフォルトゲートウェイもあわせて設定する必要があります。

[注意] 工場出荷時には、本機は DHCP サーバー経由で IP アドレスが割り振られる設定になっています。

IP アドレスとデフォルトゲートウェイの設定例は以下の通りです。

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

本機を外部と接続されたネットワークに接続する場合には、登録された IP アドレスを設定する必要があります。独立したネットワークの場合には内部で自由に IP アドレスを割り当てることができます。

本機の IP アドレスを設定した後、以下の手順で Telnet セッションを開始することができます。

(1) リモートホストから Telnet コマンドと本機の IP アドレスを入力します。

(2) プロンプト上でユーザ名とパスワードを入力します。Privileged Exec モードの場合には "Vty-0#" と表示されます。Normal Exec モードの場合には "Vty-0>" と表示されます。

(3) ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。

(4) 終了時には "quit" 又は "exit" コマンドを使用しセッションを終了します。

```
Username: admin
Password:

      CLI session with the FXC9324XG 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。

1.2 コマンド入力

1.2.1 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
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
```

1.2.2 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。

1.2.3 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。

1.2.4 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。

コマンド上で "?" と入力すると、現在のコマンドクラスの第一階層にあるすべてのキーワードが表示されます。また特定のコマンドのキーワードを表示することもできます。例えば "show ?" と入力すると、"show" コマンド内で使用できるコマンド一覧が表示されます。

```
Console#show ?
  access-group          Access groups
  access-list           Access lists
  accounting            Uses the specified accounting list
  arp                   Information of ARP cache
  authorization         Authorization configurations
  auto-traffic-control  Auto traffic control information
  bridge-ext            Bridge extension information
  cable-diagnostics     Shows the information of cable
diagnostics
  calendar              Date and time information
  class-map             Displays class maps
  cluster               Display cluster
  debug                 State of each debugging option
  dns                   DNS information
  dos-protection        Shows the system dos-protection summary
information
  dot1q-tunnel          802.1Q tunnel
  dot1x                 802.1X content
  erps                  Displays ERPS configuration
  ethernet              Shows Metro Ethernet information
  garp                  GARP properties
  gvrp                  GVRP interface information
  history               Shows history information
  hosts                 Host information
  interfaces            Shows interface information
  ip                    IP information
  ipv6                  IPv6 information
  lacp                  LACP statistics
  line                  TTY line information
  lldp                  LLDP
  log                   Log records
  logging               Logging setting
  loop                  Shows the information of loopback
  mac                   MAC access list
  mac-address-table     Configuration of the address table
  mac-vlan              MAC-based VLAN information
  management            Shows management information
  map                   Maps priority
  memory                Memory utilization
  mvr                   Multicast VLAN registration
  mvr6                  IPv6 Multicast VLAN registration
```

コマンドの表示

"show interfaces ?" と入力した場合には、以下のような情報が表示されます。

```
Console#show interfaces ?
brief            brief interface description
  counters       Interface counters information
  protocol-vlan  Protocol-VLAN information
  status         Interface status information
  switchport     Interface switchport information
Console#show     interfaces
```

1.2.5 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       sntp      spanning-tree   ssh     startup-config
systemConsole#show s
```

1.2.6 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。

1.2.7 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。

1.2.8 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、使用できるコマンドはそれぞれのモード毎に異なります。"?" コマンドを入力すると、現在のモードで使用できるすべてのコマンドの一覧が表示されます。コマンドのクラスとモードは以下の表の通りです。

クラス	モード	
Exec	Normal Privileged	
Configuration	Global	Access Control List Class Map DHCP Interface Line Multiple Spanning Tree Policy Map Router 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。

1.2.9 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:

      CLI session with the FXC9324XG is opened.
      To end the CLI session, enter [Exit].

Console#
```

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

      CLI session with the FXC9324XG is opened.
      To end the CLI session, enter [Exit].

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

1.2.10 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。
- Class Map Configuration — DiffServe クラスマップを作成するためのモードです。
- DHCP Configuration — DHCP サーバの設定を行います。
- 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。
- Multiple Spanning Tree Configuration— 選択された MSTP インスタンスの設定を行うためのモードです。
- Policy Map Configuration — DiffServe ポリシーマップを設定します。
- Router Configuration — ルーティングプロトコルのグローバル設定を行います。
- VLAN Configuration — VLAN グループを設定するためのモードです。

Global Configuration モードにアクセスするためには、Privileged Exec モードで "configure" コマンドを入力します。画面上のプロンプトが "Console(config)#" と変更になり、Global Configuration のすべてのコマンドを使用することができるようになります。

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

他のモードへは、以下の表のコマンドを入力することにより入ることができます。又、それぞれのモードからは "exit" 又は "end" コマンドを使用して Privileged Exec モードに戻ることもできます。

モード	コマンド	プロンプト	ページ
Line	Line {console | vty}	Console(config-line)#	P44
Access Control List	access-list ip permit,deny （Standard ACL） permit,deny （Extended ACL）	 Console(config-std-acl) Console(config-ext-acl)	P233 P234 P235
Class Map	class map	Console(config-cmap)	P417
DHCP	ip dhcp pool	Console(config-dhcp)	P524
Interface	Iinterface {ethernet port | port-channel id | vlan id}	Console(config-if)#	P246
MSTP	spanning-tree mst-configuration	Console(config-mstp)#	P331
Policy Map	policy map	Console(config-pmap)	P420
router	router rip	Console(config-router)	P616
VLAN	vlan database	Console(config-vlan)	P361

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)#
```

1.2.11 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の文字を削除します。
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。

1.3 コマンドグループ

システムコマンドは機能別に以下の表の通り分類されます :

コマンドグループ	内容	ページ
General	Privileged Exec モードへのアクセスやシステムの再起動、CLI からのログアウトなど基本的なコマンド	P12
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	P21
Simple Network Management Protocol	SNMP の設定（認証失敗トラップの起動、コミュニティアクセス文字列およびトラップレシーバの設定）	P80
User 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	P119
General Security Measures	共有のデータポートに接続されたクライアントのトラフィックの切り分けを行い、有効なスタティック、またはダイナミックアドレスによる認証されていないアクセス、web 認証、MAC アドレス認証、DHCP リクエスト / 応答のフィルタリング、無効な ARP 応答の破棄を行います。	P174
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	P232
Interface	Trunk、LACP や VLAN などを各ポートの設定	P245
Link Aggregation	複数ポートをグループ化するポートトランク及び Link Aggregation Control Protocol (LACP) の設定	P267
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	P279
Rate Limit	通信の最大送受信帯域のコントロール	P281
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、エイジングタイムの設定	P300
Spanning Tree	STA 設定	P323
VLANs	各ポートの VLAN グループの設定及プロトコル VLAN の設定	P355
Class of Service	タグ無しフレームへのポートプライオリティの設定、Strict プライオリティまたは wrr の設定、その他プライオリティの設定	P401
Quality of Service	Diff Serv の設定	P416
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	P427
Link Layer Discovery Protocol	LLDP 設定を行い、隣接ルータデバイスの検出情報を有効にします。	P304
Domain Name Server	DNS サーバの設定	P509

Dynamic Host Configuration Protocol	DHCP クライアント、リレー、サーバ機能の設定	P518
IP Interface	管理アクセス用 IP アドレスの設定	P545
IP Routing	静的および動的ユニキャストルーティングの設定	P603
Open Shortest Path First(OSPF2)	小規模から大規模のネットワーク向けのリンクステート型ルーティング・プロトコルの設定	P627
Open Shortest Path First(OSPF3)	小規模から大規模のネットワーク向けのリンクステート型ルーティング・プロトコルの設定	P674
マルチキャストルーティング	マルチキャストルーティングプロトコル PIM-DM および PIM-SM を設定します。	P708

本章内の表で用いられるコマンドモードは以下の括弧内のモードを省略したものです。

ACL （Access Control List Configuration）

CM （Class Map Configuration）

DC （DHCP Server Configuration）

GC （Global Configuration）

IC （Interface Configuration）

LC （Line Configuration）

MST （Multiple Spanning Tree）

NE （Normal Exec）

PE （Normal Exec）

PM （Policy Map Configuration）

RC （Router Configuration）

VC （VLAN Database Configuration）

1.4 General（一般コマンド）

コマンド	機能	モード	ページ
prompt	CLI prompt のカスタマイズ	GC	P12
reload	指定した時間（遅延、あるいは一定の間隔ごと）にシステムを再起動します。	GC	P13
enable	Privileged モードの有効化	NE	P14
quit	CLI セッションを終了	NE, PE	P15
show history	コマンド履歴バッファの表示	NE,PE	P16
configure	Global Configuration モードの有効化	PE	P17
disable	Privileged モードから Normal モードへの変更	PE	P17
reload	本機の再起動	PE	P18
show reload	現行のリロードの設定、次回リロードを行う時間を表示	PE	P19
prompt	CLI プロンプトのカスタマイズ	GC	P12
end	Privileged Exec モードへの変更	GC,IC, LC,VC	P19
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	P20
quit	CLI セッションを終了	NE,PE	P15

prompt

CLI prompt のカスタマイズを行います。コマンドの前に "no" を置くことで初期設定に戻ります。

文法

prompt string

no prompt

string - CLI prompt 用の英文字

(最大 : 255 文字)

初期設定

Console

コマンドモード

Global Configuration

例

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

reload (Global Configuration)

指定した時間（遅延、あるいは一定の間隔ごと）にシステムを再起動します。

文法

reload {at hour minute [{month day | day month} [year]] |
in {hour hours | minute minutes | hour hours minute minutes} |
regularity hour minute [period {daily | weekly day-of-week | monthly day}] | cancel [at | in | regularity]}

reload at - **本機をリロードを行う指定された時間**

hour - **リロードを行う時間単位** (**有効な範囲** : 0-23)

minute - **リロードを行う分単位の時間** (**有効な範囲** : 0-59)

month - **リロードを行う月** (1 **月～** 12 **月**)

day - **リロードを行う日** (**有効な範囲** : 1-31)

year - **リロードを行う年** (**有効な範囲** : 2001-2050)

reload in - **本機をリロード後の間隔**

hours - **本機をリセットするまでの時間（分と組み合わせたもの）**(**有効な範囲** : 0-576)

minutes - **本機をリセットするまでの分（時間と組み合わせたもの）**(**有効な範囲** : 0-59)

reload regularity - **本機のリロードを行う周期的間隔**

hour - **リロードを行う時間** (**有効な範囲** : 0-23)

minute - **リロードを行う分単位の時間** (**有効な範囲** : 0-59)

day-of-week - **リロードを行う曜日** (**有効な範囲** : **月～土**)

day - **リロードを行う日** (**有効な範囲** : 1-31)

reload cancel - **指定したオプションを取り消します。**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **システム全体をリセットします。**
- **リロードのオプションの組み合わせを指定します。同じオプションを再度指定した場合でも、前の設定は上書きされます。**
- **システムを再起動すると、**Power-On Self-Test. **を実行します。**copy running-config startup-config **コマンドを使って、不揮発メモリにストアされている設定情報をすべて保存することも可能です。**

例

ここでは、30 分後に本機をリセットする方法について表示します。

```
Console(config)#reload in minute 30
***
*** --- Rebooting at January  1 02:10:43 2007 ---
***

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

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 P6「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、P121 「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（P17）
enable password（P121）

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:
```

show history

保存されているコマンドの履歴を表示する際に利用します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- 本機に保存できるコマンド履歴は Execution コマンドと Configuration コマンドがそれぞれ最大 10 コマンドです。

例

本例では、コマンド履歴として保存されているコマンドを表示しています。

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

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

Console#
```

"!" コマンドを用いると、履歴のコマンドを実行することが可能です。Normal 又は Privileged Exec モード時には Execution コマンドを、Configuration モード時には Configuration コマンドの実行が行えます。

本例では、"!2" コマンドを入力することで、Execution コマンド履歴内の 2 番目のコマンド（"config" コマンド）を実行しています。

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

configure

Global Configuration モードを有効にする場合に使用します。スイッチの設定を行うためには Global Configuration モードにする必要があります。さらに Interface Configuration, Line Configuration, VLAN Database Configuration などを行うためには、その先のモードにアクセスします。詳細は P6「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（P19）

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 P6 「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（P14）

reload (Privileged Exec)

システムを再起動します。

[**注意**]

- **再起動時には** Power-On Self-test **が実行されます。**copy running-config startup-config **コマンドを使って、不揮発メモリにストアされている設定情報をすべて保存することも可能です。**

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（P14）

show reload

現在のリロードの設定、次回リロードされる予定時間が表示されます。

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

The switch will be rebooted at January 1 02:11:50 2001.
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

end

Privileged モードに戻る際に利用します。

初期設定

なし

コマンドモード

Global Configuration

Interface Configuration

Line Configuration

VLAN Database Configuration

Multiple Spanning Tree 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:
```

1.5 システム管理

このコマンドはシステムログ、ユーザ名、パスワード、WEB インタフェースの設定に使用されます。また、他のシステム情報の表示や設定を行えます。

コマンド	機能	ページ
Device Designation	本機を特定する情報設定	P21
System Status	管理者やシステムバージョン、システム情報の表示	P23
Fan Control	FAN の設定	P33
Frame Size	ジャンボフレームサポートの有効化	P32
File Management	コードイメージまたは設定ファイルの管理	P34
Line	シリアルポートのパラメータを設定	P43
Event logging	エラーメッセージのログをコントロール	P56
SMTP Alerts	SMTP、E メールアラートの設定	P64
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	P69
Time Range	Access Control List などの 他の機能により使用されるタイムレンジを設定	P76

1.5.1 Device Designation コマンド

コマンド	機能	モード	ページ
hostname	ホスト名の設定	GC	P22
snmp-server contact	システムコンタクト者の設定	GC	P84
snmp-server location	システムロケーションの設定	GC	P84
switch renumber	スタックユニットのリナンバリング	PE	P22

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。コマンドの前に "no" **を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)#
```

switch all renumber

スイッチユニットの識別番号をリセットします。すべてのスタック番号は、非ループスタック用に、トップユニットから開始して連続的に付けられるか、ループスタック用にマスターユニットから開始します。

文法

switch all renumaber

初期設定

- **非ループスタッキング用：トップユニットが** 1
- **ループスタッキング用：マスターユニットが** 1

コマンドモード

Global Configuration

例

```
Console#switch all renumber
Console#
```

1.5.2 システム情報の表示

コマンド	機能	モード	ページ
show access-list tcam- utilization	TCAM の使用率パラメータを表示します。	PE	P23
show memory	メモリの使用率パラメータを表示します。	NE, PE	P24
show process cpu	CPU 使用率パラメータを表示します。	NE, PE	P24
show running-config	実行中の設定ファイルの表示	PE	P25
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	P27
show system	システム情報の表示	NE,PE	P28
show tech-support	システム設定の詳細なリストが表示され、技術的なサポートの解決を行うことが可能です。 show users アクティブコンソールをすべて表示します。		P29
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	P30
show version	システムバージョン情報の表示	NE,PE	P31

show access-list tcam-utilization

TCAM (Ternary Content Addressable Memory) の使用率パラメータを表示します（使用中のナンバーポリシーコントロール、フリーエントリ数、および使用中の TCAM のパーセンテージを含む）。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- PCE(Policy control entries) は、ACL、IP ソースガードフィルタールール、QoS、あるいはトラップを含む、ルール ベースの検索に応じて各種システム機能によって使用されます例えば、ポートへの ACL のバインディング時に ACL の各ルールは 2 つの PCE を使用し、ポートの IP ソースガードフィルタルールを設定時にも、同様に 2 つの PCE が使用されます。

例

```
Console#show access-list tcam-utilization
 Total Policy Control Entries : 512
 Free Policy Control Entries  : 508
 TCAM Utilization             : 0.78%
Console#
```

show memory

メモリの使用率パラメータを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- **現在使用されていないメモリ、アクティブなプロセスに割り当てられているメモリ、システムメモリの総量が表示されます。**

例

```
Console#show memory
StatusBytes
------ ---------- Free134946816
Used133488640
Total268435456

Console#
```

show process cpu

CPU **使用率パラメータを表示します。**

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show process cpu
CPU Utilization in the past 5 seconds : 3.98%

Console#
```

show running-config

現在実行中の設定ファイルを表示するためのコマンドです。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 起動用ファイルと、実行中の設定ファイルの内容を比較する場合には "show startup-config" コマンドを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。
  - スタック内のそれぞれのスイッチの MAC アドレス
  - SNTP サーバの設定
  - SNMP コミュニティ名
  - ユーザ（ユーザ名及びアクセスレベル）
  - VLAN データベース（VLAN ID, VLAN 名及び状態）
  - 各インタフェースの VLAN 設定状態
  - MSTP インスタンス（名前、インタフェース）
  - VLAN に設定された IP アドレス
  - レイヤ 4Precedence 設定
  - ルーティングプロトコル設定
  - 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 running-config
Building running configuration. Please wait...
!<stackingDB>0000000000000000</stackingDB>
!<stackingMac>01_00-00-e8-93-82-a0_01</stackingMac>
!<stackingMac>00_00-00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00-00_00</stackingMac>
!
snmp-server community public ro
snmp-server community private rw
!
snmp-server enable traps authentication
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree mst configuration
!
interface ethernet 1/1
switchport broadcast packet-rate 500
switchport allowed vlan add 1 untagged
switchport native vlan 1
.
!
interface vlan 1
ip address dhcp
!
no ip igmp snooping proxy-reporting
!
interface vlan 1
!
line console
!
line vty
!
end
!
Console#show running-config interface ethernet 1/1
interface ethernet 1/1
switchport allowed vlan add 1 untagged
switchport native vlan 1
queue weight 1 2 4 6 8 10 12 14
!
Console#
```

関連するコマンド

show startup-config (P27)

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" コマンドを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：
  - スタック内のそれぞれのスイッチの MAC アドレス
  - SNTP サーバの設定
  - SNMP コミュニティ名
  - ユーザ（ユーザ名及びアクセスレベル）
  - VLAN データベース（VLAN ID, VLAN 名及び状態）
  - 各インタフェースの VLAN 設定状態
  - MSTP インスタンス（名前、インタフェース）
  - VLAN に設定された IP アドレス
  - レイヤ 4Precedence 設定
  - ルーティングプロトコル設定
  - スパニングツリー設定
  - コンソール及び Telnet に関する設定

起動している Config ファイルの例を参照してください。

関連するコマンド

show running-config (P25)

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

- **このコマンドによって表示される項目の説明は** P20 **「システム情報の表示」を参照してください。**
- "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    : FXC9324XG Managed L3 Stackable Switch
System OID String     : 1.3.6.1.4.1.572.17389.302
System Information
System Up Time        : 0 days, 0 hours, 21 minutes, and 47.6
seconds
System Name           :
System Location       :
System Contact        :
MAC Address (Unit 1)  : 00-00-E8-93-82-A0
Web Server            : Enabled
Web Server Port       : 80
Web Secure Server     : Enabled
Web Secure Server Port: 443
Telnet Server         : Enabled
Telnet Server Port    : 23
Jumbo Frame           : Disabled

System Fan:
Force Fan Speed Full  : Disabled
Unit 1
Fan 1: Ok                   Fan 2: Ok                   Fan 3: Ok
System Temperature: Unit 1
Temperature 1: 28 degrees    Temperature 2: 44 degrees
Console#
```

show tech-support

テクニカルサポートによりコンフィグレーション、あるいは機能上の問題点を解決できるようにシステム設定のリストの詳細を表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- **ここでは、システムの詳細およびインタフェースの設定などの情報のリストを生成します。そのため、お使いのターミナルエミュレーションプログラムで提供される適切な出力キャプチャ機能を使ってファイルに出力することをお勧めします。**

例

```
Console#show tech-support

show system:
System Description    : FXC9324XG Managed L3 Stackable Switch
System OID String     : 1.3.6.1.4.1.572.17389.302
System Information
System Up Time:         0 days, 2 hours, 17 minutes, and 6.23 seconds
System Name:            [NONE] System Location:
                        [NONE] System Contact:
[NONE]
MAC Address (Unit1)  :  00-12-CF-61-24-2F
Web Server:             Enabled
Web Server Port:        80
Web Secure Server:      Enabled
Web Secure Server Port: 443
Telnet Server:          Enable
Telnet Server Port:     23
Jumbo Frame:            Disabled
```

show users

コンソール及び Telnet で接続されているユーザの情報を表示するためのコマンドです。ユーザ名、接続時間及び Telnet 接続時の IP アドレスを表示します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- **コマンドを実行したユーザは行の先頭に "*" が表示されています。**

例

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

Online Users:
LineUser NameIdle time (h:m:s) Remote IP addr
------- ------------------------------- ----------------- ------
---------
* Console admin         0:00:00
  SSH                   00:05:59 ::FFFF:192.168.0.61
  VTY 2   admin         0:00:03  192.168.0.61

Web Online Users:
  Line  User NameIdle time (h:m:s) Remote IP Addr
----- ------------------------------- ----------------- --------
------- HTTP  admin     0:01:24 192.168.0.61

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

- **このコマンドによって表示される項目の説明は別紙の『基本設定』マニュアルの 「ハードウェア及びソフトウェアバージョンの表示」を参照してください。**

例

```
Console#show version
Unit 1
 Serial Number           : S123456
 Hardware Version        : R0A
 EPLD Version            : 1.06
 Number of Ports         : 26
 Main Power Status       : Up
 Redundant Power Status  : Not present
 Role                    : Master
 Loader Version          : 1.2.2.0
 Linux Kernel Version    : 2.6.19.2-0.1
 Boot ROM Version        : 0.0.0.1
 Operation Code Version  : 1.2.2.0

Console#
```

1.5.3 フレームサイズコマンド

コマンド	機能	モード	ページ
jumbo frame	ジャンボフレームの利用	GC	P32

jumbo frame

ジャンボフレームの使用を有効にします。コマンドの前に "no" を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閾値が毎秒 64 パケットに制限されます。（詳細は、P256 「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。

例：1522-9216byte までのフレームサイズを設定可能

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

関連するコマンド

switchport mtu (P255)

show system (P28)

show ipv6 mtu (P572)

1.5.4 FAN コントロール（ Flash/File ）

ここでは、FAN の速度で使用するコマンドについて説明します。

コマンド	機能	モード	ページ
fan-speed force-full	FAN を最大速度に設定	GC	P33
show system	FAN の速度が最大に設定されているかどうかを表示	NE, PE	P28

fan-speed force-full

すべての FAN の速度を最大に設定します。コマンドの前に "no" を付けることにより、通常の動作速度にリセットします。

文法

[no] fan-speed force-full

初期設定

Normal speed

コマンドモード

Global Configuration

例

```
Console(config)#fan-speed force-full
Console(config)#
```

1.5.5 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
boot system	システム起動ファイル、イメージの設定	GC	P42
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	P36
delete	ファイルやコードイメージの削除	PE	P39
dir	フラッシュメモリ内のファイルの一覧の表示	PE	P40
whichboot	ブートファイルの表示	PE	P41

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（範囲：**1-8）

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** (:) **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（P40）
whitchboot（P41）

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 | ftp | running-config | startup-config | sftp | tftp | unit}
copy ftp {file | public-key | running-config | startup-config}
copy running-config {file | ftp | startup-config | tftp}
copy startup-config {file | ftp | running-config | tftp}
copy tftp {file | https-certificate | public-key | running-config | startup-config}
copy unit file

- file — **ファイルのコピーを可能にするキーワード**
- ftp — FTP **サーバからのコピーを行うキーワード**
- hifittps-certcate — 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）**
- 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**
- unit — **ユニットの指定**

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、WEB のマニュアルに記載されいてる「デフォルトのセキュアサイト証明書の置き換え」の項を参照して下さい。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、P145 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 tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config; 2. opcode; 3. loader: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

本例では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。

```
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（範囲：**1-8）

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（P40）
delete public-key（P154）

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（範囲：**1-8**）**

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**
Modify Time	**ファイルが削除されたデータおよび時間**
size	**ファイルサイズ** (byte)

例

本例は、すべてのファイル情報の表示を示しています。

```
Console#dir
        File Name                   Type  Startup Modify Time         Size(bytes)
------------------------- -------------- ------- ------------------- ----------
 Unit 1:
iPECS_ES-4500G_Op_V1.2.3.18.bix  OpCode    Y    2011-10-28 05:58:27   15061840
Factory_Default_Config.cfg       Config    N    2009-10-12 12:02:08   14988120
startup1.cfg                     Config    Y    2010-06-22 02:48:51       4549
 ---------------------------------------------------------------------------
                          Free space for compressed user config files:   1556480
                                                            Used space:  65552384
                                                           Total space:  67108864
Console#
```

whichboot

現在、本機がどのファイルから起動されているかを表示します。

文法

whichboot

初期設定

なし

コマンドモード

Privileged Exec

例

本例は、すべてのファイル情報の表示を示しています。

```
Console#whichboot
        File Name                   Type  Startup Modify Time         Size(bytes)
-------------------------------- ------- ------- ------------------- -----------
 Unit 1:
ES4526G-50G_V1.2.2.0.bix         OpCode     Y    2010-12-20 03:12:19   14905940
startup1.cfg                     Config     Y    2011-02-15 01:56:56       2775
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（範囲：**1-8）

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** (:) **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（P40）
whitchboot（P41）

1.5.6 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	P44
accounting exec	アカウント方式をローカルコンソール、Telnet、SSH 接続に適用します。	LC	P140
authorization exec	認証方式をローカルコンソール、Telnet、SSH 接続に適用します。	LC	P141
databits	各文字あたりのデータビットの設定	LC	P51
login	コンソール接続時のパスワードの有効化	LC	P45
parity	パリティビット生成の設定	LC	P52
password	コンソール接続時のパスワードの設定	LC	P46
timeout login response	CLI のログイン入力待ち時間の設定	LC	P47
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	P47
password-thresh	パスワード入力時のリトライ数の設定	LC	P49
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	P50
speed	ボーレートの設定	LC	P53
stopbits	1byte あたりのストップビット値の設定	LC	P54
disconnect	接続を終了します。	PE	P54
show line	ターミナル接続の設定情報を表示	NE,PE	P55

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（P55）
show users（P30）

login

ログイン時のパスワードを有効にします。コマンドの前に "no" **を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、**"usaname" **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（P120）
password（P46）

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。コマンドの前に "no" **を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（P45）
password-thresh（P49）

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

timeout login response { seconds }

no timeout login response

- seconds — タイムアウト時間（秒）（範囲：0-300 秒、0：タイムアウト設定なし）

初期設定

- CLI：無効（0 秒）
- Telnet：300 秒

コマンドモード

Line Configuration

コマンド解説

- 設定時間内にログインが検知されなかった場合、接続は切断されます。
- 本コマンドはコンソール接続と Telnet 接続の両方に有効となります。
- Telnet のタイムアウトを無効にすることはできません。
- タイムアウトを指定せずコマンドを実行した場合、初期設定に戻します。

例

本例ではタイムアウト時間を 120 秒（2 分）に設定しています。

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

関連するコマンド

silent-time (P50)
exec-timeout (P48)

exec-timeout

ユーザ入力のタイムアウト時間の設定を行います。コマンドの前に "no" **を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かった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。コマンドの前に "no" を置くことで指定したリトライ回数は削除されます。

文法

password-thresh threshold

no password-thresh

- threshold — **リトライ可能なパスワード入力回数（設定範囲：**1-120、0**：回数の制限をなくします）**

初期設定

3 **回**

コマンドモード

Line Configuration

コマンド解説

- **リトライ数が設定値を超えた場合、本機は一定時間、ログインのリクエストに応答しなくなります（応答をしなくなる時間に関しては** "silent-time" **コマンドでその長さを指定できます）。**Telnet **時にリトライ数が制限値を超えた場合には** Telnet **インタフェースが終了となります。**

例

本例ではパスワードのリトライ回数を 5 **回に設定しています。**

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

関連するコマンド

silent-time (P50)

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。コマンドの前に** "no" **を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 (P49)

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。コマンドの前に "no" **を置くことにより、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（P52）

parity

パリティビットの設定のためのコマンドです。コマンドの前に "no" **を置くことにより、初期設定に戻します。**

文法

parity { none | even | odd }

no parity

- none — **パリティ無し**
- even — **偶数パリティ**
- odd — **奇数パリティ**

初期設定

パリティ無し

コマンドモード

Line Configuration

コマンド解説

- **接続するターミナルやモデムなどの機器によっては個々のパリティビットの設定を要求する場合があります。**

例

本例では no parity **を設定しています。**

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

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。コマンドの前に "no" **を置くことにより、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

auto

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。コマンドの前に "no" を置くことにより、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 users（P30）
show ssh（P158）

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
  Login timeout:           Disabled
  Silent time:             Disabled
  Baudrate:                auto
  Databits:                8
  Parity:                  none
  Stopbits:                1

 VTY configuration:
  Password threshold:      3 times
  Interactive timeout:     600 sec
  Login timeout:           300 sec
Console#
```

1.5.7 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	P56
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	P57
logging host	syslog を送信するホストの IP アドレスの設定	GC	P58
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	P58
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	P59
clear log	ログバッファのクリア	PE	P60
show logging	ログ関連情報の表示	PE	P62
show log	ログメッセージの表示	PE	P61

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。コマンドの前に "no" を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 (P57)
clear log (P60)

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

logging history { flash | ram } level

no logging history { flash | ram }

- flash — フラッシュメモリに保存されたイベント履歴
- ram — RAM に保存されたイベント履歴
- level — レベルは以下の表の通りです。選択した Level から Level0 までのメッセージが保存されます（範囲：0-7）

レベル引数	レベル	解説	syslog 設定
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 7 - 0)

コマンドモード

Global Configuration

コマンド解説

- フラッシュメモリには、RAM に設定する Level より高い Level を設定して下さい。

例

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

logging host

ログメッセージを受け取る syslog サーバの IP アドレスを設定します。コマンドの前に "no" を置くことで 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

- 複数回使用して、ホスト IP アドレスのリストを作成します。
- 設定できるホスト IP アドレスの最大数は 5 です。

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。コマンドの前に "no" を置くことにより、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。コマンドの前に "no" を置くことにより、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 設定
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

無効（レベル：7-0）

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 3
Console(config)#
```

clear log

ログをバッファから削除するコマンドです。

文法

clear log [flash | ram]

- flash — **フラッシュメモリに保存されたイベント履歴**
- ram — RAM **に保存されたイベント履歴**

初期設定

Flash and RAM

コマンドモード

Privileged Exec

例

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

関連するコマンド

show logging（P62）

show log

スイッチのメモリに送信された、システム / イベントメッセージを表示します。

文法

show log {flash | ram}

flash — **フラッシュメモリ (恒久的) に保存されたイベント履歴**

ram — RAM(**電源投入時に消去される) に保存されたイベント履歴**

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- **メモリに保存されたシステム / イベントメッセージを表示します。タイムスタンプ、メッセージレベル、プログラムモジュール、機能、及びイベント番号を表示します。**

例

本例では、RAM **に保存しているサンプルメッセージを表示しています。**

```
Console#show log ram
[1] 00:01:30 2001-01-01
    "VLAN 1 link-up notification."
    level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
    "Unit 1, Port 1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
Console#
```

show logging

システム、イベントメッセージに関するログを表示します。

文法

show logging {flash | ram | sendmail | trap}

- flash — フラッシュメモリに保存されたイベント履歴
- ram — RAM に保存されたイベント履歴
- sendmail — SMTP イベントハンドラの設定を表示
- 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）と設定してあり、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

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 メッセージの閾値
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 (P68)

1.5.8 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	SMTP イベントハンドリングの有効化	GC	P67
logging sendmail host	アラートメッセージを受信する SMTP サーバ	GC	P64
logging sendmail level	アラートメッセージの閾値設定	GC	P65
logging sendmail destination-email	メール受信者の設定	GC	P66
logging sendmail source-email	メールの ”From” 行に入力されるアドレスの設定	GC	P67
show logging sendmail	SMTP イベントハンドラ設定の表示	NE,PE	P68

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。

コマンドの前に "no" を置くことで 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

なし

コマンドモード

Global Configuration

コマンド解説

- 最大 3 つの SMTP サーバを指定できます。複数のサーバを指定する場合は、サーバ毎にコマンドを入力して下さい。
- e-mail アラートを送信する場合、本機はまず接続を行ない、すべての e-mail アラートを順番に 1 通ずつ送信した後、接続を閉じます。
- 接続を行なう場合、本機は前回の接続時にメールの送信が成功したサーバへの接続を試みます。そのサーバでの接続に失敗した場合、本機はリストの次のサーバでのメールの送信を試みます。その接続も失敗した場合には、本機は周期的に接続を試みます（接続が行なえなかった場合には、トラップが発行されます）

例

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

logging sendmail level

アラートメッセージの閾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。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

- **イベント閾値のレベルを指定します。設定したレベルとそれ以上のレベルのイベントが指定したメール受信者に送信されます（例：レベル** 7 **にした場合はレベル** 7 **から** 0 **のイベントが送信されます）**

例

本例ではレベル 3 **からレベル** 0 **のシステムエラーがメールで送信されます。**

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

logging sendmail destination-email

アラートメッセージのメール受信者を指定します。

コマンドの前に "no" **を置くことで受信者を削除します。**

文法

logging sendmail destination-email email-address

no logging sendmail destination-email email-address

- email-address — **アラートメッセージの送信先アドレス（設定範囲：**1-41 **文字）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **最大** 5 **つのアドレスを指定することができます。複数のアドレスを設定する際はアドレス毎にコマンドを入力して下さい。**

例

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

logging sendmail source-email

メールの "From" **行に入力されるメール送信者名を設定します。**

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）**
- logging sendmail destination-email

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@this-
company.com
Console(config)#
```

logging sendmail

SMTP **イベントハンドラを有効にします。コマンドの前に** "no" **を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#
```

1.5.9 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	P69
sntp poll	リクエスト送信間隔の設定	GC	P70
sntp server	タイムサーバの指定	GC	P71
show sntp	SNTP 設定の表示	NE,PE	P72
clock timezone	本機内部時刻のタイムゾーンの設定	GC	P72
calendar set	システム日時の設定	PE	P74
show calendar	現在の時刻及び設定の表示	NE,PE	P75

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。コマンドの前に "no" を置くことで 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)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time: Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
SNTP status:Enabled
SNTP server:10.1.0.19.0.0.0.0.0.0.0.0
Current server:10.1.0.19
Console#
```

関連するコマンド

sntp server (P71)
sntp poll (P70)
show sntp (P72)

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。コマンドの前に "no" を置くことにより、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：6-16384 秒）

初期設定

16 秒

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 (P69)

sntp server

SNTP タイムリクエストを受け付ける IP アドレスを指定します。"no" を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

sntp 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ないます。本機はタイムサーバに対して応答を受信するまで要求を送信します。"sntp poll" コマンドに基づいた間隔でリクエストを送信します。

例

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

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
Current server   :137.92.140.80
Console#
```

clock timezone

本機内部時刻のタイムゾーンの設定を行ないます。

文法

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

- name — タイムゾーン名（範囲：1-29 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 (P72)

show clock

タイムゾーンおよびサマータイム設定を表示します。

コマンドモード

Privileged Exec

例

```
Console(config)#clock summer-time MESZ recurring 1 friday june 23 59 3
 saturday september 2 55 60
Console(config)#
```

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#
```

1.5.10 タイムレンジ

Access Control List などのその他の機能により使用するタイムレンジを設定します。

コマンド	機能	モード	ページ
time-range	タイムレンジ名を指定し、Time Range configuration モードに入る	GC	P76
absolute	コマンドの実行用のタイムレンジの設定	TR	P77
periodic	定期的にコマンドを実行するタイムレンジの設定	TR	P78
show time-range	設定されたタイムレンジの表示	PE	P79

Time Range

タイムレンジ名を指定し Time Range 設定モードに入ります。コマンドの前に "no" を置くことでサービスを無効にします。

文法

[no] time-range name

name - タイムレンジ名 (有効範囲 : 1-30 文字)

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- Access Control List などの機能で使用するタイムレンジを設定します。

例

```
Console(config)#time-range r&d
Console(config-time-range)#
```

absolute

コマンドを実行するタイムレンジを設定します。コマンドの前に "no" **を置くことでサービスを無効にします。**

文法

absolute start hour minute day month year
[end hour minutes day month year]

absolute end hour minutes day month year

no absolute

- hour - 24 **時間** (**有効範囲** : 0-23)
- minute - **分** (**有効範囲** : 0-59)
- day - **日** (**有効範囲** : 1-31)
- month - january | february | march | april | may | june | july | august | september | october | november | december
- year - **年** (4 **桁**) (**有効範囲** : 2009-2109)

初期設定

なし

コマンドモード

Time Range Configuration

コマンド解説

- **タイムレンジが設定されている場合は、新しいタイムレンジを設定する前に、コマンドの前に** "no" **を置くことでサービスを無効にしてください。**

例

```
Console(config)#time-range r&d
Console(config-time-range)#absolute start 1 1 1 april 2009 end 2
1 1 april 2009
Console(config-time-range)#
```

periodic

定期的にコマンドを実行するタイムレンジを設定します。コマンドの前に "no" **を置くことでサービスを無効にします。**

文法

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

  daily - **毎日**
  friday - **金曜日**
  monday - **月曜日**
  saturday - **土曜日**
  sunday - **日曜日**
  thursday - **木曜日**
  tuesday - **火曜日**
  wednesday - **水曜日**
  weekdays - **平日**
  weekend - **週末**
  hour - 24 **時間** (**有効範囲** : 0-23)
  minute - **分** (**有効範囲** : 0-59)

初期設定

なし

コマンドモード

Time Range Configuration

コマンド解説

- **定期的にイベントが発生するタイムレンジを設定します。**

例

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

show time-range

設定されているタイムレンジを表示します。

文法

show time-range [name]

name - **タイムレンジ名** (**有効範囲** : 1-30 **文字**)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show time-range r&d
 time-range r&d:
   absolute start 01:01 01 April 2009
   periodic    Daily 01:01 to    Daily 02:01
   periodic    Daily 02:01 to    Daily 03:01

Console#
```

1.6 SNMP コマンド

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
General SNMP Commands			
snmp-server	SNMP サーバーを有効にします。	GC	P71
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を設定します。	GC	P83
snmp-server contact	システムコンタクト情報を設定します。	GC	P84
snmp-server location	システム設置情報を設定します。	GC	P84
show snmp	SNMP の設定情報を表示します。	NE,PE	P85
SNMP Target Host Commands			
snmp-server enable traps	デバイスによる SNMP トラップの送信を有効にします (例えば、SNMP 通知など)。	GC	P86
snmp-server host	SNMP 通知の受信先を指定します。	GC	P88
SNMPv3 Commands			
snmp-server engine-id	SNMP エンジン ID を設定します。	GC	P91
snmp-server group	SNMP グループの追加、SNMP エンジン ID を表示します。	PE	P92
snmp-server user	ユーザを SNMP グループに追加します。	PE	P94
snmp-server view	SNMP ビューを設定します	GC	P101
show snmp engine-id	SNMP エンジン ID を表示します。	PE	P97
show snmp group	SNMP グループを表示します。	PE	P98
show snmp user	SNMP ユーザを表示します。	GC	P100
show snmp view	SNMP ビューを表示します。	PE	P101
Notification Log Commands			
nlm	指定した notification log を有効にします。	GC	P102
snmp-server notify-filter	notification log を設定して、ターゲットホストを指定します。	GC	P103
show nlm oper-status	設定した notification logs のオペレーションステータスを表示します。	PE	P104
show snmp notify-filter	設定した notification logs を表示します。	PE	P103
ATC Trap Commands			
snmp-server enable port-traps atc broadcast-alarm-clea	帯域制御応答がトリガーとなった後、ブロードキャストトラフィックが下限の閾値より下回った場合にトラップを送信します。	IC (Port)	P292
snmp-server enable port-traps atc broadcast-alarm-fire	ブロードキャストのトラフィックが自動帯域制御の上限の閾値を上回った場合にトラップを送信します。	IC (Port)	P292
snmp-server enable port-traps atc broadcast-control-apply	ブロードキャストのトラフィックが自動帯域制御の上限の閾値を上回り、かつ有効期限が切れた場合にトラップを送信します。	IC (Port)	P293

snmp-server enable port-traps atc broadcast-control-release	帯域制御応答がトリガーとなり、リリースのタイマーが切れた後、ブロードキャストトラフィックが下位の閾値を下回った場合にトラップを送信します。	IC (Port)	P294
snmp-server enable port-traps atc multicast-alarm-clear	帯域制御応答がトリガーとなった後、マルチキャストトラフィックが下限の閾値より下回った場合にトラップを送信します。	IC (Port)	P295
snmp-server enable port-traps atc multicast-alarm-fire	マルチキャストトラフィックが自動帯域制御の上限の閾値より上回るとトラップを送信します。	IC (Port)	P296
snmp-server enable port-traps atc multicast-control-apply	マルチキャストトラフィックが自動帯域制御の上限の閾値を上回り、かつ有効期限が切れると、トラップを送信します。	IC (Port)	P297

snmp-server

すべてのマネジメントクライアントの SNMPv3 **エンジンおよびサービス** (versions 1, 2c, 3 **など）を有効にします。コマンドの前に** "no" **を置くことでサーバーを無効にします。**

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)
```

snmp-server community

コミュニティアクセスストリングを設定して、SNMP v1 あるいは v2c を用いて、クライアントによる管理アクセスの認証に使用するコマンドを設定します。コマンドの前に "no" を置くことで、指定したコミュニティストリングを削除します。

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 — **読み書き可能なアクセス。rw に指定された管理端末は MIB オブジェクトの取得及び変更が行えます。**

初期設定

- public — **読み取り専用アクセス** (ro)。MIB **オブジェクトの取得のみが行えます**
- private — **読み書き可能なアクセス** (rw)。**管理端末は** MIB **オブジェクトの取得及び変更が行えます**

コマンドモード

Global Configuration

例

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

snmp-server community

SNMP 使用時のコミュニティ名を設定します。コマンドの前に "no" を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。コマンドの前に "no" **を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 string

no snmp-server contact

- string — **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 Paul
Console(config)#
```

snmp-server location

システム設置場所情報の設定を行います。コマンドの前に "no" **を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)#
```

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

- コミュニティアクセス文字列情報、SNMP の入出力プロトコルデータ単位のカウンタ情報、SNMP ログ情報は "snmp-server enable traps" コマンドを使って有効かどうか表示されます。

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 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。

- 認証、link-up/link-down トラップはリンクアップ、リンクダウ

例

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

関連するコマンド

snmp-server host (P88)

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。コマンドの前に "no" を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。
- 認証、link-up/link-down トラップはレガシーメッセージであるため、snmp-server group コマンドにより割り当てられた Norify View 内の対応するエントリと共に有効にする必要があります。

例 :

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

関連コマンド

snmp-server host (P88)

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。コマンドの前に "no" を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 ー 再送を行う最大回数（0-255 回　初期設定：3 回）
  - timeout seconds ー 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 ー v3 使用時に設定（認証あり / 認証なし / 認証およびプライバシーあり）します。
  - port — トラップマネージャが使用する UDP ポートを指定（1-65535　初期設定：162）

初期設定

Host Address：なし　　SNMP バージョン：1

通知：トラップ　　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、信頼性は十分確保できません。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。

SNMPv2c ホストに情報を送信するには、以下の手順に従ってください。

（1）SNMP エージェントを「有効」にします。

（2）必要な通知メッセージを使って、「view」を設定します。

（3）必要な「notify view」を含むグループの設定 します。

（4）SNMP trap（例えば notifications）の送信を可能にします。

（5）snmp-server host コマンドを使って、ターゲットホストが inform メッセージを受信できるように指定します。

SNMPv3 ホストに情報を送信するには、以下の手順に従ってください。

（1）SNMP エージェントを「有効」にします。

（2）ローカルな SNMPv3 ユーザを設定して、メッセージ交換時に使用します。

（3）必要な通知メッセージを使って、「view」を設定します。

（4）必要な notify view を含むグループを設定します。SNMP trap（例えば notifications）の送信を可能にします 。

（5）NMP trap（例えば notifications）の送信を可能にします。

（6）snmp-server host コマンドを使って、ターゲットホストが inform メッセージを受信できるように指定します。

- 本機は、管理ステーションがサポートしている SNMP バージョンに応じて、SNMP Version 1, 2c /3 の通知を ホストの IP アドレスに送信することが可能です。snmp-server host コマンドに SNMP バージョンが指定されていない場合は、デフォルト設定では SNMP バージョン 1 の通知を送信します。
- SNMPv3 ホストを指定している場合、トラップマネージャのコミュニティ名は、SNMP ユーザー名として解釈されます。SNMPv3 認証または暗号化オプションを使用している際には（authNoPriv または authPriv）、最初に P326 「snmp-server user」でユーザー名を設定してください。ユーザー名が設定されていない場合、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 (P86)

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。コマンドの前に "no" を置くことでエンジン ID を初期設定値に戻します。

文法

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

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

- local — スイッチ上の SNMP エンジンを指定
- remote — リモートデバイス上の SNMP エンジンを指定
- ip address — リモートデバイスの IP アドレス
- engineid-string — エンジン ID（範囲：1-26　16 進数文字）

初期設定

固有のエンジン ID は、スイッチの MAC アドレスに応じて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 P89「snmp-server engine-id」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算出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。
- 固有にエンジン ID を固有に指定するには、後続の ”0” を入力する必要はありません。つまり “0123456789” の値は、“0123456789” の後続にローカルエンジン ID の ”0” を 16 個続けるのと同じです。
- ローカルエンジン ID はスイッチに対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)#
```

関連するコマンド

snmp-server host (P88)

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。コマンドの前に "no" を置くことでグループを削除します。

文法

snmp-server group groupname

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

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

no snmp-server group groupname

- groupname - SNMP グループ名 (有効範囲 : 1-32 文字)
- v1 | v2c | v3 - 使用する SNMP バージョンを選択します。
- auth | noauth | priv - このグループは、認証あり / 認証なし、あるいは認証かつプライバシをもつ SNMPv3 を使用します。
  - readview — Read アクセスのビューを設定します（1-32 文字）
  - writeview — write アクセスのビューを設定します（1-32 文字）
  - notify view — 通知ビューを設定します（1-32 文字）

初期設定

Default groups: public[1] (read only), private[2] (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設定します。
- 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。
- 認証、link-up/link-down メッセージはレガシートラップのため、snmp-server enable traps コマンドと共に有効にしなければなりません。
- 本機でサポートされている通知メッセージの詳細については、WEB の項に記載されている「通知メッセージ」の表を参照してください。認証、リンクアップ / ダウンメッセージはトラップのため、snmp-server enable traps コマンドを介して有効にしなければなりません。

1. view は設定されていません。
2. defaultview にマッピングを行います。

例

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

snmp-server user

SNMP ユーザーをグループへ追加します。コマンドの前に "no" を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
- 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

- ローカルユーザ (例えば、コマンドによりリモートエンジンの識別子は指定しない）は、SNMPv3 クライアントの管理アクセスを認証するため、またはローカルスイッチからの SNMPv3 トラップメッセージの送信元を識別するために設定する必要があります。
- リモートユーザ（例えば、コマンドによりリモートエンジンの識別子を指定）を指定して、ローカルスイッチから送信された SNMPv3 情報メッセージの送信元を識別するために設定する必要があります。
- SNMP のエンジン ID を使用して、パスワードから認証 / プライバシーのダイジェストを割り出すために使用するため、この設定コマンドを使用する前に、snmp-server engine-id コマンドをによりエンジン ID を設定する必要があります。
- 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算出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。

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)#
```

snmp-server view

このコマンドでは、ビューの追加を行います。コマンドの前に "no" を置くことでビューを削除します。

文法

snmp-server view view-name oid-tree {included | excluded}

no snmp-server view view-name

- 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（全ての MIB ツリーへのアクセスを含む）

コマンドモード

Global Configuration

コマンド解説

- 作成されたビューは、MIB ツリーの指定された範囲へのユーザアクセスを制限するために使用されます。
- デフォルトビューは全体の MIB ツリーへのアクセスを含みます。

例

MIB-2 を含む View を設定

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

MIB-2 インタフェーステーブル、ifDescr を含む View を設定。ワイルドカードは、このテーブル内のすべてのインデックス値を選択するのに使用されます。

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2
?included
Console(config)#
```

MIB-2 インタフェーステーブルを含む View を設定。マスクはすべてのインデックスエントリーを選択します。

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
?included
Console(config)#
```

show snmp engine-id

設定中の SNMP エンジン ID を表示します

文法

show snmp engine-id

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show snmp engine-id
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                        IP address
80000000030004e2b316c54321                  192.168.1.19
Console#
```

コマンド解説

コマンド	機能
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

関連するコマンド

snmp-server engine-ID (P91)

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

コマンドモード

Privileged Exec

コマンド解説

コマンド	機能
group name	SNMP グループ名
Security Model	SNMP のバージョン
Read View	関連のある read ビュー
Write View	関連のある write ビュー
Notify Vew	関連のある通知ビュー
Storage Type	このエントリーのストレージタイプ
Row Status	このエントリのビューの状態

例

```
Console#show snmp group
Group Name                  : public
Security Mode               : v1
Read View                   : defaultview
Write View                  : none
Notify View                 : none
Storage Type                : volatile
Row Status                  : active

Group Name                  : public
Security Model              : v2c
Read View                   : defaultview
Write View                  : none
Notify View                 : none
Storage Type                : volatile
Row Status                  : active

Group Name                  : private
Security Model              : v1
Read View                   : defaultview
Write View                  : defaultview
Notify View                 : none
Storage Type                : volatile
Row Status                  : active

Group Name                  : private
Security Model              : v2c
Read View                   : defaultview
Write View                  : defaultview
Notify View                 : none
Storage Type                : volatile
Row Status                  : active

Console#
```

show snmp user

SNMP ユーザー情報を表示します。

文法

show snmp user

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

コマンド	機能
EngineId	エンジン ID
User Name	ユーザー名
Authentication Protocol	認証プロトコル
Privacy Protocol	暗号化方式
storage-type	このエントリーのストレージタイプ
Row Status	ビューの状態
SNMP remote user	リモートデバイス上の SNMP エンジンに所属するユーザー

例

```
Console#show snmp user
EngineId: 0100000000000000000000000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

show snmp view

SNMP 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

コマンド	機能
View Name	ビュー名
Subtree OID	参照可能な MIB ツリーの OID
View Type	OID で表示される MIB ノードがビューに含まれてるか（included）、含まれていないか（excluded）
Storage Type	このエントリーのストレージタイプ
Row Status	ビューの状態

例

```
Console#show snmp view
View Name   : mib-2
Subtree OID : 1.2.2.3.6.2.1
View Type   : included
Storage Type: nonvolatile
Row Status  : active

View Name   : defaultview
Subtree OID : 1
View Type   : included
Storage Type: nonvolatile
Row Status  : active

Console#
```

nlm

指定の通知 log を有効 / 無効にします。

文法

[no] nlm filter-name

filter-name - **通知** log **名** (**有効範囲** : 1-32 **文字**)

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- **デフォルト設定では、**Notification logging **は有効ですが、**snmp-server notify-filter **コマンドにより指定されたログ用のプロファイルが** nlm **コマンドにより有効になるまで、情報の記録を開始しません。**logging **を無効にしても、**notification log **にストアされているエントリは削除されません。**

例

```
Console(config)#nlm A1
Console(config)#
```

snmp-server notify-filter

SNMP ユーザーをグループへ追加します。

文法

[no] snmp-server notify-filter profile-name remote ip-address

- profile-name - Notification log のプロファイル名 (有効範囲 : 1-32 文字)
- ip-address - リモートデバイスの内部アドレス。指定したターゲットホストは snmp-server host コマンドを使って設定されている必要があります。

[注意] notification log はローカルでストアされており、リモートデバイスには送信されません。

[注意] リモートホストパラメータは SNMP Notification MIB の必須フィールドを完了させる必要があります。

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- SNMP をサポートしているシステムには、lost notifications（再送回数の制限を超えるトラップ、または情報）に対する防御策として通知情報を記録する方式が必要となります。Notification Log MIB (NLM, RFC 3014) は、他の MIB からの情報を記録する構造を提供します。
- NLM によって提供されるサービスの場合は、Notification メッセージが紛失する可能性に対して個々の MIB はイベントに関連のある一時的な情報を記録する必要性は低くなります。アプリケーションは重要な通知が紛失していないかどうか検証するために、log を保存することが可能です。
- 本機が再起動時に notification logging が設定されていないにも関わらず有効な場合、SNMP トラップ (warm start など) の log を行うことはできません。
- 障害を避けるために、notification logging は snmp-server notify-filter コマンドおよび nlm コマンドを使って有効にしてください。これらのコマンドは startup configuration ファイルにストアされています。本機の起動時に SNMP トラップ（warm start など）の log を行うことはできません。
- コマンドを実行する際、通知 log を設定します（RFC 3014 で設定されているデフォルトのパラメータを使用)。デフォルト設定では、Notification logging は有効ですが、このコマンドで指定されている logging profile は nlm コマンドで有効になるまで情報の記録を開始しません。
- コマンドを実行すると、notification log （RFC 3014 で設定されているデフォルトのパラメータにより）が設定されます。Notification logging はデフォルト設定では有効です（nlm コマンドを参照）が、このコマンドで指定されている logging profile は nlm コマンドで有効になるまで情報の記録を開始しません。

- RFC 3014 のデフォルト設定に応じて、notification log にはエントリは「最大 256 個」まで収容可能で、エントリのエイジングタイムは「1440 分」です。notification log に記録されている情報およびエントリのエイジングタイムはネットワーク管理ステーションから SNMP を介してのみ設定可能です。
- トラップホストは snmp-server host コマンドを介して設定されます。デフォルト設定の notify filter については、show snmp notify-filter コマンドの例を参照してください。

例

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server notify-filter A1 remote 10.1.19.23
Console(config)
```

show nlm oper-status

設定されている notification logs のオペレーションスタータスが表示されます。

コマンドモード

Global Configuration

例

```
Console#show nlm oper-status
Filter Name: A1
Oper-Status: Operational
Console#
```

show nlm oper-status

設定されている notification logs のオペレーションのステータスが表示されます。

コマンドモード

Privileged Exec

例

```
Console#show nlm oper-status
Filter Name: A1
Oper-Status: Operational
Console#
```

show snmp notify-filter

設定されている notification logs **が表示されます。**

コマンドモード

Privileged Exec

例

```
Console#show snmp notify-filter
Filter profile name            IP address
----------------------------  ----------------
A1                             10.1.19.23
Console#
```

1.7 リモートモニタリング

リモートモニタリングにより、リモート機器はそれぞれ指定したイベント情報の収集、あるいは応答が可能です。RMON を備える SNMP エージェントは，設置された遠隔地の LAN セグメントのトラフィックやエラーなどのデータを収集して MIB データとして保存し，SNMP マネージャからのポーリングに応じて SNMP パケット化して転送します。管理情報を得た管理ステーションは、そのデータを表示してネットワークをリモートで監視することが可能です。

本機では、mini-RMON をサポートしており、統計情報、履歴、イベント、アラームに対応しております。RMON を有効にすると、物理インタフェースについての情報を構築し、これらの情報を関連の RMON データベースグループに保存します。管理エージェントは、SNMP プロトコルを介して本機と定期的に通信を行いますが、重要なイベントを検出すると、イベントに対応可能な管理エージェントに trap メッセージを自動的に送信します。

コマンド	機能	モード	ページ
rmon alarm	モニタリングを行う変数の閾値を設定します。	GC	P107
rmon event	アラームの応答イベントを設定します。	GC	P108
rmon collection history	統計情報を定期的にサンプリングします。	IC	P109
rmon collection rmon1	統計情報を収集を有効にします。	IC	P110
show rmon alarms	設定したアラームの設定値を表示します。	PE	P111
show rmon events	設定したイベントの設定値を表示します。	PE	P111
show rmon history	エントリごとのサンプリング値を表示します。	PE	P112
show rmon statistics	収集した統計情報を表示します。	PE	P112

rmon alarm

モニタリングした変数の閾値を設定します。コマンドの前に "no" を付けることによりアラームを削除します。

文法

rmon alarm index variable interval {absolute | delta}
rising-threshold threshold [event-index] falling-threshold threshold [event-index]
[owner name]

no rmon alarm index

- index – エントリのインデックス (有効な範囲 : 1-65535)
- variable – 参照したい MIB 変数のオブジェクト識別子。etherStatsEntry.n.n の変数のみを参照することが可能です。etherStatsEntry.n は MIB 変数を設定、etherStatsEntry.n.n は MIB 変数以外に etherStatsIndex を設定します。例えば、1.3.6.1.2.1.16.1.1.1.6.1 は etherStatsBroadcastPkts に加え、1 の etherStatsIndex を示します。
- interval – ポーリング間隔 (有効な範囲 : 1-31622400 秒)
- absolute – この変数がサンプリング期間の終了時の閾値と比較されます。
- delta – 最新の値から前回のサンプリング値が差し引かれ、そ の差分がしきい値と比較されます。
- threshold – サンプリングした変数のアラームの閾値 (有効な範囲 : 0-2147483647)
- event-index – アラームがトリガされた場合に使用するイベントのインデックス。イベントコントロールテーブルに対応するエントリのない場合は、イベントは生成されません (有効な範囲 : 1-65535)
- name – このエントリを設定した担当者名 (有効な範囲 : 1-127 文字)

初期設定

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.26

30 秒ごとにサンプリングを行います。

閾値の上限は ”event 0” に割り当てられ、「892800」です。

閾値の下限は ”event 0” に割り当てられ、「446400」です。

コマンドモード

Global Configuration

コマンド解説

インデックスのイベントが既に設定されている場合は、エントリは削除してから変更を行ってください。

- 最新の値が上限閾値以上であり 、前回のサンプリング値が上限閾値より も小さ かった場合にアラームが生成されます。上限閾値を超えたことを示すイベント が生成された場合、同様のイベントは、サンプリング値が上限閾値を下回ってから下限閾値に達した後に再び上限閾値に達するまで生成されません 。

- 最新の値が下限閾値以下で あ り 、前回の サンプリング値が下限閾値よりも大 きかった場合にアラームが生成されます。下限閾値を下回ったことを示すイ ベ ン トが生成 された場合、同様のイベントは、サンプリング値が下限閾値を上回ってから上限閾値に達 した後に再び下限閾値に達するまで生成されません。

例

```
Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta
rising-threshold 100 1 falling-threshold 30 1 owner mike
Console(config)#
```

rmon event

アラームの応答イベントを設定します。コマンドの前に "no" を付けることにより、イベントを削除します。

文法

rmon event index [log] | [trap community] | [description string] | [owner name]

no rmon event index

index – エントリのインデックス (有効な範囲 : 1-65535)

log – イベントがトリガーされた場合に RMON ログエントリが生成されます。ログメッセージは、イベントログの現在の設定情報に基づいて処理されます（「システムログの設定」を参照）。

trap – 指定されているトラップ マネージャにトラップメッセージが送信されます（「トラップマネージャの指定」を参照）。

community – パスワードと同じような役割を果たすコ ミュニティス トリングスであり、SNMPv1 ホストおよび SNMPv2c ホストに対するトラップ操作で送信されます。コミュニティストリングスは、この設定画面で設定できますが、事前に SNMP トラップ設定 画面で設定することを推奨します（「コミュニティアクセス文字列の設定」を参照）。

string – イベントについて説明してい文字列 (有効な範囲 : 1-127 文字)

name – このエントリの設定者 (有効な範囲 : 1-127 文字)

初期設定

None

コマンドモード

Global Configuration

コマンド解説

- インデックスのイベントが既に設定されている場合は、エントリは削除してから変更を行ってください。

- 指定したイベントは、アラームによりイベントのトリガーを引き起こした場合の処理方法を判別します。アラームへの応答には、アラームのログ、トラップマネージャへのメッセージの送信などが含まれます。

例

```
Console(config)#rmon event 2 log description urgent owner mike
Console(config)#
```

rmon collection history

物理インタフェース上の統計情報を定期的にサンプリングします。コマンドの前に "no" を付けることにより、定期的なサンプリングを無効にします。

文法

rmon collection history controlEntry index
[[owner name] [buckets number] [interval seconds]] |
[buckets number] [interval seconds] | interval seconds

no rmon collection history controlEntry index

- index – エントリのインデックス (有効な範囲 : 1-65535)
- number – このエントリに対して要求するバケット数 (有効な範囲 : 1-65536)
- seconds – ポーリング間隔 (有効な範囲 : 1-3600 秒)
- name – このエントリを設定した担当者名 (有効な範囲 : 1-127 文字)

初期設定

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.26

Buckets: 8

Interval: 偶数のエントリ番号の場合は 30 秒
奇数のエントリの番号の場合は 1800 秒

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- デフォルト設定では、インデックス番号が本機のポートに対応していますが、現在使用していない番号に変更可能です。
- 定期的なサンプリングが既に有効な場合は、エントリを削除してからコマンドにより変更を行ってください。
- 各サンプリングの収集情報は、以下のとおりです。
  - 入力オクテット、ブロードキャストパケット、小さいサイズのパケット、大きいサイズのパケット、フラグメント、JAVA、CRC アライメントエラー、コリジョン、ドロップイベント、およびネットワークユーティライゼーション

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection history 21 buckets 24 interval 60
owner mike
Console(config-if)#
```

rmon collection rmon1

物理インタフェース上の統計情報の収集を有効にします。コマンドの前に "no" **を付けることにより統計情報の収集を無効にします。**

文法

rmon collection rmon1 controlEntry index [owner name]

no rmon collection rmon1 controlEntry index

- index – **エントリのインデックス** (**有効な範囲** : 1-65535)
- name – **このエントリの設定した担当者名** (**有効な範囲** : 1-127 **文字**)

初期設定

Enabled

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **デフォルト設定では、インデックス番号が本機のポートに対応していますが、現在使用していない番号に変更可能です。**
- **定期的なサンプリングが既に有効な場合は、エントリを削除してからコマンドにより変更を行ってください。**
- **各サンプリングの収集情報は、以下のとおりです。**
  - **入力オクテット、ブロードキャストパケット、小さいサイズのパケット、大きいサイズのパケット、フラグメント、**JAVA、CRC **アライメントエラー、コリジョン、ドロップイベント、およびネットワークユーティライゼーション**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection rmon1 controlEntry 1 owner mike
Console(config-if)#
```

show rmon alarms

設定されているアラームすべての設定値を表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon alarms
Alarm 1 is valid, owned by
  Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds
  Taking delta samples, last value was 0
  Rising threshold is 892800, assigned to event 0
  Falling threshold is 446400, assigned to event 0
```

show rmon events

設定したイベントすべての設定情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon events
Event 2 is valid, owned by mike
Description is urgent
Event firing causes log and trap to community , last fired
00:00:00
Console#
```

show rmon history

履歴グループのエントリごとにサンプリング値を表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon history
Entry 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.2.1.1.1 every 1800 seconds
Requested # of time intervals, ie buckets, is 8
Granted # of time intervals, ie buckets, is 8
 Sample # 1 began measuring at 00:00:01
 Received 77671 octets, 1077 packets,
 61 broadcast and 978 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers packets,
 0 CRC alignment errors and 0 collisions.
 # of dropped packet events is 0
 Network utilization is estimated at 0
```

show rmon statistics

統計情報のグループのエントリごとに収集情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show rmon statistics
Interface 1 is valid, and owned by
 Monitors 1.3.6.1.2.1.2.2.1.1.1 which has
 Received 164289 octets, 2372 packets,
 120 broadcast and 2211 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 # of dropped packet events (due to lack of resources): 0
 # of packets received of length (in octets):
  64: 2245, 65-127: 87, 128-255: 31,
  256-511: 5, 512-1023: 2, 1024-1518: 2
```

.

.

.

1.8 フローサンプリング

本製品に組み込まれているフローサンプリング（sFlow）機能は、リモート sFlow Collector と共に、ネットワーク上に存在するトラフィックのタイプとレベルに関する正確かつ詳細なリアルタイムの情報を管理者に提供します。スイッチを経由するすべてのデータの n 個のパケットから抽出される sFlow Agent サンプル 1 では、サンプルが sFlow ダイアグラムとして再カプセル化されて sFlow Collector に送信されます。従来のプローブではトラフィックが監視対象のインタフェースでサンプリングされるのでトラフィックの状況は部分的にしか確認されませんが、このサンプリングは、すべてのトラフィックが確認される内部ハードウェアレベルで実行されます。それだけでなく、ローカル分析が実行されないので、sFlow エージェントによって課せられるプロセッサとメモリの負荷は最小限に抑えられます。そのため、高いトラフィックレベルでもスイッチのワイヤ速度の伝送特性が維持されます。

コマンド	機能	モード	ページ
sflow destination	コレクタによって使用される IP アドレスおよび UDP ポートを設定します。	IC	P113
sflow max-datagram-size	sFlow データのペイロードのサイズの上限を設定します。	IC	P114
sflow max-header-size	sFlow データのヘッダのサイズの上限を設定します。	IC	P114
sflow owner	受信先の名前を設定します。	IC	P115
sflow sample	パケットのサンプルレートを設定します。	IC	P116
sflow source	モニタリングしたい送信元のポートの sFlow を有効にします。	IC	P117
sflow timeout	sFlow ポートのパラメータをすべてリセットする前に、コレクタへサンプルを継続して送信する時間を設定します。	IC	P117
show sflow	sFlow プロセスのグローバルおよびインタフェース設定値を表示します。	PE	P118

sflow destination

コレクタにより使用される IP アドレスおよび UDP ポートを設定します。コマンドの前に "no" を付けることによりデフォルトの設定に戻ります。

構文

sflow destination {ipv4 ipv4-address | ipv6 ipv6-address} [destination-udp-port]

no sflow destination

- ipv4-address - sFlow コレクタの IPv4 アドレス。有効な IPv4 アドレスは、4 桁の 10 進数の形式 (0 - 255) で構成されます。
- ipv6-address - sFlow コレクタの IPv6 アドレス。IPv6 アドレスは、ネットワークのプレフィックスおよびホストアドレスのビット数が含まれます。IPv6 アドレスは 8 コロンで区切られた 16 ビットの 16 進値で構成されます。ダブルコロンを使用すると、設定されていないフィールドの記入に必要な「0」の数を示します。
- destination-udp-port - コレクタが sFlow ストリームをリスニングする先の UDP ポート (有効な範囲 : 0-65534)

初期設定

IP Address : 未設定
UDP Port　: 6343

コマンドモード

Interface Configuration (Ethernet)

例

ここでは、コレクタの IP アドレスを設定し、デフォルトの UDP ポートを使用します。

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow destination ipv4 192.168.0.4
Console(config-if)#
```

sflow max-datagram-size

sFlow データのペイロードのサイズの上限を設定します。コマンドの前に "no" を付けることによりデフォルトの設定に戻ります。

文法

sflow max-datagram-size max-datagram-size

no max-datagram-size

- max-datagram-size - sFlow データのペイロードのサイズの上限 (有効な範囲 : 200-1500 バイト)

初期設定

1400 bytes

コマンドモード

Interface Configuration (Ethernet)

例 :

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-datagram-size 1500
Console(config-if)#
```

sflow max-header-size

sFlow データのヘッダのサイズの上限を設定します。コマンドの前に "no" を付けることによりデフォルトの設定に戻ります。

構文

sflow max-header-size max-header-size

no max-header-size

max-header-size - sFlow データのヘッダのサイズの上限 (有効な範囲 : 64-256 bytes)

初期設定

128 bytes

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-header-size 256
Console(config-if)#
```

sflow owner

受信先の名前を設定します (例えば、sFlow コレクタ)。コマンドの前に "no" を付けることにより、この名前を削除します。

文法

sflow owner name

no sflow owner

- name - 受信者名 (有効な範囲 : 1-256 文字)

初期設定

None

コマンドモード

Interface Configuration (Ethernet)

例

ここでは、オーナの名前を ”Lamar” に設定します。

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow owner Lamer
Console(config-if)#
```

sflow sample

パケットのサンプルレートを設定します。コマンドの前に "no" **を付けることによりデフォルト設定に戻ります。**

文法

sflow sample rate

no sflow sample

- rate - **パケットのサンプルレート、または１つのサンプリングごとに要するパケット数** (**有効な範囲** : 256-16777215 packets)

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

サンプリングレートを 100 **パケットごとに** 1 **つずつ設定します。**

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow sample 100
Console(config-if)#
```

sflow source

モニタリングしたい送信元のポートの sFlow を有効にします。コマンドの前に "no" を付けることにより指定したポートの sFlow を無効にします。

文法

[no] sflow source

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

ここでは、ポート 9 のフローコントロールを有効にします。

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow source
Console(config-if)#
```

sflow timeout

sFlow ポートのパラメータをすべてリセットする前に、コレクタへサンプルを継続して送信する時間を設定します。コマンドの前に "no" を付けることによりデフォルト設定に戻ります。

文法

sflow timeout seconds

no sflow timeout

- seconds -sFlow ポートのパラメータをすべてリセットする前に、sFlow 処理によりコレクタへサンプルを継続して送信する時間を設定します (有効な範囲 : 0-999999999 秒、この場合の「0」は、タイムアウトなしを意味します。)

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- このコマンドで設定した sFlow パラメータには、サンプリング期間、受信者名、アドレス、UDP ポート、タイムアウト、最大ヘッダサイズ、最大データサイズが含まれます。

例

ここでは、タイムアウトを「1000 秒」に設定します。

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow timeout 10000
Console(config-if)#
```

show sflow

sFlow **プロセスのグローバル設定およびインタフェースごとの設定を表示します。**

文法

show sflow interface [interface]

interface

ethernet unit/port

- unit - **スタックユニット** (**有効な範囲** : 1-8)
- port - **ポート番号** (**有効な範囲** : 1-26)

コマンドモード

Privileged Exec

例

```
Console#show sflow interface ethernet 1/9
 Interface of Ethernet  1/9  :
   Interface status          : Enabled
   Owner name                : Lamar
   Owner destination         : 192.168.0.4
   Owner socket port         : 6343
   Time out                  : 9994
   Maximum header size       : 256
   Maximum datagram size     : 1500
   Sample rate               : 1/256

Console#
```

1.9 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
User Accounts	ユーザー名とパスワードの設定	P119
Authentication Sequence	ログイン認証方式と優先順位の設定	P122
RADIUS Client	RADIUS サーバ認証の設定	P124
TACACS+ Client	TACACS+ サーバ認証の設定	P129
Web Server setting	Web ブラウザからの管理アクセスを有効化	P143
Telnet Server setting	Telnet サーバからの管理アクセスを有効化	P147
Secure Shell Settings	Telnet 接続に SSH を設定	P148
Port Security	ポートへのセキュアアドレスの設定	P160
Port Authentication	EEE802.1X によるポート認証の設定	P162
Management IP Filter	管理アクセスを許可される IP アドレスを設定	P172

1.9.1 ユーザーアカウント

管理アクセスのための基本的なコマンドです。管理アクセスに関するその他の設定に関しては、P46「password」や P122「認証コマンド」、P162 「IEEE802.1X 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	P120
enable password	各アクセスレベルのパスワードの設定	GC	P121

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。コマンドの前に "no" を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 admin	0 15	guest 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。コマンドの前に "no" を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。
  （Level0-14 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。P248 「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 (P14)

authentication enabled (P123)

1.9.2 認証コマンド

本機のシステムへの管理アクセスに対するユーザ認証には、3 つの認証方法から指定することが可能です。

この項では、コマンドの認証方法とシーケンスを設定する方法について解説します。

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	P122
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	P123

authentication login

ログイン認証方法及び優先順位を設定します。コマンドの前に "no" を置くことにより、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

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 (P120)

authentication enable

enable コマンド（P14）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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

authentication enable {[local] [radius] [tacacs]}

no authentication enable

- local — ローカル認証を使用します
- radius — RADIUS サーバ認証を使用します
- tacacs — TACACS+ サーバ認証を使用します

初期設定

Local

コマンドモード

Global Configuration

コマンド解説

- RADIUS では UDP、TACACS+ では TCP を使用します。UDP はベストエフォート型の接続ですが、TCP は接続確立型の接続となります。また、RADIUS 暗号化はクライアントからサーバへのアクセス要求パケットのパスワードのみが暗号化されます。
- RADIUS 及び TACACS+ ログイン認証は各ユーザ名とパスワードに対しアクセスレベルを設定することができます。ユーザ名とパスワード、アクセスレベルは認証サーバ側で設定することができます。
- 3 つの認証方式を 1 つのコマンドで設定することができます。例えば、"authentication enable radius tacacs local" とした場合、ユーザ名とパスワードを RADIUS サーバに対し最初に確認します。RADIUS サーバが利用できない場合、TACACS+ サーバにアクセスします。TACACS+ サーバが利用できない場合はローカルのユーザ名とパスワードを利用します。

例

```
Console(config)#authentication enable radius
Console(config)#
```

関連するコマンド

enable password (P121) — コマンドモード変更のためのパスワードの設定

1.9.3 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	P124
radius-server port	RADIUS サーバのポートの設定	GC	P125
radius-server key	RADIUS 暗号キーの設定	GC	P126
radius-server retransmit	リトライ回数の設定	GC	P127
radius-server timeout	認証リクエストの間隔の設定	GC	P127
show radius-server	RADIUS 関連設定情報の表示	PE	P128

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

[no] radius-server index host host_ip_address [auth-port auth_port] [timeout timeout] [retransmit retransmit] [key key] [timeout timeout] [retransmit retransmit]

- index — サーバを 5 つまで設定できます。指定したサーバの順に、サーバが応答するかタイムアウトがくるまでリクエストを送信します。
- host_ip_address — RADIUS サーバの IP アドレス
- auth_port — RADIUS サーバの認証用 UDP ポート番号（範囲：1-65535）
- key — クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入れられません（最大 48 文字）
- 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）
- 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）

初期設定

- auth-port：1812
- timeout：5 秒
- retransmit：2 回

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

radius-server [acct-port] [auth-port] port_number

no radius-server [acct-port] [auth-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 acct-port 181
Console(config)#
```

radius-server key

RADIUS 暗号キーを設定します。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

radius-server key key_string

no radius-server key

- key_string — クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入れられません（最大 48 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

リトライ回数を設定します。コマンドの前に "no" を置くことにより、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 回

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。コマンドの前に "no" を置くことにより、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 秒

コマンドモード

Global Configuration

例

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

現在の RADIUS **サーバ関連の設定を表示します。**

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show radius-server
Remote RADIUS Server Configuration:
Global Settings:
Authentication Port Number  : 1812
Accounting Port Number      : 1813
Retransmit Times            : 2
Request Timeout             : 5

Server 1:
Server IP Address   : 192.168.1.1
Auth-port           : 1812
Acct-port           : 1813
Retransmit Times    : 2
Request Timeout     : 5
RADIUS Server Group:
Group Name                Member Index
------------------------- -------------
radius                    1

Console#
```

1.9.4 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	P129
tacacs-server port	TACACS+ サーバのポートの設定	GC	P130
tacacs-server key	TACACS+ 暗号キーの設定	GC	P130
show tacacs-server	TACACS+ 関連設定情報の表示	GC	P131

tacacs-server host

TACACS+ サーバの設定を行います。コマンドの前に "no" を置くことにより、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。コマンドの前に "no" を置くことにより、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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

tacacs-server key key_string

no tacacs-server key

- key_string — クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入れられません（最大 48 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

現在の TACACS+ **サーバ関連の設定を表示します。**

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show tacacs-server
Remote TACACS+ Server Configuration:
Global Settings:
Server Port Number : 49
Retransmit Times   : 2
Timeout            : 5
Server 1:
Server IP Address  : 10.11.12.13
Server Port Number : 49
Retransmit Times   : 2
Timeout            : 4
TACACS Server Group:
Group Name                  Member Index
------------------------- -------------
tacacs+                     1
Console#
```

1.9.5 AAA

AAA 機能では、ネットワーク内の設定済みの RADIUS サーバまたは TACACS+ サーバを使用する必要があります。それらのセキュリティサーバは、一連のグループとして設定して、所定のサービスに対するユーザアクセスを制御するための手段として適用することができます。

コマンド	機能	モード	ページ
aaa accounting dot1x	802.1X サービスのアカウントを有効にします。	GC	P133
aaa accounting exec	Exec サービスのアカウントを有効にします。	GC	P134
aaa accounting update	アカウントサーバへの送信元の定期的なアップデートを行います	GC	P135
aaa authorization exec	Exec セッションの認証を有効にします。	GC	P134
aaa group server	設定されたリストのセキュリティサーバをグループ化します。	GC	P137
server	グループリスト内のサーバの IP アドレスを設定します。	SG	P138
accounting dot1x	802.1X サービスリクエストのインタフェースにアカウント方式を適用します。	IC	P139
accounting exec	ローカルコンソール、Telnet、SSH 接続にアカウント方式を適用します。	Line	P140
authorization exec	ローカルコンソール、Telnet、SSH 接続に認証方式を適用します。	Line	P141
show accounting	アカウント情報をすべて表示します。	PE	P142

aaa accounting dot1x

ネットワークアクセスに対してリクエストした IEEE802.1X サービスを有効にします。

"no" を付けると、アカウントサービスは無効になります。

文法

aaa accounting dot1x {default | method-name}
start-stop group {radius | tacacs+ |server-group}

no aaa accounting dot1x {default | method-name}

- default - サービスリクエストのデフォルトのアカウント方式を指定します。
- method-name - サービスリクエストのアカウント方式を指定します (有効な範囲 : 1-255 文字)。
- start-stop - 開始ポイントおよび終了ポイントからのアカウントを記録します。
- group - 使用するサーバグループを指定します。
- radius - radius-server host コマンドで設定する RADIUS ホストをすべて指定します。
- tacacs+ - コマンドで設定する TACACS+ ホストをすべて指定します。
- server-group - aaa group server コマンドで設定するサーバグループ名を指定します (有効な範囲 : 1-255 文字)

初期設定

アカウントは有効ではありません。
サーバが指定されていません。

コマンドモード

Global Configuration

コマンド解説

- default および method-name フィールドは、指定した TACACS+ サーバ上で設定したアカウント方式を記述するためのみに使用し、実際には使用する方式についての情報はサーバに送信しません。

例

```
Console(config)#aaa accounting dot1x default start-stop group
radius
Console(config)#
```

aaa accounting exec

ネットワークアクセスに対してリクエストした Exec **サービスのアカウントを有効にします。**"no" **を付けると、アカウントサービスは無効になります。**

文法

aaa accounting exec {default | method-name}
start-stop group {radius | tacacs+ |server-group}

no aaa accounting exec {default | method-name}

- default - **サービスリクエストのデフォルトのアカウント方式を指定します。**
- method-name - **サービスリクエストのアカウント方式を指定します** (**有効な範囲** : 1-255 **文字**)。
- start-stop - **開始ポイントおよび終了ポイントからのアカウントを記録します。**
- group - **使用するサーバグループを指定します。**
- radius - radius-server host **コマンドで設定する** RADIUS **ホストをすべて指定します。**
- tacacs+ - tacacs-server host **コマンドで設定する** TACACS+ **ホストをすべて指定します。**
- server-group - aaa group server **コマンドで設定するサーバグループ名を指定します** (**有効な範囲** : 1-255 **文字**)

初期設定

アカウントは有効ではありません。
サーバが指定されていません。

コマンドモード

Global Configuration

コマンド解説

- **ローカルコンソールおよび** Telnet **接続用の** Exec **サービスリクエストのアカウントを実行します。**
- default **および** method-name **フィールドは、指定した** TACACS+ **サーバ上で設定したアカウント方式を記述するためのみに使用し、実際には使用する方式についての情報はサーバに送信しません。**

例

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

aaa accounting update

アカウンティングサーバに定期的にアップデート情報を送信します。

"no" **を付けると、アカウントのアップデートは無効になります。**

文法

aaa accounting update [periodic interval]

no aaa accounting update

- interval - **サーバにアカウントデータを送信する時間** (**有効な範囲** : 1-2147483647 **分**)

初期設定

1 **分**

コマンドモード

Global Configuration

コマンド解説

- **アカウンティングのアップデートを有効にすると、システム上のユーザに対して定期的にアカウントデータが発行されます。**
- **アップデート可能な時間を指定せずに、このコマンドを使った場合は無効になります。**

例

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

aaa authorization exec

Exec アクセス用の認証が有効になります。コマンドの前に "no" を付けることにより認証サービスは無効になります。

文法

aaa authorization exec {default | method-name}
group {tacacs+ | server-group}

no aaa authorization exec {default | method-name}

- default - Exec アクセス用のデフォルトの認証方法を指定します。
- method-name - Exec アクセス用の認証方法を指定します。(有効な範囲 : 1-255 文字)
- group - 使用するサーバグループを指定します。
- tacacs+ - tacacs-server host コマンドで設定した TACACS+ ホストをすべて指定します。
  server-group - aaa group server コマンドで設定したサーバグループの名前を指定します (有効な範囲 : 1-255 文字)。

初期設定

認証は無効です。
サーバは指定されていません。

コマンドモード

Global Configuration

コマンド解説

- ユーザが Exec shell を実行可能かどうかを認証します。認証が有効になる前に AAA 認証を行う必要があります。
- 方法を指定せずにコマンドを実行すると、特に明示されている場合を除き、デフォルトのメゾットリストがインタフェース、あるいはライン（この認証タイプが適用されたもの）に適用されます。

例

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

aaa group server

セキュリティサーバホストのグループを指定します。リストからサーバグループを削除するには、コマンドの前に ”no” **を付けてください。**

文法

[no] aaa group server {radius | tacacs+} group-name

- radius - RADIUS **サーバグループを設定します。**
- tacacs+ - TACACS+ **サーバグループを設定します。**
- group-name - **セキュリティサーバグループを指定する文字列** (**有効な範囲** : 1-7 **文字**)**。**

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

server

セキュリティサーバを AAA **サーバグループに追加します。**"no" **を付けると、グループから関連のあるサーバを削除します。**

文法

[no] server {index | ip-address}

- index - **サーバのインデックスを指定します。**
  (**有効な範囲** : RADIUS 1-5, TACACS+ 1)
- ip-address - **サーバのホスト** IP **アドレスを指定します。**

初期設定

なし

コマンドモード

Server Group Configuration

コマンド解説

- RADIUS **サーバのインデックスを指定する場合は、サーバのインデックスは** radius-server host **コマンドによって設定しておく必要があります。**
- TACACS+ **サーバのインデックスを指定する場合は、サーバのインデックスは** tacacs-server host **コマンドによって設定しておく必要があります。**

例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

accounting dot1x

インタフェース上の IEEE802.1X **サービスリクエストのアカウント方法を適用します。**"no" **を付けると、インタフェース上のアカウントを無効にします。**

文法

accounting dot1x {default | list-name}

no accounting dot1x

- default - aaa accounting dot1x **コマンドで設定したデフォルトのメゾットリストを指定します。**
- list-name - aaa accounting dot1x **コマンドで設定したメゾットリストを指定します。**

初期設定

なし

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

accounting exec

ローカルコンソール、Telnet **、**SSH **接続にアカウントメゾットを適用します。**"no" **を付けることで、ライン上のアカウントを無効にします。**

文法

accounting exec {default | list-name}

no accounting exec

- default - aaa accounting exec **コマンドで設定したデフォルトのメソッドリストを指定します。**
- list-name - aaa accounting exec **コマンドで設定したメゾットリストを指定します。**

初期設定

なし

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line-console)#authorization exec tps
Console(config-line-console)#
```

authorization exec

ローカルコンソール、Telnet**、あるいは** SSH **接続に認証方式を適用します。**"no" **を付けると、ライン上の認証を無効にします。**

文法

authorization exec {default | list-name}

no authorization exec

- default - aaa authorization exec **コマンドで設定したデフォルトのメゾットリストを指定します。**
- list-name - aaa authorization exec **コマンドで設定したメゾットリストを指定します。**

初期設定

なし

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
```

show accounting

機能およびポートごとに現行のアカウント設定値を表示します。

文法

show accounting [[dot1x [statistics [username user-name | interface interface]] | exec [statistics] | statistics]

- dot1x - dot1x **アカウント情報を表示します。**
- exec - Exec **アカウント情報を表示します。**
- statistics - **アカウント情報を表示します。**
- user-name - **指定可能なユーザ名のアカウント情報を表示します。**
- interface ethernet unit/port
  - unit - **スタックユニット** (**有効な範囲** : 1-8)
  - port - **ポート番号** (**有効な範囲** : 1-26)

初期設定

None

コマンドモード

Privileged Exec

例

```
Console#show accounting
Accounting Type     : dot1x
  Method List       : default
  Group List        : radius
  Interface         : Eth 1/1

  Method List       : tps
  Group List        : radius
  Interface         : Eth 1/2

Accounting Type  : EXEC
  Method List       : default
  Group List        : tacacs+
  Interface         : vty

Console#
```

1.9.6 Web サーバーコマンド

コマンド	機能	モード	ページ
ip http port	WEB インタフェースに使用するポートの設定	GC	P143
ip http server	管理用 WEB インタフェースの使用	GC	P144
ip http secure-server	セキュア HTTP（HTTPS）サーバの使用	GC	P145
ip http secure-port	HTTPS 接続に使用するポートの設定	GC	P146

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。コマンドの前に "no" を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（P144）
show system（P28）

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。コマンドの前に "no" を置くことで本機能は無効となります。

文法

ip http server

no ip http server

初期設定

有効

コマンドモード

Global Configuration

例

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

関連するコマンド

ip http port（P143）
show system（P28）

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、SSL(Secure Socket Layer) を使用したセキュアな HTTPS(Hypertext Transfer Protocol Secure) を使用するためのコマンドです。コマンドの前に "no" を置くことで本機能を無効にします。

文法

ip http secure-server

no ip http secure-server

初期設定

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、サーバを確証します。
  - クライアントおよびサーバは、接続のために使用する 1 セットのセキュリティ・プ ロトコルを協定します。
  - クライアントおよびサーバは、データを暗号化し解読するためのセッション・キーを生成します。
- クライアントとサーバ間の暗号化されたアクセスが確立した場合、Internet Explorer 5.x 以上または Netscape Navigator 6.2 以上または Mozilla Firefox 2.0.0.0 以上の、WEB ブラウザのステータスバーに鍵マークが表示されます。

セキュアサイト証明の詳細は WEB のマニュアルに記載されている「デフォルトのセキュアサイト証明書の置き換え」の項を参照して下さい。

例

```
Console(config)#ip http secure-server
Console(config)#
```

関連するコマンド

ip http secure-port（P146）
copy tftp https-certificate（P36）

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。コマンドの前に "no" を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 接続に使用する 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（P145）
show system（P28）

1.9.7 Telnet サーバーコマンド

コマンド	機能	モード	ページ
ip telnet server	管理用 Telnet インタフェースの使用	GC	P147

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。コマンドの前に "no" を置くことで本機能は無効となります。

文法

ip telnet server [port port-number]
no ip telnet server [port port-number]

- Port — Telnet インタフェースに使用される TCP ポート
- port_number — Telnet インタフェースに使用される TCP ポート番号
  （範囲：1-65535）

初期設定

サーバー：有効
サーバーポート：23

コマンドモード

Global Configuration

例

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

1.9.8 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	P151
ip ssh timeout	SSH サーバの認証タイムアウト設定	GC	P153
ip ssh authentication -retries	クライアントに許可するリトライ回数の設定	GC	P153
ip ssh server-key size	SSH サーバキーサイズの設定	GC	P153
copy tftp public-key	ユーザの公開キーを TFTP サーバから本機へコピー	PE	P36
delete public-key	特定ユーザの公開キーの削除	PE	P154
ip ssh crypto host-key generate	ホストキーの生成	PE	P155
ip ssh crypto zeroize	RAM からのホストキーの削除	PE	P156
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	P157
disconnect	ライン接続の終了	PE	P54
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表示	PE	P157
show ssh	SSH セッション状態の表示	PE	P158
show public-key	特定のユーザ又はホストの公開キーの表示	PE	P159
show users	SSH ユーザ、アクセスレベル、公開キータイプの表示	PE	P30

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
15684995401867669259333946775054617325313674890836547254150202455931998685443583616519999233297817660658309561082591321289023376546801726272571413428762941301196195566782595664104869574278881462065194174677298486546861571773939016477935594230357741309802273708779454524083971752646358058176716709574804776117

（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
134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 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 サービスの有効化 — "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）認証 — 以下の認証方法の内 1 つが使用されます。

- パスワード認証（SSH1.5 または V2 クライアント）

  a. クライアントが自身のパスワードをサーバへ送ります。

  b. 本機はクライアントのパスワードと、メモリに保管されているパスワードを比較します。

  c. 一致した場合、接続が許可されます。

[注意]　パスワード認証と共に SSH を使用する場合にも、ホスト公開キーは初期接続時又は手動によりクライアントのホストファイルに与えられます。クライアントキーの設定を行なう必要はありません。

- パブリックキー認証－ SSH クライアントが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。このプロセスの間に、以下の交換が行われます。

  SSH1.5 クライアントの認証

  a. クライアントが自身の RSA パブリックキーをサーバへ送ります。

b. スイッチはクライアントのパブリックキーと、メモリに保管されているパブリックキーを比較します。

c. 一致した場合、スイッチは Challenge としてランダム 256 ビット文字列を生成するために、そのシークレットキーを使用し、この文字列をユーザーのパブリックキーと共に暗号化します。その後、これをクライアントに送信します。

d. クライアントはそのプライベートキーを、Challenge 文字列を解読するために使用し、MD5 チェックサムを計算した後スイッチへ送り返します。

SSH v2 クライアントの認証

a. DSA パブリックキー認証が受容できるか否かを決定するために、クライアントは最初にスイッチへ問い合わせを行います。

b. 指定したアルゴリズムがスイッチでサポートされる場合、認証プロセスを続けるようクライアントへ知らせます。さもなければリクエストは拒絶されます。

c. クライアントはプライベートキーを使用し生成された署名をスイッチへ送信します。

d. サーバがメッセージを受信した際、それは供給されたキーが認証のために受容できるか否かを調べ、もしそうであるならば今度は署名が正しいか否かを調べます。両方のチェックが成功した場合、クライアントは認証されます。

[注意] SSH サーバは最大 4 つのクライアントセッションをサポートします。クライアントセッションの最大数は、点在と Telnet セッションと SSH セッションの両方を含みます。

ip ssh server

SSH サーバの使用を有効にします。コマンドの前に "no" を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 (P155)

show ssh (P158)

ip ssh timeout

SSH サーバのタイムアウト時間を設定します。コマンドの前に "no" を置くことで初期設定に戻ります。

文法

ip ssh timeout seconds

no ip ssh timeout

- seconds — SSH 接続調整時のクライアント応答のタイムアウト時間（設定範囲：1-120）

初期設定

10 秒

コマンドモード

Global Configuration

コマンド解説

- タイムアウトは SSH 情報交換時のクライアントからの応答を本機が待つ時間の指定を行ないます。SSH セッションが確立した後のユーザ入力のタイムアウトは vty セッションへの "exec-timeout" コマンドを使用します。

例

```
Console(config)#ip ssh timeout 60
Console(config)#
```

関連するコマンド

exec-timeout (P48)

show ip ssh (P157)

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。コマンドの前に "no" を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 回

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 (P157)

ip ssh server-key size

SSH サーバキーサイズを設定します。コマンドの前に "no" を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**

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**

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 （P156）
ip ssh save host-key （P157）

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**

コマンドモード

Privileged Exec

コマンド解説

- RAM **からホストキーを削除します。**" no ip ssh save host-key" **コマンドを使用することでフラッシュメモリからホストキーを削除できます。**
- **本コマンドを使用する際は事前に** SSH **サーバを無効にして下さい。**

例

```
Console#ip ssh crypto zeroize dsa
Console#
```

関連するコマンド

ip ssh crypto host-key generate（P155）
ip ssh save host-key（P157）

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**

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 (P155)

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 2.0
Negotiation Timeout : 120 seconds; 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
15684995401867669259333946775054617325313674890836547254150202455931 9
986854435836165199992332978176606583095861082591321289023376546801726
272571413428762941301196195566782595664104869574278881462065194174677
298486546861571773939016477935594230357741309802273708779454524083971
752646358058176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/
Dg0h2HxcYV44sXZ2JXhamLK6P8bvuiyacWbUW/
a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfvJlPdOkFgzLGMinvSNYQwiQXbKT
BH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEAsy
5YWDC99ebYHNRj5kh47wY4i8cZvH+/
p9cnrfwFTMU01VFDly3IR2G395NLy5Qd7ZDxfA9mCOfT/
yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/
Kjw6BmiFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/
ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOyDbsloBfPuSAb4oAsyjKXKVYNLQkTLZ
fcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2 o/
dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475
S7 w0W

Console#
```

1.9.9 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	P160
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	P300
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	P302

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コマンドの前に "no" を置くことでポートセキュリティを無効にします。キーワードと共にコマンドの前に "no" を置くことでポートセキュリティの動作及び最大 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の動作
  - shutdown — ポートを無効
  - trap — SNMP トラップメッセージの発行
  - trap-and-shutdown — SNMP トラップメッセージを発行しポートを無効
- max-mac-count
  - address-count — ポートにおいて学習する MAC アドレスの最大値（範囲：0-1024　0 は無効です）

初期設定

- Status：無効 (Disabled)
- Action：なし
- max-mac-count：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-address-table static" コマンドを使用して、追加したい MAC アドレスを指定します。
- セキュアポートには以下の制限があります：
  - ネットワークを相互接続するデバイスには接続できません。
  - トランクグループに加えることはできません。
- ポートセキュリティが機能しポートを無効にした場合、"no shutdown" コマンドを使用し、手動で再度有効にする必要があります。

例

本例では、5 番ポートにポートセキュリティとポートセキュリティ動作を設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

関連するコマンド

shutdown（P254）
mac-address-table static（P300）

1.9.10 IEEE802.1X 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	P162
dot1x default	dot1x の設定値をすべて初期設定に戻します。	GC	P163
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	IC	P163
dot1x port-control	ポートへの dot1x モードの設定	IC	P164
dot1x operation-mode	dot1x ポートへの接続可能ホスト数の設定	IC	P165
dot1x re-authenticate	特定ポートへの再認証の強制	IC	P166
dot1x re-authentication	全ポートへの再認証の強制	IC	P166
dot1x timeout quiet-period	認証プロセスを繰り返す最大回数を超えた場合に、クライアントの応答を待つ時間	IC	P167
dot1x timeout re-autheperiod	接続済みクライアントの再認証間隔の設定	IC	P167
dot1x timeout tx-period	認証中の EAP パケットの再送信間隔の設定	IC	P168
show dot1x	dot1x 関連情報の表示	PE	P169

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。コマンドの前に "no" を置くことにより、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。コマンドの前に** "no" **を置くことにより、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 **回**

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。キーワードなしでコマンドの前に "no" を置くことで初期設定に戻ります。" multi-host max-count" キーワードと共にコマンドの前に "no" を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 P167 「dot1x port-control」で "auto" に設定されている場合にのみ有効です。
- "multi-host" を設定すると、ポートに接続するホストのうちの 1 台のみが認証の許可を得られれば、他の複数のホストもネットワークへのアクセスが可能になります。逆に、接続するホスト再認証に失敗したり、EAPOL ログオフメッセージを送信した場合、他のホストも認証に失敗したことになります。

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 （範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**

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。コマンドの前に "no" **を置くことで再認証を無効にします。**

文法

dot1x re-authentication
no dot1x re-authentication

コマンドモード

Interface Configuration

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超えた後、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。コマンドの前に "no" を置くことにより、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。コマンドの前に** "no" **を置くことにより、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
    - unit — **ユニット番号 （範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**

コマンドモード

Privileged Exec

コマンド解説

本コマンドで表示されるのは以下の情報です。

- 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 — P168 **「**dot1x operation-mode**」の設定値**
  - Mode — dot1x port-control **で設定する** dot1x **モード**
  - 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**
  - reauth-period - **接続されたクライアントに再認証を要求する間隔**
  - 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** (P170)
  - tx-period - **認証時に** EAP **パケットの再送信を行う間隔** (P171**）**
  - 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**
  - Status - **認証ステータス** (**許可又は禁止**)
  - Operation Mode - IEEE802.1X **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**
  - 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**
  - 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 : Enabled
Authenticator Parameters:
  EAPOL Pass Through : Disabled
802.1X Port Summary
Port Type Operation Mode Control Mode Authorized
-------- ------------- -------------- ------------------ --------
1/1 Disabled Single-Host ForceAuthorized N/A
1/2 Disabled Single-Host ForceAuthorized N/A
...
1/25 Disabled Single-Host ForceAuthorized Yes
1/26 Enabled Single-Host Auto Yes

802.1X Port Details

802.1X Authenticator is enabled on port 1/1
.
.
.
802.1X Authenticator is enabled on port 26
Reauthentication       : Enabled
Reauth Period          : 3600
Quiet Period           : 60
TX Period              : 30
Supplicant Timeout     : 30
Server Timeout         : 10
Reauth Max Retries     : 2
Max Request            : 2
Operation Mode         : Multi-host
Port Control           : Auto
Intrusion Action       : Block traffic

Supplicant             : 00-e0-29-94-34-65

Authenticator PAE State Machine
  State                 : Initialize
  Reauth Count          : 0
  Current Identifier    : 0

Authenticator PAE State Machine
  State                 : Authenticated
  Reauth Count          : 0
  Current Identifier    : 3

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

Reauthentication State Machine
  State                 : Initialize

Console#
```

1.9.11 管理 IP フィルターコマンド

コマンド	機能	モード	ページ
management	管理アクセスを許可する IP アドレスを設定	GC	P172
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	P173

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。コマンドの前に "no" を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ないます。
- SNMP、Web ブラウザ、Telnet アクセスへの IP アドレス又は IP アドレス範囲の設定は合計で最大 5 つまで設定可能です。
- SNMP、Web ブラウザ、Telnet の同一グループに対して IP アドレス範囲を重複して設定することはできません。異なるグループの場合には IP アドレス範囲を重複して設定することは可能です。
- 設定した IP アドレス範囲から特定の IP アドレスのみを削除することはできません。IP アドレス範囲をすべて削除し、その後設定をし直して下さい。
- IP アドレス範囲の削除は IP アドレス範囲の最初のアドレスだけを入力しても削除することができます。また、最初のアドレスと最後のアドレスの両方を入力して削除することも可能です。

例

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#
```

1.10 セキュリティ対策

データポートに接続されているクライアントごとにトラフィックの分離方法をサポートしており、この機能により認証済みのクライアントのみネットワークへのアクセスを行うことが可能です。通常 IEEE 802.1X を用いたポートベース VLAN 認証を使用します。これらの方法以外に、ここでは、クライアントセキュリティを行うオプションについて説明しています。ポートベース認証は、特定の MAC アドレスを指定することにより、ネットワーククライアントアクセスを行います。DHCP クライアントに割り当てられているアドレスは、IP ソースガードおよび DHCP スヌーピングクライアントで制御することも可能です。

コマンド	機能	ページ
port security	管理アクセスを許可する IP アドレスを設定	P178
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	P173
802.1X Port Authentication	IEEE802.1X を使って特定ポートのホスト認証を設定します。	P162
Network Access	MAC 認証およびダイナミック VLAN の割り当てを行います。	P180
Web Authentication	Web 認証を行います。	P198
Access Control Lists	IP フレーム (アドレス、プロトコル、TCP/UDP ポート番号、TCP プロトコルコードに応じて)、あるいは IP 以外のフレーム（MAC アドレス、あるいはイーサネットタイプに応じて）のフィルタリングを行います。	P232
DHCP Snooping*	DHCP スヌーピングバインディングテーブルを設定および保持することにより、不正なポート上の不正 DHCP メッセージのフィルタリングを行います。	P204
IP Source Guard	DHCP スヌーピング、あるいはスタティックソースバインディングを介してソースアドレスを識別できない不正ポートの IP トラフィックのフィルタリングを行います。	P215
ARP Inspection	ARP パケットの MAC-to-IPA アドレスのバインディングが有効かどうか確認します。	P221

[注意] これらのフィルタリングコマンドを実行する上でのプライオリティは､ポートセキュリティ、ポート認証、ネットワークアクセス、WEB 認証、アクセスコントロールリスト、DHCP スヌーピング、IP ソースガードの順番になります。

1.10.1 ポートセキュリティ

ポートセキュリティを有効にします。インタフェース上の MAC アドレス学習機能を無効にすると、ポートのダイナミックあるいはスタティックアドレステーブルにストアされているソースアドレスをもつ受信トラフィックのみネットワークへのアクセスが許可されます。ポートセキュリティを使用する場合、設定した MAC アドレスの上限を上回ると、指定ポートの新規 MAC アドレスの学習を中断します。

認証していない MAC アドレスをもつデバイスがポートをアクセスしようとすると、侵入を探知して自動的にポートを無効にして、トラップメッセージを送信します。

コマンド	機能	モード	ページ
mac-address-table static	スタティックアドレスを VLAN のポートにマッピングします。	GC	P175
mac-learning	選択した物理インタフェース、または VLAN で学習した MAC アドレスを有効にします。	PE	P177
802.1X Port Authentication	IEEE802.1X を使って特定ポートのホスト認証を設定します。	IC	P162
port security	セキュアポートを設定します。	IC	P178
show mac-address-table	bridge-forwarding データベースのエントリを表示します。	PE	P302

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。コマンドの前に "no" を置くことで 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 （範囲：1-8）
    - port — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)
- vlan vlan-id — VLAN ID (1-4093)
- action
  - delete-on-reset — 本機が再起動されるまで登録されます。
  - permanent — 永久に登録されます。

初期設定

mac-address：なし

action：permanent

コマンドモード

Global Configuration

コマンド解説

- 静的アドレスは特定の VLAN の特定のポートに割り当てることができます。本コマンドを使用して静的アドレスを MAC アドレステーブルに追加することができます。静的アドレスは以下の特性を持っています。
  - インタフェースのリンクがダウンしても、静的アドレスはアドレステーブルから削除されません。
  - 静的アドレスは指定したインタフェースに固定され、他のインタフェースに移動することはありません。静的アドレスが他のインタフェースに現れた場合、アドレスは拒否されアドレステーブルに記録されません。
  - 静的アドレスは "no" コマンドを使って削除するまで、他のポートで学習されません。

例

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
 interface ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

mac-learning

選択したインタフェースの MAC アドレスの学習機能を有効にします。コマンドの前に ”no” を付けることにより、MAC アドレスの学習機能を無効にします。

文法

[no] mac-learning

初期設定

Enabled

コマンドモード

Interface Configuration (Ethernet or Port Channel)

コマンド解説

- no mac-learning コマンドにより、指定ポートまたはトランクの新規 MAC アドレスの学習機能を中断します。静的アドレステーブルに格納されている送信元アドレスを含んでいる受信トラフィック（「静的アドレスの設定」を参照）のみが、そのインタフェースによってネットワークにアクセス することを許可されたものとして受け入れられるようになります。MAC アドレス学習を無効にすると、アドレステーブルに格納されている動的アドレス がシステムからフラッシュされ、以降は、再び MAC アドレス学習が有効になるまで、動的アドレスが学習されなくなります。
- dot1x system-auth-control コマンドを使ってグローバルで 802.1X ポート認証が有効な場合、または同じインタフェースで port security コマンドを用いて MAC アドレスのセキュリティ機能が有効な場合は、mac-learning コマンドは使用できません。

例

以下の例では、ポート 2 の MAC アドレス学習機能を無効にします。

```
Console(config)#interface ethernet 1/2
Console(config-if)#no mac-learning
Console(config-if)#
```

関連するコマンド

show interfaces status (P258)

Port Security

ポートのセキュリティ機能を有効、または設定を行います。キーワードを付けずに、コマンドの前に ”no” を置くことにより、ポートセキュリティ機能を無効にします。適切なキーワードを付けて、コマンドの前に ”no” を置くことにより、セキュリティの破棄、あるいは許可されたアドレスの上限をデフォルトの設定に戻します。

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の動作
  - shutdown - ポートのみを無効にします。
  - trap - SNMP のトラップメッセージのみを発行します。
  - trap-and-shutdown - SNMP トラップメッセージを発行してポートを無効にします。
- max-mac-count
  - address-count - ポートで学習可能な MAC アドレスの上限 (範囲 : 0 - 1024、この場合、「0」は「無効」を意味します。)

初期設定

Status: Disabled

Action: None

max-mac-count:0

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- セキュアポートで許可される MAC アドレスのデフォルトの最大数は 0（= Disabled）です。ポートセキュリティを使用するには、port security max-mac-count コマンドを使ってポートで許可されるアドレスの最大数を設定する必要があります。
- port security コマンドにより、ポートセキュリティ機能を有効にすると、まず動的に学習したエントリはアドレステーブルからすべてクリアになります。次に、指定ポートの新規 MAC アドレスの学習を開始し、最大限に達すると中止します。ダイナミック、またはスタティックアドレステーブルにストアされている送信元アドレスの受信用トラフィックのみが受信されます。
- コマンドを使って、ポートで学習できるアドレスエントリの最大数を設定するには、まず、ポートセキュリティ機能を無効にしてから、許可される動的アドレスの最大数を指定します。スイッチ では、ポートで受信されるフレームについて、許可されているアドレスペア < 送信元 MAC アドレス、VLAN> の最大数になるまでアドレスが学習されます。mac-address-table コマンドを使って送信元アドレスをポートに手動で追加することも可能です。MAC アドレス の最大数に達すると、ポートで新しいアドレスが学習されなくなります。既にアドレ ステーブル内にある MAC アドレスは保持され、期限切れにはなりません。ただし、静的アドレステーブルを使用して、手動でセキュアアドレスを ポートに追加することができます。ポートセキュリティの状態が

Enabled から Disabled に変更されると、動的に学習されたすべてのエントリがアドレステーブルからクリアされます。ポートセキュリティが有効になっており、許可されるアドレスの最大数が 0（ゼロ）以外に設定されている場合、アドレスがアドレステーブルに含まれていないデバイスがポートを使用しようとすると、スイッチへのアクセスが拒否されます。

- セキュリティ違反のためポートが無効になっている（シャットダウンされている）場合は、no shutdown コマンドを使って手動でポ ートを再び有効にする必要があります。
- セキュアポートには、以下の制限事項があります。
  - 静的トランクまたは動的トランクのメンバーとして使用することはできません。
  - ネットワーク相互接続デバイスに接続しないようにしなければなりません。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

1.10.2 ネットワークアクセス (MAC アドレス認証)

ネットワークアクセス認証は、ポートに接続しようとする各ホストの MAC アドレスの認証を行うことにより、ネットワークへのアクセスを制御します。指定の MAC アドレスから受信したトラフィックは、送信元の MAC アドレスが RADIUS サーバによって正常に認証された場合のみ送信されます。MAC アドレスが認証中の場合は、認証が完了するまでトラフィックはすべてブロックされます。一度正常に認証が行われると、RADIUS サーバはオプションでポートの VLAN および QoS 設定を割り当てることが可能です。

コマンド	機能	モード	ページ
network-access aging	MAC アドレスのエイジングを有効にします。	GC	P181
network-access mac-filter	MAC アドレスをフィルタテーブルに追加します。	GC	P182
mac-authentication reauthtime	接続先の MAC アドレスを再認証後の有効時間を設定します。	GC	P183
network-access dynamic-qos	ダイナミック QoS 機能を有効にします。	IC	P184
network-access dynamic-vlan	RADIUS サーバからの VLAN の動的割り当てを有効にします。	IC	P185
network-access guest-vlan	guest VLAN を指定します。	IC	P186
network-access link-detection	リンク検知機能を有効にします。	IC	P187
network-access link-detection link-down	リンク検知機能を設定して、リンクダウンイベントを検知して、対応します。	IC	P188
network-access link-detection link-up	リンク検知機能を設定して、リンクアップイベントを検知して、対応します。	IC	P190
network-access link-detection link-up-down	リンク検知機能を設定して、リンクアップイベントおよびリンクダウンイベントを検知して、対応します。	IC	P190
network-access max-mac count	すべての認証形式を介して、ポートで認証可能な MAC アドレスの最大数を設定します。	IC	P191
network-access mode macauthentication	インタフェースの MAC 認証を有効にします。	IC	P192
network-access port-macfilter	指定した MAC アドレスのフィルタリングを有効にします。	IC	P193
mac-authentication intrusionaction	接続先のホストが MAC 認証に失敗した場合のポートの処理方法を設定します。	IC	P194
mac-authentication maxmac-count	MAC 認証を介して、ポートで認証可能な MAC アドレスの最大数を設定します。	IC	P191
show network-access	ポートのインタフェース用の MAC 認証の設定値を表示します。	PE	P195

show network-access macaddress-table	セキュア MAC アドレステーブルのエントリ情報を表示します。	PE	P196
show network-access macfilter	MAC フィルタリングテーブルのエントリ情報を表示します。	PE	P197

network-access aging

セキュア MAC アドレステーブルにストアされている認証済みの MAC アドレスのエイジングを有効にします。コマンドの前に "no" を付けることにより、アドレスのエイジングを無効にします。

文法

[no] network-access aging

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- 認証されている MAC アドレスは、セキュア MAC アドレステーブルにダイナミックエントリとして格納されており、エイジングタイムが切れると削除されます。アドレスのエイジングタイムは、macaddress-table aging-time コマンドによって決定されます。
- このパラメータは、このセクションで説明し ている MAC アドレス認証プロセスで設定される認証済み MAC アドレス だ けでなく、「802.1X Operation Mode」で説明している「Single-Host」、「Multi-Host」、または「MAC-Based」認証）に関係なく、802.1X によって認証されるあらゆるセキュアな MAC アドレスに適用されます。
- 認証された MAC アドレスは、スイッチのセキュアな MAC アドレステーブルに動的エントリとして保存され、期限切れになると削除されます。このスイッチシステムでサポートされる送信元 MAC アドレスの最大数は「1,024」です。

例

```
Console(config)#network-access aging
Console(config)#
```

network-access mac-filter

MAC アドレスをフィルタテーブルに追加します。コマンドの前に ”no” を付けることにより、指定した MAC アドレスを削除します。

文法

[no] network-access mac-filter filter-id

mac-address mac-address [mask mask-address]

- filter-id - MAC アドレスフィルタテーブルを指定します (有効範囲 : 1-64)
- mac-address - MAC アドレスのエントリを指定します。(形式 : xx-xx-xx-xx-xx-xx)
- mask - アドレスの範囲内の MAC アドレスのビットマスクを指定します。

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- 指定したアドレスは、ネットワークのアクセス認証から除外されます。
- mac-address-table static コマンドを使って設定するスタティックアドレスとは異なり、これにより、マスクを使ってアドレスの範囲を設定して、network-access port-mac-filter コマンドを使って１つまたは複数のポートにこれらのアドレスを設定することが可能です。
- フィルタテーブルは 64 個まで設定可能です。
- フィルタテーブルで入力可能なエントリ数には制限ありません。

例

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-
44-55-66
Console(config)#
```

mac-authentication reauth-time

接続先の MAC **アドレスを再認証した後の有効時間を設定します。コマンドの前に** "no" **を付けることにより、デフォルト設定値に戻します。**

文法

mac-authentication reauth-time seconds

no mac-authentication reauth-time

- seconds - **有効時間** (**有効範囲** : 120-1000000 **秒**)

初期設定

1800

コマンドモード

Global Configuration

コマンド解説

- **再認証後の有効時間がグローバル設定により、すべてのポートに適用されます。**
- **セキュア** MAC **アドレスの有効時間が切れると、**RADIUS **サーバにより再認証を行います。再認証処理の間、ポートを介したトラフィックには影響ありません。**

例

```
Console(config)#mac-authentication reauth-time 300
Console(config)#
```

network-access dynamic-qos

認証済みのポートのダイナミック QoS **機能を有効にします。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] network-access dynamic-qos

初期設定

Disabled

コマンドモード

Interface Configuration

コマンド解説

- **必要に応じ て、認証されたユーザのスイッチポートに適用される動的** QoS **割り当てが** RADIUS **サーバによって返されるようにすることもできます。以下の** QoS **情報を渡すように「**Filter-ID**」属性（属性** 11**）を** RADIUS **サーバで設定することができます。**
- **動的** QoS **が割り当てられているポートに最後のユーザがログオフすると、ポートの元の** QoS **設定が復元されます。**
- **戻した動的** QoS **プロファイルを使用してユーザがネットワークにログインしようとしたときに、そのプロファイルが同じポートにログインするときに既に使用されたものと異なる場合、ユーザはアクセスを拒否されます。**
- **ポートには動的** QoS **プロファイルが割り当てられていますが、**QoS **設定に手動で加えられた変更は、すべてのユーザがポートからログオフした後にのみ有効になります。**

[**注意**] **ダイナミック** QoS **の設定上の変更については、本機のコンフィグレーションファイルには保存されません。**

例

以下の例では、ポート 1 のダイナミック QoS 機能を有効にします。

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

network-access dynamic-vlan

認証済みポートのダイナミック VLAN の割り当てを有効にします。コマンドの前に "no" を付けることにより、ダイナミック VLAN の割り当てを無効にします。

文法

[no] network-access dynamic-vlan

初期設定

Enabled

コマンドモード

Interface Configuration

コマンド解説

- 有効にすると、RADIUS サーバによって返されるあらゆる VLANID がポートに適用され、スイッチで既に作成されている VLAN が提供されるようになります（GVRP による VLAN の作成は使用されません）（デフォルト :Enabled）。
- ポートには、最初に認証される MAC アドレスによって指定される VLAN 設定が実装されます。ポートで認証されるその他の MAC アドレスの VLAN 設定は同じでなければなりません。同じでない場合、それらの MAC アドレスは認証に失敗したものとして処理されます。
- 動的 VLAN 割り当てがポートで有効になっており、VLAN 設定が RADIUS サーバによって一切返されない場合でも、認証は成功したものとして処理され、ホストはデフォルトのタグなし VLAN に割り当てられます。
- ポートで動的 VLAN 割り当てのステータスが変更されると、すべての認証済みアドレスがセキュアな MAC アドレステーブルからクリアされます。

例

ここでは、ポート 1 のダイナミック VLAN 設定を有効にします。

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```

network-access guest-vlan

IEEE802.1X 認証が拒否された場合、ポート上のトラフィックをゲスト用 VLAN に割り当てます。コマンドの前に "no" を付けることにより、ゲスト用 VLAN を無効にします。

文法

network-access guest-vlan vlan-id

no network-access guest-vlan

- vlan-id - VLAN ID (有効範囲 : 1-4093)

初期設定

Disabled

コマンドモード

Interface Configuration

コマンド解説

- ゲスト用 VLAN として設定する VLAN ID を「有効」にする必要があります (vlan database コマンドを参照ください)。
- intrusion-action は、802.1X 認証を用いて、“guest-vlan” を有効にする必要があります (dot1x intrusion-action コマンドを参照してください)。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

network-access link-detection

選択したポートのリンク検知を有効にします。コマンドの前に ”no” **を付けることにより、デフォルト設定に戻ります。**

文法

[no] network-access link-detection

初期設定

Disabled

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection
Console(config-if)#
```

network-access link-detection linkdown

link-down イベントを検知します。検知すると、ポートをシャットダウンするか、または SNMP トラップを送信します（あるいはその両方）。コマンドの前に "no" を付けることにより、この機能は無効になります。

文法

network-access link-detection link-down

action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

- action - ポートセキュリティの動作
  - shutdown - ポートを無効にします。
  - trap - SNMP の trap メッセージを発行します。
  - trap-and-shutdown - SNMP の trap メッセージを発行して、ポートを無効にします。

初期設定

Disabled

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up action
trap
Console(config-if)#
```

network-access link-detection linkup

link-up イベントを検知します。検知すると、ポートをシャットダウンするか、または SNMP トラップを送信します（あるいはその両方）。コマンドの前に "no" を付けることにより、この機能は無効になります。

文法

network-access link-detection link-down

action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

- action - ポートセキュリティの動作
  - shutdown - ポートを無効にします。
  - trap - SNMP の trap メッセージを発行します。
  - trap-and-shutdown - SNMP の trap メッセージを発行して、ポートを無効にします。

初期設定

Disabled

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up action
trap
Console(config-if)#
```

network-access link-detection link-up-down

link-up **および** link-down **イベントを検知します。検知すると、ポートをシャットダウンするか、または** SNMP **トラップを送信します（あるいはその両方）。コマンドの前に** "no" **を付けることにより、この機能は無効になります。**

文法

network-access link-detection link-up-down

action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

- action - **ポートセキュリティの動作**
  - shutdown - **ポートを無効にします。**
  - trap - SNMP **の** trap **メッセージを発行します**
  - trap-and-shutdown - SNMP **の** trap **メッセージを発行して、ポートを無効にします。**

初期設定

Disabled

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up-down
action trap
Console(config-if)#
```

network-accessmax-mac-count

すべての認証形式を介して、ポートインタフェースで認証可能な MAC **アドレスの最大数を設定します。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻ります。**

文法

network-access max-mac-count count

no network-access max-mac-count

- count - **認証されている** IEEE 802.1X **および使用可能な** MAC **アドレスの最大数** (**有効範囲** : 0-1024; **この場合、「**0**」は「無制限」を 示します**)。

初期設定

1024

コマンドモード

Interface Configuration

コマンド解説

- **ポート単位の** MAC **アドレスの最大数は「**1024**」、本機のシステムでサポートされているセキュア** MAC **アドレスの最大数は「**1024**」です。上限に達すると、新規の** MAC **アドレスはすべて認証に失敗したものとみなされます。**

例

```
Console(config-if)#network-access max-mac-count 5
Console(config-if)#
```

network-access mode macauthentication

ポートのネットワークアクセスの認証を有効にします。コマンドの前に "no" を付けることにより、ネットワークアクセスの認証を無効にします。

文法

[no] network-access mode mac-authentication

初期設定

Disabled

コマンドモード

Interface Configuration

コマンド解説

- MAC アドレス認証では、スイッチポートに接続しようとする各ホストの MAC アドレスを認証することにより、ネットワークへのアクセスを制御します。特定の MAC アドレスから受信されるトラフィックは、送信元 MAC アドレスがセントラル RADIUS サーバによって正常に認証される場合にのみ、転送されます。
- MAC アドレスの認証の進行中は、認証が完了するまで、すべてのトラフィックがブロックされます。必要に応じて、認証が正常に完了した後にスイッチポートの VLAN 設定と QoS 設定が RADIUS サーバによって割り当てられるようにすることもできます。
- ポートで認証が有効になっている場合、認証プロセスでは、PAP（PasswordAuthenticationProtocol）要求が、設定済みの RADIUS サーバに送信されます。ユーザ名とパスワードは、両方とも、認証される MAC アドレスと等しくなります。
- RADIUS サーバでは、PAP ユーザ名とパスワードを XX-XX-XX-XX-XX-XX（すべて大文字）というように、MAC アドレス形式で設定する必要があります。
- 認証された MAC アドレスは、スイッチのセキュアな MAC アドレステーブルに動的エントリとして保存され、期限切れになると削除されます。このスイッチシステムでサポートされる送信元 MAC アドレスの最大数は 1,024 です。
- 設定されている静的 MAC アドレスは、スイッチポートで検出されると、セキュアなアドレステーブルに追加されます。静的アドレスは、要求が RADIUS サーバに送信されることなく、認証済みアドレスとして処理されます。
- MAC 認証の IEEE802.1X、およびポートセキュリティを同じポート上で設定することはできません。１つのセキュリティ方式の適用可能です。
- MAC 認証はトランクポート上で設定することはできません。
- ポートがダウン状態になると、そのポートにマップされているすべての MAC アドレスがセキュアな MAC アドレステーブルからクリアされます。静的 VLAN 割り当ては復元されません。
- スイッチポートに適用される VLANID リストが必要に応じて RADIUS サーバによって返すようにすることもできます。

- RADIUS サーバで以下の属性を設定する必要があります。VLANID リストは、RADIUS の「Tunnel-Private-Group-ID」属性によって伝播されます。VLAN リストには、複数の VLANID を「1u,2t,3u」という形式で含めることができます（「u」はタグなし VLAN、「t」はタグ付き VLAN を示します）。“Tunnel-Type” の属性を ”VLAN” に設定し、“Tunnel-Medium-Type” の属性を ”“802” に設定する必要があります。

例

```
Console(config-if)#network-access mode mac-authentication
Console(config-if)#
```

network-access port-mac-filter

指定した MAC アドレスのフィルタリングを有効にします。コマンドの前に "no" を付けることにより無効にします

文法

network-access port-mac-filter filter-id

no network-access port-mac-filter

- filter-id - MAC フィルタリングテーブルを指定します (有効範囲 : 1-64)

初期設定

None

コマンドモード

Interface Configuration

コマンドモード

- MAC アドレスフィルタテーブルのエントリは network-access mac-filter コマンドを用いて設定可能です。
- ポートに割り当て可能なフィルタリングテーブルは 1 つのみです。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access port-mac-filter 1
Console(config-if)#
```

mac-authentication intrusion-action

ホストの MAC **認証に失敗した場合のポートの処理方法を設定します。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻ります。**

文法

mac-authentication intrusion-action {block traffic | pass traffic}

no mac-authentication intrusion-action

初期設定

トラフィックをブロックします。

コマンドモード

Interface Configuration

例

```
Console(config-if)#mac-authentication intrusion-action block-
traffic
Console(config-if)#
```

mac-authentication max-mac-count

MAC **認証を介して、ポートで認証可能な** MAC **アドレスの最大数を設定します。コマンドの前に** "no" **を付けることによりデフォルト設定に戻ります。**

文法

mac-authentication max-mac-count count

no mac-authentication max-mac-count

- count - MAC **認証された** MAC **アドレスの最大数** (**有効範囲** : 1-1024)

初期設定

1024

コマンドモード

Interface Configuration

例

```
Console(config-if)#mac-authentication max-mac-count 32
Console(config-if)#
```

show network access

ポートインタフェースの MAC **認証の設定値を表示します。**

文法

show network-access [interface interface]

- interface - **ポートインタフェースを指定します。**

  ethernet unit/port

  unit - **スタックユニット** (**有効範囲** : 1-8)

  port - **ポート番号** (**有効範囲** : 1-26)

初期設定

インタフェースの設定値をすべて表示します。

コマンドモード

Privileged Exec

例

```
Console#show network-access interface ethernet 1/1
Global secure port information
Reauthentication Time : 1800
---------------------------------------------------
---------------------------------------------------
Port : 1/1
MAC Authentication : Disabled
MAC Authentication Intrusion action : Block traffic
MAC Authentication Maximum MAC Counts : 1024
Maximum MAC Counts : 2048
Dynamic VLAN Assignment : Enabled
Guest VLAN : Disabled
Console#
```

show networkaccess macaddress-table

セキュアな MAC アドレステーブルのエントリを表示します。

文法

show network-access mac-address-table [static | dynamic]

[address mac-address [mask]] [interface interface]

[sort {address | interface}]

- static - スタティックアドレスエントリを指定します。
- dynamic - ダイナミックアドレスエントリを指定します。
- mac-address - MAC アドレスのエントリを指定します。(形式 : xx-xx-xx-xx-xx-xx)
- mask - 表示されているアドレスのフィルタリングを行う MAC アドレスのビットマスクを指定します。
- interface - ポートのインタフェースを指定します。
- ethernet unit/port
- unit - スタックユニット (有効範囲 : 1-8)
- port - ポート番号 (有効範囲 : 1-26)
- sort - 表示されているエントリは、MAC アドレスまたはインタフェースのいずれかでソートします。

初期設定

すべてのフィルタを表示します。

コマンドモード

Privileged Exec

コマンド解説

- 表示されている MAC アドレスのフィルタリングを行うためのビットマスクを使用する場合は、1 は “care”、0 は “don't care” を意味します。例えば、00-00-01-02-03-04 の MAC、マスク FF-FF-FF-00-00-00 は、00-00-01-00-00-00 から 00-00-01-FF-FF-FF までの範囲の MAC が表示されます。その他の MAC はフィルタリングされます。

例

```
Console#show network-access mac-address-table
---- ----------------- --------------- --------- ----------------
---------
Port MAC-Address RADIUS-Server Attribute Time
---- ----------------- --------------- --------- ----------------
---------
1/1 00-00-01-02-03-04 172.155.120.17 Static 00d06h32m50s
1/1 00-00-01-02-03-05 172.155.120.17 Dynamic 00d06h33m20s
1/1 00-00-01-02-03-06 172.155.120.17 Static 00d06h35m10s
1/3 00-00-01-02-03-07 172.155.120.17 Dynamic 00d06h34m20s
Console#
```

show networkaccess mac-filter

MAC **フィルタリングテーブルのエントリ情報を表示します。**

文法

show network-access mac-filter [filter-id]

- filter-id - Specifies a MAC **フィルタリングテーブル** (**有効範囲** : 1-64)

初期設定

フィルタをすべて表示します。

コマンドモード

Privileged Exec

例

```
Consoleshownetwork-access mac-filter
Filter ID MAC Address MAC Mask
--------- ----------------- -----------------
1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF
Console#
```

1.10.3 WEB 認証

Web 認証は、IEEE802.1X 認証またはネットワークアクセス認証が実現できない状況または実用的ではない状況で管理ステーションにおけるサービス承認とネットワークアクセス認証を可能にします。Web 認証機能を使用すれば、認証していないホストが、DHCP によって割り当てられる IP アドレスを要求して受信し、DNS クエリを実行できるようになります。その他のトラフィック（ただし、HTTP プロトコルトラフィックは除く）は、すべて、ブロックされます。スイッチは、HTTP プロトコルトラフィックをインターセプトして、RADIUS によるユーザ名とパスワードの認証を容易にするためにスイッチで生成された Web ページにリダイレクトします。認証が正常に完了すると、元々要求された Web ページに転送され、そのページの内容が Web ブラウザに表示されるようになります。認証が正常に完了した場合、その認証は、ポートに接続されているすべてのホストについて有効になります。

[注意] Web 認証機能が正しく機能するには、RADIUS 認証がアクティブになっており、正しく設定されていなければなりません（「ローカルまたはリモートのログオン認証の設定」を参照）。

[注意] Web 認証はトランクポートでは設定できません。

コマンド	機能	モード	
web-auth login-attempts	WEB 認証ログインに失敗した制限回数を設定しま	GC	P199
web-auth quiet-period	WEB 認証ログインに失敗した制限回数を超えた場合の待機する合計を設定します。	GC	P199
web-auth session-timeout	WEB 認証のセッションが有効な時間を設定します。	GC	P200
web-auth system-authcontrol	本機の WEB 認証をグローバルで有効にします。	GC	P200
web-auth	インタフェースの WEB 認証を有効にします。	IC	P201
web-auth re-authenticate (Port)	ポートの WEB 認証をすべて終了し、ユーザに再認証を促します。	PE	P201
web-auth re-authenticate (IP)	指定の IP アドレスに関連のある WEB 認証を終了し、ユーザに再認証を促します。	PE	P202
show web-auth	WEB 認証の値をグローバルで表示します。	PE	P202
show web-auth interface	インタフェース固有の WEB 認証パラメータおよび統計情報を表示します。	PE	P203
show web-auth summary	WEB 認証ポートのパラメータおよび統計情報のサマリを表示します。	PE	P203

web-auth login attempts

WEB 認証ログインに失敗した制限回数を設定します。制限回数に達すると、一定の時間が過ぎるまでログインできなくなります。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

web-auth login-attempts count

no web-auth login-attempts

count - ログインに失敗した回数の上限 (有効範囲 : 1-3)

初期設定

ログイン回数 : 3 回

コマンドモード

Global Configuration

例

```
Console(config)#web-auth login-attempts 2
Console(config)#
```

web-auth quietperiod

WEB 認証ログインに失敗した制限回数を超えた場合の待機する合計を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

web-auth quiet-period time

no web-auth quiet period

- time - 再認証を行うまでのホストの待機時間 (有効範囲 : 1-180 秒)

初期設定

60 seconds

コマンドモード

Global Configuration

例

```
Console(config)#web-auth quiet-period 120
Console(config)#
```

web-auth sessiontimeout

WEB 認証のセッションの有効時間を設定します。セッションのタイムアウトが切れると、ホストはログオフされ、次のデータ伝送が実施されるまで再認証を行う必要があります。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

web-auth session-timeout timeout

no web-auth session timeout

- timeout - 認証されたセッションの有効時間 (有効範囲 : 300-3600 秒)

初期設定

3600 seconds

コマンドモード

Global Configuration

例

```
Console(config)#web-auth session-timeout 1800
Console(config)#
```

web-auth systemauth-control

本機の WEB 認証をグローバルで有効にします。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] web-auth system-auth-control

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- 本機の web-auth system-auth-control およびインタフェースの web-auth を WEB 認証機能が有効になるよう設定する必要があります。

例

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

web-auth

インタフェースの WEB **認証を有効にします。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] web-auth

初期設定

Disabled

コマンドモード

Interface Configuration

コマンド解説

- **本機の** web-auth system-auth-control **およびポートの** web-auth **を** WEB **認証機能が有効になるよう設定する必要がります。**

例

```
Console(config-if)#web-auth
Console(config-if)#
```

web-auth reauthenticate (port)

ポートに接続されている WEB **認証セッションをすべて終了し、ユーザに再認証を行わせます。**

文法

web-auth re-authenticate interface interface

- interface - **ポートインタフェースを指定します。**

  ethernet unit/port

  - unit - **スタックユニット** (**有効範囲** : 1-8)
  - port - **ポート番号** (**有効範囲** : 1-26)

初期設定

None

コマンドモード

Privileged Exec

例

```
Console#web-auth re-authenticate interface ethernet 1/2
Console#
```

web-auth reauthenticate(IP)

指定した IP **アドレスに関連のある** WEB **認証を終了させ、ユーザに再認証を行わせます。**

文法

web-auth re-authenticate interface interface ip

- interface - **ポートインタフェースを指定します。**

  ethernet unit/port

  - unit - **スタックユニット** (**有効範囲** : 1-8)
  - port - **ポート番号** (**有効範囲** : 1-26)
  - ip - IPv4 formatted IP address

初期設定

None

コマンドモード

Privileged Exec

例

```
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Console#
```

show web-auth

WEB **認証パラメータをグローバルで表示します。**

コマンドモード

Privileged Exec

例

```
Console#show web-auth

Global Web-Auth Parameters

  System Auth Control : Enabled
  Session Timeout     : 3600
  Quiet Period        : 60
  Max Login Attempts  : 3
Console#
```

show web-auth interface

インタフェース固有の WEB **認証パラメータおよび統計情報を表示します。**

文法

show web-auth interface interface

- interface - **ポートインタフェースを指定します。**

  ethernet unit/port

  - unit - **スタックユニット** (**有効範囲** : 1-8)
  - port - **ポート番号** (**有効範囲** : 1-26)

コマンドモード

Privileged Exec

例

```
Console#show web-auth interface ethernet 1/2
Web Auth Status : Enabled
Host Summary
IP address Web-Auth-State Remaining-Session-Time
--------------- -------------- -----------------------
1.1.1.1 Authenticated 295
1.1.1.2 Authenticated 111
Console#
```

show web-auth summary

WEB **認証のポートパラメータおよび統計情報を表示します。**

コマンドモード

Privileged Exec

例

```
Console#show web-auth summary
Global Web-Auth Parameters
System Auth Control : Enabled
Port Status Authenticated Host Count
---- ------ ------------------------
1/ 1 Disabled 0
1/ 2 Enabled 8
1/ 3 Disabled 0
1/ 4 Disabled 0
1/ 5 Disabled 0
...
```

1.10.4 DHCP スヌーピング

非セキュアなポートで DHCP クライアントに割り当てられているアドレスは、DHCP スヌーピングによって登録される動的バインディングを使用して（または、IP ソースガードで設定される静的バインディングを使用して）、詳細に制御することができます。スイッチで DHCP スヌーピングを使用すると、認証されていない DHCP サーバ、またはポート関連の情報を DHCP サーバに送信するその他のデバイスからネットワークを保護することができます。ポート関連の情報は、IP アドレスを物理ポートまでさかのぼって追跡する場合に利用することができます。

コマンド	機能	モード	ページ
ipdhcp snooping	Enables DHCP スヌーピング機能をグローバルで有効にします。	GC	P205
ip dhcp snooping database flash	動的に学習されたすべてのスヌーピングエントリをフラッシュメモリに書き込みます。	PE	P207
ip dhcp snooping information option	DHCP オプション 82 情報のリレーを有効 / 無効にします。	GC	P208
ip dhcp snooping information policy	DHCP オプション 82 情報を含む、DHCP クライアントパケットの情報のオプションのポリシーを設定します。	GC	P209
ip dhcp snooping verify mac-address	イーサネットヘッダの送信元の MAC アドレスに対して、DHCP パケットにストアされているクライアントのハードウェアのアドレスを検証します。	IC	P210
ip dhcp snooping vlan	指定の VLAN の DHCP スヌーピングを有効にします。	PE	P211
ip dhcp snooping trust	指定したインタフェースをトラストのインタフェースとして設定します。	PE	P212
clear ip dhcp snooping database flash	動的に学習したスヌーピングエントリをすべてフラッシュメモリから削除します。	PE	P213
show ip dhcp snooping	DHCP スヌーピングのコンフィグレーションの設定値を表示します。	PE	P213
show ip dhcp snooping binding	DHCP スヌーピングのバインディングテーブルのエントリを表示します。	PE	P214

ip dhcp snooping

DHCP スヌーピングをグローバルで有効にします。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] ip dhcp snooping

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- 不正な DHCP メッセージが外部送信元から受信されると、ネットワークトラフィックが妨げられる可能性があります。DHCP スヌーピングを使用して、非セキュアなインタフェースでネットワークやファイアウォールの外部から受信される DHCP メッセージをフィルタリングすることができます。DHCP スヌーピングをスイッチでグローバルで有効にし、VLAN インタフェースで有効にすると、信頼できないインターフェースでは、DHCP スヌーピングテーブルに含まれていないデバイスから受信された DHCP メッセージがドロップされるようになります。
- テーブルには、信頼できるインタフェースのみについて学習されたエントリが保存されます。エントリは、クライアントが IP アドレスを DHCP サーバから受け取ったり、DHCP サーバにリリースしたりすると、動的に DHCP スヌーピングテーブルに追加または削除されます。各エントリには、MAC アドレス、IP アドレス、リースタイム、VLANID、およびポート ID が含まれます。スイッチで処理できる DHCP メッセージの帯域制御は、100 パケット / 秒です。この制限を超えると、すべての DHCP パケットがドロップされます。
- DHCP スヌーピングが有効になっている場合、信頼できないインタフェースに入ってくる DHCP メッセージは、DHCP スヌーピングによって学習された動的エントリに基づいてフィルタリングされます。
- フィルタリングルールは、以下のように実装されます。
  - グローバル DHCP スヌーピングが無効になっている場合、すべての DHCP パケットが転送されます。
  - DHCP スヌーピングがグローバルで有効になっており、DHCP パケットが受信される VLAN でも有効になっている場合、信頼できるポートについては、すべての DHCP パケットが転送されます。また、受信されたパケットが DHCPACK メッセージである場合は、動的 DHCP スヌーピングエントリがバインディングテーブルに追加されます。
  - DHCP スヌーピングがグローバルで有効になっており、DHCP パケットが受信される VLAN でも有効になっているが、ポートが信頼できるポートではない場合、DHCP パケットは以下のように処理されます。DHCP パケットが DHCP サーバからの返信パケット（OFFER、ACK、または NAK メッセージなど）である場合、そのパケットはドロップされます。DHCP パケットがクライアントからのもの（DECLINE メッセージや RELEASE メッセージなど）である場合、対応するエントリがバインディングテーブルで検出されたときにのみ、そのパケットは転送されます。
- DHCP パケットがクライアントからのもの（DISCOVER、REQUEST、INFORM、DECLINE、RELEASE メッセージなど）である場合、MAC アドレス検証が無効に

なっていると、そのパケットは転送されます。ただし、MAC アドレス検証が有効になっていると、DHCP パケットに保存されているクライアントのハードウェアアドレスがイーサネットヘッダ内の送信元 MAC アドレスと同じであれば、そのパケットは転送されます。

- DHCP パケットが認識されないタイプである場合、そのパケットはドロップされます。
- クライアントからの DHCP パケットが上記のフィルタリング条件を満たす場合、そのパケットは同じ VLAN 内の信頼できるポートのみに転送されます。
- DHCP パケットがサーバからのものであり、信頼できるポートで受信された場合、そのパケットは同じ VLAN 内の信頼できるポートと信頼されていないポートのどちらにも転送されます。
- DHCP スヌーピングがグローバルで無効になると、すべての動的バインディングがバインディングテーブルから削除されます。
- スイッチ自体が DHCP クライアントである場合のその他の考慮事項として、スイッチがクライアント要求を DHCP サーバに送信するときに使用するポートは信頼できるポートとして設定されていなければならないということが挙げられます。スイッチで ACK メッセージが DHCP サーバから受信された場合、そのスイッチ自体の動的エントリはバインディングテーブルに追加されないので注意してください。また、スイッチが自らの DHCP クライアントパケットを送信する場合にはフィルタリングは実行されません。ただし、スイッチが何らかのメッセージを DHCP サーバから受信する場合には、信頼できないポートから受信されたパケットは、すべて、ドロップされます。

例

ここでは、グローバルで DHCP スヌーピング機能を有効にします。

```
Console(config)#ip dhcp snooping
Console(config)#
```

関連するコマンド

ip dhcp snooping vlan (P211)

ip dhcp snooping trust (P212)

ip dhcp snooping database flash

ダイナミックに学習されるスヌーピングエントリのすべてをフラッシュメモリに書き込みます。

コマンドモード

Privileged Exec

コマンド解説

- **現行でダイナミックに学習されるスヌーピングエントリのすべてをフラッシュメモリに書き込むために使用します。本機のリセット時にこれらのエントリをスヌーピングテーブルにリストアします。ただし、フラッシュメモリからリストアされているダイナミックエントリに対して表示されるリースタイムは無効になります。**

例

```
Console(config)#ip dhcp snooping database flash
Console(config)#
```

ip dhcp snooping information option

他のスイッチの DHCP オプション 82 情報リレーが有効になります。コマンドの前に "no" を付けることにより、この機能は無効になります。

文法

[no] ip dhcp snooping information option

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- DHCP Option 82 は、DHCP クライアントに関する情報を送信するための中継メカニズム、または中継エージェント自体を、DHCP サーバに提供します。この機能をサポートしている DHCP サーバは、IP アドレスを割り当てる場合、またはクライアントに関する他のサービスやポリシーを設定するため、DHCP クライアントに関する情報を使用することができます。また、DHCP Option 82 は、IP スヌーピング、クライアント ID スヌーピング、MAC アドレススヌーピング、アドレス消費などの DHCP サービスで、攻撃されたクライアントからの悪意あるネットワーク攻撃を防ぐ場合にも有効です。
- 要求パケットに挿入される Option 82 情報について DHCP スヌーピングを有効にする必要があります。
- Option 82 情報の DHCP スヌーピングが有効になっている場合、スイッチによって転送される DHCP 要求パケットおよび DHCP サーバから返される返信パケットによって、要求元のクライアント（または、自らの情報を記述するために Option 82 情報フィールドを使用した中継エージェント）を特定することができます。Option 82 情報によって、要求元デバイス（つまり、この場合はスイッチ）の MAC アドレスまたは IP アドレスを特定することもできます。また、本製品では、デフォルトで、DHCP クライアント要求を受け取るときに使用されるローカルインタフェースを示す情報（ポートや VLAN ID など）が Option 82 Circuit ID フィールドに入れられます。そのようにすると、DHCP クライアントサーバ交換メッセージを、VLAN 全体にフラッドさせることなく、サーバとクライアント間で転送することができます。
- スイッチで Option 82 情報の DHCP スヌーピングが有効になっている場合は、（DHCP スヌーピングフィルタリングルールに従って）VLAN 経由で受信される DHCP 要求パケットに情報を挿入することもできます。中継されるパケットに挿入される情報には、回線 ID およびリモート ID だけでなく、ゲートウェイインターネットアドレスも含まれます。

例

DHCP スヌーピング情報のオプションを有効にします。

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

ip dhcp snooping information policy

Option 82 情報を含む DHCP クライアントパケットの DHCP スヌーピング情報のオプションポリシーを設定します。

文法

ip dhcp snooping information policy {drop | keep | replace}

- Drop - クライアントの要求パケットを中継せずにドロップします。
- Keep - クライアント要求に含まれている Option 82 情報を保持し、信頼できるポートにパケットを転送します。
- Replace - クライアントの要求に含まれている Option 82 情報の circuit-id フィールドおよび remote-id フィールドを、中継エージェント自体に関する情報に置き換え、中継エージェントのアドレスを挿入し（DHCP スヌーピングが有効になっている場合）、信頼できるポートにパケットを転送します（これがデフォルトです）。

初期設定

replace

コマンドモード

Global Configuration

コマンド解説

- 既に DHCP Option 82 情報を含んでいる DHCP パケットをスイッチで受信する場合は、それらのパケットに関するアクションポリシーを設定することができます。スイッチで、DHCP パケットをドロップするか、既存の情報を維持するか、既存の情報をスイッチの中継情報に置き換えることができます。

例

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

ip dhcp snooping verify mac-address

イーサネットヘッダの送信元の MAC **アドレスに対して、**DHCP **パケットにストアされているクライアントのハードウェアのアドレスを検証します。コマンドの前に** ”no” **を置くことにより、デフォルトの設定に戻ります。**

文法

[no] ip dhcp binding verify mac-address

初期設定

Enabled

コマンドモード

Global Configuration

コマンド解説

- MAC **アドレスの検証を有効にして、パケットのイーサネットのヘッダの送信元の** MAC **アドレスが** DHCP **パケットのクライアントのハードウェアのアドレスと異なる場合、パケットは破棄されます。**

例

MAC **アドレスの検証を有効にします。**

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

関連するコマンド

ip dhcp snooping (P205)

ip dhcp snooping vlan (P211)

ip dhcp snooping trust (P212)

ip dhcp snooping vlan

指定した VLAN の DHCP スヌーピング機能を有効にします。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] ip dhcp snooping vlan vlan-id

- vlan-id - 設定された VLAN の ID(有効範囲 : 1-4093)

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- スイッチで DHCP スヌーピングが ip dhcp snooping コマンドを使ってグローバルで有効になっており、このコマンドを用いた指定された VLAN で有効な場合、ip dhcp snooping trust コマンドにより指定した VLAN 内のあらゆる信頼できないポートでは、DHCP パケットフィルタリングが実行されます。
- DHCP スヌーピングがグローバルで無効になっている場合でも、個々の VLAN について DHCP スヌーピングを設定することはできますが、DHCP スヌーピングが再びグローバルで有効にならない限り、そのような変更は適用されません。
- DHCP スヌーピングがグローバルで有効になっている場合に、ある VLAN で DHCP スヌーピングが無効にされると、その VLAN について学習されたすべての動的バインディングがバインディングテーブルから削除されます。

例

VLAN 1 の DHCP スヌーピング機能を有効にします。

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

関連するコマンド

ip dhcp snooping (P205)

ip dhcp snooping trust (P212)

ip dhcp snooping trust

指定したインタフェースを信頼できるインタフェースとして設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] ip dhcp snooping trust

初期設定

インタフェースはすべてアントラストです。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **信頼できるインタフェースとは、ネットワーク内からのメッセージのみを受信するように設定されているインタフェースです。信頼できないインタフェースとは、ネットワークやファイアウォールの外部からのメッセージを受信するように設定されているインタフェースです。**
- DHCP **スヌーピングがグローバルで有効になっており、**VLAN **でも有効になっている場合、**VLAN **内のあらゆる信頼できないポートでは、**DHCP **パケットフィルタリングが実行されます。**
- **信頼できないポートが信頼できるポートに変更されると、そのポートに関連付けられているすべての動的** DHCP **スヌーピングバインディングが削除されます。**
- **スイッチ自体が** DHCP **クライアントである場合のその他の考慮事項として、スイッチがクライアント要求を** DHCP **サーバに送信するときに使用するポートは信頼できるポートとして設定されていなければならないということが挙げられます**

例

port 5 **を信頼できないポートに設定します。**

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

関連するコマンド

ip dhcp snooping (P205)

ip dhcp snooping vlan (P211)

clear ip dhcp snooping database flash

ダイナミックに学習されたスヌーピングエントリをフラッシュメモリを削除します。

コマンドモード

Privileged Exec

例

```
Console(config)#clear ip dhcp snooping database flash
Console(config)#
```

show ip dhcp snooping

DHCP **スヌーピングの設定を表示します。**

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp snooping
Global DHCP Snooping status: disable
DHCP Snooping Information Option Status: disable
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
1
Verify Source Mac-Address: enable
Interface   Trusted
---------- ----------
Eth 1/1     No
Eth 1/2     No
Eth 1/3     No
Eth 1/4     No
Eth 1/5     Yes
..
.
```

show ip dhcp snooping binding

DHCP スヌーピングのバインディングテーブルのエントリを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp snooping binding
MacAddress   IpAddress  Lease(sec)   Type VLAN         Interface
----------------- --------------- ---------- --------------------
11-22-33-44-55-66 192.168.0.99 0 Dynamic-DHCPSNP      1 Eth 1/5
Console#
```

1.10.5 IP ソースガード

IP ソースガードは、手動で設定された IP ソースガードテーブルのエントリまたは（DHCP スヌーピングが有効になっている場合は）DHCP スヌーピングテーブルの動的エントリ（「DHCP スヌーピング」を参照）に基づいてネットワークインタフェースで IP トラフィックをフィルタリングするセキュリティ機能です。IP ソースガードは、ホストが近隣ホストの IP アドレスを利用してネットワークにアクセスしようとした場合に発生するトラフィック攻撃を防ぐために使用することができます。ここでは、IP ソースガードの使用方法について説明します。

コマンド	機能	モード	ページ
ip source-guard binding	ソースガードバインディングテーブルにスタティックアドレスを追加します。	GC	P215
ip source-guard	送信元 IP アドレス、あるいは送信元 IP アドレスおよび対応 MAC アドレスに応じて、インバウンドのトラフィックのフィルタリングを設定します。	GC	P217
ip source-guard maxbinding	インタフェースにバウンド可能なエントリの最大数を設定します。	IC	P219
show ip source-guard	各インタフェース上でソースガードの有効または無効を表示します。	PE	P220
show ip source-guard binding	ソースガードのバインディングテーブルを表示します。	PE	P220

ip source-guard binding

ソースガードのバインディングテーブルにスタティックアドレスを追加します。コマンドの前に "no" を付けることにより、スタティックエントリを削除します。

文法

ip source-guard binding mac-address vlan vlan-id ip-address

interface

no ip source-guard binding mac-address vlan vlan-id

- mac-address - 有効なユニキャスト MAC アドレス
- vlan-id - 設定した VLAN の ID(有効範囲 : 1-4093)
- ip-address - 有効なユニキャストの IP アドレス (タイプ A, B または C)
- interface - ポートインタフェースを指定します。

  ethernet unit/port

  - unit - スタックユニット (有効範囲 : 1-8)
  - port - ポート番号 (有効範囲 : 1-26)

初期設定

No configured entries

コマンドモード

Global Configuration

コマンド解説

- テーブルエントリには、MAC アドレス、IP アドレス、リースタイム、エントリタイプ（Static または Dynamic）、VLAN ID、およびポート ID が含まれます。すべての静的エントリのリースタイムは無期限（テーブルでの値が 0）に設定されます。
- IP ソースガードバインディングテーブルに入力された静的エントリのリースタイムは、自動的に無期限に設定されます。DHCP スヌーピングによって学習される動的エントリは、DHCP サーバ自体によって設定されます。
- 静的バインディングは、以下のように処理されます。
  - 同じ VLAN ID と MAC アドレスを含むエントリが存在しない場合、「静的 IP ソースガードバインディング」というタイプを使用して新しいエントリがバインディングテーブルに追加されます。
  - 同じ VLAN ID と MAC アドレスを含むエントリが存在し、エントリのタイプが静的 IP ソースガードバインディングである場合、新しいエントリによって古いエントリが置き換えられます。
  - 同じ VLAN ID と MAC アドレスを含むエントリが存在し、エントリのタイプが動的 DHCP スヌーピングバインディングである場合、新しいエントリによって古いエントリが置き換えられ、エントリのタイプが静的 IP ソースガードバインディングに変更されます。
  - 静的バインディングについてはユニキャストアドレスのみが受け入れられます。

例

port 5 のスタティックソースガードのバインディングを設定します。

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1
192.168.0.99
interface ethernet 1/5
Console(config-if)#
```

関連するコマンド

ip source-guard (P217)

ip dhcp snooping (P213)

ip dhcp snooping vlan (P211)

ip source-guard

送信元 IP アドレスまたは送信元 IP アドレスとそれに対応する MAC アドレスの組み合わせに基づいてインバウンドトラフィックがフィルタリングされるようにスイッチを設定します（デフォルト : None）。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

ip source-guard {sip | sip-mac}

no ip source-guard

- sip - バインディングテーブルにストアされている IP アドレスに応じて、トラフィックをフィルタリングします。
- sip-mac - IP アドレス、バインディングテーブルにストアされている対応の MAC アドレスをフィルタリングします。

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- ネットワークやファイアウォールの外部からメッセージを受信し、そのために近隣ホストの IP アドレスを利用しようとするホストによって引き起こされるトラフィック攻撃にさらされる可能性がある非セキュアポートでトラフィックをフィルタリングする場合は、IP ソースガードを使用することができます。
- IP ソースガードモードを「SIP」（送信元 IP）または「SIP-MAC」（送信元 IP と送信元 MAC）に設定すると、選択したポートで IP ソースガード機能が有効になります。「SIP」オプションは、VLAN ID、送信元 IP アドレス、およびポート番号をバインディングテーブル内のすべてのエントリと照らし合わせてチェックする場合に使用します。「SIP-MAC」オプションは、それらのパラメータに加え、送信元 MAC アドレスをチェックする場合に使用します。no ip source guard コマンドを使って、選択したポートの機能を無効にします。
- IP ソースガードバインディングテーブルに ip source-guard binding コマンドで入力された静的エントリのリースタイムは、自動的に無期限に設定されます。DHCP スヌーピングによって学習される動的エントリは DHCP サーバ自体によって設定されます。
- IP ソースガードを有効にすると、DHCP スヌーピングによって学習された動的エントリ（「DHCP スヌーピング」（p.360）▲を参照）、または IP ソースガードバインディングテーブルで設定されている静的アドレスに基づいて、トラフィックがフィルタリングされます。
- IP ソースガードが有効になっている場合、インバウンドパケットの IP アドレス（「SIP」オプションが選択されている場合）または着信パケットの IP アドレスとそれに対応する MAC アドレスの両方（「SIPMAC」オプションが選択されている場合）がバインディングテーブルと照らし合わせてチェックされます。マッチするエントリがない場合、パケットはドロップされます。
- フィルタリングルールは、以下のように実装されます。

- DHCP スヌーピングが無効になっている場合（p.363 ▲を参照）、IP ソースガードでは、VLAN ID、送信元 IP アドレス、ポート番号、および送信元 MAC アドレス（「SIP-MAC」オプションが選択されている場合）がチェックされます。マッチするエントリがバインディングテーブルで検出され、エントリタイプが静的 IP ソースガードバンディングである場合は、パケットが転送されます。
- DHCP スヌーピングが有効になっている場合、IP ソースガードでは、VLAN ID、送信元 IP アドレス、ポート番号、および送信元 MAC アドレス（「SIP-MAC」オプションが選択されている場合）がチェックされます。マッチするエントリがバインディングテーブルで検出され、エントリタイプが静的 IP ソースガードバンディングまたは動的 DHCP スヌーピングバインディングである場合は、パケットが転送されます。
- まだ IP ソースバインディングが設定されていない（IP ソースガードバインディングテーブルの静的エントリと DHCP スヌーピングによって学習される動的エントリのどちらも設定されていない）インタフェースで IP ソースガードが有効になっている場合、そのポートでは DHCP パケット以外のすべての IP トラフィックがドロップされます。
- スタティックバインディングには、ユニキャストアドレスのみ有効です。

例

ここでは、IP source guard on port 5 の IP ソースガードは有効です。

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

関連するコマンド

ip source-guard binding (P215)

ip dhcp snooping (P205)

ip dhcp snooping vlan (P211)

ip source-guard max-binding

インタフェースに送信可能なエントリの最大数を設定します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

ip source-guard max-binding number

no ip source-guard max-binding

- number - **バインディングテーブルのインタフェースにマッピング可能な** IP **アドレスの最大数** (**有効範囲** : 1-5)

初期設定

5

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **バインディングテーブルでインタフェースにマップできるアドレスエントリの最大数を設定します。この場合の最大数は、**DHCP **スヌーピングによって検出される動的エントリ（「**DHCP **スヌーピング」を参照）と** ipsource-guard **コマンドにより設定された静的エントリ（「**IP **ソースガードの静的バインディングの設定」を参照）の両方を含めたものです。**

例

ここでは、バインディングに許可されているエントリの最大数を設定します。

```
table for port 5 to one entry.
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
Console(config-if)#
```

show ip sourceguard

各インタフェースのソースガードが有効か、無効化を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip source-guard
Interface Filter-type Max-binding
--------- ----------- -----------
Eth 1/1 DISABLED 5
Eth 1/2 DISABLED 5
Eth 1/3 DISABLED 5
Eth 1/4 DISABLED 5
Eth 1/5 SIP 1
Eth 1/6 DISABLED 5
...
```

show ip sourceguard binding

ソースガードのバインディングテーブルを表示します。

文法

show ip source-guard binding [dhcp-snooping | static]

- dhcp-snooping - DHCP **スヌーピングコマンドで設定したダイナミックエントリを表示します。**
- static - ip source-guard binding **コマンドで設定したスタティックエントリを表示します。**

コマンドモード

Privileged Exec

例

```
Console#show ip source-guard binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
----------------- --------------- ---------- --------------------
---- --------
11-22-33-44-55-66 192.168.0.99 0 Static 1 Eth 1/5
Console#
```

1.10.6 ARP インスペクション

ARP インスペクションは、アドレス解決プロトコルパケットについて MAC アドレスのバインディングの妥当性を検証するセキュリティ機能です。ARP インスペクションは、ある種の「中間者」攻撃の足掛かりとなる MAC アドレスと IP アドレスとのバインディングが無効な ARP トラフィックに対する防御策を提供します。そのための方法として、ローカルの ARP キャッシュが更新される前、またはパケットが該当の宛先に転送される前に、すべての ARP 要求と APR 応答をインターセプトし、それらのパケットをそれぞれ検証します。無効な ARP パケットはドロップされます。

ARP インスペクションでは、DHCP スヌーピングバインディングデータベース（「DHCP スヌーピング設定」を参照）という、信頼できるデータベースに保存されている有効な IP アドレスと MAC アドレスとのバインディング情報に基づいて、ARP パケットの妥当性が判別されます。このデータベースは、DHCP スヌーピングによって作成されます（ただし、スイッチで DHCP スヌーピングがグローバルで有効になっており、必要な VLAN で有効になっていなければなりません）。また、ARP インスペクションでは、静的に設定されたアドレスをもつホストのユーザ設定の ARP ACL（「ARP ACL の設定」を参照）と照らし合わせて ARP パケットの妥当性を検証することもできます。

コマンド	機能	モード	ページ
ip arp inspection	ARP インスペクションをグローバルで有効にします。	GC	P222
ip arp inspection filter	ARP の ACL を指定して、1 つ以上の VLAN に適用します。	GC	P223
ip arp inspection log-buffer logs	log メッセージに保存されているエントリの最大値、およびメッセージの送信速度を設定します。	GC	P224
ip arp inspection validate	ARP パケットのアドレスの構成内容の追加検証を指定します。	GC	P225
ip arp inspection vlan	指定した VLAN、または VLAN の範囲の ARP インスペクションを有効にします。	GC	P226
ip arp inspection limit	受信した ARP パケットの帯域制御を設定します。	IC	P227
ip arp inspection trust	ポートを信頼できるポートとして設定することにより、APR インスペクションから除外します。	IC	P228
show ip arp inspection configuration	ARP インスペクションのグローバルコンフィグレーション設定を表示します。	PE	P228
show ip arp inspection interface	ポートのトラストステータス、およびインスペクションの帯域制御を表示します。	PE	P229
show ip arp inspection log	log にストアされているエントリ情報（関連のある VLAN、ポート、およびアドレスの構成内容を含む）を表示します。	PE	P229
show ip arp inspection statistics	処理中の ARP パケット数、何らかの理由で破棄されたパケット数の統計情報を表示します。	PE	P230
show ip arp inspection vlan	VLAN のコンフィグレーションの設定（ARP インスペクションのステータス、ARP の ACL 名、DHCP スヌーピングデータベースは ACL 検証が完了後に使用する場合）を表示します。	PE	P230

ip arp inspection

ARP インスペクションをグローバルで有効にします。コマンドの前に ”no” を置くことにより、デフォルトの設定に戻ります。

文法

[no] ip arp inspection

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- デフォルトでは、ARP インスペクションは、グローバルでも、すべての VLAN でも無効になっています。
  - ARP インスペクションは、グローバルで有効になっている場合には、ip arp inspection vlan コマンドにより有効になっている VLAN でのみ、アクティブになります。
  - ARP インスペクションがグローバルで有効になっている場合、ARP インスペクションが有効になっている VLAN では、すべての ARP 要求パケットと ARP 応答パケットが CPU にリダイレクトされ、それらのパケットのスイッチング動作は ARP インスペクションエンジンによって処理されます。
  - ARP インスペクションは、グローバルで無効になっている場合には、すべての VLAN（ARP インスペクションが有効になっている VLAN を含む）で無効になります。
  - ARP インスペクションが無効になっている場合、すべての ARP 要求パケットと ARP 応答パケットは ARP インスペクションエンジンをバイパスし、それらのパケットのスイッチング動作は他のすべてのパケットのものと一致するようになります。
  - グローバル ARP インスペクションを無効にしてから再び有効にしても、いずれの VLAN の ARP インスペクション設定にも影響しません。
  - ARP インスペクションがグローバルで無効になっている場合でも、個々の VLAN の ARP インスペクションを設定することができます。そのような設定変更は、ARP インスペクションが再びグローバルで有効にされた場合にのみ、アクティブになります。

例

```
Console(config)#ip arp inspection
Console(config)#
```

ip arp inspection filter

ARP の ACL を指定して、１つまたは複数の VLAN に適用します。コマンドの前に ”no” を置くことにより、ACL バインディングを取り除きます。

文法

ip arp inspection filter arp-acl-name vlan {vlan-id | vlan-range}

[static]

- arp-acl-name - ARP の ACL 名 (最大長 : 16 文字)
- vlan-id - VLAN ID (有効範囲 : 1-4093)
- vlan-range- VLAN の連続的な範囲はハイフンを使用し、または各々のエントリをもつランダムな VLAN のグループはコンマで分けます。
- static - ARP パケットは指定した ACL のみの確認を行い、DHCP スヌーピングのデータベース内のアドレスのバインディングはチェックされません。

初期設定

ARP の ACL はその VLAN にもバインドされません。

スタティックモードは有効ではありません。

コマンドモード

Global Configuration

コマンド解説

- スタティックモードを有効にする場合は、APR パケットを指定した ARP の ACL と比較します。permit/deny ルールにおいて IP-to-MAC アドレスバインディングが一致すると、ルールに応じてパケットは処理されます。ACL ルールのいずれにも一致しないパケットは破棄されます。DHCP スヌーピングデータベースのアドレスのバインディングは検証の対象にはなりません。
- スタティックモードが有効でない場合は、パケットは指定の ARP の ACL に対してまず検証されます。deny ルールに一致したパケットは破棄され、すべて DHCP スヌーピングデータベースのアドレスのバインディングに対して残りのパケットを検証します。

例

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

ip arp inspection log-buffer logs

log メッセージに保存されているエントリの最大値、メッセージの送信速度を設定します。コマンドの前に ”no” を置くことにより、デフォルトの設定に戻ります。

文法

ip arp inspection log-buffer logs message-number interval seconds

no ip arp inspection log-buffer logs

- message-number - log メッセージに保存されているエントリの最大値 (有効範囲 : 0-256、この場合、「0」は保存されているイベントなしを意味します。)
- seconds - log メッセージの送信間隔 (有効範囲 : 0-86400)

初期設定

Message Number: 5

Interval: 1 second

コマンドモード

Global Configuration

コマンド解説

- ARP インスペクションは、本機でコマンドを使って実行する前に、ip arp inspection コマンドで有効にしてください。
- ARP インスペクションのログ記録は、デフォルトで有効になっており、無効にすることはできません。
- 管理者は、ログファシリティレートを設定することができます。
- スイッチでパケットがドロップされる場合は、エントリがログバッファに保存され、システムメッセージがレート制御ベースで生成されます。システムメッセージが生成された後、エントリがログバッファからクリアされます。
- それぞれのログエントリには、受信先 VLAN、ポート番号、送信元 IP アドレスと宛先 IP アドレス、送信元 MAC アドレスと宛先 MAC アドレスなどのフロー情報が含まれます。
- 同一の有効な ARP パケットが複数同時に同じ VLAN で受信された場合は、ログファシリティによってログバッファのエントリが 1 つだけ生成され、対応するシステムメッセージが 1 つ生成されます。
- ログバッファが満杯になっている場合は、最も古いエントリが最も新しいエントリに置き換えられます。

例

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

ip arp inspection validate

ARP パケットのアドレスの構成内容の追加検証を指定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

ip arp inspection validate {dst-mac [ip] [src-mac] | ip [src-mac]

| src-mac}

no ip arp inspection validate

- dst-mac - イーサネットヘッダ内の宛先 MAC アドレスを ARP パケット本体内のターゲット MAC アドレスと照らし合わせてチェックします。このチェックは ARP 応答に対して実行されます。有効にすると、異なる MAC アドレスが含まれているパケットは、無効なものとして分類され、ドロップされます。
- ip - ARP パケット本体に無効な IP アドレスおよび予期されない IP アドレスが含まれていないかチェックします。そのようなアドレスとして、例えば、0.0.0.0、255.255.255.255、およびすべての IP マルチキャストアドレスなどがあります。送信者 IP アドレスはすべての ARP 要求と ARP 応答でチェックされますが、ターゲット IP アドレスは ARP 応答でのみチェックされます。
- src-mac - イーサネットヘッダ内の送信元 MAC アドレスを ARP パケット本体内の送信者 MAC アドレスと照らし合わせてチェックします。このチェックは ARP 要求と ARP 応答の両方に対して実行されます。有効にすると、異なる MAC アドレスが含まれているパケットは、無効なものとして分類され、ドロップされます。

初期設定

追加の検証は実施されません。

コマンドモード

Global Configuration

コマンド解説

- デフォルト設定では、ARP インスペクションが ARP の ACL、または DHCP スヌーピングデータベースで指定されている IP-to-MAC アドレスバインディングかのみを検証します。

例

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

ip arp inspection vlan

指定した VLAN、または VLAN の範囲の ARP インスペクションを有効にします。コマンドの前に "no" を付けることにより機能を無効にします。

文法

[no] ip arp inspection vlan {vlan-id | vlan- 有効範囲 }

- vlan-id - VLAN ID. (有効範囲 : 1-4093)
- vlan-range- VLAN の連続的な範囲はハイフンを使用し、または各々のエントリをもつランダムな VLAN のグループはコンマで分けます。

初期設定

VLAN をすべて無効にします。

コマンドモード

Global Configuration

コマンド解説

- ARP インスペクションは、グローバルで有効になっている場合には、ip arp inspection コマンドにより有効になっている VLAN でのみ、アクティブになります。
- ARP インスペクションがグローバルで有効になっている場合、ARP インスペクションが有効になっている VLAN では、すべての ARP 要求パケットと ARP 応答パケットが CPU にリダイレクトされ、それらのパケットのスイッチング動作は ARP インスペクションエンジンによって処理されます。
- ARP インスペクションは、グローバルで無効になっている場合には、すべての VLAN（ARP インスペクションが有効になっている VLAN を含む）で無効になります。
- ARP インスペクションが無効になっている場合、すべての ARP 要求パケットと ARP 応答パケットは ARP インスペクションエンジンをバイパスし、それらのパケットのスイッチング動作は他のすべてのパケットのものと一致するようになります。
- グローバル ARP インスペクションを無効にしてから再び有効にしても、いずれの VLAN の ARP インスペクション設定にも影響しません。
- ARP インスペクションがグローバルで無効になっている場合でも、個々の VLAN の ARP インスペクションを設定することができます。そのような設定変更は、ARP インスペクションが再びグローバルで有効にされた場合にのみ、アクティブになります。

例

```
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

ip arp inspection limit

ポートで受信する ARP **パケットの帯域制御を設定します。コマンドの前に** ”no” **を付けることにより、デフォルト設定に戻ります。**

文法

ip arp inspection limit {rate pps | none}

no ip arp inspection limit

- pps - **毎秒ごとの** CPU **により処理可能な** ARP **パケットの上限** (**有効範囲** : 0-2048**、この場合、「**0**」は転送可能な** ARP **パケットがないことを意味します。)**
- none - CPU **により処理可能な** ARP **パケットに制限なし。**

初期設定

15

コマンドモード

Interface Configuration (Port)

コマンド解説

- **信頼しているポートにも、信頼性のないポートにも適用します。**
- ARP **パケットの受信が設定した上限を超えると、その分のパケットをすべて破棄します。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit 150
Console(config-if)#
```

ip arp inspection trust

ポートを信頼されるポートとして設定することにより、ARP 検査から免除します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] ip arp inspection trust

初期設定

Untrusted

コマンドモード

Interface Configuration (Port)

コマンド解説

- 信頼性のないポートで受信したパケットには ARP 検査および追加の検証チェックを行います。信頼性のあるポートで受信したパケットがこれらのチェックにすべてパスすると、通常のスイッチングルールに応じて転送されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

show ip arp inspection configuration

ARP 検査のグローバルの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection configuration
ARP inspection global information:
Global IP ARP Inspection status : disabled
Log Message Interval : 10 s
Log Message Number : 1
Need Additional Validation(s) : Yes
Additional Validation Type : Destination MAC address
Console#
```

show ip arp inspection interface

ポートのトラスト状態、および ARP **検査の帯域制御を表示します。**

文法

show ip arp inspection interface [interface]

interface

ethernet unit/port

- unit - **スタックユニット** (**有効範囲** : 1-8)
- port - **ポート番号** (**有効範囲** : 1-26)

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection interface ethernet 1/1
Port Number Trust Status Limit Rate (pps)
------------- -------------------- ------------------------------
Eth 1/1 trusted 150
Console#
```

show ip arp inspection log

関連のある VLAN**、ポート、アドレス構成要素などのログに保存されているエントリ情報を表示します。**

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection log
Total log entries number is 1
Num VLAN Port Src IP Address Dst IP Address Src MAC Address Dst
MAC Address
--- ---- ---- -------------- -------------- --------------- -----
1 1 11 192.168.2.2 192.168.2.1 00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-
FF
Console#
```

show ip arp inspection statistics

処理 / 破棄された ARP **パケット数の統計情報を表示します。**

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection log
Total log entries number is 1
Num VLAN Port Src IP Address Dst IP Address Src MAC Address Dst
MAC Address
--- ---- ---- -------------- -------------- --------------- -----
------
Console#show ip arp inspection statistics
ARP packets received before rate limit        : 150
ARP packets dropped due to rate limt          : 5
Total ARP packets processed by ARP Inspection : 150
ARP packets dropped by additional validation (source MAC address)
: 0
ARP packets dropped by additional validation (destination MAC
address)                                      : 0
ARP packets dropped by additional validation (IP address) : 0
ARP packets dropped by ARP ACLs               : 0
ARP packets dropped by DHCP snooping          : 0

Console#
```

show ip arp inspection vlan

ARP **検査ステータス、**ARP **の** ACL **名の設定情報が表示されます（**ARP **の** ACL **検証が完了後は** DHCP **スヌーピングデータベースが使用されます)。**

文法

show ip arp inspection vlan [vlan-id | vlan- **有効範囲**]

- vlan-id - VLAN ID (**有効範囲** : 1-4093)
- vlan-range- VLAN **の連続的な範囲はハイフンを使用し、または各々のエントリをもつランダムな** VLAN **のグループはコンマで分けます。**

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection vlan 1
VLAN ID DAI Status ACL Name ACL Status
-------- --------------- -------------------- -------------------
-
1 disabled sales static
```

1.11 ACL（Access Control Lists）

Access Control Lists (ACL) は IP アドレス、プロトコル、TCP/UDP ポート番号よる IP パケットへのパケットフィルタリングを提供します。

入力されるパケットのフィルタリングを行うには、初めにアクセスリストを作成し、必要なルールを追加します。その後、リストに特定のポートをバインドします。

コマンド	機能	ページ
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	P232
MAC ACLs	ハードウェアアドレス、パケットフォーマット、イーサネットタイプに基づく ACL の設定	P239
ACL Information	ACL 及び関連するルールの表示。各ポートの ACL の表示	P243

1.11.1 IP ACL コマンド

この節のコマンドで、IP アドレス、TCP/UDP ポート番号、プロトコルタイプ、TCP コントロールコードを基にした ACL の設定を行います。
IP ACL を設定するには、最初に必要な許可、または拒否ルールを含むアクセスリストを作成することから始め、その後にアクセスリストを 1 つ以上のポートにバインドします。

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	P233
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	P234
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	P235
show ip access-list	設定済み IP ACL のルールの表示	PE	P236
ip access-group	IP ACL へのポートの追加	IC	P237
show ip access-group	IP ACL に指定したポートの表示	PE	P238

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。コマンドの前に "no" を置くことで特定の 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（最大 16 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 新しい ACL を作成した場合や、既存の ACL の設定モードに移行した場合、"permit" 又は "deny" コマンドを使用し、新しいルールを追加します。ACL を作成するには、最低 1 つのルールを設定する必要があります。
- ルールを削除するには "no permit" 又は "no deny" コマンドに続けて設定済みのルールを入力します。
- 1 つの ACL には最大 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（P234）
ip access-group（P237）
show ip access-list（P236）

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。コマンドの前に "no" を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 — すべての IP アドレス
- source — ソース IP アドレス
- bitmask — 一致するアドレスビットを表す 10 進数値
- host — 特定の IP アドレスを指定

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（P233）

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。コマンドの前に** "no" **を置くことでルールの削除を行います。**

文法

[no] {permit | deny} [protocol-number | udp]
{any | source address-bitmask | host source}
{any | destination address-bitmask | host destination}
[precedence precedence] [tos tos] [dscp dscp]
[source-port sport [bitmask]] [destination-port dport [port-bitmask]]
[no] {permit | deny} tcp
{any | source address-bitmask | host source}
{any | destination address-bitmask | host destination}
[precedence precedence] [tos tos] [dscp dscp]
[source-port sport [bitmask]] [destination-port dport [port-bitmask]]
[control-flag control-flags flag-bitmask]

- protocol-number — **特定のプロトコル番号（範囲：**0-255**）**
- source — **ソース** IP **アドレス**
- destination — **ディスティネーション** IP **アドレス**
- address-bitmask — **アドレスビットマスク**
- host — **特定の** IP **アドレスの指定**
- precedence— **優先レベル（範囲：**0-7**）**
- tos — ToS **レベル（範囲：**0-7**）**
- dscp — DSCP **プライオリティレベル**（0-63）
- 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**）**
- port-bitmask — **ポートビットマスク**
- control-flags —TCP**ヘッダの**14**バイト内フラッグビットを指定する**10**進数（範囲：**0-63**）**
- flag-bitmask — **フラッグビットマスク**

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、ディスティネーション TCP ポート番号 80 のクラス C アドレス 192.168.1.0 からすべてのディスティネーションアドレスへの TCP パケットを許可します。

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
destination-port 80
Console(config-ext-acl)#
```

関連するコマンド

access-list ip（P233）

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#
```

関連するコマンド

permit, deny（P234）
ip access-group（P237）

ip access-group

IP ACL へのポートのバインドを行います。コマンドの前に "no" を置くことでポートを外します。

文法

[no] ip access-group acl_name in

- acl_name — 最大 16 文字
- in — 入力パケットへのリスト

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)#interface ethernet 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 （P236）

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 (P237)

1.11.2 MAC ACL コマンド

コマンド	機能	モード	ページ
access-list mac	MAC ACL の作成と configuration mode への移行	GC	P239
permit,deny	ソース又はディスティネーションアドレス、パケットフォーマット、イーサネットタイプに基づくフィルタリング	MAC-ACL	P240
show mac access-list	設定済み MAC ACL のルールの表示	PE	P242
mac access-group	MAC ACL へのポートの追加	IC	P242
show mac access-group	MAC ACL に指定したポートの表示	PE	P243

access-list mac

MAC アドレスリストを追加し、MAC ACL 設定モードに移行します。コマンドの前に "no" を置くことで指定した ACL を削除します。

文法

access-list mac acl_name
no access-list mac acl_name

- acl_name — ACL 名（最大 16 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 新しい ACL を作成した場合や、既存の ACL の設定モードに移行した場合、"permit" 又は "deny" コマンドを使用し、新しいルールを追加します。ACL を作成するには、最低 1 つのルールを設定する必要があります。
- ルールを削除するには "no permit" 又は "no deny" コマンドに続けて設定済みのルールを入力します。
- 1 つの ACL には最大 32 個のルールが設定可能です。

例

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

関連するコマンド

permit, deny (MAC ACL)（P240）
mac access-group（P242）
show mac access-list（P242）

permit,deny（MAC ACL）

MAC ACL へのルールの追加を行います。MAC ソース / ディスティネーションアドレス、イーサネットプロトコルタイプによりフィルタリングを行います。コマンドの前に "no" を置くことでルールを削除します。

文法

[no] {permit | deny}
{any |host source|source address-bitmask}
{any | host destination | destination address-bitmask}
[vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]

[注意]　初期設定は Ethernet2 パケットです。

[no] {permit | deny} tagged-eth2
{any |host source|source address-bitmask}
{any | host destination | destination address-bitmask}
[vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]

[no] {permit | deny} untagged-eth2
{any |host source|source address-bitmask}
{any | host destination | destination address-bitmask}
[ethertype protocol [protocol-bitmask]

[no] {permit | deny} tagged-802.3
{any |host source|source address-bitmask}
{any | host destination | destination address-bitmask}
[vid vid vid-bitmask]

[no] {permit | deny} untagged-802.3
{any |host source|source address-bitmask}
{any | host destination | destination address-bitmask}

protocol-number — 特定のプロトコル番号（範囲：0-255）

- tagged-eth2 — タグ付きイーサネット 2 パケット
- untagged-eth2 — タグ無しイーサネット 2 パケット
- tagged-802.3 — タグ付きイーサネット 802.3 パケット
- untagged-802.3 — タグ無しイーサネット 802.3 パケット
- any — すべての MAC ソース / ディスティネーションアドレス
- host — 特定の MAC アドレス
- source — ソース MAC アドレス
- destination — ビットマスクを含むディスティネーション MAC アドレス範囲

- address-bitmask — MAC アドレスのビットマスク（16 進数）
- vid — VLAN ID（範囲：1-4093）
- vid — VLAN ビットマスク（範囲：1-4093）
- protocol — イーサネットプロトコル番号（範囲：600-fff 16 進数）
- protocol -bitmask— プロトコルビットマスク（範囲：600-fff 16 進数）

初期設定

なし

コマンドモード

MAC ACL

コマンド解説

- 新しいルールはリストの最後に追加されます。
- イーサネットタイプオプションは Ethernet II のフィルタにのみ使用します。
- イーサネットプロトコルタイプのリストは RFC 1060 で設定されていますが、一般的なタイプは以下の通りです。
  - — 0800(IP)
  - — 0806(ARP)
  - — 8137(IPX)

例

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

関連するコマンド

access-list mac (P239)

show mac access-list

MAC ACL のルールを表示します。

文法

show mac access-list [acl_name]

- acl_name — ACL 名（最大 16 文字）

コマンドモード

Privileged Exec

例

```
Console#show mac access-list
MAC access-list jerry:
   permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

関連するコマンド

permit, deny（P240）
mac access-group（P242）

mac access-group

MAC ACL へのポートのバインドを行います。コマンドの前に "no" を置くことでポートを外します。

文法

[no] mac access-group acl_name in

- acl_name— ACL 名（最大 16 文字）
- in — 入力パケットへのリスト

コマンドモード

Privileged Exec

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

関連するコマンド

show mac access-list（P242）

show mac access-group

MAC ACL に指定されたポートを表示します。

コマンドモード

Privileged Exec

例

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
Console#
```

関連するコマンド

mac access-group （P242）

1.11.3 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	P242
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	P243

show access-list

すべての ACL とユーザ設定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

コマンド解説

- ACL がインタフェースに結合されると、ルールが表示される順序は関連するマスクによって決定されます。

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 Exec

例

```
Console#show access-group
Interface ethernet 1/1
 IP access-list jerry in
.
.
.
Interface ethernet 1/26
 IP access-list jerry in
Console#
```

1.12 インタフェース設定モード

コマンド	機能	モード	ページ
Interface Configuration			
interface	本機の DHCP クライアント ID の指定	GC	P246
alias	インタフェースのエリアス名の設定	IC	P247
description	指定したインタフェースへのコメントや解説の追加	IC	P248
speed-duplex	オートネゴシエーション有効時の通信速度、通信方式の設定	IC	P249
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	P250
capabilities	オートネゴシエーション有効時の通信速度、通信方式の設定	IC	P251
flowcontrol	インタフェースへのフローコントロール設定	IC	P252
media-type	コンボポートの強制ポートタイプの設定	IC	P253
shutdown	インタフェースを無効化	IC	P254
switchport mtu	インタフェースの最大伝送単位を設定	IC	P255
switchport packet-rate	ブロードキャスト帯域制御の設定	IC	P256
clear counters	インタフェースの統計情報のクリア	PE	P257
show interfaces status	インタフェースの設定状況を表示	NE,PE	P258
show interfaces counters	インタフェースの統計情報の表示	NE,PE	P259
show interfaces switchport	インタフェースの管理、運用状況の表示	NE,PE	P261
Cable Diagnostics			
test cable-diagnostics dsp	指定ポートのケーブル診断の実行	PE	P263
test loop internal	指定ポートの内部ループバックテストの実行	PE	P264
show cable-diagnostics dsp	ケーブル診断テストの結果を表示	PE	P263
show loop internal	ループバックテストの結果を表示	PE	P266

interface

インタフェースタイプを設定したり、インタフェースの config モードに入ります。トランクの場合は、コマンドの前に ”no” を置くことによりインタラクティブインタフェースを取り除きます。レイヤーの 3 VLAN の場合はコマンドの前に ”no” を置くことによりレイヤ 2 に変更します。

文法

[no] interface interface

interface

ethernet unit/port-list

- unit - Stack unit. (有効範囲 :1-8)
- port-list - 物理ポート番号、ポート番号のリスト。非連続のポート番号をコンマ / スペースで区別したり、ハイフンを使ってポート番号の範囲を指定します (有効範囲 :1-26)。
- port-channel channel-id (有効範囲 :1-32)
- vlan vlan-id (有効範囲 :1-4093)

初期設定

None

コマンドモード

Global Configuration

例

port 4 を指定するには、以下のコマンドを入力します。

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

alias

インタフェースのエイリアス名を設定します。コマンドの前に "no" を置くことにより、エイリアス名を削除します。

文法

alias string

no alias

- string - ニーモニック名（インタフェースに接続されている内容を記憶可能）(有効範囲 :1-64 文字)

初期設定

None

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- running-configuration ファイルのエイリアスが表示されます。ネットワーク管理者が WAN インタフェースのオブジェクトにストアしている値の例は、インタフェースの Telco(回路番号)/ 識別子です。

例

以下の例では、port 4 にエイリアスを追加します。

```
Console(config)#interface ethernet 1/4
Console(config-if)#alias finance
Console(config-if)#
```

description

指定したインタフェースへのコメントや解説の追加を行います。コマンドの前に "no" **を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。コマンドの前に "no" **を置くことにより、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。また、**"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下さい。**
- "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（P250）
capabilities（P251）

negotiation

各ポートのオートネゴシエーションを有効にします。コマンドの前に "no" **を置くことでオートネゴシエーションを無効にします。**

文法

negotiation
no negotiation

初期設定

有効 (Enabled)

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **オートネゴシエーションが有効になっている場合、**"capabilities" **コマンドに指定された内容に基づき、最適な通信方法を選択します。オートネゴシエーションが無効の場合には** "speed-duplex" **コマンドと** "flowcontrol" **コマンドを使用して手動で通信方式を設定する必要があります。**
- **オートネゴシエーションが無効の場合には** RJ-45 **ポートの** MDI-MDI-X **自動認識機能も無効となります。**

例

本例では 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（P251）
speed-duplex（P249）

capabilities

オートネゴシエーション時のポートの通信方式を設定します。

"no" **を前に置きパラメータを設定することで指定したパラメータの値を削除します。パラメータを設定せず** "no" **を前に置いた場合には初期設定に戻ります。**

文法

capabilities [1000full | 100full | 100half | 10full | 10half | flowcontrol | symmetric]

no capabilities { 1000full | 100full | 100half | 10full | 10half | flowcontrol | symmetric }

- 1000full — 1000Mbps full-duplex **通信**
- 100full — 100Mbps full-duplex **通信**
- 100half — 100Mbps half-duplex **通信**
- 10full — 10Mbps full-duplex **通信**
- 10half — 10Mbps half-duplex **通信**
- flowcontrol — flow control **サポート**
- symmetric — **フローコントロールからポーズフレームを送受信（本機では**symmetric **ポーズフレームのみがサポートされています）** < **ギガビット環境のみ** >

初期設定

- 100BASE-TX：10half, 10full, 100half, 100full
- 1000BASE-T：10half, 10full, 100half, 100full, 1000full
- SFP：1000full

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- "negotiation" **コマンドを使用しオートネゴシエーションが有効になっている場合、** "capabilites" **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 **に設定しています。**

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#
```

flow control

フローコントロールを有効にします。コマンドの前に "no" を置くことでフローコントロールを無効にします。

文法

flowcontrol
no flowcontrol

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- フローコントロールを使用するとスイッチのバッファ容量がいっぱいになった場合に通信のロスが発生するのを防ぐことができます。フローコントロールを有効にした場合、full-duplex では IEEE802.3x 準拠、half-duplex ではバックプレッシャを用いてフローコントロールを行います。"negotiation" コマンドを使用しオートネゴシエーションを有効にした場合、"capabilities" コマンドによりフローコントロールを使用するか決定されます。オートネゴシエーション時にフローコントロールを有効にするためには各ポートの機能 (Capabilities) に "flowcontrol" を含める必要があります。
- flowcontrol" コマンド又は "no flowcontrol" コマンドを使用してフローコントロールを固定設定する場合には、"no negotiation" コマンドを使用してオートネゴシエーションを無効にする必要があります。
- ハブ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 （P250）
capabilities (flowcontrol, symmetric)（P251）

media-type

21-26 番ポートの強制 / 優先設定を行ないます。コマンドの前に "no" を置くことで初期設定に戻ります。

文法

media-type mode

no media-type

- mode
  - copper-forced — 標準の RJ-45 ポートを使用
  - sfp-forced — オプションの SFP ポートを使用（モジュールが搭載されていない場合も含む）
  - sfp-preferred-auto — RJ-45 ポートのリンクが有効な場合、RJ-45 ポートを優先

初期設定

sfp-preferred-auto

コマンドモード

Interface Configuration (Ethernet)

例

本例では 5 番ポートを無効にしています。

```
Console(config)#interface ethernet 1/48
Console(config-if)#media-type copper-forced
Console(config-if)#
```

shutdown

インタフェースを無効にします。コマンドの前に "no" **を置くことでインタフェースを有効にします。**

文法

shutdown
no shutdown

初期設定

すべてのインタフェースが有効になっています。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **コリジョンの発生などによる異常な動作を回避するなどの目的や、セキュリティの目的でポートを無効にすることができます。問題が解決した場合や、ポートを使用する場合には再度ポートを有効にすることができます。**

例

本例では 5 **番ポートを無効にしています。**

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

switchport mtu

ギガビット、10 ギガビットイーサネットポート、あるいはトランク間のレイヤ 2 パケットに対応可能な MTU(maximum transfer unit) を設定します。コマンドの前に ”no” を置くことにより、デフォルトの設定に戻ります。

文法

switchport mtu size

no switchport mtu

- size - ギガビットまたは 10 ギガビットイーサネットのポートあるいはトランクの最大転送単位（MTU: Maximum Transmission Unit）（範囲 : 1,500 ～ 9,216 bytes）。

初期設定

1518 bytes

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- jumbo frame コマンドを使って、ギガビットおよび 10 ギガビットすべてのイーサネットポートのジャンボフレームを有効 / 無効にします。特定のインタフェースの MTU を設定するには、ジャンボフレームを有効にして、コマンドを使って MTU の必要なサイズをしてしてください。
- 設定済みポートの MTU に対するパケットサイズの比較では、着信パケットのサイズのみが考慮されます。また、この比較は、イングレスポートがタグ付きポートであるか QinQ イングレスポートであるかということに影響されません。つまり、その他のすべてのサイズ（例えば、チップによって追加される 4bytes のタグ付きフィールドなど）は、設定されている MTU に対するエグレスパケットのサイズの比率を計算するときには考慮されないということです。
- 外部デバイスからスイッチへの ping 時には、イーサネットヘッダ用に追加される情報のため、パケットサイズがタグなしパケットの場合は少なくとも 42bytes、タグ付きパケットの場合は 46 bytes 増加することがあります。調整されたフレームサイズが設定済みポートの MTU を超える場合、スイッチは ping メッセージに応答しません。
- 他のトラフィックタイプについては、全体的なフレームサイズの計算方法は、追加ヘッダフィールド SA(6)+DA(6)+Type(2)+VLAN-Tag(4)（タグ付きパケットの場合。タグなしパケットの場合、4 bytes フィールドは追加されません）とペイロードを含め、基本的には同じです。全体的なフレームサイズは、すべて、フレームの最後の CRC を含め、設定済みポートの MTU よりも小さくなければなりません。
- QinQ についても、全体的なフレームサイズは、上記のように計算され、2 番目のタグの長さはフレームに追加されません。
- ポートの MTU のサイズは show interfaces status コマンドを使って表示することが可能です。

例

以下の例では、レイヤ 2 パケットジャンボフレームをまず有効にした後、port 1 の MTU を設定します。

```
Console(config)#jumbo frame
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mtu 9216
Console(config-if)#
```

関連コマンド

jumbo frame (P32)

show interfaces status (P258)

switchport broadcast packet-rate

ブロードキャスト帯域制御の設定を行います。コマンドの前に "no" を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閾値 (pps/ 秒) （範囲：500-14880000）

初期設定

有効（全ポート）

パケットレートの上限：500 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閾値を超えた場合、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、閾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 500pps の閾値を設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast octet-rate 500
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 （範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id (**範囲：**1-32)

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　（範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id (**範囲：**1-32)
  - vlan vlan-id — VLAN ID (1-4093)

初期設定

すべてのインタフェースの状況が表示されます。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- **ポートを指定しない場合は、すべてのポートの状況が表示されます。**
- **本コマンドを使用した際に表示される情報の詳細は「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:                1000T
  Mac Address:              00-17-2E-0F-E2-A5
 Configuration:
  Name:
  Port Admin:               Up
  Speed-duplex:             Auto
  Capabilities:             10half, 10full, 100half, 100full, 1000full
  Broadcast Storm:          Enabled
  Broadcast Storm Limit:    500 packets/second
  Flow Control:             Disabled
  LACP:                     Disabled
  Port Security:            Disabled
  Max MAC Count:            0
  Port Security Action:     None
  Media Type:               None
  Jumbo Frame state:        DISABLE
  Jumbo Frame size:         1522
 Current Status:
  Link Status:              Down
  Operation Speed-duplex:   1000full
  Flow Control Type:        None
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（範囲：**1-8）
    - port — **ポート番号（範囲：**1-26）
  - port-channel channel-id（**範囲：**1-32）

初期設定

すべてのポートのカウンタを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- **ポートを指定しない場合は、すべてのポートの状況が表示されます。**
- **本コマンドを使用した際に表示される情報の詳細は** 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: 0, Octets Output: 0
  Unicast Input: 0, Unicast Output: 0
  Discard Input: 0, Discard Output: 0
  Error Input: 0, Error Output: 0
  Unknown Protos Input: 0, QLen Output: 0
 Extended Iftable Stats:
  Multi-cast Input: 0, Multi-cast Output: 0
  Broadcast Input: 0, Broadcast Output: 0
 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
  Frames Too Long: 0, Carrier Sense Errors: 0
  Symbol Errors: 0
 RMON Stats:
  Drop Events: 0, Octets: 0, Packets: 0
  Broadcast PKTS: 0, Multi-cast PKTS: 0
  Undersize PKTS: 0, Oversize PKTS: 0
  Fragments: 0, Jabbers: 0
  CRC Align Errors: 0, Collisions: 0
  Packet Size <= 64 Octets: 0, Packet Size 65 to 127 Octets: 0
  Packet Size 128 to 255 Octets: 0, Packet Size 256 to 511 Octets: 0
  Packet Size 512 to 1023 Octets: 0, Packet Size 1024 to 1518 Octets: 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（範囲：**1-8）
    - port — **ポート番号（範囲：**1-26）
  - port-channel channel-id (**範囲：**1-32）

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 23 **番ポートの情報を表示しています。**

```
Console#show interfaces switchport ethernet 1/23
Information of Eth 1/23
 Broadcast Threshold:             Enabled, 500 packets/second
 LACP Status:                          Disabled
 Ingress Rate Limit:                 Disabled, 1000M bits per second
 Egress Rate Limit:                  Disabled, 1000M bits per second
 VLAN Membership Mode:      Hybrid
 Ingress Rule:                          Disabled
 Acceptable Frame Type:        All frames
 Native VLAN:                          1
 Priority for Untagged Traffic:  0
 GVRP Status:                          Disabled
 Allowed VLAN:                       1(u),
 Forbidden VLAN:
 802.1Q-tunnel Status:            Disable
 802.1Q-tunnel Mode:             NORMAL
 802.1Q-tunnel TPID:              8100(Hex)
Console#
```

コマンド解説

項目	解説
Broadcast threshold	ブロードキャスト帯域制御機能の有効 / 無効の表示。有効時には閾値を表示
Lacp status	LACP の有効 / 無効
Ingress/Egress rate limit	入力 / 出力帯域制御の有効 / 無効。現在の設定
VLAN membership mode	トランク又は Hybrid のメンバーモードを表示
Ingress rule	イングレスフィルタの有効 / 無効の表示
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
Native VLAN	デフォルトポート VLAN ID の表示
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
Gvrp status	GVRP の有効 / 無効
Allowed Vlan	参加している VLAN の表示。"(u)" はタグなし、"(t)" はタグ
Forbidden Vlan	GVRP によって動的に参加できない VLAN の表示
802.1Q-tunnel Status	このインタフェース上で 802.1Q トンネルが使用可能か否かを表示
802.1Q-tunnel Mode	トンネルモードが 802.1Q トンネルまたは 802.1Q トンネルアップリンクを表示
802.1Q-tunnel TPID	学習およびスイッチパケットに使用されるタグプロトコル識別子を表示

ケーブル診断用コマンド

test cable-diagnostics dsp

指定したポートのケーブル診断機能を実行して、ケーブルの障害（ショート、切断等）の診断およびケーブル長のレポートを行います。

文法

test cable-diagnostics dsp interface interface

interface

ethernet unit/port

- unit - **スタックユニット** (**有効範囲** :1-8)
- port - Port number. (**有効範囲** :1-26)

コマンドモード

Privileged Exec

コマンド解説

- **ケーブル診断は、デジタル信号処理（**DSP:Digital Signal Processing**）テストモードを使用して実行されます。**DSP **では、パルス信号をケーブルに送信してからパルスの反射を調べるという方法でケーブルの分析が行われます。**
- **ケーブル診断は、ツイストペアメディアでのみ実行することができます。**
- **このケーブルテストは、**7 **〜** 140m **の長さのケーブルでのみ、正確に実行されます。**
- **テストには約** 5 **秒かかります。テストが完了するとすぐに、スイッチに結果が表示され、障害のステータスや障害発生箇所までのおおよその距離に加え、一般的なケーブル障害などを確認することができます。**
- **診断で表示される可能性のある状況として、以下のものがあります。**
  - OK: **正しく終端されているペア。**
  - Open: **オープンペア。リンクパートナーなし。**
  - Short: **ショートペア**
  - Not Supported: **このメッセージは、ギガビットイーサネットポートが** 1,000Mbps **未満でリンクアップしている場合または** 10G **イーサネットポートの場合に表示されます。**
- Impedance mismatch: **終端インピーダンスが基準範囲内にありません。**
- **ポートは、ケーブル診断の実行中はリンクダウンします。**

例

```
Console#test cable-diagnostics dsp interface ethernet 1/1
Cable Diagnostics on interface Ethernet 1/1:
Cable Short with accuracy 0 meters.
Pair A OK, length 1 meters
Pair B OK, length 2 meters
Pair C Short, length 1 meters
Pair D Short, length 2 meters
Last Update 0n 2010-04-23 07:59:26
Console#
```

test loop internal

指定したポートの内部ループバックテストを実行します。

文法

test loop internal interface interface

interface

ethernet unit/port

- unit - Stack unit. (**有効範囲** :1-8)
- port - Port number. (**有効範囲** :1-26)

コマンドモード

Privileged Exec

コマンド解説

内部ループバックテスを実行する際、指定したインタフェースからのパケットは内部 PHY **にループバックされます。出力用データは、実際に送信を行わずに受信先にループバックしされます。この内部ループバックにより、インタフェースはネットワークの接続を行わずに適切に動作しているかどうかを確認できるようになります。**

例

```
Console#test loop internal interface ethernet 1/1
Internal loopback test: succeeded
Console#
```

show cable-diagnostics dsp

ケーブル診断テストの結果を表示します。

文法

show cable-diagnostics dsp interface [interface]

interface

ethernet unit/port

- unit - Stack unit. (**有効範囲** :1-8)
- port - Port number. (**有効範囲** :1-26)

コマンドモード

Privileged Exec

例

```
Console#show cable-diagnostics dsp interface ethernet 1/1
Cable Diagnostics on interface Ethernet 1/1:
Cable OK with accuracy 0 meters.
Pair A OK, length 0 meters
Pair B OK, length 0 meters
Pair C OK, length 1 meters
Pair D OK, length 1 meters
Last Update 0n 2009-10-21 15:08:20
Console#
```

show loop internal

ループバックテストの結果を表示します。

文法

show loop internal interface [interface]

interface

ethernet unit/port

- unit - Stack unit. (**有効範囲** :1-8)
- port - Port number. (**有効範囲** :1-26)

コマンドモード

Privileged Exec

例

```
Console#show loop internal interface ethernet 1/1
Port Test Result Last Update
-------- -------------- --------------------
Eth 1/1 Succeeded 2024-07-15 15:26:56
Console#
```

1.13 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 32 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 4Gpbs のバンド幅となります。

コマンド	機能	モード	ページ
Manual Configuration Commands			
interface port-channel	interface 設定モードへの移動とトランク設定	GC	P246
channel-group	トランクへのポートの追加	IC	P268
Dynamic Configuration Command			
lacp	現在のインタフェースでの LACP の設定	IC	P269
lacp system-priority	ポート LACP システムプライオリティの設定	IC (Ethernet)	P271
lacp admin-key	ポートアドミンキーの設定	IC (Ethernet)	P272
lacp admin-key	ポートチャンネルアドミンキーの設定	IC(Port Channel)	P273
lacp port-priority	LACP ポートプライオリティの設定	IC (Ethernet)	P274
Trunk Status Display Command			
show interfaces status	トランク情報の表示	NE,PE	P258
show lacp	LACP 関連情報の表示	PE	P275

トランク設定ガイドライン

- ループを防ぐため、ネットワークケーブルを接続する前にトランクの設定を完了させて下さい。
- 各トランクは最大 8 ポートまでトランク可能です。
- トランクの両端のポートはトランクポートとして設定される必要があります。
- トランクに参加するすべてのポートは、通信速度、duplex モード、フローコントロール、VLAN、CoS などすべて同一の設定である必要があります。
- port-channel を使用し VLAN からの移動、追加、削除する場合、トランクされたすべてのポートは１つのものとして扱われます。
- STP、VLAN および IGMP の設定は、指定したポートチャンネルを使用しすべてのトランクに設定することができます。

LACP 設定ガイドライン

ポートを同一ポートチャンネルに設定するには以下の条件に一致する必要があります。

- ポートは同一の LACP システムプライオリティの必要があります
- ポートは同一のポートアドミンキーの必要があります (Ethernet Interface)
- チャンネルグループが形成される場合に、ポートチャンネルアドミンキーをセットしなければ、このキーは、グループのインタフェースのポートアドミンキーと同一の値に設定されます。
- ポートチャンネルアドミンキーを設定する場合には、ポートアドミンキーはチャンネルグループへの参加が可能な同じ値を設定する必要があります。
- リンクが落ちた場合、LACP ポートプライオリティはバックアップリンクを選択します。

channel-group

トランクにポートを追加します。コマンドの前に "no" を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：1-32）

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いけません。
- " no channel-group" コマンドを使うことでポートグループをトランクからはずします。
- " no interfaces port-channel" コマンドを使うことでスイッチからトランクを削除します。

例

本例では、trunk 1 を生成し、11 番ポートをメンバーに加えています。

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

IEEE802.3ad 準拠の LACP を現在のインタフェースに対して設定します。コマンドの前に "no" を置くことで本機能を無効にします。

文法

lacp
no lacp

初期設定

無効 (Disabled)

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- LACP トランクの両端は固定設定もしくはオートネゴシエーションにより full duplex に設定されている必要があります。
- LACP を使用したトランクは自動的に使用可能なポートチャンネル ID を割り当てられます。
- 対向のスイッチも接続するポートで LACP を有効にしている場合、トランクは自動的に有効になります。
- 8 つ以上のポートが同じ対向のスイッチに接続されて、LACP が有効になっている場合、追加されるポートはスタンバイモードとなり、他のアクティブなリンクが落ちた場合にのみ有効となります。

例

本例では、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。コマンドの前に** "no" **を置くことにより、初期設定に戻します。**

文法

lacp {actor | partner} system-priority priority

no lacp {actor | partner} system-priority

- actor — **リンクアグリゲーションのローカル側**
- partner — **リンクアグリゲーションのリモート側**
- priority — **プライオリティは、リンクアグリゲーショングループ** (LAG) **メンバーシップを決定し、又** LAG **接続時に他のスイッチが本機を識別するために使用します（範囲：**0-65535**）**

初期設定

32768

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **同一** LAG **に参加するポートは同一システムプライオリティに設定する必要があります。**
- **システムプライオリティは本機の** MAC **アドレスと結合し** LAG ID **となります。**ID **は他のシステムとの** LACP **接続時の特定の** LAG **を表すために使用されます。**
- **リモート側のリンクが確立されると、**LACP **運用設定は使用されている状態です。パートナーの** LACP **設定は運用状態ではなく管理状態を表し、今後** LACP **がパートナーと確立される際に使用されます。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key（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。コマンドの前に** "no" **を置くことにより、初期設定に戻します。**

文法

lacp {actor | partner} admin-key key

no lacp {actor | partner} admin-key

- actor — **リンクアグリゲーションのローカル側**
- partner — **リンクアグリゲーションのリモート側**
- key — **ポートアドミンキーは同じ** LAG **のポートが同一の値を設定する必要があります（範囲：**0-65535**）**

初期設定

0

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **同じ** LAG **に参加するには、**LACP **システムプライオリティが一致し、**LACP **ポートアドミンキーが一致し、**LACP **ポートチャンネルキーが一致した場合となります。**
- **ポートチャンネルアドミンキーを設定する場合には、ポートアドミンキーはチャンネルグループへの参加が可能な同じ値を設定する必要があります。**
- **リモート側のリンクが確立されると、**LACP **運用設定は使用されている状態です。パートナーの** LACP **設定は運用状態ではなく管理状態を表し、今後** LACP **がパートナーと確立される際に使用されます。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp 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。コマンドの前に "no" を置くことにより、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。コマンドの前に "no" を置くことにより、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 | sys-id }

- port-channel — リンクアグリゲーショングループ ID（範囲：1-32）
- counters — LACP プロトコルメッセージの統計情報
- internal — ローカルサイドの運用状況と設定情報
- neighbors — リモートサイドの運用状況と設定情報
- sys-id— すべてのチャンネルグループの MAC アドレスとシステムプライオリティのサマリ

初期設定

Port Channel：すべて

コマンドモード

Privileged Exec

例

```
Console#show lacp 1 counters
Port channel              : 1
-------------------------------------------------------------------
Eth 1/ 1
-------------------------------------------------------------------
LACPDUs Sent         : 21
LACPDUs Received : 21
Marker Sent              : 0
Marker Received      : 0
LACPDUs Unknown Pkts : 0
LACPDUs Illegal Pkts : 0
```

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

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

例

```
Console#show lacp 1 neighbors
Port channel : 1 neighbors
-------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------
Partner Admin System ID : 32768, 00-00-00-00-00-00
Partner Oper System ID : 32768, 00-00-00-00-00-01
Partner Admin Port Number : 1
Partner Oper Port Number : 1
Port Admin Priority : 32768
Port Oper Priority : 32768
Admin Key : 0
Oper Key : 4
Admin State : defaulted, distributing, collecting,
synchronization, long timeout,
Oper State : distributing, collecting, synchronization,
aggregation, long timeout, LACP-activity
```

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

例

```
Console#show lacp sysid
Port Channel     System Priority     System MAC Address
----------------------------------------------------------------
             1                 32768      00-30-F1-D3-26-00
             2                 32768      00-30-F1-D3-26-00
             3                 32768      00-30-F1-D3-26-00
             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。

1.14 ミラーポート

ミラーポート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	P279
show port monitor	ミラーポートの設定の表示	PE	P280

port monitor

ミラーセッションの設定を行います。コマンドの前に "no" を置くことでミラーセッションをクリアします。

文法

port monitor interface [rx | tx | both]
no port monitor interface

- interface – ethernet unit/port (source port)
  - unit — ユニット番号 （範囲：1-8）
  - port — ポート番号（範囲：1-26）
- rx — 受信パケットのミラー
- tx — 送信パケットのミラー
- both— 受信 / 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えます。ディスティネーションポートにネットワーク解析装置（Sniffer 等) 又は RMON プローブを接続し、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（範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**

初期設定

すべてのセッションを表示

コマンドモード

Privileged Exec

コマンド解説

- **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
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
Destination port(listen port):Eth1/1
Source port(monitored port) :Eth1/6
Mode :RX/TX
Console#
```

1.15 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	P281

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。コマンドの前に "no" **を置くことで本機能を無効とします。**

文法

rate-limit < input | output > [rate]
no rate-limit < input | output >

- input — **入力帯域（レート）**
- output — **出力帯域（レート）**
- rate — **最大値**（1-1000Mbps）

初期設定

Gigabit **イーサネット：**1000Mbps

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 600
Console(config-if)#
```

1.16 自動トラフィック制御

ATC にはブロードキャストトラフィックまたはマルチキャストトラフィックの帯域制御機能が組み込まれています。

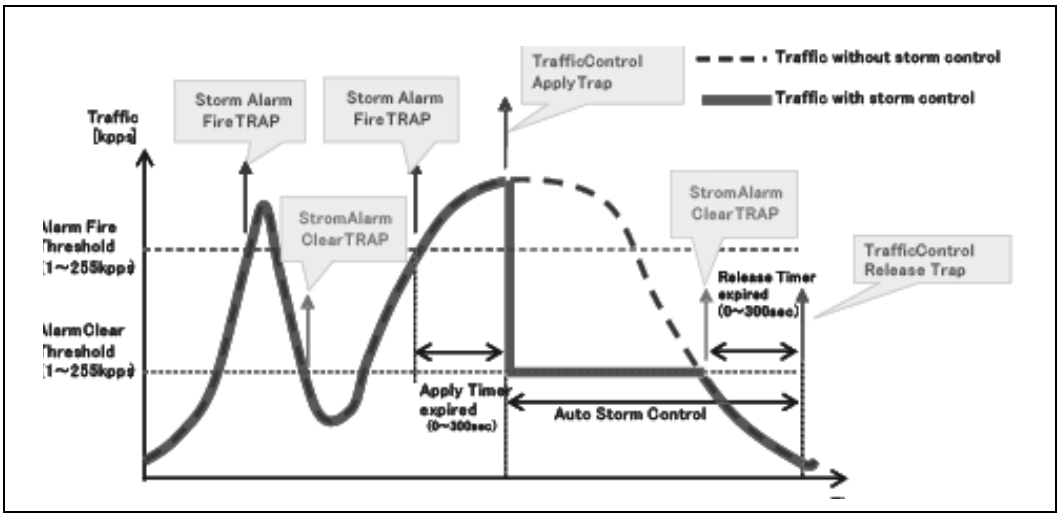
コマンド	機能	モード	ページ
Threshold Commands			
auto-traffic-control apply-timer	イングレストラフィックが閾値を上回った場合の制御アクションを実行する時間を設定します。	GC	P285
auto-traffic-control release-timer	イングレストラフィックの閾値を下回った場合の制御機能を解除する時間を設定します。	GC	P286
auto-traffic-control*	ブロードキャスト、またはマルチキャストストームの自動トラフィック制御を有効にします。	IC (Port)	P287
auto-traffic-control action	制御アクションを設定して、問題のあるポートのイングレストラフィックを制限するか、シャットダウンします。	IC (Port)	P288
auto-traffic-control alarm-clear-threshold	cleared storm control トラップを送信した値よりも低くなるように、イングレストラフィックの閾値を設定します。	IC (Port)	P289
auto-traffic-control alarm-fire-threshold	タイマーが切れた後に帯域制御アクションがトリガーとなる値を上回るように、イングレストラフィックの閾値の上限を設定します。	IC (Port)	P290
auto-traffic-control auto-control-release	制御アクションを自動的に解除します。	IC (Port)	P291
auto-traffic-control control-release	制御アクションを手動にて解除します。	PE	P291
SNMP Trap Commands			
snmp-server enable port-traps atc broadcast-alarm-clear	ストームコントロールがトリガーになった後にブロードキャストトラフィックが下限しきい値を下回った場合にトラップを送信します。	IC (Port)	P292
snmp-server enable port-traps atc broadcast-alarm-fire	ブロードキャストトラフィックが自動帯域制御の閾値の上限を超えると、トラップを送信します。	IC (Port)	P293
snmp-server enable port-traps atc broadcast-controlapply	ブロードキャストトラフィックが自動帯域制御の閾値の上限を超えて、適用タイマーが切れると、トラップを送信します。	IC (Port)	P294
snmp-server enable port-traps atc broadcast-controlrelease	帯域制御アクションがトリガーとなり、解除タイマーが切れた後にブロードキャストトラフィックが閾値を下回った場合にトラップを送信します。	IC (Port)	P294
snmp-server enable port-traps atc multicast-alarm-clear	帯域制御アクションがトリガーとなり、マルチキャストトラフィックが閾値を下回った時にトラップを送信します。	IC (Port)	P295
snmp-server enable port-traps atc multicast-alarm-fire	マルチキャストトラフィックが自動帯域制御の上限を上回ると、トラップを送信します。	IC (Port)	P296

snmp-server enable port-traps atc multicast-controlapply	マルチキャストトラフィックが自動帯域制御の上限を上回りかつ適用タイマーが切れると、トラップを送信します。	IC (Port)	P297
snmp-server enable port-traps atc multicast-controlrelease	帯域制御アクションがトリガーとなり、解除タイマーが切れた場合、マルチキャストトラフィックが閾値を下回るとトラップを送信します。	IC (Port)	P297
ATC Display Commands			
show auto-trafficcontrol	自動帯域制御のグローバル設定を表示します。	PE	P298
show auto-trafficcontrol interface	指定したポートのインタフェースのコンフィグの設定値、および帯域制御のステータスについて表示します。	PE	P298

ポートの自動帯域制御を有効にすると、switchport packet-rate コマンドで設定した場合は、同じポート上のハードウェアレベルの帯域制御は無効になります。

コマンドの使用

ATC にはブロードキャストトラフィックまたはマルチキャストトラフィックの帯域制御機能が組み込まれています。以下の図に示すように、それらのトラフィックタイプのいずれについても制御アクションは同じです。



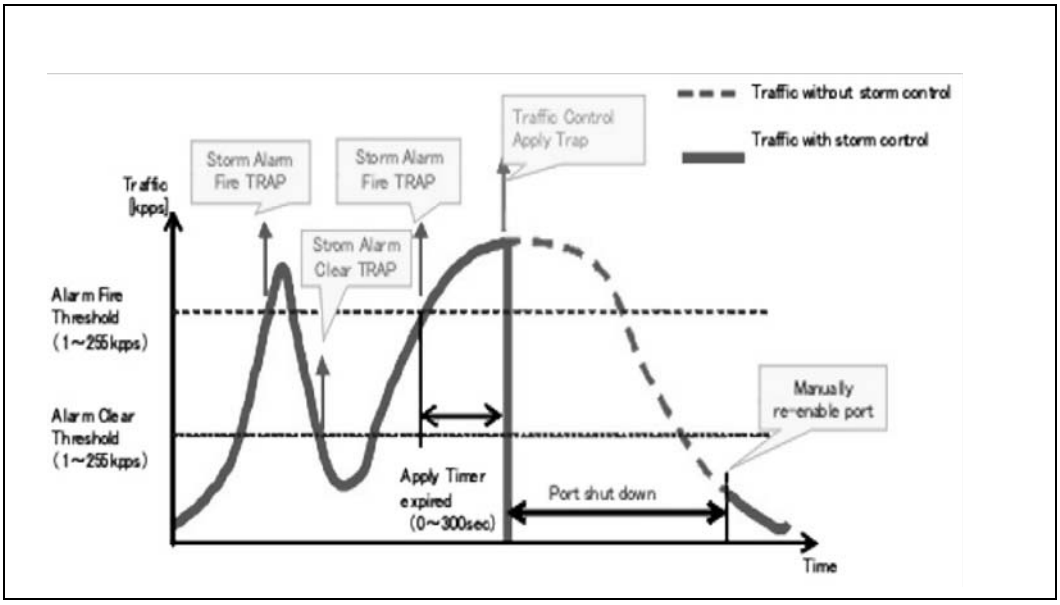
図：1-1: トラフィックレートリミットによる帯域制御

この図の要素については、以下に説明します。

- Control Apply トラップが送信されてログに記録されます。
- Alarm Clear しきい値 - トラフィックがこの下限しきい値を下回ってから解除タイマーで設定されている期間が過ぎると、制御アクションが自動的に停止されます。
- イングレストラフィックがこのしきい値を下回ると、ATC によって Storm Alarm Clear トラップが送信されてログに記録されます。
- トラフィックが Alarm Clear しきい値を下回ってから解除タイマーで設定されている期間が過ぎると、(レートリミットのための)トラフィック制御が

停止され、Traffic Control Release トラップが送信されてログに記録されます。制御アクションによって

- ポートがシャットダウンされている場合、そのポートは、手動制御解除機能を使用して手動でのみ再び有効にすることができます。



図：1-2: ポートのシャットダウンによる帯域制御

この図の主要な要素は、制御アクションの自動解除機能が用意されていない点を除き、直前の図に表されているものと同じです。トラフィック制御が適用された場合は、手動でポートを有効にする必要があります。

機能に関する制限事項

自動帯域制御は、ソフトウェアレベルの制御機能です。トラフィックストームは、ポートブロードキャスト制御機能またはポートマルチキャスト制御機能を参照）を使用してハードウェアレベルで制御することもできます。ただし、1 つのポートに適用できるのは、それらの制御タイプのうちの 1 つだけです。ポートで自動帯域制御を有効にすると、そのポートではハードウェアレベルの帯域制御は無効になります。

Threshold Commands

auto-traffic-control apply-timer

イングレストラフィックが閾値を上回った場合の制御アクションを実行する時間を設定します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

auto-traffic-control {broadcast | multicast} apply-timer seconds

no auto-traffic-control {broadcast | multicast} apply-timer

- broadcast - **ブロードキャストトラフィックの自動帯域制御を指定します。**
- multicast - **マルチキャストトラフィックの自動帯域制御を指定します。**
- seconds - **上限しきい値を超えてから制御アクションがブロードキャストストームに適用されるまでの期間（範囲** :1 **〜** 300 **秒、デフォルト** : 300 **秒）。**

初期設定

300 seconds

コマンドモード

Global Configuration

コマンド解説

- **タイマーが切れると、**auto-traffic-control action **コマンドで指定することにより制御アクションのトリガーとなり、**snmp-server enable port-traps atc broadcast-control-apply **コマンド、または** snmp-server enable port-traps atc multicast-control-apply **コマンドで指定することによりトラップメッセージを送信します。**

例

ここでは、すべてのポートのタイマーを「200 **秒」に設定します。**

```
Console(config)#auto-traffic-control broadcast apply-timer 200
Console(config)#
```

auto-traffic-control release-timer

イングレストラフィックの閾値を下回った場合の制御アクションを解除する時間を設定します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

auto-traffic-control {broadcast | multicast}

release-timer seconds

no auto-traffic-control {broadcast | multicast} release-timer

- broadcast - **ブロードキャストトラフィックの自動帯域制御を指定します。**
- multicast - **マルチキャストトラフィックの自動帯域制御を指定します。**
- seconds - **イングレストラフィックは閾値を下回った場合に制御アクションを解除する時間。**(**有効範囲** :1-900 seconds)

初期設定

900 seconds

コマンドモード

Global Configuration

コマンド解説

- **制御アクションを終了後の遅延時間を設定します。**auto-traffic-control auto-control-release **コマンドを使用して、自動解除を有効 / 無効にしてください。**

例

ここでは、すべてのポートの解除タイマーを「800**」秒に設定します。**

```
Console(config)#auto-traffic-control broadcast release-timer 800
Console(config)#
```

auto-traffic-control

ブロードキャスト、またはマルチキャストストームの自動トラフィック制御を有効にします。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] auto-traffic-control {broadcast | multicast}

- broadcast - **ブロードキャストトラフィックの自動帯域制御を指定します。**
- multicast - **マルチキャストトラフィックの自動帯域制御を指定します。**

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **ブロードキャスト、またはマルチキャストトラフィックの自動帯域制御を有効にすることができます。これらのトラフィックは同時に有効にすることはできません。**
- **自動帯域制御は、ソフトウェアレベルの制御機能です。トラフィックストームは、**switchport packet-rate **コマンドを使用してハードウェアレベルで制御することも可能ですが、**1 **ポートについて適用可能なのはいずれか** 1 **つのみです。自動帯域制御により、ポートのハードウェアレベルのストームを無効にすることができます。**

例

port 1 **のブロードキャストトラフィックの自動帯域制御を有効にします。**

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast
Console(config-if)#
```

auto-traffic-control action

制御アクションを設定して、問題のあるポートのイングレストラフィックを制限するか、シャットダウンします。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

auto-traffic-control {broadcast | multicast}

action {rate-control | shutdown}

no auto-traffic-control {broadcast | multicast} action

- broadcast - ブロードキャストトラフィックの自動帯域制御を指定します。
- multicast - マルチキャストトラフィックの自動帯域制御を指定します。
- rate-control - 制御アクションがトリガーとなる場合は、イングレストラフィックレーは autotraffic-control alarm-clear-threshold コマンドによって設定された閾値に応じて制限されます。
- shutdown - 制御アクションがトリガーとなる場合は、ポートは設定上無効になります。自動トラフィック制御によって無効となったポートは手動でのみ再度有効に設定することが可能です。

初期設定

rate-control

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- Alarm Fire しきい値（上限しきい値）を超えてから適用タイマーで設定されている期間が過ぎると、このコマンドに応じて制御アクションがトリガーになります。
- このコマンドによって制御アクションをレートリミットに設定する場合、auto-traffic-control alarm-clearthreshold コマンドによってレートリミットを決定されます。
- 制御アクションをイングレストラフィックのレートに設定する場合は、トラフィックレートが下限閾値を下回って、解除タイマーが切れると、制御アクションは自動的に終了します。
- 制御アクションによってポートをシャットダウンすると、自動トラフィック制御によって再度有効にすることはできません。auto-traffic-control control-release コマンドを使用して手動でのみ再度有効にすることが可能です。

例

port 1 のブロードキャストトラフィックの制御アクションを設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

auto-traffic-control alarm-clearthreshold

cleared storm control トラップを送信する値よりも低くなるように、イングレストラフィックの閾値を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

auto-traffic-control {broadcast | multicast}

alarm-clear-threshold threshold

no auto-traffic-control {broadcast | multicast}

alarm-clear-threshold

- broadcast - ブロードキャストトラフィックの自動帯域制御を指定します。
- multicast - マルチキャストトラフィックの自動帯域制御を指定します。
- threshold - イングレストラフィックの下限を cleared storm control トラップを送信する値よりも低い閾値 (有効範囲 :1-255 キロパケット / 秒)

初期設定

128 キロパケット / 秒

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- トラフィックレートが下限の閾値より低くなると、nmp-server enable port-traps atc broadcast-alarm-clear コマンド、または snmp-server enable port-traps atc multicast-alarm-clear コマンドによって設定されている場合は、トラップメッセージを送ります。
- レートリミットを制御アクションとして設定する場合は、トラフィックレートが下限を下回ると中断し、解除タイマーが切れます。ポートは制御アクションによってシャットダウンした場合は、auto-traffic-control control-release コマンドを使用して手動にてのみ再度有効にすることができます。

例

ここでは、port 1 のブロードキャストトラフィックの自動帯域制御の clear 閾値を設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-clear-
threshold 155
Console(config-if)#
```

auto-traffic-control alarm-fire-threshold

適用タイマーが切れた後に帯域制御アクションがトリガーとなる値を上回るように、イングレストラフィックの閾値の上限を設定します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

auto-traffic-control {broadcast | multicast}

alarm-fire-threshold threshold

no auto-traffic-control {broadcast | multicast}

alarm-fire-threshold

- broadcast - **ブロードキャストトラフィックの自動帯域制御を指定します。**
- multicast - **マルチキャストトラフィックの自動帯域制御を指定します。**
- threshold - **適用タイマーが切れると、帯域制御アクションがトリガーとなる値よりも大きいイングレストラフィックの閾値の上限** (**有効範囲** :1-255 **キロパケット** / **秒**)

初期設定

128 **キロパケット** / **秒**

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **一度上限の閾値を上回ると、**snmp-server enable port-traps atc broadcast-alarmfire **コマンド、または** snmp-server enable port-traps atc multicast-alarmfire **コマンドを使って設定されている場合は、トラップメッセージが送信されます。**
- **一度上限の閾値を上回ると、**auto-trafficcontrol action **コマンドで設定した場合は制御アクションがトリガーとなる前に、制御タイマーをまず** auto-traffic-control apply-timer **コマンドで設定して終了する必要があります。**

例

port 1 **のブロードキャストトラフィックの自動帯域制御のトリガーの閾値を設定します。**

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-fire-
threshold 255
Console(config-if)#
```

auto-traffic-control auto-control-release

auto-traffic-control release-timer **コマンドで指定した時間が切れると、制御アクションを自動的に解除します。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻ります。**

文法

auto-traffic-control {broadcast | multicast}

auto-control-release

- broadcast - **ブロードキャストトラフィックの自動帯域制御を指定します。**
- multicast - **マルチキャストトラフィックの自動帯域制御を指定します。**

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **指定のアクションがトリガーとなり、解除タイマーが切れた後に制御アクションを自動的に終了します。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-
release
Console(config-if)#
```

auto-traffic-control control-release

制御アクションを手動で解除します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

auto-traffic-control {broadcast | multicast} control-release

- broadcast - **ブロードキャストトラフィックの自動帯域制御を指定します。**
- multicast - **マルチキャストトラフィックの自動帯域制御を指定します。**

コマンドモード

Privileged Exec

コマンド解説

- **指定したアクションがトリガーとなると、制御アクションを手動で終了します。**

例

```
Console#auto-traffic-control broadcast control-release interface
ethernet 1/1
Console#
```

snmp-server enable port-traps atc broadcast-alarmclear

帯域制御アクションがトリガーとなった場合、ブロードキャストトラフィックが下限の閾値よりも下回った時にトラップを送信します。

文法

[no] snmp-server enable port-traps atc broadcast-alarm-clear

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-
alarm-clear
Console(config-if)#
```

関連するコマンド

auto-traffic-control action (P288)

auto-traffic-control alarm-clear-threshold (P289)

snmp-server enable port-traps atc broadcast-alarm-fire

ブロードキャストトラフィックが自動帯域制御の上限の閾値よりも上回ると、トラップを送信します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] snmp-server enable port-traps atc broadcast-alarm-fire

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-
alarm-fire
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold (P290)

snmp-server enable port-traps atc broadcast-controlapply

ブロードキャストトラフィックが自動帯域制御の上限の閾値よりも上回り、かつ適用タイマが切れると、トラップを送信します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] snmp-server enable port-traps atc broadcast-control-apply

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-
control-apply
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold (P290)

auto-traffic-control apply-timer (P285)

snmp-server enable port-traps atc broadcast-controlrelease

ブロードキャストトラフィックが自動帯域制御の下限の閾値よりも下回り、かつ解除タイマが切れると、トラップを送信します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] snmp-server enable port-traps atc

broadcast-control-release

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-
controlrelease
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-clear-threshold (P289)

auto-traffic-control action (P288)

auto-traffic-control release-timer (P286)

snmp-server enable port-traps atc multicast-alarmclear

帯域制御応答がトリガーとなった後に、マルチキャストトラフィックが下限の閾値よりも下回ると、トラップを送信します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] snmp-server enable port-traps atc multicast-alarm-clear

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-
alarm-clear
Console(config-if)#
```

関連するコマンド

auto-traffic-control action (P288)

auto-traffic-control alarm-clear-threshold (P289)

snmp-server enable port-traps atc multicast-alarm-fire

マルチキャストトラフィックが自動帯域制御の閾値の上限を超えると、トラップを送信します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] snmp-server enable port-traps atc multicast-alarm-fire

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-
alarm-fire
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold (P290)

snmp-server enable port-traps atc multicast-controlapply

マルチキャストトラフィックが自動帯域制御の上限を上回りかつ適用タイマーが切れると、トラップを送信します。コマンドの前に ”no” **を置くことにより、トラップを無効にします。**

文法

[no] snmp-server enable port-traps atc multicast-control-apply

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-
control-apply
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold (P290)

auto-traffic-control apply-timer (P285)

snmp-server enable port-traps atc multicast-controlrelease

帯域制御アクションがトリガーとなり、解除タイマーが切れた場合、マルチキャストトラフィックが閾値を下回るとトラップを送信します。

文法

[no] snmp-server enable port-traps atc

multicast-control-release

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-
controlrelease
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-clear-threshold (P289)

auto-traffic-control action (P288)

auto-traffic-control release-timer (P286)

ATC Display Commands

show auto-trafficcontrol

自動帯域制御のグローバル設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show auto-traffic-control
Storm-control: Broadcast
Apply-timer (sec) : 300
release-timer (sec) : 900
Storm-control: Multicast
Apply-timer(sec) : 300
release-timer(sec) : 900
Console#
```

show auto-trafficcontrol interface

指定したポートのインタフェースのコンフィグの設定値、および帯域制御のステータスについて表示します。

文法

show auto-traffic-control interface [interface]

interface

ethernet unit/port

unit - **ユニットの識別子** (**有効範囲** :1-8)

port - **ポート番号** (**有効範囲** :1-26)

コマンドモード

Privileged Exec

例

```
Console#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
-----------------------------------------------------------------
--------
Storm Control: Broadcast Multicast
State: Disabled Disabled
Action: rate-control rate-control
Auto Release Control: Disabled Disabled
Alarm Fire Threshold(Kpps): 128 128
Alarm Clear Threshold(Kpps):128 128
Trap Storm Fire: Disabled Disabled
Trap Storm Clear: Disabled Disabled
Trap Traffic Apply: Disabled Disabled
Trap Traffic Release: Disabled Disabled
-------------------------------------------------------
```

1.17 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、エイ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	P300
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	P301
show mac-address-table	転送データベースに登録された情報の表示	PE	P302
mac-address-table aging-time	アドレステーブルのエイジングタイムの設定	GC	P303
show mac-address-table aging-time	アドレステーブルのエイジングタイムの表示	PE	P303

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。コマンドの前に "no" を置くことで 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 （範囲：1-8）
    - port — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)
- vlan vlan-id — VLAN ID (1-4093)
- action
  - delete-on-reset — 本機が再起動されるまで登録されます。
  - permanent — 永久に登録されます。

初期設定

mac-address：なし

action：permanent

コマンドモード

Global Configuration

コマンド解説

静的アドレスは特定の VLAN の特定のポートに割り当てることができます。本コマンドを使用して静的アドレスを MAC アドレステーブルに追加することができます。静的アドレスは以下の特性を持っています。

- インタフェースのリンクがダウンしても、静的アドレスはアドレステーブルから削除されません。
- 静的アドレスは指定したインタフェースに固定され、他のインタフェースに移動することはありません。静的アドレスが他のインタフェースに現れた場合、アドレスは拒否されアドレステーブルに記録されません。
- 静的アドレスは "no" コマンドを使って削除するまで、他のポートで学習されません。

例

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
 interface ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

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　（範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
- port-channel channel-id**（範囲：**1-8**）**
- vlan-id — VLAN ID (1-4093)
- sort — **アドレス、**VLAN**、インタフェースによる並び替え**

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show mac-address-table
  Interface MAC Address VLAN Type
  --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de 1 Delete-on-reset
Console#
```

mac-address-table aging-time

アドレステーブルのエイジングタイムを設定します。コマンドの前に "no" **を置くことにより、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** (10-1000000 **の値。**0 **に設定した場合はエイ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

- **エイジングタイムは動的転送情報を本機に保持する時間を表します。**

例

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

アドレステーブルのエイ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#
```

1.18 LLDP コマンド

Link Layer Discovery Protocol（LLDP）はローカルブロードキャストドメインの中の接続デバイスについての基本的な情報を発見するために使用します。LLDP はレイヤ 2 のプロトコルであり、デバイスについての情報を周期的なブロードキャストで伝達します。伝達された情報は IEEE802.1ab に従って Type Length Value（TLV）で表され、そこにはデバイス自身の識別情報、能力、設定情報の詳細が含まれています。また LLDP は発見した近隣のネットワークノードについて集められた情報の保存方法と管理方法を設定します。

Link Layer Discovery Protocol - Media Endpoint Discovery（LLDP-MED）は VoIP やスイッチのようなエンドポイントのデバイスを管理するための拡張された LLDP です。LLDP-MED の TLV はネットワークポリシー、電力、インベントリ、デバイスのロケーションの詳細情報を伝達します。LLDP と LLDP-MED の情報は、トラブルシューティングの簡易化、ネットワーク管理の改善、間違いのないネットワークトポロジーを維持するため、SNMP アプリケーションによって使用することができます。

コマンド	機能	モード	ページ
lldp	スイッチで LLDP を有効	GC	P305
lldp holdtime-multiplier	TTL(time-to-live) 値の設定	GC	P306
lldp notification-interval	LLDP の変更に関する SNMP 通知送信の間隔を設定	GC	P307
lldp refresh-interval	LLDP 配信の転送間隔を設定	GC	P307
lldp reinit-delay	LLDP ポートが無効またはリンクダウン時の再初期化までの待ち時間を設定	GC	P308
lldp tx-delay	ローカル LLDP MIB の変数に変化が起こった後に、アドバタイズメントを送信するまでの時間を設定します	GC	P308
lldp admin-status	LLDP メッセージの送信・受信のモードを有効	IC	P309
lldp notification	LLDP 変更の SNMP トラップ通知送信を有効	IC	P310
lldp basic-tlv port-description	TLV Type “port-description“ を設定	IC	P311
lldp basic-tlv system-capabilities	TLV Type “system-capabilities“ を設定	IC	P311
lldp basic-tlv system-description	TLV Type “system-description“ を設定	IC	P312
lldp basic-tlv system-name	TLV Type “system-name“ を設定	IC	P313
lldp dot1-tlv proto-ident*	lldp dot1-TLV“ proto-ident“ を設定	IC	P313
lldp dot1-tlv proto-vid*	lldp dot1-TLV“ proto-vid“ を設定	IC	P314
lldp dot1-tlv pvid*	lldp dot1-TLV“pvid“ を設定	IC	P314
lldp dot1-tlv vlan-name*	lldp dot1-TLV“vlan-name“ を設定	IC	P316
lldp dot3-tlv link-agg	lldp dot3-TLV“link-agg“ を設定	IC	P316
lldp dot3-tlv mac-phy	lldp dot3-TLV“mac-phy“ を設定	IC	P317

lldp dot3-tlv max-frame	lldp dot3-TLV“max-frame“ を設定	IC	P317
lldp dot3-tlv poe	dot3-tlv “poe” を設定	IC	P318
show lldp config	LLDP 設定の表示	PE	P319
show lldp info local-device	LLDP ローカルデバイス情報を表示	PE	P320
show lldp info remote-device	LLDP リモートデバイス情報を表示	PE	P321
show lldp info statistics	LLDP 統計情報を表示	PE	P322

lldp

スイッチで LLDP を有効にします。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp

no lldp

初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#lldp
Console(config)#
```

lldp holdtime-multiplier

LLDP のアドバタイズメントで送信された Time-To-Live（TTL）値を設定します。コマンドの前に "no" を置くことで設定を初期状態に戻します。

文法

lldp holdtime-multiplier value

no lldp holdtime-multiplier

- value - TTL 値を設定します。TTL は秒で表され、下の数式で計算します。
  Transmission Interval × Hold Time Multiplier ≦ 65536
  （範囲：2-10）

初期設定

Holdtime multiplier：4

TTL：4×30 = 120 秒

コマンドモード

Global Configuration

コマンド解説

- TTL は、タイムリーな方法でアップデートが送信されない場合、送信した LLDP エージェントに関係のあるすべての情報をどのくらいの期間維持するかを受信した LLDP エージェントに伝達します。

例

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

lldp notification-interval

LLDP MIB の変更を行い、SNMP 通知が送信されるまでの時間を設定します。コマンドの前に "no" を置くことで設定を初期状態に戻します。

文法

lldp notification-interval seconds

no lldp notification-interval

- seconds - SNMP 通知が送られる周期的な間隔を指定します
  （範囲：5 ～ 3600 秒　初期設定 5 秒）

初期設定

5 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp notification-interval 30
Console(config)#
```

lldp refresh-interval

LLDP アドバタイズが送信されるまでの間隔を設定します。コマンドの前に "no" を置くことで設定を初期状態に戻します。

文法

lldp refresh-interval seconds

no lldp refresh-delay

- seconds - LLDP アドバタイズが送信されるまでの間隔を指定します
  （範囲：5 ～ 32768 秒）

初期設定

30 秒

コマンドモード

Global Configuration

コマンド解説

- refresh-interval× Hold Time Multiplier ≦ 65536

例

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

lldp reinit-delay

LLDP ポートが無効になるかリンクダウンした後、再初期化を試みるまでの時間を設定します。コマンドの前に "no" を置くことで設定を初期状態に戻します。

文法

lldp reinit-delay seconds

no lldp reinit-delay

- seconds - 再初期化を試みるまでの時間を指定します（範囲：1-10 秒）

初期設定

2 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay

ローカル LLDP MIB の変数に変化が起こった後に引き続き、アドバタイズメントを送信するまでの時間を設定します。コマンドの前に "no" を置くことで設定を初期状態に戻します。

文法

lldp tx-delay seconds

no lldp tx-delay

- seconds - アドバタイズメントを送信するまでの時間を設定を指定します
（範囲：1-8192 秒）

初期設定

2 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status

個別のインタフェースに対し、メッセージの内容を指定するために LLDP **ポート・トランクの設定を行います。コマンドの前に** "no" **を置くことでこの機能を無効にします。**

文法

lldp admin-status < rx-only | tx-only | tx-rx >

no lldp admin-status

- rx-only - LLDP PDUs. **受信のみ**
- tx-only - LLDP PDUs. **送信のみ**
- tx-rx - LLDP PDUs. **送受信**

初期設定

tx-rx

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp notification

LLDP 変更について SNMP トラップ通知の送信を可能にします。コマンドの前に "no" を置くことでこの機能を無効にします。

文法

lldp notification
no lldp notification

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

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

lldp basic-tlv management-ip-address

LLDP 有効ポートで "management-ip-address" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp basic-tlv management-ip-address

no lldp basic-tlv management-ip-address

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- management-ip-address には、スイッチの IPv4 アドレスが含まれます。スイッチに管理用のアドレスがない場合、アドレスはスイッチの CPU の MAC アドレスが、このアドバタイズメントを送信するポートの MAC アドレスになります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description

LLDP 有効ポートで "port-description" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp basic-tlv port-description
no lldp basic-tlv port-description

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- port-description には、RFC2863 の ifDescr オブジェクトで規定されています。これには製造者、スイッチの製品名、インタフェースのハードウェアとソフトウェアのバージョンが含まれます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

lldp basic-tlv system-capabilities

LLDP 有効ポートで "system-capabilities" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp basic-tlv system-capabilities
no lldp basic-tlv system-capabilities

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- system-capabilities には、システムの主な機能が含まれます。この情報には機能自体が有効かどうかは関係ありません。この TLV によってアドバタイズされる情報は IEEE802.1AB 規格に記述されています。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description

LLDP 有効ポートで "system-description" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp basic-tlv system-description

no lldp basic-tlv system-description

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- system-description は RFC3418 の sysDescr オブジェクトで規定されています。システムのハードウェア、オペレーティングソフト、ネットワーキングソフトのフルネームとバージョンが含まれています。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name

LLDP 有効ポートで "system-name" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp basic-tlv system-name
no lldp basic-tlv system-name

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- System-name は RFC3418 の sysName オブジェクトで規定されています。システムの管理用に割り当てられた名前が含まれます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dot1-tlv proto-ident

LLDP 有効ポートで "proto-ident" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp dot1-tlv proto-ident
no lldp dot1-tlv proto-ident

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

lldp dot1-tlv proto-vid

LLDP 有効ポートで "proto-vid" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp dot1-tlv proto-vid
no lldp dot1-tlv proto-vid

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ポートベースおよびプロトコルベース VLAN 情報をアドバタイズします。
  詳細については P363 「VLAN インタフェースの設定」および P378 「プロトコル VLAN の設定」を参照してください。

例

```
Console(config)#inter ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

lldp dot1-tlv pvid

LLDP 有効ポートで "pvid" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp dot1-tlv pvid
no lldp dot1-tlv pvid

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- PVID 情報をアドバタイズします。
  詳細については P367 「switchport native vlan」を参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

lldp dot1-tlv vlan-name

LLDP 有効ポートで "vlan-name" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp dot1-tlv vlan-name
no lldp dot1-tlv vlan-name

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 指定したインタフェースが割り当てられた、全ての VLAN 名をアドバタイズします。VLAN については P368 「switchport allowed vlan」および P384「protocol-vlan protocol-group (Configuring Groups)」を参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg

LLDP 有効ポートで "link-agg" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp dot3-tlv link-agg
no lldp dot3-tlv link-agg

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- リンクアグリゲーションステータスをアドバタイズします。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy

LLDP 有効ポートで "mac-phy" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp dot3-tlv mac-phy
no lldp dot3-tlv mac-phy

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- MAC/PHY 設定およびステータスをアドバタイズします。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv max-frame

LLDP 有効ポートで "max-frame" のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp dot3-tlv max-frame
no lldp dot3-tlv max-frame

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 最大フレームサイズ情報をアドバタイズします。フレームサイズについての詳細は P32「フレームサイズコマンド」を参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp dot3-tlv poe

LLDP 有効ポートで "PoE”（Power-over-Ethernet）のアドバタイズを行います。コマンドの前に "no" を置くことで機能を無効にします。

文法

lldp dot3-tlv poe
no lldp dot3-tlv poe

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- このオプションでは、PoE をサポートしているかどうかを含み、Power-over-Ethernet 機能についてアドバタイズします。電源が供給されるポートの pin が制御可能な場合は、選択されたポートの pin は電源および電源クラスを供給します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv poe
Console(config-if)
```

show lldp config

全てのポートの LLDP 設定を表示します。

文法

show lldp config [detail interface]

- detail — **設定サマリを表示**
- interface
  - ethernet unit/port
    - unit — **ユニット番号（範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id**（範囲：**1-32**）**

コマンドモード

Privileged Exec

例

```
Console#show lldp config

LLDP Global Configuration

 LLDP Enabled                  : Yes
 LLDP Transmit interval        : 30 sec.
 LLDP Hold Time Multiplier     : 4
 LLDP Delay Interval           : 2 sec.
 LLDP Re-initialization Delay  : 2 sec.
 LLDP Notification Interval    : 5 sec.


LLDP Port Configuration
 Port     Admin Status Notification Enabled
 -------- ------------ --------------------
 Eth 1/1  Tx-Rx        False
 Eth 1/2  Tx-Rx        False
 Eth 1/3  Tx-Rx        False
 Eth 1/4  Tx-Rx        False
 Eth 1/5  Tx-Rx        False
 Eth 1/6  Tx-Rx        False
 Eth 1/7  Tx-Rx        False
 Eth 1/8  Tx-Rx        False
 Eth 1/9  Tx-Rx        False
 Eth 1/10 Tx-Rx        False
Console#
```

show lldp info local-device

スイッチについての情報を表示します。

文法

show lldp info local-device [detail interface]

- detail — **詳細情報を表示**
- interface
  - ethernet unit/port
    - unit — **ユニット番号（範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id**（範囲：**1-32**）**

コマンドモード

Privileged Exec

例

```
Console#show lldp info local-device

 LLDP Local System Information
  Chassis Type                     : MAC Address
  Chassis ID                         : 00-12-CF-F3-DE-46
  System Name                   :
  System Description           : FXC3110
  System Capabilities Support : Bridge, Router
  System Capabilities Enabled : Bridge, Router

 LLDP Port Information
  Port    PortID Type      PortID            Port Description
 -------- ---------------- ----------------- -------------------------------
-
 Eth 1/1  MAC Address      00-12-CF-F3-DE-47 Ethernet Port on unit 1, port 1
 Eth 1/2  MAC Address      00-12-CF-F3-DE-48 Ethernet Port on unit 1, port 2
 Eth 1/3  MAC Address      00-12-CF-F3-DE-49 Ethernet Port on unit 1, port 3
 Eth 1/4  MAC Address      00-12-CF-F3-DE-4A Ethernet Port on unit 1, port 4
 Eth 1/5  MAC Address      00-12-CF-F3-DE-4B Ethernet Port on unit 1, port 5
 Eth 1/6  MAC Address      00-12-CF-F3-DE-4C Ethernet Port on unit 1, port 6
 Eth 1/7  MAC Address      00-12-CF-F3-DE-4D Ethernet Port on unit 1, port 7
 Eth 1/8  MAC Address      00-12-CF-F3-DE-4E Ethernet Port on unit 1, port 8
 Eth 1/9  MAC Address      00-12-CF-F3-DE-4F Ethernet Port on unit 1, port 9
 Eth 1/10 MAC Address      00-12-CF-F3-DE-50 Ethernet Port on unit 1, port 10
Console#
```

show lldp info remote-device

ローカルスイッチの指定されたポートに接続された、LLDP が有効のデバイスについての詳細情報を表示します。

文法

show lldp info remote-device [detail interface]

- detail — **詳細情報を表示**
- interface
  - ethernet unit/port
    - unit — **ユニット番号（範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id**（範囲：**1-32**）**

コマンドモード

Privileged Exec

例

```
Console#show lldp info remote-device
LLDP Remote Devices Information
Interface | ChassisId PortId SysName
--------- + ---------------- ---------------- ----------------
----
Eth 1/1 | 00-01-02-03-04-05 00-01-02-03-04-06
Console#show lldp info remote-device detail ethernet 1/1
LLDP Remote Devices Information Detail
----------------------------------------------------------------
Local PortName : Eth 1/1
Chassis Type : MAC Address
Chassis Id : 00-01-02-03-04-05
PortID Type : MAC Address
PortID : 00-01-02-03-04-06
SysName :
SysDescr : 24PORT GIGABIT L2 INTELLIGENT SWITCH
PortDescr : Ethernet Port on unit 1, port 1
SystemCapSupported : Bridge
SystemCapEnabled : Bridge
Remote Management Address :
00-01-02-03-04-05 (MAC Address)
Console#
```

show lldp info statistics

このスイッチに接続されている LLDP が有効なすべてのデバイスの統計を表示します。

文法

show lldp info statistics [detail interface]

- detail — **詳細情報を表示**
- interface
  - ethernet unit/port
    - unit — **ユニット番号（範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id**（範囲：**1-32**）**

コマンドモード

Privileged Exec

例

```
Console#show lldp info statistics

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 0 seconds
  New Neighbor Entries Count         : 0
  Neighbor Entries Deleted Count     : 0
  Neighbor Entries Dropped Count     : 0
  Neighbor Entries Ageout Count      : 0

  Port     NumFramesRecvd NumFramesSent NumFramesDiscarded
  -------- -------------- ------------- ------------------
  Eth 1/1               0             0                  0
  Eth 1/2               0             0                  0
  Eth 1/3               0             0                  0
  Eth 1/4               0             0                  0
  Eth 1/5               0             0                  0
  Eth 1/6               0             0                  0
  Eth 1/7               0             0                  0
  Eth 1/8               0             0                  0
  Eth 1/9               0             0                  0
  Eth 1/10             0             0                  0
Console#
```

1.19 スパニングツリー の設定

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をします。	GC	P324
spanning-tree forward-time	スパニングツリーのブリッジの転送時間を設定します。	GC	P326
spanning-tree mode	STP/RSTP/MSTP モードの選択をします。	GC	P325
spanning-tree hello-time	スパニングツリーブリッジハロー時間を設定します。	GC	P327
spanning-tree max-age	スパニングツリーブリッジ最長時間を設定します。	GC	P328
spanning-tree priority	スパニングツリーブリッジプライオリティを設定します。	GC	P329
spanning-tree path-cost method	RSTP/MSTP のパスコスト方法を設定します。	GC	P330
spanning-tree transmission-limit	RSTP/MSTP の送信リミットを設定します。	GC	P331
spanning-tree-mst-configuration	MSTP 設定モードを変更します。	GC	P331
spanning-tree systembpdu-flooding	スパニングツリー機能がグローバルで無効な場合、ポートすべてに、または同一の VLAN 上のポートにのみ BPDU のフラッディングを行います。		P333
mst vlan	スパニングツリーインスタンスへの VLAN を追加します	MST	P332
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。	MST	P334
name	MST 名を設定します。	MST	P335
revision	MST リビジョンナンバーを設定します。	MST	P336
max-hops	BPDU が破棄される前の最大ホップ数を設定します。	MST	P338
spanning-tree bpdu-filter	エッジポートの BPDU のフィルタリングを行います。		P338
spanning-tree bpdu-guard	BPDU を受信した場合に、エッジポートをシャットダウンします。		P339
spanning-tree spanning-disabled	インタフェースのスパニングツリーを無効化します。	IC	P338
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を行います。	IC	P340
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を行います。	IC	P342
spanning-tree edge-port	エッジポートへのポートファストを有効化します。	IC	P343
spanning-tree portfast	インタフェースのポートファストを設定します。	IC	P344
spanning-tree link-type	RSTP/MSTP のリンクタイプを設定します。	IC	P345
spanning-tree loopback-detection	ポートの BPDU のループバック検出を有効にします。	IC	P346
spanning-tree loopbackdetection release-mode	ポートのループバックのリリースモードを設定します。	IC	P347
spanning-tree loopbackdetection trap	ポートの BPDU ループバックの SNMP トラップ通知を有効にします。	IC	P348
spanning-tree mst cost	MST インスタンスのパスコストを設定します。	IC	P349

spanning-tree mst port-priority	MST インスタンスプライオリティを設定します。	IC	P350
spanning-tree protocol-migration	適切な BPDU フォーマットを再確認します。	PE	P351
show spanning-tree	スパニングツリーの設定を表示します。	PE	P352
show spanning-tree mst configuration	MST 設定を表示します。	PE	P354

spanning-tree

本機に対して STA を有効に設定します。コマンドの前に "no" を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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

spanning-tree mode { stp | rstp | mstp }

no spanning-tree mode

- stp — Spanning Tree Protocol（IEEE 802.1D 準拠）
- rstp — Rapid Spanning Tree Protocol（IEEE 802.1w 準拠）
- mstp— 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。コマンドの前に "no" **を置くことにより、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** [(max-age / 2) + 1] **のどちらか小さい方となります。**

初期設定

15**（秒）**

コマンドモード

Global Configuration

コマンド解説

- **ルートデバイスがステータスを変更するまでの最大時間を設定することができます。各デバイスがフレームの転送をはじめる前にトポロジー変更を受け取るために遅延時間が必要です。また、各ポートの競合する情報を受信し、廃棄するためにも時間が必要となります。そうしなければ一時的にでも、データのループが発生します。**

例

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

スパニングツリー Hello **タイムを設定します。コマンドの前に** "no" **を置くことにより、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** [(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イジングタイムを設定します。コマンドの前に "no" **を置くことにより、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 x (hello-time + 1)] **のどちらか大きい値です。**
  最大値は 40 **又は** [2 x (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。コマンドの前に "no" を置くことにより、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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

spanning-tree pathcost method { long | short }
no spanning-tree pathcost method

- long — 1-200,000,000 までの 32 ビットの値
- short — 1-65535 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。コマンドの前に "no" を置くことにより、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。

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（P332）
mst priority（P334）
name（P335）

mst vlan

スパニングツリーインスタンスに VLAN **を追加します。コマンドの前に** "no" **を置くことで特定の** 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- **有効な範囲**
no mst instance_id vlan vlan- **有効な範囲**

- instance_id — MST **インスタンス** ID（**範囲：**0-4094）
- vlan- **有効な範囲** — VLAN **範囲**（**範囲：**1-4093）

初期設定

なし

例

```
Console(config-mstp)#mst 10 vlan 10
Console(config-mstp)#
```

関連するコマンド

revision（P336）

spanning-tree system-bpduflooding

スパニングツリーをグローバルで無効にしたり、特定のポートを無効にする場合は、またはポートすべて、または同一の VLAN 上のポートにのみ BPDU のフラッディングを行います。コマンドの前に "no" を置くことにより、デフォルトの設定に戻ります。

文法

spanning-tree system-bpdu-flooding {to-all | to-vlan}

no spanning-tree system-bpdu-flooding

- to-all - スイッチのポートすべてに BPDU をフラッディングします。
- to-vlan - ポートのネイティブ VLAN のポートをすべてに BPDU（例えば、ポートの PVID により判別される）をフラッディングします。

初期設定

同一の VLAN 上のポートにのみフラッディンを行います。

コマンドモード

Global Configuration

コマンド解説

- ポートの BPDU フラッディングが無効な場合は、spanning-tree system-bpdu-flooding コマンドは効力を持ちません（spanning-tree port-bpduflooding コマンドを参照ください)。

例

```
Console(config)#spanning-tree system-bpdu-flooding to-all
Console(config)#
```

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。コマンドの前に "no" を置くことにより、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。コマンドの前に "no" を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(P336)

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。コマンドの前に** "no" **を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（P335）

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。コマンドの前に "no" を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 リジョンは 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 bpdu-filter

エッジポートで受信した BPDU をすべてフィルタリングします。コマンドの前に "no" を置くことにより、この機能は無効になります。

文法

[no] spanning-tree bpdu-filter

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **インタフェースで受信した** BPDUs **のフィルタリングを行って、**CPU **処理時間を節約します。この機能は、本機のエンドステーションにのみ接続されているエッジポートと共に動作するように設定されているため、**BPDUs **を処理する必要がありません。ただし、別のスイッチ、ブリッジデバイスに接続されているとランキングポートが誤ってエッジポートとして設定された場合、**BPDU **フィルタリング有効な場合については、スパニングツリーのループを引き起こす可能性があるため注意が必要です。**
- BPDU **フィルタリング機能を有効にする場合は、まずインタフェースを** spanning-tree edge-port **コマンドを使用してエッジポートに設定する必要があります。**

例

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

関連するコマンド

spanning-tree edge-port(P343)

spanning-tree bpdu-guard

BPDU を受信した場合に、エッジポート（高速転送用に設定されたインタフェースなど）をシャットダウンします。コマンドの前に "no" を置くことにより、この機能は無効になります。

文法

[no] spanning-tree bpdu-guard

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- エッジポートは、BPDU を生成しないエンドノードに接続する必要があります。エッジポートで BPDU を受信した場合は、ネットワークの設定が無効になるか、外部の侵入者により攻撃された可能性があることを示します。インタフェースが BPDU ガードによりシャットダウンされた場合は、no spanning-tree spanning-disabled コマンドを使って手動で再度有効にしなければなりません。
- BPDU ガードを有効にする場合は、インタフェースを spanning-tree edge-port コマンドを使ってエッジポートに設定する必要があります。インタフェースのエッジポートの属性が無効な場合は、BPDU ガードも無効になるため注意が必要です。

例

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

関連するコマンド

spanning-tree edge-port(P343)

spanning-tree spanning-disabled(P340)

spanning-tree spanning-disabled

特定のポートの STA を無効にします。コマンドの前に "no" を置くことで再び 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。コマンドの前に "no" を置くことにより、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。

ポートタイプ	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (IEEE 802.1D-2004)
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	200-20,000	200-20,000

初期設定

- デフォルトでは、各ポートで使用されている速度と Duplex モードが自動的に検出され、以下の値に応じてパスコストが設定されます。パスコスト「0」は、自動設定モードを 示します。ショートパスコスト方式が選択されており、IEEE 802.1w 規格で推奨

され ているデフォルトのパスコストが 65,535 **より大きい場合、デフォルトは** 65,535 **に設 定されます。**

ポートタイプ	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (IEEE 802.1D-2004)
Fast Ethernet	100,000	100,000
Gigabit Ethernet	100,000	100,000
10G Ethernet	1,000	1,000

コマンドモード

Interface (Ethernet, Port Channel)

spanning-tree port-priority

指定ポートのプライオリティを設定します。コマンドの前に "no" **を置くことにより、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 0
```

関連するコマンド

spanning-tree cost (P340)

spanning-tree edge-port

エッジに対するポートを指定します。コマンドの前に "no" **を置くことにより、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

- **インタフェースがブリッジ** LAN**、またはエンドノードの** LAN **セグメントに接続されている場合に使用可能です。エンドノードは、転送ループを発生させる可能性がないので、直接、スパニングツリー転送状態に移行することができます。　エッジポートを指定すると、ワークステーションやサーバなどのデバイスの速やかな輻輳制御を実現すること、最新の転送データベースを保持して再設定イベント時のアドレステーブルの再構築に必要なフレームフラッディングの量を削減すること、インタフェースの状態が変更された場合にスパニングツリーで再設定が開始されないようにすること、および、**STA **関連のその他のタイムアウト問題を克服することができます。ただし、エッジポートはエンドノードデバイスに接続されているポートに対してのみ有効にしなければならないという点に留意してください。**

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（P344）

spanning-tree portfast

ポートをポートファストに指定します。コマンドの前に "no" を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

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（P343）

spanning-tree link-type

RSTP のリンクタイプを設定します。コマンドの前に "no" を置くことにより、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 — ポイント間リンク
- 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 loopback-detection

ポートの STP **ループバック** BPDU **パケットの検出および応答が可能になります。コマンドの前に** "no" **を置くことにより機能は無効になります。**

文法

[no] spanning-tree loopback-detection

初期設定

Enabled

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **ループバック検出が有効になっておらず、インタフェースでそのインタフェースの** BPDU **が受信されると、**IEEE 802.1w-2001 9.3.4**（注** 1**）に従い、ループバック** BPDU **がドロップされます。**
- **ループバック検出は、スイッチでスパニングツリーが無効になっている場合はアクティブになりません。**

例

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

spanning-tree loopback-detection release-mode

loopback BPDU を受信した場合、破棄するためにポートをリリースモードを設定します。コマンドの前に "no" を置くことにより、デフォルト設定に戻ります。

文法

spanning-tree loopback-detection release-mode

{auto | manual}

no spanning-tree loopback-detection release-mode

- auto - ループバック状態が終了後、ポートは自動的に破棄状態を解除可能です。
- manual - ポートは、破棄状態を手動でのみ解除可能です。

初期設定

auto

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- インタフェースで自動ループバック解除が設定されている場合には、以下のいずれかの条件が満たされた時にのみ、ポートが転送状態に戻されます。
  - ポートでそのポートの BPDU 以外の BPDU が受信される場合
  - ポートのリンクステータスが、リンクダウンになってから再びリンクアップになる場合
  - ポートでそのポートの BPDU の受信が転送待機期間内に停止される場合
- ループバック検出が有効になっておらず、インタフェースでそのインタフェースの BPDU が受信されると、IEEE802.1w-20019.3.4（注 1）に従い、ループバック BPDU がドロップされます。
- ループバック検出は、スイッチでスパニングツリーが無効になっている場合はアクティブになりません。
- 手動解除モードが設定されている場合、リンクダウンイベントまたはリンクアップイベントが発生してもポートの破棄モードは解除されません。spanning-tree loopback-detection release コマンドを使用してのみ解除可能です。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode
manual
Console(config-if)#
```

spanning-tree loopback-detection trap

ポートの BPDU **ループバックの** SNMP **トラップ通知を有効にします。コマンドの前に** "no" **を置くことにより、デフォルト設定に戻ります。**

文法

[no] spanning-tree loopback-detection trap

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

spanning-tree mst cost

MST のインスタンスのパスコストの設定を行ないます。コマンドの前に "no" を置くことにより、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（ショートパスコスト：1-65535　ロングパスコスト：1-200,000,000　0 は自動設定 ）

初期設定

- デフォルトでは、各ポートで使用されている速度と Duplex モードが自動的に検出され、以下の値に応じてパスコストが設定されます。パスコスト「0」は、自動設定モードを示します。ショートパスコスト方式が選択されており、IEEE 802.1w 規格で推奨され ているデフォルトのパスコストが 65,535 より大きい場合、デフォルトは 65,535 に設 定されます。

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。
- 複数の spanning-tree アリゴリズムを用いて、デバイス間のベストなパスを決定するため、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。
- no spanning-tree mst cost コマンドを使用して、自動設定モードを指定します。
- 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 （P342）

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。コマンドの前に "no" を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 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

- 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（P349）

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（範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id**（範囲：**1-32**）**

コマンドモード

Privileged Exec

コマンド解説

- **本機が設定、トポロジーチェンジ** BPDU **を含む** STP BPDU **を検知した場合、該当するポートは自動的に** STP **互換モードにセットされます。**"spanning-tree protocol-migration" **コマンドを使用し、手動で選択したポートに対して最適な** BPDU **フォーマット（**RSTP **又は** STP **互換）の再確認を行うことができます。**

例

```
Console#spanning-tree protocol-migration ethernet 1/5
Console#
```

show spanning-tree

STP の設定内容を表示します。

文法

show spanning-tree [interface | mst instance-id]

interface

- ethernet unit/port
  - unit - スタックユニット (有効範囲 : 1-8)
  - port - ポート番号 (有効範囲 : 1-26)

instance-id - 複数のスパニングツリーのインスタンスの識別子

(有効範囲 : 0-4094、ゼロは先頭にきません。)

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- パラメータを使わず "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。
- show spanning-tree mst instance-id コマンドを使用した場合、MST 内のインスタンスのスパニングツリーの設定を表示します。
- “Spanning-tree information” の下に表示されている項目の詳細については、「Configuring Global Settings for STA」の項を、特定のインタフェースについて表示されている項目の詳細については、「Displaying Interface Settings for STA」の項を参照してください。

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                         : 32768.0.0001ECF8D8C6
Current Root Port                       : 21
Current Root Cost                       : 100000
Number of Topology Changes              : 5
Last Topology Change Time (sec.)        : 11409
Transmission Limit                      : 3
Path Cost Method                        : Long
---------------------------------------------------------------
Eth 1/ 1 information
---------------------------------------------------------------
Admin Status : Enabled
Role : Disabled
State : Discarding
External Admin Path Cost                : 0
Internal Admin Path Cost                : 0
External Oper Path Cost                 : 100000
Internal Oper Path Cost                 : 100000
Priority                                : 128
Designated Cost                         : 100000
Designated Port                         : 128.1
Designated Root                         : 32768.0.0001ECF8D8C6
Designated Bridge                       : 32768.0.123412341234
Fast Forwarding                         : Disabled
Forward Transitions                     : 4
Admin Edge Port                         : Disabled
Oper Edge Port                          : Disabled
Admin Link Type                         : Auto
Oper Link Type                          : Point-to-point
Spanning-Tree Status                    : Enabled
Loopback Detection Status               : Enabled
Loopback Detection Release Mode         : Auto
Loopback Detection Trap                 : Disabled
Root Guard Status                       : Disabled
BPDU Guard Status                       : Disabled
BPDU Filter Status                      : Disabled
...
```

show spanning-tree mst configuration

MST の設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-----------------------------------------------------------------
Configuration Name : R&D
Revision Level :0
Instance VLANs
-----------------------------------------------------------------
0             1-4093
Console
```

1.20 VLAN の設定

VLAN はネットワーク上のどこにでも位置することができますが、あたかもそれらが物理的な同一セグメントに属するかのように動作し、通信を行うポートのグループです。

ここでは VLAN 関連コマンドを使用し、指定するポートの VLAN グループの生成、メンバーポートの追加、VLAN タグ使用法の設定、自動 VLAN 登録の有効化を行います。

コマンドグループ	機能	ページ
GVRP and Bridge Extension	GVRP の設定	P356
Editing VLAN Groups	VLAN 名、VID、状態を含む VLAN の設定	P361
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	P363
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	P370
Configuring IEEE 802.1Q Tunneling	802.1Q トンネリング（QinQ）の設定	P371
Configuring Port-based Traffic Segmentation	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	P376
Configuring Protocolbased VLANs	フレームタイプおよびプロトコルを基にしたプロトコル VLAN の設定	P383
Configuring IP Subnet VLANs	IP サブネットベース VLAN を設定します。	P388
Configuring MAC Based VLANs	MAC-based VLAN を設定します。	P390
Configuring Voice VLANs	VoIP のトラフィックの検出を設定し、Voice VLAN を有効にします。	P392

1.20.1 GVRP およびブリッジの拡張

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設定します。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	P356
show bridge-ext	bridge extension 情報の表示	PE	P357
switchport gvrp	インタフェースへの GVRP の有効化	IC	P357
switchport forbidden vlan	インタフェースへの登録禁止 VLAN の設定	IC	P369
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	P358
garp timer	選択した機能への GARP タイマーの設定	IC	P359
show garp timer	選択した機能への GARP タイマーの表示	NE,PE	P360

bridge-ext gvrp

GVRP を有効に設定します。コマンドの前に "no" を置くことで機能を無効にします。

文法

bridge-ext gvrp

no bridge-ext gvrp

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- GVRP は、スイッチがネットワークを介してポートを VLAN メンバーとして登録するために VLAN 情報を交換する方法を設定します。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

例

```
Console#show bridge-ext
Maximum Supported VLAN Numbers : 4093
Maximum Supported VLAN ID : 4093
Extended Multicast Filtering Services : No
Static Entry Individual Port : Yes
VLAN Learning : IVL
Configurable PVID Tagging : Yes
Local VLAN Capable : No
Traffic Classes : Enabled
Global GVRP Status : Disabled
GMRP : Disabled
Console#
```

switchport gvrp

ポートの GVRP を有効に設定します。コマンドの前に "no" を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

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
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
    - unit — ユニット番号 （範囲：1-8）
    - port — ポート番号（範囲：1-26）
- port-channel channel-id（範囲：1-32）

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 1/7
Eth 1/ 7:
GVRP Configuration : Disabled
Console#
```

garp timer

leave、leaveall、join タイマーに値を設定します。コマンドの前に "no" を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である必要があります :
  leave >= (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 (P360)

show garp timer

選択したポートの GARP **タイマーを表示します。**

文法

show garp timer [interface]

- interface
  - ethernet unit/port
    - unit — **ユニット番号 （範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id**（範囲：**1-32**）**

初期設定

すべての GARP **タイマーを表示します。**

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP Timer Status:
Join Timer          : 20 centiseconds
Leave Timer       : 60 centiseconds
Leave All Timer : 1000 centiseconds

Console#
```

関連するコマンド

garp timer (P359)

1.20.2 VLAN グループの設定

コマンド	機能	モード	ページ
vlan database	VLAN database モードに入り、VLAN の設定を行う	GC	P361
VLAN	VID,VLAN 名、ステートなど VLAN の設定	VC	P362

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 (P370)

vlan

VLAN を設定します。コマンドの前に "no" を置くことで 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：1-4093）
- name — 識別するための VLAN 名
- vlan-name — 1-32 文字
- media ethernet — イーサネットメディアの種類
- state — VLAN のステートの識別
  - active — VLAN の実行
  - suspend — VLAN の中断。中断中の VLAN はパケットの転送を行いません。

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 4,094VLAN 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 (P370)

1.20.3 VLAN インタフェースの設定

コマンド	機能	モード	ページ
interface vlan	VLAN を設定するための Interface 設定モードへの参加	IC	P363
switchport mode	インタフェースの VLAN メンバーモードの設定	IC	P364
switchport acceptable frame types	インタフェースで受け入れ可能なフレームタイプの設定	IC	P365
switchport ingress-filtering	インタフェースへの入力フィルタの有効化	IC	P366
switchport native vlan	インタフェースの PVID(native VLAN) の設定	IC	P367
switchport allowed vlan	インタフェースに関連した VLAN の設定	IC	P368
switchport gvrp	インタフェースへの GVRP の有効化	IC	P357
switchport forbidden vlan	インタフェースの登録を禁止する VLAN の設定	IC	P369
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	P369

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：1-4093）

初期設定

なし

コマンドモード

Global Configuration

例

本例では、VLAN 1 の interface 設定モードに参加し、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 (P370)

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

switchport mode { hybrid | trunk }
no switchport mode

- hybrid — ハイブリッド VLAN インタフェースを指定。ポートはタグ付及びタグなしフレームを送信します。
- trunk — VLAN トランクに使用されるポートを指定します。トランクは 2 つのスイッチ間の直接接続で、ポートはソース VLAN を示すタグ付フレームを送信します。デフォルト VLAN に所属するフレームもタグ付フレームを送信します。

初期設定

すべてのポートは hybrid に指定され、VLAN 1 が PVID に設定されています。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

本例では、1 番ポートの設定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。コマンドの前に "no" **を置くことにより、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（P364）

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

[no] switch port ingress-filtering

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **イングレスフィルタリングはタグ付フレームにのみ有効です。**
- **イングレスフィルタリングが有効の場合、メンバーでない VLAN へのタグがついたフレームを受信すると、そのフレームは捨てられます。**
- **イングレスフィルタリングは GVRP や STP などの VLAN と関連のない BPDU フレームには影響を与えません。但し、VLAN に関連した GMRP などの BPDU フレームには影響を与えます。**

例

本例では、1 番ポートを指定し、イングレスフィルタリングを有効にしています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport 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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

switchport native vlan vlan-id

no switchport native vlan

- vlan-id — ポートへのデフォルト VLAN ID（範囲：1-4093）

初期設定

VLAN 1

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- PVID を設定するためには、対象のポートが指定する PVID と同じ VLAN に所属しており、またその VLAN がタグなしである必要があります。
- 受け入れ可能なフレームタイプを "all" にしている場合か、switchport モードを "hybrid" にしている場合、入力ポートに入るすべてのタグなしフレームには PVID が挿入されます。

例

本例では PVID を VLAN3 として 1 番ポートに設定しています。

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

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

switchport allowed vlan { add vlan-list [tagged | untagged] | remove vlan-list }

no switchport allowed vlan

- add vlan-list — 追加する VLAN の ID のリスト
- remove vlan-list — 解除する VLAN の ID のリスト
- vlan-list — 連続しない VLAN ID をカンマで分けて入力（スペースは入れない）。連続する ID はハイフンで範囲を指定（範囲：1-4093）

初期設定

すべてのポートが VLAN 1 に参加

フレームタイプはタグなし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- switchport モードが " trunk" に設定されている場合、インタフェースをタグ付メンバーとしてしか VLAN に設定できません。
- インタフェースの switchport mode が "hybrid" に設定されている場合、インタフェースを最低 1 つの VLAN にタグなしメンバーとして設定する必要があります。
- スイッチ内では常にフレームはタグ付となっています。タグ付及びタグなしパラメータはインタフェースへ VLAN を加えるとき使われ、出力ポートでフレームのタグをはずすか保持するかを決定します。
- ネットワークの途中や対向のデバイスが VLAN をサポートしていない場合、インタフェースはこれらの VLAN をタグなしメンバーとして加えます。1 つの VLAN にタグなしとして加え、その VLAN がネイティブ VLAN となります。
- インタフェースの禁止リスト上の VLAN が手動でインタフェースに加えられた場合、VLAN は自動的にインタフェースの禁止リストから削除されます。
- ポートへの接続装置にかかわらず、タグなし VLAN へ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 つのタグ無し VLAN にしか所属ができないので、もし 2 つ目の VLAN がタグなしと設定された場合、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。コマンドの前に** "no" **を置くことで禁止** VLAN **リストから削除します。**

文法

switchport forbidden vlan { add vlan-list | remove vlan-list }

no switchport forbidden vlan

- add vlan-list — **追加する** VLAN **の** ID **のリスト**
- remove vlan-list — **解除する** VLAN **の** ID **のリスト**
- vlan-list — **連続しない** VLAN ID **をカンマで分けて入力（スペースは入れない）。連続する** ID **はハイフンで範囲を指定（範囲：**1-4093**）**

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- GVRP **で自動的に** VLAN **に加えられることを防ぐためのコマンドです。**
- **インタフェース上で** VLAN **が許可** VLAN **にセットされている場合、同じインタフェースの禁止** VLAN **リストに加えることはできません。**

例

本例では 1 **番ポートを** VLAN 3 **に加えることを防いでいます。**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

1.20.4 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	P370
show interfaces status	特定 VLAN インタフェースの状態の表示	NE,PE	P258
show interfaces switchport	インタフェースの管理、運用状態の表示	NE,PE	P261

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、P377 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#
```

1.20.5 IEEE802.1Q トンネリングの設定

IEEE 802.1Q トンネリング（QinQ）機能を使用することにより、サービス プロバイダは複数の VLAN を設定しているカスタマを、1 つの VLAN を使用してサポートできます。カスタマの VID は保持されるため、さまざまなカスタマからのトラフィックは、同じ VLAN 上に存在するように見える場合でも、サービスプロバイダのインフラストラクチャ内では分離されています。QinQ トンネリングでは、VLAN 内 VLAN 階層を使用して、タグ付きパケットに再度タグ付けを行うこと（ダブルタギングとも呼ばれます）によって、VLAN スペースを拡張します。

この節では、QinQ トンネリングの設定に使用されるコマンドについて説明します。

コマンド	機能	モード	ページ
dot1q-tunnel system-tunnel-control	スイッチをノーマルモードまたは QinQ モードに設定	GC	P372
switchport dot1q-tunnel mode	インタフェースを QinQ トンネルポートに設定	IC	P373
switchport dot1q-tunnel tpid	トンネルポートの TPID（Tag Protocol Identifier）値を設定	IC	P374
show dot1q-tunnel	QinQ トンネルポートの設定を表示	PE	P375
show interfaces switchport	QinQ ポートステータスを表示	PE	P261

QinQ の一般的な設定方法

（1）スイッチを QinQ モードに設定（dot1q-tunnel system-tunnel-control P372）

（2）SPVLAN を作成 (vlan P362)

（3）QinQ トンネルアクセスポートを dot1Q トンネルアクセスモードに設定
（switchport dot1q-tunnel mode P373）

（4）トンネルアクセスポートの Tag Protocol Identifier (TPID) 値を設定。このステップは、接続されているクライアントが、802.1Q タグ付きフレームの識別に非標準 2-byte イーサタイプを使用している場合に必要です。
（switchport dot1q-tunnel tpid　P374）

（5）QinQ トンネルアクセスポートをタグ無しメンバーとして SPVLAN に追加
（switchport allowed vlan　P368）

（6）QinQ トンネルアクセスポートの SPVLAN ID をネイティブ VID として設定
（switchport native vlan　P367）

（7）QinQ トンネルアップリンクポートを dot1Q トンネルアップリンクモードに設定
（switchport dot1q-tunnel mode　P373）

（8）QinQ トンネルアップリンクポートをタグ付きメンバーとして SPVLAN に追加
（switchport allowed vlan　P368）

QinQ の制限事項

- トンネルアップリンクポートのネイティブ VLAN とトンネルアクセスポートは同一には出来ませんが、同じサービス VLAN を両方のトンネルポートタイプに設定することは可能です。
- トンネルポートでは IGMP スヌーピングを有効に出来ません。
- スパニングツリープロトコルが有効時に、スパニングツリー構造がツリーの中断を克服するために自動で再配置された場合、トンネルアクセスまたはトンネルアップリンクポートは無効になります。これらのポートではスパニングツリーを無効にすることが賢明です。

dot1q-tunnel system-tunnel-control

スイッチが QinQ モードで動作するよう設定を行います。"no" を前に置くと QinQ オペレーティングモードを無効にします。

文法

[no]dot1q-tunnel system-tunnel-control

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- QinQ インタフェース設定が機能するために、QinQ トンネルモードをスイッチで有効にしてください。

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

関連するコマンド

show dot1q-tunnel（P375）
show interfaces switchport（P261）

switchport dot1q-tunnel mode

インタフェースを QinQ **トンネルポートとして設定します。コマンドの前に** "no" **を置くことでインタフェースの** QinQ **を無効にします。**

文法

switchport dot1q-tunnel mode < access | uplink >
no switchport dot1q-tunnel mode

- access — **ポートを** 802.1Q **トンネルアクセスポートに設定**
- uplink — **ポートを** 802.1Q **トンネルアップリンクポートに設定**

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- switchport dot1q-tunnel mode **インタフェースコマンドを使用する前に、**dot1q-tunnel system-tunnel-control **コマンド（**P372**）を使用して** QinQ **トンネリングを有効にする必要があります。**
- **トンネルアップリンクポートがカスタマからのパケットを受信した際、カスタマタグ（**1**つ以上のタグレイヤがあるか否かにかかわらず）は内側に保持され、サービスプロバイダのタグが外側のタグに付加されます。**
- **トンネルアップリンクポートがサービスプロバイダからのパケットを受信した際、外側のサービスプロバイダタグは取り除かれ、パケットは内側のタグが示す** VLAN **へ渡されます。内側のタグが見つからない場合、パケットはアップリンクポートに設定されたネイティブ** VLAN **へ渡されます。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

関連するコマンド

show dot1q-tunnel（P375）
show interfaces switchport（P261）

switchport dot1q-tunnel tpid

トンネルポートの Tag Protocol Identifier (TPID) **値を設定します。コマンドの前に** "no" **を置くことで設定を初期値へ戻します。**

文法

switchport dot1q-tunnel tpid tpid
no switchport dot1q-tunnel tpid

- tpid — 802.1Q **カプセル化のイーサタイプ値を設定。この識別子は** 802.1Q **タグ付きフレームの識別に非標準** 2-byte **を選択するために使用します。標準イーサタイプ値は** 0x8100**（範囲：**0800-FFFF16 **進数）**

初期設定

0x8100

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- "switchport dot1q-tunnel tpid" **コマンドは選択されたインタフェースのカスタム** 802.1Q **イーサタイプ値を設定します。**
  この機能は本機へ、802.1Q **タグ付きフレームの識別に標準** 0x8100 **イーサタイプを使用しないサードパーティ製スイッチとインタオペレートすることを許可します。**
  例えば、0x1234 **はトランクポートのカスタム** 802.1Q **イーサタイプとして設定され、このイーサタイプを含む入力フレームは、イーサタイプフィールドに続くタグに含まれる** VLAN **へ、標準的** 802.1Q **トランクとして割り当てられます。**
  その他のイーサタイプを持つポートへ到着したフレームはタグ無しフレームとして見られ、このポートのネイティブ VLAN **へ割り当てられます。**
- **スイッチの全てのポートは同じイーサタイプに設定されます。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

関連するコマンド

show interfaces switchport（P261）

show dot1q-tunnel

QinQ トンネルポート情報を表示します。

コマンドモード

Privileged Exec

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel

Current double-tagged status of the system is Enabled

The dot1q-tunnel mode of the set interface 1/1 is Access mode,
TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/2 is Uplink mode,
TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/3 is Normal mode,
TPID is 0x8100.
.
.
.
```

関連するコマンド

switchport dot1q-tunnel mode（P375）

1.20.6 ポートベースのトラフィックセグメンテーション

ローカルネットワークでダウンリンクポートを使用して別々のクライアントからアップリンクポート経由でトラフィックをサービスプロバイダに渡すために高いセキュリティが必要な場合は、ポート単位のトラフィックセグメント化を使用して別々のダウンリンクポートのクライアント間でトラフィックを分離することができます。ダウンリンクポートでは、データトラフィックはアップリンクポートのみに転送され、アップリンクポートのみから転送されます。

各クライアントに属するトラフィックは、割り当てられているダウンリンクポートへと分離されます。ただし、スイッチは、クライアントで割り当てられているアップリンクポートを経由するトラフィックを他のクライアントに割り当てられているアップリンクポートから分離するように設定することも、他のクライアントで使用されているアップリンクポートによってトラフィックを転送するように設定して別々のクライアントがセキュリティ侵害の可能性の低いアップリンクポートへのアクセスを共有できるようにすることもできます。

コマンド	機能	モード	ページ
traffic-segmentation	**トラフィックのセグメント化を有効にします。**	GC	P377
traffic-segmentation session	**クライアントのセッションを設定します。**	IC	P379
traffic-segmentation uplink/ downlink	**クライアントのセッションのアップリンク / ダウンリンクポートを設定します。** Configures uplink/downlink ports for client sessions	IC	P380
traffic-segmentation uplink- to-uplink	**各クライアントセッションに割り当てられているアップリンクポート間で伝送可能かどうかを指定します。**	PE	P381
show traffic-segmentation	**設定されているトラフィックセグメントを表示します。**	PE	P382

traffic-segmentation

このコマンドは、トラフィックのセグメント化を有効にします。コマンドの前に ”no” **を付けることにより、無効になります。**

文法

[**no**] **traffic-segmentation**

デフォルト設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- **トラフィックのセグメント化により、ポートベースセキュリティおよび** VLAN **のポート間の切り離しを行うことができます。ダウンリンクポート上のデータのトラフィックは指定したアップリンクポート間でのみ伝送可能です。セグメント化された同じグループのダウンリンクポート間、同じグループに属さないポートにはデータの伝送を行うことはできません。**
- **トラフィックのセグメント化および通常の** VLAN **は同じスイッチ内で同時に存在することができます。トラフィックは、セグメント化されたグループのアップリンクポート間、および通常の** VLAN **のポート間では自由にトラフィックの送受信が可能です。**
- **トラフィックのセグメント化が有効な場合、クライアントセッションに割り当てられたアップリンクポートおよびダウンリンクポートの伝送状態は、以下の表を参照してください。**

Table 115: Traffic Segmentation Forwarding

宛先 **送信元**	**Session #1** **ダウンリンク**	Session #1 **アップリンク**	**Session #2** Downlinks	**Session #2** Uplinks	**Normal** Ports
Session #1 Downlink Ports	Blocking	Forwarding	Blocking	Blocking	Blocking
Session #1 Uplink Ports	Forwarding	Forwarding	Blocking	Blocking/ Forwarding	Forwarding
Session #2 Downlink Ports	Blocking	Blocking	Blocking	Forwarding	Blocking
Session #2 Uplink Ports	Blocking	Blocking/ Forwarding	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

* **アップリンクポート間の転送状態は、**traffic- segmentation uplink-to-uplink **コマンドにより設定されます。**

- トラフィックのセグメント化が無効になっている場合、すべてのポートは、VLAN やスパニングツリープロトコルなどの他の機能の設定に基づいて通常の転送モードで動作します。

- パラメータを指定せずに、traffic-segmentation コマンドを入力すると、トラフィックのセグメント化は有効になります。 traffic-segmentation uplink/downlink コマンドを使って、セグメント化されたグループのメンバーを設定します。
- no traffic-segmentation を入力すると、トラフィックのセグメント化が無効になり、セグメント化されたグループの設定がクリアになります。

例：

ここでは、トラフィックのセグメント化をグローバルで有効にします。

```
Console(config)#traffic-segmentation
Console(config)#
```

traffic-segmentation session

このコマンドにより、トラフィックセグメントのクライアントセッションを設定します。コマンドの前に "no" を付けると、クライアントセッションは無効になります。

文法

[**no**] **traffic-segmentation session** *session-id*

session-id – トラフィックのセグメントセッション (有効範囲 : 1-4)

デフォルト設定

None

コマンドモード

Global Configuration

コマンド解説

- 新規のトラフィックセグメントのクライアントセッションを設定します。
- コマンドの前に ”no” を付けことにより、割り当てられたアップリンク、またはダウンリンクを解除し、通常のオペレーティングモードにリストアします。

例：

```
Console(config)#traffic-segmentation session 1
Console(config)#
```

traffic-segmentation uplink/downlink

セグメント化されたポートのグループのアップリンク / ダウンリンクポートを設定します。コマンドの前に "no" を付ける前に、セグメント化されたグループのポートは無効になります。

文法

[**no**] **traffic-segmentation** [**session** *session-id*] {**uplink** *interface-list*
[**downlink** *interface-list*] | **downlink** *interface-list*}

session-id – トラフィックのセグメントセッション (有効範囲 : 1-4)

uplink – アップリンクインタフェースを指定します。

downlink – ダウンリンクインタフェースを指定します。

interface

ethernet *unit*/*port*

unit - ユニットの識別子 (有効範囲 : 1-8)

port - ポートの識別子 (有効範囲 : 1-26)

port-channel *channel-id* (有効範囲 : 1-32)

デフォルト設定

定義されていない場合は、セッション 1 となります。

セグメントされているポートグループは定義されてない。

コマンドモード

Global Configuration

コマンド解説

- ポートは、アップリンクポートおよびダウンリンクポートのリストには定義されていません。
- ポートは、1 つのトラフィックのセグメント化セッションにのみ割り当て可能です。
- アップリンク / ダウンリンクを指定する場合は、port フィールドではポートのリストは、ハイフンやコンマを使って入力可能です。*channel-id フィールドのリストはサポートされていません。*
- ダウンリンクポートは、同じセッションのアップリンクポートにのみ通信可能です。っそのため、アップリンクポートがセッションに設定されていない場合は、割り当てられたダウンリンクポートは、その他のポートとの通信を行うことはできません。
- セッションのダウンリンクポートが設定されていない場合は、割り当てれらたアップリンクポートは通常のポートとして動作します。

例：

ここでは、トラフィックのセグメント化は有効になった後、port 10 **をアップリンクとして設定し、**port 5-8 **をダウンリンクとして設定します。**

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/10
downlink ethernet 1/5-8
Console(config)#
```

traffic-segmentation uplink-to-uplink

このコマンドは、各クライアントセッションに割り当てられてアップリンクポート間でのトラフィックの伝送が可能かどうかを指定します。コマンドの前に "no" **を付ける前に、デフォルト設定に戻します。**

文法

[**no**] **traffic-segmentation uplink-to-uplink** {**blocking** |

forwarding}

blocking – **各セッションに割り当てれらえたアップリンク間のトラフィックをブロックします。**

forwarding – **各セッションに割り当てれらえたアップリンク間のトラフィックを伝送します。**

デフォルト設定

Blocking

コマンドモード

Global Configuration

例：

ここでは、各クライアントセッションに割り当てられたアップリンクポート間のトラフィックの伝送を可能にします。

```
Console(config)#traffic-segmentation uplink-to-uplink forwarding
Console(config)#
```

show traffic- segmentation

ここでは、設定されたトラフィックセグメントを表示します。

コマンドモード

Privileged Exec

例：

```
Console#show traffic-segmentation
Private VLAN Status : Enabled
Uplink-to-Uplink Mode : Forwarding
Session Uplink Ports Downlink Ports
--------- ------------------------------ -----------------------
------
1 Ethernet 1/1 Ethernet 1/2
Ethernet 1/3
Ethernet 1/4
Console#
```

1.20.7 プロトコル VLAN の設定

通常の VLAN では、プロトコル毎の VLAN グループの形成を容易に行なうことはできません。そのため、特定のプロトコルに関連するすべての機器が通信を行えるよう、特殊なネットワーク機器を使用して異なる VLAN 間の通信をサポートする必要があります。
しかし、このような方法では、セキュリティと容易な設定が可能な VLAN のメリットを失ってしまいます。

このような問題を回避するため、本機では物理的なネットワークの構成を、プロトコルを基にした論理的 VLAN のネットワーク構成とすることが可能なプロトコルベース VLAN 機能を提供します。ポートがフレームを受信した際、受信フレームのプロトコルタイプに応じて VLAN メンバーシップが決定されます。

コマンド	機能	モード	ページ
protocol-vlan protocol-group	プロトコルグループの作成及びサポートプロトコルの指定	GC	P384
protocol-vlan protocol-group	プロトコルグループの VLAN へのマッピング	IC	P385
show protocol-vlan protocol-group	プロトコルグループの設定の表示	PE	P386
show interfaces protocol-vlan protocol-group	プロトコルグループにマッピングされたインタフェースと関連する VLAN の表示	PE	P387

プロトコル VLAN の設定は以下の手順で行ないます。

（1）使用するプロトコルのための VLAN グループを作成します。主要なプロトコル毎に VLAN の作成を行なうこと推奨します。また、この時点ではポートメンバーの追加を行なわないで下さい。

（2）VLAN に設定するプロトコル毎のグループを "protocol-vlan protocol-group" コマンド (General Configuration mode) を利用して生成します。

（3）適切な VLAN に各インタフェースのプロトコルを "protocol-vlan protocol-group" コマンド (Interface Configuration mode) を利用してマッピングします。

protocol-vlan protocol-group (Configuring Groups)

プロトコルグループの作成及び特定のプロトコルのグループへの追加を行ないます。コマンドの前に "no" **を置くことでプロトコルグループを削除します。**

文法

protocol-vlan protocol-group group-id [{ add | remove } frame-type frame protocol-type protocol]

no protocol-vlan protocol-group group-id

- group-id — **プロトコルグループ** ID**（設定範囲：**1-2147483647**）**
- frame — **プロトコルのフレームタイプ（選択肢：**ethernet,rfc_1042, snap_8021h, snap_other, llc_other**）**
- protocol — **プロトコルタイプ。フレームタイプが** llc_other **のフレームの選択肢は** ipx_raw **です。その他のフレームタイプの場合は** ip, arp, rarp **です。（範囲：**0801-FFFF 16 **進数）**

初期設定

プロトコルグループ未設定

コマンドモード

Global Configuration

例

プロトコルグループ "1" **を作成し、フレームタイプを** "Ethernet"**、プロトコルタイプを** "IP" **及び** "ARP" **に設定しています。**

```
Console(config)#protocol-vlan protocol-group 1 add frame-type
 ethernet protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type
 ethernet protocol-type arp
Console(config)#
```

protocol-vlan protocol-group (Configuring Interfaces)

インタフェースにおいてプロトコルグループを VLAN にマッピングします。"no" を前におくことでインタフェースのプロトコルのマッピングを解除します。

文法

protocol-vlan protocol-group group-id vlan vlan-id

no protocol-vlan protocol-group group-id vlan

- group-id — **プロトコルグループ** ID（**設定範囲：**1-2147483647）
- vlan-id — **致したプロトコルの通信が転送される** VLAN（**設定範囲：**1-4093）

初期設定

プロトコルグループはインタフェースにマッピングされていません。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **インタフェースの設定を行なって下さい。他の** VLAN **コマンドを使用した場合、設定したインタフェースはすべてのプロトコルタイプの通信を関連した** VLAN **に対して行います。**
- **フレームがプロトコル** VLAN **に割り当てられたポートに入力する場合、以下の方法で処理されます。**
  - **フレームにタグ付フレームの場合、タグの情報に基づき処理されます。**
  - **フレームがタグなしフレームで、プロトコルタイプが一致した場合、フレームは適切な** VLAN **に転送されます。**
  - **フレームがタグなしフレームで、プロトコルタイプが一致しない場合、フレームはインタフェースのデフォルト** VLAN **に転送されます。**

例

本例では、1 **番ポートに入ってきた通信でプロトコルグループ** 1 **と一致する通信が** VLAN2 **にマッピングしています。**

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

プロトコルグループに関連したフレーム及びプロトコルタイプの表示

文法

show protocol-vlan protocol-group [group-id]

- group-id — **プロトコルグループ** ID（**設定範囲：**1-2147483647）

初期設定

すべてのプロトコルグループを表示

コマンドモード

Privileged Exec

例

プロトコルグループ 1 **が** Ethernet、IP **に設定されていることを表示しています。**

```
Console#show protocol-vlan protocol-group
ProtocolGroup ID     Frame Type   Protocol Type
------------------ ------------- ---------------
               1     ethernet           08 00
Console#
```

show interfaces protocol-vlan protocol-group

選択したインタフェースのプロトコルグループと VLAN **のマッピング情報を表示します。**

文法

show interfaces protocol-vlan protocol-group [interface]

- Interface
  - ethernet unit/port
    - unit — **ユニット番号 （範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
- - port-channel channel-id (**範囲：**1-32)

初期設定

すべてのプロトコルグループを表示

コマンドモード

Privileged Exec

例

1 **番ポートに入ってきた通信でプロトコルグループ** 1 **と一致する通信が** VLAN2 **にマッピングされています。**

```
Console#show interfaces protocol-vlan protocol-group
   Port      ProtocolGroup ID   Vlan ID
---------- ----------------- -----------
   Eth 1/1                 1       vlan2
Console#
```

1.20.8 サブネット VLAN の設定

IP サブネットベースの VLAN 分類を有効にすると、タグなしイングレスフレームの送信元アドレスが IP subnet-to-VLAN テーブルと照合されます。そのサブネットのエントリが見つかった場合、フレームは、エントリで示されている VLAN に割り当てられます。該当する IP サブネットがない場合、タグなしフレームは、受信ポートの VLAN ID（PVID）に属するものとして分類されます。

コマンド	機能	モード	ページ
subnet-vlan	IP サブネット VLAN を設定します。	GC	P388
show subnet-vlan	IP サブネット VLAN の設定を表示します。	PE	P389

subnet-vlan

IP サブネット VLAN の設定を行います。コマンドの前に ”no” を置くことにより、IP subnet-to-VLAN 設定を削除します。

構文

subnet-vlan subnet ip-address mask vlan vlan-id [priority priority]

no subnet-vlan subnet {ip-address mask | all}

- ip-address – T サブネットの IP アドレス。有効な IP アドレスは、0 〜 255 の 10 進数を 4 つ組み合わせ、それぞれをピリオドで区切って設定されます。
- mask– このマスクによって IP サブネットのホストアドレスビットを識別します。
- vlan-id– 対応する IP サブネットトラフィックの転送先の VLAN（範囲 :1 〜 4,093）。
- priority– タグなしイングレストラフィックに割り当てられる優先度（範囲 :0 〜 7（7 が最も高い）、デフォルト :0）。

初期設定

Priority: 0

コマンドモード

Global Configuration

コマンド解説

- それぞれの IP サブネットは 1 つの VLANID にのみマップすることができます。IP サブネットは IP アドレスとマスクから設定されます。
- タグなしのフレームがポートで受信されると、その送信元 IP アドレスが IP サブネット - VLAN マッピングテーブルと照合され、エントリが見つかった場合は、対応する VLANID がフレームに割り当てられます。該当するエントリが見つからない場合は、受信ポートの PVID がフレームに割り当てられます。
- IP サブネットは、ブロードキャスト IP アドレスまたはマルチキャスト IP アドレスにすることはできません。
- MAC ベース VLAN、IP サブネットベース VLAN、およびプロトコルベース VLAN が同時にサポートされる場合、優先順位は、MAC ベース、IP サブネットベース、プロトコルベースの順になり、ポートベースが最後になります。

例

以下の例では、サブネット 192.168.12.192、マスク 255.255.255.224 のトラフィックを VLAN 4 に設定します。

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224
vlan 4
Console(config)#
```

show subnet-vlan

IP サブネットの VLAN 設定を表示します。

コマンドモード

Privileged Exec

コマンド解説

subnet-to-VLAN マッピングを表示します。

複数のエントリが一致した場合は、最後に一致したエントリを使用します。

例

以下の例では、設定した IP subnet-based VLAN を表示します。

```
Console#show subnet-vlan
IP Address Mask VLAN ID Priority
--------------- --------------- ------- --------
192.168.12.0 255.255.255.128 1 0
192.168.12.128 255.255.255.192 3 0
192.168.12.192 255.255.255.224 4 0
192.168.12.224 255.255.255.240 5 0
192.168.12.240 255.255.255.248 6 0
192.168.12.248 255.255.255.252 7 0
192.168.12.252 255.255.255.254 8 0
192.168.12.254 255.255.255.255 9 0
192.168.12.255 255.255.255.255 10 0
Console#
```

1.20.9 MAC ベース VLAN の設定

IP サブネットベースの VLAN 分類を有効にすると、タグなしイングレスフレームの送信元アドレスが IP サブネット –VLAN マッピングテーブルと照合されます。そのサブネットのエントリが見つかった場合、フレームは、エントリで示されている VLAN に割り当てられます。該当する IP サブネットがない場合、タグなしフレームは、受信ポートの VLAN ID（PVID）に属するものとして分類されます。

IEEE 802.1Q ポート VLAN を使用する場合は、ポートで受信されたタグなしフレームはそのポートに関連のある PVID の VLAN に属するものとして分類されます。

MAC ベース VLAN を有効にすると、タグなしイングレスフレームの送信元アドレスが MAC address-to-VLAN mapping テーブルと照合されます。そのサブネットのエントリが見つかった場合、フレームは、エントリで示されている VLAN に割り当てられます。該当する MAC アドレスがない場合、タグなしフレームは、受信ポートの VLAN ID（PVID）に属するものとして分類されます。

コマンド	機能	モード	ページ
mac-vlan	MAC address-to-VLAN マッピングを設定します。	GC	P390
show mac-vlan	MAC address-to-VLAN 設定を表示します。	PE	P391

mac-vlan

MAC address-to-VLAN マッピングを設定します。コマンドの前に ”no” を置くことにより設定は解除されます。

文法

mac-vlan mac-address mac-address vlan vlan-id [priority priority]

no mac-vlan mac-address {mac-address | all}

- mac-address – 照合する MAC アドレス。設定した MAC アドレスはユニキャストアドレスのみです。MAC アドレスは xx-xx-xx-xx-xx-xx 、または xxxxxxxxxxxx 形式で設定してください。
- vlan-id – 送信元 MAC アドレスのトラフィックを転送する VLAN(有効範囲 : 1-4093)
- priority – タグなし入力トラフィックに割り当てられるプライオリティ (有効範囲 : 0-7、この場合プライオリティの一番高い値は「7」です)

初期設定

None

コマンドモード

Global Configuration

コマンド解説

- MAC-to-VLAN マッピングは、すべてのポートに適用されます。
- 送信元の MAC アドレスはがマッピング可能な VLAN ID は 1 つのみです。
- 設定した MAC アドレスは、ブロードキャスト、あるいはマルチキャストアドレスは設定できません。

- MAC ベース VLAN、IP サブネットベース VLAN、およびプロトコルベース VLAN が同時にサポートされる場合、優先順位は、MAC ベース、IP サブネットベース、プロトコルベースの順になり、ポートベースが最後になります。

例

以下の例では、送信元の MAC アドレス 00-00-00-11-22-33 からのトラフィックを VLAN 10 に設定します。

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10
Console(config)#
```

show mac-vlan

MAC address-to-VLAN 設定を表示します。

コマンドモード

Privileged Exec

コマンド解説

MAC address-to-VLAN マッピングを表示します。

例

以下の例では、設定している MAC アドレスベース VLAN をすべて表示します。

```
Console#show mac-vlan
MAC Address VLAN ID Priority
----------------- -------- --------
00-00-00-11-22-33 10 0
Console#
```

1.20.10 音声 VLAN の設定

ネットワークの音声 VLAN を指定して、VoIP トラフィックの CoS 優先度を設定することができます。パケットの送信元 MAC アドレスを使用して VoIP トラフィックをスイッチポートで検出するか、LLDP（IEEE 802.1AB）を使用して、接続されている VoIP デバイスを検出することができます。設定されたポートで VoIP トラフィックが検出されると、そのポートは、自動的に、音声 VLAN のタグ付きメンバーとして割り当てられます。あるいは、スイッチポートを手動で設定することができます。

コマンド	機能	モード	ページ
voice vlan	音声 VLAN ID を設定します。	GC	P392
voice vlan aging	音声 VLAN ポートのエイジングタイムを設定します。	GC	P394
voice vlan mac-address	VoIP デバイスの MAC アドレスを設定します。	GC	P395
switchport voice vlan	音声 VLAN ポートモードを設定します。	IC	P396
switchport voice vlan priority	ポートの VoIP トラフィックのプライオリティを設定します。	IC	P397
switchport voice vlan rule	ポートの VoIP トラフィックの自動検出方法を設定します。	IC	P398
switchport voice vlan security	音声 VLAN セキュリティを有効にします。	IC	P399
show voice vlan	音声 VLAN の設定を表示します。	PE	P400

voice vlan

VoIP トラフィックの検出を有効にして、音声 VLAN ID を設定します。コマンドの前に ”no” を置くことにより音声 VLAN を無効にします。

文法

voice vlan voice-vlan-id

no voice vlan

- voice-vlan-id - 音声 VLAN ID を指定します (有効範囲 : 1-4093)

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- IP テレフォニーがエンタープライズネットワークで展開されている場合には、VoIP（Voice over IP）トラフィックを他のデータトラフィックから分離することをお勧めします。トラフィックを分離すると、過度のパケット遅延、パケット損失、およびジッタを防いで、より高い音声品質を実現することができます。そのための最善策は、すべての VoIP トラフィックを単一の音声 VLAN に割り当てることです。

-
- ネットワークの音声 VLAN を指定して、VoIP トラフィックの CoS 優先度を設定することができます。パケットの送信元 MAC アドレスを使用して VoIP トラフィックをスイッチポートで検出するか、LLDP（IEEE 802.1AB）を使用して、接続されている VoIP デバイスを検出することができます。設定済されたポートで VoIP トラフィックが検出されると、そのポートは、自動的に、音声 VLAN のタグ付きメンバーとして割り当てられます。あるいは、スイッチポートを手動で設定することができます。
- ネットワークの音声 VLAN ID を設定します。サポートされる音声 VLAN は 1 つだけであり、その音声 VLAN は既にスイッチで設定されていなければなりません。
- global auto-detection のステータスが有効な場合、音声 VLAN ID を修正することはできません (switchport voice vlan を参照ください)。

例

以下の例では、VoIP トラフィックの検出を有効にして、音声 VLAN ID を「1234」に設定します。

```
Console(config)#voice vlan 1234
Console(config)#
```

voice vlan aging

音声 VLAN ID のタイムアウトを設定します。コマンドの前に "no" を置くことによりデフォルト設定に戻ります。

文法

voice vlan aging minutes

no voice vlan

- minutes - ポートの音声 VLAN のメンバーのタイムアウトを指定します (有効範囲 : 5-43200 分)

初期設定

1440 分

コマンドモード

Global Configuration

コマンド解説

- 音声 VLAN のエイジングタイムは、ポート上で VoIP トラフィックが受信されなくなった場合に、音声 VLAN からポートを削除するために要する時間です。

例

以下の例では、音声 VLAN のエイジングタイムを「3000 分」に設定します。

```
Console(config)#voice vlan aging 3000
Console(config)#
```

voice vlan macaddress

MAC アドレスの範囲を指定して、OUI Telephony リストに追加します。コマンドの前に ”no” を置くことにより、リストからエントリを削除します。

文法

voice vlan mac-address mac-address mask mask-address

[description description]

no voice vlan mac-address mac-address mask mask-address

- mac-address - ネットワークの VoIP デバイスを識別する MAC アドレスの OUI を設定します (例えば、01-23-45-00-00-00)
- mask-address - MAC アドレスの範囲を指定します (有効範囲 : 80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF)
- description - VoIP デバイスを識別するユーザに設定されたテキスト (有効範囲 : 1-32 文字)

初期設定

None

コマンドモード

Global Configuration

コマンド解説

- スイッチに接続されている VoIP デバイスは、受信パケットの送信元 MAC アドレスに含まれているベンダーの OUI（Organizational Unique Identifier）によって識別することができます。OUI 番号は、ベンダーに割り当てられ、デバイスの MAC アドレスの先頭の 3 octets を形成します。VoIP 装置の MAC OUI 番号は、それらの装置からのトラフィックが VoIP トラフィックとして認識されるようにスイッチで設定することができます。
- FF-FF-FF-00-00-00 というマスクを設定すると、同じ OUI（先頭の 3octets）をもつすべてのデバイスが特定されます。他のマスクは、MAC アドレス範囲を制限します。FF-FF-FF-FF-FF-FF というマスクは、単一の MAC アドレスを指定します（デフォルト :FF-FF-FF-00-00-00）。

例

以下の例では、MAC OUI を OUI Telephony リストに追加します。

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-
ff-ff-00-00-
00 description A new phone
Console(config)#
```

switchport voice vlan

ポートの音声 VLAN モードを指定します。コマンドの前に "no" を置くことにより、ポートの VLAN 機能を無効にします。

文法

switchport voice vlan {manual | auto}

no switchport voice vlan

- manual - ポートの音声 VLAN 機能を有効にしますが、ポートは音声 VLAN に手動で追加する必要があります。
- auto - ポートの VoIP トラフィックが検出された場合、ポートをタグ付きメンバーとして音声 VLAN に追加します。

初期設定

Disabled

コマンドモード

Interface Configuration

コマンド解説

「auto」を選択する場合は、switchport voice vlan rule コマンドを使用して、VoIP トラフィック、OUI あるいは IEEE802.1ab(LLDP) を検出する方法を指定する必要があります。「OUI」を選択する場合は、voice vlan mac-address コマンドを使って、Telephony OUI リストの MAC アドレスの範囲を必ず設定してください。

例

以下の例では、port 1 を音声 VLAN 自動モードに設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

switchport voice vlan priority

VoIP トラフィックの CoS プライオリティを指定します。コマンドの前に ”no” を置くことにより、デフォルトのプライオリティに戻ります。

文法

switchport voice vlan priority priority-value

no switchport voice vlan priority

- priority-value - CoS プライオリティの値 (有効範囲 : 0-6)

初期設定

6

コマンドモード

Interface Configuration

コマンド解説

CoS プライオリティを指定して、音声 VLAN にポートの VoIP トラフィックを適用します。音声 VLAN 機能が有効な場合、受信した VoIP パケットのプライオリティは新しいプライオリティにより上書きされます。

例

以下の例では、port 1 の CoS プライオリティを「5」に設定します。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

switchport voice vlan rule

ポートの VoIP トラフィックの検出方法を選択します。コマンドの前に ”no” を置くことにより、ポートの検出方法が無効になります。

文法

[no] switchport voice vlan rule {oui | lldp}

- oui - VoIP デバイスからのトラフィックを送信元の MAC アドレスの OUI により検出します。
- lldp - LLDP を使用して、ポートに接続されている VoIP デバイスを検出します。

初期設定

OUI: Enabled

LLDP: Disabled

コマンドモード

Interface Configuration

コマンド解説

- 「OUI」を選択する場合は、Telephony OUI リストの MAC アドレスの範囲を必ず設定してください (詳細については、voice vlan mac-address コマンドを参照ください)。MAC アドレスの OUI 番号は、Telephony OUI リストで設定する必要があるため、本機は VoIP デバイスからのトラフィックを認識します。
- LLDP はシステム対応 TLV の “telephone bit” が「ON」であるかどうか確認します（詳細については、LLDP コマンドを参照ください。

例

以下の例では、VoIP トラフィックを検出するために port 1 の OUI 方式を有効にします。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

switchport voice vlan security

ポートの VoIP **トラフィックのセキュリティのフィルタリングを有効にします。コマンドの前に** ”no” **を置くことにより、フィルタリング機能を無効にします。**

文法

[no] switchport voice vlan security

初期設定

Disabled

コマンドモード

Interface Configuration

コマンド解説

- **セキュリティフィルタリング機能は、ポートで受信される音声** VLANID **タグ付きの非** VoIP **パケットを破棄します。**
- VoIP **トラフィックは、**TelephonyOUI **リストで設定されている送信元** MAC **アドレスによって、または、スイッチに接続されている** VoIP **デバイスを検出する** LLDP **を使用して、特定されます。**VoIP **送信元以外の送信元から受信されるパケットはドロップされます。**
- **有効にする場合は、**VoIP **デバイスの** MAC **アドレスの範囲を** Telephony OUI **リスト（**voice vlan mac-address**）に必ず設定してください。**

例

以下の例では、port 1 **のセキュリティのフィルタリング機能を有効にします。**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

show voice vlan

音声 VLAN **設定値および** OUI Telephony **リストを表示します。**

文法

show voice vlan {oui | status}

- oui - OUI Telephony **リストを表示します。**
- status - **グローバルおよびポートの音声** VLAN **設定値を表示します。**

初期設定

None

コマンドモード

Privileged Exec

例

```
Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status : Enabled
Voice VLAN ID : 1234
Voice VLAN aging time : 1440 minutes
Voice VLAN Port Summary
Port Mode Security Rule Priority Remaining Age
(minutes)
-------- -------- -------- --------- -------- -------------
Eth 1/ 1 Auto Enabled OUI 6 100
Eth 1/ 2 Disabled Disabled OUI 6 NA
Eth 1/ 3 Manual Enabled OUI 5 100
Eth 1/ 4 Auto Enabled OUI 6 100
Eth 1/ 5 Disabled Disabled OUI 6 NA
Eth 1/ 6 Disabled Disabled OUI 6 NA
Eth 1/ 7 Disabled Disabled OUI 6 NA
Eth 1/ 8 Disabled Disabled OUI 6 NA
Eth 1/ 9 Disabled Disabled OUI 6 NA
Eth 1/10 Disabled Disabled OUI 6 NA
Console#show voice vlan oui
OUI Address Mask Description
----------------- ----------------- ----------------------------
--
00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone
Console#
```

1.21 CoS (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	P401
Priority (Layer 3 and 4)	TCP ポート、IP DSCP タグの CoS 値への設定	P408

1.21.1 プライオリティコマンド（Layer 2）

コマンド	機能	モード	ページ
queue mode	キューモードを "strict" 又は " Weighted Round-Robin (WRR)" に設定	IC	P402
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	P403
queue weight	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	IC	P404
queue cos map	プライオリティキューに Class of Service(CoS) を指定	IC	P405
show queue mode	現在のキューモードを表示	PE	P406
show queue weight	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	P406
show queue cos-map	CoS マップの表示	PE	P407
show interfaces switchport	インタフェースの管理、運用ステータスの表示	PE	P261

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。コマンドの前に "no" を置くことにより、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 0-7 にそれぞれスケジューリングウエイト 1、2、4、6、8、10、12、14 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

Interface Configuration

コマンド解説

- プライオリティモードを "strict" に設定した場合、出力キューの高いプライオリティのキューが優先され、低いプライオリティのキューは高いプライオリティのキューがすべてなくなった後に送信されます。
- プライオリティモードを "wrr" に設定した場合、WRR はキュー 0-3 にそれぞれスケジューリングウエイト 1、2、4、6 を設定し、その値に応じて各キューの使用する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。コマンドの前に "no" を置くことにより、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 IEEE8021Q タグ付フレームの場合、IEEE802.1p のプライオリティ bit が使用されます。このプライオリティは IEEE802.1Q VLAN tagging フレームには適用されません。
- 本機では 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 weight" 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 weight

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

queue weight weight0...weight7
no queue weight

- weight0...weight7 - キュー 0 〜 7 の WRR スケジューラで使用される重みの比率（範囲：1-15)

初期設定

1、2、4、6、8、10、12、14 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

Interface 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 if)#queue weight 6 9 12
Console(config if)#
```

関連するコマンド

show queue weight（P406）

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

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

no queue cos-map

- queue_id - CoS プライオリティキュー ID

  ー 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 で設定されています。設定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

```
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 weight

ラウンドロビン（WRR）バンド幅を表示します。

文法

show queue weight [interface]

- Interface
  - ethernet unit/port
    - unit — **ユニット番号 （範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
- port-channel channel-id (**範囲：**1-32)

初期設定

なし

コマンドモード

Privileged Exec

例

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

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
    - unit — ユニット番号 （範囲：1-8）
    - port — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)

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#
```

1.21.2 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 port	サービスマッピングの TCP/UDP クラスを有効化	GC	P408
map ip port	TCP/UDP ソケットを CoS にマップ	IC	P409
map ip precedence	IP precedence の CoS マッピングの有効化	GC	P409
map ip precedence	IP precedence 値を CoS キューへマッピング	IC	P410
map ip dscp	IP DSCP の CoS マッピングの有効化	GC	P411
map ip dscp	IP DSCP 値を CoS キューへマッピング	IC	P412
show map ip port	IP ポートマップの表示	IC	P413
show map ip precedence	IP Precedence マップの表示	PE	P414
show map ip dscp	IP DSCP マップの表示	PE	P415

map ip port（Global Configuration）

IP ポートプライオリティを設定します。コマンドの前に "no" を置くことで設定を解除します。

文法

[no] map ip port

初期設定

無効

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 ポート、IP Precedence/DSCP/ToS、デフォルトポートプライオリティです。

例

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

map ip port（interface Configuration）

IP ポートプライオリティマッピングの設定を行います。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

map ip port [port-number cos cos-queue]

no map ip port [port-number]

- port-number — 16-bit TCP/UDP ポート番号（範囲：0-65535）
- cos-queue — CoS 値（範囲：0-7）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

map ip precedence（Global Configuration）

IP precedence マッピングを設定します。コマンドの前に "no" を置くことで設定を解除します。

文法

[no] map ip precedence

初期設定

無効

コマンドモード

Global Configuration

例

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

map ip precedence（interface Configuration）

IP precedence プライオリティマッピングの設定を行います。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

map ip precendence [ip-precedence-value cos cos-value]

no map ip precedence

- ip-precedence-value — 3bit precedence 値（範囲：0-7）
- cos-queue — CoS 値（範囲：0-7）

初期設定

以下はデフォルトプライオリティマッピング値になります。

IP Precedence 値	0	1	2	3	4	5	6	7
CoS 値	0	1	2	3	4	5	6	7

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

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

map ip dscp（Global Configuration）

IP DSCP (Differentiated Services Code Point mapping) マッピングを有効にします。コマンドの前に "no" を置くことで機能を無効にします。

文法

[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。コマンドの前に "no" を置くことにより、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 port

IP ポートプライオリティマップを表示します。

文法

show map ip port [interface]

- interface
  - ethernet unit/port
    - unit — ユニット番号 （範囲：1-8）
    - port — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip port
TCP port mapping status: disabled

 Port      Port no.  COS
 --------- --------  ---
 Eth 1/ 5    80       0
Console#
```

show map ip precedence

IP ポートプライオリティマップを表示します。

文法

show map ip precedence [interface]

- interface
  - ethernet unit/port
    - unit — ユニット番号 （範囲：1-8）
    - port — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence  COS
 --------- ----------  ---
  Eth 1/ 5         0    0
  Eth 1/ 5         1    1
  Eth 1/ 5         2    2
  Eth 1/ 5         3    3
  Eth 1/ 5         4    4
  Eth 1/ 5         5    5
  Eth 1/ 5         6    6
  Eth 1/ 5         7    7
Console
```

関連するコマンド

map ip precedence（P414）

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　（範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id (**範囲：**1-32)

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: disabled

  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）（P411）
map ip dscp（Interface Configuration）（P412）

1.22 QoS

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

コマンド	機能	モード	ページ
class-map	クラスマップを作成	GC	P417
match	クラス分類のためトラフィックに使う条件を設定	CM	P418
rename	クラスマップの名前を再設定	CM	P419
description	クラスマップの説明を指定	CM	P419
policy-map	ポリシーマップを作成	GC	P420
class	ポリシー上で実行するクラスを設定	PM	P421
rename	クラスマップの名前を再設定	PM	P419
set	IP パケットに適用する CoS、DSCP、IP Precedence の値を設定	PM-C	P422
police	クラス分けされたトラフィックに制限を設定	PM-C	P423
service-policy	ポリシーマップをインタフェースに適用	IC	P424
show class-map	クラスマップの情報を表示	PE	P425
show policy-map	ポリシーマップの情報を表示	PE	P426
show policy-map interface	インタフェースに設定されたポリシーマップの情報を表示	PE	P426

特定の入力トラフィックにポリシーを設定する方法は下記の通りです。

(1) class-map コマンドを使用してクラスの名前を設定し、クラスマップコンフィグレーションモードに入ります。

(2) アクセスリスト、DSCP と IP Precedence の値、VLAN 情報を基にトラフィックをフィルタするため match コマンドを使用します。

(3) match コマンドで指定した条件でのトラフィックのフィルタを有効にするため、ACL を設定します。

(4) ポリシーの名前を指定し、ポリシーマップコンフィグレーションモードに入るため、policy-map コマンドを使用します。

(5) クラスマップをポリシーマップに割り当てるために class コマンドを使用し、ポリシーマップ・クラスコンフィグレーションモードに入ります。ポリシーマップには複数のクラス設定を含めることができます。

(6) クラス情報と一致するトラフィックに QoS の値を設定するため set コマンドを使用します。また帯域幅とバーストレートを制限するため police コマンドを使用します。police コマンドではトラフィックが指定したレートを越えたとき、そのトラフィックを破棄するか、トラフィックの DSCP の値を減少させるよう設定できます。

（7）インタフェースにポリシーマップを割り当てるため、service-policy コマンドを使用します。

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

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

class-map

このコマンドはクラスマップを作成し、クラスマップコンフィグレーションモードに移行します。"no" を付けるとクラスマップを削除し、グローバルコンフィグレーションモードに戻ります。

文法

[no] class-map class-map-name [match-any]

- match-any — クラスマップの条件のうちいずれか 1 つに一致するトラフィックを対象
- class-map-name — クラスマップ名（1-16 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 最初にこのコマンドを実行してクラスマップを作成し、クラスマップコンフィグレーションモードに入ります。次に入力トラフィックの分類条件を match コマンドで指定します。
- 1 つのクラスマップあたり最大 16 個、match コマンドを実行することができます。
- クラスマップは、パケットの分類、タグの付与、帯域幅の制限をインタフェースに対して行うため、ポリシーマップと同時に使用されます。

例

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

関連するコマンド

show class map (P425)

match

このコマンドはトラフィックを分類するために使用する条件を設定します。

文法

[no] match {access-list acl-name | ip dscp dscp | ip precedence ip-precedence | vlan vlan}

- acl-name — **アクセスコントロールリスト名**（1-16 **文字**）
- dscp — DSCP **値**（0-63）
- ip-precedence — IP Precedence **値**（0-7）
- vlan — VLAN ID（1-4094）

初期設定

なし

コマンドモード

Class Map Configuration

コマンド解説

- **最初に** class-map **コマンドを実行してクラスマップを作成し、クラスマップコンフィグレーションモードに入ります。次にこのクラスマップ上で合致させたい入力パケット中の値を** match **コマンドで指定します。**
- 1 **つのクラスマップあたり** 1 **つの** match **コマンドのみ入力することができます。**

例

“rd_class#1,” **という名前のクラスマップを作成し、**DSCP **値** 3 **をマークします。**

```
Console(config)#class-map rd_class#1_ match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

“rd_class#2,” **という名前のクラスマップを作成し、**IP Precedence **値** 5 **をマークします。**

```
Console(config)#class-map rd_class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

“rd_class#3,” **という名前のクラスマップを作成し、**VLAN1 **をマークします。**

```
Console(config)#class-map rd_class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

rename

クラスマップまたはポリシーマップの名前を再設定します。

文法

rename map-name

map-name — **クラスマップまたはポリシーマップの名前（範囲：**1-16 **文字）**

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

description

クラスマップまたはポリシーマップの説明を入力します。

文法

description string

string — **クラスマップまたはポリシーマップの説明（範囲：**1-64 **文字）**

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description matches packets marked for DSCP service
?value 3
Console(config-cmap)#
```

policy-map

このコマンドはポリシーマップを作成し、ポリシーマップコンフィグレーションモードに入ります。"no" を付けるとポリシーマップは削除され、グローバルコンフィグレーションモードに戻ります。

文法

[no] policy-map policy-map-name

- policy-map-name — **ポリシーマップ名（**1-16 **文字）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **ポリシーマップの名前を設定するために** policy-map **コマンドを使用します。次にクラスマップで指定された条件に合致するトラフィックにポリシーを設定するため、**class **コマンドを使用します。**
- **ポリシーマップに複数のクラス設定を含めることができます。**
- **ポリシーマップを作成する前にクラスマップを作成する必要があります。**

例

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

class

このコマンドはポリシーマップが実行するクラスマップを指定し、ポリシーマップ・クラスコンフィグレーションモードに入ります。"no" を付けるとクラスマップを削除し、ポリシーマップコンフィグレーションモードに戻ります。

文法

[no] class class-map-name

- class-map-name — クラスマップ名（1-16 文字）

初期設定

なし

コマンドモード

Policy Map Configuration

コマンド解説

- ポリシーマップの設定を行うために policy-map コマンドを使用し、ポリシーマップコンフィグレーションモードに入ります。次にポリシーマップ・クラスコンフィグレーションモードに入るために class コマンドを使用します。そして最後に、set コマンドと police コマンドを使用して設定を行います。
  - set －コマンドは受信した IP パケットをクラス分けします。
  - police －コマンドは最大スループット、バーストレート、ポリシーに反した場合の動作を設定します。
- 1 つのクラスマップあたり最大 16 個のルールを設定できます。また、ポリシーマップには複数のクラスを所属させることができます。

例

この例では "rd_policy" という名前のポリシーを作成し、class コマンドを使って前もって設定されたクラス "rd_class" を設定しています。次に set コマンドを使用して受信された入力パケットのクラス分けを行い、police コマンドで平均帯域幅を 100,000kbps、バーストレートを 1522bytes に制限し、それに反したパケットを破棄するよう設定しています。

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

set

このコマンドは match コマンドで設定した条件に合致したパケットに CoS、DSCP、IP Precedence の値を IP パケットに付加します。"no" を付けるとトラフィックのクラス分けを取り止めます。

文法

[no] set {cos new-cos | ip dscp new-dscp | ip precedence new-precedence}

- new-cos — 新しく付加する CoS の値（0-7）
- new-dscp — 新しく付加する DSCP の値（0-63）
- new-precedence — 新しく付加する IP Precedence Value（0-7）

初期設定

なし

コマンドモード

Policy Map Configuration

例

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

police

このコマンドはクラス分けされたトラフィックにポリサを設定します。"no" を付けるとポリサの適用を取り止めます。

文法

[no] police rate-kbps burst-byte [exceed-action {drop | set}]

- rate-kbps — 1 秒あたりの転送レート（単位：kbps　範囲：1 ～ 100,000kbps）
- burst-byte — バーストレート (範囲：64-1522 bytes)
- drop — 設定した帯域幅とバーストレートを超えたパケットは破棄する。
- set — 設定した帯域幅とバーストレートを超えたパケットに DSCP の値を設定する。

初期設定

drop

コマンドモード

Policy Map Configuration

コマンド解説

- 各アクセスリスト（Standard ACL、Extended ACL、MAC ACL）のそれぞれに最大 64 個のポリサを構成できます。
- ポリシングはトークンバケットを基にしています。バケットの深さ（バケットがオーバーフローする前の最大バーストレート）は burst-byte オプションで指定します。またバケットから移動するトークンの平均レートは rate-kbps オプションで指定します。

例

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

service-policy

このコマンドはインタフェースの入力キューに policy-map **コマンドで設定されたポリシーマップを割り当てます。**"no" **を付けるとこのインタフェースからポリシーマップの割り当てを外します。**

文法

[no] service-policy input policy-map-name

- input — **入力トラフィックにインタフェースを適用**
- policy-map-name — **ポリシーマップ名（**1-16 **文字）**

初期設定

インタフェースにポリシーマップは未適用

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **インタフェースには** 1 **つのポリシーマップのみ割り当てることができます。**
- **最初にクラスマップを設定し、次にポリシーマップを設定し、最後に** service-policy **コマンドを使用して必要なインタフェースにポリシーマップを関連付けてください。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd_policy
Console(config-if)#
```

show class-map

このコマンドは match **コマンドで設定した** QoS **のクラスマップを表示します。**

文法

show class-map [class-map-name]

- class-map-name — **クラスマップ名（**1-16 **文字）**

初期設定

全てのクラスマップを表示

コマンドモード

Privileged Exec

例

```
Console#show class-map
Class Map match-any rd_class#1
Match ip dscp 3
Class Map match-any rd_class#2
Match ip precedence 5
Class Map match-any rd_class#3
Match vlan 1
Console#
```

show policy-map

このコマンドは QoS **のポリシーマップを表示します。**

文法

show policy-map [policy-map-name [class class-map-name]]

- policy-map-name — **ポリシーマップ名**（1-16 **文字**）
- class-map-name — **クラスマップ名**（1-16 **文字**）

初期設定

全てのポリシーマップおよびクラスマップを表示

コマンドモード

Privileged Exec

例

```
Console#show policy-map
Policy Map rd_policy
class rd_class
set ip dscp 3
Console#show policy-map rd_policy class rd_class
Policy Map rd_policy
class rd_class
set ip dscp 3
Console#
```

show policy-map interface

このコマンドはインタフェースに割り当てられたサービスポリシーを表示します。

文法

show policy-map interface interface input

- Interface
  - ethernet unit/port
    - unit — **ユニット番号　（範囲：**1-8）
    - port — **ポート番号（範囲：**1-26）
  - port-channel channel-id (**範囲：**1-32)

コマンドモード

Privileged Exec

例

```
Console#show policy-map interface ethernet 1/5
Service-policy rd_policy input
Console#
```

1.23 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。

i 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	P427
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	P434
Static Multicast Interface	静的マルチキャストルータポートの設定	P436

1.23.1 IGMP Snooping コマンド

コマンド	機能	モード	ページ
ip igmp snooping	IGMP snooping を有効化	GC	P428
ip igmp snooping vlan static	インタフェースを、マルチキャストグループのメンバとして追加	GC	P429
ip igmp snooping version	IGMP バージョンを設定	GC	P430
ip igmp snooping immediate-leave	ポートで Leave パケットが受信され、親 VLAN で immediate-leave が有効の場合、マルチキャストサービスのメンバーポートを直ちに削除	GC	P431
show ip igmp snooping	IGMP スヌーピングとクエリの設定を表示	PE	P432
show mac-address-table multicast	IGMP スヌーピング MAC マルチキャストリストの表示	PE	P433

ip igmp snooping

IGMP snooping を有効にします。コマンドの前に "no" を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。コマンドの前に "no" を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：**1-4093）
- ip-address — **マルチキャストグループの** IP **アドレス**
- interface
  - ethernet unit/port
    - unit — **ユニット番号** （**範囲：**1-8）
    - port — **ポート番号**（**範囲：**1-26）
  - port-channel channel-id（**範囲：**1-32）

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。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

ip igmp snooping version {1 | 2 | 3 }

no ip igmp snooping version

- 1 — IGMP Version1
- 2 — IGMP Version2
- 3 — IGMP Version3

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)#
```

ip igmp snooping immediate-leave

ポートで leave packet が受信され、immediate-leave が親 VLAN で有効になっている時、マルチキャストサービスのメンバーポートをただちに削除します。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

[no] ip igmp snooping immediate-leave

初期設定

無効

コマンドモード

Interface Configuration（VLAN）

コマンド解説

- immediate-leave が使用されない場合、IGMPv2/v3 グループが leave メッセージを受信した時、マルチキャストルータ（またはクエリア）はグループ指定クエリメッセージを送信します。タイムアウト期間の内にホストがクエリに返答しない場合に限り、ルータ / クエリはグループのトラフィック転送を停止します。（このリリースのタイムアウトは現在 Last Member Query Interval によって設定されています（1 秒に固定）*RFC2236 で設定される信頼関数（2 に固定））
- このコマンドは IGMP スヌーピング有効で、IGMPv2 または IGMPv3 スヌーピングが使用されている時のみ効果があります。

例

```
Console(config-if-vlan1)#ip igmp snooping immediate-leave
Console(config-if-vlan1)#
```

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

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 { interface | user | igmp-snooping | multicast-address }

- interface
  - ethernet unit/port
    - unit — **ユニット番号 （範囲：**1-8**）**
    - port — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id**（範囲：**1-32**）**
- user— **ユーザーに設定されたマルチキャストエントリのみを表示**
- igmp-snooping— IGMP **スヌーピングで学習されたエントリのみを表示**
- multicast-address —IP **マルチキャストグループアドレス**
  （範囲：224.0.0.0- 239.255.255.255**）**

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#
```

1.23.2 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	P434
ip igmp snooping rouoter-port-expire-time	クエリータイムアウトの設定	GC	P435

ip igmp snooping querier

IGMP snooping クエリアとしての機能を有効にします。コマンドの前に "no" を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

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、ホストへ問い合わせを行います。

例

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

ip igmp snooping router-port-expire-time

クエリータイムアウト時間の設定を行います。コマンドの前に "no" **を置くことにより、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（P430）

1.23.3 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	P436
show ip igmp snooping mrouter	マルチキャストルータポートの表示	PE	P437

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。コマンドの前に "no" を置くことで設定を削除します。

文法

ip igmp snooping vlan vlan-id mrouter interface

no ip igmp snooping vlan vlan-id mrouter interface

- vlan-id - VLAN ID（範囲：1-4093）
- Interface
  - ethernet unit/port
    - unit — ユニット番号 （範囲：1-8）
    - port — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)

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：**1-4093）

初期設定

VLAN **に設定されたすべてのマルチキャストルータポートを表示します。**

コマンドモード

Privileged Exec

コマンド解説

- **マルチキャストルータポートとして表示されるタイプには静的及び動的の両方が含まれます。**

例

本例では、VLAN 1 **のマルチキャストルータに接続されたポートを表示します。**

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Ports Type
---- ------------------- -------
 1             Eth 1/11   Static
 2             Eth 1/12   Static
Console#
```

1.23.4 IGMP グループのフィルタリングとスロットリング

特定のスイッチアプリケーションでは、エンドユーザが使用できるマルチキャストサービスを管理者が制御することが必要な場合もあります。そのような例として、特定の加入プランに基づく IP/TV サービスが挙げられます。IGMP フィルタリング機能を使用すれば、スイッチポートで所定のマルチキャストサービスへのアクセスを制限することによって、そのような要件を満たすことができます。また、IGMP スロットリング機能によってポートが同時に加入できるマルチキャストグループの数を制限することもできます。

コマンド	機能	モード	
ip igmp filter	本機の IGMP フィルタリングおよびスロットリング機能を有効にします。	GC	P439
ip igmp profile	プロファイル番号を設定し、IGMP フィルタプロファイルのコンフィグレーションモードに入ります。	GC	P440
permit, deny	プロファイルのアクセスモード (permit/deny) を設定します。	IPC	P441
range	プロファイルのマルチキャストアドレスを１つ、または範囲を指定します。	IPC	P442
ip igmp filter	IGMP のフィルタプロファイルをインタフェースに割り当てます。	IC	P443
ip igmp max-groups	インタフェースの IGMP スロットリング番号を設定します。	IC	P444
ip igmp max-groups action	インタフェースの IGMP スロットリングのアクションを設定します。	IC	P445
ip igmp query-drop	受信した IGMP クエリパケットを破棄します。	IC	P446
ip multicast-data-drop	マルチキャストデータパケットをすべて破棄します。	IC	P452
show ip igmp filter	IGMP フィルタリングのグローバルおよびインタフェースの設定値を表示します。	PE	P448
show ip igmp profile	IGMP プロファイルおよび設定値を表示します。	PE	P449
show ip igmp query-drop	インタフェース上で IGMP クエリパケットを破棄するように設定されているかどうかを表示します。	PE	P450
show ip igmp throttle interface	インタフェースの IGMP スロットリングの設定を表示します。	PE	P451
show ip multicast-datadrop	インタフェース上でマルチキャストデータパケットを破棄するように設定されているかどうかを表示します。	PE	P452

ip igmp filter (Global Configuration)

本機の IGMP フィルタリングおよびスロットリング機能を有効にします。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] ip igmp filter

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- IGMP フィルタリングを使用すると、ポートで許可または拒否されるマルチキャストグループを指定するプロファイルをスイッチポートに割り当てることができるようになります。IGMP フィルタプロファイルには、1 つまたは複数のアドレスあるいは特定の範囲のマルチキャストアドレスを含めることができますが、1 つのポートに割り当てることができるプロファイルは 1 つだけです。IGMP フィルタリングが有効になっている場合、ポートで受信される IGMP 加入レポートがフィルタプロファイルと照らし合わせてチェックされます。要求されたマルチキャストグループが許可される場合は、IGMP 加入レポートが通常どおり転送されます。要求されたマルチキャストグループが拒否される場合は、IGMP 加入レポートがドロップされます。
- IGMP フィルタリングおよびスロットリングは、動的に学習されたマルチキャストグループにのみ適用され、静的に設定されたグループには適用されません。
- IGMP フィルタリング機能は、MVR を用いてマルチキャストトラフィックを転送する場合と同じ方法で動作します。

例

```
Console(config)#ip igmp filter
Console(config)#
```

ip igmp profile

プロファイル番号を設定し、IGMP **フィルタプロファイルのコンフィグレーションモードに入ります。コマンドの前に** "no" **を付けることにより、プロファイル番号を削除します。**

文法

[no] ip igmp profile profile-number

- profile-number - IGMP **フィルタプロファイル番号** (**有効範囲** : 1-4294967295)

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- **プロファイルは、加入者による加入を許可** / **拒否されているマルチキャストグループを設定します。同じプロファイルを多くのインタフェースに適用可能ですが、**1 **つのインタフェースに割り当てられるプロファイルは** 1 **つのみです。各プロファイルには、それぞれ１つずつアクセスモード** (permit/deny) **があります。**

例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

permit, deny

プロファイルのアクセスモード (permit/deny) **を設定します。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻ります。**

文法

{permit | deny}

初期設定

Deny

コマンドモード

IGMP Profile Configuration

コマンド解説

- **各プロファイルには、アクセスモードが１つずつあります** (permit/deny)**。**
- **アクセスモードを** ”permit” **に設定すると、マルチキャストグループが制御された範囲内であれば** IGMP join **レポートの処理を行います。アクセスモードを** ”deny” **に設定すると、マルチキャストグループが制御された範囲内でない場合は** IGMP join **レポートのみの処理を行います。**

例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range

プロファイルのマルチキャストアドレスを１つ、または範囲を指定します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] range low-ip-address [high-ip-address]

low-ip-address - **マルチキャストグループの** IP **アドレス、またはグループ範囲の最初。**

high-ip-address - **マルチキャストグループの範囲の最後の有効な** IP **アドレス。**

初期設定

None

コマンドモード

IGMP Profile Configuration

コマンド解説

- **このコマンドを複数回入力して、複数のマルチキャストアドレス、またはプロファイルのアドレスの範囲を指定します。**

例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

ip igmp filter (Interface Configuration)

IGMP のフィルタプロファイルをインタフェースに割り当てます。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] ip igmp filter profile-number

profile-number - IGMP フィルタのプロファイル番号

(有効範囲 : 1-4294967295)

初期設定

None

コマンドモード

Interface Configuration

コマンド解説

- インタフェースに割り当てる前に、IGMP フィルタリングのプロファイルをまず ip igmp profile コマンドで設定する必要があります。
- インタフェースに割り当て可能なプロファイルは 1 つのみです。
- プロファイルをトランクインタフェースに割り当てることも可能です。ポートをトランクメンバーに設定すると、トランクはトランク内の最初のポートメンバーに割り当てられたフィルタリングプロファイルを使用します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups

インタフェースの IGMP **スロットリング番号を設定します。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻ります。**

文法

ip igmp max-groups number

no ip igmp max-groups

- number - **インタフェースが同時に加入可能なマルチキャストグループの最大数** (**有効範囲** : 1-1024)

初期設定

1024

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- IGMP **スロットリングでは、ポートが同時に加入できるマルチキャストグループの最大数が設定されます。スイッチでは、ポートにおけるグループの最大数に達した場合に** 2 **つのアクションのうちの** 1 **つ（「拒否」と「置換」のどちらか）を実行することができます。アクションが「拒否」に設定されている場合には、新規の** IGMP **加入レポートはドロップされます。アクションが「置換」に設定されている場合には、既存のグループがランダムに削除されて新規のマルチキャストグループに置き換えられます。**
- IGMP **スロットリングはトランクインタフェースに設定することも可能です。ポートをトランクメンバーに設定されると、トランクはトランク内の最初のポートメンバーのスロットリングの設定を使用します。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action

インタフェースの IGMP **スロットリングのアクションを設定します。**

文法

ip igmp max-groups action {replace | deny}

replace - **既存グループを新しいマルチキャストグループで置き換えます。**

deny - **新しいマルチキャストグループの** join **レポートは破棄されます。**

初期設定

Deny

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **ポートのグループ数が上限に達すると、以下の** “deny” **、または** “replace” **のいずれかを実行します。**“deny” **に設定すると新しい** IGMP **の** join **レポートは破棄され、**“replace” **に設定すると、既存グループはランダムに削除され、新しいマルチキャストグループに置き換えられます。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

ip igmp query-drop

受信した IGMP **クエリパケットを破棄します。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] ip igmp query-drop

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **指定したインタフェースで受信したクエリパケットを破棄することが可能です。クエリアとして動作する場合は、他のクエリアから受信したメッセージによる影響を受けることから回避します。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

ip multicast-datadrop

マルチキャストデータパケットをすべて破棄します。

文法

[no] ip multicast-data-drop

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **マルチキャストサービスによるダウンストリームポートに接続されているユーザへの転送を中断します。(例えば、このコマンドにより指定されているインタフェース)。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip multicast-data-drop
Console(config-if)#
```

show ip igmp filter

IGMP **フィルタリングのグローバルおよびインタフェースの設定値を表示します。**

文法

show ip igmp filter [interface interface]

- interface

  ethernet unit/port

  - unit - **スタックユニット** (**有効範囲** : 1-8)
  - port - **ポート番号** (**有効範囲** : 1-26)

  port-channel channel-id (**有効範囲** : 1-32)

初期設定

None

コマンドモード

Privileged Exec

例

```
Console#show ip igmp filter
IGMP filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
---------------------------------
IGMP Profile 19
Deny
range 239.1.1.1 239.1.1.1
range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile

本機上で設定した IGMP **フィルタリングのプロファイルを表示します。**

文法

show ip igmp profile [profile-number]

- profile-number - **既存の** IGMP **フィルタのプロファイル番号** (**有効範囲** : 1-4294967295)

初期設定

None

コマンドモード

Privileged Exec

例

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
Deny
range 239.1.1.1 239.1.1.1
range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp query-drop

インタフェース上で IGMP **クエリパケットを破棄するように設定されているかどうかを表示します。**

文法

show ip igmp query-drop interface [interface]

- interface

  ethernet unit/port

  - unit - **スタックユニット** (**有効範囲** : 1-8)
  - port - **ポート番号** (**有効範囲** : 1-26)

  port-channel channel-id (**有効範囲** : 1-32)

初期設定

None

コマンドモード

Privileged Exec

コマンド解説

- **インタフェースを指定しないでこのコマンドを使用すると、**すべてのインタフェースの情報が表示されます。

例

```
Console#show ip igmp query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

show ip igmp throttle interface

IGMP **スロットリングのインタフェースの設定を表示します。**

文法

show ip igmp throttle interface [interface]

- interface

  ethernet unit/port

  - unit - **スタックユニット** (**有効範囲** : 1-8)
  - port - **ポート番号** (**有効範囲** : 1-26)

  port-channel channel-id (**有効範囲** : 1-32)

初期設定

None

コマンドモード

Privileged Exec

コマンド解説

- **インタフェースを指定しないでこのコマンドを使用すると、インタフェースがすべて表示されます。**

例

```
Console#show ip igmp throttle interface ethernet 1/1
Eth 1/1 Information
Status : TRUE
Action : Deny
Max Multicast Groups : 32
Current Multicast Groups : 0

Console#
```

show ip multicastdata-drop

インタフェース上でマルチキャストデータパケットを破棄するように設定されているかどうかを表示します。

文法

show ip multicast-data-drop interface [interface]

- interface

  ethernet unit/port

  - unit - **スタックユニット** (**有効範囲** : 1-8)
  - port - **ポート番号** (**有効範囲** : 1-26)

  port-channel channel-id (**有効範囲** : 1-32)

初期設定

None

コマンドモード

Privileged Exec

コマンド解説

- **インタフェースを指定しないでこのコマンドを使用すると、インタフェースがすべて表示されます。**

例

```
Console#show ip multicast-data-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

1.24 マルチキャスト VLAN の登録

MVR は、マルチキャストトラフィック（TV チャネルやビデオオンデマンドのトラフィック）をサービスプロバイダーのネットワーク経由で送信する場合に最もよく使用されている単一のネットワークワイド VLAN に対するアクセスを制御するプロトコルです。MVR VLAN に入るあらゆるマルチキャストトラフィックは、その VLAN に接続しているすべてのサブスクライバに送信されます。このプロトコルを使用すると、平均的なマルチキャスト VLAN の配信ツリーを動的に監視および確立するために必要な処理のオーバーヘッドを大幅に削減することができます。その結果、マルチキャストルーティングプロトコルを一切使用しなくても、一般的なマルチキャストサービスをネットワーク内の広い範囲でサポートすることが可能になります。

MVR では、サブスクライバが属している他の VLAN のみにトラフィックを渡すことにより、VLAN セグリゲーションで実現されるユーザ分離とデータセキュリティが維持されます。共通のマルチキャストストリームが MVR VLAN から別々の VLAN グループに渡されますが、異なる IEEE 802.1Q VLAN またはプライベート VLAN 内のユーザは、（上位のルーティングサービスを使用しない限り）情報を交換することはできません。

コマンド	機能	モード	
mvr	MVR をグローバルで有効にするか、MVR グループのアドレスを静的に有効にするか、MVR VLAN の識別子を指定します。	GC	P454
mvr upstream-source-ip	アップストリームに送信されたすべての制御パケットに割り当てられた送信元の IP アドレスを設定します。	GC	P455
mvr immediate-leave	immediate leave ケーパビリティを有効にします。	IC	P456
mvr type	インタフェースを MVR 受信側、または送信元のポートに設定します。	IC	P457
mvr vlan group	インターフェスを MVR グループのスタティックメンバーに設定して、MVR の VLAN から受信側の VLAN の指定のインタフェースに伝送します。	IC	P459
show mvr	グローバルの MVR のコンフィグレーションの設定値、MVR の VLAN に接続されているインタフェース、または MVR の VLAN に割り当てられているマルチキャストグループの情報について表示します。	PE	P460

mvr

本機の MVR(マルチキャスト VLAN 登録) を有効にして、group キーワードを使用して、MVR マルチキャストグループの IP アドレスを静的に設定します。キーワードを使用しないでコマンドの前に "no" を置くと、MVR はグローバルで無効になります。　デフォルト設定に戻ります。group キーワードを使用してマンドの前に "no" を置くと特定のアドレス、またはアドレスの範囲が削除されます。もしくは、vlan キーワードを使用してコマンドの前に "no" を置くと、デフォルトの MVR の VLAN に戻ります。

文法

[no] mvr [group ip-address [count] | vlan vlan-id]

group - 接続先のサブスクライバすべてに送信されたマルチキャストサービスを設定します。

ip-address - MVR マルチキャストグループの IP アドレス (有効範囲 : 224.0.1.0 - 239.255.255.255)

count - 連続する MVR グループアドレス数 (有効範囲 : 1-255)

vlan - MVR マルチキャストデータを受信する VLAN を指定します。この VLAN は送信元ポートをすべて割り当てる必要があります。

vlan-id - MVR VLAN ID (有効範囲 : 1-4093)

初期設定

MVR は「無効」です。

MVR グループアドレスは設定されています。

連続するアドレスのデフォルトの値は「0」です。

MVR の VLAN ID は「1」です。

コマンドモード

Global Configuration

コマンド解説

- mvr group コマンドを使用して、MVR VLAN に加入するすべてのマルチキャストグループのアドレスを静的に設定することができます。MVR グループに関連付けられているあらゆるマルチキャストグループは、スイッチ上のすべての送信元ポートから送信され、そのマルチキャストアドレスのデータを受信するために選択されているすべての受信先ポートで受信されます。
- マルチキャストストリームには、IP アドレス範囲 224.0.0.0 ～ 239.255.255.255 が使用されます。MVR グループアドレスには、予約 IP マルチキャストアドレス範囲 224.0.0.x に該当するアドレスを使用することはできません。
- MVR の送信元ポートは switchport allowed vlan コマンドおよび switchport native vlan コマンドを使用して、MVR の VLAN のメンバーに設定することが可能です。
- IGMP スヌーピングにより、サブスクライバは MVR グループを動的に加入 / 退会することが可能です（ ip igmp snooping を参照)。IGMP のバージョン 2 または 3 のホストのみマルチキャスト join、または leave メッセージを発行することが可能です。

- IGMP スヌーピングと MVR で最大 255 のグループを共有します。この上限値を超えて受信されたマルチキャストストリームは、関連付けられている VLAN 内のすべてのポートにフラッドされます。

例

ここでは、MVR は MVR グループのアドレスの範囲をグローバルで設定します。

```
Console(config)#mvr
Console(config)#mvr group 228.1.23.1 10
Console(config)#
```

mvr upstreamsource-ip

アップストリームに送信されたすべての制御パケットに割り当てられた送信元の IP アドレスを設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

mvr upstream-source-ip source-ip-address

no mvr upstream-source-ip

- source-ip-address – アップストリームに送信された MVR 制御パケットすべてに割り当てられた送信元の IP アドレス。

初期設定

アップストリームに送信された MVR レポートはすべて、0.0.0.0 の送信元 IP アドレスを使用します。

コマンドモード

Global Configuration

例

```
Console(config)#mvr upstream-source-ip 192.168.0.3
Console(config)#
```

mvr immediate-leave

グループの leave メッセージを受信するとすぐにマルチキャストストリームからインタフェースを削除します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] mvr immediate-leave

初期設定

Disabled

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- immediate leave は受信先ポートのみに適用されます。immediate leave が有効になっている場合には、受信先ポートは、離脱メッセージで示されるマルチキャストグループから即座に削除されます。immediate leave が無効になっている場合には、スイッチは、標準のルールに従って、クエリメッセージを受信先ポートに送信し、マルチキャストグループに残っているサブスクライバがいないかどうかを確認するために応答を待機してから、ポートをグループリストから削除します。
  - immediate leave は、離脱に伴う遅延を減らすのに役立ちますが、同じインタフェースに接続している他のグループメンバーに対するサービスが妨げられることがないようにするため、1 つのマルチキャストサブスクライバに接続しているポートでのみ、有効にしてください。
  - immediate leave はポートに静的に割り当てられているマルチキャストグループには適用されません。

例

受信側ポートの immediate leave を有効にします。

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr immediate
Console(config-if)#
```

mvr type

インタフェースを MVR 受信側、または送信元のポートに設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] mvr type {receiver | source}

- receiver - マルチキャストデータを受信可能なサブスクライバとしてインタフェースを設定します。
- source - 設定したマルチキャストグループのマルチキャストデータを送受信可能なアップリンクポートとしてインタフェースを設定します。

初期設定

ポートタイプは設定されていません。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- MVR 受信先ポート、または送信元ポートとして設定されていないポートは、マルチキャストフィルタリングの標準ルールに基づいて、IGMP スヌーピングを使用してマルチキャストグループを加入 / 離脱することが可能です。
- 受信先ポートは異なる VLAN に属すことは可能ですが、MVR の VLAN のメンバーとして設定してはなりません。IGMP スヌーピングを使用して、受信先ポートは MVR の VLAN を介して受信したマルチキャストグループを動的に加入 / 離脱することができます。MVR 受信先のポートの VLAN メンバーはトランクモードに設定することはできませんので注意して下さい（switchport mode コマンドを参照）。
- １つ、または複数のインタフェースを MVR 送信元ポートに設定することが可能です。送信元ポートは、IGMP スヌーピングを介して加入したり、mvr group コマンド (グローバル設定) を介して割り当てられるマルチキャストグループのデータの送受信が可能になります。
- IGMP スヌーピングを有効にして、サブスクライバによる MVR グループの 加入 / 離脱が動的にできるように設定可能しなければなりません（ip igmp snooping コマンドを参照）。IGMP バージョン 2/3 のホストのみ multicast join/leave メッセージを発行可能です。

例

ここでは、送信元ポートを１ポートおよび複数の受信先ポートを設定します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#
```

mvr vlan group

ホストに関連のある長期のマルチキャストストリームを受信するポートにマルチキャストグループを静的にバインドします。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

[no] mvr vlan vlan-id group ip-address

- vlan-id - **指定のマルチキャストトラフィックがフラッドした受信元** VLAN(**有効範囲** : 1-4093)
- group - **選択したポートに送信されたマルチキャストサービスを設定します。**
- ip-address - **インタフェースを静的に設定して、**MVR **マルチキャストグループに指定したアドレスからマルチキャストトラフィックを受信します。**(**有効範囲** : 224.0.1.0 - 239.255.255.255)

初期設定

設定したマルチキャストグループのメンバーとなる受信元ポートはありません。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **マルチキャストグループは受信先ポートに静的に割り当て可能です。**
- IP **アドレス（有効範囲** : 224.0.0.0 **〜** 239.255.255.255**）はマルチキャストストリームに使用されます。**MVR **グループアドレスは、予約されている** IP **マルチキャストアドレス** (224.0.0.x) **の範囲内に設定することはできません。**
- IGMP **スヌーピングを有効にして、サブスクライバによる** MVR **グループの 加入** / **離脱が動的にできるように設定可能しなければなりません（**ip igmp snooping **コマンドを参照)。**IGMP **バージョン** 2/3 **のホストのみ** multicast join/leave **メッセージを発行可能です。**

例

ここでは、マルチキャストグループを受信先ポートに静的に割り当てます。

```
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#mvr vlan 3 group 225.0.0.5
Console(config-if)#
```

show mvr

キーワードなしで入力時のグローバルの MVR のコンフィグレーションの設定値、インタフェースのキーワードを使った MVR の VLAN に接続されているインタフェース情報、またはメンバーのキーワードを使った MVR の VLAN に割り当てられているマルチキャストグループ情報について表示します。

文法

show mvr [interface | members [ip-address]]

- interface
  - port-channel channel-id (**有効範囲** : 1-32)
- ip-address - MVR **マルチキャストグループの** IP **アドレス**

  (**有効範囲** : 224.0.1.0 - 239.255.255.255)

初期設定

キーワードなしの場合は MVR **のグローバルのコンフィグレーションの設定値が表示されます。**

コマンドモード

Privileged Exec

コマンド解説

- **キーワードなしでコマンドを入力すると、**MVR **のグローバルの設定値を表示します。インタフェースのキーワードを使うと** MVR **の** VLAN **に接続されているインタフェース情報が表示されます。もしくは、メンバーのキーワードを使って、**MVR **の** VLAN **に割り当てられているマルチキャストグループ情報を表示します。**

例

ここでは、グローバルの MVR **の設定値を表示します。**

```
Console#show mvr
MVR Config Status : Enabled
MVR Running Status : Active
MVR Multicast VLAN : 1
MVR Current Learned Groups : 10
MVR Upstream Source IP : 192.168.0.3
MVR Group Range :
Start End
--------------- ---------------
228.1.23.1 228.1.23.10
Console#
```

コマンド	機能
MVR Config Status	MVR がグローバルで有効かどうかを表示します。
MVR Running Status	MVR 環境の必須条件を満たしているかどうかを示します（MVR Status が有効な場合、かつ指定の MVR の VLAN が存在する場合に限り動作状況は「true」です。
MVR Multicast VLAN	すべての MVR マルチキャストトラフィックの伝送に使用する VLAN を表示します。
MVR Current Learned Groups	現行の MVR グループアドレス数
MVR Upstream Source IP	アップストリーム制御パケットに割り当てられた送信元 IP アドレス
MVR Group Range	MVR の VLAN 内の代表サービスに使用するマルチキャストグループのアドレス

以下の例では、MVR の VLAN に接続されているインタフェース情報について表示します。

```
Console#show mvr interface
Port Type Status Immediate Static Group Address
-------- -------- ------------- --------- --------------------
Eth1/ 2 Source Active/Up
Eth1/ 3 Source Inactive/Down
Eth1/ 1 Receiver Active/Up Disabled 225.0.0.1(VLAN1)
225.0.0.9(VLAN3)
Eth1/ 4 Receiver Active/Down Disabled
Console#
```

コマンド	機能
Port	MVR に接続されているインタフェースを表示します。
Type	MVR ポートのタイプを表示します。
Status	MVR ステータス、およびインタフェースのステータスを表示します。MVR がグローバルで有効な場合は 送信元ポートの MVR ステータスは「ACTIVE」です。 MVR グループのいずれかからのマルチキャストトラフィックを受信するサブスクライバがある場合、あるいはマルチキャストグループがインタフェースに静的に割り当てられる場合のみ受信先ポートの MVR ステータスは「ACTIVE」です。
Immediate Leave	immediate leave が有効 / 無効の状態であることを示します。
Static Group Address	インタフェース、および受信先 VLAN に割り当てられているスタティック MVR グループを表示します。

以下の例では、MVR の VLAN に割り当てられているマルチキャストグループに関連のあるインタフェース情報について表示します。

```
Console#show mvr members
MVR Forwarding Entry Count:1
Group Address Source Address VLAN Forwarding Port
------------- -------------- ---- --------------
225.0.0.9 * 2 Eth1/ 1(VLAN3) Eth1/ 2(VLAN2)
Console#
```

コマンド	機能
MVR Forwarding Entry Count	MVR の VLAN から現在伝送されているマルチキャストサービス数
Group Address	MVR VLAN に割り当てられるマルチキャストグループ数
Source Address	マルチキャストサービスの送信元アドレスを示します。 グループアドレスを静的に割り当てる場合はアスタリスク ”*” で表示します。
VLAN	マルチキャストサービスを受信する MVR の VLAN を示します。
Forwarding Port	インタフェースが、MVR VLAN を使用して提供されるマルチキャストサービスのサブスクライバと共に表示されます。サービスの受信に使用される VLAN も同様に表示します。この VLAN は、グループアドレスが静的に割り当てられている場合は MVR VLAN と異なることがあるという点に注意してください。

1.24.1 IGMP (LAYER 3)

レイヤ 3 の IGMP(インターネットグループマネジメントプロトコル）の設定に使用するコマンドについて説明します。

コマンド	機能	モード	ページ
ip igmp	指定のインタフェースの IGMP を有効にします。	IC	P463
ipv6 mld last-member-query-interval	leave メッセージの受信に応じてクエリメッセージの送信間隔を設定します。	IC	P465
ip igmp max-resp-interval	ホストの最大応答時間を設定します。	IC	P466
ip igmp query-interval	ホストのクエリメッセージの送信間隔を設定します。	IC	P467
ip igmp robustval	パケットロスの期待値を設定します。	IC	P468
ip igmp static-group	ルータを指定の VLAN インタフェースのマルチキャストグループのスタティックメンバに設定します。	IC	P469
ip igmp version	インタフェースで使用する IGMP のバージョンを設定します。	IC	P470
clear ip igmp group	IGMP キャッシュからのエントリを削除します。	PE	P471
show ip igmp groups	IGMP グループの情報を表示します。	PE	P472
show ip igmp interface	指定のインタフェースのマルチキャスト情報を表示します。	PE	P475

ip igmp

VLAN インタフェースの IGMP を有効にします。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

[no] ip igmp

初期設定

Disabled

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ip igmp コマンドを介してレイヤ 3 の特定の VLAN インタフェースの IGMP (クエリ機能を含む）を有効にすることが可能です。
- PIM - Dense モードなどのマルチキャストルーティングプロトコルを有効にすると、IGMP も同様に有効になります。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp
Console(config-if)#end
Console#show ip igmp interface
IGMP : Enabled
IGMP Version : 2
IGMP Proxy : Disabled
IGMP Unsolicited Report Interval : 400 sec
Robustness Variable : 2
Query Interval : 125 sec
Query Max Response Time : 100 (resolution in 0.1 sec)
Last Member Query Interval : 10 (resolution in 0.1 sec)
Querier : 0.0.0.0
Joined Groups :
Static Groups :
Console#
```

関連するコマンド

ip igmp snooping (P428)

show ip igmp snooping (P432)

ip igmp last-member-queryinterval

group-specific、または group-source-specific leave メッセージの受信した場合の IGMP groupspecific、または IGMPv3 group-source-specific クエリメッセージの送信間隔を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

ip igmp last-member-query-interval seconds

no ip igmp last-member-query-interval

- seconds - leave メッセージを受信した場合の group-specific または group-source-specific クエリの送信間隔 （有効範囲 : 1-255 10 分の 1 秒）

初期設定

10 分の 1 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- スイッチは、マルチキャストグループ、送信元、またはチャネルから離脱するホストから IGMPv2 または IGMPv3 離脱メッセージを受信すると、「Last Member Query Count」で指定されている数の GS または GSS クエリメッセージをこの「Last Member Query Interval」で指定されている間隔で送信します。この間隔よりも長い間、応答がスイッチで受信されない場合、グループ、送信元、またはチャネルのトラフィックの転送が停止されます。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp last-member-query-interval 20
Console(config-if)#
```

ip igmp max-respinterval

IGMP クエリでアドバタイズされる最大応答時間を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

ip igmp max-resp-interval seconds

no ip igmp max-resp-interval

- seconds - IGMP クエリでアドバタイズされているレポートの遅延 (有効範囲 : 0-255 10 分の 1 秒)

初期設定

100 (10 秒)

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- IGMPv1 の場合、クエリメッセージの最大応答時間は、指定不可であり、10 秒に固定されます。
- 「Query Max Response Time」の値を変更することにより、サブネットで渡される IGMP メッセージのバースト性を調整することができます。値が大きいほど、応答間隔が長くなるのでホスト応答の到達範囲が広がるため、トラフィックでバーストが発生する可能性は低くなります。
- 最大応答時間の値は、「Query Interval」よりも小さくなければなりません。

例

ここでは、最大応答時間を「20 秒」に設定する方法について説明します。

```
Console(config-if)#ip igmp query-max-response-time 200
Console(config-if)#
```

関連するコマンド

ip igmp version (P430)

ip igmp query-interval (P467)

ip igmp queryinterval

ホストのクエリメッセージの送信間隔を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

ip igmp query-interval seconds

no ip igmp query-interval

- seconds - IGMP host-query **メッセージの送信間隔** (**有効範囲** : 1-255 **秒**)

初期設定

125 seconds

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **マルチキャストルータは、特定のマルチキャストサービスを要求しているダウンストリームホストに接続しているインタフェースを判別するため、ホストクエリメッセージを送信します。ホストクエリメッセージを送信するのは、サブネットの代表マルチキャストルータのみです。**
- **ホストクエリメッセージは、マルチキャストアドレス** 224.0.0.1 **宛に、**TTL（Time-To-Live）**値** 1 **を使用して送信されます。**IGMPv1 **の場合、代表ルータは、**LAN **で実行されているマルチキャストルーティングプロトコルに応じて選択されます。一方、**IGMPv2 **および** IGMPv3 **の場合には、サブネットで** IP **アドレスが最も小さいマルチキャストルータが代表クエリアになります。**

例

以下に、クエリ間隔を「100 **秒」に設定する方法について説明します。**

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

関連するコマンド

ip igmp max-resp-interval (P482)

ip igmp robustval

インタフェースのパケットロスの期待値を設定します。コマンドの前に "no" **を付けることにより、デフォルト設定に戻ります。**

文法

ip igmp robustval robust-value

no ip igmp robustval

- robust-value - **インタフェースのパケット損失の期待値** (**有効範囲** : 1-255)

初期設定

2

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **インタフェースの信頼性（パケット損失の期待値）を指定します。この信頼性の値は、「**Group Membership Interval**」、「**Other Querier Present Interval**」、「**Startup Query Count**」（**RFC 2236**）など、他の** IGMP **変数の適性範囲を求めるときに使用されます（範囲** :1 **〜** 255**、デフォルト** :2**）。**
- **ルータでは、最新の受信クエリから取得される信頼性値「**f**」が採用されます。クエリアの信頼性値 （**QRV: Querier's Robustness Variable**）が** 0 **の場合は、**QRV **フィールドで信頼性値が宣言されていないことを意味し、信頼性変数は、このコマンドによって静的に設定される値に設定されます。**QRV **は、**7**（**QRV **フィールドの最大値）よりも大きい場合には、**0 **に設定されます。値** 0 **は、以降に送信されるクエリメッセージでは** QRV **がアドバタイズされないことを意味します。**

例

```
Console(config-if)#ip igmp robustval 3
Console(config-if)#
```

ip igmp static-group

ルータを指定の VLAN インタフェースのマルチキャストグループのスタティックメンバに設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

ip igmp static-group group-address [source source-address]

no ip igmp static-group

group-address - IP マルチキャストグループのアドレス (グループのアドレスは 224.0.0.1 - 239.255.255.255 の範囲内には設定できません .)

source-address - 対応するマルチキャストグループアドレスのトラフィックを送信するマルチキャストサーバのソースアドレス。

初期設定

None

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- マルチキャストグループアドレスの全範囲内のグループアドレスを指定することができます。ただし、SSM（Source-SpecificMulticast）アドレス範囲（デフォルトは 232/8）内のアドレスが指定されているが、送信元アドレスがコマンドに含まれていない場合、逆方向パスツリー内の次のノードで該当のグループが特定の送信元アドレスに静的にマップされていない限り、マルチキャストグループ加入要求は失敗します。また、SSM アドレス範囲外のアドレスが指定されており、特定の送信元アドレスがコマンドに含まれている場合、逆方向パスツリー内の次のノードで PIMSSM プロトコルが有効になっていると、やはり、マルチキャストグループ加入要求が失敗します。
- ASM（*,G）のための静的グループを設定すると、以降は、該当のエントリを削除しない限り、そのグループについて送信元アドレスを設定することができなくなります。
- 1 つまたは複数の SSM（S,G）について静的グループを設定すると、以降は、関連付けられている SSM（S,G）エントリをすべて削除しない限り、そのグループについて ASM（*,G）を設定することができなくなります。
- コマンドの前に "no" を付けることにより、スタティックグループを削除します。ソースアドレスを指定しない場合は、指定のグループのソースおよびソース固有のマルチキャストエントリをすべて削除します。
- 本製品は最大 64 の静的グループエントリをサポートします。

例

ここでは、LAN1 を指定したマルチキャストグループのスタティックメンバに割り当てます。

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp static-group 225.1.1.1
```

ip igmp version

インタフェースで使用する IGMP のバージョンを設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

ip igmp version {1 | 2 | 3}

no ip igmp version

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

初期設定

IGMP Version 2

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **サブネット上のルータはすべて同じバージョンをサポートしている必要があります。ただし、サブネット上のマルチキャストホストは IGMP バージョン 1 ～ 3 のいずれかをサポート可能です。**
- **IGMP バージョン 1 のメンバーシップレポートを受信すると、タイマーを設定して、バージョン 1 のホストがレポートを受信したグループのメンバーであることを注記します。バージョン 1 のホストが特定グループを表わす場合は、グループを受信する Leave Group メッセージをすべて無視します。**

例

```
Console(config-if)#ip igmp version 1
Console(config-if)#
```

clear ip igmp group

IGMP キャッシュからのエントリを削除します。

文法

clear ip igmp group [group-address | interface]

- group-address - マルチキャストグループの IP アドレス
- interface
  - vlan vlan-id - VLAN ID. (有効範囲 : 1-4093)

初期設定

オプションが選択されていない場合は、キャッシュ内のエントリをすべて削除します。

コマンドモード

Privileged Exec

コマンド解説

- マルチキャストグループのアドレスを入力して、指定したグループのエントリをすべて削除します。インタフェースのオプションを入力して、指定したインタフェースのマルチキャストグループをすべて削除します。オプションを入力しない場合は、キャッシュからマルチキャストグループをすべてクリアにします。

例

VLAN 1 のマルチキャストグループのエントリをすべてクリアにします。

```
Console#clear ip igmp interface vlan 1
Console#
```

show ip igmp groups

本機上の有効なマルチキャストグループ情報および IGMP を介して学習した情報について表示します。

文法

show ip igmp groups [{group-address | interface} [detail] | detail]

group-address - IP マルチキャストグループのアドレス

interface

vlan vlan-id - VLAN ID (有効範囲 : 1-4093)

detail - 使用可能なマルチキャストプロセスおよびソースアドレスの詳細について表示します。

コマンドモード

Privileged Exec

コマンド解説

- マルチキャストグループについての情報を表示するには、ip igmp コマンドを使ってグループに割り当てられたインタフェースの IGMP を有効にしなければなりません。システムのマルチキャストルーティングを ip multicast-routing コマンドを使ってグローバルで有効にしなければなりません。

例

ここでは、インタフェース、グループアドレス、スタティックリストごとに IGMP グループ情報を示すオプションについて表示します。

```
Console#show ip igmp groups
Group Address Interface VLAN Last Reporter Uptime Expire V1 Timer
--------------- --------------- --------------- -------- --------
--------
224.0.17.17 1 192.168.1.10 0:0:1 0:4:19 0:0:0
Console#show ip igmp groups 234.5.6.8
Group Address Interface VLAN Last Reporter Uptime Expire V1 Timer
--------------- --------------- --------------- -------- --------
--------
224.0.17.17 1 192.168.1.10 0:0:1 0:4:19 0:0:0
Console#show ip igmp groups interface vlan 1
Group Address Interface VLAN Last Reporter Uptime Expire V1 Timer
--------------- --------------- --------------- -------- --------
--------
224.0.17.17 1 192.168.1.10 0:0:1 0:4:19 0:0:0
Console#
```

コマンド	機能
Group Address	直接接続されたサブスクライバ、または本機からのダウンストリームの IP マルチキャストグループのアドレス

Interface VLAN	マルチキャストグループのアドレスに関連のトラフィックをもつ本機のインタフェース
Last Reporter	インタフェースで指定されたマルチキャストグループアドレスについて最後に受信されたメンバーシップレポートの送信元の IP アドレス。
Uptime	エントリが作成されてから経過した時間
Expire	エントリが期限切れになるまでの残り時間（デフォルト :260 秒）。グループモードが ”INCLUDE” の場合は、フィールドには “stopped” と表示されます。
V1Timer	インタフェースに接続している IP サブネットに IGMPv1 メンバーがいなくなったものとみなされるまでの残り時間。 • スイッチは、IGMPv1 メンバーシップレポートを受信すると、レポートが受信されたグループのメンバーである IGMPv1 ホストが存在していることを示すため、タイマーを設定します。 • 特定のグループについて IGMPv1 ホストが存在する場合、スイッチは、そのグループについて受信するあらゆるグループ離脱メッセージを無視します。

以下の例では、動的に学習したマルチキャストグループのリストに表示される情報について表示します。

```
Console#show ip igmp groups detail
Interface : VLAN 1
Group : 224.1.2.3
Uptime : 0h:0m:12s
Group mode : Include
Last reporter : 0.0.0.0
Group Source List:
Source Address Uptime v3 Exp Fwd
--------------- ----------- ----------- ---
192.1.2.3 0h:0m:12s 0h:0m:0s Yes
Console#
```

コマンド	機能
Interface	マルチキャストグループのアドレスに関連のトラフィックをもつ本機のインタフェース
Group	直接接続されたサブスクライバ、または本機からのダウンストリームを IP マルチキャストグループのアドレス
Uptime	エントリが作成されてから経過した時間
Groupmode	「Include」の場合、指定されたマルチキャストアドレスに送信されたパケットの受信は、source-list パラメータで指定される IP 送信元アドレスのみから要求されます。「Exclude」の場合、指定されたマルチキャストアドレスに送信されたパケットの受信は、source-list パラメータで指定されている IP 送信元アドレスおよび送信元タイマーのステータスが期限切れになっているその他の IP 送信元アドレス以外のすべての IP 送信元アドレスから要求されます。EXCLUDE モードは SSM アドレスには適用されません。
LastReporter	インタフェースで指定されたマルチキャストグループアドレスについて最後に受信されたメンバーシップレポートの送信元の IP アドレス。

Group Source List	マルチキャストの受信を要求する IP ユニキャストアドレスまたはマルチキャストの受信を要求しない IP ユニキャストアドレス（フィルタモードによって異なる）が 0 個以上含まれているリスト。
Source Address	指定されたグループにトラフィックを送信しているマルチキャストサーバの 1 つのアドレス。
Uptime	エントリが作成されてから経過した時間
v3 Exp	エントリが期限切れになるまでの残り時間（デフォルトは 260 秒）。「V3 Expire」というように「V3」が付いている場合は、IGMP v3 によって学習された送信元に関する時間のみが表示されていることを意味します（デフォルトは 260 秒）。
Fwd	マルチキャスト送信元からのトラフィックが転送されるかどうかを示します。

show ip igmp interface

指定したインタフェースのマルチキャスト情報を表示します。

文法

show ip igmp interface [interface]

interface

vlan vlan-id - VLAN ID. (**有効範囲** : 1-4093)

初期設定

None

コマンドモード

Privileged Exec

例

ここでは、VLAN 1 **の** IGMP **設定、インタフェース上のアクティブなマルチキャストサービスの** IGMP **クエリアとして現在動作しているデバイスを表示します。**

```
Console#show ip igmp interface vlan 1
VLAN 1 : up
IGMP : Disabled
IGMP Version : 2
IGMP Proxy : Enabled
IGMP Unsolicited Report Interval : 400 sec
Robustness Variable : 2
Query Interval : 125 sec
Query Max Response Time : 100 (resolution in 0.1 sec)
Last Member Query Interval : 10 (resolution in 0.1 sec)
Querier : 0.0.0.0
Joined Groups :
Static Groups :
Console#
```

1.24.2 IGMP プロキシールーティング

本機の IGMP Proxy ルーティングの設定に使用するコマンドについて説明します。

コマンド	機能
ip igmp proxy	マルチキャストルーティングの IGMP proxy サービスを有効にします。
ip igmp proxy unsolicitedreport-interval	アップストリームインタフェースによる不要な IGMP レポートの送信間隔を指定します。
show ip igmp interface	エントリが作成されてから経過した時間を表示します。

IGMP プロキシーサービスを有効にするには、次の手順に従ってください。

1. ip multicast-routing コマンドを使って、IP マルチキャスティングをグローバルで有効にします。
2. ip igmp proxy コマンドを使って、アップストリームのマルチキャストルータの接続先のアップストリームインタフェース上の IGMP プロキシーを有効にします。
3. ip igmp コマンドを使って、ダウンストリームインタフェース上の IGMP を有効にして、IGMP メンバーシップレポートを伝送します。
4. Optional – ip igmp proxy unsolicited-report-interval コマンドを使って、アップストリームルータへの不要なレポートの送信頻度を表します。

ip igmp proxy

マルチキャストルーティングの IGMP プロキシサービスを有効にして、ダウンストリームインタフェースで監視される IGMP メンバーシップ情報が要約レポートで示されるアップストリームインタフェースに転送されるようにします（デフォルト :Disabled）。コマンドの前に "no" を付けることにより、プロキシーサービスを無効にします。

文法

[no] ip igmp proxy

初期設定

Disabled

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- IGMP プロキシをインタフェースで有効にすると、そのインタフェースがアップストリームインタフェース（ホストインタフェース）として認識されます。このインタフェースでは、IGMP メンバーシップレポートを送信することによって、IGMP のホスト部分の機能のみを実行します。そのため、自動的に IGMP ルータ機能が無効になります。
- IGMP が有効になっているがマルチキャストツリーのルート方向に位置していないインタフェースは、ダウンストリームインタフェース（ルータインタフェース）として認識されます。このインタフェースは、自らが保有しているすべての IGMP サブスクライバのデータベースを保守することによって、標準の IGMP ルータ機能を実行します。そのため、プロキシマルチキャストサービスを必要とするすべてのインタフェースで IGMP を有効にする必要があります。
- 本システムでは、定期的にマルチキャストルートテーブルの ASM（Any-SourceMulticast）（*,G）転送エントリがチェックされます。ダウンストリーム IGMP グループに関する変更が発生すると、IGMP 状態変更レポートが作成されて、アップストリームルータに送信されます。
- アップストリームネットワーク上に IGMPv1 クエリアまたは IGMPv2 クエリアがある場合、プロキシデバイスは、アップストリームインタフェースで IGMPv1 ホストまたは IGMPv2 ホストとして機能し、VLAN 内にアクティブな IGMPv1 クエリアまたは IGMPv2 クエリアが存在していることを示すため、v1/v2 クエリア存在確認タイマーを設定します。アップストリームネットワーク上に IGMPv1 クエリアまたは IGMPv2 クエリアがない場合、プロキシデバイスは IGMPv3 ホストとして機能します。
- マルチキャストルーティングプロトコルは、IGMP プロキシサービスが有効になっている場合はサポートされません。
- 本システムでサポートされるアップストリームインタフェースは 1 つだけです。
- サポートされるマルチキャストエントリの最大数は 1,024 です。

例

ここでは、マルチキャストルーティングをグローバルで有効にし、VLAN2 をダウンストリームインタフェースに設定後、VLAN 1 をアップストリームインタフェースに設定します。

```
Console(config)#ip multicast-routing
Console(config)#interface vlan 2
Console(config-if)#ip igmp
Console(config-if)#exit
Console(config)#interface vlan 1
Console(config-if)#ip igmp proxy
Console(config-if)#
```

ip igmp proxy unsolicited-reportinterval

アップストリームインタフェースによる不要な IGMP レポートの送信間隔を指定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります

文法

ip igmp proxy unsolicited-report-interval seconds

no ip igmp proxy unsolicited-report-interval

- seconds - 不要なレポートを発行する間隔 (有効範囲 : 1-65535 seconds)

初期設定

400 秒

コマンドモード

Interface Configuration (VLAN)

例

ここでは、不要な IGMP レポートの送信間隔を「5 秒」に設定します。

```
Console(config)#interface vlan
Console(config-if)#ip igmp proxy unsolicited-report-interval 5
Console(config)#
```

1.24.3 MLD (LAYER 3)

レイヤ 3 の MLD（マルチキャストリスナーディスカバリ) の設定に使用するコマンドについて説明します。

コマンド	機能		
ipv6 mld	指定のインタフェースの MLD を有効にします。	IC	P480
ipv6 mld last-memberquery-response-interval	leave メッセージを受信した際のクエリメッセージの送信頻度を設定します。	IC	P481
ipv6 mld max-respinterval	ホストの最大応答時間を設定します。	IC	P482
ipv6 mld query-interval	ホストのクエリメッセージの送信頻度を設定します。	IC	P483
ipv6 mld robustval	パケットロスの期待値を設定します。	IC	P484
ipv6 mld static-group	マルチキャストグループを VLAN インタフェースに静的にバインドします。	IC	P485
ipv6 mld version	インタフェース上で使用する MLD バージョンを設定します。	IC	P486
clear ipv6 mld group	MLD キャッシュからエントリを削除します。	PE	P487
show ipv6 mld groups	MLD グループ情報を表示します。	PE	P488
show ip igmp interface	インタフェースのマルチキャスト情報を表示します。	PE	P490

ipv6 mld

VLAN インタフェースの MLD を有効にします。コマンドの前に ”no” を置くことにより、選択したインタフェースの MLD を無効にします。

文法

[no] ipv6 mld

初期設定

Disabled

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- MLD (Multicast Listener Discovery) は、ipv6 mld コマンドを介してレイヤ 3 の特定の VLAN インタフェースに対して有効に設定することができます。

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld
Console(config-if)#end
Console#show ipv6 mld interface
VLAN 1                              : Up
MLD                                 : Enabled
MLD Version                         : 2
MLD Proxy                           : Disabled
MLD Unsolicited Report Interval     : 400 sec
Robustness Variable                 : 2
Query Interval                      : 125 sec
Query Max Response Time             : 10 sec
Last Member Query Interval          : 1 sec
Querier                             : ::
Joined Groups                       :
Static Groups                       :

Console#
```

ipv6 mld last-member-query-interval

サブネット上の最後に認識された有効なホストから group-specific**、あるいは** group-source-specific leave **メッセージを受信した後の** MLD groupspecific**、あるいは** MLDv2 group-source-specific query **メッセージの送信頻度を設定します。コマンドの前に** ”no” **を置くことにより、デフォルト設定に戻ります。**

文法

ipv6 mld last-memb-query-interval

no ipv6 mld last-memb-query-interval

- seconds - leave **メッセージを受信してから** group-specific**、あるいは** group-source-specific queries **メッセージの送信頻度** (**有効範囲** : 1-255 **秒**)

初期設定

10 (second)

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **マルチキャストグループ、ソース、チャネルを離脱したいホストから** MLD**、あるいは** MLDv2 **の** leave **メッセージを受信すると、このコマンドで設定された間隔ごとに** roup-specific**、あるいは** group-source-specific query **メッセージを送信します。この設定時間後に応答がない場合は、本機はグループ、ソース、チャネルの伝送を中断します。**

例

```
Console(config)#interface vlan 1
Console(config-if)#iipv6 mld last-memb-query-interval 20
Console(config-if)#
```

ipv6 mld max-respinterval

MLD クエリでアドバタイズされている最大応答時間を設定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

ipv6 mld max-resp-interval seconds

no ipv6 mld max-resp-interval

- seconds - MLD クエリでアドバタイズされるレポート遅延 (有効範囲 : 0-255 10 秒の 1 秒)

初期設定

100 (10 秒)

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 「Query Max Response Time」の値を変更することにより、サブネットで渡される IGMP メッセージのバースト性を調整することができます。値が大きいほど、応答間隔が長くなるのでホスト応答の到達範囲が広がるため、トラフィックでバーストが発生する可能性は低くなります。
- 最大応答時間の値は、「Query Interval」よりも小さくなければなりません。

例

下記の例では、最大応答時間を「20 秒」に設定する方法について説明します。

```
Console(config-if)#ipv6 mld max-resp-interval 200
Console(config-if)#
```

関連するコマンド

ipv6 mld query-interval (P483)

ipv6 mld queryinterval

ホストのクエリメッセージの送信頻度を設定します。コマンドの前に ”no” **を置くことにより、デフォルト設定に戻ります。**

文法

ipv6 mld query-interval seconds

no ipv6 mld query-interval

- seconds - **本機による** MLD host-query **メッセージの送信頻度** (**有効範囲** : 1-255 **秒**)

初期設定

125 **秒**

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **マルチキャストルータは、特定のマルチキャストサービスを要求しているダウンストリームホストに接続しているインタフェースを判別するため、ホストクエリメッセージを送信します。ホストクエリメッセージを送信するのは、サブネットの代表マルチキャストルータのみです。ホストクエリメッセージは、マルチキャストアドレス** FF02::1 **宛に、**TTL（Time-To-Live）**値** 1 **を使用して送信されます。**
- **サブネット上の一番小さい** IP **対応マルチキャストルータが代表クエリアになります。**

例

以下の例では、クエリ間隔を「100 **秒」に設定する方法について説明します。**

```
Console(config-if)#ipv6 mld query-interval 100
Console(config-if)#
```

関連するコマンド

ipv6 mld max-resp-interval (P482)

ipv6 mld robustval

インタフェースの信頼性 (パケットロスの期待値) を指定します。コマンドの前に ”no” **を置くことにより、デフォルト設定に戻ります。**

文法

ipv6 mld robustval robust-value

no ipv6 mld robustval

- robust-value - **インタフェースの信頼性** (**有効範囲** : 1-255)

初期設定

2

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **信頼値は、リンク上のパケットロスの期待値を補填するために使用します。それらの状態を終結せずに、ロストする可能性のある現行の** MLD **の状態に関連のある** refresh **パケット数を示します。**
- **ルータでは、最新の受信クエリから取得される信頼性値「ｆ」が採用されます。クエリアの信頼性値（**QRV: Querier's Robustness Variable**）が「**0**」の場合は、**QRV **フィールドで信頼性値が宣言されていないことを意味し、信頼性変数は、このコマンドによって静的に設定される値に設定されます。**QRV **は、「**7**」（**QRV **フィールドの最大値）よりも大きい場合には、「**0**」に設定されます。値「**0**」は、以降に送信されるクエリメッセージでは** QRV **がアドバタイズされないことを意味します。**

例

```
Console(config-if)#ipv6 mld robustval 3
Console(config-if)#
```

ipv6 mld staticgroup

マルチキャストグループを VLAN インタフェースに静的バインドします。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

ipv6 mld static-group group-address [source source-address]

no ipv6 mld static-group [group-address [source source-address]]

- group-address - IPv6 マルチキャストグループアドレス (link-local scope addresses FF02:* は使用不可のため注意してください)
- source-address - 対応するマルチキャストグループアドレスに送信を行うマルチキャストサーバの IPv6 送信元アドレス

初期設定

None

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ASM（*,G）のための静的グループを設定すると、以降は該当のエントリを削除しない限り、そのグループについて送信元アドレスを設定することができなくなります。
- 1 つまたは複数の SSM（S,G）について静的グループを設定すると、以降は、関連付けられている SSM（S,G）エントリをすべて削除しない限り、そのグループについて ASM（*,G）を設定することができなくなります。
- グループのアドレスを指定せずにコマンドの前に ”no” を置くことにより、any-source および source-specific マルチキャストエントリをすべて削除します。
- コマンドの前に ”no” を置くことにより、送信元アドレスを指定せずにスタティックグループを削除し、指定グループの any-source および sourcespecific マルチキャストエントリを削除します。
- 本製品は最大 64 の静的グループエントリをサポートします。

例

以下の例では、VLAN 1 を指定したマルチキャストグループのスタティックメンバーに割り当てます。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld static-group FFEE::0101
Console(config-if)#
```

ipv6 mld version

インタフェースで使用する MLD バージョンを設定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

ipv6 mld version {1 | 2}

no ipv6 mld version

1 - MLD Version 1

2 - MLD Version 2

初期設定

MLD Version 2

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- MLDv1 は IGMPv2、MLDv2 は IGMPv3 から派生します。IGMP は、IP Protocol のメッセージタイプを使用し、MLD は IP Protocol 58 のメッセージタイプを使用します。これらは、ICMPv6 メッセージのサブネットです。
- MLDv2 は、SSM（Source-Specific Multicast）をサポートするために必要に応じて特定の送信元アドレス、または特定の送信元アドレスを除いた送信元アドレスすべてからのみ特定のマルチキャストアドレスによりパケットの受信をレポートする機能を追加します。
- MLDv2 は、マルチキャストサーバのバックアップサービスを要求するホストからリバースツリーを構築する SSM(Source-Specific Multicast) をサポートします。
- サブネット上のマルチキャストホストは、MLD のバージョン 1 または 2 のいずれかをサポートすることが可能です。

例

```
Console(config-if)#ipv6 mld version 1
Console(config-if)#
```

clear ipv6 mld group

MLD キャッシュからのエントリを削除します。

文法

clear ipv6 mld group [group-address | interface vlan vlan-id]

- group-address - マルチキャストグループの IPv6 アドレス
- interface

  vlan vlan-id - VLAN ID(有効範囲 : 1-4093)

初期設定

オプションが選択されていない場合は、キャッシュのエントリはすべて削除します。

コマンドモード

Privileged Exec

コマンド解説

- マルチキャストグループのアドレスを入力して、指定したグループのエントリをすべて削除します。インタフェースのオプションを入力して、指定のインタフェースのマルチキャストグループをすべて削除します。オプションを入力しない場合は、キャッシュかマルチキャストグループをすべてクリアにします。

例

下記の例では、VLAN 1 のマルチキャストグループのエントリをすべてクリアにします。

```
Console#clear ipv6 mld interface vlan 1
Console#
```

show ipv6 mld groups

アクティブなマルチキャストグループ、MLD を介して学習されている情報について表示します。

文法

show ipv6 mld groups [{group-address | interface} [detail] |detail]

- group-address - IPv6 マルチキャストグループアドレス (link-local scope addresses FF02:* は使用不可のため注意してください)
- interface
  - vlan vlan-id - VLAN ID (有効範囲 : 1-4093)
- detail - 使用可能なマルチキャストプロセスおよびソースアドレスについての詳細を表示します。

コマンドモード

Privileged Exec

コマンド解説

- マルチキャストグループの情報について表示するには、まず ipv6 mld コマンドを使って割り当てられたグループのインタフェースをまず有効にする必要あります。マルチキャストルーティングは、ip multicast-routing コマンドを介してシステム全体を有効にする必要があります。

例

以下の例では、MLD グループ情報を表わるためのオプションについて表示します。

```
Console#show ipv6 mld groups
Group Address        Interface   VLAN      Uptime    Expire
----------------  ------------------  ---------------  -----
FFEE::101 1 0:1:59 Never
Console#show ipv6 mld groups detail
Interface        : VLAN 1
Group            : FFEE::101
Uptime : 0h:2m:7s
Group Mode       : Include
Last Reporter    : FE80::0101
Group Source List:
Source Address Uptime Expire Fwd
---------------------------------------- ----------- ----------- -
--
FFEE::0101 0h:0m:12s 0h:0m:0s Yes
Console#
```

コマンド	機能

Group Address	直接接続されたサブスクライバ、または本機からのダウンストリームの IP マルチキャストグループのアドレス
Interface VLAN	マルチキャストグループのアドレスに関連のトラフィックをもつ本機のインタフェース
Last Reporter	インタフェースで指定されたマルチキャストグループアドレスについて最後に受信されたメンバーシップレポートの送信元の IP アドレス。
Uptime	エントリが作成されてから経過した時間
Expire	エントリが期限切れになるまでの残り時間（デフォルト :260 秒）。グループモードが ”INCLUDE” の場合は、フィールドには “stopped” と表示されます。
Group mode	「Include」の場合、指定されたマルチキャストアドレスに送信されたパケットの受信は、source-list パラメータで指定される IP 送信元アドレスのみから要求されます。「Exclude」の場合、指定されたマルチキャストアドレスに送信されたパケットの受信は、source-list パラメータで指定されている IP 送信元アドレスおよび送信元タイマーのステータスが期限切れになっているその他の IP 送信元アドレス以外のすべての IP 送信元アドレスから要求されます。EXCLUDE モードは SSM アドレスには適用されません。
Last Reporter	インタフェースで指定されたマルチキャストグループアドレスについて最後に受信されたメンバーシップレポートの送信元の IP アドレス。
Group Source List	マルチキャストの受信を要求する IP ユニキャストアドレスまたはマルチキャストの受信を要求しない IP ユニキャストアドレス（フィルタモードによって異なる）が 0 個以上含まれているリスト。
Source Address	指定されたグループにトラフィックを送信しているマルチキャストサーバの 1 つのアドレス。
Fwd	マルチキャスト送信元からのトラフィックが転送されるかどうかを示します。

show ipv6 mld interface

指定したインタフェースのマルチキャスト情報を表示します。

文法

show ipv6 mld interface [interface]

- interface

  vlan vlan-id - VLAN ID (**有効範囲** : 1-4093)

初期設定

None

コマンドモード

Privileged Exec

例

以下の例では、VLAN1 **の** MLD **設定、インタフェース上のアクティブなマルチキャストサービスの** MLD **クエリアとして現在動作しているデバイスについて表示します。**

```
Console#show ipv6 mld interface vlan 1
VLAN 1                    : Up
MLD                       : Enabled
MLD Version               : 2
MLD Proxy                 : Disabled
MLD Unsolicited Report Interval : 400 sec
Robustness Variable       : 2
Query Interval            : 125 sec
Query Max Response Time   : 10
Last Member Query Interval : 1
Querier : FE80::200:E8FF:FE93:82A0
Joined Groups :
Static Groups :
FFEE::101
Console#
```

1.24.4 MLD PROXY ROUTING

ここでは、本機の MLD プロキシールーティングを設定するために使用するコマンドについて説明します。

コマンド	機能	モード	
ipv6 mld proxy	マルチキャストルーティングの MLD プロキシーサービスを有効にします。	IC	P492
ipv6 mld proxy unsolicited-reportinterval	アップストリームインタフェースにより不正な IGMP レポートの送信頻度を指定します。	IC	P494
show ipv6 mld interface	指定したインタフェースのマルチキャスト情報を表示します。	PE	P490

MLD proxy サービスを有効にするには、以下の手順に従ってください。

1. ipv6 multicast-routing コマンドを使用して、ルータの IP マルチキャスティングをグローバルで有効にします。
2. ipv6 mld proxy コマンドを使用して、アップストリームのマルチキャストルータに接続されているアップストリームインタフェース上の MLD プロキシを有効にします。
3. ipv6 mld コマンドを使用して、システムによるアップストリームルータへの不正なレポートの送信頻度を表示します。

ipv6 mld proxy

マルチキャストルーティングの MLD プロキシーサービスを有効にして、要約したレポートのアップストリームインタフェース上のダウンストリームインタフェースでモニタリングを行った MLD メンバーシップ情報を伝送します。コマンドの前に ”no” を置くことにより、プロキシーサービスを無効にします。

文法

[no] ipv6 mld proxy

初期設定

Disabled

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- MLD プロキシをインタフェースで有効にすると、そのインタフェースがアップストリームインタフェース（ホストインタフェース）として認識されます。このインタフェースでは、MLD メンバーシップレポートを送信することによって、MLD のホスト部分の機能のみを実行します。そのため、自動的に MLD ルータ機能が無効になります。
- MLD が有効になっているがマルチキャストツリーのルート方向に位置していないインタフェースは、ダウンストリームインタフェース（ルータインタフェース）として認識されます。このインタフェースは、自らが保有しているすべての MLD サブスクライバのデータベースを保守することによって、標準の MLD ルータ機能を実行します。そのため、プロキシマルチキャストサービスを必要とするすべてのインタフェースで MLD を有効にする必要があります。
- MLD グループのダウンストリームに変更が生じると、MLD 変更状態レポートが作成され、アップストリームルータに送信されます。
- アップストリームネットワーク上に MLDv1 クエリアがある場合は、プロキシーデバイスはこれに応じてアップストリームインタフェース上の MLDv1 ホストとして動作します。それ以外は、MLDv2 ホストとして動作します。
- MLD プロキシサービスが有効なインタフェースでは、マルチキャストルーティングプロトコルはサポートされてません。
- システム上でサポート可能なアップストリームインタフェースは 1 つのみです。
- MLD および MLD プロキシは同じインタフェース上では無効になります。
- サポート可能なマルチキャストストリームは最大 1024 までです。

例

以下の例では、マルチキャストルーティングをグローバルで有効にして、VLAN2 **をダウンストリームインタフェースに設定後、**VLAN 1 **をアップストリームインタフェースに設定します。**

```
Console(config)#ip multicast-routing
Console(config)#interface vlan 2
Console(config-if)#ipv6 mld
Console(config-if)#exit
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld proxy
Console(config-if)#
```

ipv6 mld proxy unsolicited-reportinterval

アップストリームインタフェースにより不正な MLD レポートの送信頻度を指定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

ipv6 mld proxy unsolicited-report-interval seconds

no ipv6 mld proxy unsolicited-report-interval

- seconds - **不正なレポートの発行間隔** (**有効範囲** : 1-65535 **秒**)

初期設定

400 **秒**

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **不正なレポート間隔は、**MLD **プロキシーが有効なインタフェースにのみ適用されます。**
- MLD **および** MLD **プロキシは、同じインタフェース上では無効です。**

例

以下の例では、不正な MLD **の送信間隔を「**5 **秒」に設定します。**

```
Console(config)#interface vlan
Console(config-if)#ip igmp proxy unsolicited-report-interval 5
Console(config)#
```

1.25 MLD スヌーピング

MLD(Multicast Listener Discovery) スヌーピングが IPv6 トラフィック上で動作し、IPv4 の IGMP スヌーピングと同等の機能を実行します。つまり、MLD スヌーピングは、本機のポートの IPv6 マルチキャストトラフィックを動的に制限して、受信したいユーザのポートにのみ転送します。これにより、指定した VLAN の IPv6 マルチキャストパケットのフラッディングを軽減します。

MLD プロトコルのバージョンには、バージョン 1 と 2 の 2 つあります。

MLDv1 制御パケットには、Listener Query、Listener Report、Listener Done メッセージ (IGMPv2 query, report, leave メッセージと同等) が含まれます。

MLDv2 制御パケットには、MLDv1 レポートおよび done メッセージだけでなく、MLDv2 query および report メッセージが含まれます。本機は、MLD クエリア機能をサポートしていませんが、特定のマルチキャストサービスを受信したいホストを検出するためにクエリメッセージを送信します。IGMP スヌーピングおよび MLD スヌーピングは独立した機能のため、同時に機能します。

コマンド	機能	モード	
ipv6 mld snooping	MLD スヌーピングをグローバルで有効にします。	GC	P496
ipv6 mld snooping querier	本機が MLD スヌーピングのクエリアとして動作するのを許可します。	GC	P497
ipv6 mld snooping queryinterval	MLD の general クエリメッセージの送信間隔を設定します。	GC	P498
ipv6 mld snooping querymax-response-time	general クエリの最大応答時間を設定します。	GC	P499
ipv6 mld snooping robustness	バースト値を設定します。	GC	P500
ipv6 mld snooping routerport-expire-time	ルータのポートの期限を設定します。	GC	P501
ipv6 mld snooping unknown-multicast mode	認識されていないマルチキャストパケットのアクションを設定します。	GC	P502
ipv6 mld snooping version	MLD スヌーピングのバージョンを設定します。	GC	P503
ipv6 mld snooping vlan immediate-leave	leave パケットをポート側で受信したり、MLD immediate-leave がペアレント VLAN に対して有効な場合は、leave マルチキャストサービスのメンバーポートを削除します	GC	P506
ipv6 mld snooping vlan mrouter	IPv6 マルチキャストルータのポートを追加します。	GC	P504
ipv6 mld snooping vlan static	マルチキャストグループのメンバーとしてインタフェースを追加します。	GC	P505
show ipv6 mld snooping	MLD スヌーピングの設定を表示します。	PE	P507

show ipv6 mld snooping group	学習したグループを表示します。	PE	P507
show ipv6 mld snooping mrouter	マルチキャストルータのポート情報を表示します。	PE	P508

ipv6 mld snooping

MLD スヌーピングをグローバルで有効にします。コマンドの前に ”no” を置くことにより、MLD スヌーピングを無効にします。

文法

[no] ipv6 mld snooping

初期設定

Disabled

コマンドモード

Global Configuration

例

以下の例では、MLD スヌーピングを有効にします。

```
Console(config)#ipv6 mld snooping
Console(config)#
```

ipv6 mld snooping querier

本機が MLDv2 スヌーピングのクエリアとして動作するのを許可します。コマンドの前に ”no” を置くことにより、この機能を無効にします。

文法

[no] ipv6 mld snooping querier

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- 本機がクエリアとして動作する場合は、クエリアはホストに対してマルチキャスのトラフィックを受信したいかどうかを確認します。
- IPv6 アドレスは、クエリアが動作している VLAN インタフェース上で設定しなければなりません。クエリアとして動作する場合、本機は IPv6 をクエリソースアドレスとして使用します。
- ネットワーク上で IPv6 マルチキャストルータを検出した場合、クエリアは開始せず、既に開始した場合は無効にします。

例

```
Console(config)#ipv6 mld snooping querier
Console(config)#
```

ipv6 mld snooping query-interval

MLD の general クエリメッセージの送信間隔を設定します。

文法

ipv6 mld snooping query-interval interval

no ipv6 mld snooping query-interval

- interval - MLD の general クエリメッセージの送信間隔 (有効範囲 : 60-125 秒)

初期設定

125 秒

コマンドモード

Global Configuration

コマンド解説

- 本機がクエリアとして動作する際に適用されます。
- MLD general query メッセージは、このコマンドで指定した間隔で送信されます。このメッセージがダウンストリームホストにより受信されると、受信先はすべてマルチキャストグループを結合して MLD レポートを構築します。

例

```
Console(config)#ipv6 mld snooping query-interval 100
Console(config)#
```

ipv6 mld snooping query-maxresponse-time

MLD の general クエリでアドバタイズされている最大応答時間を設定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

ipv6 mld snooping query-max-response-time seconds

no ipv6 mld snooping query-max-response-time

- seconds - MLD の general クエリでアドバタイズされている最大応答時間 (有効範囲 : 5-25 秒)

初期設定

10 秒

コマンドモード

Global Configuration

コマンド解説

- 最後のメンバーである場合、そのグループを削除するまでの MLD クエリメッセージへの応答時間を制御します。

例

```
Console(config)#ipv6 mld snooping query-max-response-time seconds
15
Console(config)#
```

ipv6 mld snooping robustness

MLD スヌーピングの信頼性の値を設定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

ipv6 mld snooping robustness value

no ipv6 mld snooping robustness

- value - MLD スヌーピングの信頼性の値 (有効範囲 : 2-10)

初期設定

2

コマンドモード

Global Configuration

コマンド解説

- MLD クエリ数に応じて MLD レポートが検出されない場合は、マルチキャストサービスを受信するポートを取り除きます。信頼性の値は、レポートのないポート上のクエリ数を設定します。

例

```
Console(config)#ipv6 mld snooping robustness 2
Console(config)#
```

ipv6 mld snooping router-port-expiretime

MLD クエリのタイムアウトの値を設定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

ipv6 mld snooping router-port-expire-time time

no ipv6 mld snooping router-port-expire-time

- time - 動的に学習されたルータポートのタイムアウトの値を指定します。(有効範囲 : 300-500 秒)

初期設定

300 秒

コマンドモード

Global Configuration

コマンド解説

- ルータのポートの有効期限は、従来のクエリが中断してからルータのポートの期限が切れるまで（例えば、クエリパケットを受信したインタフェース）待機する時間です。

例

```
Console(config)#ipv6 mld snooping router-port-expire-time 300
Console(config)#
```

ipv6 mld snooping unknown-multicast mode

アンノウンマルチキャストパケットの処理を行うアクションを設定します。コマンドの前に ”no” **を置くことにより、デフォルト設定に戻ります。**

文法

ipv6 mld snooping unknown-multicast mode {flood | to-router-port}

[no] ipv6 mld snooping unknown-multicast mode

- flood - **アンノウンマルチキャストデータパケットをすべてのポートにフラッディングします。**
- to-router-port - **アンノウンマルチキャストデータパケットをルータポートに伝送します。**

初期設定

to-router-port

コマンドモード

Global Configuration

コマンド解説

- “flood” **に設定した場合、ホストによって要求されていない** IPv6 **マルチキャストパケットを受信すると、**VLAN **のポートすべてにフラッディングされます。**
- “router-port” **に設定した場合、ホストによって要求されていない** IPv6 **マルチキャストパケットを受信すると、検出したマルチキャストルータに接続されているポートに伝送されます。**

例

```
Console(config)#ipv6 mld snooping unknown-multicast mode flood
Console(config)#
```

ipv6 mld snooping version

MLD スヌーピングのバージョンを設定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

ipv6 mld snooping version {1 | 2}

1 - MLD version 1.

2 - MLD version 2.

初期設定

Version 2

コマンドモード

Global Configuration

例

```
Console(config)#ipv6 mld snooping version 1
Console(config)#
```

ipv6 mld snooping vlan mrouter

IPv6 マルチキャストポートを静的に設定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

[no] ipv6 mld snooping vlan vlan-id mrouter interface

- vlan-id - VLAN ID (有効範囲 : 1-4093)
- interface
  - ethernet unit/port
    unit - スタック番号 (有効範囲 : 1-8)
    port - ポート番号 (有効範囲 : 1-26)
  - port-channel channel-id (有効範囲 : 1-32)

初期設定

スタティックのマルチキャストルータポートは設定されていません。

コマンドモード

Global Configuration

コマンド解説

- お使いのネットワーク接続に応じて、MLD スヌーピングは常に MLD クエリアを検出することはできないため、MLD クエリアが認識済みのマルチキャスト / スイッチであり、本機のインタフェース（ポート、またはトランク）のネットワークに接続されている場合、インタフェースを手動で設定して、現行のマルチキャストグループをすべて結合することができます。

例

以下の例では、port 1 を VLAN 1 のマルチキャストルータポートに設定する方法について説明します。

```
Console(config)#ipv6 mld snooping vlan 1 mrouter ethernet 1/1
Console(config)#
```

ipv6 mld snooping vlan static

IPv6 マルチキャストグループにポートを追加します。コマンドの前に ”no” を置くことにより、ポートを取り除きます。

文法

[no] ipv6 mld snooping vlan vlan-id static ipv6-address interface

- vlan - VLAN ID (有効範囲 : 1-4093)
- ipv6-address - マルチキャストグループの IPv6 アドレス (形式 : X:X:X:X::X)
- interface
  - ethernet unit/port
    unit - スタックユニット (有効範囲 : 1-8)
    port - ポート番号 (有効範囲 : 1-26)
  - port-channel の channel-id (有効範囲 : 1-32)

初期設定

None

コマンドモード

Global Configuration

例

```
Console(config)#ipv6 mld snooping vlan 1 static
FF00:0:0:0:0:0:0:10C ethernet 1/6
Console(config)#
```

ipv6 mld snooping vlan immediateleave

leave パケットをポート側で受信したり、MLD immediate-leave がペアレント VLAN に対して有効な場合は、leave マルチキャストサービスのメンバーポートを削除します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

[no] ipv6 mld snooping vlan vlan-id immediate-leave

- vlan-id - VLAN 識別子 (有効範囲 : 1-4093)

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- MLD の immediate leave が使用されていない場合には、マルチキャストルータ（またはクエリア）は、MLD グループ離脱メッセージを受信すると、GS （Group Specific）クエリメッセージを送信します。ルータまたはクエリアは、指定されているタイムアウト期間内にクエリに対するホストからの応答がない場合にのみ、そのグループのトラフィックの転送を停止します。
- MLD の immediate leave が有効になっている場合、スイッチは、1 つのホストのみがインタフェースに接続しているものとみなします。したがって、immediate leave は、インタフェースが 1 つの MLD 対応デバイス（サービスホストと MLD スヌーピングを実行している隣接ホストのいずれか）のみに接続している場合に限り、有効にすることができます。

例

MLD の immediate leave を有効にする方法について表示します。

```
Console(config)#ipv6 mld snooping vlan 1 immediate-leave
Console(config)#
```

show ipv6 mld snooping

現行の MLD スヌーピングの設定を表示します。

文法

show ipv6 mld snooping

コマンドモード

Privileged Exec

例

以下の例では、MLD スヌーピング情報を表示します。

```
Console#show ipv6 mld snooping
Service Status : Disabled
Querier Status : Disabled
Robustness ?: 2
Query Interval : 125 sec
Query Max Response Time : 10 sec
Router Port Expiry Time ?  : 300 sec
Immediate Leave                  : Disabled on all VLAN
Unknown Flood Behavior     : To Router Port
MLD Snooping Version        : Version 2
Console#
```

show ipv6 mld snooping group

MLD スヌーピンググループの統計情報を表示します。

文法

show ipv6 mld snooping group

コマンドモード

Privileged Exec

例

以下の例では、MLD スヌーピンググループの設定情報を表示します。

```
Console#show ipv6 mld snooping group
VLAN Multicast IPv6 Address Member port Type
---- ---------------------------------------- ----------- --------
-------
1 FF08::10C Eth 1/ 6 User
Console#
```

show ipv6 mld snooping mrouter

MLD スヌーピングマルチキャストルータ情報を表示します。

文法

show ipv6 mld snooping mrouter vlan vlan-id

- vlan-id - VLAN の識別子 (有効範囲 : 1-4093)

コマンドモード

Privileged Exec

例

```
Console#show ipv6 mld snooping mrouter vlan 1
VLAN Multicast Router Port Type
---- --------------------- ---------
1 Eth 1/ 2 Static
Console#
```

1.25.1 DNS

本コマンドは DNS(Domain Naming System) サービスの設定を行ないます。ドメイン名と IP アドレスのマッピングを行なう DNS テーブルの手動での設定を行なえる他、デフォルトドメイン名の設定又はアドレス変換を行なうための複数のネームサーバの指定を行なうことができます。

DNS は "ip name-server" コマンドを使用し最低 1 つのネームサーバを指定しなければ有効にすることはできません。また、ドメインルックアップは " ip domain-lookup" コマンドにより有効にします

コマンド	機能	モード	ページ
ip host	静的ホスト名－アドレスマッピング	GC	P510
clear host	ホスト名－アドレステーブルからのエントリの削除	PE	P511
ip domain-name	不完全なホスト用のデフォルトドメイン名の設定	GC	P512
ip domain-list	不完全なホスト用のデフォルトドメイン名リストの設定	GC	P513
ip name-server	ホスト名－アドレス変換のための 1 つ又は複数のネームサーバの指定	GC	P514
ip domain-lookup	DNS によるホスト名－アドレス変換の有効化	GC	P515
show hosts	静的ホスト名－アドレスマッピングテーブルの表示	PE	P516
show dns	DNS サービスの設定の表示	PE	P516
show dns cache	DNS キャッシュのエントリの表示	PE	P517
clear dns cache	DNS キャッシュのエントリのクリア	PE	P517

ip host

DNS テーブルのホスト名と IP アドレスのマッピングの静的設定を行ないます。コマンドの前に "no" を置くことでエントリを削除します。

文法

ip host name address1 [address2 … address8]

no ip host name address1 [address2 … address8]

- name — ホスト名（設定範囲：1-64 文字）
- address1 — 関連する IP アドレス
- address2 … address8 — 関連する IP アドレス（追加分）

初期設定

静的エントリなし

コマンドモード

Global Configuration

コマンド解説

- サーバや他のネットワーク機器は複数の IP アドレスによる複数接続をサポートしています。2 つ以上の IP アドレスを静的テーブルやネームサーバからの応答によりホスト名と関連付けを行う場合、DNS クライアントは接続が確立するまで各アドレスに接続を試みます。

例

2 つのアドレスをホスト名にマッピングしています。

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
?rd5
Inet address
?10.1.0.55 192.168.1.55
Alias
Console#
```

clear host

DNS テーブルのエントリを削除します。

文法

clear host {name | *}

- name — ホスト名（設定範囲：1-64 文字）
- * — すべてのエントリを削除

初期設定

なし

コマンドモード

Privileged Exec

例

本例ではすべての DNS テーブルのエントリを削除しています。

```
Console#clear host *
Console#
```

ip domain-name

不完全なホスト名に追加するデフォルトドメイン名を設定します。コマンドの前に "no" **を置くことでドメイン名を削除します。**

文法

ip domain-name name

no ip domain-name

- name — **ホスト名。ドメイン名とホスト名の間のドット** (.) **は入力しないで下さい（設定範囲：**1-64 **文字）**

例

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS disabled
Default Domain Name:
  sample.com
Domain Name List:
Name Server List:
Console#
```

関連するコマンド

ip domain-list（P513）
ip name-server（P514）
ip domain-lookup（P515）

ip domain-list

このコマンドは、不完全なホスト名に追加するドメイン名のリストを設定します。コマンドの前に "no" を置くことでリストからドメイン名を削除します。

文法

ip domain-list name
no ip domain-list name

- name — ホスト名。ドメイン名とホスト名の間のドット (.) は入力しないで下さい（設定範囲：1-64 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- ドメイン名はリストの最後に追加されます。
- 本機の DNS サーバが不完全なホスト名を受信し、ドメイン名リストが指定された場合、本機は追加するリスト内の各ドメイン名をホスト名に加え、一致する特定のネームサーバを確認して、ドメインリストにより動作します。
- ドメインリストがない場合、デフォルトドメイン名が使用されます。ドメインリストがある場合には、デフォルトドメイン名は使用されません。

例

本例では、現在のリストに 2 つのドメイン名を追加し、その後リストを表示しています。

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS disabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
Console#
```

関連するコマンド

ip domain-name（P512）

ip name-server

ドメイン名解決のために 1 つ又は複数のドメインネームサーバのアドレスを指定します。コマンドの前に "no" を置くことでリストからネームサーバを削除します。

文法

ip name-server server-address1 [server-address2 … server-address6]
no ip name-server server-address1 [server-address2 … server-address6]

- server-address1 — **ドメインネームサーバの IP アドレス**
- server-address2 … server-address6 — **ドメインネームサーバの IP アドレス（追加分）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **応答を受信するまで、又はリストの最後に到達するまで、リスト内のネームサーバに対して順番にリクエストを送信します。**

例

```
Console(config)#ip domain-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
   DNS disabled
Default Domain Name:
   .sample.com
Domain Name List:
   .sample.com.jp
   .sample.com.uk
Name Server List:
192.168.1.55
10.1.0.55
Console#
```

関連するコマンド

ip domain-name(P509)
ip domain-lookup(P512)

ip domain-lookup

DNS ホスト名・アドレス変換を有効にします。コマンドの前に "no" を置くことで DNS を無効にします。

文法

[no] ip domain-lookup

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- DNS を有効にする前に最低 1 つのネームサーバを指定する必要があります。
- すべてのネームサーバが削除された場合には DNS は自動的に無効になります。

例

本例では、DNS を有効にし、設定を表示しています。

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS enabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

関連するコマンド

domain-name（P525）
ip name-server（P514）

show hosts

静的ホスト名－アドレスマッピングテーブルを表示します。

コマンドモード

Privileged Exec

例

以前に設定されたエントリと同じアドレスがマッピングされた場合、ホスト名はエイリアスとして表示されます。

```
onsole#show hosts
No. Flag Type IP Address TTL Domain
---- ---- ------- -------------------- ----- --------------------
-----------
  0   2 Address 192.168.1.55               rd5
  1   2 Address 2001:DB8:1::12             rd6
  3   4 Address 209.131.36.158       65 www-real.wa1.b.yahoo.com
  4   4 CNAME POINTER TO:3           65 www.yahoo.com
  5   4 CNAME POINTER TO:3           65 www.wa1.b.yahoo.com
Console#
```

show dns

DNS サーバの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show dns
Domain Lookup Status:
   DNS enabled
Default Domain Name:
   sample.com
Domain Name List:
   sample.com.jp
   sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

show dns cache

DNS キャッシュの内容を表示します。

コマンドモード

Privileged Exec

例

```
Console#show dns cache
No. Flag Type IP Address TTL Domain
------- ------- ------- --------------- ------- --------
  3 4 Host 209.131.36.158 115 www-real.wa1.b.yahoo.com
  4 4 CNAME POINTER TO:3 115 www.yahoo.com
  5 4 CNAME POINTER TO:3 115 www.wa1.b.yahoo.com
Console#
```

項目	解説
NO	各リソースレコードのエントリ番号
FLAG	キャッシュエントリのフラグは常に "4"
TYPE	標準的又はプライマリ名が指定された「CNAME」、既存のエントリと同じ IP アドレスをマッピングされている多数のドメイン名が指定された「ALIAS」
IP	レコードに関連した IP アドレス
TTL	ネームサーバにより報告された生存可能時間
DOMAIN	レコードに関連するドメイン名

clear dns cache

DNS キャッシュのすべての値をクリアします。

コマンドモード

Privileged Exec

例

```
Console#clear dns cache
Console#show dns cache
No. Flag Type IP Address TTL Domain
------- ------- ------- --------------- ------- --------
Console#
```

1.26 DHCP

コマンドグループ	機能	ページ
DHCP Client	DHCP クライアントの設定	P518
DHCP Relay	DHC リレーの設定	P520
DHCP Server	DHCP サーバーの設定	P522

1.26.1 DHCP Client

DHCP (Dynamic Host Configuration Protocol) クライアントの設定を行ないます。任意の VLAN インタフェースに対して DHCP を使用し、IP アドレスを自動的に設定することが可能です。

コマンド	機能	モード	ページ
ip dhcp client class-id	本機の DHCP クライアント ID の指定	IC	P518
ip dhcp restart client	BOOTP 又は DCHP クライアントリクエストの送信	PE	P519

ip dhcp client class-id

インタフェースに対して DHCP クライアント ID の指定をします。コマンドの前に "no" を置くことで ID を削除します。

文法

ip dhcp client class-id{text text | hex hex}

no ip dhcp client class-id

- text — テキスト（範囲：1-15 文字）
- hex — 16 進数値

初期設定

なし

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- DHCP サーバと接続する際のクライアント ID として使用されます。ID タイプは DHCP サーバの要求に依存します。

例

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 00-00-e8-66-65-72
Console(config-if)#
```

関連するコマンド

ip dhcp restart client（P519）

ip dhcp restart client

BOOTP 又は DHCP リクエストを送信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

- ip address コマンドで BOOTP 又は DHCP モードを選択した場合に、IP インタフェースに対して BOOTP 又は DHCP クライアントリクエストを発行します。
- DHCP はサーバに対し使用可能であれば最後に取得したアドレスの使用を要求します。
- BOOTP 又は DHCP サーバが他のドメインに移動していた場合、指定されるアドレスは新しいドメインに基づいたアドレスとなります。

例

本例では、本機が再度同じアドレスを取得しています。

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
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（P546）

1.26.2 DHCP Relay

コマンド	機能	モード	ページ
ip dhcp relay	DHCP リレーエージェントを有効化	IC	P520
ip dhcp relay server	DHCP サーバアドレスを指定	IC	P521

ip dhcp relay

指定した VLAN **で** DHCP **リレーを有効にします。コマンドの前に** "no" **を置くことで無効にします。**

文法

[no] ip dhcp relay

初期設定

無効

コマンドモード

Interface Configuration (VLAN)

例

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay
Console(config-if)#end
Console#show ip interface
Vlan 1 is up, addressing mode is Dhcp
 Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
 MTU is 1500 bytes
 Proxy ARP is disabled
 Split horizon is enabled
Console#
```

ip dhcp relay server

スイッチのリレーエージェントに使用される、DHCP サーバのアドレスを指定します。コマンドの前に "no" を置くことで全てのアドレスを消去します。

文法

ip dhcp relay server address1 [address2 [address3 ...]]

no ip dhcp relay server

- address — DHCP **サーバの** IP **アドレス（**1-3 **アドレス）**

初期設定

なし

コマンドモード

Interface Configuration (VLAN)

例

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

1.26.3 DHCP Server

コマンド	機能	モード	ページ
service dhcp	スイッチで DHCP サーバ機能を有効化	GC	P523
ip dhcp excluded-address	DHCP サーバが除外する DHCP クライアントの IP アドレスを指定	GC	P523
ip dhcp pool	DHCP サーバーの DHCP アドレスプールを設定	GC	P524
network	DHCP アドレスプールのサブネット番号およびマスクを設定	DC	P524
default-router	DHCP クライアントのデフォルトルータリストを指定	DC	P525
domain-name	DHCP クライアントのドメインネームを指定	DC	P525
dns-server	DHCP クライアントで使用可能な DNS サーバを指定	DC	P526
next-server	DHCP クライアントのブートプロセスで、次のサーバを設定	DC	P526
bootfile	DHCP クライアントのデフォルトブートイメージを指定	DC	P527
netbios-name-server	DHCP クライアントで使用可能な NetBios ネームサーバを指定	DC	P528
netbios-node-type	DHCP クライアントの NetBIos ノードタイプを設定	DC	P529
lease	DHCP クライアントにアサインされた IP アドレスの継続時間を設定します。	DC	P530
host*	IP アドレスおよびネットワークマスクを、マニュアルで DHCP クライアントにバインド	DC	P531
client-identifier*	DHCP クライアントのクライアント識別子を指定	DC	P532
hardware-address*	DHCP クライアントのハードウェアアドレスを指定	DC	P533
clear ip dhcp binding	DHCP サーバデータベースから自動アドレスを削除	PE	P534
show ip dhcp binding	DHCP サーバーのアドレスバインディングを表示	PE, NE	P534

* これらのコマンドは、マニュアルでクライアントにアドレスをバインドする際に使用します。

service dhcp

スイッチで DHCP **サーバを有効にします。コマンドの前に** "no" **を置くことで** DHCP **サーバを無効にします。**

文法

[no] service dhcp

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#service dhcp
Console(config)#
```

ip dhcp excluded-address

DHCP **サーバが除外する** DHCP **クライアントを指定します。コマンドの前に** "no" **を置くことで指定したアドレスを削除します。**

文法

ip dhcp excluded-address low-address [high-address]
no ip dhcp excluded-address

- low-address — **除外する** IP **アドレスまたは、除外されるアドレス範囲の最初のアドレス。**
- high-address — **除外されるアドレス範囲の最後のアドレス。**

初期設定

全ての IP **プールアドレスはアサイン可能**

コマンドモード

Global Configuration

例

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```

ip dhcp pool

DHCP アドレスプールの設定を行うとともに、DHCP プール設定モードへ移行します。コマンドの前に "no" を置くことでアドレスプールを削除します。

文法

ip dhcp pool name

no ip dhcp pool

- name — プール名（範囲：1-8 文字）

初期設定

DHCP アドレスプールは設定されていません

コマンドモード

Global Configuration

例

```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

関連するコマンド

network (P524)

host (P531)

network

DHCP アドレスプールに、サブネット番号およびマスクを設定します。コマンドの前に "no" を置くことで設定した値を削除します。

文法

network network-number [mask]

no network

- network-number — DHCP サアドレスプールの IP アドレス
- mask — DHCP アドレスプールのサブネット番号、マスク

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#
```

default-router

DHCP プールのデフォルトルータを指定します。コマンドの前に "no" を置くことで設定された値を削除します。

文法

default-router address1 [address2]

no default-router

- address1 — プライマリルータの IP アドレス
- address2 — 代替ルータの IP アドレス

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#default-router 10.1.0.54 10.1.0.64
Console(config-dhcp)#
```

domain-name

DHCP クライアントのドメイン名を指定します。コマンドの前に "no" を置くことで設定したドメイン名を削除します。

文法

domain-name domain
no domain-name

- domain — クライアントのドメイン名を指定します。（範囲：1-32 文字）

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

dns-server

DHCP クライアントで利用可能な、DNS サーバを指定します。コマンドの前に "no" を置くことでサーバーをリストから削除します。

文法

dns-server address1 [address2]

no dns server

- address1 — プライマリ DNS サーバのアドレスを指定
- address2 — 代替 DNS サーバのアドレスを指定

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

next-server

DHCP クライアントのブートプロセスの、次のサーバを設定します。コマンドの前に "no" を置くことでブートサーバーリストから削除します。

文法

next-server address
no next-server address

- address — IP アドレスを指定します。

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

関連するコマンド

bootfile（P527）

bootfile

DHCP クライアントのデフォルトブートイメージの名前を指定します。このファイルは next-server コマンドで指定された TFTP サーバに置かれます。コマンドの前に "no" を置くことでブートイメージファイル名を削除します。

文法

bootfile filename

no bootfile

- filename — デフォルトブートイメージファイル名

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

関連するコマンド

next-server（P526）

netbios-name-server

DHCP クライアントで利用可能な、NetBIOS WINS ネームサーバを設定します。コマンドの前に "no" を置くことでサーバリストから NetBIOS 名を削除します。

文法

netbios-name-server address1 [address2]

no netbios-name-server

- address1 — プライマリ NetBIOS WINS ネームサーバ名を指定
- address2 — 代替 NetBIOS WINS ネームサーバ名を指定

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

関連するコマンド

netbios-node-type (P529)

netbios-node-type

DHCP クライアントの、NetBIOS ノードタイプを指定します。コマンドの前に "no" を置くことで設定した NetBIOS ノードタイプを削除します。

文法

netbios-node-type type

no netbios-node-type

- type — NetBIOS ノードタイプを指定
  - broadcast
  - hybrid（推奨）
  - mixed
  - peer-to-peer

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

関連するコマンド

netbios-name-server（P528）

lease

DHCP クライアントにアサインされた IP アドレスの継続時間を設定します。コマンドの前に "no" を置くことで初期値に戻します。

文法

lease {days [hours][minutes] | infinite}

no lease

- days — 日数を指定（範囲：0-364）
- hours — 時間を指定（範囲：0-23）
- minutes — 分を指定（範囲：0-59）
- infinite — 期限無し。このオプションは通常 host コマンドによって、BOOTP クライアントへ手動でアドレスをバウンドする際に使用します。

初期設定

1 日

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

host

DHCP クライアントへ手動でバインドする際に、IP アドレスおよびネットワークマスクを指定します。コマンドの前に "no" を置くことで設定した IP アドレスを削除します。

文法

host address [mask]

no host

- address — クライアントの IP アドレスを指定します。
- mask — クライアントのネットワークマスクを指定します。

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

関連するコマンド

client-identifier（P532）
hardware-address（P533）

client-identifier

DHCP クライアントの識別子を指定します。コマンドの前に "no" を置くことで設定したクライアント識別子を削除します。

文法

client-identifier {text text | hex hex}
no client-identifier

- text — クライアント識別子を指定します。（範囲：1-15 文字）
- hex — 16 進数の値

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#client-identifier text steve
Console(config-dhcp)#
```

関連するコマンド

host （P531）

hardware-address

DHCP クライアントのハードウェアアドレスを指定します。コマンドの前に "no" を置くことで設定したハードウェアアドレスを削除します。

文法

hardware-address hardware-address type

no hardware-address

- hardware-address — クライアントデバイスの MAC アドレスを指定
- type — クライアントデバイスで使用されるプロトコル

  ethernet

  ieee802

初期設定

タイプが未指定の場合、デフォルトプロトコルは Ethernet になります。

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#
```

関連するコマンド

host（P531）

clear ip dhcp binding

DHCP サーバーデータベースから、バインドされた自動アドレスを削除します。

文法

clear ip dhcp binding {address | * }

- address — アドレスを指定
- * — 全ての自動バインディングを削除

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#clear ip dhcp binding *
Console#
```

関連するコマンド

show ip dhcp binding (P534)

show ip dhcp binding

DHCP サーバ上のバインディングアドレスを表示します。

文法

show ip dhcp binding [address]

- address — IP アドレスを指定

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show ip dhcp binding

     IP              MAC         Lease Time       Start
                                 (dd/hh/mm/ss)
------------- ----------------- ---------------- -----------
   192.1.3.21    00-00-e8-98-73-21         86400 Dec 25 08:01:57 2002
Console#
```

1.27 VRRP

ルータ冗長性プロトコルは、プライマリ ルータおよび複数のバックアップ ルータをサポートするために、仮想 IP アドレスを使用します。
マスター ルータに障害が発生した時にワークロードを引き継ぐように、バックアップ ルータを構成することができます。また、トラフィック ロードを共有するように構成することもできます。ルータ冗長性の主な目的は、プライマリ ゲートウェイの障害発生時に、固定ゲートウェイで構成されたホスト デバイスがネットワーク コネクティビティを保持できるようにすることです。

コマンド グループ	機能	ページ
Virtual Router Redundancy Protocol	VRRP のインタフェース設定を構成します。	P535

1.27.1 仮想ルータ冗長性プロトコル（VRRP）コマンド

コマンド	機能	モード	ページ
vrrp ip	VRRP を有効にし、仮想ルータの IP アドレスを設定します。	IC	P536
vrrp authentication key	他のルータから受信した VRRP パケットの認証に使用されるキーを構成します。	IC	P537
vrrp priority	VRRP グループ内でのこのルータのプライオリティを設定します。	IC	P538
vrrp timers advertise	マスター仮想ルータの連続するアドバタイズメントの間隔を設定します。	IC	P539
vrrp preempt	現在のマスター仮想ルータよりも高いプライオリティを持つルータが VRRP グループに参加した時、このルータがマスター仮想ルータとして処理を引き継ぐように構成します。	IC	P540
show vrrp	VRRP ステータス情報を表示します。	PE	P541
show vrrp interface	指定インタフェースの VRRP ステータス情報を表示します。	PE	P541
show vrrp router counters	VRRP 統計情報を表示します。	PE	P543
show vrrp interface counters	指定インタフェースの VRRP 統計情報を表示します。	PE	P544

vrrp ip

インタフェース上の仮想ルータ冗長性プロトコル（VRRP）を有効にし、仮想ルータの IP アドレスを指定します。コマンドの前に "no" を置くことで、インタフェース上の VRRP が無効になり、IP アドレスが仮想ルータから削除されます。

文法

[no] vrrp group ip ip-address

- group — 仮想ルータ グループを識別（範囲 : 1-255）
- ip-address — 仮想ルータの IP アドレス

初期設定

仮想ルータ グループは構成されていません。

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 仮想ルータ グループに参加しているすべてのルータのインタフェースは、同じ IP サブネットに属する必要があります。
- 仮想ルータに割り当てられる IP アドレスは、オーナーになるルータ上で予め構成されている必要があります。すなわち、このコマンドで指定された IP アドレスは、仮想ルータ グループの 1 台の、かつ唯一のルータ上にすでに存在している必要があります。また、仮想ルータ アドレスのネットワーク マスクはオーナーから派生します。また、オーナーは、グループ内のマスター仮想ルータとしての役割も果たします。
- 現在の VLAN インタフェース上で複数のセカンダリ アドレスを構成した場合、このコマンドを secondary キーワードとともに使用することで、仮想ルータによってサポートされる任意のセカンダリ アドレスを追加することができます。
- このコマンドを入力すると、VRRP は即座に有効になります。VRRP の他のパラメータ（認証、プライオリティ、アドバタイズメント間隔てなど）をカスタマイズする必要がある場合、最初にこれらのパラメータを構成してから、VRRP を有効にしてください。

例

このコマンドでは、VRRP グループのオーナーとして VLAN 1 のプライマリ インタフェースを使用して、VRRP グループ 1 を作成し、グループのメンバーとしてセカンダリ インタフェースを追加します。

```
Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#
```

vrrp authentication key

他のルータから受信した VRRP **パケットの認証に使用されるキーを指定します。コマンドの前に** "no" **を置くことで、認証は無効になります。**

文法

vrrp group authentication key

no vrrp group authentication

- group — **仮想ルータ グループを識別（範囲** : 1-255）
- key— **認証ストリング（範囲** : 1-8 **英数字文字）。**

初期設定

設定されているキーはありません。

初期設定

なし

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **同じ** VRRP **グループ内のすべてのルータは、同じ認証キーで構成されている必要があります。**
- **グループ内の別のルータから** VRRP **パケットが受信されると、その認証キーは、このルータ上で構成されたストリングと比較されます。キーが合致すれば、メッセージは受理されます。合致しない場合、パケットは廃棄されます。**
- **プレーン テキスト認証では、現実的なセキュリティは何も提供されません。プレーンテキストは、誤設定されたルータが** VRRP **に参加することを防ぐためにのみサポートされています。**

例

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

vrrp priority

VRRP グループ内でのこのルータのプライオリティを設定します。コマンドの前に "no" を置くことで、設定を初期値に戻します。

文法

vrrp group priority level

no vrrp group priority

- group — VRRP グループを識別（範囲 : 1-255）
- level— VRRP グループ内でのこのルータのプライオリティを設定（範囲 : 1-254）

初期設定

100

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 仮想ルータに使用されるのと同じ IP アドレスの物理インタフェースを持つルータが、マスター仮想ルータになります。現在のマスターが故障した時には、最も高いプライオリティを持つバックアップ ルータがマスター ルータになります。元のマスタールータが障害から回復すると、アクティブなマスター ルータとして再び処理を引き継ぎます。
- 2 つまたはそれ以上のルータが同じ VRRP プライオリティで構成されている場合、現在のマスターの故障時には、最も高い IP アドレスを持つルータが、新規マスター ルータとして選出されます。
- vrrp preempt コマンドによりバックアップ プリエンプト機能が有効になっており、現在マスターとして動作しているルータよりも高いプライオリティを持つバックアップルータがオンラインになった場合、このバックアップ ルータが新規マスターとして処理を引き継ぎます。ただし、元のマスター（VRRP IP アドレスのオーナー）がオンラインに戻ると、常にマスターとしての制御を再開します。

例

```
Console(config-if)#vrrp 1 priority 1
Console(config-if)#
```

関連するコマンド

vrrp preempt（P537）

vrrp timers advertise

マスター仮想ルータが、マスターとしてのその状態を通信するためのアドバタイズメントを送信する間隔を設定します。コマンドの前に "no" を置くことで、設定を初期値に戻します。

文法

vrrp group timers advertise interval

no vrrp group timers advertise

- group — VRRP **グループを識別（範囲** : 1-255）
- level— **マスター仮想ルータがアドバタイズメントを行う間隔（範囲** : 1-255 **秒）**

初期設定

1 **秒**

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **現在のマスター仮想ルータからの** VRRP **アドバタイズメントには、そのプライオリティとマスターとしての現在の状態に関する情報が含まれています。**
- VRRP **アドバタイズメントは、マルチキャスト アドレス** 224.0.0.8 **へ送信されます。**
- **マルチキャスト アドレスを使用すると、指定** VRRP **グループに参加していないネットワーク デバイスによって処理される必要のあるトラフィックの量を削減できます。**
- **マスター ルータがアドバタイズメントの送信を停止すると、バックアップ ルータは、プライオリティに基づいてマスター ルータの候補となります。マスターとして処理を引き継ごうとする前の** dead **間隔の値は、**hello **間隔の** 3 **倍に** 0.5 **秒を加えたものになります。**

例

```
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#
```

vrrp preempt

現在マスターとして動作しているルータよりも高いプライオリティを持つルータが VRRP グループに参加した時、このルータがマスター仮想ルータとして処理を引き継ぐように構成します。コマンドの前に "no" を置くことで、プリエンプションは無効になります。

文法

vrrp group preempt [delay seconds]

no vrrp group preempt

- group — VRRP グループを識別（範囲 : 1-255）
- seconds— マスターになる宣言を発行するまでの待機時間です（範囲 : 0-120 秒）。

初期設定

プリエンプション : 有効
待機時間 : 0 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- プリエンプト機能が有効になっており、このバックアップ ルータが現在マスターとして動作しているルータよりも高いプライオリティを持つ場合、新規マスターとして処理を引き継ぎます。ただし、元のマスター（VRRP IP アドレスのオーナー）がオンラインに戻ると、常にマスターとしての制御を再開します。
- この遅延を設定することにより、新規ルータが制御を引き継ぐ前に、現在のマスターからアドバタイズメント メッセージを受信するための追加の時間を与えることができます。マスターになろうとしているルータがオンラインになった時、（新規ルータが）現在のアクティブ ルータを実際にプリエンプトする前に、この遅延時間により、ルーティング テーブルの情報を収集する時間が与えられます。

例

```
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#
```

関連するコマンド

vrrp priority（P538）

show vrrp

VRRP のステータス情報を表示します。

文法

show vrrp [brief | group]

- brief — このルータ上のすべての VRRP グループに関するサマリー情報を表示
- group — VRRP グループを識別します（範囲 : 1-255）

初期設定

なし

コマンド モード

Privileged Exec

コマンド解説

- キーワードを指定せずに、このコマンドを使用すると、このルータ上で構成されたすべての VRRP グループのステータス情報が完全にリスト表示されます。
- このコマンドを brief キーワードとともに使用すると、このルータ上で構成されたすべての VRRP グループのステータスに関する要約情報が表示されます。
- 特定のグループに関するステータス情報を表示するには、グループ番号を指定します。

例

この例では、すべてのグループに関するステータス情報をリスト表示します。

```
Console#show vrrp
 Vlan 1 - Group 1,
 state                          Master
 Virtual IP address             192.168.1.6
 Virtual MAC address            00-00-5E-00-01-01
 Advertisement interval         5 sec
 Preemption                     enabled
 Min delay                      10 sec
 Priority                       1
 Authentication                 SimpleText
 Authentication key             bluebird
 Master Router                  192.168.1.6
 Master priority                255
 Master Advertisement interval  5 sec
 Master down interval           15
Console#
```

項目	解説
State	このインタフェースの VRRP 役割（マスターまたはバックアップ）です。
Virtual IP address	仮想 IP アドレスのオーナーから派生する仮想 MAC アドレスです。
Virtual MAC address	経路情報が変更された回数
Advertisement interval	マスター仮想ルータが、マスターとしての自身の役割をアドバタイズする間隔です。
Preemption	より高いプライオリティのルータが、現在マスターとして動作しているルータをプリエンプトできるか表示します。
Min delay	より高いプライオリティのルータが、現在マスターとして動作しているルータをプリエンプトするまでの遅延時間です。
Priority	このルータのプライオリティです。
Authentication	パケットの検証に使用される認証モードです。
Authentication key	他のルータから受信した VRRP パケットの認証に使用されるキーです。
Master Router	グループ マスターとして現在動作しているルータの IP アドレスです。
Master priority	グループ マスターとして現在動作しているルータのプライオリティです。
Master Advertisement interval	VRRP マスター上で構成されるアドバタイズメント間隔です。
Master down interval	VRRP マスター上で構成される、ダウン間隔です（この間隔は、ローカル設定に関わらず、グループ内のすべてのルータで使用されます）。

この例では、すべてのグループに関するステータス情報の概略をリスト表示します。

```
Console#show vrrp brief
Interface Grp State Virtual Addr Interval Preempt Priority
---------- ----- -------- --------------- ----------- --------
VLAN 1   1 Master    192.168.0.3      1        E          255
Console#
```

項目	解説
Interface	VLAN インタフェース
Grp	VRRP グループ
State	このインタフェースの VRRP 役割（マスターまたはバックアップ）です。
Virtual addr	この VRRP グループを識別する仮想アドレスです。
Int	マスター仮想ルータが、マスターとしての自身の役割をアドバタイズする間隔です。
Pre	より高いプライオリティのルータが、現在マスターとして動作しているルータをプリエンプトできるか表示します。
Prio	このルータのプライオリティです。

show vrrp interface

このコマンドでは、指定した VRRP **インタフェースのステータス情報を表示します。**

文法

show vrrp interface vlan vlan-id { brief }

- vlan-id — **構成された** VLAN **インタフェースの識別子（範囲** : 1 **〜** 4094**）**
- brief — **このルータ上のすべての** VRRP **グループに関するサマリー情報を表示**

初期設定

なし

コマンドモード

Privileged Exec

例

この例では、VLAN 1 **に関するステータス情報を完全にリスト表示します。**

```
Console#show vrrp interface vlan 1
 Vlan 1 - Group 1,
 state Master
 Virtual IP address 192.168.1.6
 Virtual MAC address 00-00-5E-00-01-01
 Advertisement interval 5 sec
 Preemption enabled
 Min delay 10 sec
 Priority 1
 Authentication SimpleText
 Authentication key bluebird
 Master Router 192.168.1.6
 Master priority 1
 Master Advertisement interval 5 sec
 Master down interval 15
Console#
```

* **表示される項目に関する説明は、「**show vrrp（P538)**」を参照してください。**

show vrrp router counters

VRRP プロトコル パケット内のエラーに対するカウンタを表示します。

コマンド モード

Privileged Exec

例

```
Console#show vrrp router counters
 Total Number of VRRP Packets with Invalid Checksum : 0
 Total Number of VRRP Packets with Unknown Error    : 0
 Total Number of VRRP Packets with Invalid VRID     : 0
Console#
```

[注意] Unknown Errorは、未知または非サポート対象のバージョン番号で受信された VRRP パケットを示すことに注意してください。

show vrrp interface counters

指定グループまたはインタフェースで発生した VRRP プロトコル イベントとエラーのカウンタを表示します。

文法

show vrrp group interface vlan interface counters

- group — VRRP グループを識別（範囲 : 1-255）
- interface — 構成された VLAN インタフェースの識別子（範囲 : 1-4094）

初期設定

なし

コマンド モード

Privileged Exec

例

```
Console#show vrrp 1 interface vlan 1 counters
 Total Number of Times Transitioned to MASTER                      : 6
 Total Number of Received Advertisements Packets                   : 0
 Total Number of Received Error Advertisement Interval Packets      : 0
 Total Number of Received Authentication Failures Packets           : 0
 Total Number of Received Error IP TTL VRRP Packets                 : 0
 Total Number of Received Priority 0 VRRP Packets                   : 0
 Total Number of Sent Priority 0 VRRP Packets                       : 5
 Total Number of Received Invalid Type VRRP Packets                 : 0
 Total Number of Received Error Address List VRRP Packets           : 0
 Total Number of Received Invalid Authentication Type VRRP Packets  : 0
 Total Number of Received Mismatch Authentication Type VRRP Packets  : 0
 Total Number of Received Error Packet Length VRRP Packets          : 0
Console#
```

1.28 IP インタフェース

IP アドレスは本機へのネットワーク経由での管理用アクセスの際に使用されます。本機へのアクセスを同時に行うには IPv4/IPv6 アドレスを両方使用することができます。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。

コマンドグループ	機能	ページ
IPv4 Interface	本機の IPv4 アドレスを設定します。	P545
IPv6 Interface	本機の IPv6 アドレスを設定します。	P560
IPv6 to IPv4 Tunnels	IPv4 トンネルを介して IPv6 を設定します。	P592

コマンドグループ	機能
Basic IP Configuration	インタフェースへ IP アドレス、デフォルトゲートウェイを設定
Address Resolution Protocol (ARP)	静的、動的、プロキシ ARP の設定

1.28.1 IPv4 設定

デフォルト設定では、本機に IP アドレスが割り当てられていないため、お使いのネットワーク上で新しいアドレスを手動で設定して本機を管理したり、既存の IP サブネットに本機を接続する必要があります。また、デバイスおよび管理ステーション間、または他のネットワーク上に存在する他のデバイス間でデフォルトゲートウェイを設定することも必要な場合があります（ルータが無効な場合）。ここでは、IP インタフェース、ARP およびプロキシー ARP を設定するコマンドいついて説明します。

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	P546
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	P548
show ip interface	本機の IP 設定の表示	PE	P549
show ip routes	ルーティングテーブル内の指定したエントリを表示します。	PE	P549
traceroute	指定したホストへのルートパケットを表示します。	PE	P550
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	P551

ip address

本機への IP アドレスの設定を行います。コマンドの前に "no" を置くことにより、初期設定に戻します。

文法

ip address { ip-address netmask | bootp | dhcp } { secondary }

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
- dhcp — IP アドレスを DHCP から取得
- secondary — セカンダリ IP アドレスを指定

初期設定

DHCP

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- スイッチがルータとして特定のサブネットに割り当てられるエンドノードデバイスに直接接続している場合（または、共有メディアを使用してエンドノードに接続している場合）は、ルーティングをサポートする VLAN ごとにルータインタフェースを作成する必要があります。ルータインタフェースのアドレスは IP アドレスとサブネットマスクから設定されます。インタフェースアドレスは、ルータインタフェースが接続するネットワークのプリフィックス番号とそのネットワークにおけるルータのホスト番号の両方を設定します。つまり、ルータインタフェースアドレスは、インタフェースに接続されるネットワークセグメントを設定し、ルータに対する IP パケットの送受信を可能にするということです。
- ネットワークインタフェースをルータに設定する前に、まず VLAN を設定してください。
- ネットワークを介して管理用アクセスを取得したり、既存の IP サブネットにルータを接続するには、IP アドレスをデバイスに割り当てる必要があります。特定の IP アドレスは手作業で設定することができ、BOOTP、または DHCP サーバからアドレスを取得しするために、ルータを設定することができます。
- 1 つのインターフェースについて指定できるプライマリ IP アドレスは 1 つだけですが、セカンダリ IP アドレスは複数指定することができます。言い換えれば、インターフェースを使用して複数の IP サブネットにアクセスできるようにする場合にはセカンダリ IP アドレスを指定する必要があるということです。初期設定では、このパラメータを「Primary」に設定します（オプション :Primary または Secondary、デフォルト :Primary）。

- 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] それぞれの VLAN グループに独自の IP インタフェースのアドレスを割り当てることができるため、ルーティングが有効な場合は、これらの IP アドレスのいずれかを使ってルータを管理することが可能です。

例

本例では、VLAN 1 に対して IP アドレスを設定しています。

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

関連するコマンド

ip dhcp restart client (P519)

ipv6 address (P562)

ip default-gateway

セグメントが分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。コマンドの前に "no" **を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

- **デフォルトのゲートウェイは、**ip route 0.0.0.0 0.0.0.0 gateway-address **コマンドを使って設定することも可能です。**
- **スタティックルートは、**ip route **コマンドを使って、トラフィックが指定のアドレスへ到達したか、またはサブネットがゲートウェイを通過したかどうかを確認することも可能です。**
- **デフォルトのゲートウェイは、ゲートウェイに直接接続されたネットワークのインタフェースがルータに設定されている場合にのみ正常に設定可能です。**
- **同一の** link-local **アドレスは各種ゾーン** (RFC 4007) **の異なるインタフェース** / **ノードで使用することが可能であるため、**link-local **ローカルを指定する際、**zone-id **情報（**% **の区切り文字の後の** VLAN **識別子を示す）を含みます。例えば、**FE80::7272%1 **は、**VLAN1 **を** ping **の送信元からのインタフェースとみなします。**

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)#end
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
           IS inter area
* - candidate default
S*   0.0.0.0/0 [1/0] via 10.1.1.254, VLAN1
C    127.0.0.0/8 is directly connected, lo0
C    192.168.2.0/24 is directly connected, VLAN1
```

show ip interface

IP インタフェースの設定を表示します。

初期設定

すべてのインタフェース

コマンドモード

Privileged Exec

例

```
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
Address is 00-00-E8-93-82-A0
Index: 1001, MTU: 1500
Address Mode is DHCP
IP Address: 192.168.0.2 Mask: 255.255.255.0
Proxy ARP is disabled
Console#
```

関連するコマンド

ip address (P546)
show ipv6 interface (P571)

traceroute

指定先の宛先へのルートパケットを表示します。

文法

traceroute host

- host - **ホストの** IP **アドレス、またはエイリアス**

初期設定

None

コマンドモード

Privileged Exec

コマンド解説

- traceroute **コマンドを使用して、指定の宛先に到達するためのパスを決定します。**
- TTL**、または最大ホップ数の上限を超えたり、宛先の応答時にトレースは終了します。**
- traceroute **コマンドは、まず** TTL **の値をもつ** probe **データを送信します。これにより、まずルータはデータを破棄して、エラーメッセージを戻すと、トレース機能は後続の** TTL **レベルの一部の** probe **メッセージを送信し、各メッセージの往復時間を表示します。すべてのデバイスは** “ICMP port unreachable” **メッセージを戻すことにより、**probe **に正しく応答するわけではありません。応答が戻る前にタイマーが切れると、トレース機能により一連のアスタリスクおよび** “Request Timed Out” **メッセージを出力されます。これらの一連のメッセージは、最大のタイムアウトに達した場合のみ終了し、ターゲットデバイスの問題点が表示されます。**

例

```
Console#traceroute 192.168.0.1
Press "ESC" to abort.
Source address     : 192.168.0.9
Destination address: 192.168.0.1
Hop IP Address Packet 1 Packet 2 Packet 3
----------------------------------------------------------------
------------
1 192.168.0.1 <10 ms <10 ms <10 ms
Trace completed.
Console#
```

ping

ネットワーク上の他のノードに対し ICMP echo リクエストパケットを送信します。

文法

ping host [count count][size size]

- host — ホストの IP アドレス / エイリアス
- count — 送信するパケット数（範囲：1-16、初期設定：5）
- size — パケットのサイズ (bytes)（範囲 32-512、初期設定：32）
  ヘッダ情報が付加されるため、実際のパケットサイズは設定した値より 8bytes 大きくなります。

初期設定

サイズ 32bytes、カウント 5 回

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られない場合
- ホスト名の ping を行う場合、DNS サーバが有効であることを確認してください。必要に応じて、ローカルデバイスは、DNS のスタティックホストテーブルで指定することも可能です。

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:
Å@Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

1.28.2 ARP

コマンド	機能	モード	ページ
arp	ARP キャッシュの静的エントリを追加します。	GC	P552
arp-timeout	ARP キャッシュの動的エントリのエージングタイムを設定します。	GC	P553
clear arp-cache	すべての動的エントリを ARP キャッシュから削除します。	PE	P553
show arp	ARP キャッシュのエントリを表示します。	NE, PE	P554
ip-proxy-arp	プロキシ ARP を有効にします。	VC	P555

arp

ARP キャッシュの静的エントリを追加します。コマンドの前に "no" を置くことでキャッシュからエントリを削除します。

文法

arp ip-address hardware-address

no arp ip-address

- ip-address — IP **アドレスを指定します。**
- hardware-address — **ハードウェアアドレスを指定します。**

初期設定

エントリなし

コマンドモード

Global Configuration

例

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

関連するコマンド

clear arp-cache

show arp

arp-timeout

ARP キャッシュの動的エントリのエイジングタイムを設定します。コマンドの前に "no" を置くことで初期設定値に戻します。

文法

arp-timeout seconds
no arp-timeout

- seconds — 動的エントリが ARP キャッシュに残存する時間
（範囲：300-86400 秒、86400 秒は 1 日）

初期設定

1200 秒（20 分）

コマンドモード

Global Configuration

例

```
Console(config)#arp-timeout 900
Console(config)#
```

clear arp-cache

すべての動的エントリを ARP キャッシュから削除します。

コマンドモード

Privileged Exec

例

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp

ARP キャッシュのエントリを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- ARP キャッシュの情報を表示します。最初の行はキャッシュのタイムアウトを表示し、それぞれ IP アドレス、MAC アドレス、タイプ (static, dynamic, other)、および VLAN インタフェースを含む キャッシュエントリが表示されます。“other” のエントリタイプは、このルータのローカルアドレスを示します。

例

```
Console#show arp
Arp cache timeout: 1200(seconds)
IP Address        MAC Address           Type       Interface
---------------  -----------------   --------- -----------
10.1.0.0          ff-ff-ff-ff-ff-ff     other        1
10.1.0.254        00-00-ab-cd-00-00     other        1
10.1.0.255        ff-ff-ff-ff-ff-ff     other        1
123.20.10.123     02-10-20-30-40-50     static       2
345.30.20.23      09-50-40-30-20-10     dynamic      3

Total entry : 5
Console#
```

ip-proxy-arp

プロキシ ARP を有効にします。コマンドの前に "no" を置くことで無効にします。

文法

[no] ip proxy-arp

初期設定

無効

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- Proxy ARP **により、ルーティング以外のデバイスは、別のサブネット、または別のネットワーク上のホストの** MAC **アドレスの判別が可能になります。**
- Proxy ARP **を必要とするエンドステーションは、ネットワーク全体を** 1 **つのネットワークとして表示する必要があります。そのためこれらのノードは、ルータ、またはその他の関連ネットワークデバイスによって使用されるサブネットマスクよりも小さいものを使用する必要があります。**
- Proxy ARP **を拡張して使用することにより、**ARP **トラフィックが増加することにより、大規模な** ARP **アドレスタブレットの検出にかかる時間が増えるため、ルータのパフォーマンスが低下する可能性があります。**

例

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

1.28.3 UDP ヘルパー

UDP(User Datagram Protocol) ヘルパーにより、ホストアプリケーションは、本機から他のネットワークに UDP ブロードキャストパケットを伝送することが可能です。

UDP ヘルパーを設定するために使用するコマンドについて説明します。

コマンド	機能	モード	ページ
ip forward-protocol udp	ブロードキャストトラフィックの伝送先の UDP 宛先ポートを指定します。	GC	P556
ip helper	本機の UDP ヘルパーをグローバルで有効にします。	GC	P557
ip helper-address	代表の UDP プロトコルパケットの伝送先のサーバを指定します。	IC	P558
show ip helper	UDP ヘルパーのコンフィグの設定を表示します。	PE	P559

ip forward-protocol udp

UDP ヘルパーを有効にする際、ブロードキャストのトラフィックの伝送先の UDP 宛先ポートを指定します。コマンドの前に "no" を付けることにより伝送リストから UDP ポートを削除します。

文法

[no] ip forward-protocol udp destination-port

- destination-port - UDP サービスのリクエストの転送先の UDP アプリケーションポート (有効範囲 : 1-65535)

初期設定

UDP ヘルパーを ip helper コマンドで有効にする際、またはリモートサーバのアドレスを ip helper-address コマンドで設定する場合、以下の UDP ポートが伝送リストに含まれます。

BOOTP client	port 67
BOOTP server	port 68
Domain Name Service	port 53
IEN-116 Name Service	port 42
NetBIOS Datagram Server	port 138
NetBIOS Name Server	port 137
NTP	port 37
TACACS service	port 49
TFTP	port 69

コマンドモード

Global Configuration

コマンド解説

- 1 つ以上のリモートサーバへ伝送するコマンドで指定可能な UDP ポート数は、最大 100 つまでです。

例

以下の例では、DHCPv6 UDP パケットの伝送を有効にします。

```
Console(config)#ip forward-protocol udp 547
Console(config)#
```

zzzz

ip helper

本機の UDP ヘルパーをグローバルで有効にします。コマンドの前に "no" を付けることによりこの設定を無効にします。

文法

[no] ip helper

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- ネットワークホストでは、UDP ブロードキャストを使用して、アドレス設定やドメイン名のマッピングなどの情報を判別することがあります。それらのブロードキャストは、ローカルサブネット内でのみ送信され、全ホストブロードキャスト（all-ones ブロードキャスト -255.255.255.255）とダイレクトサブネットブロードキャスト（例 :10.10.10.255 など）のどちらかになります。マルチセグメントネットワーク内に展開されるアプリケーションサーバの数を減らすため、UDP ヘルパーを使用して、指定した UDP アプリケーションポートのブロードキャストパケットが別のネットワークセグメント内のリモートサーバに転送されるようにすることができます。
- UDP ヘルパーを設定するには、ip helper コマンドでを使ってグローバルで有効にしなければなりません。（「DNS サービスの全般パラメータの設定」を参照）、ブロードキャストトラフィックの転送先となる UDP 宛先ポートを ip forward-protocol udp コマンドで指定する必要があります。また、ip helperaddress コマンドで指定した別のネットワーク上で UDP クライアントを動作させるようリモートサーバを設定します。

例

以下の例では、本機の UDP ヘルパーをグローバルで有効にします。

```
Console(config)#iphelper
Console(config)#
```

ip helper-address

代表の UDP プロトコルパケットの伝送先のアプリケーションサーバ、またはサブネット（指定したブロードキャストアドレス）を指定します。コマンドの前に "no" を付けることによりこの設定を無効にします。

文法

[no] ip helper-address ip-address

- ip-address - UDP ブロードキャストパケットの転送先のホストアドレス、あるいは指定のブロードキャストアドレス (有効範囲 : 1-65535)

初期設定

None

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- このコマンドにより指定可能な helper アドレスは 20 個までです。
- UDP ヘルパーを使用して UDP パケットを転送するには、選択されたインタフェースにクライアントが接続されており、そのインタフェースが IP アドレスを指定して設定されていなければなりません。
  - 転送される UDP パケットは、「IP Service」→ 「UDP Helper」→ 「Forwarding」を選択して表示される画面で指定する必要があり、以下の条件を満たすものでなければなりません。
  - 受信されるフレームの MAC アドレスが all-ones ブロードキャストアドレス（ffff.ffff.ffff）であること。
  - IP 宛先アドレスは、以下のいずれかであること。

    -all-ones ブロードキャスト（255.255.255.255）

    - 受信先インタフェースのサブネットブロードキャスト
  - IP TTL（Time To Live）値が 2 以上であること 。
  - IP が UDP(17) である こ と。
  - UDP 宛先ポ ー ト は、TFTP、DNS、Time、NetBIOS、BOOTP、ま た は DHCP ポ ー ト は ip forward-protocol udp コマンドにより指定されている UDP ポ ー ト で な け れ ば な り ま せ ん。
- ヘルパーアドレスをこのコマンドで指定する場合は、UDP ポートは ipforward-protocoludp コマンドで指定されておらず、デフォルト設定では ip forward-protocol udp コマンドで記述しているように一部の UDP プロトコルタイプのブロードキャストトラフィックが転送されます。

例

以下の例では、代表 UDP **ブロードキャストパケットが指定のブロードキャストアドレス** (192.168.2.255) **に転送されていることを示します。**

```
Console(config)#interface vlan 1
Console(config-if)#ip helper-address 192.168.2.255
Console(config-if)#
```

show ip helper

UDP **ヘルパーのコンフィグレーションの設定を表示します。**

コマンドモード

Privileged Exec

コマンド解説

- UDP **ヘルパーのコンフィグレーションの設定（機能上のステータス、ブロードキャストトラフィックの伝送先の** UDP **ポート、トラフィックの転送先のリモートサーバまたはサブネットを含む）をすべて表示します。**

例

```
Console#show ip helper
Helper mechanism is enabled
Forward port list (maximum count: 100)
  547
Total port number now is: 1
Helper address list (maximum count: 1024)
Interface VLAN 1:
  192.168.1.44
  192.168.2.255
Total helper number now is: 2
Console#
```

1.28.4 IPv6 インタフェース

コマンド	機能	モード	ページ
Interface Address Configuration and Utilities			
ipv6 default-gateway	認識されていない次のホップをもつ宛先に使用する IPv6 デフォルトゲートウェイを設定します。	GC	P561
ipv6 address	IPv6 グローバルユニキャストアドレスを設定し、インタフェースの IPv6 を有効にします。	IC	P562
ipv6 address eui-64	下位の 64 ビットで EUI-64 のインタフェース ID を使用して、インタフェースの IPv6 グローバルユニキャストアドレスを設定し、インタフェース上の IPv6 を有効にします。	IC	P564
ipv6 address link-local	インタフェースの IPv6 link-local アドレスを設定し、インタフェース上の IPv6 を有効にします。	IC	P566
ipv6 enable	明示的に IPv6 アドレスで設定されていないインタフェース上の IPv6 を有効にします。	IC	P568
ipv6 mtu	インタフェース上で送信される IPv6 パケットの MTU を設定します。	IC	P570
show ipv6 interface	IPv6 インタフェースの有用性、および設定した値を表示します。	NE, PE	P571
show ipv6 mtu	IPv6 インタフェースの MTU を表示します。	NE, PE	P572
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。	NE, PE	P573
clear ipv6 traffic	IPv6 トラフィックのカウントをリセットします。	PE	P578
ping6	IPv6 の ICMP echo request パケットをネットワーク上の他のノードに送信します。	PE	P579
traceroute6	指定したホストへのルートパケットを表示します。	PE	P583
Neighbor Discovery			
ipv6 hop-limit	このルータにより設定されたルータアドバタイズメントで使用される最大ホップ数を設定します。	GC	P584
ipv6 neighbor	IPv6 ネイバーディスカバリキャッシュのスタティックエントリを設定します。	GC	P581
ipv6 nd dad attempts	アドレスの重複を検出時にインターフェースで連続して送信されるネイバー要請メッセージ の数を設定します。	IC	P585
ipv6 nd ns-interval	IPv6 ネイバー要請を再送信する間隔を設定します。	IC	P587
ipv6 nd reachable-time	一部の到達可能な確証イベントが発生後、リモート IPv6 ノードが到達可能と見なすまでの時間を設定します。	IC	P589
clear ipv6 neighbors	IPv6 ネイバー検出キャッシュ内のダイナミックエントリすべてを削除します。	PE	P590
show ipv6 neighbors	IPv6 ネイバー検出キャッシュ内の情報を表示します。	PE	P590

ipv6 default-gateway

認識されていない次のホップをもつ宛先に使用する IPv6 デフォルトゲートウェイを設定します。コマンドの前に "no" を付けることにより、以前設定したゲートウェイを削除します。

文法

ipv6 default-gateway ipv6-address

no ipv6 address

- ipv6-address - 認識されていない次のホップをもつ宛先に使用するデフォルトの次のホップルータの IPv6 アドレス。

初期設定

デフォルトのゲートウェイ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

- IPv6 アドレスはすべてコロンで区切られた 16 ビットの 16 進数値を 8 つ使用し、アドレスでダブルコロンを 1 つ使用します。また未設定フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。
- 同一の link-local アドレスは各種ゾーン (RFC4007) の異なるインタフェース / ノードで使用することが可能であるため、link-local ローカルを指定する際、zone-id 情報（% の区切り文字の後の VLAN 識別子を示す）を含みます。例えば、FE80::7272%1 は、VLAN1 を ping の送信元からのインタフェースとみなします。
- IPv6 デフォルトゲートウェイは、そのゲートウェイに直接接続するネットワークインタフェースがスイッチで設定されている場合にのみ、正常に設定することができます。

例

以下の例では、デバイスのデフォルトゲートウェイを設定します。

```
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)#
```

関連するコマンド

show ipv6 route (P607)

ip default-gateway (P548)

ipv6 address

IPv6 グローバルユニキャストアドレスを設定し、インタフェースの IPv6 を有効にします。引数を使用せずにコマンドの前に "no" を付加することにより、インタフェースから IPv6 アドレスを手動で削除するか、特定の IPv6 アドレスを指定してコマンドの前に "no" を付けることによりインタフェースから IPv6 アドレスを削除します。

文法

ipv6 address ipv6-address/prefix-length

no ipv6 address [ipv6-address/prefix-length]

- ipv6-address - ネットワークプレフィクスとホストアドレスビットを含む完全な IPv6 アドレス
- prefix-length - プレフィックス（つまり、アドレスのネットワーク部）を設定するアドレスの（先頭からの）連続ビットの数を示す 10 進数。

初期設定

IPv6 アドレスは設定されていません。

コマンドモード

Interface Configuration (VLAN, IPv6/v4 Tunnel)

コマンド解説

- IPv6 アドレスはすべてコロンで区切られた 16 ビットの 16 進数値を 8 つ使用し、アドレスでダブルコロンを 1 つ使用します。また未設定フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。
- 同一の link-local アドレスは各種ゾーン (RFC4007) の異なるインタフェース / ノードで使用することが可能であるため、link-local ローカルを指定する際、zone-id 情報（% の区切り文字の後の VLAN 識別子を示す）を含みます。例えば、FE80::7272%1 は、VLAN1 を ping の送信元からのインタフェースとみなします。
- IPv6 デフォルトゲートウェイは、そのゲートウェイに直接接続するネットワークインタフェースがスイッチで設定されている場合にのみ、正常に設定することができます。
- スタティックトンネルのグローバル IPv6 アドレスを設定すると、このコマンドにより設定される link-local アドレスは、基本となる送信元インタフェースの 32-bit の IPv4 アドレスである IPv4 パケットのヘッダ部分に表示され、頭から 0 で表示され合計 64 ビットで埋められます。
- “Universal/Local” ビットが ”0” の場合は、インタフェースの識別子はグローバルで固有のものではないということを表します。ホストの該当する物理インタフェース上に使用中の IPv4 アドレスが複数ある場合は、インタフェースのプライマリアドレスを使用します。IPv4 の仮想インタフェースの IPv6 の link-local アドレスは、前述のようにインタフェースの識別子をプレフィックスの FE80::/64 に追加することにより設定されるため、注意してください。
- 重複するアドレスが検出された場合は、警告メッセージがコンソールに送信されます。

例

以下の例では、完全な IPv6 アドレスおよびプレフィックスの長さを指定します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::72/96
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

関連するコマンド

ipv6 address eui-64(P607)

show ipv6 interface(P571)

ip address(P546)

ipv6 address eui-64

下位の 64 ビットで EUI-64 のインタフェース ID を使用して、インタフェースの IPv6 グローバルユニキャストアドレスを設定し、インタフェース上の IPv6 を有効にします。引数を使用せずにコマンドの前に "no" を付加することにより、インタフェースから IPv6 アドレスを手動で削除するか、特定の IPv6 アドレスを指定してコマンドの前に "no" を付けることによりインタフェースから IPv6 アドレスを削除します。

文法

ipv6 address ipv6-prefix/prefix-length eui-64

no ipv6 address [ipv6-prefix/prefix-length eui-64]

- ipv6-prefix - **インタフェースに割り当てられたアドレスの IPv6 ネットワーク部分**
- prefix-length - **アドレスの頭から連続ビット数を示す 10 進数値は、プレフィックスより構成されます（例えば、アドレスのネットワーク部分）。**

初期設定

IPv6 **アドレスは設定されていません。**

コマンドモード

Interface Configuration (VLAN, IPv6/v4 Tunnel)

コマンド解説

- **送信元 IPv6 アドレスまたはネットワーククラス。アドレスは、コロンで区切られた 16 ビットの 16 進数値を 8 つ使用して、RFC 2373 「IPv6 Addressing Architecture」に準拠する形式で指定しなければなりません。アドレスでダブルコロンを 1 つ使用して、未設定フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。**
- **リンクローカルアドレスがインタフェースに割り当てされていない場合は、グローバルユニキャストアドレス、およびインタフェースのリンクローカルアドレスをを動的に設定します（link-local アドレスは、プレフィックス FE80 と EUI-64 形式に修正された MAC アドレスより構成されます。）**
- ipv6-prefix **で指定されている値には、指定のプレフィックスの長さが 64 ビットを下回る場合は高位のホストビットが含まれる場合があります。指定のプレフィックスの長さが 64 ビットを上回る場合は、アドレスのネットワーク部分がインタフェースの識別子よりも優先されます。**
- **アドレスの重複が検出された場合は、警告メッセージがコンソールに送信されます。**
- IPv6 **アドレスの長さは 16bytes であり、そのうちの下位 8bytes は、通常、デバイスの MAC アドレスに基づく固有のホスト ID を形成します。EUI-64 仕様は、8bytes の拡張 MAC アドレスを使用するデバイスを対象としています。（EUI-48 形式としても知られる）従来の 6bytes の MAC アドレスを使用するデバイスについては、アドレスのユニバーサルビットまたはローカルビットを反転させて MAC アドレスの上位 3bytes と 下位 3bytes との間に 16 進数値 FFFE を挿入することにより、MAC アドレスを EUI-64 形式に変換する必要があります。**
- **例えば、デバイスの EUI-48 アドレスが 28-9F-18-1C-82-35 である場合は、最初に、EUI-64 要件が満たされるようにする（つまり、グローバルに設定されているアドレスについては 1、ローカルに設定されているアドレスについては 0 となるようにする）ため、**

グローバルビットまたはローカルビットを反転させて、28 を 2A に変更します。2bytes の FFFE が OUI（組織ごとに固有の ID、または企業 ID）とアドレスの残りの部分の間に挿入されて、修正版の EUI-64ID である 2A-9F-18-FF-FE-1C-82-35 となります。

- このホストアドレス指定方式を使用すると、単一のデバイスの複数の IP インタフェースで同じインタフェース ID を使用できるようになります（ただし、それらのインタフェースが異なるサブネットに接続していることが前提となります）。
- “Universal/Local” ビットが ”0” の場合は、インタフェースの識別子はグローバルで固有のものではないということを表します。ホストの該当する物理インタフェース上に使用中の IPv4 アドレスが複数ある場合は、インタフェースのプライマリアドレスを使用します。IPv4 の仮想インタフェースの IPv6 の link-local アドレスは、前述のようにインタフェースの識別子をプレフィックスの FE80::/64 に追加することにより設定されるため、注意してください。

例

ここでは、ネットワークのプレフィックス 2001:0DB8:0:1::/64 を指定して、EUI-64 インタフェースの識別子がアドレスの下位の 64 ビットで使用されていることを示します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/
64[EUI]
2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

関連するコマンド

show ipv6 interface (P571)

ipv6 address linklocal

インタフェースの IPv6 link-local アドレスを設定し、インタフェース上の IPv6 を有効にします。

引数を使用せずにコマンドの前に "no" を付加することにより、インタフェースから IPv6 アドレスを手動で削除するか、特定の IPv6 アドレスを指定してコマンドの前に "no" を付けることによりインタフェースから IPv6 アドレスを削除します。

文法

ipv6 address ipv6-address link-local

no ipv6 address [ipv6-address link-local]

- ipv6-address - インタフェースに割り当てられた IPv6 アドレス

初期設定

IPv6 アドレスは設定されていません。

コマンドモード

Interface Configuration (VLAN, IPv6/v4 Tunnel)

コマンド解説

- 指定したアドレスは、コロンで区切られた 16 ビットの 16 進数値を 8 つ使用して、RFC2373 「IPv6 Addressing Architecture」に準拠する形式で指定しなければなりません。アドレスでダブルコロンを 1 つ使用して、未設定フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。アドレスのプレフィックスは、FE80~FEBF の範囲内の値に設定しなければなりません。
- このコマンドで指定されたアドレスは、インタフェースに自動的に設定されたリンクローカルアドレスに置き換えられます。
- 複数の IPv6 グローバルユニキャストアドレスを設定することが可能ですが、インタフェースにつき設定可能なリンクローカルアドレスは 1 つです。
- アドレスの重複が検出された場合は、警告メッセージがコンソールに送信されます。

例

以下の例では、link-local アドレス FE80::269:3EF9:FE19:6779 を VLAN1 に置き換えます。リンクローカルアドレスに対して、FE80~FEBF 範囲内のプレフィックスが必要となり、ホストアドレスの最初の 16 ビットのグループは 0269 形式で ”0” で埋められます。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-
local
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
FE80::269:3EF9:FE19:6779/64
Global unicast address(es):
2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/
64[EUI]
2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
FF02::1:FF19:6779
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

関連するコマンド

ipv6 enable (P568)

show ipv6 interface (P571)

ipv6 enable

明示的に IPv6 アドレスで設定されていないインタフェース上の IPv6 を有効にします。コマンドの前に "no" を付加することにより明示的に IPv6 アドレスで設定されていないインタフェース上の IPv6 を無効にします。

文法

[no] ipv6 enable

初期設定

IPv6 は無効です。

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 現行の VLAN インタフェースの Pv6 を有効にして、link-local ユニキャストアドレスを自動的に設定します。アドレスのプレフィックスは ”FE80” を使用し、本機の MAC アドレスを EUI-64 形式に修正したアドレスに変換することによりアドレスのホスト部分を設定します。
- アドレスのタイプにより、同一のローカルサブネットに接続されているすべてのデバイスに対して、IPv6 を介してアクセス可能となります。
- ローカルセグメント上でアドレスの重複が検出されると、インタフェースは無効となり、警告メッセージがコンソールに表示されます。
- no ipv6 enable コマンドにより、IPv6 アドレスに明示的に設定されていないインタフェースの IPv6 を無効にすることはありません。

例

以下の例では、VLAN 1 **の** IPv6 **を有効にすると、**link-local **アドレスの** FE80::2E0:CFF:FE00:FD/64 **は自動的に設定されます。**

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
FE80::200:E8FF:FE93:82A0/64
Global unicast address(es):
2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
FF02::1:2
FF02::1:FF00:72
FF02::1:FF00:0
FF02::1:FF93:82A0
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

関連するコマンド

ipv6 address link-local (P566)

show ipv6 interface (P571)

ipv6 mtu

インタフェース上で送信される IPv6 パケットの MTU を設定します。コマンドの前に "no" を付けることによりデフォルト設定に戻ります。

文法

ipv6 mtu size

no ipv6 mtu

- size - MTU サイズをしています (有効範囲 : 1280-65535 bytes)

初期設定

1500 bytes

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- このコマンドで設定する最大値は、物理インタフェースの MTU（現在は 1,500bytes に固定）を超えてはなりません。
- デフォルト以外の値を設定すると、このデバイスから送信されるルータアドバタイズメントに MTU オプションが含まれます。このオプションは、（そのようにしないとリンク MTU が十分に認識されない場合に）リンク上のすべてのノードが同じ MTU 値を使用するようにするために用意されています。
- IPv6 ルータは、他のルータから転送される IPv6 パケットをフラグメント化しません。ただし、IPv6 ルータに接続しているエンドステーションから発信されるトラフィックはフラグメント化することができます。
- 同じ物理メディア上のすべてのデバイスは、正しく動作するには、同じ MTU を使用する必要があります。
- MTU を設定できるようにするため、先に IPv6 を有効にしなければなりません。

例

以下の例では、VLAN 1 の MTU を 1280 bytes に設定します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mtu 1280
Console(config-if)#
```

関連するコマンド

show ipv6 mtu (P572)

jumbo frame (P32)

show ipv6 interface

IPv6 インタフェースの有用性、および設定した値を表示します。

文法

show ipv6 interface [brief [vlan vlan-id [ipv6-prefix/prefix-length]]]

- brief - IPv6 オペレーションステータスの概要、およびインタフェースごとに設定したアドレスを表示します。
- vlan-id - VLAN ID (有効範囲 : 1-4093)
- iipv6-address - ネイバーデバイスの IPv6 アドレス。アドレスは、コロンで区切られた 16 ビットの 16 進数値を 8 つ使用して、RFC2373「IPv6Addressing Architecture」に準拠する形式で指定しなければなりません。アドレスでダブルコロンを 1 つ使用して、未設定フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。

コマンドモード

Normal Exec, Privileged Exec

例

以下の例では、本機に設定されている IPv6 アドレスをすべて表示します。

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
FE80::200:E8FF:FE93:82A0/64
Global unicast address(es):
2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
FF02::1:2
FF02::1:FF00:72
FF02::1:FF00:0
FF02::1:FF93:82A0
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

関連するコマンド

show ip interface (P549)

show ipv6 mtu

受信可能な MTU と併せて、ICMP packet-too-big メッセージを戻す先の宛先の MTU キャッシュを表示します。

コマンドモード

Normal Exec, Privileged Exec

例

以下の例では、デバイスの MTU キャッシュを表示します。

```
Console#show ipv6 mtu
MTU Since Destination Address
1400 00:04:21 5000:1::3
1280 00:04:50 FE80::203:A0FF:FED6:141D
Console#
```

項目	解説
MTU	宛先から返された ICMP packet-too-big メッセージに含まれていた調整済みの MTU であり、現在は、このパスで送信されるすべてのトラフィックに使用されている MTU
Since	ICMP packet-too-big メッセージを宛先から受信するまでの経過時間
Destination Address	ICMP packet-too-big メッセージの送信元アドレス

show ipv6 traffic

本機で送受信される IPv6 トラフィックの統計情報を表示します。

コマンドモード

Normal Exec, Privileged Exec

例

以下の例では、IPv6 ユニキャストおよびマルチキャストトラフィック、同様に ICMP, UDP および TCP 統計等の統計情報が表示されます。

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received
total received
header errors
too big errors
no routes
address errors
unknown protocols
truncated packets
discards
```

パラメータ	説明
IPv6 Statistics	
IPv6 Received	
Total	インタフェースで受信された入力データグラムの総数（エラーとして受信されたものを含む）。
Header Errors	IPv6 ヘッダに、バージョン番号の不一致、フォーマット違いエラー、過剰ホップ数、IPv6 オプションなどのエラーが含まれていたために破棄された入力データグラムの数。
Too Big Errors	サイズが発信インタフェースのリンク MTU を超えていたため転送できなかった入力データグラムの数。
No Routes	宛先に送信するためのルートを検出できなかったために破棄された入力データグラムの数。
Address Errors	IPv6 ヘッダの宛先フィールド内の IPv6 アドレスがこのエンティティで受信される有効なアドレスではなかったために破棄された入力データグラムの数。この数には、無効なアドレス（例 : ::0）およびサポートされていないアドレス（例 : 割り当てられていないプレフィックスをもつアドレス）をもつデータグラムが含まれます。IPv6 ルータではないためデータグラムを転送しないエンティティの場合、この数には、宛先アドレスがローカルアドレスではないために破棄されたデータグラムが含まれます。
Unknown Protocols	正常に受信されたが、プロトコルが不明であるため、またはサポートされていないために破棄されたローカルアドレス宛のデータグラムの数。この値は、該当のデータグラムの宛先インタフェース（データグラムによっては必ずしも入力インタフェースとはならない）でインクリメントされます。

Truncated Packets	データグラムのフレームに十分なデータが含まれていなかったために破棄された入力データグラムの数。
Discards	処理の続行を妨げる問題は検出されなかったが（バッファ領域不足などのために）破棄された入力 IPv6 データグラムの数。ただし、この数には、再アセンブリの待機中に破棄されたデータグラムは含まれません。
Delivers	IPv6 ユーザプロトコル（ICMP を含む）について正常に配信されたデータグラムの総数。この値は、該当のデータグラムの宛先インタフェース（データグラムによっては必ずしも入力インタフェースとはならない）でインクリメントされます。
Reassembly Request Datagrams	インタフェースで再アセンブリする必要があった受信 IPv6 フラグメントの数。この値は該当のフラグメントの宛先インタフェース（フラグメントによっては必ずしも入力インタフェースとはならない）でインクリメントされるという点に注意してください。
Reassembled Succeeded	正常に再アセンブリされた IPv6 データグラムの数。この値は該当のデータグラムの宛先インタフェース（データグラムによっては必ずしも入力インタフェースとはならない）でインクリメントされるという点に注意してください。
Reassembled Failed	IPv6 再アセンブリアルゴリズムによって検出された（タイムアウトやエラーなど、何らかの原因による）問題の数。この数は必ずしも破棄された IPv6 フラグメントの数ではないので注意してください。 それは、アルゴリズムによっては（特に、RFC 815 のアルゴリズムでは）フラグメントが受信時に結合されるのでフラグメントの数を追跡できないからです。この値は、該当のフラグメントの宛先インタフェース（フラグメントによっては必ずしも入力インタフェースとはならない）でインクリメントされます。
IPv6 Transmitted	
Forwards Datagrams	このエンティティで受信されて最終的な宛先に転送された出力データグラムの数。IPv6 ルータとして使用されていないエンティティの場合、この数には、エンティティ経由でソースルーティングされ、ソースルーティングプロセスが正常に完了したパケットのみが含まれます。正常に転送されたデータグラムについては、この数は発信インタフェースでインクリメントされるので注意してください。
Requests	ローカル IPv6 ユーザプロトコル（ICMP を含む）によって送信要求時に IPv6 に提供された IPv6 データグラムの総数。この数には ipv6IfStatsOutForw データグラムでカウントされるデータグラムは含まれないので注意してください。
Discards	宛先への送信を妨げる問題は検出されなかったが（バッファ領域不足などのために）破棄された出力 IPv6 データグラムの数。該当のパケットが（任意指定の）破棄条件を満たす場合はこの数に ipv6IfStatsOutForw データグラムでカウントされるデータグラムが含まれるので注意してください。
No Routes	宛先に送信するためのルートを検出できなかったために破棄された入力データグラムの数。
Generated Fragments	出力インタフェースでのフラグメント化の結果として生成された出力データグラムフラグメントの数。
Fragment Succeeded	出力インタフェースで正常にフラグメント化された IPv6 データグラムの数。

Fragment Failed The	出力インタフェースでフラグメント化する必要があったがフラグメント化できなかったために破棄された IPv6 データグラムの数。
ICMPv6 Statistics	
ICMPv6 received	
Input	インタフェースで受信された ICMP メッセージの総数（ipv6IfIcmpInErrors でカウントされるすべてのメッセージを含む）。この場合のインタフェースは ICMP メッセージの宛先インタフェース（データグラムによっては必ずしも入力インタフェースとはならない）であるという点に注意してください。
Errors	インタフェースで受信された ICMP メッセージの総数（ipv6IfIcmpInErrors でカウントされるすべてのメッセージを含む）。この場合のインタフェースは ICMP メッセージの宛先インタフェース（データグラムによっては必ずしも入力インタフェースとはならない）であるという点に注意してください。
Destination Unreachable Messages	インタフェースで受信された ICMP 宛先到達不能（Destination Unreachable）メッセージの数。
Packet Too Big Messages	インタフェースで受信された ICMP パケットサイズ超過（Packet Too Big）メッセージの数。
Time Exceeded Messages	インタフェースで受信された ICMP 時間切れ（Time Exceeded）メッセージの数。
Parameter Problem Messages	インタフェースで受信された ICMP パラメータ障害（Parameter Problem）メッセージの数。
Echo Request Messages	インタフェースで受信された ICMP エコー（要求）（Echo (request)）メッセージの数。
Echo Reply Messages	インタフェースで受信された ICMP エコー応答（Echo Reply）メッセージの数。
Router Solicit Messages	インタフェースで受信された ICMP ルータ要請（Router Solicit）メッセージの数。
Router Advertisement Messages	インタフェースで受信された ICMP ルータアドバタイズメント（Router Advertisement）メッセージの数。
Neighbor Solicit Messages	インタフェースで受信された ICMP 近傍要請（Neighbor Solicit）メッセージの数。
Neighbor Advertisement Messages	インタフェースで受信された ICMP 近傍アドバタイズメント（Neighbor Advertisement）メッセージの数。
Redirect Messages	インタフェースで受信されたリダイレクトメッセージの数。
Group Membership Query Messages	インタフェースで受信された ICMPv6 グループメンバーシップクエリ（Group Membership Query）メッセージの数。
Group Membership Response Messages	インタフェースで受信された ICMPv6 グループメンバーシップ応答（Group Membership Response）メッセージの数。
Group Membership Reduction Messages	インタフェースで受信された ICMPv6 グループメンバーシップ離脱（Group Membership Reduction）メッセージの数。

Multicast Listener Discovery Version 2 Reports	インタフェースで受信された MLDv2 レポートの数。
ICMPv6 Transmitted	
Output	インタフェースが送信しようとした ICMP メッセージの総数。この数には icmpOutErrors でカウントされるすべてのメッセージが含まれるので注意してください。
Destination Unreachable Messages	インタフェースで送信された ICMP 宛先到達不能（Destination Unreachable）メッセージの数。
Packet Too Big Messages	インタフェースで送信された ICMP パケットサイズ超過（Packet Too Big）メッセージの数。
Time Exceeded Messages	インタフェースで送信された ICMP 時間切れ（Time Exceeded）メッセージの数。
Echo Request Messages	インタフェースで送信された ICMP エコー（要求）（Echo (request)）メッセージの数。
Echo Reply Messages	インタフェースで送信された ICMP エコー応答（Echo Reply）メッセージの数。
Router Solicit Messages	インタフェースで送信された ICMP ルータ要請（Router Solicit）メッセージの数。
Router Advertisement Messages	インタフェースで送信された ICMP ルータアドバタイズメント（Router Advertisement）メッセージの数。
Neighbor Solicit Messages	インタフェースで送信された ICMP 近傍要請（Neighbor Solicit）メッセージの数。
Neighbor Advertisement Messages	インタフェースで送信された ICMP 近傍アドバタイズメント（Neighbor Advertisement）メッセージの数。
Redirect Messages	送信されたリダイレクトメッセージの数。ホストの場合、リダイレクトは送信されないので、このオブジェクトは常にゼロになります。
Group Membership Query Messages	インタフェースで送信された ICMPv6 グループメンバーシップクエリ（Group Membership Query）メッセージの数。
Group Membership Response Messages	送信された ICMPv6 グループメンバーシップ応答（Group Membership Response）メッセージの数。
Group Membership Reduction Messages	送信された ICMPv6 グループメンバーシップ離脱（Group Membership Reduction）メッセージの数。
Multicast Listener Discovery Version 2 Reports	インタフェースで送信された MLDv2 レポートの数。
UDP Statistics	
Input	UDP ユーザに配信された UDP データグラムの総数。
No Port Errors	宛先ポートにアプリケーションがなかった受信 UDP データグラムの総数。

Other Errors	宛先ポートにアプリケーションがないこと以外の理由で配信できなかった受信 UDP データグラムの数。
Output	このエンティティから送信された UDP データグラムの総数。

コマンドモード

Privileged Exec

コマンド解説

- ping6 コマンドを使用して、ネットワーク上に別のサイトが到達可能か、パス上の遅延を確認します。
- 同一の link-local アドレスは各種ゾーン (RFC 4007) の異なるインタフェース / ノードで使用することが可能であるため、link-local を指定する際、zone-id 情報（% の区切り文字の後の VLAN 識別子を示す）を含みます。例えば、FE80::7272%1 は、VLAN1 が ping の送信元のインタフェースとみなします。
- ホスト名の ping を行う場合、DNS サーバが有効であることを確認してください。必要に応じて、ローカルデバイスは、DNS のスタティックホストテーブルで指定することも可能です。
- ホスト名をもつ ping6 を使用する場合は、ルータはまず IPv6 アドレスのエイリアスを解決後、IPv4 アドレスのエイリアスを解決します。

例

```
Console#ping6 FE80::2E0:CFF:FE9C:CA1?0%1/64
Type ESC to abort.
PING to FE80::2E0:CFF:FE9C:CA10%1/64, by 5 0-byte payload ICMP
packets,
timeout is 3 seconds
response time: 20 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 1
response time: 0 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 2
response time: 10 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 3
response time: 0 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 4
response time: 10 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 5
Ping statistics for FE80::2E0:CFF:FE9C:CA10%1/64:
5 packets transmitted, 5 packets received (100%), 0 packets lost
(0%)
Approximate round trip times:
Minimum = 0 ms, Maximum = 20 ms, Average = 8 ms
Console#
```

clear ipv6 traffic

IPv6 トラフィックのカウンタをリセットします。

コマンドモード

Privileged Exec

コマンドの解説

show ipv6 traffic コマンドによって表示されたカウンタをすべてリセットします。

例

```
Console#clear ipv6 traffic
Console#
```

ping6

ICMP echo (IPv6) リクエストパケットをネットワーク上の別のノードに送信します。

文法

ping6 {ipv6-address | host-name} [count count] [size size]

- ipv6-address - ipv6-address - ネイバーデバイスの IPv6 アドレス。アドレスは、コロンで区切られた 16 ビットの 16 進数値を 8 つ使用して、RFC 2373「IPv6 Addressing Architecture」に準拠する形式で指定しなければなりません。アドレスでダブルコロンを 1 つ使用して、未設定フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。
- host-name - ドメインネームサーバを介して、IPv6 アドレスで解決可能なホスト名の文字列。
- count - パケットの送信数 (有効範囲 : 1-16)
- size - パケットのバイト（有効範囲 : 48-18024 bytes)。実際のパケットサイズは、ルータによりヘッダ情報が追加されるため、指定したサイズより 8bytes 大きくなります。

初期設定

count: 5

size: 100 bytes

コマンドモード

Privileged Exec

コマンドの解説

- ping6 コマンドを使って、ネットワークの別のサイトに到達していないか、パス上の遅延の有無を評価します。
- 同一の link-local アドレスは各種ゾーン (RFC 4007) の異なるインタフェース / ノードで使用することが可能であるため、link-local ローカルを指定する際、zone-id 情報（% の区切り文字の後の VLAN 識別子を示す）を含みます。例えば、FE80::7272%1 は、VLAN1 を ping の送信元からのインタフェースとみなします。
- ホスト名の ping を行う場合、DNS サーバが有効であることを確認してください。必要に応じて、ローカルデバイスは、DNS のスタティックホストテーブルで指定することも可能です。
- ホスト名をもつ ping6 を使用する場合は、ルータはまず IPv6 アドレスのエイリアスを解決後、IPv4 アドレスのエイリアスを解決します。

例

```
Console#ping6 FE80::2E0:CFF:FE9C:CA10%1/64
Type ESC to abort.
PING to FE80::2E0:CFF:FE9C:CA10%1/64, by 5 0-byte payload ICMP
packets,
timeout is 3 seconds
response time: 20 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 1
response time: 0 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 2
response time: 10 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 3
response time: 0 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 4
response time: 10 ms [FE80::2E0:CFF:FE9C:CA10] seq_no: 5
Ping statistics for FE80::2E0:CFF:FE9C:CA10%1/64:
5 packets transmitted, 5 packets received (100%), 0 packets lost
(0%)
Approximate round trip times:
Minimum = 0 ms, Maximum = 20 ms, Average = 8 ms
Console#
```

ipv6 neighbor

IPv6 ネイバーディスカバリ キャッシュのスタティックエントリを設定します。コマンドの前に ”no” を置くことにより、キャッシュからスタティックエントリを除去します。

文法

ipv6 neighbor ipv6-address vlan vlan-id hardware-address

no ipv6 mtu

- ipv6-address - ネットワークインタフェースの 1 つを介して設定可能なネイバーデバイスの IPv6 アドレス。送信元 IPv6 アドレスまたはネットワーククラス。アドレスは、コロンで区切られた 16 ビットの 16 進数値を 8 つ使用して、RFC 2373「IPv6 Addressing Architecture」に準拠する形式で指定しなければなりません。アドレスでダブルコロンを 1 つ使用して、未設定フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。
- vlan-id - VLAN ID (有効範囲 : 1-4093)
- hardware-address - ネイバーデバイスの 48 ビット IPv6 が有効なの MAC レイヤアドレス。アドレスは、ハイフンで区切られた 6 つの 16 進数のペアとして形式化されなければなりません。

初期設定

None

コマンドモード

Global Configuration

コマンド解説

- IPv6 の ARP は、NDP に置き換えれます。ipv6 neighbor コマンドは、ARP によって実装される mac-address-table static コマンドと同じです。
- スタティックエントリは IPv6 が有効なインタフェース上でのみ設定可能です。
- 本機では、スタティックエントリが IPv6 ネイバーディスカバリキャッシュに移行する前に到達可能であるかどうかを判別しません。
- 指定したエントリが IPv6 ネイバーディスカバリを介して動的に学習され、かつネイバーディスカバリキャッシュに既に存在する場合は、スタティックエントリに変換されます。ネイバーディスカバリプロセスによってその後検出された場合は、IPv6 ネイバーディスカバリキャッシュは修正されません。
- no ipv6 enable コマンドによりインタフェースの IPv6 を無効にすると、インタフェースの IPv6 ネイバーディスカバリキャッシュで動的に学習されたエントリはすべて削除されますが、スタティックエントリは削除されません。

例

以下の例では、グローバルユニキャストアドレスのスタティックエントリを MAC アドレスにマッピングします。

```
Console(config)#ipv6 neighbor 2009:DB9:2229::81 vlan 1 30-65-14-
01-11-86
Console(config)#end
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D
- Delay,
P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address Age Link-layer Addr State VLAN
2009:DB9:2229::80 956 12-34-11-11-43-21 R 1
2009:DB9:2229::81 Permanent 30-65-14-01-11-86 R 1
FE80::1034:11FF:FE11:4321 961 12-34-11-11-43-21 R 1
Console#
```

関連するコマンド

show ipv6 neighbors (P704)

mac-address-table static (P300)

traceroute6

指定する宛先へのルートパケットを表示します。

文法

traceroute {ipv6-address | host-name}

- ipv6-address - **ネイバーデバイスの** IPv6 **アドレス。アドレスは、コロンで区切られた** 16 **ビットの** 16 **進数値を** 8 **つ使用して、**RFC2373「IPv6Addressing Architecture」**に準拠する形式で指定しなければなりません。アドレスでダブルコロンを** 1 **つ使用して、未設定フィールドを埋めるために必要な該当数の** 0（**ゼロ**）**を示すこともできます。**
- host-name - **ドメインネームサーバを介して、**IPv6 **アドレスで解決可能なホスト名の文字列。**

初期設定

None

コマンドモード

Privileged Exec

コマンド解説

- traceroute6 **コマンドを使用して、指定した宛先に到達するためのパスを判別します。**
- **同一の** link-local **アドレスは、各種ゾーン** (RFC 4007) **の異なるインタフェース** / **ノードごとに使用可能です。そのため、**link-local **アドレスを指定する場合は、**% **デリミタの後に** VLAN **識別子を示す** zone-id **情報を含めます。例えば、**FE80::7272%1 **は、**ping **送信先のインタフェースとして** VLAN1 **を識別します。トレースは、宛先から応答が返された場合、タイムアウト期間**（TTL）**を超えた場合、または最大ホップ数を超えた場合、終了されます。**
- **トレースルート機能では、最初に、**TTL **値が** 1 **に設定されているプローブデータグラムが送信されます。すると、そのデータグラムが最初のルータで破棄され、エラーメッセージが返されます。次に、以降のそれぞれの** TTL **レベルのプローブメッセージがいくつか送信され、メッセージごとのランドトリップ時間が表示されます。すべてのデバイスが「**ICMP Port Unreachable （ICMP **ポート到達不能）」メッセージを返して正常に応答するわけではありません。応答が返される前にタイマーに設定されている時間が経過すると、トレース機能によって一連のアスタリスク**（*）**と「**Request Timed Out （**要求タイムアウト）」メッセージがプリントされます。それらの長い一連のメッセージは、最大タイムアウト時間に達したときにのみ終了し、ターゲットデバイスに関する問題が発生している可能性あることを示します。**

例

```
Console#traceroute6 FE80::2E0:CFF:FE9C:CA10%1/64
Press "ESC" to abort.
Traceroute to FE80::2E0:CFF:FE9C:CA10%1/64, 30 hops max, timeout
is 3
seconds, 5 max failure(s) before termination.
Hop Packet 1 Packet 2 Packet 3 IPv6 Address
--- -------- -------- -------- ----------------------------------
----------
1 <10 ms <10 ms <10 ms FE80::2E0:CFF:FE9C:CA10%1/64
Trace completed.
Console#
```

Neighbor Discovery

ipv6 hop-limit

このルータにより設定されたルータアドバタイズメントで使用される最大ホップ数を設定します。コマンドの前に "no" **を付けることによりデフォルト設定に戻ります。**

文法

ipv6 hop-limit hops

no ipv6 hop-limit

- hops - **ルータアドバタイズメントおよびすべての** IPv6 **パケットの最大ホップ数。**
  (**有効範囲** : 1-255)

初期設定

1

コマンドモード

Interface Configuration (VLAN)

例

以下の例では、ルータのアドバタイズメントのホップリミットを「64**」に設定します。**

```
Console(config-if)#interface vlan 1
Console(config)#ipv6 hop-limit 64
Console(config)#
```

ipv6 nd dad attempts

アドレスの重複を検出時に インタフェースで連続して送信されるネイバー要請メッセージの数を設定します。コマンドの前に "no" を付けることによりデフォルト設定に戻ります。

文法

ipv6 nd dad attempts count

no ipv6 nd dad attempts

- count - 重複アドレスがインタフェース上で存在するかどうかを判別するために送信されたネイバー要請メッセージ数 (有効範囲 : 0-600)

初期設定

1

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 値 0 を指定すると、重複アドレスの検出が無効になります。
- 重複アドレスの検出によって、新規ユニキャスト IPv6 アドレスをインタフェースに割り当てる前に、そのアドレスが既にネットワーク上に存在しているかどうかが確認されます。
- 重複アドレスの検出は、サスペンドになっているインタフェース（「VLAN グループの設定」を参照）では停止されます。
- インタフェースがサスペンドになっている間は、そのインタフェースに割り当てられているすべてのユニキャスト IPv6 アドレスが「Pending」状態になります。インタフェースが管理者によって再びアクティブにされると、自動的に重複アドレスの検出が再開されます。
- 再アクティブ化されたインタフェースでは、そのインタフェース上のすべてのユニキャスト IPv6 アドレスに対する重複アドレスの検出が再開されます。インタフェースのリンクローカルアドレスに対する重複アドレスの検出が実行されている間、他の IPv6 アドレスは「Tentative」状態に維持されます。重複するリンクローカルアドレスが検出されなかった場合は、残りの IPv6 アドレスに対する重複アドレスの検出が開始されます。
- 重複するアドレスが検出されると、そのアドレスが「Duplicate」状態に設定され、警告メッセージがコンソールに送信されます。重複するものとして検出されたアドレスがリンクローカルアドレスである場合、そのインタフェースで IPv6 プロセスが無効になります。重複するものとして検出されたアドレスがグローバルユニキャストアドレスである場合、そのアドレスは使用されません。重複アドレスに関連付けられているすべての設定コマンドは、そのアドレスが「Duplicate」状態の間は設定された状態に維持されます。
- インタフェースのリンクローカルアドレスが変更された場合、新規のリンクローカルアドレスについては重複アドレスの検出が実行されますが、既にそのインタフェースに関連付けられている IPv6 グローバルユニキャストアドレスについては重複アドレスの検出は実行されません。

例

以下の例では、VLAN 1 に設定したアドレスに対して、ネイバー要請を 5 回行うように設定します。show ipv6 interface コマンドにより、重複アドレス検出プロセスが現在進行中であることを示します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
FE80::2E0:CFF:FE9C:CA10/64
Global unicast address(es):
2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
2009:DB9:2229::79, subnet is ::
Joined group address(es):
FF02::2
FF02::1:FF00:0
FF02::1:2
FF02::1:FF9C:CA10
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

関連するコマンド

ipv6 nd ns-interval (P587)

show ipv6 neighbors (P590)

ipv6 nd ns-interval

インタフェース上の IPv6 ネイバー要請メッセージの送信間隔を設定します。コマンドの前に "no" を付けることによりデフォルト設定に戻ります。

文法

- milliseconds - IPv6 ネイバー要請メッセージの送信間隔 (有効範囲 : 1000-3600000)

初期設定

1000ms はネイバーディスカバリの動作に対して使用します。

0ms はルータアドバタイズメントでアドバタイズします。

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- デフォルト以外の値を指定すると、その指定した間隔がルータアドバタイズメントとルータ自体の両方で使用されます。
- アドレスの解決時またはネイバーの到達可能性の検証時に近傍要請メッセージを送信する間隔を指定します。そのため、通常の IPv6 動作には極めて短い間隔を使用しないようにしてください。

例

以下の例では、ネイバー要請メッセージの送信間隔を「30000ms」に設定します。

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
FE80::2E0:CFF:FE9C:CA10/64
Global unicast address(es):
2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
2009:DB9:2229::79, subnet is ::
Joined group address(es):
FF02::2
FF02::1:FF00:0
FF02::1:2
FF02::1:FF9C:CA10
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 30000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

関連するコマンド

show running-config (P25)

ipv6 nd reachabletime

一部の到達可能性確認イベントが発生後、リモート IPv6 **ノードが到達可能と見なすまでの時間を設定します。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻ります。**

文法

ipv6 nd reachable-time milliseconds

no ipv6 nd reachable-time

- milliseconds - **到達可能な確認を受けた後、ノードが到達可能とみなされる時間** (**有効範囲** : 1000-3600000)

初期設定

近傍検出動作には デフォルトの 30,000 ms **が使用され、**0 ms **がルータアドバタイズメントでアドバタイズされます。**

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **このパラメータで時間制限を指定することによって、使用不可になっている隣接ノードをルータが検出できるようになります。**
- **この制限時間は、同じリンク上のノードで同じ時間値が使用されるようにするため、インタフェース経由で送信されるすべてのルータアドバタイズメントに含まれます。**
- **時間制限を** 0 **に設定するということは、ルータについて時間制限を指定しないことを意味します。**

例

以下の例では、リモートノードの到達可能な時間を「1000 **ミリ秒」に設定します。**

```
Console(config)#interface vlan 1
Console(config)#pv6 nd reachable-time 1000
Console(config)#
```

clear ipv6 neighbors

IPv6 ネイバー検出キャッシュ内のダイナミックエントリすべてを削除します。

コマンドモード

Privileged Exec

例

以下の例では、IPv6 ネイバーのキャッシュのダイナミックエントリをすべて削除します。

```
Console#clear ipv6 neighbors
Console#
```

show ipv6 neighbors

すべての IPv6 ネイバーディスカバリキャッシュの情報を表示します。

文法

show ipv6 neighbors [vlan vlan-id | ipv6-address]

vlan-id - VLAN ID (有効範囲 : 1-4093)

ipv6-address - ネイバーデバイスの IPv6 アドレス。アドレスは、コロンで区切られた 16 ビットの 16 進数値を 8 つ使用して、RFC2373「IPv6Addressing Architecture」に準拠する形式で指定しなければなりません。アドレスでダブルコロンを 1 つ使用して、未設定フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。

初期設定

すべての IPv6 ネイバーディスカバリのキャッシュエントリが表示されます。

コマンドモード

Privileged Exec

例

以下の例では、本機に認識されている IPv6 ネイバーすべてを表示します。

```
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D
- Delay,
P1 - Probe, P2 - Permanent, U - Unknown
```

パラメータ	説明
IPv6 Address	隣接デバイスの IPv6 アドレス。

Age	アドレスが到達可能であると確認されてからの経過時間（単位 : 秒）。スタティックエントリは値「Permanent」で示されます。
Link-layer Address	物理レイヤの MAC アドレス。
State	ダイナミックエントリについては以下の状態が使用されます。 • Incomplete - エントリに対するアドレス解決の実行中です。近傍要請メッセージがターゲットのマルチキャストアドレスに送信されましたが、まだ近傍アドバタイズメントメッセージが返されていません。 • Invalid - 無効なマッピング。状態が「Invalid」になると、このエントリによって特定されるインタフェースのマッピング（RFC 4293）が解除されます。 • Reachable - 隣接デバイスへの転送パスが機能していた前回の ReachableTime 内に肯定応答が受信されました。デバイスは、Reachable 状態の間は、パケットの送信時に何も特別なアクションを実行しなくなります。 • Stale - 転送パスが機能しているという肯定応答が前回受信されてから ReachableTime を超える時間が経過しています。デバイスは、Stale 状態の間は、パケットが送信されるまで何のアクションも実行しなくなります。 • Delay - 転送パスが機能しているという肯定応答が前回受信されてから ReachableTime を超える時間が経過しています。パケットが前回の DELAY_FIRST_PROBE_TIME 内に送信されました。Delay 状態になってからこの期間が経過するまでに到達可能性確認メッセージを受信しない場合、スイッチは、近傍要請メッセージを送信して、Probe 状態になります。 • Probe - 到達可能性確認メッセージが受信されるまで、近傍要請メッセージが RetransTimer の間隔で再送されて、到達可能性確認メッセージがアクティブに探索されます。 Unknown - 不明な状態。 スタティックエントリについては以下の状態が使用されます。 • Incomplete - エントリで示されているインタフェースが Down 状態になっています。 • Permanent - スタティックエントリであることを示します。 • Incomplete - エントリで示されているインタフェースが Up 状態になっています。到達可能性の検出は、IPv6 近傍探索キャッシュ内のスタティックエントリには適用されません。
VLAN	VLAN 到達先アドレスの VLAN インタフェース。

1.28.5 IPV6 から IPV4 へのトンネリング

本機は、手動により設定したトンネルを使用して IPv4 ネットワーク上の隔離されている IPv6 ノード間の接続 (RFC 2893)、また明示的なトンネル設定をもたない IPv4 クラウドを上の隔離されている IPv6 ドメイン間の接続 (RFC 3056) を行います。

コマンド	機能	モード	
interface tunnel	トンネルインタフェースを設定し、トンネル設定モードに入ります。	GC	P594
ipv6 address	IPv6 グローバルユニキャストアドレスを設定し、インタフェースの IPv6 を有効にします。	IC (tunnel)	P562
ipv6 address link-local	インタフェースの IPv6 の link-local アドレスを設定し、IPv6 を有効にします。	IC (tunnel)	P566
ipv6 address eui-64	下位の 64 ビットの EUI-64 インタフェース ID を使用してインタフェースの IPv6 グローバルユニキャストアドレスを設定し、インタフェースの IPv6 を有効にします。	IC (tunnel)	P564
tunnel destination*	トンネルの宛先の IPv4 アドレスを設定します。	IC (tunnel)	P595
tunnel mode ipv6ip	トンネルモードを手動設定、または「6-to-4 自動トンネル」に設定します。	IC (tunnel)	P597
tunnel source vlan	トンネルの送信元を割り当てる VLAN を設定します。	IC (tunnel)	P599
tunnel ttl	IPv6 トラフィックのトンネルに使用するパケットの IPv4 ヘッダの TTL 値を設定します。	IC (tunnel)	P600
show ipv6 tunnel	IPv4 トンネルを介して、すべての IPv6 のステータス、およびコンフィグレーションの設定値を表示します。	PE	P601

トンネルの宛先は、手動によるトンネルの設定 (RFC 2893) に適用します。

コマンド解説

トンネルを手動 / 自動で設定するには、以下の手順に従って下さい。

1. vlan コマンドで VLAN を設定します。
2. ローカルサービスには VLAN を使用するポートを割り当てて、IPv4 トンネルを介して IPv6 のエントリポイントを設定します（switchport allowed vlan コマンドの使用）
3. IPv4 アドレスを VLAN に割り当てて、ip address コマンドを使ってトンネルのソース (ローカルのエンドポイント）として動作します。
4. interface tunnel コマンドを使って、IPv4 をトンネルを介して IPv6 を設定します。
5. トンネルモードを “configured”（host-to-router、または router-torouter 接続)、あるいは “6to4”(tunnel mode ipv6ip コマンドを使用して router-to-host 、または host-to-host 接続）に設定します。

6.“configured” トンネルモードの場合は、tunnel destination コマンドを使用してトンネルの末端の IPv4 を指定します。

7. tunnel source vlan コマンドを使って、トンネルを VLAN にバインドします。

8. ipv6 address コマンドを使って、IPv6 グローバルユニキャストアドレスをトンネルに割り当てます。

9. 次に、show ipv6 tunnel コマンドを使って、現在お使いのコンフィグレーションの設定値、show ip interface コマンド、または show ip interface brief コマンドを使ってトンネルのインタフェースのステータスを確認してください。

interface tunnel

IPV6 から IPV4 へのトンネリングのインタフェースを設定し、トンネルの設定モードに入ります。トンネル番号をもつ場合はコマンドの前に "no" を付けることによりトンネルを 1 つ削除し、トンネル番号を持たない場合はコマンドの前に "no" を付けることによりトンネルをすべて削除します。

文法

interface tunnel tunnel-number

no interface tunnel [tunnel-number]

- tunnel-number - トンネルインタフェースの識別子 (有効範囲 : 1-16)

初期設定

None

コマンドモード

Global Configuration

コマンド解説

- コマンドに “tunnel,” というラベルを付けた場合でも、RFC 2893 に応じて IPv4 伝送ネットワークを介して IPv6 を手動により設定するか、あるいは RFC 3056 を使用して明示的にトンネルをもたない IPv4 クラウドを介して IPv6 トラフィックの自動伝送方式による設定が可能になります。
- IPv4 トンネルを介して IPv6 を設定する場合、IPv4 ヘッダ内の IPv6 パケットをカプセル化することによって point-to-point トンネルを行い、IPv4 ルーティングインフラストラクチャを介して伝送します。
- IPv4 クラウドを介して IPv6 の伝送を行うこと（RFC 3056 をベースとして) により、固有の IPv4 アドレスを 1 個以上所有するサイトに固有の IPv6 アドレスのプレフィックスを割り当てる方式を設定し、カプセル化方式を指定して、グローバルの IPv4 ネットワークを介してこれらのプレフィックスを使って IPv6 パケットを送信します。

例

```
Console(config)#interface tunnel 1
Console(config-if)#
```

tunnel destination

トンネルの宛先 (あるいは、トンネルのエンドポイント) の IPv4 **アドレスを設定します。コマンドの前に** ”no” **を置くことにより、割り当てた** IPv4 **アドレスを取り除きます。**

文法

tunnel destination ip-address

no tunnel destination

- ip-address - **トンネルの一方にあるデバイスの** IPv4 **アドレス**

初期設定

None

コマンドモード

Interface Configuration (IPv6/v4 Tunnel)

コマンド解説

- “configured” **トンネルモードにのみ適用可能です（**tunnel mode ipv6ip **コマンドを参照ください）。**
- IPv6 **パケットをトンネルを介して伝送する場合、コマンドにより設定されたトンネルの** end-point **アドレスは、**IPv4 **ヘッダをカプセル化するための宛先アドレスとして使用します。**
- **パケットが通過する宛先は、ルーティングテーブル（プレフィックスマスクおよび合致技術を使用した宛先アドレスに応じてパケットを転送）の情報に応じて異なります。**
- IPv6/IPv4 **ホストは、**IPv6 **ルータを持たないデータリンクに接続されており、設定されたトンネルを使用して** IPv6 **ルータに到達することが可能です。このトンネルにより、ホストはそれ以外の** IPv6 **インターネット（例えば、**IPv6-native **アドレスをもつノード）との通信か可能になります。**
- IPv6 **バックボーンに隣接する** IPv6/IPv4 **ルータの** IPv4 **アドレスを認識する場合は、トンネルのエンドポイントアドレスとして使用可能です。このトンネルは、ルーティングテーブルに** IPv6 **の** “default route” **として使用することが可能です。あるいは、トンネルのエンドポントは、**IPv4 **の** “anycast address” **になる場合があります。この方法を使用すると、境界線上の複数の** IPv6/IPv4 **は、**IPv4 **が同じ** IPv4 **アドレスに到達したことをアドバタイズします。これらのルータのすべてがこのアドレスへの独自のアドレスとしてパケットを受信し、このアドレスへのトンネルを通過した** IPv6 **パケットをカプセル解除します。**IPv6/IPv4 **のノードは、カプセル化されたパケットをこのアドレスに送信すると、ボーダールータの** 1 **つにのみ伝送され、通常一番近いルータになります。**
- **デフォルトのトンネルを使用する際は、異なる** IPv4 **フラグメントによる再構築用の各種ルータへの到達を防ぐように注意する必要があります。これにより、カプセル化されたパケットの分裂を避けたり（**1300 bytes **以上の** IPv4 **の** MTU **を確保することにより）、**IPv4 **ルーティングが頻繁に変更されることを防ぐことができます。**
- **デカプセル化ノードのプロトコルを転送するためにパケットを伝送すると、そのパケットは入力フィルタリングに影響されなくなります。双方向のトンネルを設定には、送信元アドレスを変更すると、トンネルのもう一端の** IPv4 **アドレスであることを認証することにより実行されます。一方向のトンネルを設定するには、デカプセル化されているノードは受信可能な送信元アドレスのプレフィックスのリストによって設定されなければなりません。**

- それらのリストのデフォルトでは、エントリを持たないように設定しなければなりません（つまり、ノードは明示的に設定され、一方方向で受信したデカプセル化パケットを伝送します）。

例

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel destination 192.168.1.5
Console(config-if)#
```

tunnel mode ipv6ip

トンネルモードを手動設定、または「6-to-4 自動トンネル」に設定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

tunnel mode ipv6ip {configured | 6to4}

no tunnel mode ipv6ip

- configured - IPv4 ヘッダ内の IPv6 パケットのカプセル化による point-to-point トンネルを使用して、point-topoint トンネルを介して IPv6 を設定し、IPv4 ルーティング（RFC 2893 をベース）を介して実行します。
- 6to4 - あらゆるサイト（グローバルで固有の IPv4 アドレスを持ち、グローバルの IPv4 ネットワークを介してこれらのプレフィックスを使用し、IPv6 パケットを伝送するカプセル化方式を指定します (この方式は RFC 3056 がベースとなります) に、IPv6 パケットを伝送するカプセル化方式を指定します) に 固有の IPv6 アドレスのプレフィックスを割り当てることにより、IPv4 クラウドを介して IPv6 を伝送します。

初期設定

configured

コマンドモード

Interface Configuration (IPv6/v4 Tunnel)

コマンド解説

- IPv4 を介して IPv6 のトンネルを設定するには、RFC2893(IPv4 ルーティングフラストラクチャを介して伝送するために、IPv4 ヘッダ内の IPv6 パケットのカプセル化による point-to-point トンネルを使用）がベースとなります。

  これらのトンネルは、一方方向、あるいは双方向のいずれでも可能です。双方向でトンネルを設定すると、仮想の point-to-point リンクとして動作します。設定したトンネルを使用する場合は、IPv4 トンネルのエンドポイントアドレスは、tunnel destination コマンドによりカプセル化されているノード上に手動で設定されたものでなければなりません。

  6to4 メカニズムは、通常 IPv4 と IPv6 間の境界となるルータ内で多くの場合実施されます。6to4 トンネルのエンドポイントアドレスは IPv6 の 6to4 ホストから送信されるパケットの IPv6 の 6to4 アドレスを介してトンネルの送信元によって決定されます。

  6to4 エンドポイントのアドレスは、IPv6 アドレスのプレフィックスとして “2002:Public IPv4 Address::/48” を使って構築されます。プレフィックスは、RFC2461 で設定されている “Neighbor Discovery for IP Version 6 (IPv6)” など、その他の有効な IPv6 プレフィックスと同じように使用することが可能です。

- IPv6/IPv4 ホストおよびルータは IPv4 パケット内でカプセル化することにより、IPv4 ルーティングトポロジーの領域上で IPv6 データをトンネリングすることができます。トンネルングとは、幅広い方向で使用されており、以下のとおりです。
  - Router-to-Router:IPv4 インフラストレクチャによって接続された IPv6/IPv4 ルータは、IPv6/IPv4 ルータ間で IPv6 パケットをトンネリングすることができます。この場合、トンネルは、IPv6 パケットに受け取られる end-to-end パスのセグメントの１つにまたがります。

- Host-to-Router:IPv6/IPv4 ホストは、IPv4 インフラストラクチャを介して到達可能な中間の IPv6/IPv4 ルータに対して IPv6 パケットをトンネリングすることが可能です。
- Host-to-Host:IPv4 インフラストラクチャによって接続された IPv6/IPv4 ホストは、その間の IPv6 パケットをトンネリングすることが可能です。この場合は、トンネルはパケットが受信可能な end-to-end パス全体にまたがり、またホストは 6to4 ノード、またはネイティブ IPv6 ホストのいずれかになります。
- Router-to-Host:IPv6/IPv4 ルータは、IPv6 パケットを IPv6/IPv4 ホストの最後の宛先までトンネリングすることができます。このトンネルは、end-to-end パスの最後のセグメントにのみまたがります。

トンネリング技術は、カプセル化されているノードによりトンネルの最後にあるノードのアドレスが決定される方式に応じて分類されます。最初の 2 つのトンネリング方式 (router-to-router 方式と host-to-router 方式) は、IPv6 パケットはルータまでトンネリングを行います。このタイプのトンネルのエンドポントは、トンネリングを行っているパケットの宛先と異なります。ルータまでトンネリングする際、IPv パケットをデカプセル化し、それを最終宛先まで伝送を行わなければならない中間ルータです。ルータのトンネリングを行う際、トンネルのエンドポイントは、トンネルの対象となるパケットの宛先と異なるため、トンネルの対象となる IPv6 のアドレスはトンネルのエンドポイントの IPv4 アドレスを提供することはできません。その代りに、トンネルのエンドポイントの IPv4 アドレスは、トンネルの end-point アドレスはカプセル化するノード上で設定されている情報とは異なります。すなわち、“configured tunneling” は、エンドポイントを明示的に識別するために使用しなければなりません。

最後の 2 つのトンネル方式 (host-to-host および router-to-host) では、IPv6 パケットは最終宛先まですべてトンネリングします。この場合、IPv6 パケットとカプセル化 IPv4 ヘッダの両方と同じノードを識別します。実際には、IPv6 宛先アドレスのコード化情報 (これにより、カプセル化ノードはトンネルのエンドポイントの IPv4 アドレスを自動的に判別しまることが可能です）によって明示化することができます。

“6to4 automatic tunneling” ではこの技術を採用し、トンネルのエンドポイントの IPv4 アドレスを自動的に判別するために、IPv4 アドレスを組み込んだ特別な Pv6 アドレス形式を使用します。このことにより、トンネルのエンドポイントのアドレスを明示的に設定する必要がなります。

2 つのトンネル技術（手動及び自動による）では、トンネルのエンドポイントを決定する方法が主に異なります。基本となる方式の大半が以下のとおりです。

- トンネルのエントリノード（カプセル化ノード）により、IPv4 ヘッダのカプセル化を行い、カプセル化されているパケットを送信します。
- トンネルの exit ノードは、カプセル化されたパケットを受信し、パケットの再アセンプリを行い、必要に応じて IPv4 ヘッダの削除、IPv6 ヘッダの更新、受信した IPv6 パケットの処理を行います。

例

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel mode ipv6ip configured
Console(config-if)#
```

tunnel source vlan

トンネルの送信元（トンネルのローカルエンドポイント) を割り当てる先の VLAN **を設定します。コマンドの前に** "no" **を付けることにより、割り当てられた** VLAN **からトンネルを取り除きます。**

文法

tunnel source vlan vlan-id

no tunnel source vlan

- vlan-id - VLAN ID (**有効範囲** : 1-4093)

初期設定

None

コマンドモード

Interface Configuration (IPv6/v4 Tunnel)

コマンド解説

- **トンネルンに割り当てられた** VLAN **は、**IPv4 **アドレスをもつ** L3 VLAN **でなければなりません。それ以外は、エラーメッセージがコンソールに表示されます。**

例

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel source vlan 2
Console(config-if)#
```

tunnel ttl

IPv6 トラフィックのトンネリングに使用するパケットの IPv4 ヘッダにストアされている TTL (Time to Live) の値を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

tunnel ttl ttl-value

no tunnel ttl

ttl-value - IPv4 パケットのカプセル化の TTL 値

(有効範囲 : 0-255、この場合の ”0” は、TTL 値がカプセル化された IPv6 パケットの IP ヘッダに設定されている Hop Limit から取得されることを意味します。)

初期設定

0

コマンドモード

Interface Configuration (IPv6/v4 Tunnel)

コマンド解説

- IPv4 カプセル化パケットの hop limit を設定します。ただし、IPv4 トンネルを通過した IPv6 は “single-hop” としてモデル化されます。つまり、IPv6 がトンネルを通過ごとに、IPv6 hop limit は 1 つずつ減少します。single-hop モデルは、トンネルの存在を隠します。トンネルは、ネットワークユーザには見えないため、経路探索などのネットワーク診断ツールにより検出することはできません。

例

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel ttl 5
Console(config-if)#
```

show ipv6 tunnel

IPv4 を介してすべての IPv6 のステータスおよびコンフィグの設定値を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ipv6 tunnel
Tunnel:1
Tunnel Current State : Up
Tunnel Source Address : [VLAN1]192.168.0.3
Tunnel Destination Address : 192.168.0.2
Time to Live : 255
Tunnel Mode (Configured / 6-to-4 / ISATAP) : Configured
Console#
```

設定したトンネルのインタフェースのステータスを表示します。

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
(None)
Global unicast address(es):
(None)
Joined group address(es):
FF02::1:2
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Tunnel 1 is up
IPv6 is stale.
Link-local address:
FE80::C0A8:3/64
Global unicast address(es):
2002:DB9:2222:7272::72/48, subnet is 2002:DB9:2222::/48
Joined group address(es):
FF02::1
IPv6 link MTU is 0 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#show ipv6 interface brief
Interface VLAN IPv6 IPv6 Address
--------------- ---------- ---------- ---------------------------
------------
VLAN 1 Up Down Unassigned
TUNNEL 1 Up Down 2002:DB9:2222:7272::72/48
TUNNEL 1 Up Down FE80::C0A8:3
Console#
```

1.29 IP ルーティング

本機は IP ルーティング機能をサポートしており、ルーティングパスの管理は、手動によるルーティングの設定、または RIP や OSPF による動的な設定が可能になります。

IP ルーティング機能を有効に設定すると、本機はワイヤスピードを実現するルータ同様に動作するため、異なる IP インタフェースを介した VLAN 間通信や、外部 IP ネットワークへのトラフィックのルーティングを行います。しかし、本機の初期設定ではルーティング機能は設定されていません。ルーティング機能を使用するには、既存のルータ製品のように、最初にこれらの設定を行う必要があります。

工場出荷時の設定では、ポートはすべて単一の VLAN に所属し、レイヤ 2 機能のみを使用するようになっています。そのため、まず、各ユーザグループまたはトラフィックのアプリケーション別に VLAN を作成し、同じグループに所属するすべてのポートを各 VLAN に割り当て、それから各 VLAN に IP インタフェースを設定する必要があります。ネットワークを複数の異なる VLAN に分けることによって、レイヤ 2 レベルで分割されているサブネットワークで分けることができます。同一サブネット内でやり取りされるトラフィックは、レイヤ 2 のスイッチング機能を使用して通信されます。そして、必要な場合には、レイヤ 3 のスイッチング機能を使用して VLAN 間通信ができることになります。

各 VLAN はレイヤ 3 での仮想的なインタフェースに相当します。この仮想インタフェースに対してネットワークアドレスを設定しさえすれば、トラフィックは、異なるサブネット間でレイヤ 3 レベルでルーティングされるようになります。

コマンドグループ	機能	ページ
Global Routing Configuration	静的または動的ルーティングのための、グローバルパラメータの設定および、ルーティングテーブルや、情報交換のためにしようされるプロトコルの統計の表示。	P604
Routing Information Protocol （RIP）	グローバルまたはインタフェースで RIP のパラメータを設定	P615
Open Shortest Path First （OSPF2）	グローバルまたはインタフェースで OSPF2 のパラメータを設定	P708
Open Shortest Path First （OSPF3）	グローバルまたはインタフェースで OSPF3 のパラメータを設定	P717

P601

1.29.1 グローバルルーティング設定

コマンド	機能	モード	ページ
IPv4 Commands			
IP route	スタティックルートを設定します。	GC	P604
maximum-paths	許容範囲のパス数の上限を設定します。		P605
show ip host-route	認識されているルートに関連のあるインタフェースを表示します。	PE	P606
show ip route	ルーティングテーブル内の指定したエントリを表示します。	PE	P607
show ip route database	ルーティングテーブルの静的 / 動的に学習したエントリを表示します。		P609
show ip route summary	ルーティングテーブルのサマリ情報を表示します。	PE	P609
show ip traffic	IP、ICMP、UDP、TCP および ARP プロトコルの統計情報を表示	PE	P610
IPv6 Commands			
ipv6 route	スタティックルートを設定します。	GC	P611
show ipv6 route	ルーティングテーブルの IPv6 のルートのエントリを表示します。	PE	P613

IPv4 コマンド

ip route

スタティックルートの設定を行います。コマンドの前に "no" を置くことで、設定されたスタティックルートを削除します。

文法

ip route destination-ip netmask next-hop [distance]

no ip route {destination-ip netmask next-hop | *}

- destination-ip - 宛先ネットワーク、サブネットワーク、ホストのいずれかの IP アドレス。
- netmask - 関連付けられている IP サブネットのネットワークマスク。このマスクは、個々のサブネットへのルーティングに使用されるホストアドレスビットを示します。
- next hop - ルートで使用されるネクストホップルータの IP アドレス。
- Distance - 管理距離であり、動的ルートの距離が静的ルートについて設定されている距離よりも短い場合は、ルートを動的ルーティング情報によって上書きできることを示します。ただし、動的ユニキャストルーティングプロトコルで使用されるデフォルトの管理距離は、OSPF の場合は 110 であり、RIP の場合は 120 であるという点に注意してください（範囲 : 1 ～ 255、デフォルト : 1）。
- * – スタティックルーティングテーブルのエントリをすべて削除します。

初期設定

スタティックルートは設定されていません。

コマンドモード

Global Configuration

コマンド解説

- 最大 512 の静的ルートを設定することができます。
- 静的ルーティングについては最大 8 つのイコールコストマルチパス（ECMP: Equal-Cost Multipath）を設定することができます（「イコールコストマルチパスルーティング」を参照）。
- 静的ルートの管理距離が設定されており、動的ルートを使用するとより短い管理距離で同じ宛先に到達できる場合は、動的ルートが使用されます。
- 静的パスと動的パスの両方の最低コストが同じ場合は、ルーティングテーブルに保存されている順序が先の方のルートが使用されます（静的に設定されているルートか、ルーティングプロトコルを使用して動的に学習されたルートかは関係ありません）。
- 静的ルート情報は、ルータによって定期的に送信される RIP および OSPF 更新パケットに含まれます（ただし、この機能が RIP または OSPF で有効にされている場合）。

例

デフォルト設定の測定基準 1 を使用して、サブネット 192.168.1.0 のトラフィックをすべてゲートウェイルータ 192.168.5.254 に転送します。

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

maximum-paths

許容範囲のパス数の上限を設定します。コマンドの前に ”no” を置くことにより、デフォルト設定に戻ります。

文法

maximum-paths path-count

no maximum-paths

- path-count - をルーティングテーブルに付加できる同じ宛先への equal-cost パスの上限 (有効範囲 : 1-8)

初期設定

Enabled, 4 paths

コマンドモード

Global Configuration

例

```
switch(config)#maximum-paths 8
switch(config)#
```

show ip host-route

認識されているルートに関連のあるインタフェースを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip host-route
Total count: 0
 IP address                     Mac address       VLAN     Port
 --------------------    --------------------    ------   ------
 192.168. 1.250          00-00-30-01-01-01         3       1/ 1
  10. 2. 48. 2           00-00-30-01-01-02         1       1/ 1
  10. 2. 5. 6            00-00-30-01-01-03         1       1/ 2
  10. 3. 9. 1            00-00-30-01-01-04         2       1/ 3

Console#
```

項目	解説
IP Address	送信先ネットワーク、サブネットワークまたはホストの IP アドレス
MAC アドレス	IP アドレスに対応したフィジカルレイヤアドレス
VLAN	この IP アドレスにつながる VLAN
Port	この IP アドレスにつながるポート

show ip route

ルーティングテーブル内の指定したエントリを表示します。

文法

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

- connected – 現在接続されているエントリをすべて表示します。
- database – アクティブではないルートを含む既知のルート。
- ospf – ルーティングドメインの OSPF プロトコルからインポートしたルータを表示します。
- rip – RIP により学習した すべ て の エ ン ト リ を 表示します。
- static – す べ て の静的 エ ン ト リ を 表示します。
- summary – ルーティングテーブルのエントリのサマリ情報 (サポートされているエントリの最大数、接続先のルータ数、ルーティングテーブルに現在ストアされているルータの総数、FIB のエントリ数を含む) のリストを表示します。

コマンドモード

- Privileged Exec

コマンド解説

- 転送情報ベ ー ス （FIB: Forwarding Information Base）には、IP トラフィックを転送するのに必要な情報が含まれます。それらの情報とは、IP ルーティングテーブルに基づく到達可能な宛先ネットワークのプレフィックスごとのインタフェース ID とネクストホップ情報です。ネットワークでルーティングまたはトポロジの変更が発生すると、ルーティングテーブルが更新され、それらの変更が即座に FIB に反映されます。FIB は、ルーティングピアから受信されたすべてのルーティング情報が保持されるルーティングテーブル（つまり、ルーティング情報ベース（RIB: Routing Information Base））とは個別のものです。FIB には、一意のパスのみが含まれ、セカンダリパスは一切含まれません。FIB エントリは、特定のパケットの転送に関する決定を行うために必要な最小限の情報から設定されています。FIB エントリの代表的な設定要素は、ネットワークプレフィックス、ルータ（VLAN）インタフェース、およびネクストホップ情報です。
- show ip route コマンドを実行した場合には、その時点で転送のためにアクセスできるルートのみが表示されます。ルータはネクストホップに直接到達できなければならないので、動的ルートエントリまたは静的ルートエントリに関連付けられている VLAN は Up 状態でなければなりません。show ip route database コマンドを使用した場合はその時点で転送のためにアクセスできないルートも表示されることがあるので注意してください。

例

以下の例では、RIP のエントリは、ルートの距離および測定基準の両方を表示します。

```
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default
R 10.1.1.0/24 [120/2] via 192.168.1.10, VLAN1, 00:00:14
C 127.0.0.0/8 is directly connected, lo
C 192.168.1.0/24 is directly connected, VLAN1
Console#
```

show ip route database

RIB のエントリを表示します。

コマンドモード

Privileged Exec

コマンド解説

- RIB には、スタティックルートなどの追加で設定されたルート、ダイナミックルーティングプロトコルにより学習したルートがすべて含まれます。RIB には、FIB 用に選択された 最適なエントリからのルートがすべて含まれます（show ip route コマンドの使用方法を参照）。

例

```
Console#show ip route database
Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
> - selected route, * - FIB route, p - stale info
C *> 127.0.0.0/8 is directly connected, lo0
C *> 192.168.1.0/24 is directly connected, VLAN1
Console#
```

show ip route summary

ルーティングテーブルのサマリ情報を表示します。

コマンドモード

Privileged Exec

例

以下の例では、ルーティングテーブルの数の識別子（つまり FIB）は、FIB の ID を表します。

```
Console#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 8
Connected 2
Total 2
Console#
```

show ip traffic

UIP、ICMP、UDP、TCP および ARP プロトコルの解析情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip traffic
IP statistics:
  Rcvd:  5 total, 5 local destination
         0 checksum errors
         0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
         0 fragmented, 0 couldn't fragment
  Sent:  9 generated
         0 no route
ICMP statistics:
  Rcvd:  0 checksum errors, 0 redirects, 0 unreachable, 0 echo
         5 echo reply, 0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp
  Sent:  0 redirects, 0 unreachable, 0 echo, 0 echo reply
         0 mask requests, 0 mask replies, 0 quench, 0 timestamp
         0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd:  0 total, 0 checksum errors, 0 no port
  Sent:  0 total
TCP statistics:
  Rcvd:  0 total, 0 checksum errors
  Sent:  0 total
ARP statistics:
  Rcvd:  0 requests, 1 replies
  Sent:  1 requests, 0 replies
Console#
```

IPv6 Commands

ipv6 route

スタティック IPv6 **ルートを設定します。コマンドの前に** ”no” **を置くことによりスタティックルートを削除します。**

文法

[no] ipv6 route destination-ipv6-address/prefix-length

{gateway-address [distance] |

link-local-address%zone-id [distance] |

tunnel interface-number}

- destination-ipv6-address – **宛先ネットワーク、サブネットワーク、あるいはホストの** IPv6 **アドレス。ネットワークのプレフィックスおよびホストのアドレスのビット数などの完全な** IPv6 **アドレスでなければなりません。**
- prefix-length - **プレフィックス（つまり、アドレスのネットワーク部）を設定するアドレスの（先頭からの）連続ビットの数を示す** 10 **進数（範囲** :0 **〜** 64 **ビット）。**
- gateway-address – **ルートに使用するネクストホップルータの** IP **アドレス。**
- link-local-address%zone-id–zone-id（% **の後ろは** VLAN **識別子を表す）を含む** link-local **アドレス。**
- distance– **管理距離であり、動的ルートの距離が静的ルートについて設定されている距離よりも短い場合は、ルートを動的ルーティング情報によって上書きできることを示します。ただし、動的ユニキャストルーティングプロトコルで使用されるデフォルトの管理距離は、**OSPF **の場合は** 110 **であり、**RIP **の場合は** 120 **であるという点に注意してください（範囲** :1 **〜** 255**、デフォルト** :1**）。**)
- interface-number – **宛先の** IPv6 **アドレスに到達するために使用する出力用トンネルインタフェースの数** (**有効範囲** :1-16)**。詳細については、**interfacetunnel **コマンドを参照ください。**

初期設定

スタティックルートは設定されていません。

コマンドモード

GlobalConfiguration

コマンド解説

- **スタティックルータは** 1K **まで設定可能です。**
- **静的ルーティングについては最大** 8 **つのイコールコストマルチパス（**ECMP: Equal-Cost Multipath**）を設定することができます（「イコールコストマルチパスルーティング」を参照）。**
- **静的ルートの管理距離が設定されており、動的ルートを使用するとより短い管理距離で同じ宛先に到達できる場合は、動的ルートが使用されます。**
- **静的パスと動的パスの両方の最低コストが同じ場合は、ルーティングテーブルに保存されている順序が先の方のルートが使用されます（静的に設定されているルートか、ルーティングプロトコルを使用して動的に学習されたルートかは関係ありません）。**

- 静的ルート情報は、ルータによって定期的に送信される RIP および OSPF 更新パケットに含まれます（ただし、この機能が OSPF3 の redistribute コマンドで有効になっている場合）。

例

以下の例では、デフォルトの設定基準 1 を使って、サブネット 2001::/64 のトラフィックをすべて、ネクストホップルータ 2001:DB8:2222:7272::254 に転送します。

```
Console(config)#ipv6 route 2001::/64 2001:DB8:2222:7272::254
Console(config)#
```

関連するコマンド

show ip route summary (P609)

show ipv6 route

FIB(Forwarding Information Base) の情報を表示します。

文法

show ipv6 route [ipv6-address[/prefix-length] | database |

interface [tunnel tunnel-number | vlan vlan-id] | local | ospf |

rip | static]

- ipv6-address - ネットワークのプレフィックスおよびホストアドレスのビット数を含む完全な IPv6 アドレス。
- prefix-length - プレフィックス（つまり、アドレスのネットワーク部）を設定するアドレスの（先頭からの）連続ビットの数を示す 10 進数。
- database – 非アクティブルータを含む既知のルータすべて。
- interface – インタフェースを介してアクセスされているルータをすべて表示します。
- local – ルータに直接接続されている宛先のエントリをすべて表示します。
- ospf – 外部ルートが OSPF プロトコルからこのルーティングドメインにインポートされるルータを表示します。
- rip – RIP(Routing Information Protocol) を介して学習したエントリをすべて表示します。
- static – スタティックエントリをすべて表示します。
- tunnel-number - トンネルインタフェースの識別子 (有効範囲 : 1-16)
- vlan-id - VLAN ID (有効範囲 : 1-4093)

コマンドモード

Privileged Exec

コマンド解説

- 転送情報ベース（FIB: Forwarding Information Base）には、IP トラフィックを転送するのに必要な情報が含まれます。それらの情報とは、IP ルーティングテーブルに基づく到達可能な宛先ネットワークのプレフィックスごとのインタフェース ID とネクストホップ情報です。ネットワークでルーティングまたはトポロジの変更が発生すると、ルーティングテーブルが更新され、それらの変更が即座に FIB に反映されます。FIB は、ルーティングピアから受信されたすべてのルーティング情報が保持されるルーティングテーブル（つまり、ルーティング情報ベース（RIB: Routing Information Base））とは個別のものです。FIB には、一意のパスのみが含まれ、セカンダリパスは一切含まれません。FIB エントリは、特定のパケットの転送に関する決定を行うために必要な最小限の情報から設定されています。FIB エントリの代表的な設定要素は、ネットワークプレフィックス、ルータ（VLAN）インタフェース、およびネクストホップ情報です。
- 転送のためにアクセスできるルートのみが表示されます。ルータはネクストホップに直接到達できなければならないので、動的ルートエントリまたは静的ルートエントリに関連付けられている VLAN は動作状態でなければなりません。

例

以下の例では、最後のエントリは、ルートの距離および測定基準の両方を表示します。

```
Console#show ipv6 route
Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
C ::1/128, lo0
? FE80::/64, VLAN1 inactive
C FE80::/64, VLAN1
? FF00::/8, VLAN1 inactive
O IA 3FFF:1::/32 [110/3]
via FE80::204:FF:FE05:6, VLAN1
Console#
```

1.29.2 RIP

コマンド	機能	モード	ページ
router rip	RIP ルーティングプロトコルを有効化	GC	P616
default-metric	デフォルトメトリックを設定	RC	P617
timers basic	基本タイマーを設定	RC	P618
network	RIP ルーティングに使用されるネットワークインタフェースを指定	RC	P619
neighbor	情報を交換する、隣接ルータを設定	RC	P620
version	RIP バージョンを設定	RC	P620
redistribute	１つのドメインからのルート再配布	RC	P621
ip rip receive version	RIP レシーババージョンの設定	IC	P622
ip rip send version	RIP センドバージョンの設定	IC	P623
ip split-horizon	Split Horizon または Poison Reverse の有効化	IC	P624
ip rip authentication key	RIPv2 パケット認証の有効化および、パスワードを設定	IC	P624
ip rip authentication mode	RIPv2 パケット認証のタイプを指定	IC	P625
show rip globals	グローバル設定および RIP 統計情報の表示	PE	P626
show ip rip	各ネットワークインタフェースごとの、RIP 設定情報の表示	PE	P626

router rip

全ての IP インタフェースで RIP ルーティングを有効にします。コマンドの前に "no" を置くことで、無効にします。

文法

router rip
no router rip

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- RIP **はルータが経路情報を交換する方法を設定するのに使用されます。**
- **本コマンドはルータコンフィグレーションモードへの移行にも使用します。**

例

```
Console(config)#router rip
Console(config-router)#
```

関連するコマンド

network （P619）

default-metric

デフォルトメトリック値を設定します。コマンドの前に "no" を置くことで、初期設定値に戻ります。

文法

default-metric metric-value

no default-metric

- metric-value — 外部ルータにアサインされたメトリック値（範囲：0-15）

初期設定

8

コマンドモード

Privileged Exec

コマンド解説

- 静的な経路情報の再分配のメトリックが設定されていない場合、default-metric コマンド（P617）により、読み込むすべての外部経路情報に使用するメトリック値を設定します。
- 経路のメトリックは、互換性のないメトリックを含む外部の経路情報を再分配するという問題を解決するために使用されなくてはなりません。
- ルーティング・プロトコルから RIP へ経路情報を再分配する場合、小さなメトリックを使用することを推奨します。大きなメトリックを設定すると、RIP への外部経路情報の再分配の実用性が制限されてしまいます。例えば、経路情報の再分配にメトリック 10 を設定した場合、これらの経路情報は 5 ホップ先のルータまで（ここでメトリックが最大のホップ数 15 を超過するため）しかアドバタイズされません。小さなメトリック 1 を設定することにより、RIP のドメイン内で許可された最大のホップ数で読み込まれた経路で通信することができます。しかし、小さいメトリックを採用した場合、経路でループが発生する可能性が高くなります。たとえば、複数の再分配箇所があり、ルータが同じ外部ネットワークについて、元のソースからではなく再分配ポイントから、より良いメトリックを学習するようなケースが発生します。

例

本例ではデフォルトメトリック値を「5」に設定しています。

```
Console(config-router)#default-metric 5
Console(config-router)#
```

関連するコマンド

redistribute（P621）

timers basic

RIP アップデートタイマー、タイムアウトタイマーおよび Garbage コレクションタイマーの設定を行います。コマンドの前に "no" を置くことで、初期設定値に戻します。

文法

timers basic update-seconds
no timers basic

- update-seconds — アップデート情報の送信頻度送信頻度を設定します。この値を 6 倍した値がタイムアウト時間として、4 倍した値がガベージコレクション時間として設定されます。（範囲：15-60 秒）

初期設定

Update: 30 秒

Timeout: 180 秒

Garbage collection: 120 秒

コマンドモード

Router Configuration

コマンド解説

- アップデートタイマーはすべての基本的な RIP プロセスを制御するのに使用される、重要なタイマーです。
- アップデートタイマーの間隔を短くしすぎると、ルータがアップデートの処理に膨大な時間を費やすことになります。一方、長くしすぎるとネットワーク構成の変更を検出しにくいルーティングプロトコルになってしまいます。
- アップデートタイマーは、同一ネットワークのすべてのルータに同じ値を設定しなくてはなりません。

例

```
Console(config-router)#timers basic 15
Console(config-router)#
```

network

RIP ルーティングプロセスに含まれる、ネットワークインタフェースを指定します。コマンドの前に "no" を置くことでエントリを削除します。

文法

network subnet-address
no network subnet-address

- subnet-address — サブネットの IP アドレス

初期設定

ネットワークは指定されていません。

コマンドモード

Router Configuration

コマンド解説

- このコマンドで設定したインタフェースにのみ RIP のアップデート情報が送信されます
- サブネットアドレスは、設定したアドレスの最初のフィールドに基付き、クラス A、B、C のいずれかに解釈されます。つまり、サブネットアドレス nnn.xxx.xxx.xxx を入力した場合、最初のフィールド（nnn）がクラスを決定します。
  - 0 ～ 127 の場合クラス A となり、ネットワークアドレスの最初のフィールドのみ使用されます。
  - 128 ～ 191 の場合はクラス B となり、ネットワークアドレスの最初から 2 つのフィールドのみ使用されます。
  - 192 ～ 223 の場合はクラス C となり、ネットワークアドレスの最初から 3 つのフィールドのみ使用されます。

例

本例では 10.1.0.0 のネットワークインタフェースを RIP のルーティングプロセスに組み込みます。

```
Console(config-router)#network 10.1.0.0
Console(config-rou
```

neighbor

隣接ルータを設定します。コマンドの前に "no" **を置くことでエントリを削除します。**

文法

neighbor ip-address

no neighbor ip-address

- ip-address — MAC **アドレスにマップされた** IP **アドレス**

初期設定

隣接ルータは設定されていません。

コマンドモード

Router Configuration

例

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

version

ルータでグローバルに使用される RIP **バージョンを指定します。コマンドの前に** "no" **を置くことで初期設定値に戻します。**

文法

version {1 | 2}

no version

- 1 — RIP **バージョン** 1
- 2 — RIP **バージョン** 2

初期設定

RIP **バージョン** 1

コマンドモード

Router Configuration

例

```
Console(config-router)#version 2
Console(config-router)#
```

redistribute

経路情報の再分配を設定します。コマンドの前に "no" **を置くことでこの機能を無効にします。**

文法

redistribute (static} [metric <metric-value>]

no redistribute (static} [metric <metric-value>]

- static — **スタティックルート**
- metric-value — **メトリック値（範囲：**1-15**）**

初期設定

再分配：無効

メトリック値："default-metric" **コマンドで設定された値**

コマンドモード

Router Configuration

コマンド解説

- **静的な経路情報の再分配のメトリックが設定されていない場合、**default-metric **コマンド（**P613**）により、読み込むすべての外部経路情報に使用するメトリック値を設定します。**
- **経路のメトリックは、互換性のないメトリックを含む外部の経路情報を再分配するという問題を解決するために使用されなくてはなりません。**
- **他のプロトコルから** RIP **へ経路情報を再分配する場合、小さなメトリックを使用することを推奨します。大きなメトリックを設定すると、**RIP **への外部経路情報の再分配の実用性が制限されてしまいます。例えば、経路情報の再分配にメトリック** 10 **を設定した場合、これらの経路情報は** 5 **ホップ先のルータまで（ここでメトリックが最大のホップ数** 15 **を超過するため）しかアドバタイズされません。小さなメトリック** 1 **を設定することにより、**RIP **のドメイン内で許可された最大のホップ数で読み込まれた経路で通信することができます。しかし、小さいメトリックを採用した場合、経路でループが発生する可能性が高くなります。たとえば、複数の再分配箇所があり、ルータが同じ外部ネットワークについて、元のソースからではなく再分配ポイントから、より良いメトリックを学習するようなケースが発生します。**

例

本例では静的な経路情報を再分配し、これらの経路のメトリック値をすべて 3 **に設定しています。**

```
Console(config-router)#redistribute static metric 3
Console(config-router)#
```

ip rip receive version

RIP ルーティングプロセスに組み込む各インタフェースに対し、受信に使用するプロトコルメッセージの種類（RIP のバージョン）を設定します。コマンドの前に "no" を置くことで初期設定値に戻します。

文法

ip rip receive version [none | 1 | 2 | 1 2]

no ip rip receive version

- 1 — RIP v 1 パケットのみ許可
- 2 — RIP v 2 パケットのみ許可

初期設定

Global RIPv1 - RIPv1 or RIPv2 packets

Global RIPv2 - RIPv2 packets

コマンドモード

Router Configuration

コマンド解説

- Receive Version は次の選択肢から設定できます。
  - ローカルネットワークですべてのルータが RIPv1 または RIPv2 のどちらか一方だけを使用している場合は、それぞれ "RIPv1" または "RIPv2" を設定します。
  - ローカルネットワークでルータが RIPv1 と RIPv2 の両方を使用している場合は、"RIPv1 or RIPv2" を設定します。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

ip rip send version

RIP ルーティングプロセスに組み込む各インタフェースに対し、送信に使用するプロトコルメッセージの種類（RIP のバージョン）を設定します。コマンドの前に "no" を置くことで初期設定値に戻します。

文法

ip rip send version [none | 1 | 2 | v2-broadcast]

no ip rip send version

- 1 — RIP v 1 パケットのみ許可。
- 2 — RIP v 2 パケットのみ許可。
- 1-compatible - ルート情報を RIPv2 をもつ他のルータへブロードキャスト

初期設定

Global RIPv1 - ルート情報は、他の RIPv2 ルータへブロードキャストします。

Global RIPv2 - RIPv2 パケットのみ許可

コマンドモード

Router Configuration

コマンド解説

- Send Version は次の 3 つの選択肢から設定できます
  - ローカルネットワークのすべてのルータが RIPv1 または RIPv2 のどちらか一方だけを使用している場合は、それぞれ "RIPv1" または "RIPv2" を設定します。
  - ネットワークの他のルータに経路情報をブロードキャストする際、RIPv2 で通常要求されるマルチキャストではなく、RIPv2 のアドバタイズリストを使用する場合は "RIPv1 Compatible" を設定します。（このモードを使用すると、RIPv1 のルータはプロトコルメッセージを受信でき、RIPv2 のルータは RIPv2 で提供される追加情報（サブネットマスク、ネクストホップ、および認証情報）を受信できます。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

関連するコマンド

redistribute（P621）

ip split-horizon

スプリットホライズン（経路情報を送信してきたインタフェースポートには経路情報をアドバタイズしない）を有効にします。コマンドの前に "no" **を置くことで無効にします。**

文法

ip split-horizon [poison-reverse]
no ip split-horizon

- poison-reverse — **その経路情報を送信してきたインタフェースポートに経路情報をアドバタイズするが、距離ベクトル型のメトリックは無限大に設定します。（これにより収束時間を短縮できます）**

初期設定

split-horizon

コマンドモード

Interface Configuration(VLAN)

例

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

ip rip authentication key

インタフェースに RIPv2 **パケット認証を有効化および認証キーを指定します。コマンドの前に** "no" **を置くことで認証を無効にします。**

文法

ip rip authentication key key-string

no ip rip authentication

- key-string — **認証に使用されるパスワード（範囲：**1-16 **文字）**

初期設定

無効

コマンドモード

Interface Configuration（VLAN）

例

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication string small
Console(config-if)#
```

関連するコマンド

ip rip authentication mode（P625）

ip rip authentication mode

インタフェースに認証タイプを設定します。コマンドの前に "no" **を置くことで初期設定値に戻します。**

[**注意**] **現在のファームウェアバージョンでは、シンプルパスワードのみサポートしています。**

文法

ip rip authentication mode {md5 | text}
no ip rip authentication mode

- md5 -- md5 **で暗号化する。**
- text — **シンプルパスワードを指定**

初期設定

認証無し

コマンドモード

Interface Configuration（VLAN）

コマンド解説

- **本コマンドは、動的学習ルートのみ削除を行います。**
- "no ip address" **コマンドはローカルインタフェースを削除するために使用します。**
- "no ip route" **コマンドはスタティックルートを削除するために使用します。**

例

```
Console(config)#interface vlan 1
Console(config-if)#no ip address
```

関連するコマンド

ip rip authentication key（P624）

show ip rip

RIP インタフェース設定情報を表示します。

文法

show ip rip {configuration | status | peer}

- Interface - インタフェースごとの RIP 設定を表示します。
  - vlan-id - VLAN ID(有効範囲 : 1-4093)

初期設定

認証無し

コマンドモード

Privileged Exec

例

```
Console#show ip rip
Codes: R - RIP, Rc - RIP connected, Rs - RIP static,
       C - Connected, S - Static, O - OSPF

   Network Next Hop    Metric From         Interface Time
Rc 192.168.0.0/24       1                   VLAN1     01:57
Console#show ip rip interface vlan 1
Interface: vlan1
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 Compatible
    Passive interface: Disabled
    Authentication mode: (None)
    Authentication string: (None)
    Split horizon: Enabled with Poisoned Reverse
    IP interface address: 192.168.0.2/24
Console#
```

1.30 Open Shortest Path First (OSPFv2)

コマンド	機能	モード	ページ
General Configuration			
router ospf	OSPF を有効または無効にします。	GC	P629
router-id	このデバイスのルータ ID を設定します。	RC	P630
compatible rfc1583	RFC 1583 (OSPFv1) を使用して、サマリー ルートのコストを計算します。	RC	P631
default-information originate	自律システム（Autonomous System; AS）へのデフォルトの外部ルートを生成します。	RC	P632
timers spf	連続する SPF 計算間のホールド タイムを構成します。	RC	P633
clear ip ospf process	OSPF ルーティングプロセスのクリアおよびリスタートを行います。	PE	P634
Route Metric and Summaries			
area range	ABR によってアドバタイズされるルートを要約します。	RC	P635
auto-cost referencebandwidth	帯域幅に応じて、インタフェースのデフォルトのメトリックを算出します。	RC	P636
default-metric	その他のプロトコルからインポートした外部ルートのデフォルトのメトリックを設定します。	RC	P637
summary-address	ASBR によってアドバタイズされるルートを要約します。	RC	P639
redistribute	1 つのルーティング ドメインから別のルーティング ドメインへルートを再配布します。	RC	P640
Area Configuration			
network area	指定したインタフェースを特定のエリアに割り当てます。	RC	P642
area stub	LSA を送信または受信できないスタブ エリアを設定します。	RC	P643
area nssa	外部ルートをインポートできる、準スタブ エリアを設定します。	RC	P644
area virtual-link	エリア境界ルータからバックボーンへの仮想リンクを設定します。	RC	P646
Interface Configuration			
ip ospf authentication	インタフェースの認証タイプを指定します。	IC	P649
ip ospf authentication-key	隣接ルータによって使用されるシンプル パスワードを割り当てます。	IC	P650
ip ospf message-digest-key	MD5 認証を有効にし、インタフェース用のキーを設定します。	IC	P651
ip ospf cost	インタフェース上でのパケット送信コストを指定します。	IC	P652
ip ospf dead-interval	Hello パケットが受信されないまま時間が経過すると、隣接ルータによってルータのダウンが宣言されるまでの間隔を設定します。	IC	P653
ip ospf hello-interval	Hello パケットの送信頻度を指定します。	IC	P654
ip ospf priority	指定ルータの決定に使用されるルータ プライオリティを設定します。	IC	P655
ip ospf retransmit-interval	リンクステート アドバタイズメント（LSA）を再送信する間隔を指定します。	IC	P656
ip ospf transmit-delay	インタフェースでリンクステート アップデート パケットを送信するまでの時間を予測します。	IC	P658
Display Information			

show ip ospf	ルーティング プロセスに関する一般情報を表示します。	PE	P659
show ip ospf border-routers	エリア境界ルータ（Area Border Router; ABR）および自律システム境界ルータ（Autonomous SystemBoundaryRouter; ASBR）のルーティング テーブル エントリを表示します。	PE	P661
show ip ospf database	データベース内の各種 LSA に関する情報を表示します。	PE	P662
show ip ospf interface	インタフェース情報を表示します。	PE	P669
show ip ospf neighbor	隣接ルータ情報を表示します。	PE	P670
show ip ospf route	OSPF ルーティングテーブルを表示します。	PE	P671
show ip ospf virtual-links	仮想リンクのパラメータと隣接状態を表示します。	PE	P672
show ip protocols ospf	OSPF プロセスのパラメータを表示します。	PE	P673

router ospf

スイッチ上のすべての IP **インタフェースで** Open Shortest Path First(OSPF) **を有効にします。コマンドの前に** "no" **を置くことで、無効になります。**

文法

[no] router ospf [process-id]

- process-id - **複数のルーティングインスタンスを設定する際に入力するプロセス** ID (**有効範囲** : 1-65535; **デフォルト設定** : 1)

コマンド モード

Global Configuration

初期設定

無効

コマンド解説

- OSPF **は、ルータがルーティング テーブル情報を交換する方法を指定するのに使用されます。**
- **このコマンドを使用しても、ルータ設定モードに入ることができます。**
- **プロセス** ID **が設定されていない場合、デフォルト設定はインスタンス** 1 **です。**

例

```
Console(config)#router ospf
Console(config-router)#
```

関連するコマンド

network area （P642）

router-id

自律システム内のこのデバイスに対して一意のルータ ID を割り当てます。コマンドの前に "no" を置くことで、デフォルトのルータ識別方式（最も小さいインタフェース アドレス）が使用されます。

文法

router-id ip-address

no router-id

- ip-address— IP アドレスと同じ形式でルータ ID を指定します。

コマンドモード

Router Configuration

初期設定

最も小さいインタフェース アドレス

コマンド解説

- ルータ ID は、自律システム内のすべてのルータに対して一意である必要があります。最も小さいインタフェース アドレスに基づくデフォルト設定を使用することで、各ルータ ID が一意であることを保証できます。また、ルータ ID は 0.0.0.0 または 255.255.255.255 には設定できないことに注意してください。
- このルータが、すでに隣接ルータを登録している場合、ルータのリブート時または norouter ospf の後に router ospf コマンドを入力して手動で再起動した時、新規のルータ ID が使用されます。
- あるエリアに対する指定ルータまたはバックアップ指定ルータの候補となるルータのプライオリティ値が等しい場合、最も大きい ID を持つルータが選出されます。

例

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

関連するコマンド

router ospf（P629）

compatible rfc1583

RFC 1583 (OSPFv1) を使用して、サマリー ルートのコストを計算します。コマンドの前に "no" を置くことで、RFC 2328 (OSPFv2) を使用してコストを計算します。

文法

[no] compatible rfc1583

コマンドモード

Router Configuration

初期設定

RFC 1583 互換

コマンド解説

- OSPF ルーティングドメイン内のすべてのルータは、サマリールートの計算に同じ RFC を使用する必要があります。
- RFC1583 互換モードが有効になっている場合、同じ宛先をアドバタイズする複数の AS 外部 LSA ルートから 1 つを選択するときにはコストのみが使用されます。無効になっている場合、優先順位はパスのタイプに基づいて決まり、コストは順位が同じ場合にのみ使用されます（RFC2328 を参照）。
- サマリ情報を交換するエリア内に OSPFv2（RFC2328）にアップグレードされていない OSPF ルータ（特に、ABR）がある場合は、依然として古い OSPFv2 コードを実行しているルータとの互換性を確保するため、アップグレードされている OSPFv2 ルータで RFC1583 を使用しなければなりません。

例

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```

default-information originate

自律システム（Autonomous System; AS）へのデフォルトの外部ルートを生成します。コマンドの前に "no" を置くことで、この機能は無効になります。

文法

default-information originate [always] [metric interface-metric] [metric-type metric-type]

no default-information originate

- always — ルータにデフォルト ルートがあるかどうかに関わらず、ローカル AS に対して常にデフォルト ルートをアドバタイズします。
  （P604 「ip route」の「ip route」を参照）
- interface-metric — デフォルト ルートに割り当てられるメトリックです
  （範囲 : 1 〜 65535、デフォルト : 10）
- metric-type — デフォルト ルートのアドバタイズに使用される外部リンクのタイプです
  （オプション : Type 1、Type 2、デフォルト : Type 2）

コマンドモード

Router Configuration

初期設定

無効

コマンド解説

- デフォルトの外部ルートに対するメトリックは、ASBR から出て AS 内の他のルータを通過するトラフィックのパス コストを算出するのに使用されます。
- このコマンドを使用してルーティング ドメイン（すなわち自律システム ; AS）へルートを再配布すると、このルータは自動的に自律システム境界ルータ（ASBR）になります。ただし、デフォルトでは、ASBR は、ルーティング ドメインへのデフォルトルートを生成しません。
  - always キーワードを使用すると、ルータは、デフォルトの外部ルートが実際には存在しない場合でも、自身を AS へのデフォルト外部ルートとしてアドバタイズします（デフォルト ルートを設定するには、ip route コマンドを使用します）。
  - always キーワードを使用しないと、ルータが AS へのデフォルト外部ルートとしてアドバタイズできるのは、redistribute コマンドにより、RIP またはスタティック ルーティングを介して外部ルートがインポートされており、このようなルートが既知である場合のみです。
- タイプ 1 ルート アドバタイズメントでは、外部ルート メトリックに内部コストを追加します。タイプ 2 ルートは、内部コスト メトリックを追加しません。タイプ 2 ルートを比較する時、複数のタイプ 2 ルートが同じコストを持っている場合、内部コストはタイブレーカーとしてのみ使用されます。

例

この例では、自律システムにアドバタイズされるデフォルト外部ルートにメトリック 20 を割り当て、これをタイプ 2 外部メトリックとして送信します。

```
Console(config-router)#default-information originate metric 20
metric-type 2
Console(config-router)#
```

関連するコマンド

ip route（P604）
redistribute（P621）

timers spf

連続する 2 つの SPF （最短パス優先）計算のホールド タイムを構成します。コマンドの前に "no" を置くことで、設定を初期値に戻します。

文法

timers spf spf-delay spf-holdtime

no timers spf

- spf-delay - **トポロジーの変更通知を受信してから SPF 計算を開始する迄の遅延時間 (有効範囲 : 0-2147483647 秒)**
- spf-holdtime — **連続する 2 つの SPF 計算の最小間隔です（範囲 : 0 〜 65535 秒）。**

コマンドモード

Router Configuration

初期設定

10 **秒**

コマンド解説

- SPF **ホールドタイムを 0 に設定すると、連続する計算間に遅延がまったくないことになります。**
- **値を小さくすると、ルータは高速に新規パスをスイッチングできますが、CPU 処理時間がより長くかかります。**

例

```
Console(config-router)#timers spf 20
Console(config-router)#
```

clear ip ospf process

OSPF ルーティングプロセスのクリアおよびリスタートを行います。プロセス ID を指定すると、特定の OSPF プロセスがクリアになります。プロセス ID を指定しない場合は、このコマンドにより、現在動作している OSPF プロセスはすべてクリアになります。

文法

clear ip ospf [process-id] process

- process-id - ルーティングプロセス ID を指定します (有効範囲 : 1-65535)。

初期設定

ルーティングプロセスをすべてクリアにします。

コマンド設定

Privileged Exec

例

```
Console#clear ip ospf process
Console#
```

area range

エリア境界ルータ（ABR）によってアドバタイズされるルートを要約します。コマンドの前に "no" を置くことで、この機能は無効になります。

構文

[no] area area-id range ip-address netmask [advertise | not-advertise]

- area-id — **ルートを要約するエリアを識別します（エリア ID は、IP アドレスと同じ形式である必要があります）**
- ip-address — **要約するルートのベース アドレスです**
- netmask — **サマリー ルートのネットワーク マスクです**
- advertise — **指定されたアドレス範囲をアドバタイズします**
- not-advertise — **サマリーは送信されず、ルートは残りのネットワークから隠されたままです**

コマンドモード

Router Configuration

初期設定

無効

コマンド解説

- **このコマンドは、エリア間ルートをアドバタイズするのに使用されます。**
- **ルートがアドバタイズされるよう設定されている場合、ルータは、このコマンドで指定された各アドレス範囲に対して、タイプ 3 サマリー LSA を発行します。**
- **このルータは、各エリア範囲につき最大 64 のサマリー ルートをサポートします。**

例

この例では、10.2.x.x の範囲内にあるすべてのエリア ルートのサマリー アドレスを作成します。

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0
advertise
Console(config-router)#
```

auto-cost referencebandwidth

帯域幅に応じて、インタフェースのデフォルトのメトリックを算出します。コマンドの前に ”no” を置くことにより、インタフェスのタイプに応じてコストを自動的に割り当てます。

文法

auto-cost reference-bandwidth reference-value

no auto-cost reference-bandwidth

- reference-value - インタフェースの帯域幅 (有効範囲 : 1-4294967 Mbps)

コマンドモード

Router Configuration

初期設定

1 Mbps

コマンド解説

- 基準帯域幅をインターフェース帯域幅で割ってインターフェースのコストが計算されます。基準帯域幅は、Mbits/ 秒単位で設定されます（範囲 :1 〜 4,294,967）。デフォルトでは、すべてのポートタイプのコストは 1Mbps（100Mbps/1Gigabit/10Gigabit ポートを含む)
- アグリゲーションリンクについては、基準帯域幅の値を大きくして、コストの低いリンクとして優先的に使用されるようにすることができます。
- ip ospf cost コマンドにより、autocost reference-bandwidth コマンドにより算出したコストを上書きします。

例

この例では、参照する値を「10000」に設定します（この場合、100Mbps ポートのコストに対しては「100」、1Gbps ポートのコストに対しては「10」、10Gbps ポートのコストに対しては「1」）

```
Console(config-router)#auto-cost reference-bandwidth 10000
Console(config-router)#
```

関連コマンド

ip ospf cost (P652)

default-metric

その他のプロトコルからインポートした外部ルートのデフォルトのメトリックを設定します。コマンドの前に ”no” **を置くことにより、サポートしているプロトコルタイプのデフォルトのメトリックを削除します。**

文法

default-metric metric-value

no default-metric

- metric-value – **他のプロトコルからインポートされた外部ルート全てに割り当てられたメトリック** (**有効範囲** : 0-16777214)

コマンドモード

Router Configuration

初期設定

20

コマンド解説

- **デフォルトメトリックは、互換性のないメトリックを使用している他のプロトコルか ら学習した外部ルートの再配信の問題を解決するために使用する必要があります。**
- redistribute **コマンドにより設定されたメトリックの値はこのコマンドにより上書きされません。メトリックの値が** redistribute **コマンドでは設定されていない場合は、インポートした外部ルートすべてに使用するメトリックの値は** default-metric **コマンドより設定されます。**

例

```
Console(config-router)#default-metric 100
Console(config-router)#
```

関連コマンド

redistribute(P684)

area default-cost

エリア境界ルータ（ABR）からスタッブ エリアまたは準スタブ エリア（not-so-stubby area ; NSSA**）へ送信されるデフォルト サマリー ルートのコストを指定します。コマンドの前に** "no" **を置くことで、割り当てられたデフォルト コストが削除されます。**

文法

area area-id default-cost cost

no area area-id default-cost

- area-id — **スタブまたは** NSSA **の識別子です。**IP **アドレスと同じ形式である必要があります（エリア** ID **は、**IPv4 **アドレスの形式、または** 4 **バイトの符号なし整数** (0-4294967295))
- cost — **スタブまたは** NSSA **へ送信されるデフォルト サマリー ルートのコストです。（範囲：**0-1677215**）**

コマンドモード

Router Configuration

初期設定

1

コマンド解説

- **デフォルト コストが「**0**」に設定されている場合、ルータは、接続されたスタブまたは** NSSA **に対してデフォルト ルートをアドバタイズしません。**

例

```
Console(config-router)#area 10.3.9.0 default-cost 10
Console(config-router)#
```

関連するコマンド

area stub（P685）

summary-address

他のプロトコルから学習したルートを集約します。コマンドの前に "no" **を置くことで、サマリー アドレスが削除されます。**

文法

[no] summary-address summary-address netmask

- summary-address— **アドレス範囲をカバーするサマリー アドレスです**
- netmask— **サマリー ルートのネットワーク マスクです**

コマンドモード

Router Configuration

初期設定

無効

コマンド解説

- **他のプロトコルのルート情報を** OSPF **エリアに再配信する場合、通常は、直前のセクションで説明したように、ルータが外部** LSA **によって各ルートを個別にアドバタイズする必要があります。それらの外部ルート情報の再配信に必要なプロトコルメッセージの数を減らすため、代わりに、他のプロトコルから学習したルートを接続先のすべての** AS **に再配信するように** ASBR **を設定することができます。**

例

この例では、192.168.x.x **の範囲内に含まれるすべてのルートのサマリー アドレスを作成します。**

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

関連するコマンド

area range(P635)

redistribute(P621)

redistribute

他のルーティング ドメイン（プロトコル）から自律システムに外部ルーティング情報をインポートします。コマンドの前に "no" **を置くことで、この機能は無効になります。**

文法

redistribute {connected | rip | static} [metric metric-value] [metric-type type-value] [tag tag-value]

no redistribute {connected | rip | static} [metric] [metric-type] [tag]

- connected - **現在さ津属されているエントリをすべてインポートします。**
- rip — **ルーティング情報プロトコル（**RIP**）からこの自律システム（**AS**）へ、外部ルートをインポートします。**
- static — **この自律システムへスタティック ルートをインポートします。**
- metric-value —**指定したプロトコルのすべての外部ルートに割り当てられるメトリックです（範囲** : 1 **〜** 65535**、デフォルト** : 10**）。**
- type-value— 1 - **タイプ** 1 **外部ルート、** 2 - **タイプ** 2 **外部ルート（デフォルト）**
- tag-value - **特定の外部ルーティングドメインを識別したり、ルータ間の追加情報を通過させるために** AS-external LSA **に付けられているタグ** (**有効範囲** : 0-4294967295)**。**

コマンドモード

Router Configuration

初期設定

再配布 - **なし**

プロトコル - RIP **およびスタティック**

メトリック値 - 0

タイプ メトリック - 2

コマンド解説

- **このルータでは、**RIP **およびスタティック両方のルートの再配布をサポートしています。**
- OSPF **自律システム（**AS**）に外部ルートを再配布すると、ルータは自動的に自律システム境界ルータ（**ASBR**）になります。**redistribute **コマンドを** default-informationoriginate **コマンドと組み合わせて使用することにより** AS **への「デフォルト」外部ルートを生成した場合、このコマンドで指定されたメトリック値は、**default-information originate **コマンドで指定されたメトリックを上書きします。**
- **メトリック タイプは、外部** LSA **を介して、**AS **外部の宛先へのルートをアドバタイズする方法を指定します。外部ルート メトリックに内部コスト メトリックを追加するには、タイプ** 1 **を指定します。すなわち、**AS **内の任意のルータのルートのコストは、アドバタイジング** ASBR **への到達コストと、外部ルートのコストを加えたものに等しいことになります。外部ルート メトリックのみをアドバタイズするには、タイプ** 2 **を指定します。**
- **タグは、別の外部** AS**（他のルーティングプロトコル）から学習した個々のルートを区別するために使用することができます。例えば、ルーティングドメインに** 2 **つの** ASBR**、**A **と** B **があるとします。**ASBR A **は** RIP **ドメイン** 1**（**Tag 1 **によって識別）か**

ら学習したルートを再配信するように設定し、ASBR B は RIP ドメイン 2（Tag 2 によって識別）から学習したルートを再配信するように設定することができます。

例

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

関連するコマンド

default-information originate（P632）

network area

このエリア内で動作する OSPF エリアとインタフェースを設定します。コマンドの前に "no" を置くことで、指定インタフェースの OSPF は無効になります。

文法

[no] network ip-address netmask area area-id

- ip-address — エリアに追加するインタフェースのアドレス
- netmask — エリアに追加するアドレス範囲のネットワーク マスク
- area-id— 指定アドレスまたは範囲が割り当てられるエリア。OSPF エリアは、共通のルーティング情報を共有するルータのグループを識別します（エリア ID は、IP アドレスと同じ形式である必要があります）

コマンドモード

Router Configuration

初期設定

無効

コマンド解説

- エリア ID は、OSPF ブロードキャスト エリアを一意に設定するものです。エリア ID0.0.0.0 は、自律システムの OSPF バックボーンを示します。各ルータは、直接接続または仮想リンクを介してバックボーンに接続されている必要があります。
- 1 つまたは複数のインタフェースをエリアに追加するには、ネットワーク マスクを使用して、ネットワーク セグメント上のすべてのルータのエリア ID を同じ値に設定します。
- ネットワーク エリア内に存在するインタフェースのプライマリ アドレスを確実に含めるようにします。そうしないと、OSPF は、このコマンドでカバーされるセカンダリ アドレスに対して動作しません。
- インタフェースは、1 つのエリアにのみ割り当てることができます。その後のネットワーク エリア コマンドによりアドレス範囲が重複して指定された場合、ルータは、最初のコマンドで指定されたエリアのアドレス範囲を実装し、後のコマンドで重複したエリアを無視します。ただし、より特定性の高いアドレス範囲をエリアから削除すると、このエリアをカバーする特定性の低いアドレスが指定された場合に、この範囲に属するインタフェースがアクティブのままになります。
- このルータは、最大 64 の OSPF ルータ インタフェースと、最大 16 のエリア（ノーマル トランジット エリア、スタブ、または NSSA のいずれかの合計）をサポートします。

例

この例では、クラス B アドレス 10.1.x.x をカバーするバックボーン 0.0.0.0、およびクラス C アドレス 10.2.9.x をカバーするノーマル トランジット エリア 10.2.9.0 を作成します。

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area
10.1.0.0
Console(config-router)#
```

area stub

スタブ エリアを設定します。スタブを削除するには、オプション キーワードを指定せずに no 形式を使用します。サマリー属性を削除するには、サマリー キーワードを指定せずに no 形式を使用します。

文法

[no] area area-id stub [summary]

- area-id - スタブ エリアの識別子です
  （エリア ID は、IP アドレスと同じ形式である必要があります）。
- summary - エリア境界ルータ（ABR）は、スタブ エリアにサマリー リンク アドバタイズメントを送信します（デフォルト : no summary）。

コマンドモード

Router Configuration

初期設定

スタブは構成されていません。

コマンド解説

- スタブ内のすべてのルータは、同じエリア ID で構成されている必要があります。
- ルーティング テーブル スペースは、タイプ 4 AS サマリー LSA およびタイプ 5 外部 LSA をブロックすることにより、スタブ内に保存されます。このコマンドのデフォルト設定では、ローカル エリアまたは自律システム外部の宛先へのデフォルト ルートをアドバタイズするタイプ 3 サマリー LSA をブロックすることにより、スタブを完全に分離します。
- ABR によってスタブへ送信されるデフォルト サマリー ルートのコストを指定するには、area default-cost コマンドを使用します。
- このルータは、最大 16 のエリア（ ノーマル トランジット エリア、スタブ、または NSSA のいずれかの合計）をサポートします。

例

この例では、スタブ エリア 10.2.0.0 を作成し、クラス B アドレス 10.2.x.x を持つインターフェースをすべてスタブに割り当てます。

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area
10.2.0.0
Console(config-router)#
```

関連するコマンド

area default-cost（P638）

area nssa

準スタブ エリア（NSSA）を設定します。NSSA を削除するには、オプション キーワードを指定せずに コマンドの前に "no" を置きます。オプション属性を削除するには、関連するキーワードを指定せずにコマンドの前に "no" を置きます。

文法

[no] area area-id nssa

[translator-role [candidate | never | always]] |

[no-redistribution] | [no-summary] | [default-informationoriginate

[metric metric-value | metric-type type-value]]

- area-id - NSSA **の識別子です（エリア** ID **は、**IP **アドレスと同じ形式である必要があります）。**
- translator-role - **タイプ** 5 external LSA **の** NSSA-ABR **変換を行います。**
  - candidate - **選択されている場合は、ルータにより** NSSA LSA **から** Type-5 external LSA **への変換を行います。**
  - never - **ルータにより** NSSA LSA **から** Type-5 external LSA **への変換を行いません。**
  - always - **ルータにより** NSSA LSA **から** Type-5 external LSA **への変換を行います。**
- no-redistribution - **ルータが** NSSA **のエリア境界ルータ（**ABR**）であり、なおかつ** redistribute **コマンドを使って（**NSSA **にではなく）ノーマル エリアにのみルートをインポートしたい場合、このキーワードを使用します。すなわち、このキーワードでは、**NSSA ABR **が（他のエリアのルータを介して学習された）外部ルーティング情報を** NSSA **へアドバタイズするのを防ぎます。**
- default-information-originate - **ルータが** NSSA **エリア境界ルータ（**ABR**）または** NSSA **自律システム境界ルータ（**ASBR**）である時、このパラメータを指定すると、**NSSA **に対するタイプ** -7 **デフォルト** LSA **が生成されます。このデフォルトは、**NSSA ABR **には** AS **内の他エリアに対するルートを、また** NSSA ASBR **には** AS **外部のエリアに対するルートを提供します。**

コマンドモード

Router Configuration

初期設定

NSSA **は構成されていません。**

コマンド解説

- NSSA **内のすべてのルータは、同じエリア** ID **で構成されている必要があります。**
- NSSA **はスタブに似ています。この理由は、ルータが** ABR **である場合、**default-information-originate **キーワードを使用して、**AS **内の他のエリアに対するデフォルト ルートを** NSSA **に送信できるためです。ただし、**NSSA **がスタブと異なる点は、ルータが** ASBR **である場合、**default-information-originate **キーワードを使用して、デフォルトの外部** AS **ルート（**NSSA **に隣接しているが** OSPF AS **内にはないルーティング プロトコル ドメイン宛）を** NSSA **にインポートできることです。**
- NSSA **にアドバタイズされる外部ルートには、**OSPF **を介して学習された** AS **外部のネットワーク宛先のほか、デフォルト ルート、スタティック ルート、他のルーティング プロト**

コル（RIP など）からインポートされたルート、OSPF を実行していないルータに直接接続されたネットワークなどを含めることができます。

- NSSA 外部 LSA （タイプ 7）は、NSSA に隣接した任意の ABR によって外部 LSA （タイプ 5）に変換され、AS 内の他のエリアへ伝播されます。
- また、アンリンク スタブ エリア、すべてのタイプ 3 サマリー LSA は常に NSSA へインポートされ、内部ルートが常にタイプ 7 NSSA 外部ルートよりも優先して選択されることを保証します。
- このルータは、最大 16 のエリア（ノーマル トランジット エリア、スタブ、または NSSA のいずれかの合計）をサポートします。

例

この例では、スタブ エリア 10.3.0.0 を作成し、クラス B アドレス 10.3.x.x を持つインタフェースをすべて NSSA に割り当てます。また、ルータが NSSA ABR または NSSA ASBR の場合、NSSA への外部 LSA を生成するように指示します。

```
Console(config-router)#area 10.3.0.0 nssa default-information-originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```

area virtual-link

仮想リンクを設定します。仮想リンクを削除するには、オプション キーワードを指定せずに no 形式を使用します。属性のデフォルト値に戻すには、要求されるキーワードを指定せずに no 形式を使用します。

文法

area area-id virtual-link router-id

[authentication] [dead-interval seconds] [hellointerval

seconds] [retransmit-interval seconds]

[transmit-delay seconds]

no area area-id virtual-link router-id

[authentication | dead-interval | hello-interval |

retransmit-interval | transmit-delay]

area area-id virtual-link router-id

authentication [message-digest | null]

[authentication-key key | message-digest-key key-id md5 key]

no area area-id virtual-link router-id

authentication [authentication-key |

message-digest-key key-id]

area area-id virtual-link router-id

[authentication-key key | message-digest-key key-id md5 key]

no area area-id virtual-link router-id

[authentication-key | message-digest-key key-id]

- area-id - 仮想リンクのトランジット エリアの識別子です（エリア ID は、IP アドレスと同じ形式である必要があります）。
- router-id - 仮想リンクの隣接ルータのルータ ID です。このルータは、仮想リンクの他方の端にあるバックボーンとトランジット エリア両方に隣接するエリア境界ルータ（ABR）である必要があります。
- authentication - 認証モードを指定します。キーワードの後にオプション パラメータを指定しないと、authentication-key で指定されたパスワードとともにプレーンテキスト認証が使用されます。message-digest 認証を指定する場合、message-digest-key および md5 パラメータも同時に指定する必要があります。null オプションを指定した場合、OSPF ルーティング プロトコル メッセージには認証は実行されません。
- message-digest - メッセージ ダイジェスト（MD5）認証を指定します。
- null - 使用される認証はないことを示します。
- hello-interval seconds - Hello パケット送信間の伝送遅延を指定します。Hello 間隔を小さい値に設定すると、トポロジ変更を検知する際の遅延は短縮されますが、ルーティング トラフィックは増加します。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲 : 1 ～ 65535 秒、デフォルト : 10 秒）。

- retransmit-interval seconds - ABR が仮想リンク上でリンクステートアドバタイズメント（LSA）を再送信する間隔を指定します。この送信間隔は、ルーティング情報の適切なフローを提供しつつも、不必要なプロトコル トラフィックを発生させない程度の控えめな値に設定してください。ただし、この値は、仮想リンクの値よりは大きく設定する必要があることに注意してください（範囲 : 1 〜 3600 秒、デフォルト : 5 秒）。
- transmit-delay seconds - 仮想リンク上でリンクステート アップデート パケットを送信するのに必要な時間を、伝送遅延および伝播遅延を考慮に入れて予測します。LSA のエージには、この値が送信前に加算されます。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲 : 1 〜 3600 秒、デフォルト : 1 秒）。
- dead-interval seconds - ルータのダウンを宣言する前に、隣接ルータが Hello パケットを待機する時間です。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲 : 1 〜 65535 秒、デフォルト : 4 × Hello 間隔、または 40 秒）。
- authentication - 認証モードを指定します。キーワードの後ろにオプションのパラメータがない場合は、認証キーで指定したパスワードと共にテキスト認証を使用します。message-digest 認証を指定すると、message-digest-key および md5 パラメータを指定する必要あります。null オプションを指定すると、OSPF ルーティングプロトコルメッセージの認証は行われません。
  - message-digest - message-digest (MD5) 認証を指定します。
  - null - 認証されていないことを示します。
- authentication-key key - プロトコル メッセージのヘッダ内の認証フィールドを生成または検証するために、仮想リンク上の隣接ルータによって使用されるプレーンテキスト パスワード（最大 8 文字）を設定します。各ネットワーク インタフェースに個別のパスワードを割り当てることができます。ただし、このキーは、同じネットワーク（自律システム）上のすべての隣接ルータに対して同じ値に設定する必要があります。このキーは、バックボーンで認証が有効になっている時のみ使用されます。
- message-digest-key key-id md5 key - メッセージ ダイジェスト（MD5）認証を使用時、隣接ルータとこのルータ間を通過するプロトコル メッセージの認証に使用されるキー識別子とパスワードを設定します。key-id は、1 〜 255 までの整数で、key は、最大 16 文字長の英数字ストリングです。仮想リンク上で MD5 認証が使用されている場合、自律システム内のすべてのルータ上で MD5 が有効になっている必要があります。また、キー識別子とキーは、すべてのルータに対して同じである必要があります。

コマンドモード

Router Configuration

初期設定

area-id: なし

router-id: なし

hello-interval:10 秒

retransmit-interval:5 秒

transmit-delay:1 秒

dead-interval:40 秒

authentication-key: なし

message-digest-key: なし

コマンド解説

- 自律システム全体のルーティング コネクティビティを保持するには、すべてのエリアが、バックボーン エリア（0.0.0.0）に接続されている必要があります。特定のエリアをバックボーンに接続することが物理的に不可能な場合、仮想リンクを使用することができます。仮想リンクは、分離されたエリアのバックボーンへの論理パスを提供するものです。このルータでは、最大 32 の仮想リンクを指定することができます。
- バックボーンから切断された各エリアには、トランジット エリア ID、およびバックボーンに隣接する仮想リンク隣接ルータのルータ ID が含まれている必要があります。
- このルータでは、最大 64 の仮想リンクをサポートします。

例

この例では、すべてのオプション パラメータのデフォルト値を使用して、仮想リンクを作成します。

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

この例では、MD5 認証を使用して、仮想リンクを作成します。

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
message-digest-key 5 md5 ld83jdpq
Console(config-router)#
```

関連するコマンド

show ip ospf virtual-links（P672）

ip ospf authentication

インタフェースで使用される認証タイプを指定します。プレーン テキスト（シンプル パスワード）認証を指定するには、オプション パラメータを使用せずに、こ

のコマンドを入力します。コマンドの前に "no" を置くことで、デフォルトの認証なしに戻ります。

文法

ip ospf authentication [message-digest | null]

no ip ospf authentication

- message-digest - メッセージ ダイジェスト（MD5）認証を指定します。
- null - 使用される認証はないことを示します。

コマンドモード

Router Configuration

初期設定

認証なし

コマンド解説

- ルータが意図せずに非承認エリアに参入するのを防ぐため、認証を使用してください。同じエリア内のルータは同じパスワード（またはキー）を指定して設定してください。同じネットワーク上にあり、同じパスワードを使用するすべてのネイバールータで、ルーティングデータが交換されます。
- 簡易パスワード認証を使用すると、パスワードがパケットに含まれます。そのパスワードが受信ルータで設定されているパスワードと一致しなければ、パケットは破棄されます。この方法では、ルーティングプロトコルパケットのスヌーピングによって認証キーを学習することが可能であるため、セキュリティはほとんど確保されません。
- MD5（Message-Digest 5）認証を使用する場合、ルータは、MD5 アルゴリズムに基づいて、認証キーから 128 bits のメッセージダイジェストを作成することにより、データの整合性を検証します。
- インタフェースにプレーン テキスト パスワード認証を指定する際は、ip ospfauthentication-key コマンドでパスワードを予め構成しておきます。インタフェースに MD5 認証を指定する際は、ip ospf message-digest-key コマンドで、メッセージダイジェスト キー ID とキーを予め構成しておきます。
- プレーンテキスト認証キー、または MD5 キー ID およびキーの使用では、自律システム全体で整合性を保つ必要があります。。

例

この例では、指定インタフェースでメッセージダイジェスト認証を有効にします。

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

ip ospf authentication-key

隣接ルータによって使用されるシンプル パスワードを割り当てます。コマンドの前に "no" **を置くことで、パスワードが削除されます。**

文法

ip ospf [ip-address] authentication-key key

no ip ospf [ip-address] authentication-key

- ip-address - **現行のインタフェースに接続されている特定の** IP **アドレスを示すために使用されるパラメータです。指定されていない場合は、このコマンドは現行のインタフェースの接続先のネットワークすべてに適用されます。**
- key - **プレーン テキスト パスワードを設定します（範囲** : 1-8 **文字）。**

コマンドモード

Interface Configuration (VLAN)

初期設定

パスワードなし

コマンド解説

- **インタフェースにプレーン テキスト パスワード認証を指定する際は、**ip ospfauthentication-key **コマンドでパスワードを予め構成しておきます。各ネットワーク インタフェース ベースで異なるパスワードを割り当てることが可能ですが、パスワードの使用では、ネットワーク（自律システム）全体のすべての隣接ルータ上で整合性を保つ必要があります。**

例

この例では、指定インタフェースのパスワードを設定します。

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

ip ospf message-digest-key

指定インタフェースでメッセージダイジェスト（MD5）認証を有効にします。また、隣接ルータによって使用されるキー ID およびキーの割当てを有効にします。
コマンドの前に "no" を置くことで、既存のキーが削除されます。

文法

ip ospf [ip-address] message-digest-key key-id md5 key

no ip ospf [ip-address] message-digest-key key-id

- ip-address - **現行のインタフェースに接続されている特定の IP アドレスを示すために使用されるパラメータです。指定されていない場合は、このコマンドは現行のインタフェースの接続先のネットワークすべてに適用されます。**
- key-id - MD5 **キーのインデックス番号です（範囲** : 1-255**）。**
- key - 128 **ビットのメッセージダイジェストまたは「フィンガープリント」を生成するのに使用される英数字パスワードです（範囲** : 1-16 **文字）。**

コマンド モード

Interface Configuration (VLAN)

初期設定

MD5 **認証は無効です。**

コマンド解説

-
- **通常、アウトバウンド パケット用の認証情報の生成および着信パケットの認証に使用されるキーは、インタフェースごとに** 1 **つのみです。隣接ルータ同士は、同じキー識別子とキー値を使用する必要があります。**
- **新規キーに変更する時、ルータは、すべてのプロトコル メッセージの複数のコピーを、**1 **つは古いキーで、もう** 1 **つは新しいキーで送信します。すべての隣接ルータが新しいキーで、このルータへプロトコル メッセージの送信を開始すると、ルータは古いキーの使用を止めます。このロールオーバ プロセスにより、ネットワーク管理者には、ネットワーク コネクティビティを低下させることなくネットワーク上のすべてのルータをアップデートする時間の余裕ができます。すべてのネットワーク ルータが新しいキーでアップデートされると、古いキーは、セキュリティ上の理由により削除されます。**

例

この例では、メッセージダイジェスト キーの識別子およびパスワードを設定します。

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```

ip ospf cost

インタフェース上でのパケット送信コストを明示的に設定します。コマンドの前に "no" を置くことで、設定を初期値に戻します。

文法

ip ospf [ip-address] cost cost

no ip ospf [ip-address] cost

- ip-address - 現行のインタフェースに接続されている特定の IP アドレスを示すために使用されるパラメータです。指定されていない場合は、このコマンドは現行のインタフェースの接続先のネットワークすべてに適用されます。
- cost - このインタフェースのリンク メトリックです。低速ポートを示すには、この値を大きくします（範囲 : 1- 65535）。

コマンドモード

Interface Configuration（VLAN）

初期設定

1

コマンド解説

- インタフェース コストは、ポートのスピードを反映します。このルータでは、すべてのポートに対してデフォルトのコスト 1 を使用します。したがって、ギガビット モジュールをインストールする場合、すべての 100 Mbps ポートのコストを 2 以上の値にリセットする必要があります。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```

ip ospf dead-interval

Hello パケットを受信しないまま、この時間が経過すると、隣接ルータによってルータのダウンが宣言されるまでの間隔を設定します。コマンドの前に "no" を置くことで、設定を初期値に戻します。

文法

ip ospf [ip-address] dead-interval seconds

no ip ospf [ip-address] dead-interval

- ip-address - 現行のインタフェースに接続されている特定の IP アドレスを示すために使用されるパラメータです。指定されていない場合は、このコマンドは現行のインタフェースの接続先のネットワークすべてに適用されます。
- seconds - 隣接ルータが送信ルータのダウンを宣言する前に、Hello パケットを待機する最大時間です。この間隔は、ネットワーク上のすべてのルータに対して同じ値に設定されている必要があります（範囲 : 1-65535）。

コマンドモード

Interface Configuration (VLAN)

初期設定

40 秒、または ip ospf hello-interval コマンドにより指定された間隔の 4 倍

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

関連コマンド

ip ospf hello-interval(P654)

ip ospf hello-interval

インタフェース上で送信する Hello パケットの間隔を指定します。コマンドの前に "no" を置くことで、設定を初期値に戻します。

文法

ip ospf [ip-address] hello-interval seconds

no ip ospf [ip-address] hello-interval

- ip-address - 現行のインタフェースに接続されている特定の IP アドレスを示すために使用されるパラメータです。指定されていない場合は、このコマンドは現行のインタフェースの接続先のネットワークすべてに適用されます。
- seconds - インタフェースから送信される Hello パケットの間隔です。この間隔は、ネットワーク上のすべてのルータに対して同じ値に設定されている必要があります（範囲 : 1-65535）。

コマンドモード

Router Configuration

初期設定

10 秒

コマンド解説

- Hello パケットは、送信ルータがまだアクティブであることを他のルータに通知するために使用されます。Hello 間隔を小さい値に設定すると、トポロジ変更の検出における遅延は短縮されますが、ルーティング トラフィックは増加します。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

ip ospf priority

エリアの指定ルータ（DR）およびバックアップ指定ルータ（BDR）を決定する際に使用されるルータ プライオリティを設定します。コマンドの前に "no" を置くことで、設定を初期値に戻します。

文法

ip ospf [ip-address] priority priority

no ip ospf [ip-address] priority

- ip-address - **現行のインタフェースに接続されている特定の** IP **アドレスを示すために使用されるパラメータです。指定されていない場合は、このコマンドは現行のインタフェースの接続先のネットワークすべてに適用されます。**
- priority - **このルータのインタフェース プライオリティです（範囲** : 0-255**）。**

コマンドモード

Interface Configuration（VLAN）

初期設定

1

コマンド解説

- **ルータのプライオリティ応じて** OSPF **ネットワークごとに** DR **および** BDR **が選択されます。**DR **は、ルーティングプロトコル情報を交換するためにネットワーク内の他のルータに対してアクティブな近隣を設定します。何らかの理由で** DR **が失敗した場合は、**BDR **がこの役割を引き継ぎます。**
- **ルータが** DR **または** BDR **として選出されないようにするには、プライオリティを** 0 **に設定します。**0 **以外の任意の値に設定すると、最も高いプライオリティのルータが** DR **になり、次に高いプライオリティのルータが** BDR **になります。**2 **つまたはそれ以上のルータに同じ最高のプライオリティが割り当てられている場合、より高い** ID **を持つルータが選出されます。**
- DR **がすでに存在しているエリアにこのインタフェースが追加された場合、新規ルータの持つプライオリティに関わらず、現行の** DR **が存続します。**DR **は、次に選出プロセスが初期化されるまで変更されません。**
- **マルチアクセスネットワークのみのルータのプライオリティを設定し、ポイント間ネットワークのプライオリティは設定しません。**

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```

ip ospf retransmit-interval

リンクステート アドバタイズメント（LSA）を再送信する間隔を指定します。コマンドの前に "no" を置くことで、設定を初期状態に戻します。

文法

ip ospf retransmit-interval seconds
no ip ospf retransmit-interval

- seconds - **このインタフェースで** LSA **を再送信する間隔を設定します（範囲** : 1-65535**）。**

コマンド モード

Interface Configuration (VLAN)

初期設定

5 **秒**

コマンド解説

- **ルータは、**ACK **を受信しないと、隣接ルータに** LSA **を再送信します。この送信間隔は、ルーティング情報の適切なフローを提供しつつも、不必要なプロトコル トラフィックを発生させない程度の控えめな値に設定してください。この値は、仮想リンクの値より大きく設定する必要があることに注意してください。**
- **この間隔は接続先のネットワーク上 のいずれか** 2 **つのルータ間のラウンドトリップ遅延よりも大きい値に設定してください。**

例：

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

passive-interface

指定したインタフェースの OSPF **ルーティングトラフィックを制御します。コマンドの前に** ”no” **を置くことにより、指定のインタフェースへのルーティングトラフィックの送受信が可能になります。**

文法

[no] passive-interface vlan vlan-id [ip-address]

- vlan-id - VLAN ID(**有効範囲** : 1-4093)
- ip-address - **インタフェースに設定した** IPv4 **アドレス**

コマンドモード

Router Configuration

初期設定

None

コマンド解説

- OSPF **インタフェースを無効にして、インタフェースから** OSPF **ルーティングトラフィックのインタフェースを制御します。関連のあるインタフェースの１つが「**passive **モードに設定されている場合は、**OSPF **近隣ルータは設定されません。**OSPF **ドメインのスタブとして表示されます。近隣ルータが存在する場合に** OSPF **インタフェースを無効に設定すると、近隣ルータは破棄されます。**

例

```
Console(config-router)#passive-interface vlan 1
Console(config-router)#
```

ip ospf transmit-delay

インタフェースでリンクステート アップデート パケットを送信するまでの時間を予測します。コマンドの前に "no" を置くことで、設定を初期状態に戻します。

文法

ip ospf [ip-address] transmit-delay seconds

no ip ospf [ip-address] transmit-delay

- ip-address - 現行のインタフェースに接続されている特定の IP アドレスを示すために使用されるパラメータです。指定されていない場合は、このコマンドは現行のインタフェースの接続先のネットワークすべてに適用されます。
- seconds - リンクステート アップデートを送信するまでの予測待機時間を設定します（範囲 : 1-65535）。

コマンド モード

Interface Configuration (VLAN)

初期設定

1 秒

コマンド解説

- LSA のエージには、この遅延が送信前に加算されます。送信遅延を予測するには、インタフェースの送信遅延および伝播遅延を考慮に入れます。低速リンクに大きい値を使用し、リンク スピードに従って送信遅延を設定します。この送信遅延は、自律システムに接続されたすべてのルータで同じに設定される必要があります。
- この遅延値を追加しない場合、LSA をリンクで送信するのに必要な時間は、ルーティ ングプロセスで考慮されなくなります。低速リンクでは、デバイスが受信できるより も速い速度でルータからパケットが送信される可能性があります。そのような問題が 発生しないようにするため、「Transmit Delay」を使用して、ルータが送信から次の送 信までの間、指定された時間の分だけ待機するようにすることができます。

例：

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

show ip ospf

このコマンドでは、ルーティング 設定に関する基本情報を表示します。

文法

show ip ospf [process-id]

- process-id - **表示する情報のルータプロセス** (**有効期限** : 1-65535)

コマンド モード

Privileged Exec

例

```
Console#show ip ospf
 Routing Process "ospf 1" with ID 192.168.1.3
 Process uptime is 20 minutes
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 LSDB database overflow limit is 20480
 Number of LSA originated 1
 Number of LSA received 0
 Number of areas attached to this router: 1

  Area 192.168.1.3
    Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 0
    Area has no authentication
    SPF algorithm last executed 00:00:08.739 ago
    SPF algorithm executed 1 times
    Number of LSA 1. Checksum 0x007f09
Console#
```

コマンド	機能
Routing Process	
Routing Process with ID	OSPF **プロセス名およびルータ** ID。**ルータ** ID **は、自律システムのルータを固有に識別します。慣例により、通常ルータの** IP **インタフェースアドレスの１つに設定されます。**
Process uptime	**プロセスが稼働している時間**
Conforms to RFC2328	OSPF **バージョン** 2 **と互換性のあるルータを表示します。**

RFC1583 Compatibility flag	RFC 1583 (OSPFv2y よりも古い) と互換性があるかどうかを表示します。
Supports only single TOS (TOS0) routes	OSPF Version 2 で指定されているオプションの ToS(Type of Service) 。Appendix F.1.2 はサポートされていませんが、インタフェースごとのコストのみ１つずつ割り当てられます。
SPF schedule delay	トポロジー変更通知を受信してから SPF 計算を開始するまでの遅延時間。
Hold time	2 つの連続する SPF 計算間の待ち時間を設定します。
Refresh timer	LSA データベースをリフレッシュする間の時間
Number of concurrent DD exchange neighbors	DVD(database descriptor) パケットを現在変換しているネイバールータの数。
Number of external LSA	リンクステートデータベース内の外部リンクステートアドバタイズメント (Type 5 LSAs) の数。これらの LSA は、自律システム以外のルートについての情報をアドバタイズします。
Checksum	リンクステートデータベースに含まれる外部リンクステートアドバタイズメントの LS チェックサムの合計。
Number of opaque AS LSA	リンクステートデータベースの不透明なリンクステートアドバタイズメント Type 9, 10 および 11 LSAs) の数。これらの SLA は、外部のアプリケーションについての情報をアドバタイズして、正しい再開プロセスの OSPF によってのみ使用されます。
Checksum	リンクステートデータベースに含まれる不透明なリンクステートアドバタイズメントの LS チェックサムの合計。
Number of LSA received	受信されているリンクステートアドバタイズメント数。
Number of areas attached to this router	ルータへの接続先の設定されているエリアの数。
Area Information	
Area has (no) authentication	認証が有効化どうかを表示します。
SPF algorithm executed x times	このエリアでの最短パスの最初のアリゴリズムの実行回数。
Number of LSA	AS External LSA を除く、エリアのリンクステートデータベース内のリンクステートアドバタイズメントの総数。
Checksum	リンクステートデータベースに含まれるネットワーク（エリア）のリンクステートアドバタイズメントの LS チェックサムの総数。

show ip ospf border-routers

エリア境界ルータ（ABR）または自律システム境界ルータ（ASBR）についてのルーティング テーブルのエントリを表示します。

文法

show ip ospf [process-id] border-routers

- process-id - **情報を表示するルータプロセスの** ID(**有効範囲** : 1-65535)

コマンド モード

Privileged Exec

例

```
Console#show ip ospf border-routers
OSPF process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.0.3 [1] via 192.168.0.3, vlan1, ABR, ASBR, Area 0.0.0.0
Console#
```

show ip ospf database

このルータのデータベース内に保存された各種 OSPF リンクステート アドバタイズメント（LSA）に関する情報を表示します。

文法

show ip ospf [process-id] database

[asbr-summary | external | network | nssa-external | router

| summary] [adv-router ip-address | link-state-id |

self-originate]

- process-id - LSA 情報を閲覧したいルータプロセスの ID（有効範囲 :1-65535)。
- adv-router - アドバタイジング ルータの IP アドレスです。入力しない場合、すべてのアドバタイジング ルータに関する情報が表示されます。
- ip-address - 指定ルータの IP アドレスです。アドレスを入力しない場合、ローカルルータに関する情報が表示されます。
- asbr-summary - ASBR （自律システム境界ルータ）サマリー LSA に関する情報を表示します。
- link-state-id - LSA によって記述されるネットワーク部分です。link-state-id には、次を入力する必要があります。
  - タイプ 3 サマリーおよび外部 LSA の IP ネットワーク番号
  - ルータのルータ ID、ネットワーク、タイプ 4 AS サマリー LSA。また、タイプ 5 ASBR 外部 LSA によってデフォルト ルートが記述される時、その link-state-id はデフォルトの宛先（0.0.0.0）に設定されることに注意してください。
- self-originate - このルータによって送信される LSA を表示します。
- asbr-summary - ASBR サマリの LSA の総数を表示します。
- external - 外部 LSA に関する情報を表示します。
- network - ネットワーク LSA に関する情報を表示します。
- nssa-external - NSSA 外部 LSA に関する情報を表示します。
- router - ルータ LSA に関する情報を表示します。
- summary - サマリー LSA に関する情報を表示します。

コマンド モード

Privileged Exec

例

次の例は、show ip ospf database コマンドの出力を示します。

```
Console#show ip ospf database

     OSPF Router with ID (192.168.0.2) (Process ID 1)

       Router Link States (Area 0.0.0.0)

Link ID        ADV Router Age Seq# CkSum   Link  count
192.168.0.2   192.168.0.2 225 0x80000004  0xdac5 1
192.168.0.3   192.168.0.3 220 0x80000004  0xd8c4 1

      Net Link States (Area 0.0.0.0)

Link ID     ADV Router Age Seq# CkSum
192.168.0.2 192.168.0.2 225 0x80000001 0x9c0f

      AS External Link States

Link ID ADV Router  Age Seq#        CkSum Route Tag
0.0.0.0 192.168.0.2 487 0x80000001 0xd491 E2 0.0.0.0/0 0
0.0.0.0 192.168.0.3 222 0x80000001 0xce96 E2 0.0.0.0/0 0

Console#
```

項目	解説
OSPF Router Process with ID	OSPF ルータの ID およびプロセス ID。ルータ ID は自律システムのルータを固有に識別します。したがって、これはルータの IP インタフェースのアドレスの 1 つに設定されます。
Link ID	ルータ ID
ADV Router	アドバタイジング ルータ ID
Age	LSA のエージです（秒単位）
Seq#	LSA のシーケンス番号（古い重複した LSA の検出に使用されます）
CkSum	LSA の完全コンテンツのチェックサム
Link count	ルータに接続されているインタフェース数
Route	Type 1、または Type 2 の外部メトリック (redistribute コマンド) およびルート
Tag	定義されているオプションタグ (redistribute コマンドを参照)

次の例は、asbr-summary キーワードを使用した場合 です。

```
Console#show ip ospf database asbr-summary

    OSPF Router with ID (0.0.0.0) (Process ID 1)

       ASBR-Summary Link States (Area 0.0.0.1)

  LS Age: 0
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: ASBR-summary-LSA
  Link State ID: 2.1.0.0 (AS Boundary Router address)
  Advertising Router: 192.168.2.1
  LS Seq Number: 80000001
  Checksum: 0x7b67
  Length: 28
  Network Mask: /0
       TOS: 0 Metric: 10

Console#
```

項目	解説
OSPF Router id	ルータ ID
LS age	LSA のエージ（秒単位）
Options	LSA と関連付けられたオプション機能
LS Type	AS External Links - LSA は、AS 外部の宛先へのルート（AS へのデフォルト外部ルートを含む）を記述
Link State ID	リンクステート ID
Advertising Router	アドバタイジング ルータ ID
LS Sequence Number	LSA のシーケンス番号（古い重複した LSA の検出に使用されます）
Checksum	LSA の完全コンテンツのチェックサム
Length	LSA の長さをバイト単位で示
Network Mask	ネットワークのアドレス マスク
Metric Type	タイプ 1 またはタイプ 2 外部メトリック
Metrics	リンクのコスト

次の例は、external キーワードを使用した場合 です。

```
OSPF Router process 100 with ID (10.10.11.50)
AS External Link States LS age: 298
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 10.10.100.0 (External Network Number)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x7033
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 10.10.11.50
External Route Tag: 0

       OSPF Router with ID (0.0.0.0) (Process ID 1)

          AS External Link States

LS Age: 0
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 0.0.0.0 (External Network Number)
Advertising Router: 192.168.0.2
LS Seq Number: 80000005
Checksum: 0xcc95
Length: 36
Network Mask: /0
   Metric Type: 2 (Larger than any link state path)
   TOS: 0
   Metric: 1
   Forward Address: 0.0.0.0
   External Route Tag: 0

Console#
```

項目	解説
OSPF Router id	ルータ ID
LS age	LSA のエージ（秒）
Options	LSA と関連付けられたオプション機能
LS Type	Network Link - LSA は、ネットワークに接続されたルータを記述
Link State ID	自律システム境界ルータ（ASBR）のインタフェース アドレス
Advertising Router	アドバタイジング ルータ ID
LS Sequence Number	LSA のシーケンス番号（古い重複した LSA の検出に使用されます）
Checksum	LSA の完全コンテンツのチェックサム
Length	LSA の長さをバイト単位で示します
Network Mask	ネットワークのアドレス マスク

Forward Address	アドバタイズされた宛先へ渡されるデータのフォワーディング アドレスです（フォワーディング アドレスが 0.0.0.0 に設定されている場合、データはアドバタイズメントの発信元へ転送されます）
External Route Tag	各外部ルートに割り当てられた 32 ビット フィールドです（OSPF では使用されません。特定のアプリケーションで指定されたとおりに境界ルータ間で他の情報を通信するのに使用されます）。

次の例は、network キーワードを使用した場合 です。

```
Console#show ip ospf database network

       OSPF Router with ID (0.0.0.0) (Process ID 1)

           Net Link States (Area 0.0.0.0)

LS Age: 0
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.168.0.2 (address of Designated Router)
Advertising Router: 192.168.0.2
LS Seq Number: 80000005
Checksum: 0x9413
Length: 32
Network Mask: /24
     Attached Router: 192.168.0.2
     Attached Router: 192.168.0.3
```

項目	解説
OSPF Router id	ルータ ID
LS age	LSA のエージ（秒単位）
Options	LSA と関連付けられたオプション機能
LS Type	Network Link - LSA は、ネットワークに接続されたルータを記述
Link State ID	自律システム境界ルータ（ASBR）のインタフェース アドレス
Advertising Router	アドバタイジング ルータ ID
LS Sequence Number	LSA のシーケンス番号（古い重複した LSA の検出に使用されます）
LS Checksum	LSA の完全コンテンツのチェックサム
Length	LSA の長さをバイト単位で示します
Network Mask	ネットワークのアドレス マスク
Attached Router	ネットワークに接続されたルータ（指定ルータ自身を含む、指定ルータに完全に隣接したルータ）のリスト

次の例は、router キーワードを使用した場合 です。

```
Console#show ip ospf database router

        OSPF Router with ID (0.0.0.0) (Process ID 1)

            Router Link States (Area 0.0.0.0)

LS Age: 0
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x2 : ASBR
LS Type: router-LSA
Link State ID: 192.168.0.2
Advertising Router: 192.168.0.2
LS Seq Number: 80000008
Checksum: 0xd2c9
Length: 36
  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.168.0.2
    (Link Data) Router Interface address: 192.168.0.2
      Number of TOS metrics: 0
      TOS 0 Metric: 1
.
.
.
```

項目	解説
OSPF Router id	ルータ ID
LS age	LSA のエージ（秒単位）
Options	LSA と関連付けられたオプション機能
Flags	このルータが仮想リンクのエンドポイントの ASBR、または ABR であるかどうか
LS Type	Network Link - LSA は、ネットワークに接続されたルータを記述
Link State ID	自律システム境界ルータ（ASBR）のインタフェース アドレス
Advertising Router	アドバタイジング ルータ ID
LS Sequence Number	LSA のシーケンス番号（古い重複した LSA の検出に使用されます）
Checksum	LSA の完全コンテンツのチェックサム
Length	LSA の長さをバイト単位で示します
Link connected to	Link-state タイプ (送信ネットワーク、スタブネットワーク、または仮想リンクを含む)
Link ID	リンクタイプと対応のルータ ID、またはネットワークアドレス
Link Data	• 送信ネットワーク用のルータ ID • スタブネットワークのネットワーク IP アドレスマスク • 仮想リンクのネイバールータ ID
Number of TOS metrics	Type of Service metric – TOS 0 のみサポートしているルータ (あるいは、通常のサービス)
TOS	Type of Service – TOS 0 のみサポートしているルータ (あるいは、通常のサービス)

Metrics	リンクのコスト

次の例は、summary キーワードを使用した場合 です。

```
Console#show ip ospf database summary
OSPF Router with ID (0.0.0.0) (Process ID 1)
Summary Link States (Area 0.0.0.0)
LS Age: 1
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: summary-LSA
Link State ID: 192.168.10.0 (summary Network Number)
Advertising Router: 2.1.0.0
LS Seq Number: 80000005
Checksum: 0x479d
Length: 28
Network Mask: /24
TOS: 0 Metric: 0
```

項目	解説
OSPF Router id	ルータ ID
LS age	LSA のエージ（秒単位）
Options	LSA と関連付けられたオプション機能
LS Type	Network Link - LSA は、ネットワークに接続されたルータを記述
Link State ID	自律システム境界ルータ（ASBR）のインタフェース アドレス
Advertising Router	アドバタイジング ルータ ID
LS Sequence Number	LSA のシーケンス番号（古い重複した LSA の検出に使用されます）
Checksum	LSA の完全コンテンツのチェックサム
Length	LSA の長さをバイト単位で示します
Network Mask	宛先ネットワーク IP アドレスのマスク
Metrics	リンクのコスト

show ip ospf interface

OSPF インタフェースのサマリー情報を表示します。

文法

show ip ospf interface [vlan vlan-id]

- vlan-id - VLAN ID です（範囲：1-4093）

コマンド モード

Privileged Exec

例

```
VLAN1 is up, line protocol is up
Internet Address 192.168.0.2/24, Area 0.0.0.0, MTU 1500
  Process ID 1, Router ID 192.168.0.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.0.2, Interface Address 192.168.0.2
  Backup Designated Router (ID) 192.168.0.3, Interface Address
192.168.0.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:10
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 920 sent 975, DD received 5 sent 4
  LS-Req received 1 sent 1, LS-Upd received 14 sent 18
  LS-Ack received 17 sent 13, Discarded 0
Console#
```

項目	解説
Vlan	物理リンクの VLAN ID とステータスです。
Interface Address	OSPF インタフェースの IP アドレス
Mask	インタフェース アドレスのネットワーク マスク
Area	このインタフェースが属している OSPF エリア
Router ID	ルータ ID
Network Type	ブロードキャスト、非ブロードキャスト、またはポイントツーポイント ネットワークのいずれか
Cost	インタフェースの送信コスト
Transmit Delay	インタフェースの送信遅延（秒単位）
State	• Disabled - このインタフェース上で OSPF は有効になっていません。 • Down . - このインタフェース上で OSPF は有効になっていますが、インタフェースがダウンしています。 • Loopback - ループバック インタフェースです。 • Waiting - ルータは DR と BDR を見つけようとしています。 • DR - 指定ルータ（Designated Router）です。 • BDR - バックアップ指定ルータ（Backup Designated Router）です。 • DRother - インタフェースはマルチアクセス ネットワーク上にありますが、DR または BDR ではありません。
Priority	ルータのプライオリティ
Designated Router	指定ルータ ID （DR ID）、および対応するインタフェース アドレス
Backup Designated Router	バックアップ指定ルータの ID と対応するインタフェース アドレス

Timer intervals	タイマー間隔（Hello 間隔、Dead 間隔、Retransmit 間隔を含む）のコンフィグレーション設定

show ip ospf neighbor

OSPF エリア内の各インタフェース上の隣接ルータに関する情報を表示します。

文法

show ip ospf [process-id] neighbor

- process-id - LSA 情報を閲覧したいルータプロセスの ID（有効範囲 :1-65535)。

コマンド モード

Privileged Exec

例

```
Console#show ip ospf neighbor
ID     Pri        State          Address            Interface
--------------- ------ --------------- --------------- ---------
192.168.0.3     1      FULL/BDR     192.168.0.3     VLAN1
Console#
```

項目	解説
Neighbor ID	隣接ルータのルータ ID
Pri	近隣のルータプライオリティ
State	OSPF の状態と識別フラグ。各状態は、次のとおりです。 Down - 接続がダウンしています。 Attempt - 接続はダウンしているが、コンタクトが試みられています（非ブロードキャスト ネットワーク用)。 Init - Hello パケットは受信されたが、通信はまだ確立されていません。 Two-way - 双方向通信が確立しています。 ExStart - 隣接ルータ間の隣接性を初期化しています。 Exchange - データベース記述を交換しています。 Loading - LSA データベースを交換しています。 Full - 隣接ルータは完全に隣接関係にあります。 各識別フラグは次のとおりです。 D - ダイナミック隣接ルータです。 S - スタティック隣接ルータです。 DR - 指定ルータです。 BDR - バックアップ指定ルータです。

show ip ospf route

OSPF ルーティングテーブルを表示します。

文法

show ip ospf [process-id] route

- process-id - 情報を表示するルータのプロセス ID(有効範囲 : 1-65535)

コマンドモード

Privileged Exec

例

```
Console#show ip ospf route
OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external   type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
O 10.10.0.0/24 [10] is directly connected, fe1/1, Area 0.0.0.0
O 10.10.11.0/24 [10] is directly connected, fe1/2, Area 0.0.0.0
O 10.10.11.100/32 [10] is directly connected, lo, Area 0.0.0.0
E2 10.15.0.0/24 [10/50] via 10.10.0.1, VLAN1
IA 172.16.10.0/24 [30] via 10.10.11.50, VLAN2, Area 0.0.0.0
E2 192.168.0.0/16 [10/20] via 10.10.11.50, VLAN2

Console#
```

show ip ospf virtual-links

仮想リンクに関する詳細情報を表示します。

文法

show ip ospf virtual-links

コマンド モード

Privileged Exec

例

```
Console#show ip ospf virtual-links
Virtual Link VLINK1 to router 192.168.0.2 is up
  Transit area 0.0.0.1 via interface VLAN1
  Local address 192.168.0.3
  Remote address 192.168.0.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:08
  Adjacency state Down
Console#
```

項目	解説
Virtual Link to router	OSPF **隣接ルータとリンク状態（アップまたはダウン）**
Transit area	**仮想リンクがターゲット ルータに到達するために横断する共通エリア**
Local address	**共通のトランジットエリアに孤立したエリアを接続するエンドポイントしての役割を果たす** ABR **の** IP **アドレス。**
Remote address	**仮想ネイバーが使用する** IP **アドレス。ネイバーは他のバックボーンに共通のトランジットエリアを接続するエンドポイントの** ABR **でなければならない。**
Transmit Delay	**仮想リンク上の予測送信遅延（秒単位）**
Timer intervals	**タイマー間隔（**Hello **間隔、**Dead **間隔、**Retransmit **間隔を含む）のコンフィギュレーション設定**

関連するコマンド

area virtual-link（P686）

show ip protocols ospf

OSPF プロセスパラメータを表示します。

文法

show ip protocols ospf

コマンド モード

Privileged Exec

例

この例では、サマリー アドレス、および関連付けられたネットワーク マスクを表示します。

```
Console#show ip protocols ospf
Routing Protocol is "ospf 200" Redistributing: rip
Routing for Networks:
192.30.30.0/24
192.40.40.0/24
Routing for Summary Address:
192.168.1.0/24
192.168.3.0/24
Distance: (default is 110)
Console#
```

項目	解説
Routing Protocol	OSPF プロセスの名前および AS 番号
Redistributing	redistribute コマンドにより、ルーティングプロトコルの再配送が可能かどうかを表示します。
Routing for Networks	OSPF によって現在登録中のルーティング情報のネットワーク
Routing for Summary Address	ルート集約が有効なネットワークを表示します。
Distance	OSPF によって学習される外部ルートに使用される管理上の距離

1.31 Open Shortest Path First (OSPFv3)

コマンド	機能	モード	ページ
General Configuration			
router ipv6 ospf	OSPFv3 ルーティングプロセスを有効 / 無効にします。	GC	P676
abr-type	ルータ自身で ABR を宣言し、Type 3 and Type 4 のサマリ LSA を発行しているかどうかを判断するための基準を設定します。	RC	P677
max-current-dd	dd パケットを同時に交換可能なスイッチの隣接ルータの最大値を設定します。	RC	P678
router-id	デバイスのルータ ID を設定します。	RC	P679
timers spf	トポロジ変更時の遅延および連続する SPF 計算中の保持時間を設定します。	RC	P680
Route Metrics and Summaries			
area default-cost	stub に送信されるデフォルトのサマリルートのコストを設定します。	RC	P681
area range	ABR によって通知されるルートを集約します。	RC	P682
default-metric	他のプロトコルからインポートされる外部ルートの default metric を設定します。	RC	P683
redistribute	ルーティングドメイン間のルートを再配布します。	RC	P684
Area Configuration			
area stub	LSA の送受信が不可能な stubby area を設定します。	RC	P685
area virtual-link	エリア教会ルータからバックボーンまでの仮想リンクを設定します。	RC	P686
ipv6 router ospf area	エリアを選択したインタフェースにバインドします。	IC	P688
IC ipv6 router ospf tag area	エリアを設定したインタフェースおよびプロセスにバインドします。	IC	P690
Interface Configuration			
ipv6 ospf cost	インタフェース上のパケットを送信するコストを指定します。	IC	P692
ipv6 ospf dead-interval	隣接ルーターから Hello パケットを受信できなくなったときに、隣接ルーターがダウンしたと判断するまでの 時間を指定します。	IC	P693
pv6 ospf hello-interval	hello パケットの送信間隔を指定します。	IC	P694
ipv6 ospf priority	指定のルータを判別するために使用するプライオリティを設定します。	IC	P695
ipv6 ospf retransmit-interval	link-state アドバタイスメントを再送信する間隔を指定します。	IC	P696
ipv6 ospf transmit-delay	インタフェース上の link-state update パケットの送信時間を設定します。	IC	P697
passive-interface	指定したインタフェース上の OSPF ルーティングトラフィックを 抑止します。	RC	P698
Display Information			
show ipv6 ospf	ルーティングプロセスの情報を表示します。	PE	P699

show ipv6 ospf database	データベースの各 LSA 情報を表示します。	PE	P701
show ipv6 ospf interface	インタフェース情報を表示します。	PE	P702
show ipv6 ospf neighbor	隣接ルータ情報を表示します。	PE	P704
show ipv6 ospf route	OSPF ルーティングテーブルを表示します。	PE	P704
show ipv6 ospf virtual- links	パラメータおよび仮想リンクの近隣状態を表示します。	PE	P706

OSPFv3 を設定するには、以下の手順に従ってください。

（1）OSPF ルーティングプロセス中の各 VLAN インタフェースに IPv6 link-local アドレスを割り当てます。ipv6 enable コマンドを使用して、link-local ローカルアドレスを自動設定するか、または ipv6 address link-local コマンドを使って、インタフェースへアドレスを手動で指定してください。

（2）router ipv6 ospf コマンドを使用して、ローカルの OSPF ルータプロセスを設定して、ルータコンフィグレーションモードに入ります。

（3）router-id コマンドを使用して、ルータに固有の識別子を割り当てます。

[注意]　デフォルトのルータ ID“0.0.0.0” は、現行のソフトウェアバージョンでは使用できません。

（4）ルータに固有の識別子を割り当てます。

（5）デフォルトのルータ “0.0.0.0” は、現在のソフトウェアでは使用できません。

（6）ipv6 router ospf area コマンド、または ipv6 router ospf tag area コマンドを使用して、指定した OSPF プロセスを行う各インタフェースにエリアを割り当てます。

OSPFv3 の設定方法については、以下の手順に従ってください。

（1）OSPF ルーティングを行う VLAN インタフェースに IPv6 link-local アドレスを割り当てると、自動的に ipv6 enable コマンドを使って link-local アドレスが設定されます。また、ipv6 address link-local コマンドを使ってインタフェースにアドレスを手動で割り当てることができます。

（2）router ipv6 ospf コマンドを使用して、ローカルの OSPF ルータプロセスを設定し、ルータ設定モードに入ります。

（3）router-id コマンドを使用すると、ルータに固有の識別子を割り当てます。ドフォルトのルータ ID“0.0.0.0” は、現行のソフトウェアのバージョンでは使用できませんので、注意してください。

（4）ipv6 router ospf area コマンドを使用すると、特定の OSPF プロセスに設定するインタフェースにエリアを割り当てます。

router ipv6 ospf

Open Shortest Path First (OSPFv3) ルーティングプロセスを設定し、router configuration モードに入ります。コマンドの前に "no" を付けることにより特定のプロセス、またはすべての OSPF は無効になります。

文法

[no] router ipv6 ospf [tag process-name]

process-name - 複数のルーティングインスタンスを設定する場合は、プロセス名を入力してください (有効範囲 : 16 文字以内の英数字)

コマンドモード

Global Configuration

初期設定

無効です。

コマンド解説

- このコマンドを使用して、OSPFv3 ルーティングプロセスを有効にして、ルータコンフィグレーションモードに入ります。
- process-name はローカルルータでのみ使用され、各ルーティングプロセスを区別します。ipv6 router ospf area コマンドで設定した instance-id （同じリンクローカルネットワーク上で動作するルーティングプロセスを区別するためのもの）とは異なりますので注意してください。

```
Console(config)#router ipv6 ospf tag 0
Console(config-router)#end
Console#show ipv6 ospf
 Routing Process "ospf r&d" with ID 192.168.0.2
 Process uptime is 1 hour 34 minutes
 Supports only single TOS(TOS0) routes
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Number of incoming concurrent DD exchange neighbors 0/5
 Number of outgoing concurrent DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of LSA received 0
 Number of areas attached to this router: 1

    Area 0.0.0.0 (BACKBONE)
        SPF algorithm executed 1 times
        Number of LSA 2. Checksum 0x00ab4f

Console#
```

関連するコマンド

ipv6 router ospf area (P688)

abr-type

ルータが自分自身を ABR と宣言し、Type 3 および Type 4 サマリ LSA を発行可能かどうか判断する基準を設定します。コマンドの前に "no" を付けることによりデフォルトの設定に戻ります。

文法

abr-type {cisco | ibm | standard}

no abr-type

- cisco - ABR 基準により、機能的動作は RFC 3509 に従って実行されます。
- ibm - ABR 基準により、機能的動作は RFC 3509 に概要が記述されており、詳細については、IBM Nways Multiprotocol Routing Services (MRS) 3.3 に記載しています。
- standard - ABR 基準により、機能的動作は RFC 2328 に従って実行されます。

コマンドモード

Router Configuration

初期設定

cisco

コマンド解説

ABR としての役割を果たすルータの基準は、以下のとおりです。

- Cisco Systems Interpretation: 複数のエリアが互いに有効に繋げられ、そのうちの 1 つがバックボーンエリアであると、ルーターは ABR とみなされる。
- IBM Interpretation: 複数のエリアが互いに有効に繋げられ、バックボーンエリアが設定されていると、ルーターは ABR とみなされる。
- Standard Interpretation: ルーターが 2 個又はそれ以上のエリアに繋げられていると、そのルーターは ABR とみなされる。そのルーターはバックボーンエリアに繋げられている必要はない。
- トラフィックをエリア間及び外部 AS 送信先へ正常にルーティングするには、ABR がバックボーンに接続されていなければならない。ABR にバックボーン接続がない場合、それに接続されていないエリア及び AS 外部のエリアが送信先となるすべてのトラフィックが中断されます。このような状況は通常、ABR からバックボーンエリアへ仮想リンクを設定することにより解消されます。
- Cisco の説明でも、IBM の説明でも、複数のエリアに接続されているルーターは、前述の残りの条件を満たさない限り、自ら ABR と宣言して、タイプ 1 のルーター LSA を発行することはできないと指定されている。
- ルーターは ABR ではないが、複数の繋がったエリアを有する場合、又は有効なバックボーン接続がない場合、繋がっているすべてのエリアからのサマリー LSA をルーターが検討できるようルーティング・テーブルの計算方法が変更されます。
- い換えると、エリア間のルーティングはサマリー LSA を調べることで計算されます。ルーターが ABR であり、有効なバックボーン接続がある場合には、バックボーンのサマリー LSA だけが調べられる。そうでない場合（ルーターが ABR ではない場合、又は

有効なバックボーン接続がない場合)、ルーターは、すべての有効に繋がったエリアからのサマリー LSA を検討しなければならない。

- これにより、ルーターに有効なバックボーン接続があり、他のエリアまでのエリア内及びエリア間の両方のルートにアドバタイズする場合、エリア境界ルーターによって生成されたサマリー LSA は、バックボーンまでのエリア内ルートだけにアドバタイズするようになります。そうでない場合、ルーターは、バックボーン以外のエリアまでのエリア内ルートにアドバタイズするだけです。

例：

```
Console(config-router)#abr-type ibm
Console(config-router)#
```

max-current-dd

現在データベースディスクリプター（DD) パケットを変更可能な隣接ルータの最大数を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻します。

文法

max-current-dd max-packets

no max-current-dd

- max-packets - 現在データベースディスクリプター（DD) パケットの送受信が可能な隣接ルータの最大数を設定します (有効範囲 : 1-65535)。

コマンドモード

Router Configuration

初期設定

5

コマンド解説

- 現在 DD パケットを送受信可能な隣接ルータ数を制限します。

例

```
Console(config-router)#maximum-current-dd 10
Console(config-router)#
```

関連するコマンド

show ipv6 ospf (P699)

router-id

現行の OSPFv3 プロセスの自律システム内のデバイスごとに固有のルータ ID を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻ります。

文法

router-id ip-address

no router-id

- ip-address - IPv4 アドレスにフォーマット化されたルータ ID

コマンドモード

Router Configuration

初期設定

None

コマンド解説

- router ipv6 ospf コマンドで指定された OSPF プロセスごとにルータ ID を設定します。
- ルータ ID は、自律システムのルータごとに固有でなければなりません (ルータ ID は 255.255.255.255 に設定可能)。
- ルータにすでに隣接ルータが登録されている場合は、ルータをリブートしたり、no router ipv6 ospf の後に router ipv6 ospf コマンドを入力して手動で再起動すると、新しいルータ ID が使用されます。
- 指定されたルータ、あるいはエリアに指定されたバックアップルータのプライオリティの値が同じ場合は、プライオリティが一番高い ID をもつルータが選ばれます。
- 現行のルーティングプロセスは ID がこのコマンドで設定されるまで無効となります。

例：

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

関連するコマンド

router ipv6 ospf (P676)

timers spf

トポロジの変更を受信してから SPF(shortest path first) **計算を開始する迄に要する遅延時間と** 2 **回連続して** SPF **計算時にかかる時間を設定します。コマンドの前に** "no" **を付けることによってデフォルト設定に戻ります。**

文法

timers spf spf-delay spf-holdtime

no timers spf

- spf-delay - **トロポジの変更通知を受信してから、**SPF **計算を開始する迄の遅延時間** (**有効範囲** : 0-2147483647 **秒**)
- spf-holdtime - 2 **回連続して** SPF **計算時にかかる時間** (**有効範囲** : 0-2147483647 **秒**)

コマンドモード

Router Configuration

初期設定

SPF delay: 5 **秒**
SPF holdtime: 10 **秒**

コマンド解説

- SPF holdtime **を「**0**」に設定すると、連続する計算の間の遅延はありません。**
- holdtime **の値が小さいと、ルータは新しいパスを早く設定可能ですが、**CPU **処理時間が大きくなります。**

例

```
Console(config-router)#timers spf 20
Console(config-router)#
```

area default-cost

ABR(Area Border Router) からスタブに送信されるデフォルトのサマリルーティングのコストを指定します。コマンドの前に "no" を付けることにより指定したデフォルトのコストは消去されます。

文法

area area-id default-cost cost

no area area-id default-cost

- area-id - スタブを指定します (エリア ID は IPv4 アドレス形式、あるいは 0-4294967295 までの 4 桁のオクテットの形式)
- cost - スタブに送信されるデフォルトのサマリルートのコスト (有効範囲 : 0-16777215)

コマンドモード

Router Configuration

デフォルト設定

Default cost: 1

コマンド解説

- デフォルトのコストは「0」に設定されている場合は、ルータは接続先のスタブにデフォルトのルートをアドバタイズしません。
- area nssa コマンドを使用して、NSSA に送信されるデフォルトのルートのコストを指定します。

例

```
Console(config)#router ipv6 ospf tag 1
Console(config-router)#area 1 default-cost 1
Console(config-router)#
```

関連するコマンド

area stub (P685)
area nssa (P644)

area range

ABR(Area Border Router) によってアドバタイズされるルートを要約します。コマンドの前に コマンドの前に "no" を付けることにより、この機能は無効になります。

文法

[no] area area-id range ipv6-prefix/prefix-length {advertise | not-advertise}

- area-id - ルートをサマライズするエリアを表します。エリア ID は、IPv4 アドレス形式、あるいは 0-4294967295 までの 4 桁のオクテットで表します。
- ipv6-prefix - IPv6 アドレス（ネットワークのプレフィックス、ホストアドレスのビット数を含む）
- prefix-length - プレフィックスを構成するアドレスの連続するビット数（左から）を表す 10 進数の値（例えば、要約するアドレスの部分）。
- advertise - 指定のアドレスの範囲をアドバタイズします。
- not-advertise - サマリは送信されず、ルートはネットワークから隠蔽された状態になります。

コマンドモード

Router Configuration

初期設定

Disabled

コマンド解説

- エリア内のルーティングをサマライズして、ABR 内のエリアに情報をアドバタイズします。
- エリア内のネットワークアドレスが連続する方法で設定されている場合は、ABR は area range コマンドを使用して、指定した範囲内のエリアの個々のネットワークをすべて網羅するサマリールートをアドバタイズすることが可能です。
- ルートがこのコマンドによりアドバタイズできるように設定されている場合、ルータは、このコマンドによって指定されているアドレス範囲ごとにタイプ 3 のサマリー LSA を発行します。
- このルータは、エリア範囲ごとにサマリールートを最大 64 個までサポートしています。

例

ここでは、73::/8 までの範囲のエリアのルートすべてのサマリアドレス、あるいは 73 バイトで始まる IPv6 アドレスをすべて設定します。

```
Console(config-router)#area 1 range 73::/8 advertise
Console(config-router)#
```

default-metric

他のプロトコルからインポートされた外部ルートのデフォルトのメトリックを設定します。

コマンドの前に "no" **を付けることにより、デフォルトのプロトコルタイプの設定基準が削除されます。**

文法

default-metric metric-value

no default-metric

- metric-value – **他のプロトコルからインポートされた外部ルートすべてに設定されたメトリック** (**有効範囲** : 0-16777214)**。**

コマンドモード

Router Configuration

初期設定

20

コマンド解説

- **デフォルトのメトリックは、互換性のないメトリックを用いた他のプロトコルからの外部ルートを再送する問題を解決するために使用します。**
- redistribute **コマンドを使用しても、メトリック値は上書きされません。メトリック値が** redistribute **コマンドによって設定されていない場合は、**default-metric **コマンドにより、メトリック値がインポートされた外部ルートすべてに使用できるように設定します。**

例

```
Console(config-router)#default-metric 100
Console(config-router)#
```

関連するコマンド

redistribute (P684)

redistribute

他のルーティングプロトコルからの外部ルーティング情報、および自律システムのスタティックルーツを再送します。コマンドの前に "no" **を付けることによりこの機能は無効になり、デフォルトの設定に戻ります。**

文法

redistribute {connected | static} [metric metric-value] [metric-type type-value]

no redistribute {connected | static} [metric] [metric-type] [route-map]

- connected - **現行で接続されているエントリをすべてインポートします。**
- static - IPv6 **スタティックルートは自律システムにインポートされます。**
- metric-value - **指定のプロトコルの外部ルートすべてに割り当てられるメトリック** (**有効範囲** : 0-16777214: **デフォルト** : 20)**。**
- type-value
  - 1 - Type 1 **外部ルート**
  - 2 - Type 2 **外部ルート** (**デフォルト設定**) - **ルータは外部ルートのメトリックに内部ルートのメトリックを追加しません。**

コマンドモード

Router Configuration

初期設定

redistribution - none
metric-value - 20
type-metric - 2

コマンド解説

- OSPF **ドメインの他のルーティングプロトコルから学習したルーツをインポートしたり、**AS-external-LSAs **を生成するために使用します。**
- OSPF **自律システムの外部ルートを送信すると、ルータは自動的に** ASBR**（自律システム境界ルータ）になります。**
- **メトリックのタイプにより、外部の** LSAs **を介して** AS **以外の宛先にルートをアドバタイズする方法を指定します。**Type 1 **の** LSA **は、ルータにより受信されると、外部ルータのメトリックに内部コストを追加します。つまり、**AS **内のルータからのルートのコストは、アドバイスする先の** ASBR **に届くまでのコストに、外部ルートのコストを加えたものと同じです。**Type 2 **の** LSA **がルートにより受信されると、外部ルートのメトリックを使用してルートコストを算出します。**

例

この例では、Type 1 の外部ルートとして自動的に接続されるルートを送信します。

```
Console(config-router)#redistribute connected metric-type 1
Console(config-router)#
```

area stub

スタブエリアを設定します。スタブを削除するには、オプションのキーワードを使用せずにコマンドの前に ”no” を付けます。サマリの属性を削除するには、サマリーキーワードを使ってコマンドの前に ”no” を付けます。

文法

[no] area area-id stub [no-summary]

- area-id - スタブエリアを示します。エリア ID は、IPv4 アドレスのフォーマット、または 0-4294967295 までの 4 桁のオクテッドで表記します。
- no-summary - ABR がスタブエリアにサマリリンクのアドバタイズを送信するのを中止します。

コマンドモード

Router Configuration

初期設定

スタブは設定されていません。
サマリアドバタイズメントはスタブに送信されます。

コマンド解説

- スタブ内のすべてのルータは同じエリア ID で設定する必要があります。
- ルーティングテーブルのスペースは ABR によるスタブ内の Type-4 のエリア内ルータと Type 5 の AS-External LSA のフラッディングを回避することによりセーブします。外部ルータの情報がスタブ内で認識されていないため、ABR は Type 3 の Inter-Area Prefix LSA を使用して、デフォルトのルート 0::0/0 をアドバタイズします。
- コマンドのデフォルト設定により、Type-4 のエリア内ルータと Type 5 の AS-External LSA をブロックします。そのため、エリア内、またはエリア間ルートに一致しない宛先はすべてデフォルトのルートを使用しなければなりません。
- スタブに接続されている ABR 上のコマンドの no-summary パラメータを使って、スタブエリアを設定し、Type 3 のネットワークサマリ LSA をすべてブロックします。エリア内のルータ他のエリアからのサマリ LSA を必要としない場合はのみ、トータリースタブエリアとして設定します。
- area default-cost コマンドを使用して、スタブエリアに接続された ABR によってスタブに送信されたデフォルトのサマリールートのコストを指定します。

例

ここでは、スタブエリア 2 を設定し、Type 3 のサマリ LSAs をすべてブロックすることにより、トータリースタブを設定します。

```
Console(config-router)#area 2 stub no-summary
Console(config-router)#
```

関連するコマンド

area default-cost (P638)

area virtual-link

バーチャルリンクを設定します。バーチャルリンクを削除するには、オプションキーワードなしでコマンドの前に ”no” を付けます。属性のデフォルト値をリストアするには、必要なキーワードの前に ”no” を付けます。

文法

area area-id virtual-link router-id
[dead-interval seconds] [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds]

no area area-id virtual-link router-id
[dead-interval | hello-interval | retransmit-interval | transmit-delay]

- area-id - **仮想リンクの通過エリアを表します。エリア** ID **は** IPv4 **アドレス、または** 0-4294967295 **までの** 4 **桁のオクテットで表記します。**
- router-id - **仮想リンクの隣接ルータのルータ** ID **です。このルータは、仮想リンクの他方の端にあるバックボーンとトランジットエリア両方に隣接するエリア境界ルータ（**ABR**）である必要があります。**
  - dead-interval seconds - **ルータのダウンを宣言する前に、隣接ルータが** Hello **パケットを待機する時間です。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲** : 1 **〜** 65535 **秒、デフォルト** : 4 × Hello **間隔、または** 40 **秒）。**
  - hello-interval seconds - Hello **パケット送信間の伝送遅延を指定します。**Hello **間隔を小さい値に設定すると、トポロジ変更を検知する際の遅延は短縮されますが、ルーティング トラフィックは増加します。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲** : 1 **〜** 65535 **秒、デフォルト** : 10 **秒）。(** **有効範囲** : 1-65535 seconds; Default: 10 **秒**)
- retransmit-interval seconds - ABR **が仮想リンク上でリンクステートアドバタイズメント（**LSA**）を再送信する間隔を指定します。この送信間隔は、ルーティング情報の適切なフローを提供しつつも、不必要なプロトコル トラフィックを発生させない程度の控えめな値に設定してください。ただし、この値は、仮想リンクの値よりは大きく設定する必要があることに注意してください（範囲** : 1 **〜** 3600 **秒、デフォルト** : 5 **秒）。**
- transmit-delay seconds - **仮想リンク上でリンクステート アップデート パケットを送信するのに必要な時間を、伝送遅延および伝播遅延を考慮に入れて予測します。**LSA **のエージには、この値が送信前に加算されます。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲** : 1 **〜** 3600 **秒、デフォルト** : 1 **秒）。**

コマンドモード

Router Configuration

初期設定

area-id: None
router-id: None
hello-interval: 10 秒
retransmit-interval: 5 秒
transmit-delay: 1 second
dead-interval: 40 秒

コマンド解説

- 自律システム内のルーティングの接続性を維持するには、すべてのエリアをバックボーンエリア (0.0.0.0) に接続する必要があります。バックボーンのエリアに物理的に接続することができない場合は、仮想リンクを使用することができます。仮想リンクでは、隔離されたエリアのバックボーンに論理パスを提供したり、バックボーンへの通常の接続に失敗した場合はバックアップ接続を設定し引き継ぐことができます。
- バックボーン以外の共通のエリアのインタフェースをもつ 2 つのバックボーンルータ間で仮想リンクを設定することが可能です。仮想リンクで接続された２つのルータは、ポイント間通信ネットワークで接続されているように見なされます。
- バックボーンに接続されていないエリアには、バックボーンに接続されているトランジットエリア ID および仮想リンク隣接ルータの ID を含む必要があります。

例

ここでは、オプションのパラメータのデフォルト値を使って仮想リンクを設定します。

```
Console(config-router)#area 3 virtual-link 192.168.0.9
Console(config-router)#
```

ipv6 router ospf area

OSPF エリアを選択したインタフェースにバインドします。コマンドの前に "no" を付けることにより、OSPF エリアは削除され、OSPF プロセスは無効になるか、インタフェースからインスタンスの識別子が削除されます。

文法

[no] ipv6 router ospf area area-id [tag process-name |
instance-id instance-id]

- area-id - 現行のレイヤ 3 インタフェースにバインドするためのエリアです。OSPF エリアは共通のルーティング情報を共有するルータのグループを表します。エリア ID は、IPv4 アドレス、または 0-4294967295 までの 4 桁のオクテットで表記します。
- process-name - 複数のルーティングインスタンスを設定する場合は、プロセス名を入力してください (有効範囲 : 16 文字以内の英数字)
- instance-id - インタフェースに接続されたリンクローカルネットワーク上の特定の OSPFv3 ルーティングプロセスを表します (有効範囲 : 0-255)。

コマンドモード

Interface Configuration

初期設定

None

コマンド解説

- area-id は、OSPF ブロードキャストエリアを固有に設定します。エリア ID の 0.0.0.0 は、自律システムの OSPF バックボーンを指します。ルータはそれぞれバックボーンに直接接続するか、仮想リンクを介して接続する必要があります。
- ネットワークセグメント上のルータのエリア ID はすべて同じ値に設定してください。
- process-name は、各ルーティングプロセス間で区別するためにローカルルータ上でのみ使用します。ipv6 router ospf area コマンドを使用する前に router ipv6 ospf コマンドを使って設定してください。
- instance-id は、同じリンク上で動作するルーティングプロセス間を区別するために、リンクローカルネットワークセグメント上で使用することにより、ルータは隣接情報を設定したり、ルーティング情報を交換するために共通のルーティングプロセスで設定できるようにします。
- バックボーン (エリア 0.0.0.0) は、その他のエリアの前に設定してください。

例

ここでは、バックボーン 0.0.0.0 を設定します。

```
Console(config)#router ipv6 ospf tag 0
Console(config-router)#router-id 192.168.0.2
Console(config-router)#exit
Console(config)#interface vlan 1
Console(config-if)#ipv6 router ospf area 0 tag 0 instance-id 0
Console(config-if)#
```

関連するコマンド

router-id (P630)
ipv6 router ospf tag area (P690)

ipv6 router ospf tag area

OSPF エリアを選択したインタフェースおよびプロセスにバインドします。コマンドの前に "no" を付けることにより、指定したエリアをインタフェースから削除します。

文法

[no] ipv6 router ospf tag process-name area area-id
[instance-id instance-id]

- area-id は、OSPF ブロードキャストエリアを固有に設定します。エリア ID の 0.0.0.0 は、自律システムの OSPF バックボーンを指します。ルータはそれぞれバックボーンに直接接続するか、仮想リンクを介して接続する必要があります。エリア ID は IPv4 アドレス、または 0-4294967295 までの 4 桁のオクテットで表記します。
- process-name は、各ルーティングプロセス間で区別するためにローカルルータ上でのみ使用します。ipv6 router ospf area コマンドを使用する前に router ipv6 ospf コマンドを使って設定してください (有効範囲 : 16 文字以内の英数字)。
- instance-id は、同じリンク上で動作するルーティングプロセス間を区別するために、リンクローカルネットワークセグメント上で使用することにより、ルータは隣接情報を設定したり、ルーティング情報を交換するために共通のルーティングプロセスで設定できるようにします (有効範囲 : 0-255)。

コマンドモード

Interface Configuration (VLAN)

初期設定

No areas are defined.

コマンド解説

- area-id は、OSPF ブロードキャストエリアを固有に設定します。エリア ID の 0.0.0.0 は、自律システムの OSPF バックボーンを指します。ルータはそれぞれバックボーンに直接接続するか、仮想リンクを介して接続する必要があります。
- ネットワークセグメント上のルータのエリア ID はすべて同じ値に設定してください。
- process-name は、各ルーティングプロセス間で区別するためにローカルルータ上でのみ使用します。ipv6 router ospf area コマンドを使用する前に router ipv6 ospf コマンドを使って設定してください。
- instance-id は、同じリンク上で動作するルーティングプロセス間を区別するために、リンクローカルネットワークセグメント上で使用することにより、ルータは隣接情報を設定したり、ルーティング情報を交換するために共通のルーティングプロセスで設定できるようにします。
- バックボーン (エリア 0.0.0.0) は、その他のエリアの前に設定してください。

例

ここでは、エリア 0.0.0.1 **をルーティングプロセス** “1” **で現在選択されているインタフェースに割り当てます。**

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 router ospf tag 1 area 0.0.0.1
Console(config-if)#
```

関連するコマンド

router ipv6 ospf (P629)
router-id (P630)
ipv6 router ospf tag area (P690)

ipv6 ospf cost

インタフェース上のプロトコルパケットの送信するコストを設定します。この値が大きいと、ポートの通信速度が遅くなります。コマンドの前に "no" **を付けることによりデフォルト値に戻ります。**

文法

ipv6 ospf cost cost [instance-id instance-id]

no ipv6 ospf cost [instance-id instance-id]

- cost - **インタフェースのリンクメトリック。この値が大きいと、ポートの通信速度が遅くなります** (**有効範囲** : 1-65535)**。**
- instance-id - **このインタフェースに接続されたリンクローカルネットワークセグメント上の特定の** OSPFv3 **ルーティングプロセスを表します** (**有効範囲** : 0-255)**。**

コマンドモード

Interface Configuration (VLAN)

初期設定

1

コマンド解説

- **インタフェースコストは、特定のインタフェース間のパケットを送信するために必要ないオーバーヘッドを表します。ルータリンクステートアドバタイズメントのリンクコストとしてアドバタイズします。**
- **ルートは、ルート内の各インタフェースリンクごとにすべてのメトリックの合計に等しいメトリックに割り当てられます。**
- **このルートは、すべてのインタフェースに対してデフォルトのコストを使用します。そのため、**10 **ギガビットのモジュールをインストールする場合は、実際のインタフェースの帯域を確保するために、**1 Gbps **ポートの** VLAN **インタフェースのコストを** 1 **よりも大きい値にリセットしてください。**

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf cost 10
Console(config-if)#
```

ipv6 ospf dead-interval

hello パケットの送信間隔を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ipv6 ospf dead-interval seconds [instance-id instance-id]

no ipv6 ospf dead-interval [instance-id instance-id]

- seconds - ルータのダウンを宣言する前に、隣接ルータが Hello パケットを待機する時間です。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲 : 1 〜 65535 秒）。
- instance-id - インタフェースに接続されたリンクローカルネットワークセグメント上の特定の OSPFv3 ルーティングプロセスを指します (有効範囲 : 0-255)。

コマンドモード

Interface Configuration (VLAN)

初期設定

40 秒、または ipv6 ospf hello-interval コマンドによって指定した間隔の 4 倍。

コマンド解説

- dead-interval はルータの hello パケットにアドバタイズされます。hello-interval の倍数、かつ特定のネットワーク上のルータはすべて同じ値でなければなりません。

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf dead-interval 50
Console(config-if)#
```

関連するコマンド

ipv6 ospf hello-interval (P694)

ipv6 ospf hello-interval

インタフェース上の hello **パケットの送信間隔を指定します。コマンドの前に** "no" **を付けることにより、デフォルト値に戻ります。**

文法

ipv6 ospf hello-interval seconds [instance-id instance-id]

no ipv6 ospf hello-interval [instance-id instance-id]

- seconds - **インタフェースからの** hello **パケットの送信間隔。ネットワーク上のルータすべての値は同じ値に設定して下さい** (**有効範囲** : 1-65535)。
- instance-id - **このインタフェースに接続されているリンクローカルネットワークセグメント上の特定の** OSPFv3 **ルーティングプロセスを指します** (**有効範囲** : 0-255)。

コマンドモード

Interface Configuration (VLAN)

初期設定

10 **秒**

コマンド解説

- Hello **パケットにより、送信元のルータが現在アクティブであることを知らせます。** hello **の送信間隔を設定する場合、値が小さいと、トポロジの変更を検出する際の遅延を軽減することができますが、ルーティングのトラフィックが大きくなってしまいます。**

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf hello-interval 5
Console(config-if)#
```

関連するコマンド

ipv6 ospf dead-interval (P693)

ipv6 ospf priority

エリアの DR**（指定ルータ）および** BDR(**バックアップ指定ルータ）を決定する際に使用するルータのプライオリティを設定します。コマンドの前に** "no" **を付けることにより、デフォルト値に戻ります。**

文法

ipv6 ospf priority priority [instance-id instance-id]

no ipv6 ospf priority [instance-id instance-id]

- priority - **ルータのインタフェースのプライオリティを設定します** (**有効範囲** : 0-255)。
- instance-id - **このインタフェースに接続されているリンクローカルネットワーク上の特定の** OSPFv3 **ルーティングプロセスを指します** (**有効範囲** : 0-255)。

コマンドモード

Interface Configuration (VLAN)

初期設定

1

コマンド解説

- **それぞれの** OSPF **ごとに** OSPF **エリアエリアの** DR**（指定ルータ）および** BDR(**バックアップ指定ルータ）は、ルータのプライオリティに応じて** OSPFA **エリアごとに設定されます。**DR **は、エリア内のその他のルータすべて有効な接続を行って、ルーティングトポロジー情報を交換します。**DR **が何らかの理由で失敗した場合は、**BDR **がその役割を引き継ぎます。**
- **プライオリティを** ”0” **に設定すると、ルータを** DR**、または** BDR **に割り当てられないように設定することができます。プライオリティの値を** ”0” **以外に設定すると、プライオリティが一番高いルータが** DR**、次にプライオリティの高いルータが** BDR **になります。２つ以上のルータのプライオリティが同じ場合は、**ID **の高いルータが選択されます。**
- **ネットワーク上に** DR **が既に存在する場合は、新しいルータは独自のプライオリティに関係なく、現行の** DR **を受け入れます。**
- **ルータのプライオリティは、マルチアクセス用ネットワーク用であり、ポイント間通信のネットワーク向けではありません。**

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf priority 5
Console(config-if)#
```

ipv6 ospf retransmit-interval

LSA（link-state advertisements）の再送間隔を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ipv6 ospf retransmit-interval seconds [instance-id instance-id]

no ipv6 ospf retransmit-interval [instance-id instance-id]

- seconds - インタフェースからの LSA の再送間隔を設定します (有効範囲 : 1-65535)。
- instance-id - インタフェースに接続されているリンクローカルネットワーク上の特定の OSPFv3 ルーティングプロセスを指します (有効範囲 : 0-255)。

コマンドモード

Interface Configuration (VLAN)

初期設定

5 秒

コマンド解説

- ルータは指定した再送後に LSA を受信しない場合は、近隣ルータに LSA を再送します。この送信間隔は、ルーティング情報の適切なフローを提供しつつも、不必要なプロトコル トラフィックを発生させない程度の控えめな値に設定してください。ただし、この値は、仮想リンクの値よりは大きく設定する必要があることに注意してください（範囲 : 1 ～ 3600 秒、デフォルト : 5 秒）。
- 不要な再送を避けるには、送信間隔を接続したネットワーク上の 2 つのルータ間の往復遅延時間の値よりも大きい値に設定してください。

例

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf retransmit-interval 7
Console(config-if)#
```

ipv6 ospf transmit-delay

インタフェース上のリンクステートアップデートパケットを送信するための予測時間を設定します。

コマンドの前に "no" **を付けることにより、デフォルト値に戻ります。**

文法

ipv6 ospf transmit-delay seconds [instance-id instance-id]

no ipv6 ospf transmit-delay [instance-id instance-id]

- seconds - **リンクステートアップデートを送信するために必要な予測時間を設定します** (**有効範囲** : 1-65535)
- instance-id - **インタフェースに接続しているリンクローカルネットワーク上の特定の** OSPFv3 **ルーティングプロセスを指します** (**有効範囲** : 0-255)

コマンドモード

Interface Configuration (VLAN)

初期設定

1 **秒**

コマンド解説

- LSA **の時間は、再送前の遅延が加算されます。送信遅延を予測する際は、送信および伝搬遅延の両方を考慮して下さい。通信速度に応じて送信遅延を設定する場合は、通信速度の低いリンクよりも値を大きくしてください。遅延が加算されない場合、ルーティングプロセスではリンク上の** LSA **の送信に要する時間は考慮されません。通信速度が遅いリンクの場合、デバイスがパケットを受信するよりも早くパケットを送信してしまいます。この問題を回避するためには、送信遅延時間を使って通信間の時間を制御します。**

例：

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf transmit-delay 6
Console(config-if)#
```

passive-interface

指定したインタフェース上の OSPF **のルーティングトラフィックを抑制します。コマンドの前に** "no" **を付けることにより、指定したインタフェース上でルーティングトラフィックを送受信できるようになります。**

文法

[no] passive-interface vlan vlan-id [ipv6-address]

- vlan-id - VLAN ID(**有効範囲** : 1-4093)
- ipv6-address - **ネットワークプレフィックスとホスト・アドレスのビット数を含む完全な** IPv6 **アドレス。**

コマンドモード

Router Configuration

初期設定

None

コマンド解説

- OSPF **インタフェースを無効にして、既存のインタフェースからの** OSPF **ルーティングトラフィックを回避することが可能です。関連のあるインタフェースの１つを受動モードに設定されている場合は、隣接する** OSPF **ルータを設定することができません。指定したインタフェースは、**OSPF **ドメインのスタブとして表示されます。また既存の隣接ルータがある時に** OSPF **インタフェースを無効にすると、隣接ルータは即時破棄します。**

例：

```
Console(config-router)#passive-interface vlan 1 73::9
Console(config-router)#
```

show ipv6 ospf

ルーティング設定についての基本情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ipv6 ospf
  Routing Process "ospf 1" with ID 192.168.0.2
 Process uptime is 24 minutes
 Supports only single TOS(TOS0) routes
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Number of incoming concurrent DD exchange neighbors 0/5
 Number of outgoing concurrent DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of LSA received 0
 Number of areas attached to this router: 2

    Area 0.0.0.0 (BACKBONE)
        SPF algorithm executed 2 times
        Number of LSA 1. Checksum 0x001aa9
    Area 0.0.0.1
        SPF algorithm executed 2 times
        Number of LSA 1. Checksum 0x001aa9

Console#
```

コマンド	機能
Routing Process	
Routing Process	OSPF プロセス名およびルータ ID。ルータ ID は、自律システムのルータを固有に識別します。慣例により、通常ルータの IP インタフェースアドレスの１つに設定されます。
Process uptime	プロセスが稼働している時間
Supports only single TOS (TOS0) routes	OSPF Version 2 で指定されているオプションの ToS(Type of Service) 。Appendix F.1.2 はサポートされていませんが、インタフェースごとのコストのみ１つずつ割り当てられます。
SPF schedule delay	トポロジー変更通知を受信してから SPF 計算を開始するまでの遅延時間。
Hold time	2 つの連続する SPF 計算間の待ち時間を設定します。
Number of concurrent DD exchange neighbors	DVD(database descriptor) パケットを現在変換しているネイバールータの数。
Number of external LSA	リンクステートデータベース内の外部リンクステートアドバタイズメント (Type 5 LSAs) の数。これらの LSA は、自律システム以外のルートについての情報をアドバタイズします。

Checksum	リンクステートデータベースに含まれる外部リンクステートアドバタイズメントの LS チェックサムの合計。
Number of opaque AS LSA	リンクステートデータベースの不透明なリンクステートアドバタイズメント Type 9, 10 および 11 LSAs) の数。これらの SLA は、外部のアプリケーションについての情報をアドバタイズして、正しい再開プロセスの OSPF によってのみ使用されます。
Checksum	リンクステートデータベースに含まれる不透明なリンクステートアドバタイズメントの LS チェックサムの合計。
Number of LSA received	受信されているリンクステートアドバタイズメント数。
Number of areas attached to this router	ルータへの接続先の設定されているエリアの数。
Area Information	
Area	エリアの識別子。インタフェースに対して IPv6 アドレスが設定されていない場合は、“(Inactive)” と表示されます。
SPF algorithm executed x times	このエリアでの最短パスの最初のアリゴリズムの実行回数。
Number of LSA	AS External LSA を除く、エリアのリンクステートデータベース内のリンクステートアドバタイズメントの総数。
Checksum	リンクステートデータベースに含まれるネットワーク（エリア）のリンクステートアドバタイズメントの LS チェックサムの総数。

show ipv6 ospf database

ルータのデータベースにストアされている各 OSPF リンクステートアドバタイズメントについての情報を表示します。

文法

show ipv6 ospf [tag process-id] database

- process-id - **情報を表示するルータのプロセスの** ID(**有効範囲** : 1-10)

コマンドモード

Privileged Exec

例：

以下に、show ip ospf database **コマンドの出力を表示します。**

```
Console#show ipv6 ospf database

            OSPF Router with ID (192.168.0.2) (TAG: 1)

                Link-LSA
Link State ID   ADV Router      Age  Seq#       CkSum    Link
1001            192.168.0.2       71 0x80000001 0x06b7     0

                        Router-LSA (Area 0)
Link State ID   ADV Router      Age  Seq#       CkSum
0               192.168.0.2       31 0x80000002 0x14b1

                AS-external-LSA
Link State ID   ADV Router      Age  Seq#       CkSum
Console#
```

コマンド	機能
OSPF Router Process with ID	OSPF **ルータの** ID **およびプロセス** ID。**ルータ** ID **は自律システムのルータを固有に識別します。したがって、これはルータの** IP **インタフェースのアドレスの** 1 **つに設定されます。**
Link State ID	**このフィールドは、アドバタイズメントで記述されているルーティングドメインの一部を指します。**
ADV Router	**アドバタイズ元のルータ** ID
Age	Age of LSA (**秒単位**)
Seq#	LSA **のシーケンス番号（古い重複した** LSA **の検出に使用されます）**
CkSum	LSA **の完全なコンテントのチェックサム**
Link	**ルータに接続されているインタフェース数**

show ipv6 ospf interface

OSPF **インタフェースのサマリ情報を表示します。**

文法

show ipv6 ospf interface [vlan vlan-id]

- vlan-id - VLAN ID (**有効範囲** : 1-4093)

コマンドモード

Privileged Exec

例

```
Console#show ipv6 ospf interface vlan 1
 VLAN 1 is up, line protocol is up
 Link local Address FE80::200:E8FF:FE93:82A0/64, Area 0.0.0.0
 Tag 1, Router ID 192.168.0.2, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 192.168.0.2, Interface Address
FE80::200:E8FF:FE93:82A0
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
 Neighbor Count is 0, Adjacent neighbor count is 0
 Hello received 0 sent 92, DD received 0 sent 0
 LS-Req received 0 sent 0, LS-Upd received 0 sent 0
 LS-Ack received 0 sent 0, Discarded 0
Console#
```

コマンド	機能
State	Backup – バックアップ指定のルータ Down – OSPF はインタフェース上で有効であるが、インタフェースがダウンしています。 DR – 指定ルータ（Designated Router）です。 DROther – インタフェースはマルチアクセス ネットワーク上にありますが、DR または BDR ではありません。 Loopback – ループバック インタフェースです。 PointToPoint – 2 つのルータ間は直接リンクされています。 Waiting – ルータは DR と BDR を見つけようとしています。
Priority	ルータのプライオリティ
Designated Router	指定のルータ ID および各インタフェースのアドレス
Backup Designated Router	バックアップ指定のルータ ID および各インタフェースアドレス
Timer intervals	タイマー間隔（Hello 間隔、Dead 間隔、Retransmit 間隔を含む）のコンフィグレーション設定
Neighbor Count	ネットワークネイバールートおよび近隣ネイバー数 Count of network neighbors and adjacent neighbors
Hello	Number of Hello LSAs の送受信回数
DD	Database Descriptor パケットの送受信回数
LS-Req	LSA の要求回数
LS-Upd	LSA のアップデート回数
LS-Ack	LSA の認識回数
Discarded	LSAs の破棄した回数

show ipv6 ospf neighbor

OSPF **エリア内の各インタフェース上のネイバールータについての情報を表示します。**

文法

show ipv6 ospf [tag process-id] neighbor

- process-id - **情報を表示するルータのプロセスの** ID(**有効範囲** : 1-10)

コマンドモード

Privileged Exec

例：

```
Console#show ipv6 ospf neighbor

       ID         Pri        State       Interface ID     Interface
--------------- ------ ---------------- --------------- ---------
    192.168.0.2      1          FULL/DR            1001    vlan1
Console#
```

show ipv6 ospf route

OSPF **ルーティングテーブルを表示します。**

文法

show ipv6 ospf [tag process-id] route

process-id - **情報を表示するルータのプロセスの** ID(**有効範囲** : 1-10)

コマンドモード

Privileged Exec

例：

```
Console#show ipv6 ospf route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
C    ::1/128, lo0
O    2001:DB8:2222:7272::/64, VLAN1
C    2001:DB8:2222:7272::/64, VLAN1
?    FE80::/64, VLAN1 inactive
C    FE80::/64, VLAN1
?    FF00::/8, VLAN1 inactive

Console#
```

show ipv6 ospf virtual-links

仮想リンクの詳細情報を表示します。

文法

show ipv6 ospf [tag process-id] virtual-links

process-id - **情報を表示するルータのプロセスの** ID(**有効範囲** : 1-10)

コマンドモード

Privileged Exec

例：

```
Console#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 192.168.0.2 is up
  Transit area 0.0.0.1 via interface VLAN1
  Local address 192.168.0.3
  Remote address 192.168.0.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:02
    Adjacency state Full
Console#
```

コマンド	機能
Virtual Link to router	OSPF **ネイバーおよびリンク状態** (up/down)
Transit area	**仮想リンクがターゲット ルータに到達するために横断する共通エリア**
Local address	ABR **の** IP **アドレス** (**共通のトランジットエリアに孤立したエリアを接続するエンドポイントとしての役割**)
Remote address	**仮想ネイバーが使用している** IP **アドレス。ネイバーの** ABR **は、バックボーンに共通の伝送領域を接続するエンドポントでなければなりません。**
Transmit Delay	**仮想リンク上の伝送遅延の期待値** (**秒単位**) **。**
Timer intervals	**タイマー間隔（**Hello **間隔、**Dead **間隔、**Retransmit **間隔を含む）のコンフィグレーション設定**
Hello due	**ネイバーからの** hello **メッセージを受信するまでのタイムアウト**

Adjacency state	各状態は、次のとおりです。 Down - 接続がダウンしています。 Attempt - 接続はダウンしているが、コンタクトが試みられています（非ブロードキャスト ネットワーク用）。 Init - Hello パケットは受信されたが、通信はまだ確立されていません。 Two-way - 双方向通信が確立しています。 ExStart - 隣接ルータ間の隣接性を初期化しています。 Exchange - データベース記述を交換しています。 Loading - LSA データベースを交換しています。 Full - 隣接ルータは完全に隣接関係にあります。

関連するコマンド

area virtual-link (P646)

1.32 マルチキャストルーティングコマンド

マルチキャストルータは、各種マルチキャストルーティングプロトコルを使用して、各サブネット間のマルチキャストパケットを伝送します。このルータは PIM(Protocol Independent Multicasting) をサポートしています。

[注意] IGMP はマルチキャストルーティングを使用しているインタフェースに対して有効です。

コマンドグループ	機能
マルチキャストルーティング	IP マルチキャストルーティングをグローバルで有効にします。またスタティックおよびダイナミックルーティング情報から設定された IP マルチキャストルーティングテーブルをを表示します。
スタティックマルチキャストルーティング	スタティックマルチキャストルータポートを設定します。
PIM マルチキャストフィルタリング	PIM-DM および PIM-SM のグローバルおよびインタフェースの設定を行います。

1.32.1 マルチキャストルーティング

ここでは、グローバルでマルチキャストルーティング に使用するコマンドについて説明します。

コマンド	機能		
IPv4 Commands			
ip multicast-routing	IPv4 マルチキャストルーティングを有効にします。	GC	P709
show ip mroute	IPv4 マルチキャストルーティングテーブルを表示します。	PE	P710
IPv6 Commands			
ipv6 multicast-routing	IPv6 マルチキャストルーティングを有効にします。	GC	P713
show ipv6 mroute	IPv6 マルチキャストルーティングテーブルを表示します。	PE	P713

ip multicast-routing

IPv4 マルチキャストルーティングを有効にします。multicast routing コマンドの前に "no" を付けることにより IP マルチキャストルーティングは無効になります。

文法

[no] ip multicast-routing

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- ルータの IPv4 マルチキャストルーティングをグローバルに有効にします。特定のマルチキャストルーティングプロトコルは、router pim コマンドを使ってマルチキャストルーティングをサポートしているインタフェース上で有効にしてから、ip pim dense-mode、または ip pim sparse-mode コマンドを使ってマルチキャストルーティングをサポートしているインタフェースを指定する必要があります。
- マルチキャストルーティングを使用すると、IGMP proxy はデバイスのインタフェース上で無効になります (「igmp proxy 」を参照してください)。

例：

```
Console(config)#ip multicast-routing
Console(config)#
```

show ip mroute

IPv4 マルチキャストルーティングテーブルを表示します。

文法

show ip mroute [group-address source] [summary]

- group-address - ルータに直接接続されているサブスクライバ、またはルータからのダウンストリームをもつ Pv4 マルチキャストグループのアドレスを指します。
- source - マルチキャストデリバリツリーのルートの IPv4 サブネットワークを指します。サブネットワークには、認識されているマルチキャストソースが含まれます。
- summary - IP マルチキャストルーティングテーブルの各エントリのサマリ情報を表示します。

コマンドモード

Privileged Exec

コマンド解説

- マルチキャストルーティングの情報を表示します。オプションのないパラメータを選択すると、マルチキャストアドレステーブル の各エントリの詳細情報が表示されます。
- マルチキャストグループおよびソースペアを選択すると、指定したエントリの詳細情報が表示されます。summary オプションを選択すると、各エントリの概略リストが１行ずつ表示されます。

例：

ここでは、指定したグループ / ソースペアのマルチキャスト情報の詳細が表示されます。

```
Console#show ip mroute 224.0.255.3 192.111.46.8

IP Multicast Forwarding is enabled.

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Channel, C - Connected, P -
Pruned,
       F - Register flag, R - RPT-bit set, T - SPT-bit set, J -
Join SPT
Interface state: F - Forwarding, P - Pruned, L - Local

(192.168.2.1, 224.0.17.17), uptime 00:00:05
Owner: PIM-DM, Flags: D
Incoming Interface: VLAN2, RPF neighbor: 192.168.2.1
Outgoing Interface List:
VLAN1(F)

Console#
```

コマンド	機能

Flags	エントリに関連のあるフラグは以下のとおりです。 D (Dense) - PIM Dense モードは使用中です。 S (Sparse) - PIM Sparse モードは使用中です。 s (SSM) - PIM-SSM に使用される IP アドレスの範囲のマルチキャストグループ C (Connected) - マルチキャストグループのメンバがインタフェース上に表示されます。 P (Pruned) - このルートは終端されています。 F (Register flag) - このデバイスはマルチキャストソースに登録されています。 R (RP-bit set) - エントリ (S,G) は、RP(Rendezvous Point) を指し、通常特定のソースの共有ツリーと併せて Prune 状態を表します。 T (SPT-bit set) - マルチキャストパケットは 最短パスツリーのソースから受信してされいています。 J (Join SPT) - 共用ツリーで受信したトラフィック速度がこのグループの SPT-threshold を超えています。(*,G) エントリに SPT フラグを設定した場合、次に (S,G) パケットを受信すると、ルータは最短パスツリーに結合されます。(S,G) に SPT フラグを設定すると、ルータは最短パスツリーに結合されます。
Interface state	表示されているインタフェースのマルチキャストの状態を表します。
group address	リクエストされているサービスの IP マルチキャストグループのアドレスを指します。
source	IP マルチキャストソースを含むサブネットワークを指します。
uptime	エントリが作成されてからの経過時間を指します。
Owner	関連のマルチキャストプロトコル (PIM) を指します。
Incoming Interface	アップストリームネイバーに接続されているインタフェース PIM は ユニキャストルーティングテーブルに応じて、マルチキャストルーティングツリーを設定します。関連のあるユニキャストルーティングテーブルが存在しない場合は、PIM は マルチキャストルーティングエントリを設定しますが、アップストリームインタフェースに “Null” と表示され、ユニキャストルーティングテーブルは無効になります。このフィールドに ”Register” と表示されると、pseudo インタフェースが PIM-SM レジスタパケットの送受信に使用されていることを表します。
RPF neighbor	このグループのアップストリームのマルチキャストルータの IP アドレス
Outgoing interface list and flags	マルチキャストサブスクライバが記録されているインタフェースです。各インタフェースに関連のあるフラグは以下のとおりです。 F (Register flag) - このデバイスはマルチキャストソースに登録されています。 P (Pruned) - このルートは終端されています。 L (Local) - ダウンストリームインタフェースがサブネットのホストから IGMP レポートメッセージを受信しました。

ここでは、サマリ形式でマルチキャストテーブルのエントリをすべて表示します。

```
Console#show ip mroute summary

IP Multicast Forwarding is enabled

IP Multicast Routing Table (Summary)
Flags: F – Forwarding,  P - Pruned
     Group         Source        Source Mask    Interface  Owner
Flags
--------------- --------------- --------------- ---------- ------
- ------
    224.0.17.17     192.168.2.1 255.255.255.255 VLAN2      PIM-DM
F
 Total Entry is 1

Console#
```

ipv6 multicast-routing

IPv6 マルチキャストルーティングを有効にします。コマンドの前に "no" を付けることにより IP マルチキャストルーティングは無効になります。

文法

[no] iv6p multicast-routing

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- ルータの IPv6 マルチキャストルーティングをグローバルに有効にします。特定のマルチキャストルーティングプロトコルは、router pim6 コマンドを使ってマルチキャストルーティングをサポートしているインタフェース上で有効にしてから、ipv6 pim dense-mode コマンドを使ってマルチキャストルーティングをサポートしているインタフェースを指定する必要があります。
- マルチキャストルーティングを使用するには、デバイスのインタフェース上で MLD proxy を有効に設定できません (「ipv6 mld proxy」(P492) を参照ください)。

例：

```
Console(config)#ipv6 multicast-routing
Console(config)#
```

show ipv6 mroute

IPv6 マルチキャストルーティングテーブルを表示します。

文法

show ipv6 mroute [group-address source] [summary]

- group-address - ルータに直接接続されているサブスクライバ、またはルータからのダウンストリームをもつ Pv4 マルチキャストグループのアドレスを指します。
- source - マルチキャストデリバリツリーのルートの IPv4 サブネットワークを指します。サブネットワークには、認識されているマルチキャストソースが含まれます。
- summary - IP マルチキャストルーティングテーブルの各エントリのサマリ情報を表示します。

コマンドモード

Privileged Exec

コマンド解説

- マルチキャストルーティングの情報を表示します。オプションのないパラメータを選択すると、マルチキャストアドレステーブル の各エントリの詳細情報が表示されます。
- マルチキャストグループおよびソースペアを選択すると、指定したエントリの詳細情報が表示されます。summary オプションを選択すると、各エントリの概略リストが１行ずつ表示されます。

例：

ここでは、指定したグループ / ソースペアのマルチキャスト情報の詳細が表示されます。

```
Console#show ipv6 mroute FF02::0101 FE80::0202

IP Multicast Forwarding is enabled.

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Channel, C - Connected, P - Pruned,
       F - Register flag, R - RPT-bit set, T - SPT-bit set, J - Join SPT
Interface state: F - Forwarding, P - Pruned, L - Local

(FF02::0101, FE80::0202), uptime 00:00:05
Owner: PIM-DM, Flags: D
Incoming Interface: VLAN2, RPF neighbor: FE80::0303
Outgoing Interface List:
VLAN1(F)
Console#
```

コマンド	機能
Flags	エントリに関連のあるフラグは以下のとおりです。 • D (Dense) - PIM Dense モードは使用中です。 • S (Sparse) - PIM Sparse モードは使用中です。 • s (SSM) - PIM-SSM に使用される IP アドレスの範囲のマルチキャストグループ • C (Connected) - マルチキャストグループのメンバがインタフェース上に表示されます。 • P (Pruned) - このルートは終端されています。 • F (Register flag) - このデバイスはマルチキャストソースに登録されています。 • R (RP-bit set) - エントリ (S,G) は、RP(Rendezvous Point) を指し、通常特定のソースの共有ツリーと併せて Prune 状態を表します。 • T (SPT-bit set) - マルチキャストパケットは 最短パスツリーのソースから受信してされいています。 • J (Join SPT) - 共用ツリーで受信したトラフィック速度がこのグループの SPT-threshold を超えています。(*,G) エントリに SPT フラグを設定した場合、次に (S,G) パケットを受信すると、ルータは最短パスツリーに結合されます。(S,G) に SPT フラグを設定すると、ルータは最短パスツリーに結合されます。
Interface state	表示されているインタフェースのマルチキャストの状態を表します。
group address	リクエストされているサービスの IP マルチキャストグループのアドレスを指します。
source	IP マルチキャストソースを含むサブネットワークを指します。
uptime	エントリが作成されてからの経過時間を指します。
Owner	関連のマルチキャストプロトコル (PIM) を指します。
Incoming Interface	アップストリームネイバーに接続されているインタフェース PIM は ユニキャストルーティングテーブルに応じて、マルチキャストルーティングツリーを設定します。 関連のあるユニキャストルーティングテーブルが存在しない場合は、PIM は マルチキャストルーティングエントリを設定しますが、アップストリームインタフェースに “Null” と表示され、ユニキャストルーティングテーブルは無効になります。このフィールドに ”Register” と表示されると、pseudo インタフェースが PIM-SM レジスタパケットの送受信に使用されていることを表します。
RPF neighbor	このグループのアップストリームのマルチキャストルータの IP アドレス
Outgoing interface list and flags	マルチキャストサブスクライバが記録されているインタフェースです。各インタフェースに関連のあるフラグは以下のとおりです。 • F (Register flag) - このデバイスはマルチキャストソースに登録されています。 • P (Pruned) - このルートは終端されています。 • L (Local) - ダウンストリームインタフェースがサブネットのホストから IGMP レポートメッセージを受信しました。

ここでは、サマリ形式でマルチキャストテーブルのエントリをすべて表示します。

```
Console#show ipv6 mroute summary

IP Multicast Forwarding is disabled

IP Multicast Routing Table (Summary)
Flags:  F - Forwarding, P - Pruned, D - PIM-DM, S – PIM-SM, V – DVMRP,
        M - MLD
Group                          Source                          Interface  Flag
------------------------------ ------------------------------  ---------- ----
                 FF02::0101                                    FE80::0101 VLAN 4096   DF
Total Entry is 1
Console#
```

1.32.2 スタティックマルチキャストルーティング

ここでは、本機のスタティックマルチキャストルートの設定に使用するコマンドについて説明します。

コマンド	機能	モード	ページ
ip igmp snooping vlan mrouter	**マルチキャストルータポートを追加します。**	GC	P717
show ip igmp snooping mrouter	**マルチキャストルータポートを表示します。**	PE	P718

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。コマンドの前に "no" **を付けることにより、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 (**有効範囲** : 1-4093)
- interface
  - ethernet unit/port

    unit - **スタックユニット** (**有効範囲** : 1-8)

    port - **ポート番号** (**有効範囲** : 1-26)
  - port-channel channel-id (**有効範囲** : 1-32)

初期設定

スタティックマルチキャストルータの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

- **お使いのネットワークの接続状況に応じて、**IGMP **スヌーピングは** IGMP **クエリアを検出することができます。そのため、**IGMP **クエリアがお使いのルータのインタフェース（ポート、またはトランク）にネットワークを介して接続されているマルチキャストルータ** / **スイッチであれば、インタフェースを自動的に設定し、現行のマルチキャストグループをすべ設定することができます。**

例：

ここでは、port 11 を VLAN 1 のマルチキャストルータポートとして設定する方法について説明します。

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

マルチキャストルータのポートを静的に設定し、かつ動的に学習した情報について表示します。

文法

show ip igmp snooping mrouter [vlan vlan-id]

vlan-id - VLAN ID (有効範囲 : 1-4093)

初期設定

設定した VLAN すべてのマルチキャストルータのポートが表示されます。

コマンドモード

Privileged Exec

コマンド解説

- 表示されているマルチキャストルータタイプには、スタティック、あるいはダイナミックが含まれます。

例：

VLAN1 の port 11 がマルチキャストルータに接続されていることを表しています。

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1            Eth 1/11  Static
    2            Eth 1/12  Dynamic
Console#
```

1.32.3 PIM マルチキャストフィルタリング

ここでは、IPv4 および IPv6 に使用する PIM コマンドについて説明します。

[注意] PIM は IPv4 ネットワーク上、PIM6 は IPv6 network 上で同時に起動することが可能です。また、IPv4 に対しては IGMP（Internet Group Management Protocol）、IPv6 ネットワークに対しては MLD(Multicast Listener Discovery) をそれぞれ使用してください。

コマンド	機能
IPv4 PIM コマンド	IPv4 PIM のマルチキャストルーティングを設定します。
IPv6 PIM-DM コマンド	IPv6 PIM のマルチキャストルーティングを設定します。

IPv4 PIM Commands

IPv4 PIM-DM および PIM-SM のダイナミックマルチキャストルーティングの設定に使用するコマンドについて説明します。

コマンド	機能		
共有モードコマンド			
router pim	ルータの IPv4 PIM をグローバルで有効にします。	GC	P721
ip pim	指定したインタフェースの PIM-DM、または PIM-SM を有効にします。	IC	P722
ip pim hello-holdtime	ダウンしたと宣言する前に、ネイバーの PIM ルータからのメッセージを受信するまでの待機時間を設定します。	IC	P723
ip pim hello-interval	PIM hello メッセージの送信間隔を設定します。	IC	P724
ip pim join-prune-holdtime	prune 状態のホールド時間を設定します。	IC	P725
ip pim lan-prune-delay	prune リクエストを受信後、フローを切断するまでの遅延をダウンストリームルータに通知します。	IC	P726
ip pim override-interval	ダウンストリームルータが lan-prune-delay メッセージに応答するまでの時間をしてします。	IC	P727
ip pim propagation-delay	LAN prune delay メッセージがダウンストリームルータに届くまでに必要な伝播遅延を設定します。	IC	P728
ip pim trigger-hello-delay	trigger hello 遅延を設定します。	IC	P729
show ip pim interface	PIM に対して設定したインタフェースについての情報を表示します。	NE, PE	P730
show ip pim neighbor	PIM ネイバールートについての情報を表示します。	NE, PE	P731

PIM-DM Commands			
ip pim graft-retry-interval	Graft メッセージの再送を行う前に、Graft を受け取るまでにかかる時間を設定します。	IC	P733
ip pim max-graft-retries	Graft メッセージを受け取っていない場合、メッセージの再送回数の上限を設定します。	IC	P733
ip pim state-refresh origination-interval	PIM-DM state refresh control メッセージの送信間隔を設定します。	IC	P734

router pim

IPv4 Protocol-Independent マルチキャストルーティングをグローバルで有効にします。コマンドの前に "no" を付けることにより PIM マルチキャストルーティングは無効になります。

文法

[no] router pim

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- ルータの PIM-DM および PIM-SM をグローバルで有効にします。ip pim dense-mode、あるいは ip pim sparse mode コマンドを使ってマルチキャストルーティングをサポートしている各インタフェースごとに PIM-DM、あるいは PIM-SM を有効にして、マルチキャストプロトコルパラメータに必要な変更をおこなってください。
- マルチキャストルーティングを使用するには、IGMP proxy はデバイスのインタフェース上で無効になります（ ip igmp proxy コマンドを参照ください)。

例：

```
Console(config)#router pim
Console(config)#exit
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                      :     Dense Mode
 IP Address                    :     192.168.0.2
 Hello Interval                :     30 sec
 Hello HoldTime                :     105 sec
 Triggered Hello Delay         :     5 sec
 Join/Prune Holdtime           :     210 sec
 Lan Prune Delay               :     Disabled
 Propagation Delay             :     500  ms
 Override Interval             :     2500  ms
 Graft Retry Interval          :     3 sec
 Max Graft Retries             :     3
 State Refresh Ori Int         :     60 sec

Console#
```

ip pim

指定したインタフェース上の PIM-DM、または PIM-SM を有効にします。コマンドの前に "no" を付けることにより、PIM-DM 、または PIM-SM は無効になります。

文法

[no] ip pim {dense-mode | sparse-mode}

- dense-mode - PIM Dense モードを有効にします。
- sparse-mode - PIM Sparse モードを有効にします。

初期設定

Disabled

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- PIM を完全に有効にするには、ip multicast-routing コマンドと一緒に使用してルータのマルチキャストルーティングを、router pim コマンドと一緒に使用して PIM をグローバルで有効にする必要があります。また マルチキャストルーティングに設定されているインタフェースごとに、PIM-DM または PIM-SM を有効にすることも可能です。マルチキャストルーティング のインタフェースごとに PIM-DM、あるいは PIM-SM を有効にします。
- インタフェース上の PIM を有効にすると、IGMP も有効に設定する必要があります。選択した PIM モードにより、マルチキャストルーティングテーブルを集結する方法、接続先の LAN から受信したパケットを転送する方法が異なります。Dense モードのインタフェースは通常マルチキャストルーティングテーブルに加算されます。Sparse モードのインタフェースは、join メッセージをダウンストリームルータから周期的に受信した場合、またはグループメンバーがインタフェースに直接接続された場合のみ追加されます。
- Dense-mode インタフェースの場合、デフォルトではマルチキャストのフラッディングが発生し、ルータがグループメンバー、またはダウンストリームルータがないと判断した場合、または prune メッセージをダウンストリームルータから受信した場合のみ、マルチキャストルーティングテーブルから削除されます。
- Sparse-mode インタフェースは、ダウンストリームルータから受信した場合、グループメンバがインタフェースに直接接続されている場合のみマルチキャストトラフィックを伝送します。ルータがマルチキャストフローを受信したい場合は、join を RP(Rendezvous Point) に定期的に送信し、RP へのバックアップのための指定したフローの共用パスに追加されます。SPT(Shortest Path Source Tree) を介してソースパスを追加したい場合は、join メッセージをソースに定期的に送信します。また、prune メッセージを RP に送信して、SPT を介してソースにすでに接続されている場合は、インタフェースに接続されているグループメンバーがない場合共用パスを切断します。

例：

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dense-mode
Console(config-if)#end
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                 :        Dense Mode
 IP Address               :        192.168.0.2
 Hello Interval           :        30 sec
 Hello HoldTime           :        105 sec
 Triggered Hello Delay :           5 sec
 Join/Prune Holdtime   :          210 sec
 Lan Prune Delay          :        Disabled
 Propagation Delay        :        500  ms
 Override Interval        :        2500  ms
 Graft Retry Interval     :         3 sec
 Max Graft Retries        :         3
 State Refresh Ori Int  :          60 sec

Console#
```

ip pim hello-holdtime

ネイバー PIM **ルータが無効と宣言する前に、**RIM **ルータからの** hello **メッセージを受信するまでの待機時間を設定します。コマンドの前に** "no" **を付けることにより、デフォルト値に戻ります。**

文法

ip pim hello-holdtime seconds

no ip pim hello-interval

- seconds - PIM **の** hello **メッセージを保持する時間** (**有効範囲** : 1-65535)

初期設定

105 **秒**

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ip pim hello-holdtime **の値は、**ip pim hello-interval **の値より大きい値に設定してください。**

例：

```
Console(config-if)#ip pim hello-holdtime 210
Console(config-if)#
```

ip pim hello-interval

PIM の hello メッセージを送信する頻度を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ip pim hello-interval seconds

no pim hello-interval

- seconds - PIM の hello メッセージの送信間隔 (有効範囲 : 1-65535)

初期設定

30 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- probes を受信したデバイスから Hello メッセージをネイバー PIM ルータに送信し、これらのネイバールータのマルチキャストツリーが有効かどうかを確認します。

例：

```
Console(config-if)#ip pim hello-interval 60
Console(config-if)#
```

ip pim join-prune-holdtime

prune 状態を保持する時間を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ip pim join-prune-holdtime seconds

no ip pim join-prune-holdtime

- seconds - prune 状態の保持時間 (有効範囲 : 0-65535)

初期設定

210 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- マルチキャストインタフェースが特定のソースから最初にマルチキャストストリームを受信すると、トラフィックをルータ上のその他の PIM インタフェースすべてに伝送します。
- インタフェース上に要求するグループがない場合は、leaf ノードは prune メッセージアップストリームを送信して、マルチキャストストリームの prune 状態になります。prune 状態は join-prune-holdtime タイマーが切れたり、伝送エントリ用に graft メッセージを受信するまで保持されます。

例：

```
Console(config-if)#ip pim join-prune-holdtime 60
Console(config-if)#
```

ip pim lan-prune-delay

デバイスが prune リクエストを受信した後、フローを切断するまでの時間をダウンストリームルータに通知させます。コマンドの前に "no" を付けることによりこの機能は無効になります。

文法

[no] ip pim lan-prune-delay

初期設定

Disabled

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **アップストリームルータが prune リクエストを受信していないことを同じ VLAN 上のダウンストリームルータに通知すると、フローの受信を継続したい場合は prune 遅延が切れるまでに prune をオーバーライドするために、join メッセージを送信する必要があります。**

  同じ VLAN 上の他のダウンストリームルータは、このアップストリームルータが Prune 要求を受信したことを通知された場合、フローを引き続き受信したければ、この「LAN Prune Delay」期間が経過する前に Join メッセージを送信して Prune メッセージをオーバーライドする必要があります。このコマンドによって生成されるメッセージを使用すると、フローを受信したホストをダウンストリームの隣接ルータに通知して、それらのルータが Join メッセージを返すという処理が効率的に実行されるようになります。この「LAN Prune Delay」期間を過ぎても Join メッセージが受信されない場合、ルータはフローを切断します。

例：

```
Console(config-if)#ip pim lan-prune-delay
Console(config-if)#
```

関連するコマンド

ip pim override-interval (P727)
ip pim propagation-delay (P728)

ip pim override-interval

オーバーライドの時間を設定したり、ダウンストリームルータによる lan-prune-delay **メッセージへの応答時間を設定します。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻します。**

文法

ip pim override-interval milliseconds

no ip pim override-interval

- milliseconds - **メッセージ内で参照すためのフローの受信を継続して行いたい場合の** join **メッセージを戻すことにより、ダウンストリームルータによる** lan-prune-delay **メッセージへの応答に必要な時間** (**有効範囲** : 500-6000 **ミリ秒**)

初期設定

2500 **ミリ秒**

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **コマンドにより設定されたオーバーライドの間隔と** ip pim propagation-delay **により設定された伝播遅延を使って、**LAN **の** prune delay **の計算を行います。ダウンストリームルータのグループメンバーが** LAN prune delay **メッセージ内で参照するフローを継続して受信したい場合は、オーバーライドの間隔は、ダウンストリームルータがメッセージの処理を行った後にフローが終端していないかどうかを確認するために** Join **メッセージをアップストリームルータに戻して応答するのに必要な時間を示します。**

例

```
Console(config-if)#ip pim override-interval 3500
Console(config-if)#
```

関連するコマンド

ip pim propagation-delay (P728)
ip pim lan-prune-delay (P726)

ip pim propagation-delay

LAN prune delay メッセージがダウンストリームルータに到達するまでに要する伝播遅延を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻します。

文法

ip pim propagation-delay milliseconds

no ip pim propagation-delay

- milliseconds - LAN prune delay メッセージが同じ VLAN インタフェースに接続されているダウンストリームルータに到達するまでに要する伝播遅延を設定します (有効範囲 : 100-5000 ミリ秒)

初期設定

500 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ip pim override-interval コマンドにより設定されたオーバーライドの間隔とこのコマンドによって設定された伝播遅延を使って LAN prune 遅延を計算します。ダウンストリームルータのグループにより LAN prune delay メッセージで参照したフローを継続して受信したい場合は、アップストリームルータから同じ VLAN インタフェースに接続されているダウンストリームルータすべてに lan-prune-delay メッセージを伝播するために必要な時間を表します。

例：

```
Console(config-if)#ip pim propagation-delay 600
Console(config-if)#
```

関連するコマンド

ip pim override-interval (P727)
ip pim lan-prune-delay (P726)

ip pim trigger-hello-delay

ルータがリブートするか、PIM がインタフェース上で有効に設定された後、トリガーとなる PIM Hello メッセージを送信するまでの時間の上限を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ip pim trigger-hello-delay seconds

no ip pim trigger-hello-delay

- seconds - トリガーとなる PIM Hello メッセージを送信するまでの時間の上限値 (有効範囲 : 0-5 秒)

初期設定

5 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ルータを初めて始動するか、インタフェースで PIM を有効にすると、Hello 遅延が 0 から「Trigger Hello Delay」の間のランダムな値に設定されます。そのようにすることで、複数のルータが同時に電源オンにされた場合にマルチアクセスリンクで Hello メッセージが同期されないようにしています。
- また、ルータは、新規ルータから Hello メッセージを受信すると、「0」から「Trigger Hello Delay」の間のランダムな値に設定されている遅延期間が経過してから自らの Hello メッセージを送信します。

例：

```
Console(config-if)#ip pim trigger-hello-delay 3
Console(config-if)#
```

show ip pim interface

PIM のインタフェースの設定情報が表示されます。

文法

show ip pim interface [vlan vlan-id]

- vlan-id - VLAN ID (有効範囲 : 1-4094)

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- 前述のとおり、指定したインタフェースの PIM 設定が表示されます。また代表の PIM ルータのアドレスおよびネイバー PIM ルータ数が表示されます。

例：

```
Console#show ip pim interface vlan 1
PIM is enabled.
VLAN 1 is up.
 PIM Mode                  :         Dense Mode
 IP Address                :         192.168.0.2
 Hello Interval            :         30 sec
 Hello HoldTime            :         105 sec
 Triggered Hello Delay     :          5 sec
 Join/Prune Holdtime       :          210 sec
 Lan Prune Delay           :          Disabled
 Propagation Delay         :          500  ms
 Override Interval         :          2500  ms
 Graft Retry Interval      :          3 sec
 Max Graft Retries         :          3
 State Refresh Ori Int     :          60 sec

Console#
```

show ip pim neighbor

PIM ネイバールータ情報を表示します。

文法

show ip pim neighbor [interface vlan vlan-id]

- vlan-id - VLAN ID (有効範囲 : 1-4094)

初期設定

認識されている PIM ネイバールータ情報をすべて表示します。

コマンドモード

Normal Exec, Privileged Exec

例：

```
Console#show ip pim neighbor
Neighbor Address VLAN Interface Uptime (sec.) Expiration Time
(sec)
---------------- -------------- ------------- -------------------
--
192.168.0.3/32   1              00:00:21      00:01:30
Console#
```

コマンド	機能
Neighbor Address	next-hop ルータの IP アドレス
VLAN Interface	ネイバールータに接続されているインタフェース数
Uptime	このエントリの有効時間
Expiration Time	このエントリを削除するまでの時間

ip pim graft-retry-interval

Graft メッセージを再送信する前に Graft 肯定応答メッセージを待機する時間を設定します（範囲 : 1 〜 10 秒、デフォルト : 3 秒）。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ip pim graft-retry-interval seconds

no ip pim graft-retry-interval

- seconds - Graft メッセージを再送信するまでの時間 (有効範囲 : 1-10 秒)

初期設定

3 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- Graft メッセージは、Prune 状態を解除するためにルータが送信します。ルータは、Graft メッセージを受信した場合には、Graft 肯定応答メッセージを返す必要があります。肯定応答メッセージがない場合、Graft メッセージを送信したルータは、何回か （ip pim max-graft-retries」で指定されている回数）Graft メッセージ再送信します。

例：

```
Console(config-if)#ip pim graft-retry-interval 9
Console(config-if)#
```

ip pim max-graft-retries

Graft メッセージが認識されない場合、再送回数の上限を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ip pim max-graft-retries retries

no ip pim max-graft-retries

- retries - Graft メッセージの最総回数の上限 (有効範囲 : 1-10)

初期設定

3 回

コマンドモード

Interface Configuration (VLAN)

例：

```
Console(config-if)#ip pim max-graft-retries 5
Console(config-if)#
```

ip pim state-refresh origination-interval

PIM-DM state refresh control メッセージの再送間隔を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ip pim state-refresh origination-interval seconds

no ip pim max-graft-retries

- seconds - PIM-DM state refresh control メッセージの再送間隔 (有効範囲 : 1-100 秒)

初期設定

60 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- Prune 状態は約 3 分間ごとにタイムアウトになり、マルチキャストパケットと Prune メッセージが PIM-DM ネットワーク全体に再びフラッディングされます。state refresh 機能では、制御メッセージを配信ツリーのダウンストリームへ定期的に転送することにより、ツリー内の各ルータの発信インタフェースの Prune 状態をリフレッシュして、Prune 状態がタイムアウトにならないようにします。また、そのようにすると、デフォルトの 3 分間のタイムアウト期間が経過する前に PIM ルータがトポロジの変更（マルチキャストグループに対する送信元の加入または離脱）を認識できるようになります。　このコマンドは、マルチキャストグループの送信元メンバーに直接接続するファーストホップの PIM-DM ルータのインタフェースについてのみ有効です。

例：

```
Console(config-if)#ip pim state-refresh origination-interval 30
Console(config-if)#
```

ip pim bsr-candidate

本機を BSR(Bootstrap Router) の候補として設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ip pim bsr-candidate interface vlan vlan-id [hash hash-mask-length] [priority priority]

no ip pim bsr-candidate

- vlan-id - VLAN ID (有効範囲 : 1-4094)
- hash-mask-length - RP の選択に使用する Hash mask の長さ (ビット単位)(see ip pim rp-candidate コマンドおよび ip pim rp-address) コマンドを参照)。マスク長で指定されるハッシュの部分は、グループアドレスとの論理積が求められるため、BSR 上でハッシュ機能を実行すると、同じ通信速度のハッシュを持つグループはすべて同じ RP にマッピングされます。マスクの長さが 32 ビット満たない場合は、最初のハッシュの部分のみ使用され、1 つの RP が複数のグループに対して設定されます (有効範囲 : 0-32 bits)
- priority - 選出プロセスで BSR 候補によって使用される優先度。この「Priority」の値が最も大きい BSR 候補が優先されます。「Priority」の値が同じ場合には、IP アドレスが大きい方の候補が BSR になるものとして選出されます。「Priority」を 0 に設定すると、そのルータが BSR として稼働する資格がなくなります。PIM-SM ドメイン内の少なくとも 1 つのルータに 0 よりも大きい値を設定する必要があります （範囲 : 0 〜 255)。

初期設定

Hash Mask Length: 10
Priority: 0

コマンドモード

Global Configuration

コマンド解説

- ip pim bsr-candidate コマンドを入力すると、ルータは PIM-SM ネイバーのすべてに対して bootstrap メッセージの送信を開始します。指定の VLAN の IP アドレスは、候補の BSR アドレスとして送信されます。bootstrap メッセージを受信したネイバーはそれぞれ、BSR アドレスと以前のメッセージからのアドレスを比較します。現行のアドレスが同じかもっと高い場合は、bootstrap メッセージを受け取って転送します。それ以外はメッセージを破棄します。
- プライオリティが候補（あるいは、もっと高いプライオリティが同じ場合は、IP アドレスが高い方）からの bootstrap メッセージを受信するまで、BSR を継続します。
- より優れたフェイルオーバーリカバリを実現するため、別々の場所にある少なくとも 2 つのコアルータを選択して、それぞれ、BSR 候補と RP 候補の両方として稼働させることをお勧めします。また、それらのルータの 1 つをプライマリ BSR と RP の両方としてセットアップすることも推奨されます。

例：

以下の例では、ルータを設定して、すべての PIM-SM **ネイバーのすべてに対して、**VLAN 1 **インタフェースからの** bootstrap **メッセージの送信を開始します。**

```
Console(config)#ip pim bsr-candidate interface vlan 1 hash 20
priority 200
Console(config)#exit
Console#show ip pim bsr-router
PIMv2 Bootstrap information
BSR Address      : 192.168.0.2/32
Uptime           : 00:00:08
BSR Priority     : 200
Hash Mask Length : 20
Expire           : 00:00:57
Role             : Candidate BSR
State            : Elected BSR
Console#
```

ip pim register-rate-limit

それぞれのエントリ（ソース、グループ）に対して DR(Designated Router) による register メッセージの送信速度を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ip pim register-rate-limit rate

no ip pim register-rate-limit

- rate - 秒単位の最大 register パケット数 (有効範囲 : 1-65535: デフォルト設定 : 「0」は「制限なし」を表します。)

初期設定

0

コマンドモード

Global Configuration

コマンド解説

- DR(Designated Router) および RP 上の負荷を軽減するために使用します。ただし、register メッセージが制限値を超えると破棄されるため、受信側によっては bursty ソースから register メッセージが送信されるまでの最初の数秒以内にデータパケットロスが起きる可能性があります。

例：

ここでは、レジスタレートの制限値が「 500 pps」に設定されます。

```
Console(config)#ip pim register-rate-limit 500
Console(config)#
```

ip pim register-source

register メッセージの IP ソースアドレスを DR(designated route) の出力用インタフェースアドレス以外のアドレスに設定し、ランデブーポイント (RP) に戻ります。コマンドの前に "no" を付けることにより、デフォルト設定に戻します。

文法

ip pim register-source interface vlan vlan-id

no ip pim register-source

- vlan-id - VLAN ID (有効範囲 : 1-4094)

初期設定

RP に戻る際の RP の出力インタフェースの IP アドレス

コマンドモード

Global Configuration

コマンド解説

- Register メッセージの送信元アドレスが中間ネットワークデバイスによってフィルタリングされるか、RP がパケットを送信できるアドレスに一意にルーティングされる場合には、RP から送信元アドレスに送信される応答が DR に到達できず、その結果、PIM-SM プロトコル障害が発生します。この種の問題は、Register メッセージの送信元アドレスを RP への戻り時のインターフェースのアドレスに手動で設定することによって克服することができます。

例：

ここでは、レジスタレートの制限値が「500 pps」に設定されます。

```
Console(config)#ip pim register-source interface vlan 1
Console(config)#
```

ip pim rp-address

特定のマルチキャストグループのランデブーポイント (RP) のスタティックアドレスを設定します。コマンドの前に "no" を付けることにより、RP アドレスまたは特定のグループの RP アドレスを削除します。

文法

[no] ip pim rp-address rp-address [group-prefix group-address mask]

- rp-address - 特定のグループの RP アドレスとなるルータのスタティック IP アドレス。
- group-address - IP マルチキャストグループアドレス。グループアドレスが指定されていない場合は、RP はすべてのマルチキャストグループに使用されます。
- mask - グループアドレスに対して使用されるサブネットマスク

初期設定

None

コマンドモード

Global Configuration

コマンド解説

- このコマンドによって指定されているルータは、グループが指定されていない場合は、ローカルな PIM-SM ドメイン内のすべてのマルチキャストグループの RP として動作します。スタティック RP は、マルチキャストグループレンジ (224.0.0.0/4)、特定のグループレンジのいずれかに設定可能です。
- このコマンドを使って同じ RP アドレスを持つ複数のスタティックを設定するこは許可れていません。RP に以前使用されていた IP アドレスを指定すると、古いエントリは置き換えられます。
- 異なるグループ、またはグループレンジに対して複数の RP が設定可能です。複数のエントリが一致するグループは、ルータはもっと長いプレフィックスをもつグループの RP を使用します。プレフィックスの長さが同じであれば、IP アドレスが一番高いスタティック RP が選ばれます。
- RP アドレスのスタティック設定は、BSR を介して動的に学習される RP アドレスと一緒に使用することが可能です。RP アドレスが BSR によって学習された場合、またこのコマンドによって静的に設定された場合は、グループレンジに対して両方可能な場合は、このコマンドによって手動で設定されたものより、BSR によって学習された RP アドレスのほうが優先されます。
- 同じ PIM-SM ドメイン内のすべてのルータは同じ RP を指定して設定する必要があります。そのため、動的選出プロセスによる RP の選出は、ほとんどの状況で望ましいものとなります。また、動的 RP 選出プロセスを使用すると、アクティブな RP ルータが使用不可になった場合に自動的にバックアップ RP ルータがその役割を引き継ぐことができるようになります。
- コマンドの前に ”no” を付けて、マルチキャストグループを指定せずに使用する場合は、デフォルトの「マスク :224.0.0.0」は削除されます。つまりマルチキャストグループはすべて削除されます。

例：

以下の例は、最初の PIM-SM **コマンドは、**RP **アドレス「**192.168.1.1**」を指定して、マルチキャストグループを動作させるために使用してることを示します。次の** PIM-SM **コマンドには、**RP **で動作するマルチキャストグループが含まれます。**

```
Console(config)#ip pim rp-address 192.168.1.1
Console(config)#ip pim rp-address 192.168.2.1 group-prefix
224.9.0.0 255.255.0.0
Console(config)#end
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups           : 224.0.0.0/4
RP address       : 192.168.1.1/32
Info source      : static
Uptime           : 00:00:33
Expire           : Never
Groups           : 224.9.0.0/16
RP address       : 192.168.2.1/32
Info source      : static
Uptime           : 00:00:21
Expire           : Never
Console#
```

ip pim rp-candidate

このコマンドは、ルータを設定して、BSR に対してそれ自体を RP 候補としてアドバタイズします。コマンドの前に "no" を付けることにより RP 候補としてルータを削除します。

文法

ip pim rp-candidate interface vlan vlan-id [group-prefix group-address mask] [interval seconds] [priority value]

no ip pim rp-candidate interface vlan vlan-id

- vlan-id - VLAN ID (有効範囲 : 1-4094)
- group-address - IP マルチキャストグループアドレス。グループアドレスが指定されていない場合は、複数のグループに対して RP はアドバタイズされます。
- mask - グループアドレスに対して使用されるサブネットマスク
- seconds - このデバイスが自身を RP 候補としてアドバタイズする間隔。(有効範囲 : 60-16383 秒)
- value - 選出プロセスで RP 候補によって使用される優先度。この「Priority」の値が最も大きい RP 候補が優先されます。「Priority」の値が同じ場合には、IP アドレスが大きい方の候補が RP になるものとして選出されます。「Priority」を 0 に設定すると、そのルータが RP として稼働する資格がなくなります（範囲 : 0 ～ 255）。

初期設定

Address: 224.0.0.0/4、または IPv4 マルチキャストグループファミリ全体

Interval: 60 秒
Priority: 0

コマンドモード

Global Configuration

コマンド解説

- ip pim rp-candidate コマンドを入力すると、ルータは指定のグループアドレスの候補 RP として自身をアドバタイズする BSR に PIMv2 メッセージを定期的に送信します。指定の VLAH を候補の RP アドレスとして送信します。　代表 VLAN の IP アドレスが候補の BSR アドレスとして送信されます。すると、その BSR は、すべての RP 候補に関する情報を、以降送信されるブートストラップメッセージに挿入するようになります。BSR は、RP 選出ハッシュアルゴリズムを使用して、それぞれのグループ範囲に対してアクティブな RP を選出します。選出プロセスは、BSR が自ら使用するためにのみ、実行します。RP 候補のリストを BSR から受け取るそれぞれの PIM-SM ルータも、同じ選出プロセスを使用して、それぞれのグループ範囲に対してアクティブな RP を選出します。
  - 各グループの選出プロセスの基準は、以下のとおりです。
  - 最も明確なグループ範囲が指定されている RP をすべて検出
  - 優先度が最も高い（優先度値が最も小さい）RP を選択

- ブートストラップメッセージに含まれているグループアドレス、RP アドレス、優先度、およびハッシュマスクに基づいてハッシュ値を計算
- ハッシュ値が同じ場合には、IP アドレスの値が最も大きい RP 候補を使用

- この分散選出プロセスを使用すると、RP で障害が発生した場合に、収束を迅速に実現し、サービスの中断期間を最小限に抑えることができます。また、グループを複数の RP に分散させるので、負荷分散にも役立ちます。それだけでなく、RP で障害が発生した場合に、それぞれのルータで処理を担当する RP が改めて選出され、グループが自動的に残りの RP に分散されます。・より優れたフェイルオーバーリカバリを実現するため、別々の場所にある少なくとも 2 つのコアルータを選択して、それぞれ、BSR 候補と RP 候補の両方として稼働させることをお勧めします。また、それらのルータの 1 つをプライマリ BSR と RP の両方としてセットアップすることも推奨されます。
- より優れたフェイルオーバーリカバリを実現するため、別々の場所にある少なくとも 2 つのコアルータを選択して、それぞれ、BSR 候補と RP 候補の両方として稼働させることをお勧めします。また、それらのルータの 1 つをプライマリ BSR と RP の両方としてセットアップすることも推奨されます。

例：

ここでは、表示されたマルチキャストグループの候補 RP として BSR に自らアドバタイズを開始するようルータを設定します。

```
Console(config)#ip pim rp-candidate interface vlan 1 group-prefix
224.0.0.0 255.0.0.0
Console(config)#end
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups              : 224.0.0.0/8
RP address          : 192.168.0.2/32
Info source         : 192.168.0.2/32, via bootstrap, priority: 0
Uptime              : 00:00:51
Expire              : 00:01:39
Console#
```

ip pim spt-threshold

last-hop PIM ルータの SPT(Shortest Path Source Tree) モードへの切り替えを回避します。コマンドの前に "no" を付けることにより、ルータの SPT モードへの切り替えを有効にします。

文法

ip pim spt-threshold infinity [group-prefix group-address mask]

no ip pim spt-threshold infinity

- group-address - IP マルチキャストグループアドレス。グループアドレスが指定されていない場合は、すべてのマルチキャストグループで適用されます。
- mask - グループアドレスに対して使用されるサブネットマスク

初期設定

新規送信元から最初のパケットを受信すると、last-hop PIM ルータは最短パスツリーをジョインします。

コマンドモード

Global Configuration

コマンド解説

- SPT Threshold - マルチキャストソースから受信先へのパケットのデフォルトパスは RP を経由します。ただし、RP を経由するパスが必ずしも最短パスであるとは限りません。そのため、新規のマルチキャストグループから最初に受け取ったパケットのみを RP を使用して受信先に転送します。最初のパケットを転送した後、受信先と送信元との間の最短パスを求め、以降は、共有ツリーではなく、最短パスツリー (SPT) を使用して、送信元からのすべてのパケットを受信先に直接送信します。SPT しきい値がこのコマンドによって設定されていない場合、PIM リーフルータは、新規の送信元から最初のパケットを受信した直後に SPT に追加されます。「SPT Threshold」を指定すると、ルータで、すべてのマルチキャストグループに、または、指定されたマルチキャストグループのみに共有ツリーが使用されるようになります。
- Group Address - IP マルチキャストグループアドレス。グループアドレスが指定されていない場合、すべてのマルチキャストグループに共有ツリーが使用されます。
- Group Mask - グループアドレスに使用されるサブネットマスク。

例：

ここでは、マルチキャストグループ (224.1.0.0~224.1.255.255) の SPT の使用を回避します。

```
Console(config)#ip pim spt-threshold infinity group-prefix
224.1.0.0 0.0.255.255
Console#
```

ip pim dr-priority

DR 候補のプライオリティの値を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻します。

文法

ip pim dr-priority priority-value

no ip pim dr-priority

- priority-value - DR を禁止する場合のルータによりアドバタイズされるプライオリティ 1 (有効範囲 : 0-4294967294)

初期設定

1

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- DR Priority - ルータが自らを代替ルータ (DR) の候補として宣言する際にアドバタイズする優先度を設定します (範囲 : 0 ～ 4,294,967,294、デフォルト : 1)。 Ethernet LAN やその他の共有メディア LAN に複数の PIM-SM が接続していることがあります。マルチキャストホストが LAN に直接接続している場合は、ルータが 1 つだけが DR として選出されて、マルチキャストホストに代わって Join メッセージや Prune メッセージを各グループのグループ固有の RP へ定期的に送信します。DR は、簡易な選出プロセスを使用してインターフェース (LAN など) ごとに 1 つずつ選出されます。
- インターフェースで設定されている最も高い優先度をもつルータが DR として選択されます。インターフェースに接続している複数のルータの優先度が同じ場合には、最上位の IP アドレスをもつ DR として選出されます。
- ルータが自らの優先度を Hello メッセージでアドバタイズしない場合は、最も高い優先度をもつものとみなされ、DR として選出されます。複数のルータが自らの優先度をアドバタイズしない場合には、最上位の IP アドレスをもつルータが DR として選出されます。

例：

ここでは、DR の競合プロセスで使用するプライオリティを設定します。

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dr-priority 20
Console(config-if)#end
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                      :     Sparse Mode
 IP Address                    :     192.168.0.2
 Hello Interval                :     30 sec
 Hello HoldTime                :     105 sec
 Triggered Hello Delay         :     5 sec
 Join/Prune Holdtime           :     210 sec
 Lan Prune Delay               :     Disabled
 Propagation Delay             :     500  ms
 Override Interval             :     2500  ms
 DR Priority                   :      20
 Join/Prune Interval           :      60 sec

Console#
```

ip pim join-prune-interval

join/prune タイマーを設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻します。

文法

ip pim join-prune-interval seconds

no ip pim join-prune-interval

- seconds - join/prune メッセージの送信間隔 (有効範囲 : 1-65535 秒)

初期設定

60 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- デフォルトでは、join/prune メッセージを 210 秒間隔で送信して、マルチキャストグループへの加入、または離脱したいクライアントについて他の PIM-SM ルータに通知します。
- 同じ PIM-SM ドメイン内の PIM-SM ルータ上の同じ join/prune メッセージ間隔を使用してください。同じ値を使用しない場合、ルーティングプロトコルのパフォーマンスに悪影響を及ぼします。
- 特定の送信元から初めてマルチキャストストリームを受信したマルチキャストインターフェースは、そのトラフィックを、ルータ上で、該当のグループへの加入を要求しているインターフェースのみに転送します。そのインターフェースにトラフィックを要求しているグループが既に存在していない場合、リーフノードは、Prune メッセージをアップストリームに送信し、そのマルチキャストストリームについて Prune 状態になります。この (S, G)（送信元とグループ）の組み合わせについて、現在の Join 状態と Pending RPT Prune 状態の両方が「Join/Prune Holdtime」が経過するまで維持されます。

例：

ここでは、DR の bidding プロセスで使用されるプライオリティを設定します。

```
Console(config)#interface vlan 1
Console(config-if)#ip pim join-prune-interval 210
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                    :     Sparse Mode
 IP Address                  :     192.168.0.2
 Hello Interval              :     30 sec
 Hello HoldTime              :     105 sec
 Triggered Hello Delay       :     5 sec
 Join/Prune Holdtime         :     210 sec
 Lan Prune Delay             :     Disabled
 Propagation Delay           :     500  ms
 Override Interval           :     2500  ms
 DR Priority                 :     20
 Join/Prune Interval         :     80 sec

Console#
```

clear ip pim bsr rp-set

PIMv2 の BSR(bootstrap router) を介して学習した RP マッピングエントリへのマルチキャストグループをクリアにします。

コマンドモード

Privileged Exec

コマンド解説

- RP への設定の変更を行った後すぐにスタティックマルチキャストフォワーディングテーブルのエントリをアップデートします。
- show ip pim rp mapping コマンドを使用して、関連のあるマルチキャストルーティングエントリで隠したアクティブな RP を表示します。

例：

ここでは、RP マッピングをクリアにします。

```
Console#clear ip pim bsr rp-set
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Console#
```

show ip pim bsr-router

BSR(bootstrap router) についての情報を表示します。

コマンドモード

Privileged Exec

コマンド解説

- 選出した BSR の情報を表示します。

例：

ここでは、BSR の情報を表示します。

```
Console#show ip pim bsr-router
PIMv2 Bootstrap information
BSR Address      : 192.168.0.2/32
Uptime           : 01:01:23
BSR Priority     : 200
Hash Mask Length : 20
Expire           : 00:00:42
Role             : Candidate BSR
State            : Elected BSR
Console#
```

コマンド	機能
BSR Address	BSR として設定されているインターフェースの IP アドレス。
Uptime	BSR が稼働状態になってからの時間。
BSR Priority	BSR 選出プロセス時に使用するインタフェースに割り当てられるプライオリティ
Hash Mask Length	この BSR 候補によるマルチキャストグループ比較マスクで使用されている上位ビットの数。このマスクによって、BSR になるルータのマルチキャストグループが決定されます。
Expire	このエントリが削除されるまでの時間
Role	BSR の候補であるかどうか

State	BSR の稼働状態として、以下のものが表示されます。 No information – 情報が一切保存されていない状態です。 Accept Any – アクティブな BSR を認識していない状態であり、最初に受信するブートストラップメッセージに新しい BSR の ID と RP-set（RP 候補のリスト）が含まれているものとみなし、そのメッセージを受け入れます。 Accept Preferred – 現行の BSR の ID を認識しており、その BSR から提供される RP-set を使用しています。その BSR からのブートストラップメッセージまたは、現行の BSR よりも重みが大きい C-BSR からのブートストラップメッセージのみが受け入れられます。 Candidate BSR – 選出プロセスに参加中です。 Pending-BSR – このルータは RP-set で BSR となる候補です。現在、他に優先される BSR はありませんが、まだ BSR として選出されていません。 Elected BSR – BSR として稼働するように選出されました。

show ip pim rp mapping

アクティブの RP および関連のあるマルチキャストルーティング エントリを表示します。

コマンドモード

Privileged Exec

例：

ここでは、RP マッピングを表示します。

```
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups              : 224.0.0.0/8
RP address          : 192.168.0.2/32
Info source         : 192.168.0.2/32, via bootstrap, priority: 0
Uptime              : 00:31:09
Expire              : 00:02:21
Console#
```

コマンド	機能
Groups	RP によって管理されているマルチキャストグループアドレス、マスク長。
RP address	表示されているマルチキャストグループの RP の IP アドレス。
Info source	マッピング、RP が選出された方法（「Static」または「Bootstrap」）、および選出プロセスで使用される優先度をアドバタイズした RP。
Uptime	RP が稼働状態になってからの時間。
Expire	このエントリが削除されるまでの時間。

show ip pim rp-hash

指定のマルチキャストグループ用の RP**、マッピングのアドバタイズを行う** RP **を表示します。**

文法

show ip pim rp-hash group-address

- group-address - IP **マルチキャストグループアドレス**

コマンドモード

Privileged Exec

例：

ここでは、指定したグループの RP **が表示されます。**

```
Console#show ip pim rp-hash 224.0.1.3
RP address           : 192.168.0.2/32
Info source          : 192.168.0.2/32, via (null)
Console#
```

コマンド	機能
RP address	**指定のマルチキャストグループで使用する** RP **の** IP **アドレス**
Info source	**マッピングをアドバタイズする** RP**、**RP **の選択方法**

IPv6 PIM-DM Commands

ここでは、IPv6 PIM-DM ダイナミックマルチキャストルーティング の設定に使用するコマンドについて説明します。

コマンド	機能	モード	ページ
router pim6	Enables IPv6 PIM globally for the router ルータの IPv6 PIM をグローバルで有効にします。	GC	P753
ipv6 pim dense-mode	指定のインタフェース上の PIM-DM を有効にします。	IC	P754
ipv6 pim graft-retry-interval	Graft メッセージを再送するまでに、Graft を認識するまでの時間	IC	P756
ipv6 pim max-graft-retries	認識されていない Graft メッセージの再送回数の最大値を設定します。	IC	P757
ipv6 pim hello-holdtime	ネイバー PIM ルータがダウンしたと宣言するまでに、hello メッセージを受け取るまでの待機時間を設定します。	IC	P758
ipv6 pim hello-interval	PIM hello メッセージの送信間隔を設定します。Sets the interval between sending PIM hello messages	IC	P759
ipv6 pim join-prune-holdtime	prune 状態の時間を設定します。	IC	P760
ipv6 pim lan-prune-delay	prune リクエストを受信した後、フローを切り取るまでの遅延をダウンストリームルータに知らせます。	IC	P762
ipv6 pim override-interval	ダウンストリームルータの lan-prune-delay メッセージに応答に要する時間を指定します。	IC	P763
ipv6 pim propagation-delay	LAN prune delay メッセージがダウンストリームルータに到達するまでに要する伝播遅延を設定します。	IC	P763
ipv6 pim state-refresh origination-interval	SPIM-DM state refresh control メッセージ間の時間を設定します。	IC	P764
ipv6 pim trigger-hello-delay	trigger hello delay を設定します。	IC	P765
show ipv6 pim interface	PIM に設定したインタフェース情報を表示します。	NE, PE	P766
show ipv6 pim neighbor	PIM ネイバールーター情報を表示します。	NE, PE	P767

Shared Mode Commands

router pim6

ルータの IPv6 Protocol-Independent マルチキャストルーティング をグローバルで有効にします。コマンドの前に "no" を付けることにより PIM マルチキャストルーティングは無効になります。

文法

[no] router pim6

初期設定

Disabled

コマンドモード

Global Configuration

コマンド解説

- ルータの IPv6 Protocol-Independent マルチキャストルーティング をグローバルで有効にします。ipv6 pim dense-mode コマンドを使って、マルチキャストルーティング をサポートしているインタフェースごとに IPv6 PIM-DM を有効にする必要があり、マルチキャストプロトコルパラメータに要する変更を行います。
- マルチキャストルーティングを使用するには、IGMP proxy はインタフェース、あるいはデバイスのインタフェースは有効にすることはできません (ip igmp proxy コマンドを参照)。

例：

```
Console(confoig)#pim6
Console(config)#
```

ipv6 pim dense-mode

指定したインタフェース上の IPv6 PIM-DM を有効にします。コマンドの前に "no" を付けることにより IPv6 PIM-DM は無効になります。

文法

[no] ipv6 pim dense-mode

初期設定

Disabled

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- PIM を完全に有効にするには、ip multicast-routing コマンドと一緒に使用してルータのマルチキャストルーティングを、router pim コマンドと一緒に使用して PIM をグローバルで有効にする必要があります。また マルチキャストルーティングに設定されているインタフェースごとに、PIM-DM または PIM-SM を有効にすることも可能です。マルチキャストルーティング のインタフェースごとに PIM-DM、あるいは PIM-SM を有効にします。
- インタフェース上の PIM を有効にすると、IGMP も有効に設定する必要があります。選択した PIM モードにより、マルチキャストルーティングテーブルを集結する方法、接続先の LAN から受信したパケットを転送する方法が異なります。Dense モードのインタフェースは通常マルチキャストルーティングテーブルに加算されます。Sparse モードのインタフェースは、join メッセージをダウンストリームルータから周期的に受信した場合、またはグループメンバーがインタフェースに直接接続された場合のみ追加されます。
- Dense-mode インタフェースの場合、デフォルトではマルチキャストのフラッディングが発生し、ルータがグループメンバー、またはダウンストリームルータがないと判断した場合、または prune メッセージをダウンストリームルータから受信した場合のみ、マルチキャストルーティングテーブルから削除されます。
- Sparse-mode インタフェースは、ダウンストリームルータから受信した場合、グループメンバがインタフェースに直接接続されている場合のみマルチキャストトラフィックを伝送します。ルータがマルチキャストフローを受信したい場合は、join を RP(Rendezvous Point) に定期的に送信し、RP へのバックアップのための指定したフローの共用パスに追加されます。SPT(Shortest Path Source Tree) を介してソースパスを追加したい場合は、join メッセージをソースに定期的に送信します。また、prune メッセージを RP に送信して、SPT を介してソースにすでに接続されている場合は、インタフェースに接続されているグループメンバーがない場合共用パスを切断します。

例：

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 pim dense-mode
Console(config-if)#end
Console#show ipv6 pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                : Dense Mode
 IPv6 Address            : None
 Hello Interval          : 30 sec
 Hello HoldTime          : 105 sec
 Triggered Hello Delay   : 5 sec
 Join/Prune Holdtime     : 210 sec
 Lan Prune Delay         : Disabled
 Propagation Delay       : 500  ms
 Override Interval       : 2500  ms
 Graft Retry Interval    : 3 sec
 Max Graft Retries       : 3
 State Refresh Ori Int   : 60 sec

Console#
```

ipv6 pim graft-retry-interval

Graft メッセージを再送する前に、Graft メッセージに応答するまでの待機時間を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ipv6 pim graft-retry-interval seconds

no ipv6 pim graft-retry-interval

- seconds - Graft メッセージを再送するまでの時間 (有効範囲 : 1-10 秒)

初期設定

3 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- Graft メッセージは、Prune 状態を解除するためにルータが送信します。ルータは、Graft メッセージを受信した場合には、Graft 肯定応答メッセージを返す必要があります。肯定応答メッセージがない場合、Graft メッセージを送信したルータは、何回か（ipv6 pim max-graft-retries コマンドで指定されている回数）Graft メッセージ再送信します。

例：

```
Console(config-if)#ipv6 pim graft-retry-interval 9
Console(config-if)#
```

関連するコマンド

ipv6 pim override-interval (P762)
ipv6 pim propagation-delay (P763)

ipv6 pim max-graft-retries

Graft メッセージが認識されない場合の再送回数の上限を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ipv6 pim max-graft-retries retries

no ipv6 pim max-graft-retries

- retries - Graft メッセージの再送回数の上限 (有効範囲 : 1-10)

初期設定初期設定

3

コマンドモード

Interface Configuration (VLAN)

例：

```
Console(config-if)#ipv6 pim max-graft-retries 5
Console(config-if)#
```

ipv6 pim hello-holdtime

ネイバー PIM ルータがダウンしたと宣言する前に、ルータからの hello メッセージを受信するまでの待機時間を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ipv6 pim hello-holdtime seconds

no ipv6 pim hello-interval

- seconds - PIM の hello メッセージの保持時間 (有効範囲 : 1-65535)

初期設定

105 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ip pim hello-holdtime は、pv6 pim hello-interval の値よりも大きい値に設定してください。

例：

```
Console(config-if)#ipv6 pim hello-holdtime 210
Console(config-if)#
```

ipv6 pim hello-interval

PIM hello メッセージの送信間隔を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ipv6 pim hello-interval seconds

no pimv6 hello-interval

- seconds - PIM hello メッセージの送信間隔 (有効範囲 : 1-65535)

初期設定

30 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- Hello メッセージは、受信したプローブの送信元の PIM 隣接ルータに送信され、それらの隣接ルータがまだマルチキャストツリーのアクティブなメンバーであるかどうかを確認するために使用されます。

例：

```
Console(config-if)#ipv6 pim hello-interval 60
Console(config-if)#
```

ipv6 pim join-prune-holdtime

prune 状態を保持する時間を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ipv6 pim join-prune-holdtime seconds

no ipv6 pim join-prune-holdtime

- seconds - prune 状態の保持時間 (有効範囲 : 0-65535)

初期設定

210 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 特定の送信元から初めてマルチキャストストリームを受信したマルチキャストインターフェースは、そのトラフィックをルータ上の他のすべての PIMDM インターフェースに転送します。そのインターフェースにトラフィックを要求しているグループがない場合、リーフノードは、Prune メッセージをアップストリームに送信し、そのマルチキャストストリームについて Prune 状態になります。「Join/Prune Holdtime」が経過するまで、または、転送先エントリに関する Graft メッセージが受信されるまで、Prune 状態は維持されます。

例：

```
Console(config-if)#ipv6 pim join-prune-holdtime 60
Console(config-if)#
```

ipv6 pim lan-prune-delay

Prune 要求を受信してからフローをプルーンするまでの待機時間がダウンストリームルータに通知されるようにします。コマンドの前に "no" を付けるとこの機能を無効にします。

文法

[no] ipv6 pim lan-prune-delay

初期設定

Disabled

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 同じ VLAN 上の他のダウンストリームルータは、このアップストリームルータが Prune 要求を受信したことを通知された場合、フローを引き続き受信したければ、この「LAN Prune Delay」期間が経過する前に Join メッセージを送信して Prune メッセージをオーバーライドする必要があります。このコマンドによって生成されるメッセージを使用すると、フローを受信したホストをダウンストリームの隣接ルータに通知して、それらのルータが Join メッセージを返すという処理が効率的に実行されるようになります。この「LAN Prune Delay」期間を過ぎても Join メッセージが受信されない場合、ルータはフローを切断します。
- 「LAN Prune Delay」は、「Override Interval」と「Propagation Delay」の合計に基づいて求められます。ここで、有効な「Override Interval」はそれぞれのネイバー (本機を含む）によってアドバタイズされたもの中から一番大きい「Propagation Delay」、また有効な「override-interval は それぞれのネイバー (本機を含む）によってアドバタイズされたもの中から一番大きい「override-interval」です。

例：

```
Console(config-if)#ipv6 pim lan-prune-delay
Console(config-if)#
```

関連するコマンド

ipv6 pim override-interval (P762)
pv6 pim propagation-delay (P763)

ipv6 pim override-interval

オーバーライドの時間を設定したり、ダウンストリームルータによる lan-prune-delay **メッセージへの応答時間を設定します。コマンドの前に** "no" **を付けることにより、デフォルト設定に戻します。**

文法文法

ipv6 pim override-interval milliseconds

no ipv6 pim override-interval

- milliseconds - **メッセージ内で参照すためのフローの受信を継続して行いたい場合、**join **メッセージを戻すことにより、ダウンストリームルータによる** lan-prune-delay **メッセージへの応答に必要な時間** (**有効範囲** : 500-6000 **ミリ秒**)

初期設定

2500 **ミリ秒**

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **コマンドにより設定されたオーバーライドの間隔と** ipv6 pim propagation-delay **により設定された伝播遅延を使って、**LAN **の** prune delay **を算出します。ダウンストリームルータのグループメンバーが** LAN prune delay **メッセージ内で参照するフローを継続して受信したい場合は、オーバーライドの間隔は、ダウンストリームルータがメッセージの処理を行った後にフローが終端していないかどうかを確認するために** Join **メッセージをアップストリームルータに戻して応答するのに必要な時間を示します。**

例：

```
Console(config-if)#ipv6 pim override-interval 3500
Console(config-if)#
```

関連するコマンド

ipv6 pim propagation-delay (P763)
ipv6 pim lan-prune-delay (P761)

ipv6 pim propagation-delay

LAN prune delay メッセージがダウンストリームルータに到達するために必要な伝播遅延を設定します。コマンドの前に "no" を付けることにより、デフォルト設定に戻します。

文法

ipv6 pim propagation-delay milliseconds

no ipv6 pim propagation-delay

- milliseconds - lan-prune-delay メッセージが同じ VLAN インタフェースに接続されているダウンストリームルータに到達するために必要な時間を設定します (有効範囲 : 100-5000 ミリ秒)。

初期設定

500 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ipv6 pim override-interval コマンドにより設定されたオーバーライドの間隔とこのコマンドによって設定された伝播遅延を使って LAN prune 遅延を計算します。ダウンストリームルータのグループにより LAN prune delay メッセージで参照したフローを継続して受信したい場合は、アップストリームルータから同じ VLAN インタフェースに接続されているダウンストリームルータすべてに lan-prune-delay メッセージを伝播するために必要な時間を表します。

例：

```
Console(config-if)#ipv6 pim propagation-delay 600
Console(config-if)#
```

関連するコマンド

ipv6 pim override-interval (P762)
ipv6 pim lan-prune-delay (P761)

ipv6 pim state-refresh origination-interval

PIM-DM state refresh control メッセージの送信間隔を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ipv6 pim state-refresh origination-interval seconds

no ipv6 pim max-graft-retries

seconds - PIM-DM state refresh control メッセージの送信間隔 (有効範囲 : 1-100 秒)

初期設定

60 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- Prune 状態は約 3 分間ごとにタイムアウトになり、マルチキャストパケットと Prune メッセージが PIM-DM ネットワーク全体に再びフロードされます。state refresh 機能では、制御メッセージを配信ツリーのダウンストリームへ定期的に転送することにより、ツリー内の各ルータの発信インターフェースの Prune 状態をリフレッシュして、Prune 状態がタイムアウトにならないようにします。また、そのようにすると、デフォルトの 3 分間のタイムアウト期間が経過する前に PIM ルータがトポロジの変更 (マルチキャストグループに対する送信元の加入または離脱) を認識できるようになります。
- このコマンドは、マルチキャストグループの送信元メンバーに直接接続するファーストホップの PIM-DM ルータのインターフェースについてのみ、有効です。

例：

```
Console(config-if)#ipv6 pim state-refresh origination-interval 30
Console(config-if)#
```

ipv6 pim trigger-hello-delay

ルータがリブートするか、PIM がインタフェース上で有効に設定された後、トリガーとなる PIM Hello メッセージを送信するまでの時間の上限を設定します。コマンドの前に "no" を付けることにより、デフォルト値に戻ります。

文法

ipv6 pim trigger-hello-delay seconds

no ipv6 pim trigger-hello-delay

- seconds - トリガーとなる PIM Hello メッセージを送信するまでの時間の上限 (有効範囲 : 0-5)

初期設定

5 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ルータを初めて始動するか、インターフェースで PIM を有効にすると、Hello 遅延が「0」から「Trigger Hello Delay」の間のランダムな値に設定されます。そのようにすることで、複数のルータが同時に電源オンにされた場合にマルチアクセスリンクで Hello メッセージが同期されないようにしています。
- また、ルータは、新規ルータから Hello メッセージを受信すると、「0」から「Trigger Hello Delay」の間のランダムな値に設定されている遅延期間が経過してから自らの Hello メッセージを送信します。

例：

```
Console(config-if)#ipv6 pim trigger-hello-delay 3
Console(config-if)#
```

show ipv6 pim interface

PIM に対して設定したインタフェースの情報を表示します。

文法

show ipv6 pim [interface vlan vlan-id]

vlan-id - VLAN ID (有効範囲 : 1-4093)

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- 前述のとおり、指定したインタフェースの PIM 設定が表示されます。また代表の PIM ルータのアドレスおよびネイバー PIM ルータ数が表示されます。

例：

```
Console#show ipv6 pim interface vlan 1
PIM is enabled.
VLAN 1 is up.
 PIM Mode                      : Dense Mode
 IPv6 Address                  : None
 Hello Interval                : 30 sec
 Hello HoldTime                : 105 sec
 Triggered Hello Delay         : 5 sec
 Join/Prune Holdtime           : 210 sec
 Lan Prune Delay               : Disabled
 Propagation Delay             : 500  ms
 Override Interval             : 2500  ms
 Graft Retry Interval          : 3 sec
 Max Graft Retries             : 3
 State Refresh Ori Int         : 60 sec

Console#
```

show ipv6 pim neighbor

PIM ネイバールータの情報を表示します。

文法

show ipv6 pim neighbor [interface vlan vlan-id]

- vlan-id - VLAN ID (有効範囲 : 1-4093)

初期設定

認識している PIM ネイバールータのすべての情報を表示します。

コマンドモード

Normal Exec, Privileged Exec

例：

```
Console#show ipv6 pim neighbor
Address                                   VLAN Interface   Uptime
Expire
------------------------------------- ---------------- --------
--------
 FF80::0101                               VLAN 1           00:01:23
00:01:23
 FF80::0202                               VLAN 2           1d 11h
Never

Console#
```

コマンド	機能	モード
Neighbor Address	next-hop ルータの IP アドレス	GC
VLAN Interface	ネイバールートに接続されているインタフェース数	IC
Uptime	このエントリが有効な時間	IC
Expiration Time	このエントリが削除されるまでの時間	IC

FXC9324XG Management Guide(CLI)
(FXC14-DC-200002-R1.3)

初版	2014 年 1 月
第二版	2014 年 8 月
第三版	2015 年 8 月
第四版	2017 年 2 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
FXC9324XG

Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide

FXC9324XG Management(CLI)

FXC14-DC-200002-R1.3

FXC株式会社